




CLI Reference Guide

T2500G-10TS (TL-SG3210)

1910012120 REV1.1.0

May 2017

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice.  tp-link is a registered trademark of TP-Link Technologies Co., Ltd. Other brands and product names are trademarks or registered trademarks of their respective holders.

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-Link Technologies Co., Ltd. Copyright © 2017 TP-Link Technologies Co., Ltd. All rights reserved.

<http://www.tp-link.com>

CONTENTS

Preface	1
Chapter 1 Using the CLI	4
1.1 Accessing the CLI	4
1.1.1 Logon by a console port	4
1.1.2 Logon by Telnet	6
1.1.3 Logon by SSH	10
1.2 CLI Command Modes	15
1.3 Privilege Restrictions	18
1.4 Conventions	19
1.4.1 Format Conventions	19
1.4.2 Special Characters	19
1.4.3 Parameter Format	19
Chapter 2 User Interface	20
2.1 enable	20
2.2 enable-admin	20
2.3 service password-encryption	21
2.4 enable password	22
2.5 enable secret	23
2.6 configure	24
2.7 exit	24
2.8 end	25
2.9 clipaging	25
2.10 show history	26
2.11 clear history	26
Chapter 3 IEEE 802.1Q VLAN Commands	28
3.1 vlan	28
3.2 interface vlan	29
3.3 name	29
3.4 switchport mode	30
3.5 switchport access vlan	31
3.6 switchport trunk allowed vlan	31
3.7 switchport trunk allowed vlan all	32

3.8	switchport general allowed vlan	33
3.9	switchport pvid	34
3.10	show vlan summary.....	34
3.11	show vlan brief.....	35
3.12	show vlan.....	35
3.13	show interface switchport.....	36
Chapter 4	MAC-based VLAN Commands.....	37
4.1	mac-vlan mac-address.....	37
4.2	mac-vlan	38
4.3	show mac-vlan.....	38
Chapter 5	Protocol-based VLAN Commands	40
5.1	protocol-vlan template	40
5.2	protocol-vlan vlan.....	41
5.3	protocol-vlan group.....	42
5.4	show protocol-vlan template.....	42
5.5	show protocol-vlan vlan	43
Chapter 6	VLAN-VPN Commands	44
6.1	dot1q-tunnel.....	44
6.2	dot1q-tunnel tpid.....	44
6.3	dot1q-tunnel mapping	45
6.4	switchport dot1q-tunnel mapping.....	46
6.5	switchport dot1q-tunnel missdrop.....	47
6.6	switchport dot1q-tunnel mode.....	47
6.7	show dot1q-tunnel.....	48
6.8	show dot1q-tunnel mapping.....	49
6.9	show dot1q-tunnel interface	49
Chapter 7	Voice VLAN Commands	50
7.1	voice vlan.....	50
7.2	voice vlan aging time	50
7.3	voice vlan priority.....	51
7.4	voice vlan mac-address	52
7.5	switchport voice vlan mode	53
7.6	switchport voice vlan security	53
7.7	show voice vlan	54
7.8	show voice vlan oui	54

7.9	show voice vlan switchport.....	55
Chapter 8	L2PT Commands	56
8.1	l2protocol-tunnel.....	56
8.2	l2protocol-tunnel type.....	56
8.3	show l2protocol-tunnel global	58
8.4	show l2protocol-tunnel interface.....	58
Chapter 9	GVRP Commands.....	60
9.1	gvrp.....	60
9.2	gvrp (interface).....	60
9.3	gvrp registration.....	61
9.4	gvrp timer	62
9.5	show gvrp interface	63
9.6	show gvrp global.....	64
Chapter 10	Etherchannel Commands	65
10.1	channel-group	65
10.2	port-channel load-balance.....	66
10.3	lacp system-priority.....	67
10.4	lacp port-priority	67
10.5	show etherchannel.....	68
10.6	show etherchannel load-balance.....	69
10.7	show lacp.....	69
10.8	show lacp sys-id.....	70
Chapter 11	User Management Commands.....	71
11.1	user name (password).....	71
11.2	user name (secret).....	72
11.3	user access-control ip-based.....	73
11.4	user access-control mac-based.....	74
11.5	user access-control port-based	75
11.6	line.....	76
11.7	password.....	77
11.8	login.....	78
11.9	login local.....	79
11.10	media-type rj45	79
11.11	telnet	80
11.12	show user account-list.....	81

11.13	show user configuration.....	81
11.14	show telnet-status.....	82
Chapter 12 HTTP and HTTPS Commands		83
12.1	ip http server	83
12.2	ip http max-users.....	84
12.3	ip http session timeout	84
12.4	ip http secure-server	85
12.5	ip http secure-protocol.....	86
12.6	ip http secure-ciphersuite	86
12.7	ip http secure-max-users	87
12.8	ip http secure-session timeout.....	88
12.9	ip http secure-server download certificate	89
12.10	ip http secure-server download key	90
12.11	show ip http configuration.....	91
12.12	show ip http secure-server	91
Chapter 13 Binding Table Commands.....		92
13.1	ip source binding	92
13.2	ip source binding index.....	93
13.3	ip dhcp snooping	94
13.4	ip dhcp snooping global	95
13.5	ip dhcp snooping information option.....	96
13.6	ip dhcp snooping information strategy.....	96
13.7	ip dhcp snooping information format.....	97
13.8	ip dhcp snooping information remote-id.....	98
13.9	ip dhcp snooping information circuit-id.....	99
13.10	ip dhcp snooping trust.....	100
13.11	ip dhcp snooping mac-verify.....	100
13.12	ip dhcp snooping limit rate	101
13.13	ip dhcp snooping decline.....	102
13.14	show ip source binding.....	102
13.15	show ip dhcp snooping information.....	103
13.16	show ip dhcp snooping interface gigabitEthernet.....	103
Chapter 14 ARP Inspection Commands.....		105
14.1	ip arp inspection(global)	105
14.2	ip arp inspection trust	105
14.3	ip arp inspection(interface).....	106

14.4	ip arp inspection limit-rate.....	107
14.5	ip arp inspection recover.....	108
14.6	show ip arp inspection.....	108
14.7	show ip arp inspection interface.....	109
14.8	show ip arp inspection statistics.....	109
14.9	clear ip arp inspection statistics.....	110
Chapter 15 DoS Defend Commands.....		111
15.1	ip dos-prevent.....	111
15.2	ip dos-prevent type.....	111
15.3	show ip dos-prevent.....	112
Chapter 16 IEEE 802.1X Commands.....		114
16.1	dot1x system-auth-control.....	114
16.2	dot1x handshake.....	115
16.3	dot1x auth-method.....	115
16.4	dot1x accounting.....	116
16.5	dot1x vlan-assignment.....	117
16.6	dot1x guest-vlan(global).....	118
16.7	dot1x quiet-period.....	118
16.8	dot1x timeout supplicant-timeout.....	119
16.9	dot1x max-reauth-req.....	120
16.10	dot1x.....	121
16.11	dot1x guest-vlan(interface).....	121
16.12	dot1x mab.....	122
16.13	dot1x port-control.....	123
16.14	dot1x port-method.....	124
16.15	show dot1x global.....	125
16.16	show dot1x interface.....	125
Chapter 17 PPPoE ID-Insertion Commands.....		127
17.1	pppoe id-insertion(global).....	127
17.2	pppoe circuit-id(interface).....	128
17.3	pppoe circuit-id type.....	128
17.4	pppoe remote-id.....	129
17.5	show pppoe id-insertion global.....	130
17.6	show pppoe id-insertion interface.....	130

Chapter 18 System Log Commands	132
18.1 logging buffer	132
18.2 logging file flash	133
18.3 logging file flash frequency	133
18.4 logging file flash level	134
18.5 logging host index	135
18.6 clear logging	136
18.7 show logging local-config	136
18.8 show logging loghost	137
18.9 show logging buffer	137
18.10 show logging flash	138
Chapter 19 SSH Commands	139
19.1 ip ssh server	139
19.2 ip ssh version	139
19.3 ip ssh algorithm	140
19.4 ip ssh timeout	141
19.5 ip ssh max-client	141
19.6 ip ssh download	142
19.7 remove public-key	143
19.8 show ip ssh	143
Chapter 20 MAC Address Commands	145
20.1 mac address-table static	145
20.2 mac address-table aging-time	146
20.3 mac address-table filtering	146
20.4 mac address-table max-mac-count	147
20.5 show mac address-table	148
20.6 clear mac address-table	149
20.7 show mac address-table aging-time	149
20.8 show mac address-table max-mac-count	150
20.9 show mac address-table interface	151
20.10 show mac address-table count	151
20.11 show mac address-table address	152
20.12 show mac address-table vlan	152
Chapter 21 System Configuration Commands	153
21.1 system-time manual	153

21.2	system-time ntp	153
21.3	system-time dst predefined	155
21.4	system-time dst date	156
21.5	system-time dst recurring	157
21.6	hostname.....	158
21.7	location.....	158
21.8	contact-info	159
21.9	reset	160
21.10	reboot	160
21.11	copy running-config startup-config.....	161
21.12	copy startup-config tftp	161
21.13	copy tftp startup-config	162
21.14	boot application	163
21.15	remove backup-image.....	163
21.16	firmware upgrade.....	164
21.17	ping.....	165
21.18	tracert	166
21.19	show system-info	167
21.20	show boot.....	167
21.21	show running-config.....	168
21.22	show running-config 	168
21.23	show startup-config	169
21.24	show system-time	169
21.25	show system-time dst.....	170
21.26	show system-time ntp	170
21.27	show cable-diagnostics interface gigabitEthernet.....	171
21.28	show cable-diagnostics careful interface.....	171
Chapter 22 IPv6 Address Configuration Commands		173
22.1	ipv6 enable.....	173
22.2	ipv6 address autoconfig.....	173
22.3	ipv6 address link-local	174
22.4	ipv6 address dhcp	175
22.5	ipv6 address ra	175
22.6	ipv6 address eui-64	176
22.7	ipv6 address	177
22.8	show ipv6 interface	178

Chapter 23 Ethernet Configuration Commands.....	179
23.1 interface gigabitEthernet.....	179
23.2 interface range gigabitEthernet.....	179
23.3 description.....	180
23.4 shutdown.....	181
23.5 flow-control	182
23.6 duplex.....	182
23.7 speed.....	183
23.8 storm-control.....	184
23.9 bandwidth.....	184
23.10 clear counters.....	185
23.11 show interface status.....	186
23.12 show interface counters	186
23.13 show interface configuration.....	187
23.14 show storm-control	187
23.15 show bandwidth	188
Chapter 24 QoS Commands.....	189
24.1 qos.....	189
24.2 qos dscp.....	190
24.3 qos queue cos-map.....	190
24.4 qos queue dscp-map	191
24.5 qos queue mode	192
24.6 show qos interface.....	193
24.7 show qos cos-map.....	194
24.8 show qos dscp-map	194
24.9 show qos queue mode.....	195
24.10 show qos status	195
Chapter 25 Port Mirror Commands.....	197
25.1 monitor session destination interface.....	197
25.2 monitor session source interface.....	198
25.3 show monitor session	199
Chapter 26 Port Isolation Commands	200
26.1 port isolation.....	200
26.2 show port isolation interface	201

Chapter 27	Loopback Detection Commands	202
27.1	loopback-detection(global)	202
27.2	loopback-detection interval	202
27.3	loopback-detection recovery-time	203
27.4	loopback-detection(interface)	204
27.5	loopback-detection config	204
27.6	loopback-detection recover	205
27.7	show loopback-detection global	206
27.8	show loopback-detection interface	206
Chapter 28	ACL Commands	208
28.1	time-range	208
28.2	absolute	208
28.3	periodic	209
28.4	holiday	210
28.5	holiday(global)	211
28.6	access-list create	211
28.7	mac access-list	212
28.8	access-list standard	213
28.9	access-list extended	214
28.10	rule	215
28.11	access-list policy name	216
28.12	access-list policy action	217
28.13	redirect interface	218
28.14	s-condition	218
28.15	s-mirror	219
28.16	qos-remark	220
28.17	access-list bind(interface)	221
28.18	access-list bind(vlan)	221
28.19	show access-list	222
28.20	show access-list status	222
28.21	show access-list policy	223
28.22	show access-list bind	223
Chapter 29	MSTP Commands	225
29.1	spanning-tree(global)	225
29.2	spanning-tree(interface)	225
29.3	spanning-tree common-config	226

29.4	spanning-tree mode	227
29.5	spanning-tree mst configuration	228
29.6	instance.....	228
29.7	name.....	229
29.8	revision.....	230
29.9	spanning-tree mst instance.....	231
29.10	spanning-tree mst.....	231
29.11	spanning-tree priority	232
29.12	spanning-tree tc-defend.....	233
29.13	spanning-tree timer	234
29.14	spanning-tree hold-count.....	235
29.15	spanning-tree max-hops.....	235
29.16	spanning-tree bpdudfilter	236
29.17	spanning-tree bpduguard.....	236
29.18	spanning-tree guard loop	237
29.19	spanning-tree guard root.....	238
29.20	spanning-tree guard tc	238
29.21	spanning-tree mcheck.....	239
29.22	show spanning-tree active	240
29.23	show spanning-tree bridge	240
29.24	show spanning-tree interface	241
29.25	show spanning-tree interface-security	241
29.26	show spanning-tree mst	242
Chapter 30 DLDP Commands		244
30.1	dldp(global)	244
30.2	dldp interval	244
30.3	dldp shut-mode.....	245
30.4	dldp reset(global).....	246
30.5	dldp(interface).....	246
30.6	dldp reset(interface)	247
30.7	show dldp	247
30.8	show dldp interface.....	248
Chapter 31 IGMP Snooping Commands.....		249
31.1	ip igmp snooping(global).....	249
31.2	ip igmp snooping(interface)	249
31.3	ip igmp snooping report-suppression.....	250

31.4	ip igmp snooping immediate-leave	251
31.5	ip igmp snooping drop-unknown	251
31.6	ip igmp snooping vlan-config	252
31.7	ip igmp snooping multi-vlan-config.....	253
31.8	ip igmp snooping filter(global).....	255
31.9	ip igmp snooping filter(interface).....	255
31.10	ip igmp snooping filter add-id.....	256
31.11	ip igmp snooping filter maxgroup	257
31.12	ip igmp snooping filter mode.....	257
31.13	ip igmp snooping querier vlan	258
31.14	ip igmp snooping querier vlan (general query)	259
31.15	ip igmp snooping querier vlan (specific query).....	260
31.16	ip igmp snooping authentication.....	261
31.17	ip igmp snooping accounting.....	262
31.18	clear ip igmp snooping statistics	262
31.19	show ip igmp snooping.....	263
31.20	show ip igmp snooping interface	263
31.21	show ip igmp snooping vlan.....	264
31.22	show ip igmp snooping multi-vlan	264
31.23	show ip igmp snooping groups.....	265
31.24	show ip igmp snooping querier.....	266
Chapter 32 MLD Snooping Commands.....		267
32.1	ipv6 mld snooping	267
32.2	ipv6 mld snooping router-aging-time.....	267
32.3	ipv6 mld snooping member-aging-time	268
32.4	ipv6 mld snooping report-suppression	269
32.5	ipv6 mld snooping unknown-filter	269
32.6	ipv6 mld snooping last-listener query-inteval	270
32.7	ipv6 mld snooping last-listener query-count.....	270
32.8	ipv6 mld snooping multicast-vlan	271
32.9	ipv6 mld snooping multicast-vlan vlan-id.....	272
32.10	ipv6 mld snooping vlan.....	272
32.11	ipv6 mld snooping vlan router-aging-time.....	273
32.12	ipv6 mld snooping vlan member-aging-time	274
32.13	ipv6 mld snooping vlan immediate-leave.....	274
32.14	ipv6 mld snooping vlan mrouter	275
32.15	ipv6 mld snooping vlan static	276

32.16	ipv6 mld snooping querier vlan.....	276
32.17	ipv6 mld snooping querier vlan max-response-time.....	277
32.18	ipv6 mld snooping querier vlan query-interval.....	278
32.19	ipv6 mld snooping querier vlan query-source.....	278
32.20	ipv6 mld snooping filter(global).....	279
32.21	ipv6 mld snooping filter(interface).....	280
32.22	ipv6 mld snooping filter-mode.....	280
32.23	ipv6 mld snooping filter-id.....	281
32.24	ipv6 mld snooping max-group.....	282
32.25	clear ipv6 mld snooping statistics.....	282
32.26	show ipv6 mld snooping.....	283
32.27	show ipv6 mld snooping vlan.....	283
32.28	show ipv6 mld snooping static-mcast.....	284
32.29	show ipv6 mld snooping group.....	284
32.30	show ipv6 mld snooping filter.....	285
32.31	show ipv6 mld snooping interface.....	285
32.32	show ipv6 mld snooping interface filter.....	286
32.33	show ipv6 mld snooping querier.....	286
32.34	show ipv6 mld snooping statistics.....	287
Chapter 33 SNMP Commands		288
33.1	snmp-server.....	288
33.2	snmp-server view.....	288
33.3	snmp-server group.....	289
33.4	snmp-server user.....	291
33.5	snmp-server community.....	292
33.6	snmp-server host.....	293
33.7	snmp-server engineID.....	295
33.8	snmp-server traps snmp.....	295
33.9	snmp-server traps link-status.....	296
33.10	snmp-server traps.....	297
33.11	snmp-server traps mac.....	298
33.12	snmp-server traps vlan.....	299
33.13	rmon history.....	300
33.14	rmon event.....	301
33.15	rmon alarm.....	302
33.16	rmon statistics.....	303
33.17	show snmp-server.....	304

33.18	show snmp-server view.....	305
33.19	show snmp-server group.....	305
33.20	show snmp-server user.....	306
33.21	show snmp-server community	306
33.22	show snmp-server host.....	306
33.23	show snmp-server engineID.....	307
33.24	show rmon history.....	307
33.25	show rmon event	308
33.26	show rmon alarm.....	309
33.27	show rmon statistics	309
Chapter 34 LLDP Commands.....		311
34.1	lldp.....	311
34.2	lldp hold-multiplier	311
34.3	lldp timer	312
34.4	lldp receive.....	313
34.5	lldp transmit.....	314
34.6	lldp snmp-trap.....	314
34.7	lldp tlv-select.....	315
34.8	lldp med-fast-count.....	316
34.9	lldp med-status.....	316
34.10	lldp med-tlv-select	317
34.11	lldp med-location.....	318
34.12	show lldp.....	319
34.13	show lldp interface	319
34.14	show lldp local-information interface	320
34.15	show lldp neighbor-information interface.....	320
34.16	show lldp traffic interface	321
Chapter 35 AAA Commands		322
35.1	aaa enable	322
35.2	enable admin password.....	323
35.3	enable admin secret	324
35.4	tacacs-server host.....	325
35.5	show tacacs-server	326
35.6	radius-server host	327
35.7	show radius-server	328
35.8	aaa group.....	329

35.9	server	329
35.10	show aaa group	330
35.11	aaa authentication login	331
35.12	aaa authentication enable.....	332
35.13	aaa authentication dot1x default.....	333
35.14	aaa accounting dot1x default.....	333
35.15	show aaa authentication	334
35.16	show aaa accounting.....	335
35.17	line console.....	335
35.18	login authentication(console).....	336
35.19	enable authentication(console)	337
35.20	line telnet	337
35.21	login authentication(telnet).....	338
35.22	line ssh.....	339
35.23	login authentication(ssh).....	339
35.24	enable authentication(telnet).....	340
35.25	enable authentication(ssh)	341
35.26	ip http login authentication.....	341
35.27	ip http enable authentication.....	342
35.28	show aaa global.....	343
Chapter 36 DHCP Relay Commands		344
36.1	ip dhcp relay	344
36.2	ip dhcp relay information option.....	344
36.3	ip dhcp relay information strategy.....	345
36.4	ip dhcp relay information format	346
36.5	ip dhcp relay information circuit-id.....	346
36.6	ip dhcp relay information remote-id.....	347
36.7	ip dhcp relay vlan	348
36.8	show ip dhcp relay.....	348

Preface

This Guide is intended for network administrator to provide referenced information about CLI (Command Line Interface). The device mentioned in this Guide stands for T2500G-10TS JetStream 8-Port Gigabit L2 Managed Switch with 2 SFP Slots without any explanation.

Overview of this Guide

Chapter 1: Using the CLI

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

Chapter 2: User Interface

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

Chapter 3: IEEE 802.1Q VLAN Commands

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

Chapter 4: MAC-based VLAN Commands

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

Chapter 5: Protocol-based VLAN Commands

Provide information about the commands used for configuring Protocol VLAN.

Chapter 6: VLAN-VPN Commands

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

Chapter 7: Voice VLAN Commands

Provide information about the commands used for configuring Voice VLAN.

Chapter 8: L2PT Commands

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

Chapter 9: GVRP Commands

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

Chapter 10: Etherchannel Commands

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

Chapter 11: User Management Commands

Provide information about the commands used for user management.

Chapter 12: HTTP and HTTPS Commands

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

Chapter 13: Binding Table Commands

Provide information about the commands used for binding the IP address, MAC address, VLAN and the connected Port number of the Host together. Besides it also provide information about the commands used for monitoring the process of the Host obtaining the IP address from DHCP server, and record the IP address, MAC address, VLAN and the connected Port number of the Host for automatic binding.

Chapter 14: ARP Inspection Commands

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

Chapter 15: DoS Defend Command

Provide information about the commands used for DoS defend and detecting the DoS attack.

Chapter 16: IEEE 802.1X Commands

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

Chapter 17: PPPoE ID Insertion Commands

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

Chapter 18: System Log Commands

Provide information about the commands used for configuring system log.

Chapter 19: SSH Commands

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

Chapter 20: MAC Address Commands

Provide information about the commands used for Address configuration.

Chapter 21: System Configuration Commands

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

Chapter 22: IPv6 Address Configuration Commands

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

Chapter 23: Ethernet Configuration Commands

Provide information about the commands used for configuring the Bandwidth Control, Negotiation Mode, and Storm Control for ethernet ports.

Chapter 24: QoS Commands

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

Chapter 25: Port Mirror Commands

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

Chapter 26: Port Isolation Commands

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

Chapter 27: Loopback Detection Commands

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

Chapter 28: ACL Commands

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

Chapter 29: MSTP Commands

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

Chapter 30: DLDP Commands

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

Chapter 31: IGMP Snooping Commands

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

Chapter 32: MLD Snooping Commands

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

Chapter 33: SNMP Commands

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

Chapter 34: LLDP Commands

Provide information about the commands used for configuring LLDP function.

Chapter 35: AAA Commands

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

Chapter 36: DHCP Relay Commands

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

Chapter 1 Using the CLI

1.1 Accessing the CLI

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

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

1.1.1 Logon by a console port

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

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

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

- 32-bit Windows XP SP3
- 64-bit Windows XP
- 32-bit Windows Vista
- 64-bit Windows Vista
- 32-bit Windows 7
- 64-bit Windows 7
- 32-bit Windows 8
- 64-bit Windows 8
- 32-bit Windows 8.1
- 64-bit Windows 8.1

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

➤ Logon

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

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

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

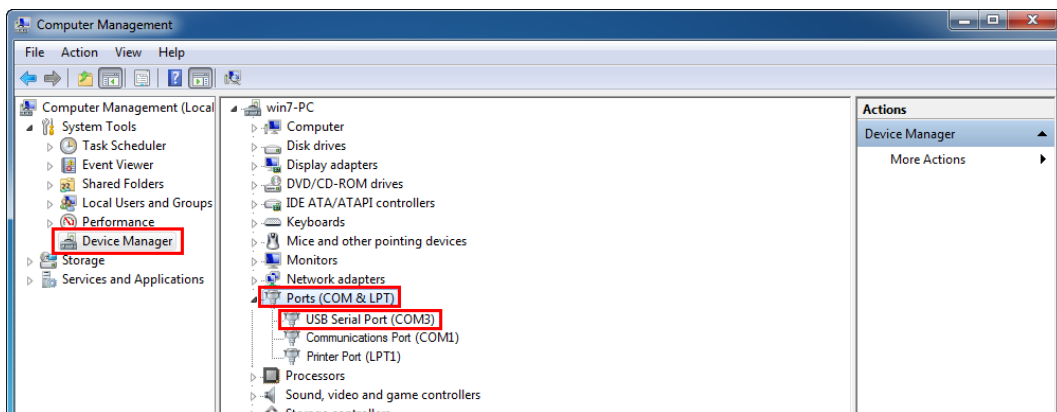


Figure 1-1 USB Serial Port Number

4. Configure the terminal emulation program or the terminal to use the following settings:
 - Baud rate: 38400 bps
 - Data bits: 8
 - Parity: none
 - Stop bits: 1
 - Flow control: none

5. The DOS prompt "T2500G-10TS>" will appear after pressing the Enter button as shown in Figure 1-1. It indicates that you can use the CLI now.

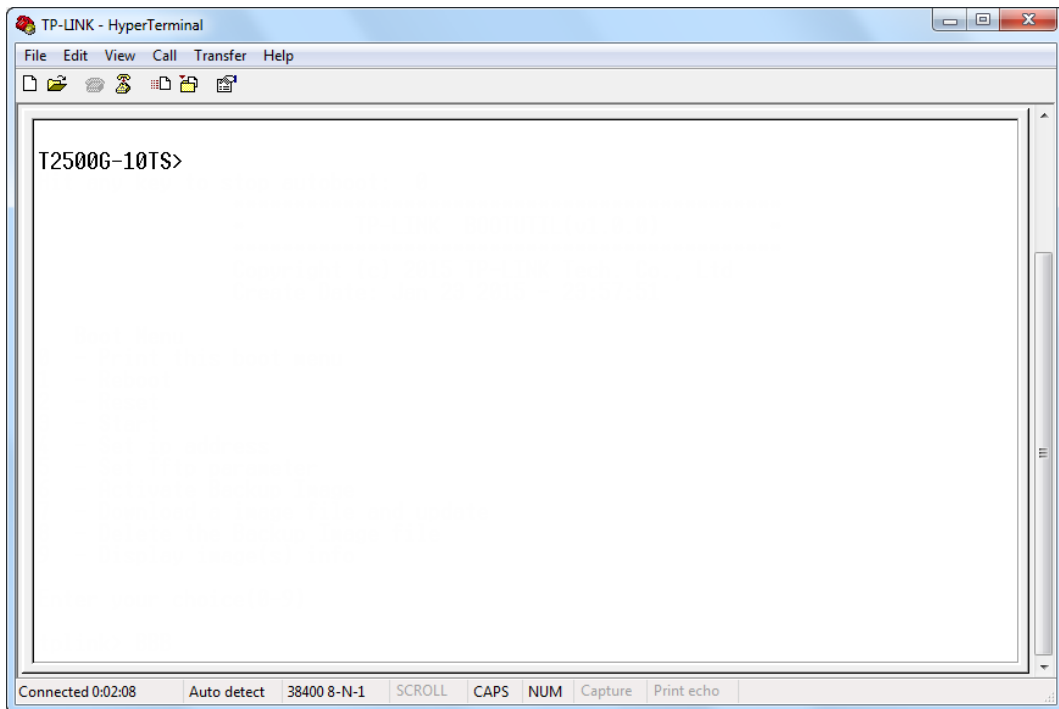


Figure 1-2 Log in the Switch

1.1.2 Logon by Telnet

Telnet login has the following two modes. You can choose one according to your needs:

Login local Mode: It requires username and password, which are both **admin** by default.

Login Mode: It doesn't require username and password, but a connection password is required.

➤ Login Local Mode

Firstly, configure the Telnet login mode as "**login local**" in the prompted DOS screen shown in Figure 1-2.

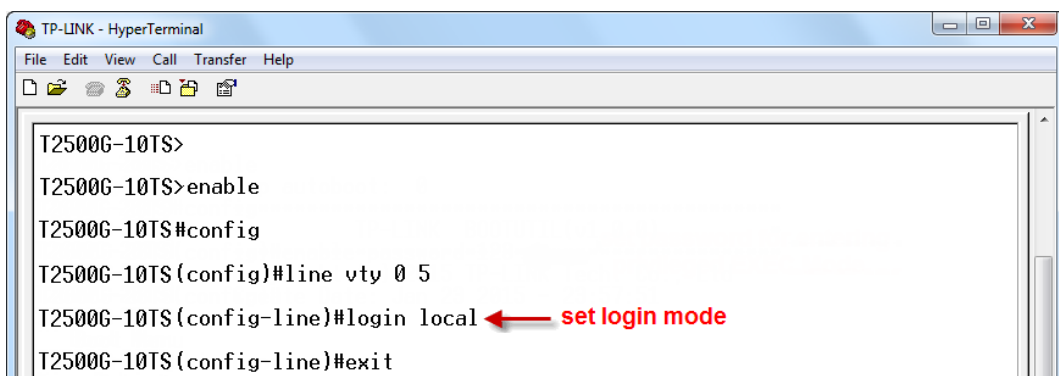


Figure 1-3 Configure login local mode

Now, you can logon by Telnet in **login local** mode.

1. Make sure the switch and the PC are in the same LAN. Click **Start** and type in **cmd** in the Search programs and files window and press the **Enter** button.

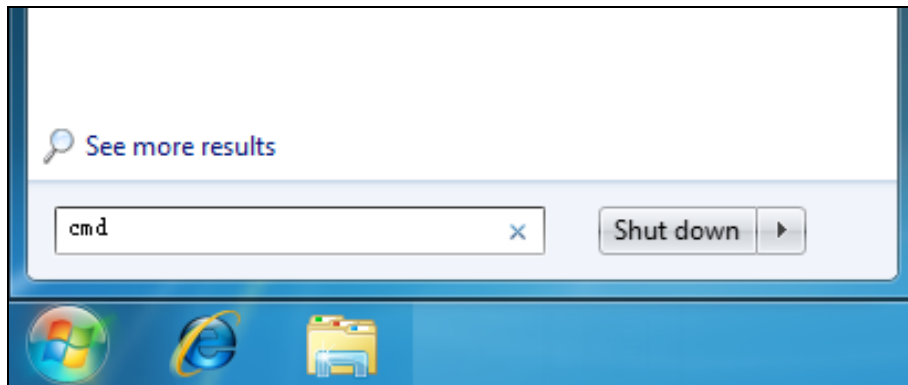


Figure 1-4 Run Window

2. Type **telnet 192.168.0.1** in the command prompt shown as Figure 1-4, and press the **Enter** button.

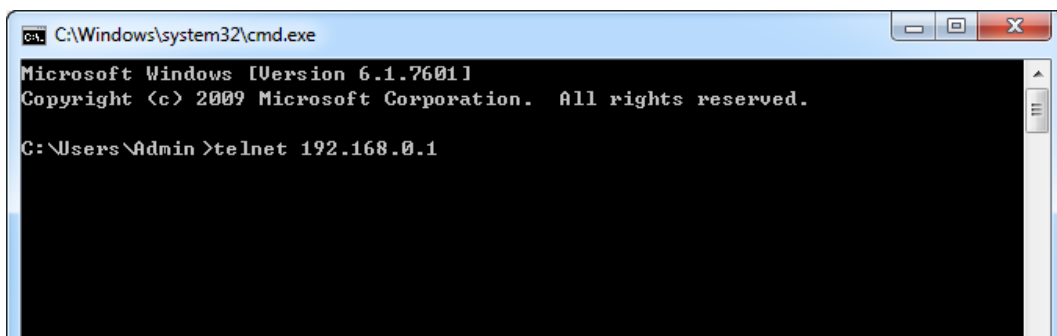


Figure 1-5 Connecting to the Switch

3. Type the default user name and password (both of them are **admin**), then press the **Enter** button so as to enter User EXEC Mode.

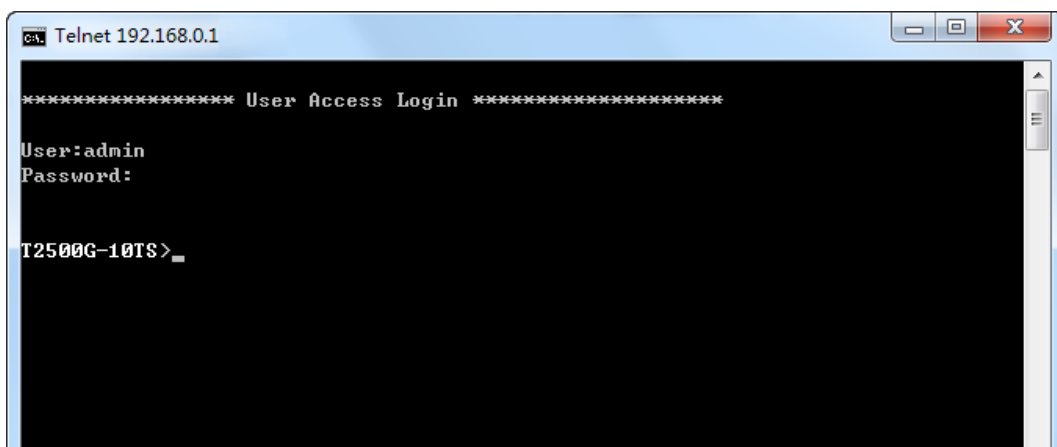


Figure 1-6 Enter into the User EXEC Mode

4. Type **enable** command to enter Privileged EXEC Mode.

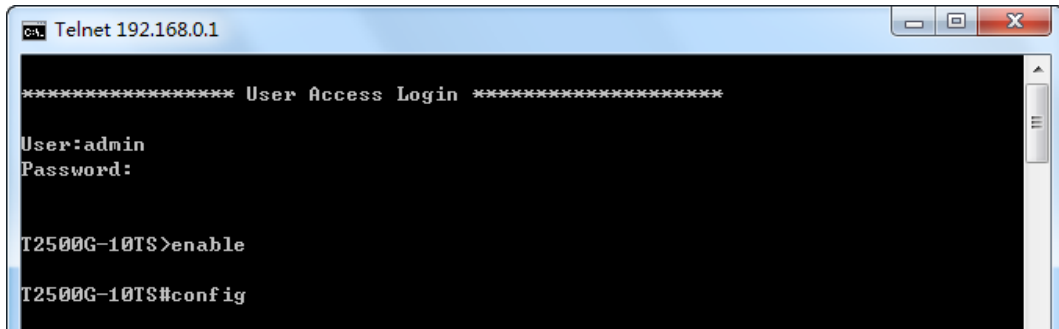


Figure 1-7 Enter into the Priviledged EXEC Mode

Now you can manage your switch with CLI commands through Telnet connection.

➤ Login Mode

Firstly configure the Telnet login mode as "login" and the connection password as **456** in the prompted DOS screen shown in Figure 1-7.

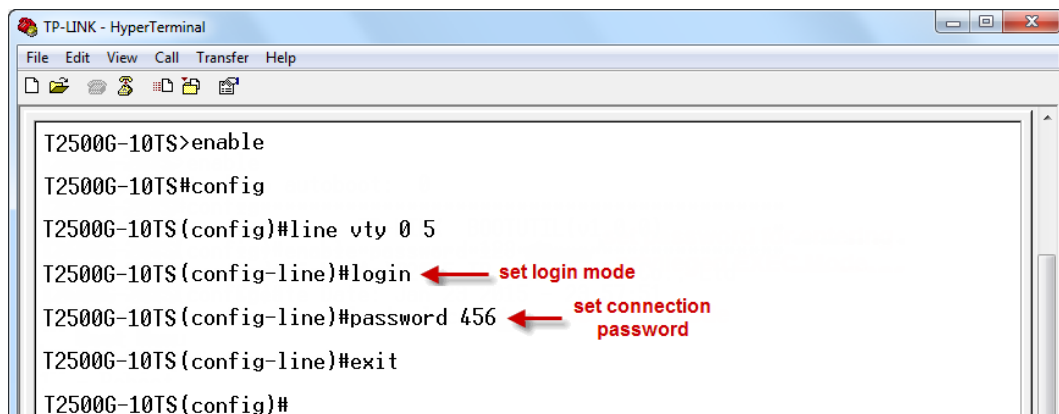


Figure 1-8 Configure login mode

Now, you can logon by Telnet in **login mode**:

1. Make sure the switch and the PC are in the same LAN. Click **Start** and type in **cmd** in the Search programs and files window and press the **Enter** button.

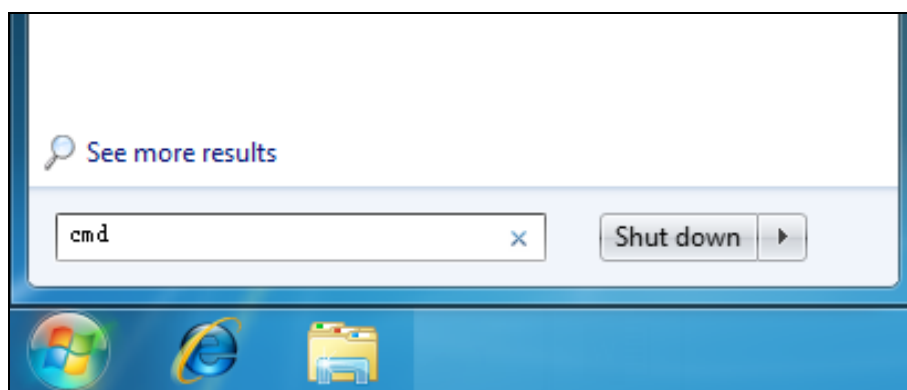


Figure 1-9 Run Window

2. Type **telnet 192.168.0.1** in the command prompt shown as Figure 1-9, and press the **Enter** button.

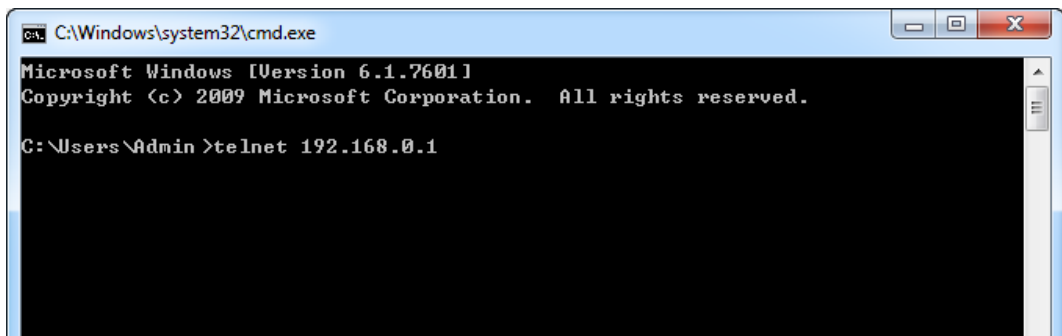


Figure 1-10 Connecting to the Switch

3. You are prompted to enter the connection password **456** you have set through Console port connection, and then you are in User EXEC Mode.

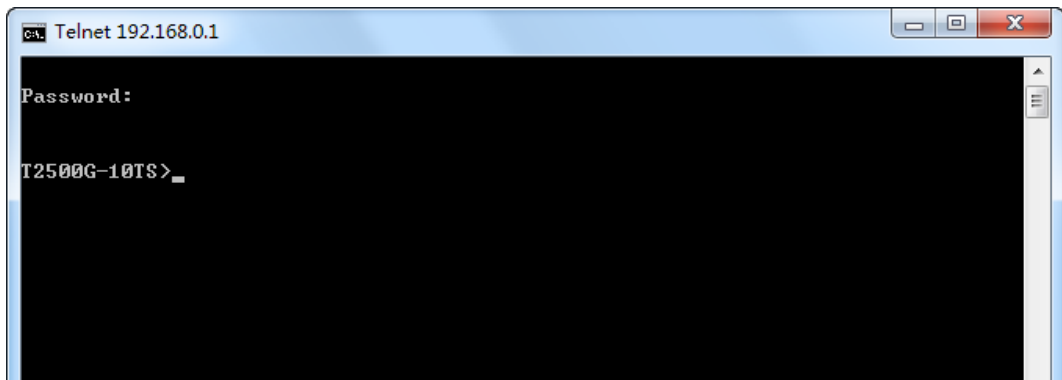


Figure 1-11 Enter into the User EXEC Mode

4. Type **enable** command to enter Privileged EXEC Mode.

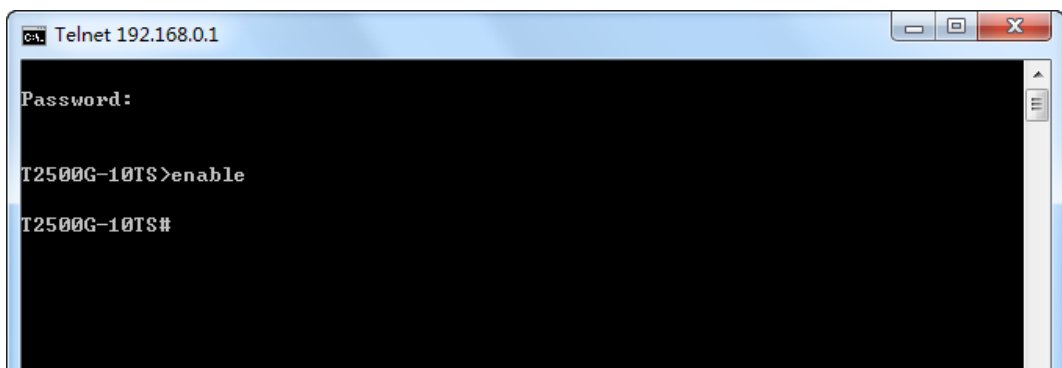


Figure 1-12 Enter into the Privileged EXEC Mode

Now you can view your switch settings with CLI commands through Telnet connection.

 **Note:**

1. Users login via Login Mode are defined as user-level and they have no permission to configure the switch.
2. You can refer to [Chapter 11 User Management Commands](#) for detailed commands information of the Telnet connection configuration.

1.1.3 Logon by SSH

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

Password Authentication Mode: It requires username and password, which are both **admin** by default.

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



Note:

Before SSH login, please follow the steps shown in Figure 1-12 to enable the SSH function through Telnet connection.

```
ca Telnet 192.168.0.1
***** User Access Login *****
User:admin
Password:

T2500G-10TS>enable
T2500G-10TS#config
T2500G-10TS(config)#ip ssh server
T2500G-10TS(config)#_
```

Figure 1-13 Enable SSH function

➤ **Password Authentication Mode**

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

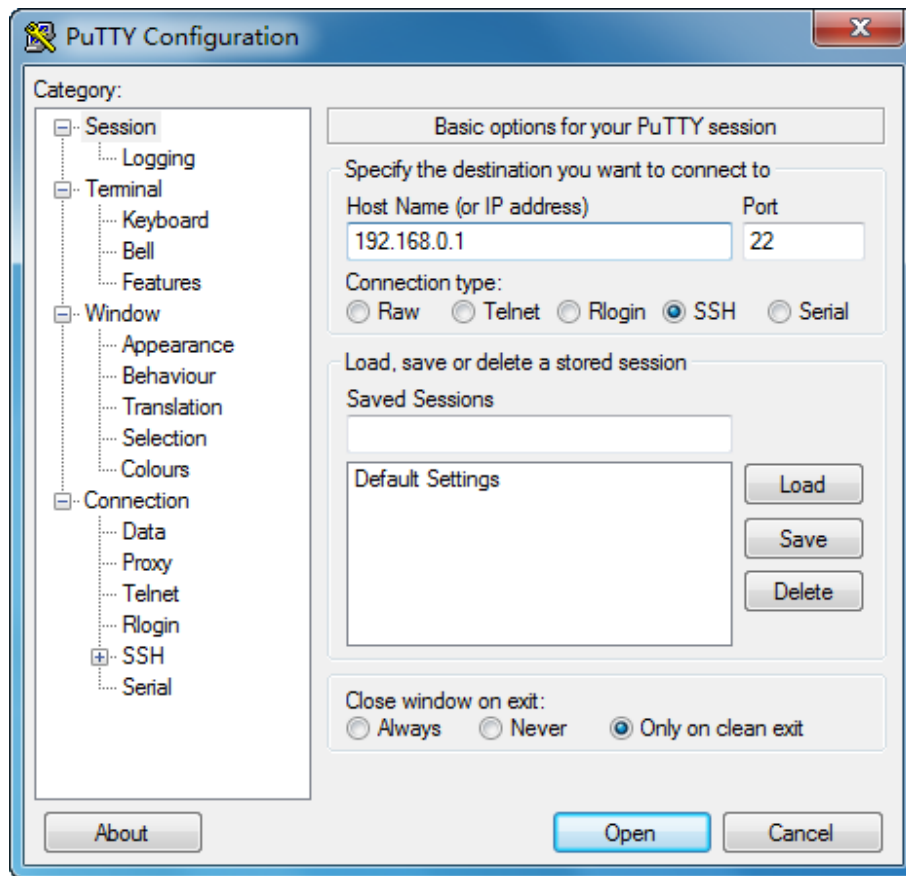


Figure 1-14 SSH Connection Config

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

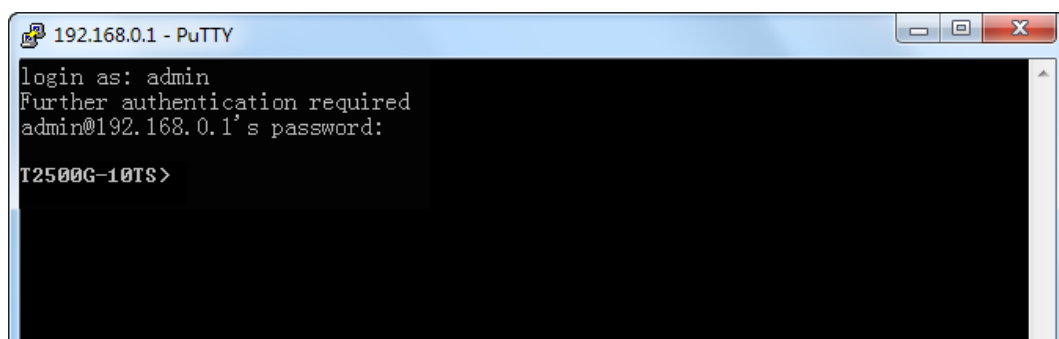


Figure 1-15 Log on the Switch

➤ **Key Authentication Mode**

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

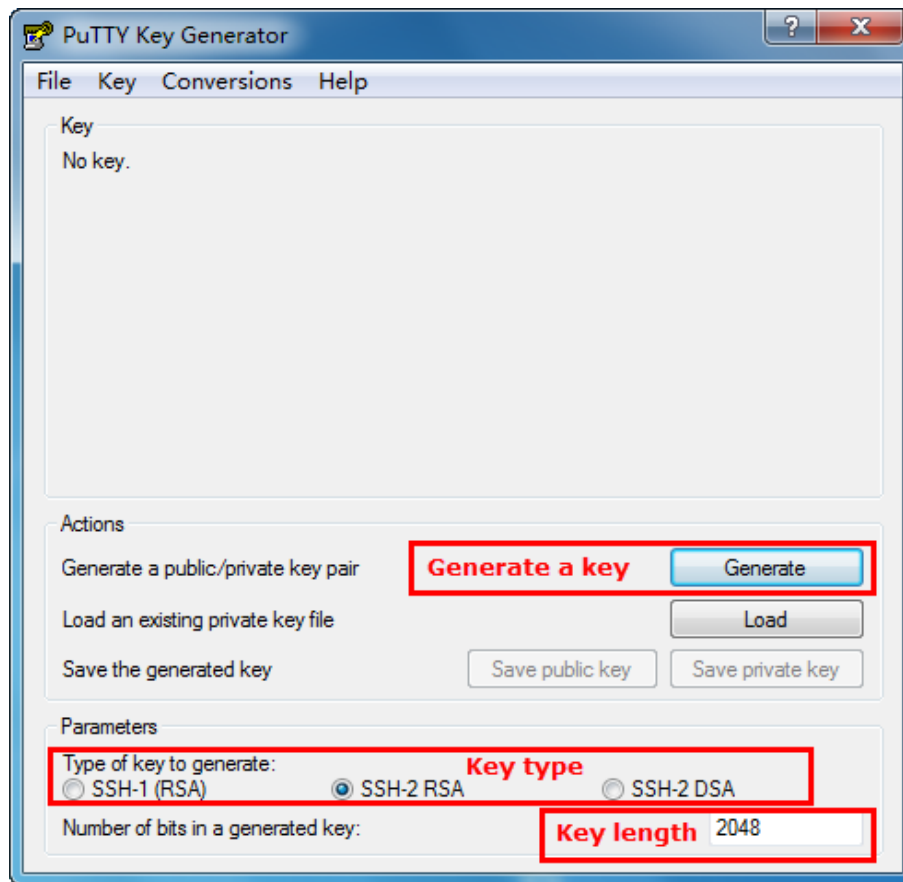


Figure 1-16 Generate SSH Key

 **Note:**

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

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

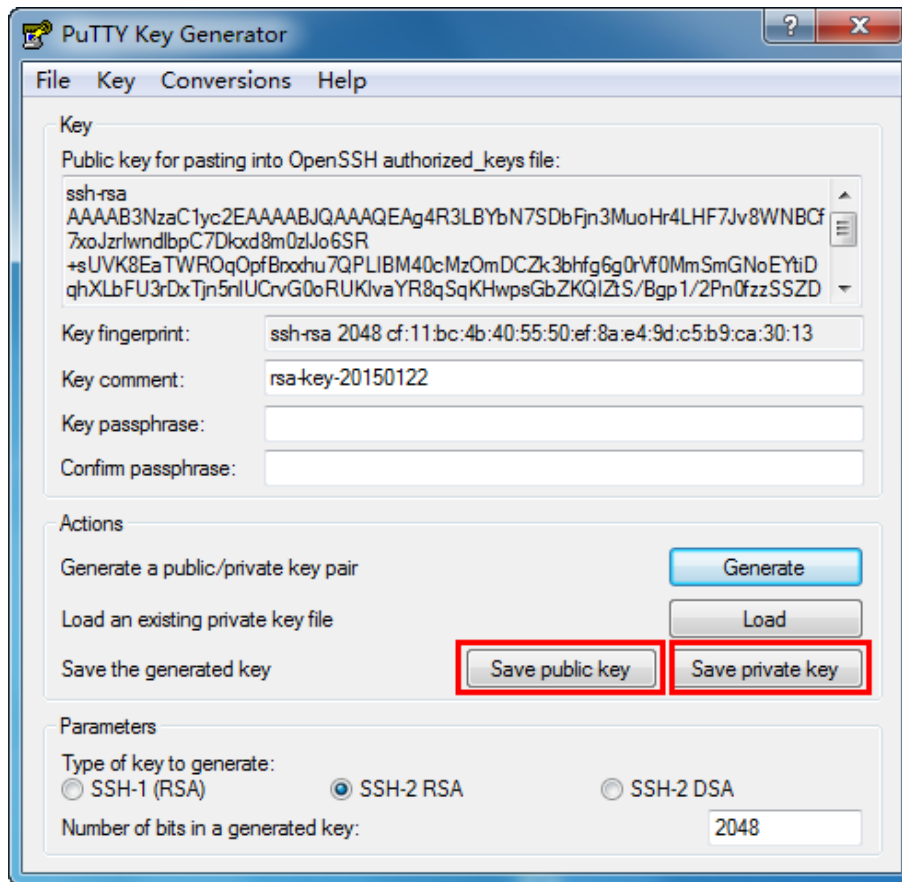


Figure 1-17 Save the Generated Key

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

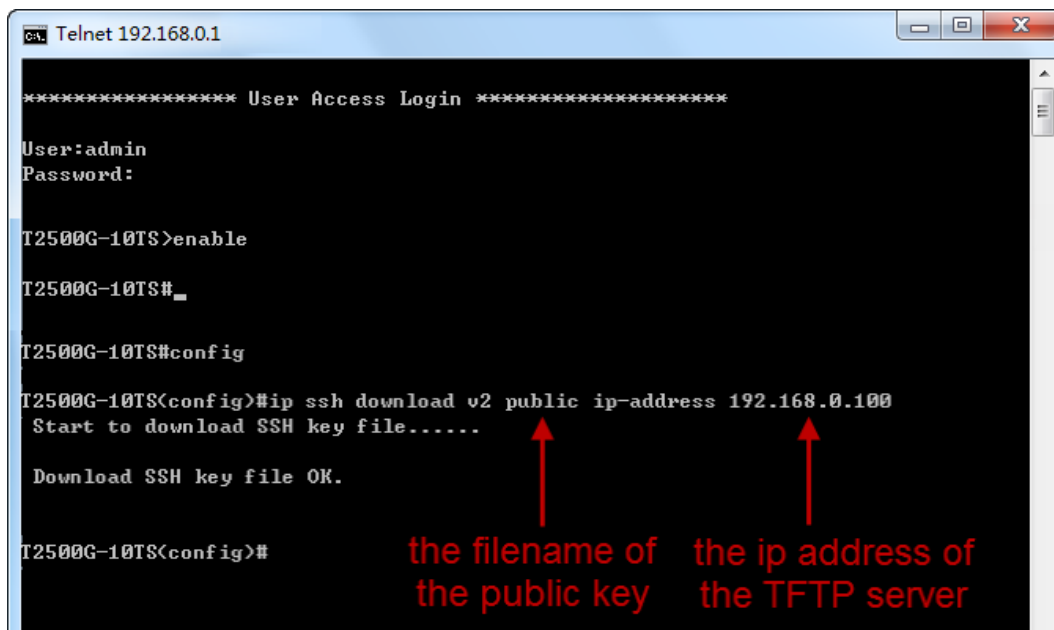


Figure 1-18 Download the Public Key

 **Note:**

1. The key type should accord with the type of the key file.
2. The SSH key downloading can not be interrupted.
4. After the public key is downloaded, please log on to the interface of PuTTY and enter the IP address for login.

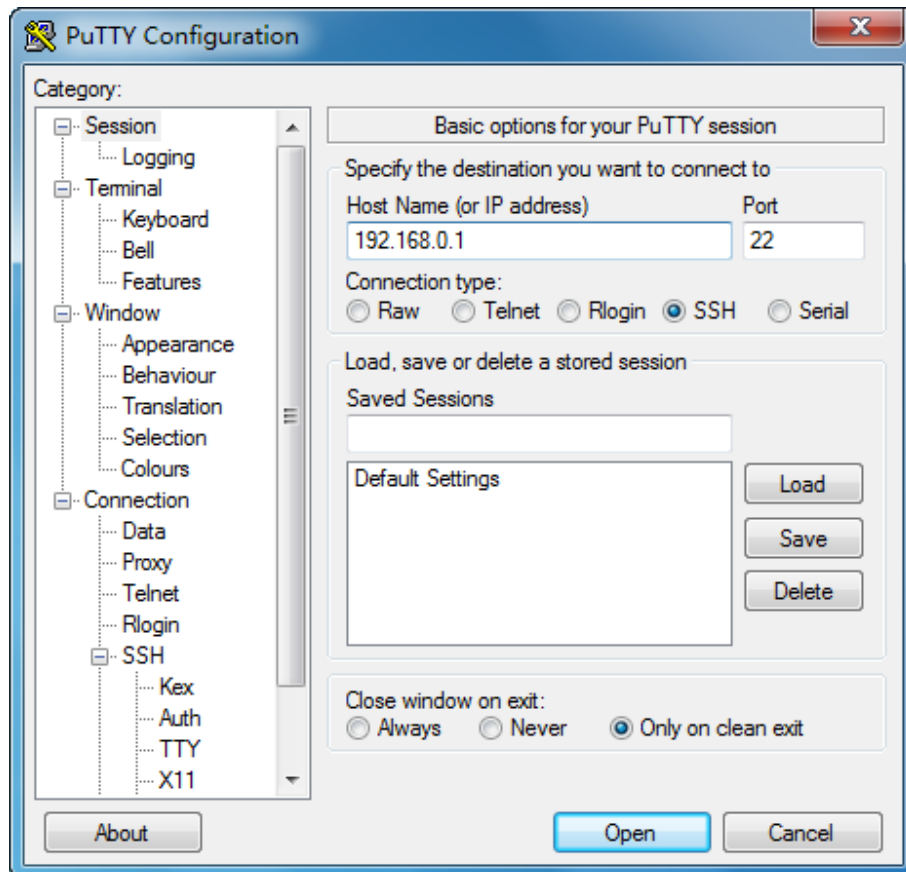


Figure 1-19 SSH Connection Config

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

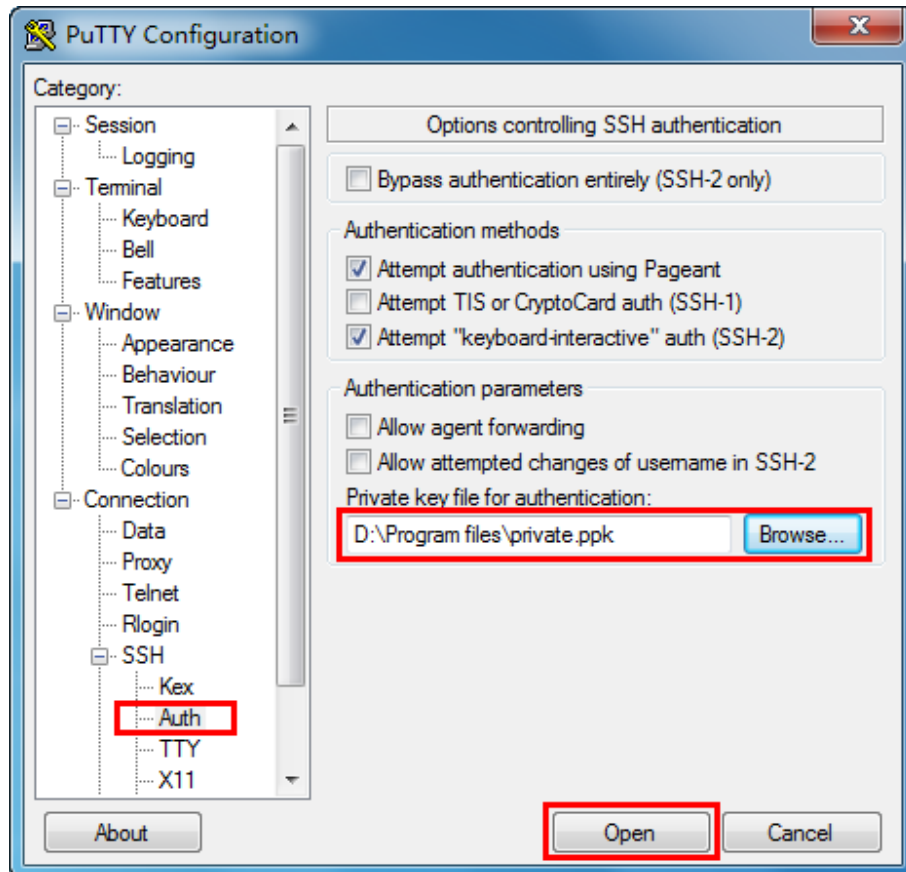


Figure 1-20 Download the Private Key

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

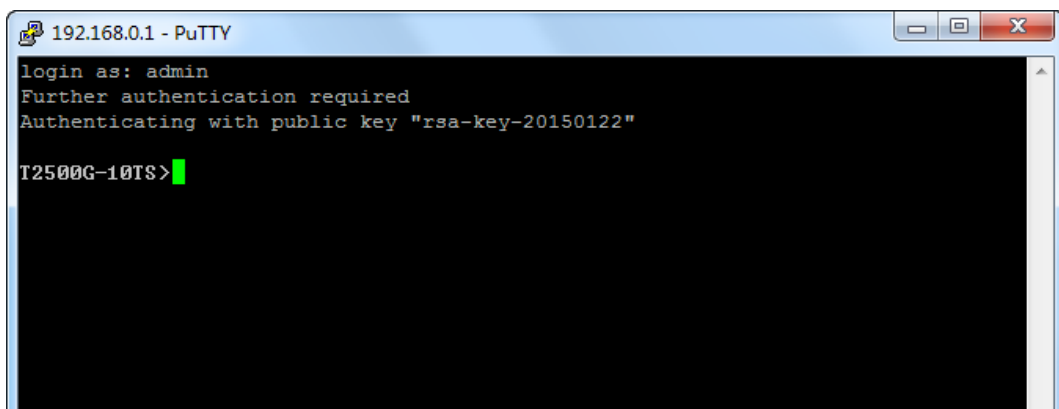
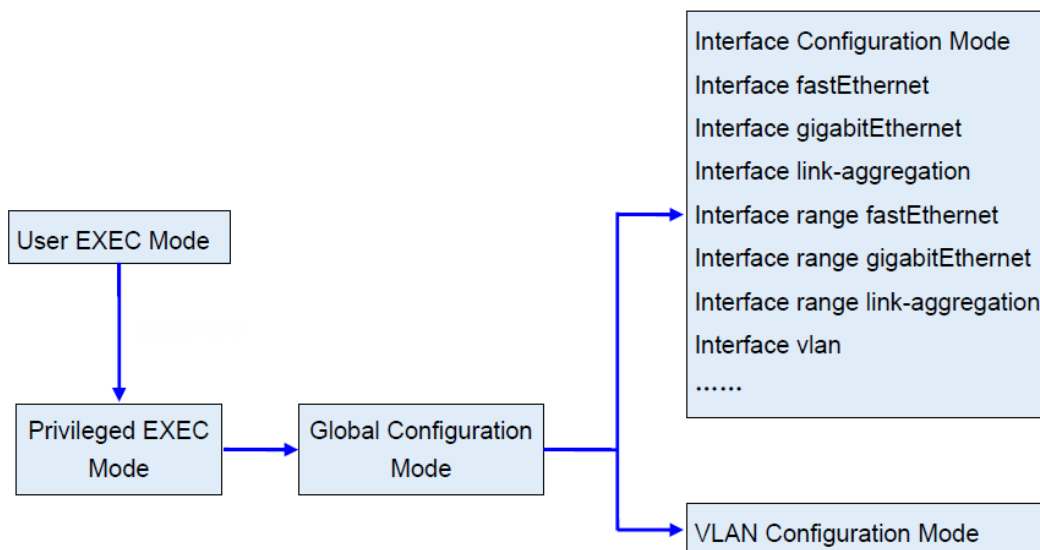


Figure 1-21 Log on the Switch

1.2 CLI Command Modes

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

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



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

Mode	Accessing Path	Prompt	Logout or Access the next mode
User EXEC Mode	Primary mode once it is connected with the switch.	T2500G-10TS>	Use the exit command to disconnect the switch. Use the enable command to access Privileged EXEC mode.
Privileged EXEC Mode	Use the enable command to enter this mode from User EXEC mode.	T2500G-10TS#	Enter the disable or the exit command to return to User EXEC mode. Enter configure command to access Global Configuration mode.
Global Configuration Mode	Use the configure command to enter this mode from Privileged EXEC mode.	T2500G-10TS(config)#	Use the exit or the end command or press Ctrl+Z to return to Privileged EXEC mode. Use the interface gigabitEthernet port or interface range gigabitEthernet port-list command to access Interface Configuration mode. Use the vlan vlan-list to access VLAN Configuration mode.

Mode	Accessing Path	Prompt	Logout or Access the next mode
Interface Configuration Mode	Layer 2 Interface: Use the interface <i>gigabitEthernet port</i> , or interface range <i>gigabitEthernet port-list</i> command to enter this mode from Global Configuration mode.	T2500G-10TS (config-if)# or T2500G-10TS (config-if-range)#	Use the end command or press Ctrl+Z to return to Privileged EXEC mode. Enter the exit or the # command to return to Global Configuration mode. A port number must be specified in the interface command.
Interface Configuration Mode	Layer 3 Interface: Use the no switchport command to enter Routed Port mode from Interface Configuration mode. Use the interface vlan <i>vlan-id</i> command to enter VLAN Interface mode from Global Configuration mode. Use the interface loopback <i>id</i> command to enter Loopback Interface mode from Global Configuration mode.	T2500G-10TS (config-if)# or T2500G-10TS(config-if-range)#	Use the switchport command to switch to the Layer 2 interface mode. Use the end command or press Ctrl+Z to return to Privileged EXEC mode. Enter the exit or the # command to return to Global Configuration mode.
VLAN Configuration Mode	Use the vlan <i>vlan-list</i> command to enter this mode from Global Configuration mode.	T2500G-10TS(config-vlan)#	Use the end command or press Ctrl+Z to return to Privileged EXEC mode. Enter the exit command or the # command to return to Global configuration mode.

 **Note:**

1. The user is automatically in User EXEC Mode after the connection between the PC and the switch is established by a Telnet/SSH connection.
2. Each command mode has its own set of specific commands. To configure some commands, you should access the corresponding command mode firstly.

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

1.3 Privilege Restrictions

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

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

1.4 Conventions

1.4.1 Format Conventions

The following conventions are used in this Guide:

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

1.4.2 Special Characters

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

- These six characters " < > , \ & can not be input.
- If a blank is contained in a character string, single or double quotation marks should be used, for example 'hello world', "hello world", and the words in the quotation marks will be identified as a string. Otherwise, the words will be identified as several strings.

1.4.3 Parameter Format

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

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

Chapter 2 User Interface

2.1 enable

Description

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

Syntax

enable

Command Mode

User EXEC Mode

Privilege Requirement

None.

Example

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

```
T2500G-10TS>enable
Enter password:
T2500G-10TS#
```

2.2 enable-admin

Description

The **enable-admin** command is used to evaluate the current log-in user to the Admin access level.

Syntax

enable-admin

Command Mode

Privileged Configuration Mode

Privilege Requirement

None.

User Guidelines

The elevation password is defined in the AAA function. Please refer to [enable admin password](#) and [enable admin secret](#).

Example

The User role user uses the pre-defined evaluation password 123 to gain the administrative privilege.

```
T2500G-10TS#enable-admin
Password:123
T2500G-10TS#
```

2.3 service password-encryption

Description

The **service password-encryption** command is used to encrypt the password when the password is defined or when the configuration is written, using the symmetric encryption algorithm. Encryption prevents the password from being readable in the configuration file. To disable the global encryption function, please use **no service password-encryption** command.

Syntax

```
service password-encryption
no service password-encryption
```

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the global encryption function:

```
T2500G-10TS(config)# service password-encryption
```

2.4 enable password

Description

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

Syntax

enable password {[0] *password* | 7 *encrypted-password*}

no enable password

Parameter

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

password — Super password, a string from 1 to 31 alphanumeric characters or symbols. The password is case sensitive, allows digits, English letters (case sensitive), underlines and sixteen special characters (!\$%()'*,.-/[]{}). By default, it is empty.

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

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

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

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

Example

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

```
T2500G-10TS(config)#enable password 0 admin
```

2.5 enable secret

Description

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

Syntax

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

Parameter

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

password — Super password, a string from 1 to 31 alphanumeric characters or symbols. The password is case sensitive, allows digits, English letters (case sensitive), underlines and sixteen special characters (!\$%'()*,-./[]{}). By default, it is empty. The password in the configuration file will be displayed in the MD5 encrypted form.

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

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

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

If both the **enable password** and **enable secret** are defined, you must enter the password set in **enable secret**.

Example

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

```
T2500G-10TS(config)#enable secret 0 admin
```

2.6 configure

Description

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

Syntax

```
configure
```

Command Mode

Privileged EXEC Mode

Privilege Requirement

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

Example

Access Global Configuration Mode from Privileged EXEC Mode:

```
T2500G-10TS# configure  
T2500G-10TS(config)#
```

2.7 exit

Description

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

Syntax

```
exit
```


Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

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

```
T2500G-10TS(config-if)# exit
T2500G-10TS(config)#exit
T2500G-10TS#
```

2.8 end

Description

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

Syntax

```
end
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Return to Privileged EXEC Mode from Interface Configuration Mode:

```
T2500G-10TS(config-if)#end
T2500G-10TS#
```

2.9 clipaging

Description

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

Syntax

```
clipaging
```

no clipaging

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Disable the pause function for the screen display:

```
T2500G-10TS(config)#no clipaging
```

2.10 show history

Description

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

Syntax

show history

Command Mode

Privileged EXEC Mode and any Configuration Mode

Privilege Requirement

None.

Example

Show the commands you have entered in the current mode:

```
T2500G-10TS (config)# show history
```

```
1 show history
```

2.11 clear history

Description

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

Syntax

clear history

Command Mode

Privileged EXEC Mode and any Configuration Mode

Privilege Requirement

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

Example

Clear the commands you have entered in the current mode:

```
T2500G-10TS(config)# clear history
```

Chapter 3 IEEE 802.1Q VLAN Commands

VLAN (Virtual Local Area Network) technology is developed for the switch to divide the LAN into multiple logical LANs flexibly. Hosts in the same VLAN can communicate with each other, regardless of their physical locations. VLAN can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

3.1 vlan

Description

The **vlan** command is used to create IEEE 802.1Q VLAN and enter VLAN Configuration Mode. To delete the IEEE 802.1Q VLAN, please use **no vlan** command.

Syntax

```
vlan vlan-list  
no vlan vlan-list
```

Parameter

vlan-list—— Specify IEEE 802.1Q VLAN ID list, ranging from 2 to 4094, in the format of 2-3, 5. It is multi-optional.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create VLAN 2-10 and VLAN 100:

```
T2500G-10TS(config)# vlan 2-10,100
```

Delete VLAN 2:

```
T2500G-10TS(config)# no vlan 2
```

3.2 interface vlan

Description

The **interface vlan** command is used to create VLAN Interface and enter Interface VLAN Mode. To delete VLAN Interface, please use **no interface vlan** command.

Syntax

```
interface vlan vlan-id  
no interface vlan vlan-id
```

Parameter

vlan-id—— Specify IEEE 802.1Q VLAN ID, ranging from 1 to 4094.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create VLAN Interface 2:

```
T2500G-10TS(config)# interface vlan 2
```

3.3 name

Description

The **name** command is used to assign a description to a VLAN. To clear the description, please use **no name** command.

Syntax

```
name descript  
no name
```

Parameter

descript ——String to describe the VLAN, which contains 16 characters at most.

Command Mode

VLAN Configuration Mode (VLAN)

Privilege Requirement

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

Example

Specify the name of VLAN 2 as "group1":

```
T2500G-10TS(config)# vlan 2
T2500G-10TS(config-vlan)# name group1
```

3.4 switchport mode

Description

The **switchport mode** command is used to configure the Link Types for the ports.

Syntax

```
switchport mode { access | trunk | general }
```

Parameter

access | trunk | general — Link Types. There are three Link Types for the ports.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Specify the Link Type of Gigabit Ethernet port 1/0/3 as "trunk":

```
T2500G-10TS(config)#interface gigabitEthernet 1/0/3
T2500G-10TS(config-if)#switchport mode trunk
```

3.5 switchport access vlan

Description

The **switchport access vlan** command is used to add the desired Access port to IEEE 802.1Q VLAN, or to remove a port from the corresponding VLAN.

Syntax

```
switchport access vlan vlan-id  
no switchport access vlan
```

Parameter

vlan-id—— Specify IEEE 802.1Q VLAN ID, ranging from 2 to 4094.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure Gigabit Ethernet port 1/0/3 whose link type is "access" to VLAN 2:

```
T2500G-10TS(config)#interface gigabitEthernet 1/0/3  
T2500G-10TS(config-if)#switchport access vlan 2
```

3.6 switchport trunk allowed vlan

Description

The **switchport trunk allowed vlan** command is used to add the desired Trunk port to IEEE 802.1Q VLAN. To remove a Trunk port from the corresponding VLAN, please use **no switchport trunk allowed vlan** command.

Syntax

```
switchport trunk allowed vlan { vlan-list }  
no switchport trunk allowed vlan { vlan-list }
```

Parameter

vlan-list — VLAN ID list, ranging from 2 to 4094, in the format of 2-3, 5. It is multi-optional.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure the link type of port 2 as trunk and add it to VLAN 2:

```
T2500G-10TS(config)#interface gigabitEthernet 1/0/2
T2500G-10TS(config-if)#switchport mode trunk
T2500G-10TS(config-if)#switchport trunk allowed vlan 2
```

3.7 switchport trunk allowed vlan all

Description

The **switchport trunk allowed vlan all** command is used to add the desired trunk port to all the IEEE 802.1Q VLANs. To remove a trunk port from all the IEEE 802.1Q VLANs, please use **no switchport trunk allowed vlan all** command.

Syntax

```
switchport trunk allowed vlan all
no switchport trunk allowed vlan all
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

Configure the link type of port 2 as trunk and add it to all the VLANs:

```
T2500G-10TS(config)#interface gigabitEthernet 1/0/2
T2500G-10TS(config-if)#switchport mode trunk
T2500G-10TS(config-if)# switchport trunk allowed vlan all
```

3.8 switchport general allowed vlan

Description

The **switchport general allowed vlan** command is used to add the desired General port to IEEE 802.1Q VLAN, or to remove a port from the corresponding VLAN.

Syntax

```
switchport general allowed vlan vlan-list { tagged | untagged }
no switchport general allowed vlan vlan-list
```

Parameter

vlan-list — VLAN ID list, ranging from 2 to 4094, in the format of 2-3, 5. It is multi-optional.

tagged | untagged — egress-rule.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure Gigabit Ethernet port 1/0/4 whose link type is "general" to VLAN 2 and its egress-rule as "tagged":

```
T2500G-10TS(config)#interface gigabitEthernet 1/0/4
T2500G-10TS(config-if)#switchport mode general
T2500G-10TS(config-if)#switchport general allowed vlan 2 tagged
```

3.9 switchport pvid

Description

The **switchport pvid** command is used to configure the PVID for the switch ports.

Syntax

```
switchport pvid vlan-id
```

Parameter

vlan-id—— VLAN ID, ranging from 1 to 4094.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Specify the PVID of port 1/0/2 as 2:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/2
T2500G-10TS(config-if)# switchport pvid 2
```

3.10 show vlan summary

Description

The **show vlan summary** command is used to display the summarized information of IEEE 802.1Q VLAN.

Syntax

```
show vlan summary
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the summarized information of IEEE 802.1Q VLAN:

```
T2500G-10TS(config)# show vlan summary
```

3.11 show vlan brief

Description

The **show vlan brief** command is used to display the brief information of IEEE 802.1Q VLAN.

Syntax

```
show vlan brief
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the brief information of IEEE 802.1Q VLAN:

```
T2500G-10TS(config)# show vlan brief
```

3.12 show vlan

Description

The **show vlan** command is used to display the information of IEEE 802.1Q VLAN.

Syntax

```
show vlan [ id vlan-id]
```

Parameter

vlan-id — Specify IEEE 802.1Q VLAN ID, ranging from 1 to 4094. It is multi-optional. Using the **show vlan** command without parameter displays the detailed information of all VLANs.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of vlan 5:

```
T2500G-10TS(config)# show vlan id 5
```

3.13 show interface switchport

Description

The **show interface switchport** command is used to display the IEEE 802.1Q VLAN configuration information of the specified port/port channel.

Syntax

```
show interface switchport [ gigabitEthernet port ]
```

Parameter

port—— The port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the VLAN configuration information of all ports and port channels:

```
T2500G-10TS(config)# show interface switchport
```

Chapter 4 MAC-based VLAN Commands

MAC VLAN (Virtual Local Area Network) is the way to classify the VLANs based on MAC Address. A MAC address is relative to a single VLAN ID. The untagged packets and the priority-tagged packets coming from the MAC address will be tagged with this VLAN ID.

4.1 mac-vlan mac-address

Description

The **mac-vlan mac-address** command is used to create a MAC-based VLAN entry. To delete a MAC-based VLAN entry, please use the **no mac-vlan mac-address** command.

Syntax

```
mac-vlan mac-address mac-addr vlan vlan-id [description descript]  
no mac-vlan mac-address mac-addr
```

Parameter

mac-addr—— MAC address, in the format of XX:XX:XX:XX:XX:XX.

vlan-id—— Specify IEEE 802.1Q VLAN ID, ranging from 1 to 4094.

descript—— Give a description to the MAC address for identification, which contains 8 characters at most.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create VLAN 2 with the MAC address 00:11:11:01:01:12 and the name "TP":

```
T2500G-10TS(config)#mac-vlan mac-address 00:11:11:01:01:12 vlan 2  
description TP
```

4.2 mac-vlan

Description

The **mac-vlan** command is used to enable a port for the MAC-based VLAN feature. Only the port is enabled can the configured MAC-based VLAN take effect. To disable the MAC-based VLAN function, please use **no mac-vlan** command. All the ports are disabled by default.

Syntax

```
mac-vlan
no mac-vlan
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the Gigabit Ethernet port 1/0/3 for the MAC-based VLAN feature:

```
T2500G-10TS(config)#interface gigabitEthernet 1/0/3
T2500G-10TS(config-if)#mac-vlan
```

4.3 show mac-vlan

Description

The **show mac-vlan** command is used to display the information of the MAC-based VLAN entry. MAC address and VLAN ID can be used to filter the displayed information.

Syntax

```
show mac-vlan { all | mac-address mac-addr | vlan vlan-id }
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Parameter

mac-addr—— MAC address, in the format of XX:XX:XX:XX:XX:XX.

vlan-id—— Specify IEEE 802.1Q VLAN ID, ranging from 1 to 4094.

Example

Display the information of all the MAC-based VLAN entry:

```
T2500G-10TS(config)#show mac-vlan all
```

Chapter 5 Protocol-based VLAN Commands

Protocol VLAN (Virtual Local Area Network) is the way to classify VLANs based on Protocols. A Protocol is relative to a single VLAN ID. The untagged packets and the priority-tagged packets matching the protocol template will be tagged with this VLAN ID.

5.1 protocol-vlan template

Description

The **protocol-vlan template** command is used to create Protocol-based VLAN template. To delete Protocol-based VLAN template, please use **no protocol-vlan template** command.

Syntax

```
protocol-vlan template name protocol-name frame { ether_2 ether-type  
type | snap ether-type type | llc dsap dsap_type ssap ssap_type }  
no protocol-vlan template template-idx
```

Parameter

protocol-name — Give a name for the Protocol-based VLAN Template, which contains 8 characters at most.

ether_2 ether-type *type* — Specify the Ethernet type.

snap ether-type *type* — Specify the Ethernet type.

llc dsap *dsap_type* **ssap** *ssap_type* — Specify the DSAP type and the SSAP type.

template-idx — The number of the Protocol-based VLAN Template. You can get the template corresponding to the number by the [**show protocol-vlan template**](#) command.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create a Protocol-based VLAN template named "TP" whose Ethernet protocol type is 0x2024:

```
T2500G-10TS(config)#protocol-vlan template name TP frame ether_2
ether-type 2024
```

5.2 protocol-vlan vlan

Description

The **protocol-vlan vlan** command is used to create a Protocol-based VLAN entry. To delete a Protocol-based VLAN entry, please use **no protocol-vlan vlan** command.

Syntax

```
protocol-vlan vlan vlan-id template template-idx
```

```
no protocol-vlan vlan group-idx
```

Parameter

vlan-id—— Specify IEEE 802.1Q VLAN ID, ranging from 1-4094.

template-idx——The number of the Protocol-based VLAN Template. You can get the template corresponding to the number by the [show protocol-vlan template](#) command.

group-idx——The number of the Protocol-based VLAN entry. You can get the Protocol-based VLAN entry corresponding to the number by the [show protocol-vlan vlan](#) command.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create Protocol-based VLAN 2 and bind it with Protocol-based VLAN Template 3:

```
T2500G-10TS(config)#protocol-vlan vlan 2 template 3
```

5.3 protocol-vlan group

Description

The **protocol-vlan** command is used to add the port to a specified protocol group. To remove the port from this protocol group, please use **no protocol-vlan group** command.

Syntax

```
protocol-vlan group index  
no protocol-vlan group index
```

Parameter

index — Specify the protocol group ID.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Add Gigabit Ethernet port 20 to protocol group 1:

```
T2500G-10TS(config)#interface gigabitEthernet 1/0/20  
T2500G-10TS(config-if)#protocol-vlan group 1
```

5.4 show protocol-vlan template

Description

The **show protocol-vlan template** command is used to display the information of the Protocol-based VLAN templates.

Syntax

```
show protocol-vlan template
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of the Protocol-based VLAN templates:

```
T2500G-10TS(config)#show protocol-vlan template
```

5.5 show protocol-vlan vlan

Description

The **show protocol-vlan vlan** command is used to display the information about Protocol-based VLAN entry.

Syntax

```
show protocol-vlan vlan
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display information of the Protocol-based VLAN entry:

```
T2500G-10TS(config)#show protocol-vlan vlan
```

Chapter 6 VLAN-VPN Commands

VLAN-VPN (Virtual Private Network) function, the implement of a simple and flexible Layer 2 VPN technology, allows the packets with VLAN tags of private networks to be encapsulated with VLAN tags of public networks at the network access terminal of the Internet Service Provider. And these packets will be transmitted with double-tag across the public networks.

6.1 dot1q-tunnel

Description

The **dot1q-tunnel** command is used to enable the VLAN-VPN function globally. To disable the VLAN-VPN function, please use the **no dot1q-tunnel** command.

Syntax

```
dot1q-tunnel  
no dot1q-tunnel
```

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the VLAN-VPN function globally:

```
T2500G-10TS(config)#dot1q-tunnel
```

6.2 dot1q-tunnel tpid

Description

The **dot1q-tunnel tpid** command is used to configure Global TPID of the VLAN-VPN. To restore to the default value, please use the **no dot1q-tunnel tpid** command.

Syntax

```
dot1q-tunnel tpid tpid  
no dot1q-tunnel tpid
```

Parameter

tpid—— The value of Global TPID. It must be 4 Hex integers. By default, it is 8100.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure Global TPID of the VLAN-VPN as 0x9100:

```
T2500G-10TS(config)#dot1q-tunnel tpid 9100
```

6.3 dot1q-tunnel mapping

Description

The **dot1q-tunnel mapping** command is used to enable the VLAN Mapping feature globally. To disable this function, please use the **no dot1q-tunnel mapping** command. By default, the VLAN Mapping feature is disabled.

Syntax

```
dot1q-tunnel mapping  
no dot1q-tunnel mapping
```

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the VLAN mapping feature globally:

6.4 switchport dot1q-tunnel mapping

Description

The **switchport dot1q-tunnel mapping** command is used to add the VLAN Mapping entry on a specified port. To delete the VLAN Mapping entry on this port, please use the **no switchport dot1q-tunnel mapping** command.

Syntax

```
switchport dot1q-tunnel mapping c-vlan sp-vlan pri descript  
no switchport dot1q-tunnel mapping c-vlan
```

Parameter

c-vlan—— Customer VLAN ID, ranging from 1 to 4094.

sp-vlan—— Service Provider VLAN ID, ranging from 1 to 4094.

pri—— Service Provider priority.

descript—— Give a description to the VLAN Mapping entry, which contains 15 characters at most.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Add a VLAN Mapping entry on the Gigabit Ethernet port 1/0/3 with the Customer VLAN as VLAN 2, the Service Provider priority as 1, the Service Provider VLAN as VLAN 3 and the description as TP:

```
T2500G-10TS(config)#interface gigabitEthernet 1/0/3
```

```
T2500G-10TS(config-if)#switchport dot1q-tunnel mapping 2 3 1 TP
```

6.5 switchport dot1q-tunnel missdrop

Description

The **switchport dot1q-tunnel missdrop** command is used to enable the VLAN-VPN missdrop function for a specific port. To disable the VLAN-VPN missdrop function, please use the **no switchport dot1q-tunnel missdrop** command.

Syntax

```
switchport dot1q-tunnel missdrop
no switchport dot1q-tunnel missdrop
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

Enable the VLAN-VPN missdrop function for Gigabit Ethernet port 1/0/3:

```
T2500G-10TS (config)#interface gigabitEthernet 1/0/3
T2500G-10TS (config-if)#switchport dot1q-tunnel missdrop
```

6.6 switchport dot1q-tunnel mode

Description

The **switchport dot1q-tunnel mode** command is used to configure the VPN port's mode. To close this VPN port, please use the **no switchport dot1q-tunnel mode** command. By default, no port has been configured as the VPN port. The VPN port mode uni and nni cannot switch to each other directly, so please close the VPN port and switch to the other mode if needed.

Syntax

```
switchport dot1q-tunnel mode { uni/nni }
no switchport dot1q-tunnel mode
```

Parameter

uni—The port connected to the clients.

nni—The port connected to the ISP.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure the Gigabit Ethernet port 1/0/3 as the VPN UNI ports:

```
T2500G-10TS(config)#interface gigabitEthernet 1/0/3
T2500G-10TS(config-if)#switchport dot1q-tunnel mode uni
```

6.7 show dot1q-tunnel

Description

The **show dot1q-tunnel** command is used to display the global configuration information of the VLAN VPN.

Syntax

```
show dot1q-tunnel
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration information of the VLAN VPN:

```
T2500G-10TS(config)#show dot1q-tunnel
```


6.8 show dot1q-tunnel mapping

Description

The **show dot1q-tunnel mapping** command is used to display the information of VLAN Mapping entry.

Syntax

```
show dot1q-tunnel mapping
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of VLAN Mapping entry:

```
T2500G-10TS(config)#show dot1q-tunnel mapping
```

6.9 show dot1q-tunnel interface

Description

The **show dot1q-tunnel mapping interface** command is used to display the VLAN VPN port type.

Syntax

```
show dot1q-tunnel interface
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the port type of all VLAN VPN ports:

```
T2500G-10TS(config)#show dot1q-tunnel interface
```

Chapter 7 Voice VLAN Commands

Voice VLANs are configured specially for voice data stream. By configuring Voice VLANs and adding the ports with voice devices attached to voice VLANs, you can perform QoS-related configuration for voice data, ensuring the transmission priority of voice data stream and voice quality.

7.1 voice vlan

Description

The **voice vlan** command is used to enable Voice VLAN function. To disable Voice VLAN function, please use **no voice vlan** command.

Syntax

voice vlan *vlan-id*

no voice vlan

Parameter

vlan-id—— Specify IEEE 802.1Q VLAN ID, ranging from 2 to 4094.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the Voice VLAN function for VLAN 10:

```
T2500G-10TS(config)# voice vlan 10
```

7.2 voice vlan aging time

Description

The **voice vlan aging time** command is used to set the aging time for a voice VLAN. To restore to the default aging time for the Voice VLAN, please use **no voice vlan aging** command.

Syntax

voice vlan aging time *time*

no voice vlan aging time

Parameter

time—— Aging time (in minutes) to be set for the Voice VLAN. It ranges from 1 to 43200 minutes and the default value is 1440 minutes.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Set the aging time for the Voice VLAN as 1 minute:

```
T2500G-10TS(config)# voice vlan aging time 1
```

7.3 voice vlan priority

Description

The **voice vlan priority** command is used to configure the priority for the Voice VLAN. To restore to the default priority, please use **no voice vlan priority** command.

Syntax

voice vlan priority *pri*

no voice vlan priority

Parameter

pri—— Priority, ranging from 0 to 7, and the default value is 6.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the priority of the Voice VLAN as 5:

```
T2500G-10TS(config)# voice vlan priority 5
```

7.4 voice vlan mac-address

Description

The **voice vlan mac-address** command is used to create Voice VLAN OUI. To delete the specified Voice VLAN OUI, please use **no voice vlan mac-address** command.

Syntax

```
voice vlan mac-address mac-addr mask mask [description descript]
```

```
no voice vlan mac-address mac-addr
```

Parameter

mac-addr — The OUI address of the voice device, in the format of XX:XX:XX:XX:XX:XX.

mask — The OUI address mask of the voice device, in the format of XX:XX:XX:XX:XX:XX.

descript — Give a description to the OUI for identification which contains 16 characters at most.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create a Voice VLAN OUI described as TP-Phone with the OUI address 00:11:11:11:11:11 and the mask address FF:FF:FF:00:00:00:

```
T2500G-10TS(config)#voice vlan mac-address 00:11:11:11:11:11 mask  
FF:FF:FF:00:00:00 description TP-Phone
```

7.5 switchport voice vlan mode

Description

The **switchport voice vlan mode** command is used to configure the Voice VLAN mode for the Ethernet port.

Syntax

```
switchport voice vlan mode { manual | auto }
```

Parameter

manual | auto — Port mode.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure the port 1/0/3 to operate in the auto voice VLAN mode:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/3
T2500G-10TS(config-if)# switchport voice vlan mode auto
```

7.6 switchport voice vlan security

Description

The **switchport voice vlan security** command is used to enable the Voice VLAN security feature. To disable the Voice VLAN security feature, please use **no switchport voice vlan security** command.

Syntax

```
switchport voice vlan security
no switchport voice vlan security
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable port 1/0/3 for the Voice VLAN security feature:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/3
T2500G-10TS(config-if)# switchport voice vlan security
```

7.7 show voice vlan

Description

The **show voice vlan** command is used to display the global configuration information of Voice VLAN.

Syntax

```
show voice vlan
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

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

Example

Display the configuration information of Voice VLAN globally:

```
T2500G-10TS(config)# show voice vlan
```

7.8 show voice vlan oui

Description

The **show voice vlan oui** command is used to display the configuration information of Voice VLAN OUI.

Syntax

```
show voice vlan oui
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

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

Example

Display the configuration information of Voice VLAN OUI:

```
T2500G-10TS(config)# show voice vlan oui
```

7.9 show voice vlan switchport

Description

The **show voice vlan switchport** command is used to display the Voice VLAN configuration information of a specified port/port channel.

Syntax

```
show voice vlan switchport [ gigabitEthernet port ]
```

Parameter

port—— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

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

Example

Display the Voice VLAN configuration information of all ports and port channels:

```
T2500G-10TS(config)# show voice vlan switchport
```

Display the Voice VLAN configuration information of port 1/0/2:

```
T2500G-10TS(config)# show voice vlan switchport gigabitEthernet 1/0/2
```

Chapter 8 L2PT Commands

L2PT (Layer 2 Protocol Tunneling) is a feature for service providers to transmit packets from different customers across their ISP networks and maintain Layer 2 protocol configurations of each customer. The supported Layer 2 protocols are STP (Spanning Tree Protocol), GVRP (GARP VLAN Registration Protocol), CDP (Cisco Discovery Protocol), VTP (VLAN Trunking Protocol), PAgP (Port Aggregation Protocol), UDLD (UniDirectional Link Detection) and PVST+(Per VLAN Spanning Tree Plus).

8.1 I2protocol-tunnel

Description

The **I2protocol-tunnel** command is used to enable the layer 2 protocol tunneling (L2PT) function globally. To disable the L2PT function, please use **no I2protocol-tunnel** command.

Syntax

```
I2protocol-tunnel  
no I2protocol-tunnel
```

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the L2PT function globally:

```
T2500G-10TS(config)# I2protocol-tunnel
```

8.2 I2protocol-tunnel type

Description

The **I2protocol-tunnel type** command is used to configure the L2PT function on a specified port. To disable the L2PT function on the specified port, please use **no I2protocol-tunnel** command.

Syntax

l2protocol-tunnel type nni

l2protocol-tunnel type uni { 01000ccccccc | 01000ccccccd | gvrp | stp | lacp
| all } [**threshold** *threshold*]

no l2protocol-tunnel

Parameter

nni — Specify the port type according to its connecting device in the network. Specify the port's type as NNI if it is connecting to the ISP network.

uni — Specify the port type according to its connecting device in the network. Specify the port's type as UNI if it is connecting to the user's local network.

01000ccccccc | 01000ccccccd | gvrp | stp | lacp | all — Select the supported Layer 2 protocol type. Packets of the specified protocol will be encapsulated with their destination MAC address before they are sent to the ISP network. Packets will be decapsulated to restore their Layer 2 protocol and MAC address information before they are sent to the customer network.

- 01000ccccccc: Enable protocol tunneling for the packets with destination MAC address 01-00-0C-CC-CC-CC. 01-00-0CC-CC-CC-CC is used as the destination MAC address of the CDP/VTP/PAgP/UDLD packets.
- 01000ccccccd: Enable protocol tunneling for the packets with destination MAC address 01-00-0C-CC-CC-CD. 01-00-0CC-CC-CC-CD is used as the destination MAC address of Cisco PVST+ BPDUs.
- gvrp: Enable protocol tunneling for the GVRP packets.
- stp: Enable protocol tunneling for the STP packets.
- lacp: Enable protocol tunneling for the LACP packets.
- all: All the above Layer 2 protocols are supported for tunneling.

threshold — Configure the threshold for packets-per-second accepted for encapsulation. Packets beyond the threshold will be dropped. It ranges from 0 to 1000.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

Configure port 1/0/3 as a UNI port for STP packets with the threshold as 1000 packets/second:

```
T2500G-10TS (config)#interface gigabitEthernet 1/0/3
T2500G-10TS (config-if)# l2protocol-tunnel type uni stp threshold 1000
```

8.3 show l2protocol-tunnel global

Description

The **show l2protocol-tunnel global** command is used to display the global L2PT status.

Syntax

```
show l2protocol-tunnel global
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global L2PT status:

```
T2500G-10TS(config)# show l2protocol-tunnel global
```

8.4 show l2protocol-tunnel interface

Description

The **show l2protocol-tunnel interface** command is used to display the L2PT configuration information of a specified Ethernet port or of all Ethernet ports.

Syntax

```
show l2protocol-tunnel interface [ gigabitEthernet port]
```

Parameter

port — The port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the L2PT configuration information of Gigabit Ethernet port 1/0/1:

```
T2500G-10TS(config)#show l2protocol-tunnel interface gigabitEthernet  
1/0/1
```

Display the L2PT configuration information of all Ethernet ports:

```
T2500G-10TS(config)#show l2protocol-tunnel interface
```

Chapter 9 GVRP Commands

GVRP (GARP VLAN registration protocol) is an implementation of GARP (generic attribute registration protocol). GVRP allows the switch to automatically add or remove the VLANs via the dynamic VLAN registration information and propagate the local VLAN registration information to other switches, without having to individually configure each VLAN.

9.1 gvrp

Description

The **gvrp** command is used to enable the GVRP function globally. To disable the GVRP function, please use **no gvrp** command.

Syntax

gvrp

no gvrp

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the GVRP function globally:

```
T2500G-10TS(config)#gvrp
```

9.2 gvrp (interface)

Description

The **gvrp** command is used to enable the GVRP function for the desired port. To disable it, please use **no gvrp** command. The GVRP feature can only be enabled for the trunk-type ports.

Syntax

gvrp

no gvrp

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the GVRP function for Gigabit Ethernet ports 1/0/2-6:

```
T2500G-10TS(config)#interface range gigabitEthernet 1/0/2-6
T2500G-10TS(config-if-range)#gvrp
```

9.3 gvrp registration

Description

The **gvrp registration** command is used to configure the GVRP registration type for the desired port. To restore to the default value, please use **no gvrp registration** command.

Syntax

```
gvrp registration { normal | fixed | forbidden }
no gvrp registration
```

Parameter

normal | fixed | forbidden — Registration mode. By default, the registration mode is "normal".

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure the GVRP registration mode as “fixed” for Gigabit Ethernet ports 1/0/2-6:

```
T2500G-10TS(config)#interface range gigabitEthernet 1/0/2-6
T2500G-10TS(config-if-range)#gvrp registration fixed
```

9.4 gvrp timer

Description

The **gvrp timer** command is used to set a GVRP timer for the desired port. To restore to the default setting of a GARP timer, please use **no gvrp timer** command.

Syntax

```
gvrp timer { leaveall | join | leave } value
```

```
no gvrp timer [leaveall | join | leave]
```

Parameter

leaveall | join | leave — They are the three timers: leave All, join and leave. Once the LeaveAll Timer is set, the port with GVRP enabled can send a LeaveAll message after the timer times out, so that other GARP ports can re-register all the attribute information. After that, the LeaveAll timer will start to begin a new cycle. To guarantee the transmission of the Join messages, a GARP port sends each Join message two times. The Join Timer is used to define the interval between the two sending operations of each Join message. Once the Leave Timer is set, the GARP port receiving a Leave message will start its Leave timer, and deregister the attribute information if it does not receive a Join message again before the timer times out.

value —The value of the timer. The LeaveAll Timer ranges from 1000 to 30000 centiseconds and the default value is 1000 centiseconds. The Join Timer ranges from 20 to 1000 centiseconds and the default value is 20 centiseconds. The Leave Timer ranges from 60 to 3000 centiseconds and the default value is 60 centiseconds.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Set the GARP leaveall timer of Gigabit Ethernet port 1/0/6 as 2000 centiseconds and restore the join timer of it to the default value:

```
T2500G-10TS(config)#interface gigabitEthernet 1/0/6
```

```
T2500G-10TS(config-if)#gvrp timer leaveall 2000
```

```
T2500G-10TS(config-if)#no gvrp timer join
```

9.5 show gvrp interface

Description

The **show gvrp interface** command is used to display the GVRP configuration information of a specified Ethernet port or of all Ethernet ports.

Syntax

```
show gvrp interface [ gigabitEthernet port ]
```

Parameter

port — The port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the GVRP configuration information of Gigabit Ethernet port 1:

```
T2500G-10TS(config)#show gvrp interface gigabitEthernet 1/0/1
```

Display the GVRP configuration information of all Ethernet ports:

```
T2500G-10TS(config)#show gvrp interface
```

9.6 show gvrp global

Description

The **show gvrp global** command is used to display the global GVRP status.

Syntax

```
show gvrp global
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global GVRP status:

```
T2500G-10TS(config)#show gvrp global
```


Chapter 10 Etherchannel Commands

Etherchannel Commands are used to configure LAG and LACP function.

LAG (Link Aggregation Group) is to combine a number of ports together to make a single high-bandwidth data path, which can highly extend the bandwidth. The bandwidth of the LAG is the sum of bandwidth of its member port.

LACP (Link Aggregation Control Protocol) is defined in IEEE802.3ad and enables the dynamic link aggregation and disaggregation by exchanging LACP packets with its partner. The switch can dynamically group similarly configured ports into a single logical link, which will highly extend the bandwidth and flexibly balance the load.

10.1 channel-group

Description

The **channel-group** command is used to add a port to the EtherChannel Group and configure its mode. To delete the port from the EtherChannel Group, please use **no channel-group** command.

Syntax

channel-group *num* **mode** { on | active | passive }

no channel-group

Parameter

num—— The number of the EtherChannel Group, ranging from 1 to 14.

on —— Enable the static LAG.

active —— Enable the active LACP mode.

passive —— Enable the passive LACP mode.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Add ports 2-4 to EtherChannel Group 1 and enable the static LAG:

```
T2500G-10TS(config)# interface range gigabitEthernet 1/0/2-4
T2500G-10TS(config-if-range)# channel-group 1 mode on
```

10.2 port-channel load-balance

Description

The **port-channel load-balance** command is used to configure the Aggregate Arithmetic for LAG. To return to the default configurations, please use **no port-channel load-balance** command.

Syntax

```
port-channel load-balance { src-dst-mac | src-dst-ip }
no port-channel load-balance
```

Parameter

src-dst-mac — The source and destination MAC address. When this option is selected, the Aggregate Arithmetic will be based on the source and destination MAC addresses of the packets. The Aggregate Arithmetic for LAG is "src-dst-mac" by default.

src-dst-ip — The source and destination IP address. When this option is selected, the Aggregate Arithmetic will be based on the source and destination IP addresses of the packets.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the Aggregate Arithmetic for LAG as "src-dst-ip":

```
T2500G-10TS(config)# port-channel load-balance src-dst-ip
```

10.3 lacp system-priority

Description

The **lacp system-priority** command is used to configure the LACP system priority globally. To return to the default configurations, please use **no lacp system-priority** command.

Syntax

```
lacp system-priority pri  
no lacp system-priority
```

Parameter

pri—— The system priority, ranging from 0 to 65535. It is 32768 by default.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the LACP system priority as 1024 globally:

```
T2500G-10TS(config)# lacp system-priority 1024
```

10.4 lacp port-priority

Description

The **lacp port-priority** command is used to configure the LACP port priority for specified ports. To return to the default configurations, please use **no lacp port-priority** command.

Syntax

```
lacp port-priority pri  
no lacp port-priority
```

Parameter

pri—— The port priority, ranging from 0 to 65535. It is 32768 by default.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure the LACP port priority as 1024 for ports 1-3:

```
T2500G-10TS(config)# interface range gigabitEthernet 1/0/1-3
T2500G-10TS(config-if-range)# lacp port-priority 1024
```

Configure the LACP port priority as 2048 for port 4:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/4
T2500G-10TS(config-if)# lacp port-priority 2048
```

10.5 show etherchannel

Description

The **show etherchannel** command is used to display the EtherChannel information.

Syntax

```
show etherchannel [ channel-group-num ] { detail | summary }
```

Parameter

channel-group-num — The EtherChannel Group number, ranging from 1 to 14. By default, it is empty, and will display the information of all EtherChannel Groups.

detail — The detailed information of EtherChannel.

summary — The EtherChannel information in summary.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the detailed information of EtherChannel Group 1:

```
T2500G-10TS(config)# show etherchannel 1 detail
```

10.6 show etherchannel load-balance

Description

The **show etherchannel load-balance** command is used to display the Aggregate Arithmetic of LAG.

Syntax

```
show etherchannel load-balance
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the Aggregate Arithmetic of LAG:

```
T2500G-10TS(config)# show etherchannel load-balance
```

10.7 show lacp

Description

The **show lacp** command is used to display the LACP information for a specified EtherChannel Group.

Syntax

```
show lacp [ channel-group-num ] { internal /neighbor }
```

Parameter

channel-group-num — The EtherChannel Group number, ranging from 1 to 14. By default, it is empty, and will display the information of all LACP groups.

internal — The internal LACP information.

neighbor — The neighbor LACP information.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the internal LACP information of EtherChannel Group 1:

```
T2500G-10TS(config)# show lacp 1 internal
```

10.8 show lacp sys-id

Description

The **show lacp sys-id** command is used to display the LACP system priority globally.

Syntax

```
show lacp sys-id
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the LACP system priority:

```
T2500G-10TS(config)# show lacp sys-id
```

Chapter 11 User Management Commands

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

11.1 user name (password)

Description

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

Syntax

```
user name name [ privilege admin | operator | power_user | user ] password
{ [ 0 ] password | 7 encrypted-password }

no user name name
```

Parameter

name —— Type a name for users' login, which contains 16 characters at most, composed of digits, English letters and under dashes only.

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

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

password —— Users' login password, a string from 1 to 31 alphanumeric characters or symbols. The password is case sensitive, allows digits, English letters (case sensitive), underlines and sixteen special characters (!\$%'()*,-./[]{}).

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

encrypted-password —— A symmetric encrypted password with fixed length, which you can copy from another switch's configuration file. After the

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

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

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

Example

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

```
T2500G-10TS(config)#user name tplink privilege admin password 0 admin
```

11.2 user name (secret)

Description

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

Syntax

```
user name name [ privilege admin | operator | power_user | user ] secret { [ 0 ]  
password | 5 encrypted-password }
```

```
no user name name
```

Parameter

name —— Type a name for users' login, which contains 16 characters at most, composed of digits, English letters and under dashes only.

admin | operator | power_user | user —— Access level. "admin" means that you can edit, modify and view all the settings of different functions. "operator" means that you can edit, modify and view most of the the settings of different functions. "power-user" means that you can edit, modify and view some of

the the settings of different functions. "user" means that you can only view some of the the settings of different functions without the right to edit or modify. It is "admin" by default.

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

password —Users' login password, a string from 1 to 31 alphanumeric characters or symbols. The password is case sensitive, allows digits, English letters (case sensitive), underlines and sixteen special characters (!\$%'()*,-./[]{}). The password will be saved to the configuration file using the MD5 encrypted algorithm.

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

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

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

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

Example

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

```
T2500G-10TS(config)#user name tplink privilege admin secret 0 admin
```

11.3 user access-control ip-based

Description

The **user access-control ip-based** command is used to limit the IP-range of the users for login. Only the users within the IP-range you set here are allowed to login. To cancel the user access limit, please use **no user access-control** command.

Syntax

```
user access-control ip-based { ip-addr ip-mask } [ snmp ] [ telnet ] [ ssh ]  
[ http ] [ https ] [ ping ] [ all ]  
no user access-control
```

Parameter

ip-addr — The source IP address. Only the users within the IP-range you set here are allowed for login. 5 IP-based entries can be configured at most.

ip-mask — The subnet mask of the IP address.

[snmp] [telnet] [ssh] [http] [https] [ping] [all] — Specify the access interface. These interfaces are enabled by default.

id — Delete the specified IP-based entry. The index ranges from 1 to 5.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the access-control of the user whose IP address is 192.168.0.148:

```
T2500G-10TS(config)# user access-control ip-based 192.168.0.148  
255.255.255.255
```

11.4 user access-control mac-based

Description

The **user access-control mac-based** command is used to limit the MAC address of the users for login. Only the user with this MAC address you set here is allowed to login. To cancel the user access limit, please use **no user access-control** command.

Syntax

```
user access-control mac-based { mac-addr } [ snmp ] [ telnet ] [ ssh ] [ http ]  
[ https ] [ ping ] [ all ]  
no user access-control
```

Parameter

mac-addr — The source MAC address. Only the user with this MAC address is allowed to login.

[snmp] [telnet] [ssh] [http] [https] [ping] [all] — Specify the access interface. These interfaces are enabled by default.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure that only the user whose MAC address is 00:00:13:0A:00:01 is allowed to login:

```
T2500G-10TS(config)# user access-control mac-based 00:00:13:0A:00:01
```

11.5 user access-control port-based

Description

The **user access-control port-based** command is used to limit the ports for login. Only the users connected to these ports you set here are allowed to login. To cancel the user access limit, please use **no user access-control** command.

Syntax

```
user access-control port-based interface { gigabitEthernet port | range gigabitEthernet port-list } [ snmp ] [ telnet ] [ ssh ] [ http ] [ https ] [ ping ] [ all ]  
no user access-control
```

Parameter

port — The Gigabit Ethernet port.

port-list — The list group of Ethernet ports, in the format of 1/0/1-4. You can appoint 5 ports at most.

[snmp] [telnet] [ssh] [http] [https] [ping] [all] — Specify the access interface. These interfaces are enabled by default.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure that only the users connected to ports 1/0/2-6 are allowed to login:

```
T2500G-10TS(config)# user access-control port-based interface range  
gigabitEthernet 1/0/2-6
```

11.6 line

Description

The **line** command is used to enter the Line Configuration Mode and make related configurations for the desired user(s), including the login mode and password configurations.

Syntax

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

Parameter

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

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

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

ssh — Configure the SSH terminal line.

telnet — Configure the Telnet terminal line.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

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

```
T2500G-10TS(config)#line console 0
```

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

```
T2500G-10TS(config)#line vty 0 5
```

11.7 password

Description

The **password** command is used to configure the connection password. To clear the password, please use **no password** command.

Syntax

```
password {[ 0 ] password | 7 encrypted-password}
```

```
no password
```

Parameter

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

password — Connection password, a string from 1 to 31 alphanumeric characters or symbols. The password is case sensitive, allows spaces but ignores leading spaces, and cannot contain question marks. By default, it is empty.

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

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

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

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

Example

Configure the connection password of Console port connection 0 as "tplink" and unencrypted:

```
T2500G-10TS(config)#line console 0
T2500G-10TS(config-line)#password 0 tplink
```

Configure the connection password of virtual terminal connection 0-5 as "tplink" and unencrypted:

```
T2500G-10TS(config)#line vty 0 5
T2500G-10TS(config-line)#password 0 tplink
```

11.8 login

Description

The **login** command is used to configure the login mode of a switch which uses connection password to login. At this situation, a connection password must be set for virtual terminal connection.

Syntax

```
login
```

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the login of Console port connection 0 as login mode:

```
T2500G-10TS(config)#line console 0
```

```
T2500G-10TS(config-line)#login
```

Configure the login of virtual terminal connection 0-5 as login mode:

```
T2500G-10TS(config)#line vty 0 5
```

```
T2500G-10TS(config-line)#login
```

11.9 login local

Description

The **login local** command is used to configure the login mode of the switch which uses the user name and password to login.

Syntax

```
login local
```

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the login of virtual terminal connection 0-5 as login local mode:

```
T2500G-10TS(config)#line vty 0 5
```

```
T2500G-10TS(config-line)#login local
```

Configure the login of Console port connection 0 as login local mode:

```
T2500G-10TS(config)#line console 0
```

```
T2500G-10TS(config-line)#login local
```

11.10 media-type rj45

Description

The **media-type rj45** command is used to configure the console media type as RJ-45 for input. The switch has two console ports available — an RJ-45 console port and a micro-USB console port. Console input is active on only one console port at a time. By default, the micro-USB connector takes precedence over the RJ-45 connector, which means that, when both the

RJ-45 console connection and micro-USB console connection are valid, input from the RJ-45 console is disabled, and input from the micro-USB console is enabled. To return to the default configuration, please use **no media-type rj45** command.

Syntax

```
media-type rj45  
no media-type rj45
```

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the RJ-45 console input:

```
T2500G-10TS(config)# line console 0  
T2500G-10TS(config-line)# media-type rj45
```

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

```
T2500G-10TS(config)# line console 0  
T2500G-10TS(config-line)# no media-type rj45
```

11.11 telnet

Description

The **telnet enable** command is used to enable the Telnet function. To disable the Telnet function, please use the **telnet disable** command. This function is enabled by default.

Syntax

```
telnet enable  
telnet disable
```

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Disable the Telnet function:

```
T2500G-10TS(config)# telnet disable
```

11.12 show user account-list

Description

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

Syntax

```
show user account-list
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of the current users:

```
T2500G-10TS(config)# show user account-list
```

11.13 show user configuration

Description

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

Syntax

```
show user configuration
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the security configuration information of the users:

```
T2500G-10TS(config)# show user configuration
```

11.14 show telnet-status

Description

The **show telnet-status** command is used to display the configuration information of the Telnet function.

Syntax

```
show telnet-status
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display whether the Telnet function is enabled:

```
T2500G-10TS(config)# show telnet-status
```

Chapter 12 HTTP and HTTPS Commands

With the help of HTTP (HyperText Transfer Protocol) or HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer), you can manage the switch through a standard browser.

HTTP is the protocol to exchange or transfer hypertext.

SSL (Secure Sockets Layer), a security protocol, is to provide a secure connection for the application layer protocol (e.g. HTTP) based on TCP. Adopting asymmetrical encryption technology, SSL uses key pair to encrypt/decrypt information. A key pair refers to a public key (contained in the certificate) and its corresponding private key. By default the switch has a certificate (self-signed certificate) and a corresponding private key. The Certificate/Key Download function enables the user to replace the default key pair.

12.1 ip http server

Description

The **ip http server** command is used to enable the HTTP server within the switch. To disable the HTTP function, please use **no ip http server** command. This function is enabled by default. The HTTP and HTTPS server function cannot be disabled at the same time.

Syntax

ip http server

no ip http server

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Disable the HTTP function:

```
T2500G-10TS(config)# no ip http server
```

12.2 ip http max-users

Description

The **ip http max-users** command is used to configure the maximum number of users that are allowed to connect to the HTTP server. To cancel this limitation, please use **no ip http max-users** command.

Syntax

ip http max-users *admin-num* *guest-num*

no ip http max-users

Parameter

admin-num — The maximum number of the users logging on to the HTTP server as Admin, ranging from 1 to 16. The total number of Admin and Guest should be less than 16.

guest-num — The maximum number of the users logging on to the HTTP server as Guest, ranging from 0 to 15. The total number of Admin and Guest should be less than 16.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the maximum number of the Admin and Guest users logging on to the HTTP server as 5 and 3:

```
T2500G-10TS(config)# ip http max-users 5 3
```

12.3 ip http session timeout

Description

The **ip http session timeout** command is used to configure the connection timeout of the HTTP server. To restore to the default timeout time, please use **no ip http session timeout** command.

Syntax

ip http session timeout *time*

no ip http session timeout

Parameter

time —The timeout time, ranging from 5 to 30 in minutes. By default, the value is 10.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the timeout time of the HTTP connection as 15 minutes:

```
T2500G-10TS(config)# ip http session timeout 15
```

12.4 ip http secure-server

Description

The **ip http secure-server** command is used to enable the HTTPS server within the switch. To disable the HTTPS function, please use **no ip http secure-server** command. This function is enabled by default. The HTTP and HTTPS server function cannot be disabled at the same time.

Syntax

```
ip http secure-server
```

```
no ip http secure-server
```

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Disable the HTTP function:

```
T2500G-10TS(config)# no ip http secure-server
```

12.5 ip http secure-protocol

Description

The **ip http secure-protocol** command is used to configure the SSL protocol version. To restore to the default SSL version, please use **no ip http secure-protocol** command. By default, the switch supports SSLv3 and TLSv1.

Syntax

```
ip http secure-protocol {[ssl3][tls1]}  
no ip http session
```

Parameter

ssl3 — The SSL 3.0 protocol.
tls1 — The TLS 1.0 protocol

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the protocol of SSL connection as SSL 3.0:

```
T2500G-10TS(config)# ip http secure-protocol ssl3
```

12.6 ip http secure-ciphersuite

Description

The **ip http secure-ciphersuite** command is used to configure the cipherSuites over the SSL connection supported by the switch. To restore to the default ciphersuite types, please use **no ip http secure-ciphersuite** command.

Syntax

```
ip http secure-ciphersuite { [ 3des-ede-cbc-sha ] [ rc4-128-md5 ]  
[ rc4-128-sha ][ des-cbc-sha ]}  
no ip http secure-ciphersuite
```

Parameter

[3des-ede-cbc-sha] [rc4-128-md5] [rc4-128-sha] [des-cbc-sha] ——
Specify the encryption algorithm and the digest algorithm to use on an SSL connection. By default, the switch supports all these ciphersuites.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the ciphersuite to be used for encryption over the SSL connection as 3des-ede-cbc-sha:

```
T2500G-10TS(config)# ip http secure-ciphersuite 3des-ede-cbc-sha
```

12.7 ip http secure-max-users

Description

The **ip http secure-max-users** command is used to configure the maximum number of users that are allowed to connect to the HTTPs server. To cancel this limitation, please use **no ip http secure-max-users** command.

Syntax

```
ip http secure-max-users admin-num guest-num
```

```
no ip secure-max-users
```

Parameter

admin-num —— The maximum number of the users logging on to the HTTPs server as Admin, ranging from 1 to 16. The total number of Admin and Guest should be less than 16.

guest-num —— The maximum number of the users logging on to the HTTPs server as Guest, ranging from 0 to 15. The total number of Admin and Guest should be less than 16.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the maximum number of the Admin and Guest users logging on to the HTTPs server as 5 and 3:

```
T2500G-10TS(config)# ip http secure-max-users 5 3
```

12.8 ip http secure-session timeout

Description

The **ip http secure-session timeout** command is used to configure the connection timeout of the HTTPS server. To restore to the default timeout time, please use **no ip http secure-session timeout** command.

Syntax

```
ip http secure-session timeout time
```

```
no ip http secure-session timeout
```

Parameter

time — The timeout time, ranging from 5 to 30 in minutes. By default, the value is 10.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the timeout time of the HTTPs connection as 15 minutes:

```
T2500G-10TS(config)# ip http secure-session timeout 15
```


12.9 ip http secure-server download certificate

Description

The **ip http secure-server download certificate** command is used to download a certificate to the switch from TFTP server.

Syntax

```
ip http secure-server download certificate ssl-cert ip-address ip-addr
```

Parameter

ssl-cert — The name of the SSL certificate which is selected to download to the switch. The length of the name ranges from 1 to 25 characters. The Certificate must be BASE64 encoded.

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Download an SSL Certificate named ssl-cert from TFTP server with the IP address of 192.168.0.146:

```
T2500G-10TS(config)# ip http secure-server download certificate ssl-cert  
ip-address 192.168.0.146
```

Download an SSL Certificate named ssl-cert from TFTP server with the IP address of fe80::1234

```
T2500G-10TS(config)# ip http secure-server download certificate ssl-cert  
ip-address fe80::1234
```

12.10 ip http secure-server download key

Description

The **ip http secure-server download key** command is used to download an SSL key to the switch from TFTP server.

Syntax

ip http secure-server download key *ssl-key* **ip-address** *ip-addr*

Parameter

ssl-key— The name of the SSL key which is selected to download to the switch. The length of the name ranges from 1 to 25 characters. The Key must be BASE64 encoded.

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Download an SSL key named ssl-key from TFTP server with the IP address of 192.168.0.146:

```
T2500G-10TS(config)# ip http secure-server download key ssl-key  
ip-address 192.168.0.146
```

Download an SSL key named ssl-key from TFTP server with the IP address of fe80::1234

```
T2500G-10TS(config)# ip http secure-server download key ssl-key  
ip-address fe80::1234
```

12.11 show ip http configuration

Description

The **show ip http configuration** command is used to display the configuration information of the HTTP server, including status, session timeout, access-control, max-user number and the idle-timeout, etc.

Syntax

```
show ip http configuration
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration information of the HTTP server:

```
T2500G-10TS(config)# show ip http configuration
```

12.12 show ip http secure-server

Description

The **show ip http secure-server** command is used to display the global configuration of SSL.

Syntax

```
show ip http secure-server
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of SSL:

```
T2500G-10TS(config)# show ip http secure-server
```

Chapter 13 Binding Table Commands

You can bind the IP address, MAC address, VLAN and the connected Port number of the Host together, which can be the condition for the ARP Inspection to filter the packets.

13.1 ip source binding

Description

The **ip source binding** command is used to bind the IP address, MAC address, VLAN ID and the Port number together manually. You can manually bind the IP address, MAC address, VLAN ID and the Port number together in the condition that you have got the related information of the Hosts in the LAN. To delete the IP-MAC-VID-PORT entry from the binding table, please use **no ip source binding index** command.

Syntax

```
ip source binding hostname ip-addr mac-addr vlan vlan-id interface  
gigabitEthernet port { none | arp-detection } [ forced-source { arp-scanning |  
dhcp-snooping } ]  
no ip source binding index idx
```

Parameter

hostname——The Host Name, which contains 20 characters at most.

ip-addr—— The IP address of the Host.

mac-addr—— The MAC address of the Host.

vlan-id——The VLAN ID needed to be bound, ranging from 1 to 4094.

port—— The number of port connected to the Host.

none | arp-detection——The protect type for the entry. arp-detection indicates ARP detection; none indicates applying none.

forced-source —— The source of the binding entry can be specified as "arp-scanning" or "dhcp-snooping". It is multi-optional.

idx —— The entry number needed to be deleted. You can use the [show ip source binding](#) command to get the idx. Pay attention that the entry number is the actual number in the binding table which is not display in an arranged order.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Bind an ACL entry with the IP 192.168.0.1, MAC 00:00:00:00:00:01, VLAN ID 2 and the Port number 5 manually. And then enable the entry for the ARP detection:

```
T2500G-10TS(config)#ip source binding host1 192.168.0.1  
00:00:00:00:00:01 vlan 2 interface gigabitEthernet 1/0/5 arp-detection
```

Delete the IP-MAC-VID-PORT entry with the index 5:

```
T2500G-10TS(config)#no ip source binding index 5
```

13.2 ip source binding index

Description

The **ip source binding index** command is used to modify the existing entry of ip source binding.

Syntax

```
ip source binding index idx {hostname hostname | mac mac-addr | vlan  
vlan-id | interface gigabitEthernet port | none | arp-detection }
```

Parameter

idx —The entry number needed to be modified. You can use the [show ip source binding](#) command to get the idx. Pay attention that the entry number is the actual number in the binding table which is not displayed in an arranged order.

hostname —The modified Host Name, which contains 20 characters at most.

mac-addr — The modified MAC address of the Host.

vlan-id —The modified VLAN ID, ranging from 1 to 4094.

port — The modified number of port connected to the Host.

none | arp-detection —The modified protect type for the entry. "none"

indicates applying none; "arp-detection" indicates ARP detection.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Modify the hostname as "tp-link" of the entry with the index 1:

```
T2500G-10TS(config)#ip source binding index 1 hostname tp-link
```

13.3 ip dhcp snooping

Description

The **ip dhcp snooping** command is used to enable DHCP-Snooping function globally. To disable DHCP-Snooping function globally, please use **no ip dhcp snooping** command. DHCP Snooping functions to monitor the process of the Host obtaining the IP address from DHCP server, and record the IP address, MAC address, VLAN and the connected Port number of the Host for automatic binding. The switch can also propagate the control information and the network parameters via the Option 82 field to provide more information for the Host.

Syntax

ip dhcp snooping

no ip dhcp snooping

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the DHCP-Snooping function globally:

```
T2500G-10TS(config)# ip dhcp snooping
```

13.4 ip dhcp snooping global

Description

The **ip dhcp snooping global** command is configure DHCP-Snooping globally. To restore to the default value, please use **no ip dhcp snooping global** command.

Syntax

```
ip dhcp snooping global [ global-rate global-rate ] [ dec-threshold dec-threshold ] [ dec-rate dec-rate ]
```

```
no ip dhcp snooping global
```

Parameter

global-rate — The value to specify the maximum amount of DHCP messages that can be forwarded by the switch per second. The excessive messages will be discarded. The options are 0/10/20/30/40/50 (packet/second).By default, it is 0 standing for disable.

dec-threshold —The value to specify the minimum transmission rate of the Decline packets to trigger the Decline protection for the specific port. The options are 0/5/10/15/20/25/30 (packet/second).By default, it is 0 standing for disable.

dec-rate —The value to specify the Decline Flow Control. The traffic flow of the corresponding port will be limited to be this value if the transmission rate of the Decline packets exceeds the Decline Threshold. The options are 5/10/15/20/25/30 (packet/second). By default, it is 5.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the Global Flow Control as 30pps, the Decline Threshold as 20 pps, and decline Flow Control as 20 pps for DHCP Snooping:

```
T2500G-10TS(config)# ip dhcp snooping global global-rate 30  
dec-threshold 20 dec-rate 20
```

13.5 ip dhcp snooping information option

Description

The **ip dhcp snooping information option** command is used to enable the Option 82 function of DHCP Snooping. To disable the Option 82 function, please use **no ip dhcp snooping information option** command.

Syntax

```
ip dhcp snooping information option  
no ip dhcp snooping information option
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the Option 82 function of DHCP Snooping on port 1/0/1:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/1  
T2500G-10TS(config)#ip dhcp snooping information option
```

13.6 ip dhcp snooping information strategy

Description

The **ip dhcp snooping information strategy** command is used to select the operation for the Option 82 field of the DHCP request packets from the Host. To restore to the default option, please use **no ip dhcp snooping information strategy** command.

Syntax

```
ip dhcp snooping information strategy strategy  
no ip dhcp snooping information strategy
```


Parameter

strategy— The operations for Option 82 field of the DHCP request packets from the Host, including three types:

keep: Indicates to keep the Option 82 field of the packets. It is the default option;

replace: Indicates to replace the Option 82 field of the packets with the switch defined one;

drop: Indicates to discard the packets including the Option 82 field

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Replace the Option 82 field of the packets with the switch defined one and then send out on port 1/0/1:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/1
T2500G-10TS(config)# ip dhcp snooping information strategy replace
```

13.7 ip dhcp snooping information format

Description

The **ip dhcp snooping information format** command is used to select the format of option 82 sub-option value field. To restore to the default option, please use **no ip dhcp snooping information format** command.

Syntax

```
ip dhcp snooping information format { normal | private }
no ip dhcp snooping information format
```

Parameter

normal | private — The format type of option 82 sub-option value field.

normal: Indicates that the format of sub-option value field is TLV (type-length-value).

private: Indicates that the format of sub-option value field is the value you configure for the related sub-option.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

Select the format of option 82 sub-option value field as TLV (type-length-value) on port 1/0/1:

```
T2500G-10TS(config)#interface gigabitEthernet 1/0/1
T2500G-10TS(config-if)#ip dhcp snooping information format normal
```

13.8 ip dhcp snooping information remote-id

Description

The **ip dhcp snooping information remote-id** command is used to enable and configure the customized sub-option Remote ID for the Option 82. To return to default Remote ID for the Option 82, please use **no ip dhcp snooping information remote-id** command.

Syntax

```
ip dhcp snooping information remote-id string
no ip dhcp snooping information remote-id
```

Parameter

string —Enter the sub-option Remote ID, which contains 32 characters at most.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable and configure the customized sub-option Remote ID for the Option 82 as tplink on port 1/0/1:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/1
T2500G-10TS(config)# ip dhcp snooping information remote-id tplink
```

13.9 ip dhcp snooping information circuit-id

Description

The **ip dhcp snooping information circuit-id** command is used to enable and configure the customized sub-option Circuit ID for the Option 82. To return to the default Circuit ID for the Option 82, please use **no ip dhcp snooping information circuit-id** command.

Syntax

```
ip dhcp snooping information circuit-id string
no ip dhcp snooping information circuit-id
```

Parameter

string —Enter the sub-option Circuit ID, which contains 32 characters at most.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable and configure the customized sub-option Circuit ID for the Option 82 as tplink on port 1/0/1:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/1
T2500G-10TS(config)#ip dhcp snooping information circuit-id tplink
```

13.10 ip dhcp snooping trust

Description

The **ip dhcp snooping trust** command is used to configure a port to be a Trusted Port. Only the Trusted Port can receive the DHCP packets from DHCP servers. To turn the port back to a distrusted port, please use **no ip dhcp snooping trust** command.

Syntax

```
ip dhcp snooping trust  
no ip dhcp snooping trust
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure port 2 to be a Trusted Port:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/2  
T2500G-10TS(config-if)# ip dhcp snooping trust
```

13.11 ip dhcp snooping mac-verify

Description

The **ip dhcp snooping mac-verify** command is used to enable the MAC Verify feature. To disable the MAC Verify feature, please use **no ip dhcp snooping mac-verify** command. There are two fields of the DHCP packet containing the MAC address of the Host. The MAC Verify feature is to compare the two fields and discard the packet if the two fields are different.

Syntax

```
ip dhcp snooping mac-verify  
no ip dhcp snooping mac-verify
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the MAC Verify feature for port 2:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/2
T2500G-10TS(config-if)# ip dhcp snooping mac-verify
```

13.12 ip dhcp snooping limit rate

Description

The **ip dhcp snooping limit rate** command is used to enable the Flow Control feature for the DHCP packets. The excessive DHCP packets will be discarded. To restore to the default configuration, please use **no ip dhcp snooping limit rate** command.

Syntax

```
ip dhcp snooping limit rate value
no ip dhcp snooping limit rate
```

Parameter

value — The value of Flow Control. The options are 0/5/10/15/20/25/30(packet/second). The default value is 0, which stands for disable.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Set the Flow Control of port 2 as 20 pps:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/2
T2500G-10TS(config-if)# ip dhcp snooping limit rate 20
```

13.13 ip dhcp snooping decline

Description

The **ip dhcp snooping decline** command is used to enable the Decline Protect feature. To disable the Decline Protect feature, please use **no ip dhcp snooping decline** command.

Syntax

```
ip dhcp snooping decline
no ip dhcp snooping decline
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the Decline Protect feature of port 2:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/2
T2500G-10TS(config-if)# ip dhcp snooping decline
```

13.14 show ip source binding

Description

The **show ip source binding** command is used to display the IP-MAC-VID-PORT binding table.

Syntax

```
show ip source binding
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IP-MAC-VID-PORT binding table:

```
T2500G-10TS(config)# show ip source binding
```

13.15 show ip dhcp snooping information

Description

The **show ip dhcp snooping information** command is used to display the Option 82 configuration status of DHCP-Snooping.

Syntax

```
show ip dhcp snooping information
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the Option 82 configuration status of DHCP-Snooping:

```
T2500G-10TS# show ip dhcp snooping information
```

13.16 show ip dhcp snooping interface gigabitEthernet

Description

The **show ip dhcp snooping interface gigabitEthernet** command is used to display the DHCP-Snooping configuration of desired Gigabit Ethernet ports.

Syntax

```
show ip dhcp snooping interface gigabitEthernet [port]
```

Parameters

port—The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DHCP-Snooping configuration of port 2:

```
T2500G-10TS# show ip dhcp snooping interface gigabitEthernet 1/0/2
```


Chapter 14 ARP Inspection Commands

ARP (Address Resolution Protocol) Detect function is to protect the switch from the ARP cheating, such as the Network Gateway Spoofing and Man-In-The-Middle Attack, etc.

14.1 ip arp inspection(global)

Description

The **ip arp inspection** command is used to enable the ARP Detection function globally. To disable the ARP Detection function, please use **no ip arp detection** command.

Syntax

ip arp inspection
no ip arp inspection

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the ARP Detection function globally:

```
T2500G-10TS(config)#ip arp inspection
```

14.2 ip arp inspection trust

Description

The **ip arp inspection trust** command is used to configure the port for which the ARP Detect function is unnecessary as the Trusted Port. To clear the Trusted Port list, please use **no ip arp detection trust** command. The specific ports, such as up-linked port and routing port and LAG port, should be set as Trusted Port. To ensure the normal communication of the switch, please configure the ARP Trusted Port before enabling the ARP Detect function.

Syntax

```
ip arp inspection trust
no ip arp inspection trust
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure the Gigabit Ethernet ports 1/0/2-5 as the Trusted Port:

```
T2500G-10TS(config)#interface range gigabitEthernet 1/0/2-5
T2500G-10TS(config-if-range)#ip arp inspection trust
```

14.3 ip arp inspection(interface)

Description

The **ip arp inspection** command is used to enable the ARP Defend function. To disable the ARP detection function, please use **no ip arp inspection** command. ARP Attack flood produces lots of ARP Packets, which will occupy the bandwidth and slow the network speed extremely. With the ARP Defend enabled, the switch can terminate receiving the ARP packets for 300 seconds when the transmission speed of the legal ARP packet on the port exceeds the defined value so as to avoid ARP Attack flood.

Syntax

```
ip arp inspection
no ip arp inspection
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the arp defend function for the Gigabit Ethernet ports 1/0/2-6:

```
T2500G-10TS(config)#interface range gigabitEthernet 1/0/2-6
T2500G-10TS(config-if-range)#ip arp inspection
```

14.4 ip arp inspection limit-rate

Description

The **ip arp inspection limit-rate** command is used to configure the ARP speed of a specified port. To restore to the default speed, please use **no ip arp inspection limit-rate** command.

Syntax

```
ip arp inspection limit-rate value
no ip arp inspection limit-rate
```

Parameter

value —The value to specify the maximum amount of the received ARP packets per second, ranging from 10 to 100 in pps(packet/second). By default, the value is 15.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure the maximum amount of the received ARP packets per second as 50 pps for Gigabit Ethernet port 5:

```
T2500G-10TS(config)#interface gigabitEthernet 1/0/5
T2500G-10TS(config-if)#ip arp inspection limit-rate 50
```

14.5 ip arp inspection recover

Description

The **ip arp inspection recover** command is used to restore a port to the ARP transmit status from the ARP filter status.

Syntax

```
ip arp inspection recover
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Restore Gigabit Ethernet port 1/0/5 to the ARP transmit status:

```
T2500G-10TS(config)#interface gigabitEthernet 1/0/5
T2500G-10TS(config-if)#ip arp inspection recover
```

14.6 show ip arp inspection

Description

The **show ip arp inspection** command is used to display the ARP detection global configuration including the enable/disable status and the Trusted Port list.

Syntax

```
show ip arp inspection
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the ARP detection configuration globally:

```
T2500G-10TS(config)#show ip arp inspection
```

14.7 show ip arp inspection interface

Description

The **show ip arp inspection interface** command is used to display the interface configuration of ARP detection.

Syntax

```
show ip arp inspection interface [ gigabitEthernet port ]
```

Parameter

port—The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of Gigabit Ethernet port 1/0/1:

```
T2500G-10TS(config)#show ip arp inspection interface gigabitEthernet  
1/0/1
```

Display the configuration of all Ethernet ports:

```
T2500G-10TS(config)#show ip arp inspection interface
```

14.8 show ip arp inspection statistics

Description

The **show ip arp inspection statistics** command is used to display the number of the illegal ARP packets received.

Syntax

```
show ip arp inspection statistics
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the number of the illegal ARP packets received:

```
T2500G-10TS(config)#show ip arp inspection statistics
```

14.9 clear ip arp inspection statistics

Description

The **clear ip arp inspection statistics** command is used to clear the statistic of the illegal ARP packets received.

Syntax

```
clear ip arp inspection statistics
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

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

Example

Clear the statistic of the illegal ARP packets received:

```
T2500G-10TS(config)#clear ip arp inspection statistics
```

Chapter 15 DoS Defend Commands

DoS (Denial of Service) Attack is to occupy the network bandwidth maliciously by the network attackers or the evil programs sending a lot of service requests to the Host. With the DoS Defend enabled, the switch can analyze the specific field of the received packets and provide the defend measures to ensure the normal working of the local network.

15.1 ip dos-prevent

Description

The **ip dos-prevent** command is used to enable the DoS defend function globally. To disable the DoS defend function, please use **no ip dos-prevent** command.

Syntax

```
ip dos-prevent
no ip dos-prevent
```

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the DoS defend function globally:

```
T2500G-10TS(config)#ip dos-prevent
```

15.2 ip dos-prevent type

Description

The **ip dos-prevent type** command is used to select the DoS Defend Type. To disable the corresponding Defend Type, please use **no ip dos-prevent type** command.

Syntax

```
ip dos-prevent type { land | scan-synfin | xma-scan | null-scan |  
port-less-1024 | blat | ping-flood | syn-flood }
```

```
no ip dos-prevent type { land | scan-synfin | xma-scan | null-scan |  
port-less-1024 | blat | ping-flood | syn-flood }
```

Parameter

land — Land attack.

scan-synfin — Scan SYNFIN attack.

xma-scan — Xma Scan attack.

null-scan — NULL Scan attack.

port-less-1024 — The SYN packets whose Source Port less than 1024.

blat — Blat attack.

ping-flood — Ping flooding attack. With the ping flood attack enabled, the switch will limit automatically the forwarding speed of ping packets to 512K when attacked by ping flood.

syn-flood — SYN/SYN-ACK flooding attack. With the syn-flood attack enabled, the switch will limit automatically the forwarding speed of ping packets to 512K when attacked by syn-flood.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the DoS Defend Type named Land attack:

```
T2500G-10TS(config)#ip dos-prevent type land
```

15.3 show ip dos-prevent

Description

The **show ip dos-prevent** command is used to display the DoS information of the detected DoS attack, including enable/disable status, the DoS Defend Type, the count of the attack, etc.

Syntax

show ip dos-prevent

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DoS information of the detected DoS attack globally:

```
T2500G-10TS(config)#show ip dos-prevent
```

Chapter 16 IEEE 802.1X Commands

IEEE 802.1X function is to provide an access control for LAN ports via the authentication. An 802.1X system include three entities: supplicant, authenticator and authentication server.

- Supplicant: the device that requests access to the LAN.
- Authentication server: performs the actual authentication of the supplicant. It validates the identity of the supplicant and notifies the authenticator whether or not the supplicant is authorized to access the LAN.
- Authenticator: controls the physical access to the network based on the authentication status of the supplicant. It is usually an 802.1X-supported network device, such as this TP-Link switch. It acts as an intermediary (proxy) between the supplicant and the authentication server, requesting identity information from the supplicant, verifying that information with the authentication server, and relaying a response to the supplicant.

This chapter handles with the authentication process between the supplicant and the switch. To realize the authentication and accounting function, you should also enable the AAA function and configure the RADIUS server. Go to [Chapter 44 AAA Commands](#) for more details.

16.1 dot1x system-auth-control

Description

The **dot1x system-auth-control** command is used to enable the IEEE 802.1X function globally. To disable the IEEE 802.1X function, please use **no dot1x system-auth-control** command.

Syntax

```
dot1x system-auth-control  
no dot1x system-auth-control
```

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the IEEE 802.1X function:

```
T2500G-10TS(config)#dot1x system-auth-control
```

16.2 dot1x handshake

Description

The **dot1x handshake** command is used enable the handshake feature. The handshake feature is used to detect the connection status between the TP-Link 802.1x supplicant and the switch. Please disable the handshake feature if you are using a non-TP-Link 802.1x-compliant client software. This feature is enabled by default.

Syntax

dot1x handshake

no dot1x handshake

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Disable the 802.1X handshake function:

```
T2500G-10TS(config)# no dot1x handshake
```

16.3 dot1x auth-method

Description

The **dot1x auth-method** command is used to configure the Authentication Method of IEEE 802.1X and the default 802.1x authentication method is "eap". To restore to the default 802.1x authentication method, please use **no dot1x auth-method** command.

Syntax

dot1x auth-method { pap | eap }

no dot1x auth-method

Parameter

pap | eap —Authentication Methods.

pap: EAP termination mode. IEEE 802.1X authentication system uses extensible authentication protocol (EAP) to exchange information between the switch and the client. The EAP packets are terminated at the switch and repackaged in the Password Authentication Protocol (PAP) packets, and then transferred to the RADIUS server.

eap: EAP relay mode. IEEE 802.1X authentication system uses extensible authentication protocol (EAP) to exchange information between the switch and the client. The EAP protocol packets with authentication data are encapsulated in the advanced protocol (such as RADIUS) packets and transmitted to the authentication server.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the Authentication Method of IEEE 802.1X as "pap":

```
T2500G-10TS(config)#dot1x auth-method pap
```

16.4 dot1x accounting

Description

The **dot1x accounting** command is used to enable the IEEE 802.1X accounting function globally. To disable the IEEE 802.1X accounting function, please use **no dot1x accounting** command.

Syntax

dot1x accounting

no dot1x accounting

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the enable the IEEE 802.1X accounting function globally:

```
T2500G-10TS(config)#dot1x accounting
```

16.5 dot1x vlan-assignment

Description

The **dot1x vlan-assignment** command is used to enable the 802.1X VLAN assignment feature. 802.1x VLAN assignment is a technology allowing the RADIUS server to send the VLAN assignment to the port when the port is authenticated.

If the assigned VLAN does not exist on the switch, the switch will create the related VLAN automatically, add the authenticated port to the VLAN and change the PVID based on the assigned VLAN.

If the assigned VLAN exists on the switch, the switch will directly add the authenticated port to the related VLAN and change the PVID instead of creating a new VLAN.

If no VLAN is supplied by the RADIUS server or if 802.1x authentication is disabled, the port will be in its original VLAN after successful authentication. To disable the 802.1X VLAN assignment feature, please use **no dot1x vlan-assignment** command.

Syntax

```
dot1x vlan-assignment
```

```
no dot1x vlan-assignment
```

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the 802.1X VLAN assignment feature globally:

```
T2500G-10TS(config)# dot1x vlan-assignment
```

16.6 dot1x guest-vlan(global)

Description

The **dot1x guest-vlan** command is used to enable the Guest VLAN function globally. To disable the Guest VLAN function, please use **no dot1x guest-vlan** command.

Syntax

```
dot1x guest-vlan vid  
no dot1x guest-vlan
```

Parameter

vid — The VLAN ID needed to enable the Guest VLAN function, ranging from 2 to 4094. The supplicants in the Guest VLAN can access the specified network source.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the Guest VLAN function for VLAN 5:

```
T2500G-10TS(config)#dot1x guest-vlan 5
```

16.7 dot1x quiet-period

Description

The **dot1x quiet-period** command is used to enable the quiet-period function. To disable the function, please use **no dot1x quiet-period** command.

Syntax

```
dot1x quiet-period [ time ]  
no dot1x quiet-period
```

Parameter

time— The length of the quiet-period time. If one user's authentication fails, its subsequent IEEE 802.1x authentication requests will not be processed during the quiet-period time. It ranges from 1 to 999 seconds and the default value is 10 seconds.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the quiet-period function:

```
T2500G-10TS(config)#dot1x quiet-period
```

Enable the quiet-period function and set the quiet-period as 5 seconds:

```
T2500G-10TS(config)#dot1x quiet-period 5
```

16.8 dot1x timeout supplicant-timeout

Description

The **dot1x timeout supplicant-timeout** command is used to configure the supplicant timeout. To restore to the default, please use **no dot1x timeout supplicant-timeout** command.

Syntax

```
dot1x timeout supplicant-timeout time
```

```
no dot1x timeout supplicant-timeout
```

Parameter

time —The maximum time for the switch to wait for the response from supplicant before resending a request to the supplicant, ranging from 1 to 9 in second. By default, it is 3 seconds.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the supplicant's timeout value as 5 seconds:

```
T2500G-10TS(config)#dot1x timeout supplicant-timeout 5
```

16.9 dot1x max-reauth-req

Description

The **dot1x max-reauth-req** command is used to configure the maximum transfer times of the repeated authentication request when the server cannot be connected. To restore to the default value, please use **no dot1x max-reauth-req** command.

Syntax

```
dot1x max-reauth-req times  
no dot1x max-reauth-req
```

Parameter

times — The maximum transfer times of the repeated authentication request, ranging from 1 to 9 in times. By default, the value is 3.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the maximum transfer times of the repeated authentication request as 5:

```
T2500G-10TS(config)#dot1x max-reauth-req 5
```


16.10 dot1x

Description

The **dot1x** command is used to enable the IEEE 802.1X function for a specified port. To disable the IEEE 802.1X function for a specified port, please use **no dot1x** command.

Syntax

```
dot1x
no dot1x
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the IEEE 802.1X function for the Gigabit Ethernet port 1:

```
T2500G-10TS(config)#interface gigabitEthernet 1/0/1
T2500G-10TS(config-if)#dot1x
```

16.11 dot1x guest-vlan(interface)

Description

The **dot1x guest-vlan** command is used to enable the guest VLAN function for a specified port. To disable the Guest VLAN function for a specified port, please use **no dot1x guest-vlan** command. Please ensure that the Control Type of the corresponding port is port-based before enabling the guest VLAN function for it.

Syntax

```
dot1x guest-vlan
no dot1x guest-vlan
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the Guest VLAN function for Gigabit Ethernet port 1/0/2:

```
T2500G-10TS(config)#interface gigabitEthernet 1/0/2
T2500G-10TS(config-if)#dot1x guest-vlan
```

16.12 dot1x mab

Description

The **dot1x mab** command is used to enable the MAB feature for the port. With MAB feature enabled, the switch automatically sends the authentication server a RADIUS access request frame with the client's MAC address as the username and password. It is also necessary to configure the RADIUS server with the client's information for authentication. You can enable this feature on IEEE 802.1x ports connected to devices without 802.1X capability. For example, most printers, IP phones and fax machines do not have 802.1X capability. To restore to the default configuration, please use **no dot1x mab** command.

Syntax

```
dot1x mab
no dot1x mab
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the MAB feature for Gigabit Ethernet port 20:

```
T2500G-10TS (config)#interface gigabitEthernet 1/0/20
T2500G-10TS (config-if)#dot1x mab
```

16.13 dot1x port-control

Description

The **dot1x port-control** command is used to configure the Control Mode of IEEE 802.1X for the specified port. By default, the control mode is "auto". To restore to the default configuration, please use **no dot1x port-control** command.

Syntax

```
dot1x port-control {auto | authorized-force | unauthorized-force}
```

```
no dot1x port-control
```

Parameter

auto | authorized-force | unauthorized-force — The Control Mode for the port.

auto: In this mode, the port will normally work only after passing the 802.1X Authentication.

authorized-force: In this mode, the port can work normally without passing the 802.1X Authentication.

unauthorized-force: In this mode, the port is forbidden working for its fixed unauthorized status.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure the Control Mode for Gigabit Ethernet port 20 as "authorized-force":

```
T2500G-10TS(config)#interface gigabitEthernet 1/0/20
T2500G-10TS(config-if)#dot1x port-control authorized-force
```

16.14 dot1x port-method

Description

The **dot1x port-method** command is used to configure the control type of IEEE 802.1X for the specified port. By default, the control type is "mac-based". To restore to the default configuration, please use **no dot1x port-method** command.

Syntax

```
dot1x port-method { mac-based | port-based }
no dot1x port-method
```

Parameter

mac-based | port-based —The control type for the port.

mac-based: Any client connected to the port should pass the 802.1X authentication for access.

port-based: All the clients connected to the port can access the network on the condition that any one of the clients has passed the 802.1X Authentication.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure the Control Type for Gigabit Ethernet port 20 as "port-based":

```
T2500G-10TS(config)#interface gigabitEthernet 1/0/20
T2500G-10TS(config-if)#dot1x port-method port-based
```

16.15 show dot1x global

Description

The **show dot1x global** command is used to display the global configuration of 801.X.

Syntax

```
show dot1x global
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of 801.X globally:

```
T2500G-10TS(config)#show dot1x global
```

16.16 show dot1x interface

Description

The **show dot1x interface** command is used to display all ports or the specified port's configuration information of 801.X.

Syntax

```
show dot1x interface [ gigabitEthernet port]
```

Parameter

port—— The Ethernet port number. If not specified, the information of all the ports will be displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration information of 801.X for Gigabit Ethernet port 20:

```
T2500G-10TS(config)#show dot1x interface gigabitEthernet 1/0/20
```

Display the configuration information of 801.X for all Ethernet ports:

```
T2500G-10TS(config)#show dot1x interface
```

Chapter 17 PPPoE ID-Insertion Commands

The PPPoE ID-Insertion feature provides a way to extract a Vendor-specific tag as an identifier for the authentication, authorization, and accounting (AAA) access requests on an Ethernet interface. When enabled, the switch attaches a tag to the PPPoE discovery packets, which is called the PPPoE Vendor-Specific tag and it contains a unique line identifier. There are two formats of Vendor-specific tags: Circuit-ID format and Remote-ID format. The BRAS receives the tagged packet, decodes the tag, and uses the Circuit-ID/Remote-ID field of that tag as a NAS-Port-ID attribute in the RADIUS server for PPP authentication and AAA (authentication, authorization, and accounting) access requests. The switch will remove the Circuit-ID/Remote-ID tag from the received PPPoE Active Discovery Offer and Session-confirmation packets from the BRAS.

17.1 pppoe id-insertion(global)

Description

The **pppoe id-insertion** command is used to enable the PPPoE ID-Insertion function globally. To disable the PPPoE ID-Insertion function, please use **no pppoe id-insertion** command.

Syntax

```
pppoe id-insertion  
no pppoe id-insertion
```

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the PPPoE ID-Insertion function:

```
T2500G-10TS(config)# pppoe id-insertion
```

17.2 pppoe circuit-id(interface)

Description

The **pppoe circuit-id** command is used to enable the PPPoE Circuit-ID Insertion function for a specified port. To disable the PPPoE Circuit-ID Insertion function on a specified port, please use **no pppoe circuit-id** command.

Syntax

```
pppoe circuit-id  
no pppoe circuit-id
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the PPPoE Circuit-ID Insertion function for the Gigabit Ethernet port 1/0/1:

```
T2500G-10TS (config)# interface gigabitEthernet 1/0/1  
T2500G-10TS (config-if)# pppoe circuit-id
```

17.3 pppoe circuit-id type

Description

The **pppoe circuit-id type** command is used to configure the type of PPPoE Circuit-ID for a specified port. By default, the PPPoE Circuit-ID type is "ip".

Syntax

```
pppoe circuit-id type { mac | ip | udf [Value] | udf-only [Value] }
```

Parameter

mac | ip | udf | udf-only — The type of PPPoE Circuit-ID for the port.

mac: The MAC address of the switch will be used to encode the Circuit-ID option.

ip: The IP address of the switch will be used to encode the Circuit-ID option. This is the default value.

udf: A user specified string with the maximum length of 40 characters will be used to encode the Circuit-ID option.

udf-only: Only the user specified string with the maximum length of 40 will be used to encode the Circuit-ID option.

Value — The value of udf/udf-only. The maximum length is 40 characters.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure the type of PPPoE Circuit-ID as "mac" for the Gigabit Ethernet port 1/0/1:

```
T2500G-10TS (config)# interface gigabitEthernet 1/0/1
T2500G-10TS (config-if)# pppoe circuit-id type mac
```

17.4 pppoe remote-id

Description

The **pppoe remote-id** command is used to enable the PPPoE Remote-ID Insertion and configure the Remote-ID value for a specified port. To disable the PPPoE Remote-ID Insertion function on a specified port, please use **no pppoe remote-id** command. By default, the PPPoE Remote-ID Insertion is disabled.

Syntax

```
pppoe remote-id [Value]
```

```
no pppoe remote-id
```

Parameter

Value — The value of UDF. The maximum length is 40 characters. If not specified, the default value will be the PPPoE client's MAC address.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure the remote-ID as "mac" for the Gigabit Ethernet port 1/0/1:

```
T2500G-10TS (config)# interface gigabitEthernet 1/0/1
T2500G-10TS (config-if)# pppoe remote-id mac
```

17.5 show pppoe id-insertion global

Description

The **show pppoe id-insertion global** command is used to display the global configuration of PPPoE Circuit-ID Insertion function.

Syntax

```
show pppoe id-insertion global
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of PPPoE Circuit-ID Insertion function globally:

```
T2500G-10TS # show pppoe circuit-id global
```

17.6 show pppoe id-insertion interface

Description

The **show pppoe id-insertion interface** command is used to display all ports' or the specified port's configuration information of PPPoE Circuit-ID Insertion function.

Syntax

show pppoe id-insertion interface [gigabitEthernet *port*]

Parameter

port—— The Gigabit Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration information of PPPoE Circuit-ID Insertion function of all Ethernet ports:

```
T2500G-10TS# show pppoe id-insertion interface
```

Display the configuration of PPPoE Circuit-ID Insertion function of the Gigabit Ethernet port 1/0/1 :

```
T2500G-10TS# show pppoe id-insertion interface gigabitEthernet 1/0/1
```

Chapter 18 System Log Commands

The log information will record the settings and operation of the switch respectively for you to monitor operation status and diagnose malfunction.

18.1 logging buffer

Description

The **logging buffer** command is used to configure the severity level and the status of the configuration input to the log buffer. To disable the logging buffer function, please use **no logging buffer** command. Local Log is the log information saved in the switch. It has two output channels, that is, it can be saved to two different positions, log buffer and log file. The log buffer indicates the RAM for saving system log and the information in the log buffer can be got by [show logging buffer](#) command. It will be lost when the switch is restarted.

Syntax

logging buffer *level*
no logging buffer

Parameter

level— Severity level of the log information output to each channel. There are 8 severity levels marked with values 0-7. The smaller value has the higher priority. Only the log with the same or smaller severity level value will be output. By default, it is 6 indicating that all the log information between level 0-6 will be saved in the log buffer.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Set the severity level as 5:

```
T2500G-10TS(config)#logging buffer 5
```

18.2 logging file flash

Description

The **logging file flash** command is used to store the log messages in a file in the flash on the switch. To disable the log file flash function, please use **no logging file flash** command. This function is disabled by default. The log file flash indicates the flash sector for saving system log. The information in the log file of the flash will not be lost after the switch is restarted and can be got by the [show logging flash](#) command.

Syntax

logging file flash
no logging file flash

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the log file flash function:

```
T2500G-10TS(config)#logging file flash
```

18.3 logging file flash frequency

Description

The **logging file flash frequency** command is used to specify the frequency to synchronize the system log file in the log buffer to the flash. To resume the default synchronizing frequency, please use the **no logging file flash frequency** command.

Syntax

logging file flash frequency { periodic *periodic* | immediate }
no logging file flash frequency

Parameter

periodic — The frequency to synchronize the system log file in the log buffer to the flash, ranging from 1 to 48 hours. By default, the synchronization process takes place every 24 hours.

immediate — The system log file in the buffer will be synchronized to the flash immediately. This option will reduce the life of the flash and is not recommended.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the log file synchronization frequency as 10 hours:

```
T2500G-10TS(config)#logging file flash frequency periodic 10
```

18.4 logging file flash level

Description

The **logging file flash level** command is used to specify the system log message severity level. Messages with a severity level equal to or higher than this value will be stored to the flash. To restore to the default level, please use **no logging file flash level** command.

Syntax

logging file flash level *level*

no logging file flash level

Parameter

level — Severity level of the log message. There are 8 severity levels marked with values 0-7. The smaller value has the higher priority. Only the log with the same or smaller severity level value will be saved to the flash. By default, it is 2 indicating that the log message marked with 0~2 will be saved in the log flash.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Save the log messages with their severities equal or higher than 7 to the flash :

```
T2500G-10TS(config)#logging file flash level 7
```

18.5 logging host index

Description

The **logging host index** command is used to configure the Log Host. To clear the configuration of the specified Log Host, please use **no logging host index** command. Log Host is to receive the system log from other devices. You can remotely monitor the settings and operation status of other devices through the log host.

Syntax

logging host index *idx host-ip level*

no logging host index *idx*

Parameter

idx—— The index of the log host. The switch supports 4 log hosts at most.

host-ip—— The IP for the log host.

level —— The severity level of the log information sent to each log host. There are 8 severity levels marked with values 0-7. The smaller value has the higher priority. Only the log with the same or smaller severity level value will be sent to the corresponding log host. By default, it is 6 indicating that the log information marked with 0~6 will be sent to the log host.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable log host 2 and set its IP address as 192.168.0.148, the level 5:

```
T2500G-10TS(config)# logging host index 2 192.168.0.148 5
```

18.6 clear logging

Description

The **clear logging** command is used to clear the information in the log buffer and log file.

Syntax

```
clear logging [ buffer | flash ]
```

Parameter

buffer | flash —The output channels: buffer and flash. Clear the information of the two channels, by default.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Clear the information in the log file:

```
T2500G-10TS(config)# clear logging buffer
```

18.7 show logging local-config

Description

The **show logging local-config** command is used to display the configuration of the Local Log output to the console, the terminal, the log buffer and the log file.

Syntax

```
show logging local-config
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of the Local Log:

```
T2500G-10TS(config)# show logging local-config
```

18.8 show logging loghost

Description

The **show logging loghost** command is used to display the configuration of the log host.

Syntax

```
show logging loghost [ index ]
```

Parameter

index —The index of the log host whose configuration will be displayed, ranging from 1 to 4. Display the configuration of all the log hosts by default.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of the log host 2:

```
T2500G-10TS(config)# show logging loghost 2
```

18.9 show logging buffer

Description

The **show logging buffer** command is used to display the log information in the log buffer according to the severity level.

Syntax

```
show logging buffer [ level level ]
```

Parameter

level — Severity level. There are 8 severity levels marked with values 0-7. The information of levels with priority not lower than the select level will display. Display all the log information in the log buffer by default.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the log information from level 0 to level 5 in the log buffer:

```
T2500G-10TS(config)# show logging buffer level 5
```

18.10 show logging flash

Description

The **show logging flash** command is used to display the log information in the log file according to the severity level.

Syntax

```
show logging flash [ level level ]
```

Parameter

level — Severity level. There are 8 severity levels marked with values 0-7. The information of levels with priority not lower than the select level will display. Display all the log information in the log file by default.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the log information with the level marked 0~3 in the log file:

```
T2500G-10TS(config)# show logging flash level 3
```

Chapter 19 SSH Commands

SSH (Security Shell) can provide the unsecured remote management with security and powerful authentication to ensure the security of the management information.

19.1 ip ssh server

Description

The **ip ssh server** command is used to enable SSH function. To disable the SSH function, please use **no ip ssh server** command.

Syntax

ip ssh server
no ip ssh server

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the SSH function:

```
T2500G-10TS(config)# ip ssh server
```

19.2 ip ssh version

Description

The **ip ssh version** command is used to enable the SSH protocol version. To disable the protocol version, please use **no ip ssh version** command.

Syntax

ip ssh version {v1 | v2}
no ip ssh version {v1 | v2}

Parameter

v1 | v2 — The SSH protocol version to be enabled. They represent SSH v1 and SSH v2 respectively.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable SSH v2:

```
T2500G-10TS(config)# ip ssh version v2
```

19.3 ip ssh algorithm

Description

The **ip ssh algorithm** command is used to configure the algorithm in SSH function. To disable the specified algorithm, please use **no ip ssh algorithm** command.

Syntax

```
ip ssh algorithm { AES128-CBC | AES192-CBC | AES256-CBC | Blowfish-CBC  
| Cast128-CBC | 3DES-CBC | HMAC-SHA1 | HMAC-MD5 }
```

```
no ip ssh algorithm
```

Parameter

AES128-CBC | AES192-CBC | AES256-CBC | Blowfish-CBC | Cast128-CBC | 3DES-CBC | HMAC-SHA1 | HMAC-MD5 — Specify the SSH algorithm.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the SSH algorithm as AES128-CBC:

```
T2500G-10TS(config)# ip ssh algorithm AES128-CBC
```

19.4 ip ssh timeout

Description

The **ip ssh timeout** command is used to specify the idle-timeout time of SSH. To restore to the factory defaults, please use **ip ssh timeout** command.

Syntax

```
ip ssh timeout value  
no ip ssh timeout
```

Parameter

value — The Idle-timeout time. During this period, the system will automatically release the connection if there is no operation from the client. It ranges from 1 to 120 in seconds. By default, this value is 120 seconds.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the idle-timeout time of SSH as 30 seconds:

```
T2500G-10TS(config)# ip ssh timeout 30
```

19.5 ip ssh max-client

Description

The **ip ssh max-client** command is used to specify the maximum number of the connections to the SSH server. To return to the default configuration, please use **no ip ssh max-client** command.

Syntax

```
ip ssh max-client num  
no ip ssh max-client
```

Parameter

num — The maximum number of the connections to the SSH server. It ranges from 1 to 5. By default, this value is 5.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the maximum number of the connections to the SSH server as 3:

```
T2500G-10TS(config)# ip ssh max-client 3
```

19.6 ip ssh download

Description

The **ip ssh download** command is used to download the SSH key file from TFTP server.

Syntax

```
ip ssh download { v1 | v2 } key-file ip-address ip-addr
```

Parameter

v1 | v2 — Select the type of SSH key to download, v1 represents SSH-1, v2 represents SSH-2.

key-file — The name of the key-file which is selected to download. The length of the name ranges from 1 to 25 characters. The key length of the downloaded file must be in the range of 512 to 3072 bits.

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Download an SSH-1 type key file named ssh-key from TFTP server with the IP address 192.168.0.148:

```
T2500G-10TS(config)# ip ssh download v1 ssh-key ip-address  
192.168.0.148
```

Download an SSH-1 type key file named ssh-key from TFTP server with the IP address fe80::1234:

```
T2500G-10TS(config)# ip ssh download v1 ssh-key ip-address fe80::1234
```

19.7 remove public-key

Description

The **remove public-key** command is used to remove the SSH public key from the switch.

Syntax

```
remove public-key { v1 | v2 }
```

Parameter

v1 | v2 — Select the type of SSH public key, v1 represents SSH-1, v2 represents SSH-2.

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Remove the SSH-1 type public key from the switch:

```
T2500G-10TS# remove public-key v1
```

19.8 show ip ssh

Description

The **show ip ssh** command is used to display the global configuration of SSH.

Syntax

```
show ip ssh
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of SSH:

```
T2500G-10TS(config)# show ip ssh
```


Chapter 20 MAC Address Commands

MAC Address configuration can improve the network security by configuring the Port Security and maintaining the address information by managing the Address Table.

20.1 mac address-table static

Description

The **mac address-table static** command is used to add the static MAC address entry. To remove the corresponding entry, please use **no mac address-table static** command. The static address can be added or removed manually, independent of the aging time. In the stable networks, the static MAC address entries can facilitate the switch to reduce broadcast packets and enhance the efficiency of packets forwarding remarkably.

Syntax

```
mac address-table static mac-addr vid vid interface gigabitEthernet port  
no mac address-table static { mac-addr | vid vid | mac-addr vid vid |  
interface gigabitEthernet port}
```

Parameter

mac-addr——The MAC address of the entry you desire to add.

vid—— The VLAN ID number of your desired entry. It ranges from 1 to 4094.

port—— The Ethernet port number of your desired entry.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Add a static Mac address entry to bind the MAC address 00:02:58:4f:6c:23, VLAN1 and port 1 together:

```
T2500G-10TS(config)# mac address-table static 00:02:58:4f:6c:23 vid 1  
interface gigabitEthernet 1/0/1
```

20.2 mac address-table aging-time

Description

The **mac address-table aging-time** command is used to configure aging time for the dynamic address. To return to the default configuration, please use **no mac address-table aging-time** command.

Syntax

mac address-table aging-time *aging-time*

no mac address-table aging-time

Parameter

aging-time — The aging time for the dynamic address. The value of it can be 0 or ranges from 10 to 630 seconds. When 0 is entered, the Auto Aging function is disabled. It is 300 by default.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the aging time as 500 seconds:

```
T2500G-10TS(config)# mac address-table aging-time 500
```

20.3 mac address-table filtering

Description

The **mac address-table filtering** command is used to add the filtering address entry. To delete the corresponding entry, please use **no mac address-table filtering** command. The filtering address function is to forbid the undesired package to be forwarded. The filtering address can be added or removed manually, independent of the aging time.

Syntax

mac address-table filtering *mac-addr* **vid** *vid*

no mac address-table filtering {[*mac-addr*] [**vid** *vid*]}

Parameter

mac-addr — The MAC address to be filtered.

vid— The corresponding VLAN ID of the MAC address. It ranges from 1 to 4094.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Add a filtering address entry of which VLAN ID is 1 and MAC address is 00:1e:4b:04:01:5d:

```
T2500G-10TS(config)# mac address-table filtering 00:1e:4b:04:01:5d vid 1
```

20.4 mac address-table max-mac-count

Description

The **mac address-table max-mac-count** command is used to configure the Port Security. To return to the default configurations, please use **no mac address-table max-mac-count** command. Port Security is to protect the switch from the malicious MAC address attack by limiting the maximum number of the MAC addresses that can be learned on the port. The port with Port Security feature enabled will learned the MAC address dynamically. When the learned MAC address number reaches the maximum, the port will stop learning. Therefore, the other devices with the MAC address unlearned can not access to the network via this port.

Syntax

```
mac address-table max-mac-count [ max-number num ] [ mode { dynamic | static | permanent } ] [ status { forward | drop | disable } ]
```

```
no mac address-table max-mac-count [ max-number | mode | status ]
```

Parameter

num — The maximum number of MAC addresses that can be learned on the port. It ranges from 0 to 64. By default this value is 64.

dynamic | static | permanent — Learn mode for MAC addresses. There are three modes, including Dynamic mode, Static mode and Permanent mode. When Dynamic mode is selected, the learned MAC address will be deleted automatically after the aging time. When Static mode is selected, the learned MAC address will be out of the influence of the aging time and can only be

deleted manually. The learned entries will be cleared after the switch is rebooted. When permanent mode is selected, the learned MAC address will be out of the influence of the aging time and can only be deleted manually too. However, the learned entries will be saved even the switch is rebooted.

status — Select the action to be taken when the number of the MAC addresses reaches the maximum learning number on the port. By default this function is disabled.

- forward: The packets will be forward but not be learned when learned MAC number exceeds the the maximum MAC address number on this port.
- drop: The packets will be dropped when learned MAC number exceeds the the maximum MAC address number on this port.
- disable: The MAC address threshold on this port is disabled.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable Port Security function for port 1/0/1, select Static mode as the learn mode, and specify the maximum number of MAC addresses that can be learned on this port as 30. When the number of MAC address entries reaches 30 on this port, new entry will be dropped :

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/1
T2500G-10TS(config-if)# mac address-table max-mac-count max-number
30 mode static status drop
```

20.5 show mac address-table

Description

The **show mac address-table** command is used to display the information of all address entries.

Syntax

```
show mac address-table { dynamic | static | drop | all }
```

Parameter

dynamic | static | drop | all — The type of your desired entry. By default all the entries are displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of all address entries:

```
T2500G-10TS(config)# show mac address-table
```

20.6 clear mac address-table

Description

The **show mac address-table** command is used to clear the specified address entries.

Syntax

```
clear mac address-table { dynamic | static | filtering }
```

Parameter

dynamic | static | filtering — The type of your desired entry.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

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

Example

Clear the information of all static address entries:

```
T2500G-10TS(config)# clear mac address-table static
```

20.7 show mac address-table aging-time

Description

The **show mac address-table aging-time** command is used to display the Aging Time of the MAC address.

Syntax

```
show mac address-table aging-time
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the Aging Time of the MAC address:

```
T2500G-10TS(config)# show mac address-table aging-time
```

20.8 show mac address-table max-mac-count

Description

The **show mac address-table max-mac-count interface gigabitEthernet** command is used to display the security configuration of all ports or the specified port.

Syntax

```
show mac address-table max-mac-count interface gigabitEthernet [port]
```

Parameter

port— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the security configuration of all ports:

```
T2500G-10TS(config)# show mac address-table max-mac-count interface  
gigabitEthernet
```

Display the security configuration of port 1/0/1:

```
T2500G-10TS(config)# show mac address-table max-mac-count interface  
gigabitEthernet 1/0/1
```

20.9 show mac address-table interface

Description

The **show mac address-table interface** command is used to display the address configuration of the specified port.

Syntax

```
show mac address-table interface { gigabitEthernet port}
```

Parameter

port—— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the address configuration of port 1/0/1:

```
T2500G-10TS(config)# show mac address-table interface gigabitEthernet  
1/0/1
```

20.10 show mac address-table count

Description

The **show mac address-table count** command is used to display the total amount of MAC address table.

Syntax

```
show mac address-table count
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the total MAC entry information:

```
T2500G-10TS(config)# show mac address-table count
```

20.11 show mac address-table address

Description

The **show mac address-table address** command is used to display the information of the specified MAC address.

Syntax

```
show mac address-table address mac-addr
```

Parameter

mac-addr——The specified MAC address.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the entry with the MAC address 00:00:00:00:23:00:

```
T2500G-10TS(config)#show mac address-table address 00:00:00:00:23:00
```

20.12 show mac address-table vlan

Description

The **show mac address-table vlan** command is used to display the MAC address configuration of the specified vlan.

Syntax

```
show mac address-table vlan vid
```

Parameter

vid——The specified VLAN id.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the MAC address configuration of vlan 1:

```
T2500G-10TS(config)# show mac address-table vlan 1
```


Chapter 21 System Configuration Commands

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

21.1 system-time manual

Description

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

Syntax

system-time manual *time*

Parameter

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

```
T2500G-10TS(config)# system-time manual 12/20/2010-17:30:35
```

21.2 system-time ntp

Description

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

Syntax

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

Parameter

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

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

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

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

UTC-10:00 — TimeZone for Hawaii.

UTC-09:00 — TimeZone for Alaska.

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

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

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

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

UTC-04:30 — TimeZone for Caracas.

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

UTC-03:30 — TimeZone for Newfoundland.

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

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

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

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

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

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

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

UTC+03:30 — TimeZone for Tehran.

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

UTC+04:30 — TimeZone for Kabul.

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

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

UTC+05:45 — TimeZone for Kathmandu.

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

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

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

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

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

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

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

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

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

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

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

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

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

```
T2500G-10TS(config)# system-time ntp UTC-12:00 133.100.9.2
139.79.100.163 11
```

21.3 system-time dst predefined

Description

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

Syntax

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

no system-time dst

Parameter

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

Following are the time ranges of each option:

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

Australia: First Sunday in October, 02:00 ~ First Sunday in April, 03:00.

Europe: Last Sunday in March, 01:00 ~ Last Sunday in October, 01:00.

New Zealand: Last Sunday in September, 02:00 ~ First Sunday in April, 03:00.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the daylight saving time as USA standard:

```
T2500G-10TS(config)#system-time dst predefined USA
```

21.4 system-time dst date

Description

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

Syntax

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

Parameter

smonth — Month to start, with the options: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec

sday — Day to start, ranging from 1 to 31. Please mind that the number of days depends on the month.

stime — Time to start, in the format of hh:mm.

emonth — Month to end, with the options: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec

eday — Day to end, ranging from 1 to 31. Please mind that the number of days depends on the month.

etime — Time to end, in the format of hh:mm.

offset — Specify the time adding in minutes when Daylight Saving Time comes. The value ranges from 1 to 1440 and the default value is 60 minutes. It is optional.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the DST start time as 00:00 am on April 1st, the end time as 00:00 am on October 1st and the offset as 30 minutes:

```
T2500G-10TS(config)# system-time dst date Apr 1 00:00 Oct 1 00:00 30
```

21.5 system-time dst recurring

Description

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

Syntax

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

Parameter

sweek — Week to start, with the options: first, second, third, fourth, last.

sday — Day to start, with the options: Sun, Mon, Tue, Wed, Thu, Fri, Sat.

smonth — Month to start, with options: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.

stime — Time to start, in the format of: hh:mm.

eweeek — Week to end, with options: first, second, third, fourth, last.

eday — Day to end, with options: Sun, Mon, Tue, Wed, Thu, Fri, Sat.

emonth — Month to end, with options: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.

etime — Time to end, in the format of: hh:mm.

offset — Specify the time adding in minutes when Daylight Saving Time comes. The range of value depends and the default value is 60 minutes. It is optional.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the DST start time of the switch as 2:00 am on the first Sunday in May, the end time as 2:00 am on the last Sunday in October and the offset as 45 minutes:

```
T2500G-10TS(config)# system-time dst recurring first Sun May 02:00 last  
Sun Oct 02:00 45
```

21.6 hostname

Description

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

Syntax

```
hostname [ hostname ]
```

```
no hostname
```

Parameter

hostname — System Name. The length of the name ranges from 1 to 32 characters. By default, it is the device name, for example "T2500G-10TS".

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the system name as TPLINK:

```
T2500G-10TS(config)# hostname TPLINK
```

21.7 location

Description

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

Syntax

```
location [ location ]
```

```
no location
```

Parameter

location — Device Location. It consists of 32 characters at most. It is "SHENZHEN" by default.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the system location as SHENZHEN:

```
T2500G-10TS(config)# location SHENZHEN
```

21.8 contact-info

Description

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

Syntax

```
contact-info [ contact_info ]
```

```
no contact-info
```

Parameter

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

```
T2500G-10TS(config)# contact-info www.tp-link.com
```

21.9 reset

Description

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

Syntax

```
reset
```

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Reset the software of the switch:

```
T2500G-10TS# reset
```

21.10 reboot

Description

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

Syntax

```
reboot
```

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Reboot the switch:

```
T2500G-10TS# reboot
```


21.11 copy running-config startup-config

Description

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

Syntax

```
copy running-config startup-config
```

Command Mode

Privileged EXEC Mode

Privilege Requirement

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

Example

Save current settings:

```
T2500G-10TS# copy running-config startup-config
```

21.12 copy startup-config tftp

Description

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

Syntax

```
copy startup-config tftp ip-address ip-addr filename name
```

Parameter

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

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

Command Mode

Privileged EXEC Mode

Privilege Requirement

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

Example

Backup the configuration files to TFTP server with the IP 192.168.0.148 and name this file config.cfg:

```
T2500G-10TS# copy startup-config tftp ip-address 192.168.0.148
filename config
```

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

```
T2500G-10TS# copy startup-config tftp ip-address fe80::1234 filename
config
```

21.13 copy tftp startup-config

Description

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

Syntax

```
copy tftp startup-config ip-address ip-addr filename name
```

Parameter

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

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

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Download the configuration file named as config.cfg to the switch from TFTP server with the IP 192.168.0.148:

```
T2500G-10TS# copy tftp startup-config ip-address 192.168.0.148
filename config
```

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

```
T2500G-10TS# copy tftp startup-config ip-address fe80::1234 filename
config
```

21.14 boot application

Description

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

Syntax

```
boot application filename { image1 | image 2 } { startup | backup }
```

```
no boot application
```

Parameter

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

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

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the image2.bin as the startup image:

```
T2500G-10TS(config)# boot application filename image2 startup
```

21.15 remove backup-image

Description

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

Syntax

```
remove backup-image
```

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Delete the backup image file:

```
T2500G-10TS# remove backup-image
```

21.16 firmware upgrade

Description

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

Syntax

```
firmware upgrade ip-address ip-addr filename name
```

Parameter

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

name—— Specify the name for the firmware file.

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

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

```
T2500G-10TS# firmware upgrade ip-address 192.168.0.148 filename
firmware.bin

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

Operation OK!

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

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

```
T2500G-10TS# firmware upgrade ip-address fe80::1234 filename
firmware.bin

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

Operation OK!

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

21.17 ping

Description

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

Syntax

```
ping [ip | ipv6] { ip_addr } [-n count] [-l count] [-i count]
```

Parameter

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

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

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

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

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

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

Command Mode

User EXEC Mode and Privileged EXEC Mode

Privilege Requirement

None.

Example

To test the connectivity between the switch and the network device with the IP 192.168.0.131, please specify the *count* (-l) as 512 bytes and *count* (-i) as 1000 milliseconds. If there is not any response after 8 times' Ping test, the connection between the switch and the network device is failed to establish:

```
T2500G-10TS# ping 192.168.0.131 -n 8 -I 512
```

To test the connectivity between the switch and the network device with the IP fe80::1234, please specify the *count* (-l) as 512 bytes and *count* (-i) as 1000 milliseconds. If there is not any response after 8 times' Ping test, the connection between the switch and the network device is failed to establish:

```
T2500G-10TS# ping fe80::1234 -n 8 -I 512
```

21.18 tracert

Description

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

Syntax

```
tracert [ ip | ipv6 ] ip_addr [ maxHops ]
```

Parameter

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

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

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

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

Command Mode

User EXEC Mode and Privileged EXEC Mode

Privilege Requirement

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

Example

Test the connectivity between the switch and the network device with the IP 192.168.0.131. If the destination device has not been found after 20 *maxHops*, the connection between the switch and the destination device is failed to establish:

```
T2500G-10TS# tracert 192.168.0.131 20
```

Test the connectivity between the switch and the network device with the IP fe80::1234. If the destination device has not been found after 20 *maxHops*, the connection between the switch and the destination device is failed to establish:

```
T2500G-10TS# tracert fe80::1234 20
```

21.19 show system-info

Description

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

Syntax

```
show system-info
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the system information:

```
T2500G-10TS# show system-info
```

21.20 show boot

Description

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

Syntax

```
show boot
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the system boot configuration information:

```
T2500G-10TS# show boot
```

21.21 show running-config

Description

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

Syntax

```
show running-config [ all ]
```

Parameter

all — Displays all the current operating configurations. Without this option, only the configurations that differ from the default value will be displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the configurations that differ from the default value:

```
T2500G-10TS# show running-config
```

21.22 show running-config |

Description

The **show running-config |** command is used to filter the output information with the keyword you specify. "|" is a separator indicating the information will be filtered.

Syntax

```
show running-config | { [exclude exclude-keyword] [include  
include-keyword] }
```

Parameter

exclude-keyword — The operating configuration excluding this keyword will be displayed.

include-keyword — The operating configuration including this keyword will be displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the operating configuration that includes the “vlan” keyword:

```
T2500G-10TS# show running-config | include vlan
```

21.23 show startup-config

Description

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

Syntax

```
show startup-config
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the saved configuration:

```
T2500G-10TS# show startup-config
```

21.24 show system-time

Description

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

Syntax

```
show system-time
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the time information of the switch

```
T2500G-10TS# show system-time
```

21.25 show system-time dst

Description

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

Syntax

```
show system-time dst
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DST time information of the switch

```
T2500G-10TS# show system-time dst
```

21.26 show system-time ntp

Description

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

Syntax

```
show system-time ntp
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the NTP mode configuration information of the switch:

```
T2500G-10TS# show system-time ntp
```

21.27 show cable-diagnostics interface gigabitEthernet

Description

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

Syntax

```
show cable-diagnostics interface gigabitEthernet port
```

Parameter

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

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Show the cable-diagnostics of port 3:

```
T2500G-10TS# show cable-diagnostics interface gigabitEthernet 1/0/3
```

21.28 show cable-diagnostics careful interface

Description

The **show cable-diagnostics careful interface gigabitEthernet** command is used to display the connection status of the cable connected to the switch. When taking the careful cable test, the switch will only test the cable for the port which is in the link-down status.

Syntax

show cable-diagnostics careful interface [gigabitEthernet *port*]

Parameter

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

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Show the cable-diagnostics of port 3:

```
T2500G-10TS# show cable-diagnostics careful interface gigabitEthernet  
1/0/3
```

Chapter 22 IPv6 Address Configuration Commands

The IPv6 address configuration commands are provided in the Interface Configuration Mode, which includes the routed port and the VLAN interface. Enter the configuration mode of these Layer 3 interfaces and configure their IPv6 parameters.

22.1 ipv6 enable

Description

This command is used to enable the IPv6 function on the specified Layer 3 interface. IPv6 function should be enabled before the IPv6 address configuration management. By default it is enabled on VLAN interface 1. IPv6 function can only be enabled on one Layer 3 interface at a time.

If the IPv6 function is disabled, the corresponding IPv6 netstack and IPv6-based modules will be invalid, for example SSHv6, SSLv6, TFTPv6 etc. To disable the IPv6 function, please use **no ipv6 enable** command.

Syntax

ipv6 enable
no ipv6 enable

Command Mode

Interface Configuration Mode

Privilege Requirement

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

Example

Enable the IPv6 function on the VLAN interface 1:

```
T2500G-10TS(config)# interface vlan 1
T2500G-10TS(config-if)# ipv6 enable
```

22.2 ipv6 address autoconfig

Description

This command is used to enable the automatic configuration of the ipv6 link-local address. The switch has only one ipv6 link-local address, which can be configured automatically or manually. The general ipv6 link-local address

has the prefix as fe80::/10. IPv6 routers cannot forward packets that have link-local source or destination addresses to other links. The autoconfigured ipv6 link-local address is in EUI-64 format. To verify the uniqueness of the link-local address, the manually configured ipv6 link-local address will be deleted when the autoconfigured ipv6 link-local address takes effect.

Syntax

ipv6 address autoconfig

Configuration Mode

Interface Configuration Mode

Privilege Requirement

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

Example

Enable the automatic configuration of the ipv6 link-local address on VLAN interface 1:

```
T2500G-10TS(config)# interface vlan 1
T2500G-10TS(config-if)# ipv6 address autoconfig
```

22.3 ipv6 address link-local

Description

The **ipv6 address link-local** command is used to configure the ipv6 link-local address manually on a specified interface. To delete the configured link-local address, please use **no ipv6 address link-local** command.

Syntax

ipv6 address *ipv6-addr* **link-local**

no ipv6 address *ipv6-addr* **link-local**

Parameter

ipv6-addr — The link-local address of the interface. It should be a standardized IPv6 address with the prefix fe80::/10, otherwise this command will be invalid.

Configuration Mode

Interface Configuration Mode

Privilege Requirement

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

Example

Configure the link-local address as fe80::1234 on the VLAN interface 1:

```
T2500G-10TS(config)# interface vlan 1
T2500G-10TS(config-if)# ipv6 address fe80::1234 link-local
```

22.4 ipv6 address dhcp

Description

The **ipv6 address dhcp** command is used to enable the DHCPv6 Client function. When this function is enabled, the Layer 3 interface will try to obtain IP from DHCPv6 server. To delete the allocated IP from DHCPv6 server and disable the DHCPv6 Client function, please use **no ipv6 address dhcp** command.

Syntax

```
ipv6 address dhcp
no ipv6 address dhcp
```

Configuration Mode

Interface Configuration Mode

Privilege Requirement

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

Example

Enable the DHCP Client function on VLAN interface 1:

```
T2500G-10TS(config)# interface vlan 1
T2500G-10TS(config-if)# ipv6 address dhcp
```

22.5 ipv6 address ra

Description

This command is used to configure the interface's global IPv6 address according to the address prefix and other configuration parameters from its

received RA(Router Advertisement) message. To disable this function, please use **no ipv6 address ra** command.

Syntax

ipv6 address ra

no ipv6 address ra

Configuration Mode

Interface Configuration Mode

Privilege Requirement

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

Example

Enable the automatic ipv6 address configuration function to obtain IPv6 address through the RA message on VLAN interface 1:

```
T2500G-10TS(config)# interface vlan 1
T2500G-10TS(config-if)# ipv6 address ra
```

22.6 ipv6 address eui-64

Description

This command is used to manually configure a global IPv6 address with an extended unique identifier (EUI) in the low-order 64 bits on the interface. Specify only the network prefix. The last 64 bits are automatically computed from the switch MAC address. To remove an EUI-64 IPv6 address from the interface, please use the **no ipv6 address eui-64** command.

Syntax

ipv6 address *ipv6-addr* eui-64

no ipv6 address *ipv6-addr* eui-64

Parameter

ipv6-addr — Global IPv6 address with 64 bits network prefix, for example 3ffe::/64.

Configuration Mode

Interface Configuration Mode

Privilege Requirement

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

Example

Configure an EUI-64 global address on the interface with the network prefix 3ffe::/64:

```
T2500G-10TS(config)# interface vlan 1
T2500G-10TS(config-if)# ipv6 address 3ffe::/64 eui-64
```

22.7 ipv6 address

Description

This command is used to manually configure a global IPv6 address on the interface. To remove a global IPv6 address from the interface, please use **no ipv6 address** command.

Syntax

```
ipv6 address ipv6-addr
no ipv6 address ipv6-addr
```

Parameter

ipv6-addr — Global IPv6 address with network prefix, for example 3ffe::1/64.

Configuration Mode

Interface Configuration Mode

Privilege Requirement

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

Example

Configure the global address 3001::1/64 on VLAN interface 1:

```
T2500G-10TS(config)# interface vlan 1
T2500G-10TS(config-if)# ipv6 address 3001::1/64
```

22.8 show ipv6 interface

Description

This command is used to display the configured ipv6 information of the management interface, including ipv6 function status, link-local address and global address, ipv6 multicast groups etc.

Syntax

```
show ipv6 interface
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the ipv6 information of the management interface:

```
T2500G-10TS(config)# show ipv6 interface
```

Chapter 23 Ethernet Configuration Commands

Ethernet Configuration Commands can be used to configure the Bandwidth Control, Negotiation Mode and Storm Control for Ethernet ports.

23.1 interface gigabitEthernet

Description

The **interface gigabitEthernet** command is used to enter the Interface gigabitEthernet Configuration Mode and configure the corresponding Gigabit Ethernet port.

Syntax

```
interface gigabitEthernet port
```

Parameter

port—— The Ethernet port number.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

To enter the Interface gigabitEthernet Configuration Mode and configure port 2:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/2
```

23.2 interface range gigabitEthernet

Description

The **interface range gigabitEthernet** command is used to enter the interface range gigabitEthernet Configuration Mode and configure multiple Gigabit Ethernet ports at the same time.

Syntax

interface range gigabitEthernet *port-list*

Parameter

port-list—— The list of Ethernet ports.

Command Mode

Global Configuration Mode

Privilege Requirement

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

User Guidelines

Command in the **Interface Range gigabitEthernet** Mode is executed independently on all ports in the range. It does not affect the execution on the other ports at all if the command results in an error on one port.

Example

To enter the Interface range gigabitEthernet Configuration Mode, and configure ports 1, 2, 3, 6, 7 and 9 at the same time by adding them to one port-list:

```
T2500G-10TS(config)# interface range gigabitEthernet  
1/0/1-3,1/0/6-7,1/0/9
```

23.3 description

Description

The **description** command is used to add a description to the Ethernet port. To clear the description of the corresponding port, please use **no description** command.

Syntax

description *string*

no description

Parameter

string—— Content of a port description, ranging from 1 to 16 characters.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Add a description Port_5 to port 1/0/5:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/5
T2500G-10TS(config-if)# description Port_5
```

23.4 shutdown

Description

The **shutdown** command is used to disable an Ethernet port. To enable this port again, please use **no shutdown** command.

Syntax

shutdown

no shutdown

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Disable port 1/0/3:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/3
T2500G-10TS(config-if)# shutdown
```

23.5 flow-control

Description

The **flow-control** command is used to enable the flow-control function for a port. To disable the flow-control function for this corresponding port, please use **no flow-control** command. With the flow-control function enabled, the Ingress Rate and Egress Rate can be synchronized to avoid packet loss in the network.

Syntax

flow-control

no flow-control

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the flow-control function for port 1/0/3:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/3
T2500G-10TS(config-if)# flow-control
```

23.6 duplex

Description

The **duplex** command is used to configure the Duplex Mode for an Ethernet port. To return to the default configuration, please use **no duplex** command.

Syntax

duplex { auto | full | half }

no duplex

Parameter

auto | full | half — The duplex mode of the Ethernet port. There are three options: auto-negotiation mode, full-duplex mode and half-duplex mode. By default the Gigabit Ethernet port is auto-negotiation mode.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure the Duplex Mode as full-duplex for port 1/0/3:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/3
T2500G-10TS(config-if)# duplex full
```

23.7 speed

Description

The **speed** command is used to configure the Speed Mode for an Ethernet port. To return to the default configuration, please use **no speed** command.

Syntax

```
speed { 10 | 100 | 1000 | auto }
```

```
no speed
```

Parameter

10 | 100 | 1000 | auto — The speed mode of the Ethernet port. There are four options: 10Mbps, 100Mbps, 1000Mbps and Auto negotiation mode (default).

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure the Speed Mode as 100Mbps for port 1/0/3:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/3
T2500G-10TS(config-if)# speed 100
```

23.8 storm-control

Description

The **storm-control** command is used to enable the broadcast, multicast, or unicast storm control function and to set threshold levels on an interface. To disable the storm control function, please use **no storm-control** command.

Syntax

```
storm-control { broadcast | multicast | unicast } rate { rate }  
no storm-control { broadcast | multicast | unicast }
```

Parameter

broadcast | multicast | unicast — Enable broadcast/multicast/unicast storm control on the interface.

rate — Specify the bandwidth for receiving packets on the port. The specified type of packet traffic exceeding the bandwidth will be discarded. The value of it can be 128k | 256k | 512k | 1m | 2m | 4m | 5m | 10m | 20m | 40m | 50m in bps.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure the broadcast storm control rate as 2Mbps on port 1/0/5:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/5  
T2500G-10TS(config-if)# storm-control broadcast rate 2m
```

23.9 bandwidth

Description

The **bandwidth** command is used to configure the bandwidth limit for an Ethernet port. To disable the bandwidth limit, please use **no bandwidth** command.

Syntax

```
bandwidth {[ ingress ingress-rate] [egress egress-rate]}
```


no bandwidth { all | ingress | egress }

Parameter

ingress-rate — Specify the bandwidth for receiving packets. Range: 1-1000000Kbps for the gigaport.

egress-rate — Specify the bandwidth for sending packets. Range: 1-1000000Kbps for the gigaport.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure the ingress-rate as 5120Kbps and egress-rate as 1024Kbps for port 1/0/5:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/5
T2500G-10TS(config-if)# bandwidth ingress 5120 egress 1024
```

23.10 clear counters

Description

The **clear counters** command is used to clear the statistics information of all the Ethernet ports.

Syntax

clear counters

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

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

Example

Clear the statistic information of all ports and port channels:

```
T2500G-10TS(config)# clear counters
```

23.11 show interface status

Description

The **show interface status** command is used to display the connection status of the Ethernet port.

Syntax

```
show interface status
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the connection status of all ports:

```
T2500G-10TS(config)# show interface status
```

23.12 show interface counters

Description

The **show interface counters** command is used to display the statistics information of all ports.

Syntax

```
show interface counters
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the statistics information of all Ethernet ports:

```
T2500G-10TS(config)# show interface counters
```

Display the statistics information of port 1/0/2:

```
T2500G-10TS(config)# show interface counters gigabitEthernet 1/0/2
```

23.13 show interface configuration

Description

The **show interface configuration** command is used to display the configurations of all ports, including Port-status, Flow Control, Negotiation Mode and Port-description.

Syntax

```
show interface configuration
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configurations of all Ethernet ports:

```
T2500G-10TS(config)# show interface configuration
```

23.14 show storm-control

Description

The **show storm-control** command is used to display the storm-control information of Ethernet ports.

Syntax

```
show storm-control [ interface gigabitEthernet port-list]
```

Parameter

port-list——The list of Ethernet ports.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the storm-control information of port 4, 5, 6, and 7:

```
T2500G-10TS(config)# show storm-control interface gigabitEthernet  
1/0/4-7
```

23.15 show bandwidth

Description

The **show bandwidth** command is used to display the bandwidth-limit information of Ethernet ports.

Syntax

```
show bandwidth [ interface gigabitEthernet port-list ]
```

Parameter

port-list——The list of Ethernet ports.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the bandwidth-limit information of port 1/0/4:

```
T2500G-10TS(config)# show bandwidth interface gigabitEthernet 1/0/4
```

Chapter 24 QoS Commands

QoS (Quality of Service) function is used to optimize the network performance. It provides you with network service experience of a better quality.

24.1 qos

Description

The **qos** command is used to configure CoS (Class of Service) based on port. To return to the default configuration, please use **no qos** command.

Syntax

qos *cos-id*

no qos

Parameter

cos-id — The priority of port. It ranges from 0 to 7, which represent CoS0-CoS7 respectively. By default, the priority is 0.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

User Guidelines

Port priority is one property of the port. When the port priority is specified, the data will be classified into the egress queue based on the CoS value of the ingress port and the mapping relation between the CoS and TC in IEEE 802.1P.

Example

Configure the priority of port 5 as 3:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/5
T2500G-10TS(config-if)# qos 3
```

24.2 qos dscp

Description

The **qos dscp** command is used to enable the mapping relation between DSCP Priority and CoS value. To disable the mapping relation, please use **no qos dscp** command.

Syntax

```
qos dscp  
no qos dscp
```

Command Mode

Global Configuration Mode

Privilege Requirement

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

User Guidelines

DSCP (DiffServ Code Point) is a new definition to IP ToS field given by IEEE. DSCP priorities are mapped to the corresponding 802.1p priorities. IP datagram will be classified into the egress queue based on the mapping relation between DSCP priority and CoS value.

Example

Enable the mapping relation between DSCP Priority and CoS value:

```
T2500G-10TS(config)# qos dscp
```

24.3 qos queue cos-map

Description

The **qos queue cos-map** command is used to configure the mapping relation between IEEE 802.1P priority tag/IEEE 802.1Q tag, CoS value and the TC egress queue. To return to the default configuration, please use **no qos queue cos-map** command. When 802.1P Priority is enabled, the packets with 802.1Q tag are mapped to different priority levels based on 802.1P priority mode. The untagged packets are mapped based on port priority mode.

Syntax

```
qos queue cos-map { tag/cos-id } { tc-id }  
no qos queue cos-map
```

Parameter

tag/cos-id — The 8 priority levels defined by IEEE 802.1P or the priority level the packets with tag are mapped to, which ranges from CoS 0 to CoS 7.

tc-id — The egress queue the packets with tag are mapped to. It ranges from 0 to 3, which represents TC0 to TC3 respectively.

Command Mode

Global Configuration Mode

Privilege Requirement

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

User Guidelines

1. By default, the mapping relation between tag/cos and the egress queue is:
0/CoS 0-TC1, 1/CoS 1-TC0, 2/CoS 2-TC0, 3/CoS 3-TC1, 4/CoS 4-TC2, 5/CoS 5-TC2, 6/CoS 6-TC3, 7/CoS 7-TC3.
2. Among the priority levels TC0-TC3, the bigger value, the higher priority.

Example

Map CoS 5 to TC 2:

```
T2500G-10TS(config)# qos queue cos-map 5 2
```

24.4 qos queue dscp-map

Description

The **qos queue dscp-map** command is used to configure the mapping relation between DSCP Priority and the CoS value. To return to the default configuration, please use **no qos queue dscp-map** command. DSCP (DiffServ Code Point) is a new definition to IP ToS field given by IEEE. This field is used to divide IP datagram into 64 priorities. When DSCP Priority is enabled, IP datagram are mapped to different priority levels based on DSCP priority mode; non-IP datagram with IEEE 802.1Q tag are mapped to different priority levels based on IEEE 802.1P priority mode if IEEE 802.1P Priority is enabled; the untagged non-IP datagram are mapped based on port priority mode.

Syntax

```
qos queue dscp-map { dscp-list } { cos-id }  
no qos queue dscp-map
```

Parameter

dscp-list — List of DSCP value. One or several DSCP values can be typed using comma to separate. Use a hyphen to designate a range of values, for instance, 1,4-7,11 indicates choosing 1,4,5,6,7,11. The DSCP value ranges from 0 to 63.

cos-id — The priority level the packets with tag are mapped to, which ranges from CoS 0 to CoS 7.

Command Mode

Global Configuration Mode

Privilege Requirement

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

User Guidelines

By default, the mapping relation between tag and the egress queue is: (0-7)-CoS 0, (8-15)-CoS 1, (16-23)-CoS 2, (24-31)-CoS 3, (32-39)-CoS 4, (40-47)-CoS 5, (48-55)-CoS 6, (56-63)-CoS 7.

Example

Map DSCP values 10-12 to CoS 2:

```
T2500G-10TS(config)# qos queue dscp-map 10-12 2
```

24.5 qos queue mode

Description

The **qos queue mode** command is used to configure the Schedule Mode. To return to the default Equal-Mode, please use **no qos queue mode** command. When the network is congested, the program that many packets complete for resources must be solved, usually in the way of queue scheduling. The switch will control the forwarding sequence of the packets according to the priority queues and scheduling algorithms you set. On this switch, the priority levels are labeled as TC0, TC1,TC2 and TC3.

Syntax

```
qos queue mode { sp | wrr | spwrr | equ }  
no qos queue mode
```


Parameter

sp — Strict-Priority Mode. In this mode, the queue with higher priority will occupy the whole bandwidth. Packets in the queue with lower priority are sent only when the queue with higher priority is empty.

wrr —Weight Round Robin Mode. In this mode, packets in all the queues are sent in order based on the weight value for each queue. The weight value ratio of TC0, TC1, TC2 and TC3 is 1:2:4:8.

spwrr —Strict-Priority + Weight Round Robin Mode. In this mode, the switch provides two scheduling groups, SP group and WRR group. Queues in SP group and WRR group are scheduled strictly based on Strict-Priority mode while the queues inside WRR group follow the WRR mode. In SP + WRR mode, TC3 is the SP group; TC0, TC1 and TC2 belong to the WRR group and the weight value ratio of TC0, TC1 and TC2 is 1:2:4. In this way, when scheduling queues, the switch allows TC3 to occupy the whole bandwidth following the SP mode and the TC0, TC1 and TC2 in the WRR group will take up the bandwidth according to their ratio 1:2:4.

equ — Equal-Mode. In this mode, all the queues occupy the bandwidth equally. The weight value ratio of all the queues is 1:1:1:1.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the Schedule Mode as Weight Round Robin Mode:

```
T2500G-10TS(config)# qos queue mode wrr
```

24.6 show qos interface

Description

The **show qos interface** command is used to display the configuration of QoS based on port priority.

Syntax

```
show qos interface [ gigabitEthernet port | range gigabitEthernet port-list ]
```

Parameter

port — The Ethernet port number.

port-list — The list of Ethernet ports.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of QoS for all ports and LAGs:

```
T2500G-10TS# show qos interface
```

Display the configuration of QoS for ports 1/0/1-4:

```
T2500G-10TS# show qos interface gigabitEthernet 1/0/1-4
```

24.7 show qos cos-map

Description

The **show qos cos-map** command is used to display the configuration of IEEE 802.1P Priority and the mapping relation between cos-id and tc-id.

Syntax

```
show qos cos-map
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of IEEE 802.1P Priority and the mapping relation between cos-id and tc-id:

```
T2500G-10TS# show qos cos-map
```

24.8 show qos dscp-map

Description

The **show qos dscp-map** command is used to display the configuration of DSCP Priority.

Syntax

```
show qos dscp-map
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of DSCP Priority:

```
T2500G-10TS# show qos dscp-map
```

24.9 show qos queue mode

Description

The **show qos queue mode** command is used to display the schedule rule of the egress queues.

Syntax

```
show qos queue mode
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the schedule rule of the egress queues:

```
T2500G-10TS# show qos queue mode
```

24.10 show qos status

Description

The **show qos status** command is used to display the status of IEEE 802.1P priority and DSCP priority.

Syntax

```
show qos status
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the status of IEEE 802.1P priority and DSCP priority:

```
T2500G-10TS# show qos status
```

Chapter 25 Port Mirror Commands

Port Mirror refers to the process of forwarding copies of packets from one port to a monitoring port. Usually, the monitoring port is connected to data diagnose device, which is used to analyze the monitored packets for monitoring and troubleshooting the network.

25.1 monitor session destination interface

Description

The **monitor session destination interface** command is used to configure the monitoring port. Each monitor session has only one monitoring port. To change the monitoring port, please use the **monitor session destination interface** command by changing the port value. The **no monitor session** command is used to delete the corresponding monitoring port or monitor session.

Syntax

```
monitor session session_num destination interface gigabitEthernet port  
no monitor session session_num destination interface gigabitEthernet port  
no monitor session session_num
```

Parameter

session_num — The monitor session number, can only be specified as 1.
port — The monitoring port number.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create monitor session 1 and configure port 1/0/1 as the monitoring port:

```
T2500G-10TS(config)# monitor session 1 destination interface  
gigabitEthernet 1/0/1
```

Delete the monitoring port 1/0/2 from monitor session 1:

```
T2500G-10TS(config)# no monitor session 1 destination interface
gigabitEthernet 1/0/2
```

Delete the monitor session 1:

```
T2500G-10TS(config)# no monitor session 1
```

25.2 monitor session source interface

Description

The **monitor session source interface** command is used to configure the monitored port. To delete the corresponding monitored port, please use **no monitor session source interface** command.

Syntax

```
monitor session session_num source interface gigabitEthernet port-list
mode
```

```
no monitor session session_num source interface gigabitEthernet port-list
mode
```

Parameter

session_num—— The monitor session number, can only be specified as 1.

port-list—— List of monitored port. It is multi-optional.

mode —— The monitor mode. There are three options: rx, tx and both. Rx (ingress monitoring mode), means the incoming packets received by the monitored port will be copied to the monitoring port. Tx (egress monitoring mode), indicates the outgoing packets sent by the monitored port will be copied to the monitoring port. Both (ingress and egress monitoring), presents the incoming packets received and the outgoing packets sent by the monitored port will both be copied to the monitoring port.

Command Mode

Global Configuration Mode

Privilege Requirement

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

User Guidelines

1. The monitoring port is corresponding to current interface configuration mode.
2. Monitored ports number is not limited, but it can't be the monitoring port at the same time.

3. Whether the monitoring port and monitored ports are in the same VLAN or not is not demanded strictly.
4. The monitoring port and monitored ports cannot be link-aggregation member.

Example

Create monitor session 1, then configure port 4, 5, 7 as monitored port and enable ingress monitoring:

```
T2500G-10TS(config)# monitor session 1 source interface
gigabitEthernet 1/0/4-5,1/0/7 rx
```

Delete port 4 in monitor session 1 and its configuration:

```
T2500G-10TS(config)# no monitor session 1 source interface
gigabitEthernet 1/0/4 rx
```

25.3 show monitor session

Description

The **show monitor session** command is used to display the configuration of port monitoring.

Syntax

```
show monitor session [session_num]
```

Parameter

session_num — The monitor session number, can only be specified as 1. It is optional.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the monitoring configuration of monitor session 1:

```
T2500G-10TS(config)# show monitor session 1
```

Chapter 26 Port Isolation Commands

Port Isolation provides a method of restricting traffic flow to improve the network security by forbidding the port to forward packets to the ports that are not on its forwarding port list.

26.1 port isolation

Description

The **port isolation** command is used to configure the forward port/port channel list of a port/port channel, so that this port/port channel can only communicate with the ports/port channels on its list. To delete the corresponding configuration, please use **no port isolation** command.

Syntax

```
port isolation { [ gi-forward-list gi-forward-list ] [ po-forward-list po-forward-list ] }
```

```
no port isolation
```

Parameter

gi-forward-list — The list of Ethernet ports.

po-forward-list — The list of port channels.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Set port 1, 2, 4 and port channel 2 to the forward list of port 1/0/5:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/5
T2500G-10TS(config-if)# port isolation gi-forward-list 1/0/1-2,1/0/4
po-forward-list 2
```

Set all Ethernet ports and port channels to forward list of port 1/0/2, namely restore to the default setting:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/2
T2500G-10TS(config-if)# no port isolation
```


26.2 show port isolation interface

Description

The **show port isolation interface** command is used to display the forward port list of a port.

Syntax

```
show port isolation interface [ gigabitEthernet port ]
```

Parameter

port — The number of Ethernet port you want to show its forward port list, in the format of 1/0/2.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the forward-list of port 1/0/2:

```
T2500G-10TS# show port isolation interface gigabitEthernet 1/0/2
```

Display the forward-list of all Ethernet ports:

```
T2500G-10TS# show port isolation interface
```

Chapter 27 Loopback Detection Commands

With loopback detection feature enabled, the switch can detect loops using loopback detection packets. When a loop is detected, the switch will display an alert or further block the corresponding port according to the configuration.

27.1 loopback-detection(global)

Description

The **loopback-detection** command is used to enable the loopback detection function globally. To disable it, please use **no loopback detection** command.

Syntax

loopback-detection
no loopback-detection

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the loopback detection function globally:

```
T2500G-10TS(config)# loopback-detection
```

27.2 loopback-detection interval

Description

The **loopback-detection interval** command is used to define the interval of sending loopback detection packets from switch ports to network, aiming at detecting network loops periodically.

Syntax

loopback-detection interval *interval-time*

Parameter

interval-time — The interval of sending loopback detection packets. It ranges from 1 to 1000 seconds. By default, this value is 30.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the interval-time as 50 seconds:

```
T2500G-10TS(config)# loopback-detection interval 50
```

27.3 loopback-detection recovery-time

Description

The **loopback-detection recovery-time** command is used to configure the time after which the blocked port would automatically recover to normal status.

Syntax

```
loopback-detection recovery-time recovery-time
```

Parameter

recovery-time—— The time after which the blocked port would automatically recover to normal status, and the loopback detection would restart. It is integral times of detection interval, ranging from 1 to 100 and the default value is 3.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the recovery-time as 3 times of detection interval:

```
T2500G-10TS(config)# loopback-detection recovery-time 3
```

27.4 loopback-detection(interface)

Description

The **loopback-detection** command is used to enable the loopback detection function of the specified port. To disable it, please use **no loopback-detection** command.

Syntax

```
loopback-detection  
no loopback-detection
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the loopback detection function of ports 1-3:

```
T2500G-10TS(config)# interface range gigabitEthernet 1/0/1-3  
T2500G-10TS(Config-if-range)# loopback-detection
```

27.5 loopback-detection config

Description

The **loopback-detection config** command is used to configure the process-mode and recovery-mode for the ports by which the switch copes with the detected loops.

Syntax

```
loopback-detection config process-mode { alert | port-based | vlan-based }  
recovery-mode { auto | manual }
```

Parameter

process-mode — The mode how the switch processes the detected loops.
alert: When a loop is detected, the switch will send a trap message and generate an entry on the log file. It is the default setting.
port-based: When a loop is detected, the switch will send a trap message and generate an entry on the log file. In addition, the switch will block the port on which the loop is detected and no packets can pass through the port.

vlan-based: When a loop is detected, the switch will send a trap message and generate an entry on the log file. In addition, the switch will block the VLAN in which the loop is detected and only the packets of the blocked VLAN cannot pass through the port.

recovery-mode — The mode how the blocked port recovers to normal status.

auto: Block status can be automatically removed after recovery time.

manual: Block status can only be removed manually.

Command Mode

Interface Configuration Mode (interface gigabitEthernet | interface range gigabitEthernet | interface port-channel | interface range port-channel)

Privilege Requirement

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

Example

Configure the loopback detection process-mode as port-based and recovery-mode as manual for port 2:

```
T2500G-10TS (config)# interface gigabitEthernet 1/0/2
T2500G-10TS (config-if)# loopback-detection config process-mode
port-based recovery-mode manual
```

27.6 loopback-detection recover

Description

The **loopback-detection recover** command is used to remove the block status of selected ports, recovering the blocked ports to normal status,

Syntax

loopback-detection recover

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Recover the blocked port 1/0/2 to normal status:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/2
T2500G-10TS(config-if)# loopback-detection recover
```

27.7 show loopback-detection global

Description

The **show loopback-detection global** command is used to display the global configuration of loopback detection function such as loopback detection global status, loopback detection interval and loopback detection recovery time.

Syntax

```
show loopback-detection global
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of loopback detection function:

```
T2500G-10TS# show loopback-detection global
```

27.8 show loopback-detection interface

Description

The **show loopback-detection interface** command is used to display the configuration of loopback detection function and the status of the specified Ethernet port.

Syntax

```
show loopback-detection interface [ gigabitEthernet port]
```

Parameter

port—— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of loopback detection function and the status of all ports:

```
T2500G-10TS# show loopback-detection interface
```

Display the configuration of loopback detection function and the status of port 5:

```
T2500G-10TS# show loopback-detection interface gigabitEthernet 1/0/5
```

Chapter 28 ACL Commands

ACL (Access Control List) is used to filter data packets by configuring a series of match conditions, operations and time ranges. It provides a flexible and secured access control policy and facilitates you to control the network security.

28.1 time-range

Description

The **time-range** command is used to add Time-Range. To delete the corresponding Time-Range, please use **no time-range** command. A time-range based ACL enables you to implement ACL control over packets by differentiating the time-ranges. A time-range can be specified in each rule in an ACL. The rule takes effect only when the specified time-range is configured and the system time is within the time-range.

Syntax

time-range *name*

no time-range *name*

Parameter

name—— The Time-Range name, ranging from 1 to 16 characters.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Add a time-range named tSeg1:

```
T2500G-10TS(config)# time-range tSeg1
```

28.2 absolute

Description

The **absolute** command is used to configure a time-range into an absoluteness mode. To delete the corresponding Absoluteness Mode time-range, please use **no absolute** command.

Syntax

absolute start *start-date* **end** *end-date*

no absolute

Parameter

start-date — The start date in Absoluteness Mode, in the format of MM/DD/YYYY. By default, it is 01/01/1970.

end-date — The end date in Absoluteness Mode, in the format of MM/DD/YYYY. By default, it is 12/31/2099. The Absoluteness Mode will be disabled if the start date and end date are both in default value.

Command Mode

Time-range Configuration Mode

Privilege Requirement

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

Example

Configure the time-range tSeg1 with time from May 5, 2012 to Oct. 5, 2012:

```
T2500G-10TS(config)# time-range tSeg1
T2500G-10TS(config-time-range)# absolute start 05/05/2012 end
10/05/2012
```

28.3 periodic

Description

The **periodic** command is used to configure the time-range into periodic mode. To delete the corresponding Periodic Mode time-range, please use **no periodic** command. To delete the corresponding Periodic Mode week-date time-range, please use **no periodic week-date** command. To delete the corresponding Periodic Mode time-slice time-range, please use **no periodic time-slice** command.

Syntax

periodic [**week-date** *week-day*] [**time-slice1** *time-slice*] [**time-slice2** *time-slice*] [**time-slice3** *time-slice*] [**time-slice4** *time-slice*]

no periodic

no periodic week-date

no periodic time-slice

Parameter

week-day — Periodic Mode, in the format of 1-3,6 or daily, weekend, weekdays. 1-3, 6 represent Monday, Tuesday, Wednesday and Saturday; daily represents every day; weekend represents weekend and weekdays represents working day. By default, the Periodic Mode is disabled.

time-slice — Create the time-slice, in the format of HH:MM-HH:MM.

Command Mode

Time-range Configuration Mode

Privilege Requirement

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

Example

Configure the time-range tSeg1 with time from 8:30 to 12:00 at weekend:

```
T2500G-10TS(config)#time-range tSeg1
T2500G-10TS(config-time-range)#periodic      week-date      weekend
time-slice1 08:30-12:00
```

28.4 holiday

Description

The **holiday** command is used to configure the time-range into Holiday Mode under Time-range Create Configuration Mode. To delete the corresponding Holiday Mode time-range, please use **no holiday** command.

Syntax

holiday

no holiday

Command Mode

Time-range Configuration Mode

Privilege Requirement

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

Example

Configure the time-range tSeg1 into Holiday Mode:

```
T2500G-10TS(config)#time-range tSeg1
```

28.5 holiday(global)

Description

The **holiday** command is used to define a holiday. To delete the corresponding holiday, please use **no holiday** command.

Syntax

holiday *name* **start-date** *start-date* **end-date** *end-date*

no holiday

Parameter

name — The holiday name, ranging from 1 to 16 characters.

start-date — The start date of the holiday, in the format of MM/DD, for instance, 05/01.

end-date — The end date of the holiday, in the format of MM/DD, for instance, 05/03.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Define National Day, configuring the start date as October 1st, and the end date as October 3rd:

```
T2500G-10TS(config)#holiday nationalday start-date 10/01 end-date
10/03
```

28.6 access-list create

Description

The **access-list create** command is used to create standard-IP ACL and extend-IP ACL.

Syntax

access-list create *access-list-num*

Parameter

access-list-num —ACL ID, ranging from 100 to 299. The ID range of Standard-IP ACL range is 100-199 and the Extend-IP ACL is 200-299.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create a standard-IP ACL whose ID is 123:

```
T2500G-10TS(config)# access-list create 123
```

28.7 mac access-list

Description

The **mac access-list** command is used to create MAC ACL. To set the detailed configurations for a specified MAC ACL, please use **mac access-list** command to access Mac Access-list Configuration Mode. To delete the MAC ACL, please use no **mac access-list**.

Syntax

```
mac access-list access-list-num
```

```
no mac access-list access-list-num
```

Parameter

access-list-num — ACL ID, ranging from 0 to 99.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create a MAC ACL whose ID is 23:

```
T2500G-10TS(config)# mac access-list 23
```

28.8 access-list standard

Description

The **access-list standard** command is used to add Standard-IP ACL rule. To delete the corresponding rule, please use **no access-list standard** command. Standard-IP ACLs analyze and process data packets based on a series of match conditions, which can be the source IP addresses and destination IP addresses carried in the packets.

Syntax

```
access-list standard acl-id rule rule-id { deny / permit } [[ sip source-ip ]  
smask source-ip-mask] [[ dip destination-ip ] dmask destination-ip-mask ]  
[ tseg time-segment ]
```

```
no access-list standard acl-id rule rule-id
```

Parameter

acl-id—— The desired Standard-IP ACL for configuration.

rule-id—— The rule ID.

deny —— The operation to discard packets.

permit —— The operation to forward packets. It is the default value.

source-ip—— The source IP address contained in the rule.

source-ip-mask —— The source IP address mask. It is required if you typed the source IP address.

destination-ip—— The destination IP address contained in the rule.

destination-ip-mask —— The destination IP address mask. It is required if you typed the destination IP address.

time-segment —— The time-range for the rule to take effect. By default, it is not limited.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create a Standard-IP ACL whose ID is 120, and add Rule 10 for it. In the rule, the source IP address is 192.168.0.100, the source IP address mask is

255.255.255.0, the time-range for the rule to take effect is "tRange1", and the packets match this rule will be forwarded by the switch:

```
T2500G-10TS(config)# access-list create 120
T2500G-10TS(config)# access-list standard 120 rule 10 permit sip
192.168.0.100 smask 255.255.255.0 tseg tSeg1
```

28.9 access-list extended

Description

The **access-list extended** command is used to add Extended-IP ACL rule. To delete the corresponding rule, please use **no access-list extended** command.

Syntax

```
access-list extended acl-id rule rule-id { deny / permit } [[ sip source-ip ]
smask source-ip-mask ] [[ dip destination-ip] dmask destination-ip-mask ]
[ tseg time-segment ] [frag {disable | enable}] [ dscp dscp ] [ s-port s-port ]
[ d-port d-port] [tcpflag tcpflag] [protocol protocol] [tos tos] [pre pre]
no access-list extended acl-idrule rule-id
```

Parameter

acl-id—The desired Extended-IP ACL for configuration.

rule-id— The rule ID.

deny — The operation to discard packets.

permit —The operation to forward packets. It is the default value.

source-ip— The source IP address contained in the rule.

source-ip-mask — The source IP address mask. It is required if you typed the source IP address.

destination-ip— The destination IP address contained in the rule.

destination-ip-mask — The destination IP address mask. It is required if you typed the destination IP address.

time-segment — The time-range for the rule to take effect. By default, it is not limited.

frag — Enable/Disable Fragment. By default, it is disabled. If Fragment is enabled, this rule will process all the fragments and the last piece of fragment will be always forwarded.

dscp— Specify the dscp value, ranging from 0 to 63.

s-port— The source port number.

d-port— The destination port number.

tcpflag— Specify the flag value when using TCP protocol.

protocol— Configure the value of the matching protocol.

tos— Enter the IP ToS contained in the rule.

pre— Enter the IP Precedence contained in the rule.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create an Extended-IP ACL whose ID is 220, and add Rule 10 for it. In the rule, the source IP address is 192.168.0.100, the source IP address mask is 255.255.255.0, the time-range for the rule to take effect is tSeg1, and the packets match this rule will be forwarded by the switch:

```
T2500G-10TS(config)# access-list create 220
T2500G-10TS(config)# access-list extended 220 rule 10 permit sip
192.168.0.100 smask 255.255.255.0 tseg tSeg1
```

28.10 rule

Description

The **rule** command is used to configure MAC ACL rule. To delete the corresponding rule, please use **no rule** command.

Syntax

```
rule rule-id { deny | permit } [[ smac source-mac ] smask source-mac-mask ]
[[ dmac destination-mac ] dmask destination-mac-mask ] [ vid vlan-id ] [ type
ethernet-type ] [ pri user-pri ] [ tseg time-segment ]
```

```
no rule rule-id
```

Parameter

rule-id— The rule ID.

deny — The operation to discard packets.

permit — The operation to forward packets. It is the default value.

source-mac — The source MAC address contained in the rule.

source-mac-mask — The source MAC address mask. It is required if you typed the source MAC address.

destination-mac — The destination MAC address contained in the rule.

destination-mac-mask — The destination MAC address mask. It is required if you typed the destination MAC address.

vlan-id — The VLAN ID contained in the rule, ranging from 1 to 4094.

ethernet-type — EtherType contained in the rule, in the format of 4-hex number.

user-pri — The user priority contained in the rule, ranging from 0 to 7. By default, it is not limited.

time-segment — The time-range for the rule to take effect. By default, it is not limited.

Command Mode

MAC Access-list Configuration Mode

Privilege Requirement

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

Example

Create a MAC ACL whose ID is 20, and add Rule 10 for it. In the rule, the source MAC address is 00:01:3F:48:16:23, the source MAC address mask is 11:11:11:11:11:00, VLAN ID is 2, the user priority is 5, the time-range for the rule to take effect is "tRange1", and the packets match this rule will be forwarded by the switch:

```
T2500G-10TS(config)# mac access-list 20
T2500G-10TS(config-mac-acl)# rule 10 permit smac 00:01:3F:48:16:23
smask 11:11:11:11:11:00 vid 2 pri 5 tseg tRange1
```

28.11 access-list policy name

Description

The **access-list policy name** command is used to add Policy. To delete the corresponding Policy, please use **no access-list policy name** command. A Policy is used to control the data packets those match the corresponding ACL rules by configuring ACLs and actions together for effect. The

operations here include stream mirror, stream condition, QoS Remarking and redirect.

Syntax

access-list policy name *name*

no access-list policy name *name*

Parameter

name—— The Policy Name, ranging from 1 to 16 characters.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Add a Policy named policy1:

```
T2500G-10TS(config)# access-list policy name policy1
```

28.12 access-list policy action

Description

The **access-list policy action** command is used to add ACLs and create actions for the policy. To set the detailed configuration of actions for a policy, please use **access-list policy action** command to access Action Configuration Mode. To delete the corresponding actions, please use **no access-list policy action** command.

Syntax

access-list policy action *policy-name acl-id*

no access-list policy action *policy-name acl-id*

Parameter

policy-name—— The Policy Name, ranging from 1 to 16 characters.

acl-id—— The ID of the ACL to which the above policy is applied.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Add ACL whose ID is 120 to policy1 and create an action for them:

```
T2500G-10TS(config)# access-list policy action policy1 120
```

28.13 redirect interface

Description

The **redirect interface** command is used to configure Direction function of policy action for specified ports.

Syntax

```
redirect interface { gigabitEthernet port}
```

Parameter

port — The Destination Port of Redirect. The data packets matching the corresponding ACL will be forwarded to the specific port. By default, it is All Ports.

Command Mode

Action Configuration Mode

Privilege Requirement

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

Example

Edit the actions for policy1. Forward the data packets matching ACL 120 in the policy to Gigabit Ethernet port 2:

```
T2500G-10TS(config)#access-list policy action policy1 120
```

```
T2500G-10TS(config-action)#redirect interface gigabitEthernet 1/0/2
```

28.14 s-condition

Description

The **s-condition** command is used to configure Stream Condition function of policy action.

Syntax

s-condition rate *rate* **osd** { none | discard }

Parameter

rate—— The rate of Stream Condition, ranging from 0 to 1000000kbps.

osd —— Out of Band disposal of Stream Condition. It is the disposal way of the data packets those are transmitted beyond the rate. There are two options, "none" and "discard". By default, the option is "none".

Command Mode

Action Configuration Mode

Privilege Requirement

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

Example

Edit the actions for policy1. For the data packets matching ACL 120 in the policy, if the rate beyond 1000kbps, they will be discarded by the switch:

```
T2500G-10TS(config)#access-list policy action policy1 120
```

```
T2500G-10TS(config-action)#s-condition rate 1000 osd discard
```

28.15 s-mirror

Description

The **s-mirror** command is used to configure Stream Mirror function of policy action to the specified port.

Syntax

s-mirror interface { gigabitEthernet *port* }

Parameter

port—— The Mirror Port number of Stream Mirror.

Command Mode

Action Configuration Mode

Privilege Requirement

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

Example

Edit the actions for policy1. Specify the mirror port as Gigabit Ethernet port 1/0/2 for the data packets matching ACL 120:

```
T2500G-10TS(config)#access-list policy action policy1 120
T2500G-10TS(config-action)#s-mirror interface gigabitEthernet 1/0/2
```

28.16 qos-remark

Description

The **qos-remark** command is used to configure QoS Remark function of policy action.

Syntax

```
qos-remark [ dscp dscp] [ priority pri]
no qos-remark
```

Parameter

dscp — DSCP of QoS Remark. Specify the DSCP region for the data packets matching the corresponding ACL. DSCP ranges from 0 to 63. By default, it is not limited.

pri — Local Priority of QoS Remark. Specify the local priority for the data packets matching the corresponding ACL. Local Priority ranges from 0 to 7.

Command Mode

Action Configuration Mode

Privilege Requirement

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

Example

Edit the actions for policy1. For the data packets matching ACL 120, specify the DSCP region as 30 and local priority 2:

```
T2500G-10TS(config)#access-list policy action policy1 120
T2500G-10TS(config-action)# qos-remark dscp 30 priority 2
```

28.17 access-list bind(interface)

Description

The **access-list bind** command is used to bind a policy to a specified port. To cancel the bind relation, please use **no access-list bind** command.

Syntax

access-list bind *policy-name*

no access-list bind *policy-name*

Parameter

policy-name—— The name of the policy desired to bind.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Bind policy1 to port 1/0/2:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/2
T2500G-10TS(config-if)# access-list bind policy1
```

28.18 access-list bind(vlan)

Description

The **access-list bind** command is used to bind a policy to a VLAN. To cancel the bind relation, please use **no access-list bind** command.

Syntax

access-list bind *policy-name*

no access-list bind *policy-name*

Parameter

policy-name—— The name of the policy desired to bind.

Command Mode

Interface VLAN Mode

Privilege Requirement

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

Example

Bind policy1 to VLAN 2:

```
T2500G-10TS(config)# interface vlan 2
T2500G-10TS(config-if)# access-list bind policy1
```

28.19 show access-list

Description

The **show access-list** command is used to display configuration of ACL.

Syntax

```
show access-list acl-id
```

Parameter

acl-id—— The ID of the ACL selected to display the configuration.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of the MAC ACL whose ID is 20:

```
T2500G-10TS(config)# show access-list 20
```

28.20 show access-list status

Description

The **show access-list status** command is used to display the status of ACL hardware entry table. Here you can view the total number and available number of the ACL entries.

Syntax

```
show access-list status
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the status of ACL hardware entry table:

```
T2500G-10TS(config)# show access-list status
```

28.21 show access-list policy

Description

The **show access-list policy** command is used to display the information of a specified policy.

Syntax

```
show access-list policy name
```

Parameter

name — The Policy Name desired to show.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of a policy named policy1:

```
T2500G-10TS(config)# show access-list policy policy1
```

28.22 show access-list bind

Description

The **show access-list bind** command is used to display the configuration of Policy bind.

Syntax

```
show access-list bind
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of Policy bind:

```
T2500G-10TS(config)# show access-list bind
```


Chapter 29 MSTP Commands

MSTP (Multiple Spanning Tree Protocol), compatible with both STP and RSTP and subject to IEEE 802.1s, can disbranch a ring network. STP is to block redundant links and backup links as well as optimize paths.

29.1 spanning-tree(global)

Description

The **spanning-tree** command is used to enable STP function globally. To disable the STP function, please use **no spanning-tree** command.

Syntax

spanning-tree

no spanning-tree

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the STP function:

```
T2500G-10TS(config)# spanning-tree
```

29.2 spanning-tree(interface)

Description

The **spanning-tree** command is used to enable STP function for a port. To disable the STP function, please use **no spanning-tree** command.

Syntax

spanning-tree

no spanning-tree

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the STP function for port 1/0/2:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/2
T2500G-10TS(config-if)# spanning-tree
```

29.3 spanning-tree common-config

Description

The **spanning-tree common-config** command is used to configure the parameters of the ports for comparison in the CIST and the common parameters of all instances. To return to the default configuration, please use **no spanning-tree common-config** command. CIST (Common and Internal Spanning Tree) is the spanning tree in a switched network, connecting all devices in the network.

Syntax

```
spanning-tree common-config [ port-priority pri ] [ ext-cost ext-cost ]
[ int-cost int-cost ] [ portfast { enable | disable } ] [ point-to-point { auto | open
| close } ]
```

```
no spanning-tree common-config
```

Parameter

pri — Port Priority, which must be multiple of 16 ranging from 0 to 240. By default, the port priority is 128. Port Priority is an important criterion on determining if the port connected to this port will be chosen as the root port. In the same condition, the port with the highest priority will be chosen as the root port. The lower value has the higher priority.

ext-cost — External Path Cost, which is used to choose the path and calculate the path costs of ports in different MST regions. It is an important criterion on determining the root port. The lower value has the higher priority. It ranges from 0 to 2000000. By default, it is 0 which is mean auto.

int-cost — Internal Path Cost, which is used to choose the path and calculate the path costs of ports in an MST region. It is an important criterion on determining the root port. The lower value has the higher priority. By

default, it is automatic. It ranges from 0 to 2000000. By default, it is 0 which means auto.

portfast — Enable/ Disable Edge Port. By default, it is disabled. The edge port can transit its state from blocking to forwarding rapidly without waiting for forward delay.

point-to-point — The P2P link status, with auto, open and close options. By default, the option is auto. If the two ports in the P2P link are root port or designated port, they can transit their states to forwarding rapidly to reduce the unnecessary forward delay.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the STP function of port 1, and configure the Port Priority as 64, ExtPath Cost as 100, IntPath Cost as 100, and then enable Edge Port:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/1
T2500G-10TS(config-if)# spanning-tree common-config port-priority 64
ext-cost 100 int-cost 100 portfast enable point-to-point open
```

29.4 spanning-tree mode

Description

The **spanning-tree mode** command is used to configure the STP mode of the switch. To return to the default configurations, please use **no spanning-tree mode** command.

Syntax

```
spanning-tree mode { stp | rstp | mstp }
no spanning-tree mode
```

Parameter

stp — Spanning Tree Protocol, the default value.
rstp — Rapid Spanning Tree Protocol
mstp — Multiple Spanning Tree Protocol

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the spanning-tree mode as mstp:

```
T2500G-10TS(config)# spanning-tree mode mstp
```

29.5 spanning-tree mst configuration

Description

The **spanning-tree mst configuration** command is used to access MST Configuration Mode from Global Configuration Mode, as to configure the VLAN-Instance mapping, region name and revision level. To return to the default configuration of the corresponding Instance, please use **no spanning-tree mst configuration** command.

Syntax

spanning-tree mst configuration

no spanning-tree mst configuration

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enter into the MST configuration mode:

```
T2500G-10TS(config)# spanning-tree mst configuration
```

```
T2500G-10TS(Config-mst)#
```

29.6 instance

Description

The **instance** command is used to configure the VLAN-Instance mapping. To remove the VLAN-instance mapping or disable the corresponding instance,

please use **no instance** command. When an instance is disabled, the related mapping VLANs will be removed.

Syntax

```
instance instance-id vlan vlan-id
```

```
no instance instance-id [vlan vlan-id]
```

Parameters

instance-id — Instance ID, ranging from 1 to 8.

vlan-id — The VLAN ID selected to mapping with the corresponding instance.

Command Mode

MST Configuration Mode

Privilege Requirement

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

Example

Map the VLANs 1-100 to Instance 1:

```
T2500G-10TS(config)# spanning-tree mst configuration
```

```
T2500G-10TS(config-mst)# instance 1 vlan 1-100
```

Disable Instance 1, namely remove all the mapping VLANs 1-100:

```
T2500G-10TS(config)# spanning-tree mst configuration
```

```
T2500G-10TS(config-mst)# no instance 1
```

Remove VLANs 1-50 in mapping VLANs 1-100 for Instance 1:

```
T2500G-10TS(config)# spanning-tree mst configuration
```

```
T2500G-10TS(config-mst)# no instance 1 vlan 1-50
```

29.7 name

Description

The **name** command is used to configure the region name of MST instance.

Syntax

```
name name
```

Parameters

name — The region name, used to identify MST region. It ranges from 1 to 32 characters.

Command Mode

MST Configuration Mode

Privilege Requirement

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

Example

Configure the region name of MST as "region1":

```
T2500G-10TS(config)# spanning-tree mst configuration
T2500G-10TS(config-mst)# name region1
```

29.8 revision

Description

The **revision** command is used to configure the revision level of MST instance.

Syntax

```
revision revision
```

Parameters

revision — The revision level for MST region identification, ranging from 0 to 65535.

Command Mode

MST Configuration Mode

Privilege Requirement

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

Example

Configure the revision level of MST as 100:

```
T2500G-10TS(config)# spanning-tree mst configuration
T2500G-10TS(config-mst)# revision 100
```

29.9 spanning-tree mst instance

Description

The **spanning-tree mst instance** command is used to configure the priority of MST instance. To return to the default value of MST instance priority, please use **no spanning-tree mst instance** command.

Syntax

spanning-tree mst instance *instance-id* **priority** *pri*

no spanning-tree mst instance *instance-id* **priority**

Parameter

instance-id—— Instance ID, ranging from 1 to 8.

pri —— MSTI Priority, which must be multiple of 4096 ranging from 0 to 61440. By default, it is 32768. MSTI priority is an important criterion on determining if the switch will be chosen as the root bridge in the specific instance.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the MST Instance 1 and configure its priority as 4096:

```
T2500G-10TS(config)# spanning-tree mst instance 1 priority 4096
```

29.10 spanning-tree mst

Description

The **spanning-tree mst** command is used to configure MST Instance Port. To return to the default configuration of the corresponding Instance Port, please use **no spanning-tree mst** command. A port can play different roles in different spanning tree instance. You can use this command to configure the parameters of the ports in different instance IDs as well as view status of the ports in the specified instance.

Syntax

spanning-tree mst instance *instance-id*[[**port-priority** *pri*] | [**cost** *cost*]]

no spanning-tree mst instance *instance-id*

Parameter

instance-id— Instance ID, ranging from 1 to 8.

pri— Port Priority, which must be multiple of 16 ranging from 0 to 240. By default, it is 128. Port Priority is an important criterion on determining if the port will be chosen as the root port by the device connected to this port.

cost — Path Cost, ranging from 0 to 200000. The lower value has the higher priority. Its default value is 0 meaning "auto".

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure the priority of port 1 in MST Instance 1 as 64, and path cost as 2000:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/1
T2500G-10TS(config-if)# spanning-tree mst instance 1 port-priority 64
cost 2000
```

29.11 spanning-tree priority

Description

The **spanning-tree priority** command is used to configure the bridge priority. To return to the default value of bridge priority, please use **no spanning-tree priority** command.

Syntax

spanning-tree priority *pri*

no spanning-tree priority

Parameter

pri— Bridge priority, ranging from 0 to 61440. It is 32768 by default.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the bridge priority as 4096:

```
T2500G-10TS(config)# spanning-tree priority 4096
```

29.12 spanning-tree tc-defend

Description

The **spanning-tree tc-defend** command is used to configure the TC Protect of Spanning Tree globally. To return to the default configuration, please use **no spanning-tree tc-defend** command. A switch removes MAC address entries upon receiving TC-BPDUs. If a malicious user continuously sends TC-BPDUs to a switch, the switch will be busy with removing MAC address entries, which may decrease the performance and stability of the network.

Syntax

```
spanning-tree tc-defend threshold threshold period period
```

```
no spanning-tree tc-defend
```

Parameter

threshold—— TC Threshold, ranging from 1 to 100 packets. By default, it is 20. TC Threshold is the maximum number of the TC-BPDUs received by the switch in a TC Protect Cycle.

period—— TC Protect Cycle, ranging from 1 to 10 in seconds. By default, it is 5.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure TC Threshold as 30 packets and TC Protect Cycle as 10 seconds:

```
T2500G-10TS(config)# spanning-tree tc-defend threshold 30 period 10
```

29.13 spanning-tree timer

Description

The **spanning-tree timer** command is used to configure forward-time, hello-time and max-age of Spanning Tree. To return to the default configurations, please use **no spanning-tree timer** command.

Syntax

```
spanning-tree timer {[ forward-time forward-time ] [ hello-time hello-time ]  
[ max-age max-age ]}
```

```
no spanning-tree timer
```

Parameter

forward-time — Forward Delay, which is the time for the port to transit its state after the network topology is changed. Forward Delay ranges from 4 to 30 in seconds and it is 15 by default. Otherwise, $2 * (\text{Forward Delay} - 1) \geq \text{Max Age}$.

hello-time — Hello Time, which is the interval to send BPDU packets, and used to test the links. Hello Time ranges from 1 to 10 in seconds and it is 2 by default. Otherwise, $2 * (\text{Hello Time} + 1) \leq \text{Max Age}$.

max-age — The maximum time the switch can wait without receiving a BPDU before attempting to reconfigure, ranging from 6 to 40 in seconds. By default, it is 20.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure forward-time, hello-time and max-age for Spanning Tree as 16 seconds, 3 seconds and 22 seconds respectively:

```
T2500G-10TS(config)# spanning-tree timer forward-time 16 hello-time 3  
max-age 22
```

29.14 spanning-tree hold-count

Description

The **spanning-tree hold-count** command is used to configure the maximum number of BPDU packets transmitted per Hello Time interval. To return to the default configurations, please use **no spanning-tree hold-count** command.

Syntax

spanning-tree hold-count *value*

no spanning-tree hold-count

Parameter

value—— The maximum number of BPDU packets transmitted per Hello Time interval, ranging from 1 to 20 in pps. By default, it is 5.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the hold-count of STP as 8pps:

```
T2500G-10TS(config)# spanning-tree hold-count 8
```

29.15 spanning-tree max-hops

Description

The **spanning-tree max-hops** command is used to configure the maximum number of hops that occur in a specific region before the BPDU is discarded. To return to the default configurations, please use **no spanning-tree max-hops** command.

Syntax

spanning-tree max-hops *value*

no spanning-tree max-hops

Parameter

value —— The maximum number of hops that occur in a specific region before the BPDU is discarded, ranging from 1 to 40 in hop. By default, it is 20.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the max-hops of STP as 30:

```
T2500G-10TS(config)# spanning-tree max-hops 30
```

29.16 spanning-tree bpdudfilter

Description

The **spanning-tree bpdudfilter** command is used to enable the BPDU filter function for a port. With the function enabled, the port can be prevented from receiving and sending any BPDU packets. To disable the BPDU filter function, please use **no spanning-tree bpdudfilter** command.

Syntax

spanning-tree bpdudfilter

no spanning-tree bpdudfilter

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the BPDU filter function for port 1/0/2:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/2
```

```
T2500G-10TS(config-if)# spanning-tree bpdudfilter
```

29.17 spanning-tree bpduguard

Description

The **spanning-tree bpduguard** command is used to enable the BPDU protect function for a port. With the BPDU protect function enabled, the port will set

itself automatically as ERROR-PORT when it receives BPDU packets, and the port will disable the forwarding function for a while. To disable the BPDU protect function, please use **no spanning-tree bpduguard** command.

Syntax

spanning-tree bpduguard

no spanning-tree bpduguard

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the BPDU protect function for port 1/0/2:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/2
```

```
T2500G-10TS(config-if)# spanning-tree bpduguard
```

29.18 spanning-tree guard loop

Description

The **spanning-tree guard loop** command is used to enable the Loop Protect function for a port. Loop Protect is to prevent the loops in the network brought by recalculating STP because of link failures and network congestions. To disable the Loop Protect function, please use **no spanning-tree guard loop** command.

Syntax

spanning-tree guard loop

no spanning-tree guard loop

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the Loop Protect function for port 2:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/2
T2500G-10TS(config-if)# spanning-tree guard loop
```

29.19 spanning-tree guard root

Description

The **spanning-tree guard root** command is used to enable the Root Protect function for a port. With the Root Protect function enabled, the root bridge will set itself automatically as ERROR-PORT when receiving BPDU packets with higher priority, in order to maintain the role of root ridge. To disable the Root Protect function, please use **no spanning-tree guard root** command.

Syntax

```
spanning-tree guard root
no spanning-tree guard root
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the Root Protect function for port 2:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/2
T2500G-10TS(config-if)# spanning-tree guard root
```

29.20 spanning-tree guard tc

Description

The **spanning-tree guard tc** command is used to enable the TC Protect of Spanning Tree function for a port. To disable the TC Protect of Spanning Tree function, please use **no spanning-tree guard tc** command. A switch removes MAC address entries upon receiving TC-BPDUs. If a malicious user continuously sends TC-BPDUs to a switch, the switch will be busy with

removing MAC address entries, which may decrease the performance and stability of the network. With the Protect of Spanning Tree function enabled, you can configure the number of TC-BPDUs in a required time, so as to avoid the process of removing MAC addresses frequently.

Syntax

spanning-tree guard tc

no spanning-tree guard tc

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the TC Protect of Spanning Tree for port 2:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/2
T2500G-10TS(config-if)# spanning-tree guard tc
```

29.21 spanning-tree mcheck

Description

The **spanning-tree mcheck** command is used to enable mcheck.

Syntax

spanning-tree mcheck

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable mcheck for port 2:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/2
T2500G-10TS(config-if)# spanning-tree mcheck
```

29.22 show spanning-tree active

Description

The **show spanning-tree active** command is used to display the active information of spanning-tree.

Syntax

```
show spanning-tree active
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the active information of spanning-tree:

```
T2500G-10TS(config)# show spanning-tree active
```

29.23 show spanning-tree bridge

Description

The **show spanning-tree bridge** command is used to display the bridge parameters.

Syntax

```
show spanning-tree bridge [ forward-time | hello-time | hold-count | max-age  
| max-hops | mode | priority | state ]
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the bridge parameters:

```
T2500G-10TS(config)# show spanning-tree bridge
```


29.24 show spanning-tree interface

Description

The **show spanning-tree interface** command is used to display the spanning-tree information of all ports or a specified port.

Syntax

```
show spanning-tree interface [ gigabitEthernet port ] [ edge | ext-cost |  
int-cost | mode | p2p | priority | role | state | status ]
```

Parameter

port—— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the spanning-tree information of all ports:

```
T2500G-10TS(config)# show spanning-tree interface
```

Display the spanning-tree information of port 1/0/2:

```
T2500G-10TS(config)# show spanning-tree interface gigabitEthernet  
1/0/2
```

Display the spanning-tree mode information of port 1/0/2:

```
T2500G-10TS(config)# show spanning-tree interface gigabitEthernet  
1/0/2 mode
```

29.25 show spanning-tree interface-security

Description

The **show spanning-tree interface-security** command is used to display the protect information of all ports or a specified port.

Syntax

```
show spanning-tree interface-security [ gigabitEthernet port ] [ bpdufilter |  
bpduguard | loop | root | tc | tc-defend ]
```

Parameter

port— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the protect information of all ports:

```
T2500G-10TS(config)# show spanning-tree interface-security
```

Display the protect information of port 1:

```
T2500G-10TS(config)# show spanning-tree interface-security
gigabitEthernet 1/0/1
```

Display the interface security bpdudfilter information:

```
T2500G-10TS(config)# show spanning-tree interface-security bpdudfilter
```

29.26 show spanning-tree mst

Description

The **show spanning-tree mst** command is used to display the related information of MST Instance.

Syntax

```
show spanning-tree mst { configuration [ digest ] | instance instance-id
[ interface [ gigabitEthernet port ] }
```

Parameter

instance-id— Instance ID desired to show, ranging from 1 to 8.

port— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the region information and mapping information of VLAN and MST Instance:

```
T2500G-10TS(config)#show spanning-tree mst configuration
```

Display the related information of MST Instance 1:

```
T2500G-10TS(config)#show spanning-tree mst instance 1
```

Display all the ports information of MST Instance 1:

```
T2500G-10TS(config)#show spanning-tree mst instance 1 interface
```

Chapter 30 DLDP Commands

DLDP (Device Link Detection Protocol) is used to monitor the link state of fiber-optic or twisted-pair Ethernet cables. When a unidirectional link is detected, the corresponding port will be shut down automatically or manually (depending on the shut mode configured).

30.1 dldp(global)

Description

The **dldp** command is used to enable the DLDP function globally. To disable it, please use **no dldp** command.

Syntax

dldp
no dldp

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the DLDP function globally:

```
T2500G-10TS(config)# dldp
```

30.2 dldp interval

Description

The **dldp interval** command is used to define the interval of sending advertisement packets on ports that are in the advertisement state.

Syntax

dldp interval *interval-time*

Parameter

interval-time — The interval of sending advertisement packets. It ranges from 1 to 30 seconds. By default, it is 5 seconds.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the interval of sending advertisement packets as 10 seconds:

```
T2500G-10TS(config)# dldp interval 10
```

30.3 dldp shut-mode

Description

The **dldp shut-mode** command is used to configure the shutdown mode when a unidirectional link is detected.

Syntax

```
dldp shut-mode { auto | manual }
```

Parameter

auto — The switch automatically shuts down ports when a unidirectional link is detected. By default, the shut-mode is auto.

manual — The switch displays an alert when a unidirectional link is detected. The operation to shut down the unidirectional link ports is accomplished by the users.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the shut-mode as manual:

```
T2500G-10TS(config)# dldp shut-mode manual
```

30.4 dldp reset(global)

Description

The **dldp reset** command is used to reset all the unidirectional links and restart the link detect process.

Syntax

```
dldp reset
```

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Reset the DLDP function globally:

```
T2500G-10TS(config)# dldp reset
```

30.5 dldp(interface)

Description

The **dldp** command is used to enable the DLDP function of the specified port. To disable it, please use **no dldp** command.

Syntax

```
dldp  
no dldp
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the DLDP function of ports 1/0/2-4:

```
T2500G-10TS (config)# interface range gigabitEthernet 1/0/2-4
```

```
T2500G-10TS (config-if-range)# dldp
```

30.6 dldp reset(interface)

Description

The **dldp reset** command is used to reset the specified port and restart the link detect process.

Syntax

```
dldp reset
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Reset the DLDP function of ports 2-4:

```
T2500G-10TS (config)# interface range gigabitEthernet 1/0/2-4
T2500G-10TS (config-if-range)# dldp reset
```

30.7 show dldp

Description

The **show dldp** command is used to display the global configuration of DLDP function such as DLDP global state, DLDP interval and shut mode.

Syntax

```
show dldp
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of DLDP function:

```
T2500G-10TS# show dldp
```

30.8 show dldp interface

Description

The **show dldp interface** command is used to display the configuration and state of the specified Ethernet port. By default, the configuration and state of all the ports will be displayed.

Syntax

```
show dldp interface [gigabitEthernet port]
```

Parameter

port—— The Gigabit Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration and state of all ports:

```
T2500G-10TS# show dldp interface
```

Display the configuration and state of port 1/0/5:

```
T2500G-10TS# show dldp interface gigabitEthernet 1/0/5
```


Chapter 31 IGMP Snooping Commands

IGMP Snooping (Internet Group Management Protocol Snooping) is a multicast control mechanism running on Layer 2 switch. It can effectively prevent multicast groups being broadcasted in the network.

31.1 ip igmp snooping(global)

Description

The **ip igmp snooping** command is used to configure IGMP Snooping globally. To disable the IGMP Snooping function, please use **no ip igmp snooping** command.

Syntax

ip igmp snooping
no ip igmp snooping

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable IGMP Snooping function:

```
T2500G-10TS(config)# ip igmp snooping
```

31.2 ip igmp snooping(interface)

Description

The **ip igmp snooping** command is used to enable the IGMP Snooping function for the desired port. To disable the IGMP Snooping function, please use **no ip igmp snooping** command.

Syntax

ip igmp snooping
no ip igmp snooping

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable IGMP Snooping function of port 1/0/3:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/3
T2500G-10TS(config-if)# ip igmp snooping
```

31.3 ip igmp snooping report-suppression

Description

The **ip igmp snooping report-suppression** command is used enable the IGMP report suppression function. When it is enabled, the switch forwards only the first IGMP report message per multicast group to the Layer 3 device, and the subsequent IGMP reports from the same multicast group are discarded. To disable the IGMP report suppression function and forward all the IGMP reports to the Layer 3 device, please use **no ip igmp snooping report-suppression** command. This function is disabled by default.

Syntax

```
ip igmp snooping report-suppression
no ip igmp snooping report-suppression
```

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the IGMP report suppression function:

```
T2500G-10TS(config)# ip igmp snooping report-suppression
```

31.4 ip igmp snooping immediate-leave

Description

The **ip igmp snooping immediate-leave** command is used to configure the Fast Leave function for port. To disable the Fast Leave function, please use **no ip igmp snooping immediate-leave** command.

Syntax

ip igmp snooping immediate-leave
no ip igmp snooping immediate-leave

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the Fast Leave function for port 1/0/3:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/3
T2500G-10TS(config-if)# ip igmp snooping immediate-leave
```

31.5 ip igmp snooping drop-unknown

Description

The **ip igmp snooping drop-unknown** command is used to process the unknown multicast as discard. To disable the operation of processing the unknown multicast as discard, please use **no ip igmp snooping drop-unknown** command.

Syntax

ip igmp snooping drop-unknown
no ip igmp snooping drop-unknown

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the operation to process unknown multicast as discard:

```
T2500G-10TS(config)# ip igmp snooping drop-unknown
```

31.6 ip igmp snooping vlan-config

Description

The **ip igmp snooping vlan-config** command is used to enable VLAN IGMP Snooping function or to modify IGMP Snooping parameters, and to create static multicast IP entry. To disable the VLAN IGMP Snooping function, please use **no ip igmp snooping vlan-config** command. To restore the default values, please use **no ip igmp snooping vlan-config** with specified parameters.

Syntax

```
ip igmp snooping vlan-config vlan-id-list [ rtime router-time | mtime member-time | ltime leave-time | rport interface gigabitEthernet port-list ]
```

```
ip igmp snooping vlan-config vlan-id-list static ip interface gigabitEthernet port-list
```

```
no ip igmp snooping vlan-config vlan-id-list [ rport interface gigabitEthernet port-list ]
```

```
no ip igmp snooping vlan-config vlan-id-list static ip interface gigabitEthernet port-list
```

Parameter

vlan-id-list — The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

router-time — Router Port Time. Within this time, if the switch does not receive IGMP query message from the router port, it will consider this port is not a router port any more. Router Port Time ranges from 60 to 600 in seconds. By default, it is 0 and the global router-time will be used.

member-time — Member Port Time. Within this time, if the switch does not receive IGMP report message from the member port, it will consider this port is not a member port any more. Member Port Time ranges from 60 to 600 in seconds. By default, it is 0 and the global member-time will be used.

leave-time — Leave Time, which is the interval between the switch receiving a leave message from a host and the switch removing the host from

the multicast groups. Leave Time ranges from 1 to 30 in seconds. By default, it is 1.

port-list—— The list of Ethernet ports.

ip—— The static multicast IP address.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the IGMP Snooping function and modify Router Port Time as 300 seconds, Member Port Time as 200 seconds for VLAN 1-3, and set the router port as 1/0/1 for VLAN 1-2:

```
T2500G-10TS(config)# ip igmp snooping vlan-config 1-3 rtime 300
T2500G-10TS(config)# ip igmp snooping vlan-config 1-3 mtime 200
T2500G-10TS(config)# ip igmp snooping vlan-config 1-2 rport interface
gigabitEthernet 1/0/1
```

Add static multicast IP address 225.0.0.1, which corresponds to VLAN 2, and configure the forward ports as ports 1/0/1-3:

```
T2500G-10TS(config)# ip igmp snooping vlan-config 2 static 225.0.0.1
interface gigabitEthernet 1/0/1-3
```

31.7 ip igmp snooping multi-vlan-config

Description

The **ip igmp snooping multi-vlan-config** command is used to create Multicast VLAN. To delete the corresponding Multicast VLAN, please use **no ip igmp snooping multi-vlan-config** command. To restore the default values, please use **no ip igmp snooping multi-vlan-config** with specified parameters.

Syntax

```
ip igmp snooping multi-vlan-config [ vlan-id ] [ rtime router-time | mtime member-time | ltime leave-time | rport interface gigabitEthernet port-list ]
```

```
no ip igmp snooping multi-vlan-config [ vlan-id ] [rport interface
gigabitEthernet port-list]
```

Parameter

vlan-id—— The ID of the multicast VLAN desired to create or modify, ranging from 2 to 4094. If not specified, the default multicast VLAN will be selected.

router-time —— Router Port Time. Within this time, if the switch does not receive IGMP query message from the router port, it will consider this port is not a router port any more. Router Port Time ranges from 60 to 600 in seconds. By default, it is 0 and the global router-time will be used.

member-time —— Member Port Time. Within this time, if the switch does not receive IGMP report message from the member port, it will consider this port is not a member port any more. Member Port Time ranges from 60 to 600 in seconds. By default, it is 0 and the global member-time will be used.

leave-time —— Leave Time, which is the interval between the switch receiving a leave message from a host and the switch removing the host from the multicast groups. Leave Time ranges from 1 to 30 in seconds. By default, it is 1.

port-list —— The list of Ethernet ports.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable Multicast VLAN 3, and configure Router Port Time as 100 seconds, Member Port Time 100 seconds, and Static Router Port port 1/0/3:

```
T2500G-10TS(config)# ip igmp snooping multi-vlan-config 3 rtime 100
T2500G-10TS(config)# ip igmp snooping multi-vlan-config 3 mtime 100
T2500G-10TS(config)# ip igmp snooping multi-vlan-config 3 rport
interface gigabitEthernet 1/0/3
```

31.8 ip igmp snooping filter(global)

Description

The **ip igmp snooping filter** command is used to add or modify the multicast filtering IP-range. To delete the multicast filtering IP-range, please use **no ip igmp snooping filter** command.

Syntax

```
ip igmp snooping filter id start-ip end-ip
```

```
no ip igmp snooping filter id
```

Parameter

id—— IP-range ID, ranging from 1 to 30.

start-ip—— The start multicast IP of the IP-range.

end-ip—— The end multicast IP of the IP-range.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Modify the multicast IP-range whose ID is 3 as 225.1.1.1–226.3.2.1:

```
T2500G-10TS(config)#ip igmp snooping filter 3 225.1.1.1 226.3.2.1
```

31.9 ip igmp snooping filter(interface)

Description

The **ip igmp snooping filter** command is used to configure Port Filter. To return to the default configuration, please use **no igmp snooping filter** command. When the switch receives IGMP report message, it examines the multicast filtering IP ID configured on the access port to determine if the port can join the multicast group. If the multicast IP is not filtered, the switch will add the port to the forward port list of the multicast group. Otherwise, the switch will drop the IGMP report message. In that way, you can control the multicast groups that users can access.

Syntax

ip igmp snooping filter

no ip igmp snooping filter

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable IGMP Snooping filter function for Gigabit Ethernet port 1/0/2:

```
T2500G-10TS(config)#interface gigabitEthernet 1/0/2
```

```
T2500G-10TS(config-if)#ip igmp snooping filter
```

31.10 ip igmp snooping filter add-id

Description

The **ip igmp snooping filter add-id** command is used to configure the multicast IP-range desired to filter. To delete the corresponding IP-range, please use **no ip igmp snooping filter add-id** command. When IGMP Snooping is enabled, you can specified the multicast IP-range the ports can join so as to restrict users ordering multicast programs via configuring multicast filter rules. Multicast IP addresses ranges from 224.0.0.0 to 239.255.255.255. The range for receivers to join is from 224.0.1.0 to 239.255.255.255.

Syntax

ip igmp snooping filter addr-id *addr-id list*

no ip igmp snooping filter addr-id *addr-id list*

Parameter

addr-id list—— The filtering address ID to be bound.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Bind the filtering address ID 2-6 to Gigabit Ethernet port 1/0/3:

```
T2500G-10TS(config)#interface gigabitEthernet 1/0/3
T2500G-10TS(config-if)#ip igmp snooping filter addr-id 2-6
```

31.11 ip igmp snooping filter maxgroup

Description

The **ip igmp snooping filter maxgroup** command is used to specify the maximum number of multicast groups for a port to join in.

Syntax

```
ip igmp snooping filter maxgroup maxgroup
```

Parameter

maxgroup — The maximum number of multicast groups for a port to join in. It is used to prevent some ports taking up too much bandwidth.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Specify the maximum number of multicast groups for Gigabit Ethernet ports 1/0/2-3 to join in as 10:

```
T2500G-10TS(config)#interface range gigabitEthernet 1/0/2-3
T2500G-10TS(config-if-range)#ip igmp snooping filter maxgroup 10
```

31.12 ip igmp snooping filter mode

Description

The **ip igmp snooping filter mode** command is used to configure the Action mode for the desired port.

Syntax

ip igmp snooping filter mode *mode*

Parameter

mode — Action Mode, with “refuse” and “accept” options. “Refuse” indicates only the multicast packets whose multicast IP is not in the IP-range will be processed, while “accept” indicates only the multicast packets whose multicast IP is in the IP-range will be processed. By default, the option is “accept”.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Specify the Action Mode as “accept” for Gigabit Ethernet port 1/0/3:

```
T2500G-10TS(config)#interface gigabitEthernet 1/0/3
T2500G-10TS(config-if)#ip igmp snooping filter mode accept
```

31.13 ip igmp snooping querier vlan

Description

The **ip igmp snooping querier vlan** command is used to enable the IGMP Snooping Querier function of the VLAN(s). To disable the IGMP Snooping Querier function of certain VLANs, please use **no ip igmp snooping querier vlan** command.

Syntax

ip igmp snooping querier vlan *vlan-id*
no ip igmp snooping querier vlan *vlan-id*

Parameter

vlan-id— VLAN ID, ranging from 1 to 4094.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the IGMP Snooping Querier function of VLAN 1:

```
T2500G-10TS(config)#ip igmp snooping querier vlan 1
```

31.14 ip igmp snooping querier vlan (general query)

Description

The **ip igmp snooping querier vlan** command is used to configure the parameters for IGMP Snooping Querier to send a general query frame. To return to the default configuration, please use **no ip igmp snooping querier vlan** command.

Syntax

```
ip igmp snooping querier vlan vlan-id { query-interval interval | max-response-time response-time | general-query source-ip ip-addr }
```

```
no ip igmp snooping querier vlan vlan-id { query-interval | max-response-time | general-query source-ip }
```

Parameter

vlan-id—— VLAN ID, ranging from 1 to 4094.

interval —— The time interval to send a general query frame by IGMP Snooping Querier, ranging from 10 to 300 (Seconds). By default, it is 60 seconds.

response-time —— The maximal time for the host to respond to a general query frame, ranging from 1 to 25 (Seconds). By default, it is 10 Seconds.

ip-addr—— The source IP of the general query frame sent by IGMP Snooping Querier. It should not be a multicast IP or a broadcast IP. By default, it is 192.168.0.1.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

For VLAN 2, specify its query-interval as 200 seconds, and the response-time as 20 seconds:

```
T2500G-10TS(config)#ip igmp snooping querier vlan 2 query-interval 200
T2500G-10TS(config)#ip igmp snooping querier vlan 2
max-response-time 20
```

31.15 ip igmp snooping querier vlan (specific query)

Description

The **ip igmp snooping querier vlan** command is used to configure the parameters for IGMP Snooping Querier to send a specific query frame. To return to the default configuration, please use **no ip igmp snooping querier vlan** command.

Syntax

```
ip igmp snooping querier vlan vlan-list {last-member-query-interval interval / last-member-query-count count / special-query source-ip ip-addr}
```

```
no ip igmp snooping querier vlan vlan-list {last-member-query-interval / last-member-query-count / special-query source-ip}
```

Parameter

vlan-list— VLAN ID list, ranging from 1 to 4094, in the format of 1-3, 5. It is multi-optional.

interval— The time interval of sending specific query frames by IGMP Snooping Querier, ranging from 1 to 5 (Seconds). By default, it is 1. A specific query will be sent on condition that "immediate-leave" is not enabled and a leave frame is received.

count— The times of sending specific query frames by IGMP Snooping Querier, ranging from 1 to 5. By default, it is 2. The switch will still treat the port as group member until the specific frames number sent by the querier reaches "last-member-query-count" and no report frame is received from the port.

ip-addr— The source IP of the specific query frame sent by IGMP Snooping Querier. It should not be a multicast IP or a broadcast IP. By default, it is 192.168.0.1.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the interval of Specific Query Message to 3 seconds in VLAN 2:

```
T2500G-10TS(config)# ip igmp snooping querier vlan 2
last-member-query-interval 3
```

31.16 ip igmp snooping authentication

Description

The **ip igmp snooping authentication** command is used to authenticate the users who want to join the limited multicast source. To disable the multicast authentication, please use **no ip igmp snooping authentication** command.

Syntax

```
ip igmp snooping authentication
no ip igmp snooping authentication
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

User Guidelines

The IGMP Authentication feature will take effect only when AAA function is enabled and the RADIUS server is configured. For how to enable AAA function and configure RADIUS server, please refer to [aaa enable](#) and [radius-server host](#).

Example

Enable IGMP authentication on port 1/0/3:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/3
T2500G-10TS(config-if)# ip igmp snooping authentication
```

31.17 ip igmp snooping accounting

Description

The **ip igmp snooping accounting** command is used to enable IGMP accounting globally. To disable the IGMP accounting, please use **no ip igmp snooping accounting** command.

Syntax

```
ip igmp snooping accounting
no ip igmp snooping accounting
```

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable IGMP accounting globally:

```
T2500G-10TS(config)# ip igmp snooping accounting
```

31.18 clear ip igmp snooping statistics

Description

The **clear ip igmp snooping statistics** command is used to clear the statistics of the IGMP packets.

Syntax

```
clear ip igmp snooping statistics
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

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

Example

Clear the statistics of the IGMP packets:

```
T2500G-10TS(config)# clear ip igmp snooping statistics
```

31.19 show ip igmp snooping

Description

The **show ip igmp snooping** command is used to display the global configuration of IGMP snooping.

Syntax

```
show ip igmp snooping
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of IGMP:

```
T2500G-10TS# show ip igmp snooping
```

31.20 show ip igmp snooping interface

Description

The **show ip igmp snooping interface** command is used to display the port configuration of IGMP snooping.

Syntax

```
show ip igmp snooping interface [ gigabitEthernet [ port | port-list ] ]  
{ basic-config | filter | packet-stat }
```

Parameter

port | *port-list* — The Ethernet port number(s). If not specified, the configuration of all ports is displayed.

basic-config | *filter* | *packet-stat* — The related configuration information selected to display.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IGMP basic configuration configuration of all ports and port channels:

```
T2500G-10TS# show ip igmp snooping interface basic-config
```

Display the IGMP basic configuration of port 1/0/2:

```
T2500G-10TS# show ip igmp snooping interface gigabitEthernet 1/0/2
basic-config
```

Display the IGMP packet statistics of ports 1/0/1-4:

```
T2500G-10TS# show ip igmp snooping interface gigabitEthernet 1/0/1-4
packet-stat
```

31.21 show ip igmp snooping vlan

Description

The **show ip igmp snooping vlan** command is used to display the VLAN configuration of IGMP snooping.

Syntax

```
show ip igmp snooping vlan [ vlan-id]
```

Parameter

vlan-id—The VLAN ID selected to display.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IGMP snooping configuration information of VLAN 2:

```
T2500G-10TS# show ip igmp snooping vlan 2
```

31.22 show ip igmp snooping multi-vlan

Description

The **show ip igmp snooping multi-vlan** command is used to display the Multicast VLAN configuration.

Syntax

show ip igmp snooping multi-vlan

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the Multicast VLAN configuration:

```
T2500G-10TS# show ip igmp snooping multi-vlan
```

31.23 show ip igmp snooping groups

Description

The **show ip igmp snooping groups** command is used to display the information of all IGMP snooping groups. It can be extended to some other commands to display the dynamic and static multicast information of a selected VLAN.

Syntax

show ip igmp snooping groups [vlan { *vlan-id* } [*multicast_addr*]] [count | dynamic | dynamic count | static | static count]

Parameter

vlan-id — The VLAN ID selected to display the information of all multicast items.

multicast_addr — IP address of the multicast group.

count — The numbers of all multicast groups.

dynamic — Display dynamic multicast groups.

dynamic count — The numbers of all dynamic multicast groups.

static — Display static multicast groups.

static count — The numbers of all static multicast groups.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of all IGMP snooping groups:

```
T2500G-10TS#show ip igmp snooping groups
```

Display all the multicast entries in VLAN 5:

```
T2500G-10TS(config)#show ip igmp snooping groups vlan 5
```

Display the count of multicast entries in VLAN 5:

```
T2500G-10TS(config)#show ip igmp snooping groups vlan 5 count
```

Display the dynamic multicast groups of VLAN 5

```
T2500G-10TS(config)#show ip igmp snooping groups vlan 5 dynamic
```

Display the static multicast groups of VLAN 5

```
T2500G-10TS(config)#show ip igmp snooping groups vlan 5 static
```

Display the count of dynamic multicast entries of VLAN 5

```
T2500G-10TS(config)#show ip igmp snooping groups vlan 5 dynamic  
count
```

Display the count of static multicast entries of VLAN 5

```
T2500G-10TS(config)#show ip igmp snooping groups vlan 5 static count
```

31.24 show ip igmp snooping querier

Description

The **show ip igmp snooping querier** command is used to display the Querier configuration of VLAN.

Syntax

```
show ip igmp snooping querier [ vlan vlan-id]
```

Parameter

vlan-id—The VLAN ID selected to display, ranging from 1 to 4094.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display all Querier information:

```
T2500G-10TS(config)# show ip igmp snooping querier
```

Chapter 32 MLD Snooping Commands

MLD Snooping (Multicast Listener Discovery Snooping) is a multicast control mechanism running on Layer 2 switch. It can effectively prevent multicast groups being broadcasted in the IPv6 network.

32.1 ipv6 mld snooping

Description

The **ipv6 mld snooping** command is used to enable MLD Snooping function globally. If this function is disabled, all related MLD Snooping function would not work. To disable this function, please use **no ipv6 mld snooping** command.

Syntax

ipv6 mld snooping
no ipv6 mld snooping

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable MLD Snooping:

```
T2500G-10TS(config)# ipv6 mld snooping
```

32.2 ipv6 mld snooping router-aging-time

Description

The **ipv6 mld snooping router-aging-time** command is used to specify router port aging time globally. The default aging time is 260 seconds. To restore the default timer, please use **no ipv6 mld snooping router-aging-time** command.

Syntax

ipv6 mld snooping router-aging-time *timer*
no ipv6 mld snooping router-aging-time

Parameter

timer—— Specify the aging time in seconds, ranging from 1 to 1000.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify MLD Snooping router port aging time as 100 seconds globally:

```
T2500G-10TS(config)# ipv6 mld snooping router-aging-time 100
```

32.3 ipv6 mld snooping member-aging-time

Description

The **ipv6 mld snooping member-aging-time** command is used to specify member port aging time globally. The default aging time is 260 seconds. To restore the default timer, please use **no ipv6 mld snooping member-aging-time** command.

Syntax

```
ipv6 mld snooping member-aging-time timer  
no ipv6 mld snooping member-aging-time
```

Parameter

timer—— Specify the aging time in seconds, ranging from 200 to 1000.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify MLD Snooping member port aging time as 300 seconds globally:

```
T2500G-10TS(config)# ipv6 mld snooping member-aging-time 300
```

32.4 ipv6 mld snooping report-suppression

Description

The **ipv6 mld snooping report-suppression** command is used to enable the Report message suppression function. By default, it is enabled. To disable this function, please use **no ipv6 mld snooping report-suppression** command.

Syntax

ipv6 mld snooping report-suppression
no ipv6 mld snooping report-suppression

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Disable Report message suppression function:

```
T2500G-10TS(config)# no ipv6 mld snooping report-suppression
```

32.5 ipv6 mld snooping unknown-filter

Description

The **ipv6 mld snooping unknown-filter** command is used to enable the unknown multicast packets filter function. To disable this function, please use **no ipv6 mld snooping unknown-filter** command. By default, it is disabled.

Syntax

ipv6 mld snooping unknown-filter
no ipv6 mld snooping unknown-filter

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable unknown multicast filter function:

```
T2500G-10TS(config)# ipv6 mld snooping unknown-filter
```

32.6 ipv6 mld snooping last-listener query-inteval

Description

The **ipv6 mld snooping last-listener query-inteval** command is used to specify the interval to send Specific Query Message. The default value is 1 second. To restore the default interval, please use **no ipv6 mld snooping last-listener query-inteval** command.

Syntax

```
ipv6 mld snooping last-listener query-inteval interval  
no ipv6 mld snooping last-listener query-inteval
```

Parameter

interval—— Specify the interval to send Specific Query Message in seconds, ranging from 1 to 5.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the interval of Specific Query Message to 3 seconds:

```
T2500G-10TS(config)# ipv6 mld snooping last-listener query-inteval 3
```

32.7 ipv6 mld snooping last-listener query-count

Description

The **ipv6 mld snooping last-listener query-count** command is used to specify the numbers of Specific Query Message to be sent. The default value is 2. To restore the default number, please use **no ipv6 mld snooping last-listener query-count** command.

Syntax

```
ipv6 mld snooping last-listener query-count num
```

no ipv6 mld snooping last-listener query-count

Parameter

num—— Specify the numbers of Specific Query Message to be sent, ranging from 1 to 7.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the number of Specific Query Message to 3:

```
T2500G-10TS(config)# ipv6 mld snooping last-listener query-count 3
```

32.8 ipv6 mld snooping multicast-vlan

Description

The **ipv6 mld snooping multicast-vlan** command is used to enable the multicast VLAN function. To disable this function, please use **no ipv6 mld snooping multicast-vlan** command. By default it is disabled.

Syntax

```
ipv6 mld snooping multicast-vlan  
no ipv6 mld snooping multicast-vlan
```

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable multicast VLAN:

```
T2500G-10TS(config)# ipv6 mld snooping multicast-vlan
```

32.9 ipv6 mld snooping multicast-vlan vlan-id

Description

The **ipv6 mld snooping multicast-vlan vlan-id** command is used to specify the multicast VLAN ID. The default multicast VLAN is VLAN1. To restore the default VLAN, please use **no ipv6 mld snooping multicast-vlan vlan-id** command.

Syntax

```
ipv6 mld snooping multicast-vlan vlan-id vid  
no ipv6 mld snooping multicast-vlan vlan-id
```

Parameter

vid—— The specified IEEE 802.1Q VLAN ID, ranging from 1 to 4094.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify multicast VLAN as VLAN 2:

```
T2500G-10TS(config)# ipv6 mld snooping multicast-vlan vlan-id 2
```

32.10 ipv6 mld snooping vlan

Description

The **ipv6 mld snooping vlan** command is used to enable MLD Snooping function on a specified VLAN. To disable it, please use **no ipv6 mld snooping vlan** command.

Syntax

```
ipv6 mld snooping vlan vlan-id  
no ipv6 mld snooping vlan vlan-id
```

Parameter

vlan-id——The specified VLAN ID to enable MLD Snooping function, ranging from 1 to 4094.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable MLD Snooping function on VLAN 2:

```
T2500G-10TS(config)# ipv6 mld snooping vlan 2
```

32.11 ipv6 mld snooping vlan router-aging-time

Description

The **ipv6 mld snooping vlan router-aging-time** command is used to specify router port aging time for a specified VLAN. If this time is set to 0, then the global router port aging time will be used. The default time is 0. To restore the default timer, please use **no ipv6 mld snooping vlan router-aging-time** command.

Syntax

```
ipv6 mld snooping vlan vlan-id router-aging-time timer  
no ipv6 mld snooping vlan vlan-id router-aging-time
```

Parameter

vlan-id—— The specified IEEE 802.1Q VLAN ID, ranging from 1 to 4094.
timer—— Aging time of the router port in seconds, ranging from 0 to 1000.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the router port aging time as 100 seconds in VLAN 2:

```
T2500G-10TS(config)# ipv6 mld snooping vlan 2 router-aging-time 100
```

32.12 ipv6 mld snooping vlan member-aging-time

Description

The **ipv6 mld snooping vlan member-aging-time** command is used to specify member port aging time for a specified VLAN. If this time is set to 0, then the global member port aging time will be used. The default time is 0. To restore the default timer, please use **no ipv6 mld snooping vlan member-aging-time** command.

Syntax

```
ipv6 mld snooping vlan vlan-id member-aging-time timer  
no ipv6 mld snooping vlan vlan-id member-aging-time
```

Parameter

vlan-id—The specified IEEE 802.1Q VLAN ID, ranging from 1 to 4094.

timer — Aging time of the member port in seconds, ranging from 200 to 1000 and 0.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the member port aging time as 300 seconds in VLAN 2:

```
T2500G-10TS(config)# ipv6 mld snooping vlan 2 member-aging-time 300
```

32.13 ipv6 mld snooping vlan immediate-leave

Description

The **ipv6 mld snooping vlan immediate-leave** command is used to enable the immediate leave function on a specified VLAN. To disable this function, please use **no ipv6 mld snooping vlan immediate-leave** command. By default, it is disabled.

Syntax

```
ipv6 mld snooping vlan vlan-id immediate-leave  
no ipv6 mld snooping vlan vlan-id immediate-leave
```

Parameter

vlan-id — The specified IEEE 802.1Q VLAN ID to enable the immediate leave function, ranging from 1 to 4094.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable immediate leave function on VLAN 2:

```
T2500G-10TS(config)# ipv6 mld snooping vlan 2 immediate-leave
```

32.14 ipv6 mld snooping vlan mrouter

Description

The **ipv6 mld snooping vlan mrouter** command is used to configure the static router port in a specified VLAN. To disable the static router port, please use **no mld snooping vlan mrouter** command.

Syntax

```
ipv6 mld snooping vlan vlan-id mrouter interface gigabitEthernet port  
no ipv6 mld snooping vlan vlan-id mrouter [interface gigabitEthernet port]
```

Parameter

vlan-id — The specified IEEE 802.1Q VLAN ID, ranging from 1 to 4094.

port — Interface number of the router port(s).

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the gigabitEthernet 1/0/2 as static router port in VLAN 2:

```
T2500G-10TS(config)# ipv6 mld snooping vlan 2 mrouter interface  
gigabitEthernet 1/0/2
```

32.15 ipv6 mld snooping vlan static

Description

The **ipv6 mld snooping vlan static** command is used to configure the static multicast groups. To disable the static multicast group, please use **no ipv6 mld snooping vlan static** command.

Syntax

```
ipv6 mld snooping vlan vlan-id static ipv6_multicast_addr interface  
gigabitEthernet port  
no ipv6 mld snooping vlan vlan-id static ipv6_multicast_addr [interface  
gigabitEthernet port]
```

Parameter

vlan-id—— The multicast group VLAN ID, ranging from 1 to 4094.

ipv6_multicast_addr—— IPv6 address of the static multicast group.

port —— Interface number of the member port(s).

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the static multicast group ff80::1234 in VLAN 2 with the member port gigabitEthernet 1/0/2:

```
T2500G-10TS(config)# ipv6 mld snooping vlan 2 static ff80::1234 interface  
gigabitEthernet 1/0/2
```

32.16 ipv6 mld snooping querier vlan

Description

The **ipv6 mld snooping querier vlan** command is used to enable the MLD Querier function. To disable this function, please use **no ipv6 mld snooping querier vlan** command.

Syntax

```
ipv6 mld snooping querier vlan vlan-id  
no ipv6 mld snooping querier vlan vlan-id
```

Parameter

vlan-id—— The VLAN that enables the MLD querier function, ranging from 1 to 4094.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable MLD Querier function on VLAN 2:

```
T2500G-10TS(config)# ipv6 mld snooping querier vlan 2
```

32.17 ipv6 mld snooping querier vlan max-response-time

Description

The **ipv6 mld snooping querier vlan max-response-time** command is used to specify the max response time of the Query message. The default value is 10 seconds. To restore the default value, please use **no ipv6 mld snooping querier vlan max-response-time** command.

Syntax

```
ipv6 mld snooping querier vlan vlan-id max-response-time time  
no ipv6 mld snooping querier vlan vlan-id max-response-time
```

Parameter

vlan-id—— The VLAN that enables the MLD Querier function, ranging from 1 to 4094.

time—— Specify the time in seconds, ranging from 1 to 25.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the max response time as 10s on VLAN 2:

```
T2500G-10TS(config)# ipv6 mld snooping querier vlan 2
max-response-time 10
```

32.18 ipv6 mld snooping querier vlan query-interval

Description

The **ipv6 mld snooping querier vlan query-interval** command is used to specify the interval to send the Query Message. The default value is 25 seconds. To restore the default value, please use **no ipv6 mld snooping querier vlan query-interval** command.

Syntax

```
ipv6 mld snooping querier vlan vlan-id query-interval interval
no ipv6 mld snooping querier vlan vlan-id query-interval
```

Parameter

vlan-id — The VLAN that enables the MLD Querier function, ranging from 1 to 4094.

interval — Specify the interval to send the Query message in seconds, ranging from 2 to 300.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the interval to send the Query Message as 10s on VLAN 2:

```
T2500G-10TS(config)# ipv6 mld snooping querier vlan 2 query-interval 10
```

32.19 ipv6 mld snooping querier vlan query-source

Description

The **ipv6 mld snooping querier vlan query-source** command is used to specify the source address which sends the Query message. The default value is FE80::02FF:FFFF:FE00:0001. To restore the default value, please use **no ipv6 mld snooping querier vlan query-source** command.

Syntax

```
ipv6 mld snooping querier vlan vlan-id query-source ipv6-addr
```

no ipv6 mld snooping querier vlan *vlan-id* query-source

Parameter

vlan-id—— IEEE 802.1Q VLAN ID, ranging from 1 to 4094.

ipv6-addr—— Specify the IPv6 source address.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the source address which sends the Query message as fe80::1234 on VLAN 2:

```
T2500G-10TS(config)# ipv6 mld snooping querier vlan 2 query-source  
fe80::1234
```

32.20 ipv6 mld snooping filter(global)

Description

The **ipv6 mld snooping filter** command is used to configure the multicast group filter entries in the format of ip-range. To disable the filter entry, please use **no ipv6 mld snooping filter** command.

Syntax

ipv6 mld snooping filter *filter-id start-ipv6 end-ipv6*

no ipv6 mld snooping filter *filter-id*

Parameter

filter-id—— Specify the filter ID, ranging from 1 to 30.

start-ipv6—— Start IPv6 multicast address of the filter entry.

end-ipv6—— End IPv6 multicast address of the filter entry.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create filter entry with filter ID as 2, start IP as ff80::1234 and end IP as ff80::1235:

```
T2500G-10TS(config)# ipv6 mld snooping filter 2 ff80::1234 ff80::1235
```

32.21 ipv6 mld snooping filter(interface)

Description

The **ipv6 mld snooping filter** command is used to enable the filter function on the interface. To disable the filter function, please use **no ipv6 mld snooping filter** command.

Syntax

```
ipv6 mld snooping filter  
no ipv6 mld snooping filter
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable filter function on interface gigabitEthernet 1/0/2:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/2  
T2500G-10TS(config-if)# ipv6 mld snooping filter
```

32.22 ipv6 mld snooping filter-mode

Description

The **ipv6 mld snooping filter-mode** command is used to configure the filter mode of the interface. The default mode is accept. To restore the default mode, please use **no ipv6 mld snooping filter-mode** command.

Syntax

```
ipv6 mld snooping filter-mode {accept | refuse}  
no ipv6 mld snooping filter-mode
```


Parameter

accept — Accept the multicast groups within the filter entry.

refuse — Refuse the multicast groups within the filter entry.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure the filter mode as refuse on interface gigabitEthernet 1/0/2:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/2
T2500G-10TS(config-if)# ipv6 mld snooping filter-mode refuse
```

32.23 ipv6 mld snooping filter-id

Description

The **ipv6 mld snooping filter-id** command is used to specify the filter id on the interface. To disable this configuration, please use **no ipv6 mld snooping filter-id** command.

Syntax

```
ipv6 mld snooping filter-id filter-list
no ipv6 mld snooping filter-id
```

Parameter

filter-list — Specify the filter id list, in format of 1,3,10.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Specify the filter id as 1 and 10 on interface gigabitEthernet 1/0/2:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/2
T2500G-10TS(config-if)# ipv6 mld snooping filter-id 1,10
```

32.24 ipv6 mld snooping max-group

Description

The **ipv6 mld snooping max-group** command is used to specify the limit number of groups for a port to join in. The default value is 256. To restore the default value, please use **no ipv6 mld snooping max-group** command.

Syntax

```
ipv6 mld snooping max-group limit
no ipv6 mld snooping max-group
```

Parameter

limit—— Specify the max number of multicast groups on a port, ranging from 0 to 256.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Specify the limit group as 128 on interface gigabitEthernet 1/0/2:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/2
T2500G-10TS(config-if)# ipv6 mld snooping max-group 128
```

32.25 clear ipv6 mld snooping statistics

Description

The **clear ipv6 mld snooping statistics** command is used to clear the statistics of the MLD packets.

Syntax

```
clear ipv6 mld snooping statistics
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

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

Example

Clear the statistics of the MLD packets:

```
T2500G-10TS(config)# clear ipv6 mld snooping statistics
```

32.26 show ipv6 mld snooping

Description

The **show ipv6 mld snooping** command is used to display the global configuration of MLD Snooping.

Syntax

```
show ipv6 mld snooping
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of MLD Snooping:

```
T2500G-10TS(config)# show ipv6 mld snooping
```

32.27 show ipv6 mld snooping vlan

Description

The **show ipv6 mld snooping vlan** command is used to display VLAN information of MLD Snooping.

Syntax

```
show ipv6 mld snooping vlan [vlan-id]
```

Parameter

vlan-id— The VLAN ID selected to display, ranging from 1 to 4094.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display all of the VLAN information:

```
T2500G-10TS(config)# show ipv6 mld snooping vlan
```

32.28 show ipv6 mld snooping static-mcast

Description

The **show ipv6 mld snooping static-mcast** command is used to display the static multicast groups configured by users.

Syntax

```
show ipv6 mld snooping static-mcast
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display static multicast groups:

```
T2500G-10TS(config)# show ipv6 mld snooping static-mcast
```

32.29 show ipv6 mld snooping group

Description

The **show ipv6 mld snooping group** command is used to display multicast groups.

Syntax

```
show ipv6 mld snooping group [ dynamic | static ][ vlan vlan-id]
```

Parameter

dynamic — Display dynamic groups.

`static` — Display static groups.

`vlan-id` — The VLAN ID selected to display, ranging from 1 to 4094.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display all of the multicast groups:

```
T2500G-10TS(config)# show ipv6 mld snooping group
```

32.30 show ipv6 mld snooping filter

Description

The **show ipv6 mld snooping filter** command is used to display the filter entries.

Syntax

```
show ipv6 mld snooping filter
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the filter entries:

```
T2500G-10TS(config)# show ipv6 mld snooping filter
```

32.31 show ipv6 mld snooping interface

Description

The **show ipv6 mld snooping interface** command is used to display the interface information of MLD Snooping.

Syntax

```
show ipv6 mld snooping interface [ gigabitEthernet port]
```

Parameter

port—— Specify the port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display all of the interface information:

```
T2500G-10TS(config)# show ipv6 mld snooping interface
```

32.32 show ipv6 mld snooping interface filter

Description

The **show ipv6 mld snooping interface filter** command is used to display the filter ids bounded to the interface.

Syntax

```
show ipv6 mld snooping interface filter [gigabitEthernet port]
```

Parameter

port—— Specify the port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display all filter ids bounded to all interface:

```
T2500G-10TS(config)# show ipv6 mld snooping interface filter
```

32.33 show ipv6 mld snooping querier

Description

The **show ipv6 mld snooping querier** command is used to display the Querier configuration of VLAN.

Syntax

```
show ipv6 mld snooping querier [vlan vlan-id]
```

Parameter

vlan-id—The VLAN ID selected to display, ranging from 1 to 4094.

Privilege Requirement

None.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display all Querier information:

```
T2500G-10TS(config)# show ipv6 mld snooping querier
```

32.34 show ipv6 mld snooping statistics

Description

The **show ipv6 mld snooping statistics** command is used to display the statistics of the MLD packets.

Syntax

```
show ipv6 mld snooping statistics [interface gigabitEthernet port]
```

Parameter

port—Specify the port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display statistics of MLD packets:

```
T2500G-10TS(config)# show ipv6 mld snooping statistics
```

Chapter 33 SNMP Commands

SNMP (Simple Network Management Protocol) functions are used to manage the network devices for a smooth communication, which can facilitate the network administrators to monitor the network nodes and implement the proper operation.

33.1 snmp-server

Description

The **snmp-server** command is used to enable the SNMP function. By default, it is disabled. To return to the default configuration, please use **no snmp-server** command.

Syntax

```
snmp-server  
no snmp-server
```

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the SNMP function:

```
T2500G-10TS(config)# snmp-server
```

33.2 snmp-server view

Description

The **snmp-server view** command is used to add View. To delete the corresponding View, please use **no snmp-server view** command. The OID (Object Identifier) of the SNMP packets is used to describe the managed objects of the switch, and the MIB (Management Information Base) is the set of the OIDs. The SNMP View is created for the SNMP management station to manage MIB objects.

Syntax

```
snmp-server view name mib-oid { include | exclude }  
no snmp-server view name mib-oid
```


Parameter

name — The entry name of View, ranging from 1 to 16 characters. Each View includes several entries with the same name.

mib-oid — MIB Object ID. It is the Object Identifier (OID) for the entry of View, ranging from 1 to 61 characters.

include | exclude — View Type, with include and exclude options. They represent the view entry can/cannot be managed by the SNMP management station individually.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Add a View named view1, configuring the OID as 1.3.6.1.6.3.20, and this OID can be managed by the SNMP management station:

```
T2500G-10TS(config)# snmp-server view view1 1.3.6.1.6.3.20 include
```

33.3 snmp-server group

Description

The **snmp-server group** command is used to manage and configure the SNMP group. To delete the corresponding SNMP group, please use **no snmp-server group** command. SNMP v3 provides the VACM (View-based Access Control Model) and USM (User-Based Security Model) mechanisms for authentication. The users in the SNMP Group can manage the device via the Read View, Write View and Notify View. And the authentication mode and the privacy mode guarantee the high security for the communication between the management station and the managed device.

Syntax

```
snmp-server group name [ smode { v1 | v2c | v3 } ] [ slev { noAuthNoPriv | authNoPriv | authPriv } ] [ read read-view ] [ write write-view ] [ notify notify-view ]
```

```
no snmp-server group name smode { v1 | v2c | v3 } slev { noAuthNoPriv | authNoPriv | authPriv }
```

Parameter

name — The SNMP Group name, ranging from 1 to 16 characters. The Group Name, Security Model and Security Level compose the identifier of the SNMP Group. These three items of the Users in one group should be the same.

smode — Security Model, with v1、v2c and v3 options. They represent SNMP v1, SNMP v2c and SNMP v3.

slev — The Security Level of SNMP v3 Group. There are three options, including noAuthNoPriv (no authorization and no encryption)、authNoPriv (authorization and no encryption) and authPriv (authorization and encryption) . By default, the Security Level is noAuthNoPriv. There is no need to configure this in SNMP v1 Mode and SNMP v2c Mode.

read-view — Select the View to be the Read View. The management access is restricted to read-only, and changes cannot be made to the assigned SNMP View.

write-view — Select the View to be the Write View. The management access is writing only and changes can be made to the assigned SNMP View. The View defined both as the Read View and the Write View can be read and modified.

notify-view — Select the View to be the Notify View. The management station can receive notification messages of the assigned SNMP view generated by the switch's SNMP agent.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Add a group, and configure the name as group 1, the Security Model as SNMP v3, the security level as authNoPriv, the management access to the assigned View viewDefault as read-write, besides the notification messages sent by View viewDefault can be received by Management station:

```
T2500G-10TS(config)# snmp-server group group1 smode v3 slev  
authNoPriv read viewDefault write viewDefault notify viewDefault
```

Delete group 1:

```
T2500G-10TS(config)# no snmp-server group group1 smode v3 slev  
authNoPriv
```

33.4 snmp-server user

Description

The **snmp-server user** command is used to add User. To delete the corresponding User, please use **no snmp-server user** command. The User in an SNMP Group can manage the switch via the management station software. The User and its Group have the same security level and access right.

Syntax

```
snmp-server user name { local | remote } group-name [ smode { v1 | v2c | v3 } ]  
[ slev { noAuthNoPriv | authNoPriv | authPriv } ] [ cmode { none | MD5 | SHA } ]  
[ cpwd confirm-pwd ] [ emode { none | DES } ] [ epwd encrypt-pwd ]  
no snmp-server user name
```

Parameter

name — User Name, ranging from 1 to 16 characters.

local | remote — User Type, with local and remote options. Local indicates that the user is connected to a local SNMP engine, while remote means that the user is connected to a remote SNMP engine.

group-name — The Group Name of the User. The User is classified to the corresponding Group according to its Group Name, Security Model and Security Level.

smode — The Security Model of the User, with v1, v2c and v3 options. By default, the option is v1. The Security Model of the User must be the same with that of the Group which the User belongs to.

slev — The Security Level of SNMP v3 Group. There are three options, including noAuthNoPriv (no authorization and no encryption), authNoPriv (authorization and no encryption) and authPriv (authorization and encryption). By default, the option is "noAuthNoPriv". The Security Level of the User must be the same with that of the Group which the User belongs to.

cmode — The Authentication Mode of the SNMP v3 User, with none, MD5 and SHA options. None indicates no authentication method is used, MD5 indicates the port authentication is performed via HMAC-MD5 algorithm and SHA indicates the port authentication is performed via SHA (Secure Hash Algorithm). SHA authentication mode has a higher security than MD5 mode. By default, the Authentication Mode is "none".

confirm-pwd — Authentication Password, ranging from 1 to 16 characters. The question marks and spaces are not allowed. This password in the configuration file will be displayed in the symmetric encrypted form.

emode — The Privacy Mode of the SNMP v3 User, with none and DES options. None indicates no privacy method is used, and DES indicates DES encryption method is used. By default, the Privacy Mode is “none”.

encrypt-pwd — Privacy Password, ranging from 1 to 16 characters. The question marks and spaces are not allowed. This password in the configuration file will be displayed in the symmetric encrypted form.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Add Local User admin to Group group2, and configure the Security Model of the user as v3, the Security Level of the group as authPriv, the Authentication Mode of the user as MD5, the Authentication Password as 11111, the Privacy Mode as DES, and the Privacy Password as 22222:

```
T2500G-10TS(config)# snmp-server user admin local group2 smode v3
slev authPriv cmode MD5 cpwd 11111 emode DES epwd 22222
```

33.5 snmp-server community

Description

The **snmp-server community** command is used to add Community. To delete the corresponding Community, please use **no snmp-server community** command. SNMP v1 and SNMP v2c adopt community name authentication. The community name can limit access to the SNMP agent from SNMP network management station, functioning as a password.

Syntax

```
snmp-server community name { read-only | read-write } mib-view
```

```
no snmp-server community name
```

Parameter

name — Community Name, ranging from 1 to 16 characters.

read-only | read-write — The access rights of the community, with read-only and read-write options.

mib-view — The MIB View for the community to access.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Add community public, and the community has read-write management right to View viewDefault:

```
T2500G-10TS(config)# snmp-server community public read-write
viewDefault
```

33.6 snmp-server host

Description

The **snmp-server host** command is used to add Notification. To delete the corresponding Notification, please use **no snmp-server host** command.

Syntax

```
snmp-server host ip udp-port user-name [ smode { v1 | v2c | v3 } ] [ slev { noAuthNoPriv | authNoPriv | authPriv } ] [ type { trap | inform } ] [ retries retries ] [ timeout timeout ]
```

```
no snmp-server host ip user-name
```

Parameter

ip — The IP Address of the management Host. Both IPv4 and IPv6 addresses are supported, for example 192.168.0.100 or fe80::1234.

udp-port — UDP port, which is used to send notifications. The UDP port functions with the IP address for the notification sending. It ranges from 1 to 65535.

user-name — The User name of the management station.

smode — The Security Model of the management station, with v1, v2c and v3 options. By default, the option is v1.

slev — The Security Level of SNMP v3 Group. There are three options, including noAuthNoPriv (no authorization and no encryption), authNoPriv (authorization and no encryption) and authPriv (authorization and encryption). By default, the option is "noAuthNoPriv".

type — The type of the notifications, with trap and inform options. Trap indicates traps are sent, while inform indicates informs are sent. The inform

type has a higher security than the trap type and resend and timeout need to be configured if you select this option. You can only select the trap type in Security Model v1. By default, the type of the notifications is "trap".

retries—— The amount of times the switch retries an inform request, ranging from 1 to 255. The switch will resend the inform request if it doesn't get the response from the management station during the Timeout interval, and it will terminate resending the inform request if the resending times reach the specified Retry times.

timeout—— The maximum time for the switch to wait for the response from the management station before resending a request, ranging from 1 to 3600 in seconds.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Add a Notification entry, and configure the IP address of the management Host as 192.168.0.146, the UDP port as 162, the User name of the management station as admin, the Security Model of the management station as v2c, the type of the notifications as inform, the maximum time for the switch to wait as 1000 seconds, and the retries time as 100:

```
T2500G-10TS(config)# snmp-server host 192.168.0.146 162 admin smode v2c type inform retries 100 timeout 1000
```

Add a Notification entry, and configure the IP Address of the management Host as fe80::1234, the UDP port as 162, the User name of the management station as admin, the Security Model of the management station as v2c, the type of the notifications as inform, the maximum time for the switch to wait as 1000 seconds, and the retries time as 100:

```
T2500G-10TS(config)# snmp-server host fe80::1234 162 admin smode v2c type inform retries 100 timeout 1000
```

33.7 snmp-server engineID

Description

The **snmp-server engineID** command is used to configure the local and remote engineID of the switch. To restore to the default setting, please use **no snmp-server engineID** command.

Syntax

```
snmp-server engineID { [local local-engineID] [remote remote-engineID] }  
no snmp-server engineID
```

Parameter

local-engineID— Local Engine ID for local clients. The Engine ID is a unique alphanumeric string used to identify the SNMP engine on the switch. Its length ranges from 10 to 64 hexadecimal characters, which must be even number meanwhile.

remote-engineID — Remote Engine ID for the switch. The Engine ID is a unique alphanumeric string used to identify the SNMP engine on the remote device which receives informs from the switch. Its length ranges from 10 to 64 hexadecimal characters, which must be even number meanwhile. The **snmp-server engineID** will be disabled if the **local** and **remote** are both not configured.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Specify the local engineID as 1234567890, and the remote engineID as abcdef123456:

```
T2500G-10TS(config)# snmp-server engineID local 1234567890 remote  
abcdef123456
```

33.8 snmp-server traps snmp

Description

The **snmp-server traps snmp** command is used to enable SNMP standard traps which include four types: linkup, linkdown, warmstart and coldstart. To

disable the sending of SNMP standard traps, please use **no snmp-server traps snmp** command.

Syntax

snmp-server traps snmp [linkup | linkdown | warmstart | coldstart | auth-failure]

no snmp-server traps snmp [linkup | linkdown | warmstart | coldstart | auth-failure]

Parameter

linkup — Enable linkup trap. It is sent when port status changes from linkdown to linkup. By default, it is enabled.

linkdown — Enable linkdown trap. It is sent when port status changes from linkup to linkdown. By default, it is enabled.

warmstart — Enable warmstart trap. It is sent upon SNMP function reboot. By default, it is enabled.

coldstart — Enable coldstart trap. It is sent upon switch reboot. By default, it is enabled.

auth-failure — Enable the auth-failure trap. It is sent when a received SNMP request fails the authentication. By default, it is enabled.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable SNMP standard linkup trap for the switch:

```
T2500G-10TS(config)# snmp-server traps snmp linkup
```

33.9 snmp-server traps link-status

Description

The **snmp-server traps link-status** command is used to enable SNMP link status trap for the specified port. To disable the sending of SNMP link status trap, please use **no snmp-server traps link-status** command.

Syntax

snmp-server traps link-status

no snmp-server traps link-status

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable SNMP link status trap for port 3:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/3
T2500G-10TS(config-if)# snmp-server traps link-status
```

33.10 snmp-server traps

Description

The **snmp-server traps** command is used to enable SNMP extended traps. To disable the sending of SNMP extended traps, please use **no snmp-server traps** command.

Syntax

snmp-server traps { bandwidth-control | cpu | flash | ipaddr-change | loopback-detection | storm-control | spanning-tree | memory }

no snmp-server traps { bandwidth-control | cpu | flash | loopback-detection | storm-control | spanning-tree | memory }

Parameter

bandwidth-control — Enable bandwidth-control trap. It is sent when the rate limit function is enabled and the bandwidth exceeds the predefined value.

cpu — Allow CPU-related trap. It is sent when CPU usage exceeds the predefined threshold. By default, the CPU usage threshold of the switch is 80%.

flash — Enable flash trap. It is sent when flash is modified during operations such as backup, reset, firmware upgrade, configuration import, etc.

ipaddr-change — Enable ipaddr-change trap. It is sent when IP address is changed such as user manually modifies the IP address or the switch obtains a new IP address from DHCP.

loopback-detection — Enable loopback-detection trap. It is sent when the switch detects loopback or loopback is cleared.

storm-control — Enable storm-control trap. It is sent when the multicast or broadcast rate exceeds the predefined value.

spanning-tree — Enable spanning-tree trap. It is sent when the port forwarding status changes or the port receives TCN packet or packet with TC fport-channel-.

memory — Enable memory trap. It is sent when memory usage exceeds 80%.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable SNMP extended bandwidth-control trap for the switch:

```
T2500G-10TS(config)# snmp-server traps bandwidth-control
```

33.11 snmp-server traps mac

Description

The **snmp-server traps mac** command is used to enable SNMP extended MAC address-related traps which include four types: new, full, learn-mode-change and max-learned. To disable the sending of SNMP extended MAC address related traps, please use **no snmp-server traps mac** command.

Syntax

```
snmp-server traps mac [ new | full | learn-mode-change | max-learned ]
```

```
no snmp-server traps mac [ new | full | learn-mode-change | max-learned ]
```

Parameter

new — Enable new MAC address trap. It is sent when the switch learns new MAC address including dynamic address, static address and filter address.

full — Enable MAC address table trap. It is sent when the MAC address table is full.

learn-mode-change — Enable MAC address learn-mode-change trap. It is sent when MAC address learning mode of the switch changes.

max-learned — Enable MAC address max-learned trap. It is sent when the amount of learned MAC address reaches the limit which is configured in port security module.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable all SNMP extended MAC address-related traps for the switch:

```
T2500G-10TS(config)# snmp-server traps mac
```

Enable new MAC address trap only for the switch:

```
T2500G-10TS(config)# snmp-server traps mac new
```

33.12 snmp-server traps vlan

Description

The **snmp-server traps vlan** command is used to enable SNMP extended VLAN-related traps which include two types: create and delete. To disable this function, please use **no snmp-server traps vlan** command.

Syntax

```
snmp-server traps vlan [ create | delete ]
```

```
no snmp-server traps vlan [create | delete ]
```

Parameter

create — Enable VLAN-created trap. It is sent when new VLAN is created successfully.

delete — Enable VLAN-deleted traps. It is sent when VLAN is deleted successfully.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable all SNMP extended VLAN-related traps for the switch:

```
T2500G-10TS(config)# snmp-server traps vlan
```

Enable VLAN-created trap only for the switch:

```
T2500G-10TS(config)# snmp-server traps vlan create
```

33.13 rmon history

Description

The **rmon history** command is used to configure the history sample entry. To return to the default configuration, please use **no rmon history** command. RMON (Remote Monitoring), basing on SNMP architecture, functions to monitor the network. History Group is one of the commonly used RMON Groups. After a history group is configured, the switch collects network statistics information periodically, based on which the management station can monitor network effectively.

Syntax

```
rmon history index interface gigabitEthernet port [ interval seconds ]  
[ owner owner-name ] [ buckets number ]  
no rmon history index
```

Parameter

index — The index number of the entry, ranging from 1 to 12, in the format of 1-3,5.

port — The Ethernet port number.

seconds — The interval to take samplings from the port, ranging from 10 to 3600 in seconds. By default, it is 1800.

owner-name — The owner of the history sample entry, ranging from 1 to 16 characters. By default, it is "monitor".

number — The maximum number of buckets desired for the RMON history group of statistics, ranging from 1 to 130. The default is 50 buckets.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the sample port as Gi1/0/2 and the sample interval as 100 seconds for the entry 1-3:

```
T2500G-10TS(config)# rmon history 1-3 interface gigabitEthernet 1/0/2
interval 100 owner owner1
```

33.14 rmon event

Description

The **rmon event** command is used to configure the entries of SNMP-RMON Event. To return to the default configuration, please use **no rmon event** command. Event Group, as one of the commonly used RMON Groups, is used to define RMON events. Alarms occur when an event is detected.

Syntax

```
rmon event index [user user-name] [description descript] [type { none |
log | notify | log-notify }] [owner owner-name]
```

```
no rmon event index
```

Parameter

index — The index number of the event entry, ranging from 1 to 12. You can only select one entry for each command.

user-name — The name of the User to which the event belongs, ranging from 1 to 16 characters. By default, it is "public".

descript — The description of the event, ranging from 1 to 16 characters. By default, it is empty.

type — The event type, with none, log, notify and both options. None indicates no processing, log indicates logging the event, notify indicates sending trap messages to the management station, and both indicates logging the event and sending trap messages to the management station.

owner-name — The owner of the event entry, ranging from 1 to 16 characters. By default, it is "monitor".

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the user name of entry 1, 2, 3 and 4 as user1, the description of the event as description1, the type of event as log and the owner of the event as owner1:

```
T2500G-10TS(config)# rmon event 1-4 user user1 description description1
type log owner owner1
```

33.15 rmon alarm

Description

The **rmon alarm** command is used to configure SNMP-RMON Alarm Management. To return to the default configuration, please use **no rmon alarm** command. Alarm Group is one of the commonly used RMON Groups. RMON alarm management allows monitoring the specific alarm variables. When the value of a monitored variable exceeds the threshold, an alarm event is generated, which triggers the switch to act in the set way.

Syntax

```
rmon alarm index { stats-index sindex } [ alarm-variable { revbyte | revpkt |
bpkt | mpkt | crc-lign | undersize | oversize | jabber | collision | 64 | 65-127 |
128-511 | 512-1023 | 1024-10240 } ] [ s-type { absolute | delta } ]
[ rising-threshold r-hold ] [ rising-event-index r-event ] [ falling-threshold
f-hold ] [ falling-event-index f-event ] [ a-type {rise | fall | all} ] [ owner
owner-name ] [ interval interval ]
```

```
no rmon alarm index
```

Parameter

index — The index number of the Alarm Management entry, ranging from 1 to 12, in the format of 1-3,5.

sindex — Specify the statistics index.

alarm-variable — The alarm variable. By default, the option is revbyte.

s-type — Sample Type, which is the sampling method for the selected variable and comparing the value against the thresholds. There are two options, absolute and delta. Absolute indicates comparing the values directly with the thresholds at the end of the sampling interval. Delta indicates subtracting the last sampled value from the current value, and then comparing the difference in the values with the threshold. By default, the Sample Type is absolute.

r-hold — The rising counter value that triggers the Rising Threshold alarm, ranging from 1 to 2147483647. By default, it is 100.

r-event — Rise Event, which is the index of the corresponding event which will be triggered if the sampled value is larger than the Rising Threshold. It ranges from 1 to 12.

f-hold — The falling counter value that triggers the Falling Threshold alarm, ranging from 1 to 2147483647. By default, it is 100.

f-event — Fall Event, which is the index of the corresponding event which will be triggered if the sampled value is lower than the Falling Threshold. It ranges from 1 to 12.

a-type — Alarm Type, with rise, fall and all options. Rise indicates that the alarm event will be triggered when the sampled value exceeds the Rising Threshold, fall indicates that the alarm event will be triggered when the sampled value is under the Falling Threshold, and all indicates that the alarm event will be triggered either the sampled value exceeds the Rising Threshold or is under the Falling Threshold. By default, the Alarm Type is all.

owner-name — The owner of the entry, ranging from 1 to 16 characters. By default, it is monitor.

interval — The alarm interval time, ranging from 10 to 3600 in seconds. By default, it is 1800.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure rmon alarm entries 1-3 binding with statistics entry 2, the owners as owner1 and the alarm intervals as 100 seconds:

```
T2500G-10TS(config)#rmon alarm 1-3 stats-index 2 owner owner1 interval
100
```

33.16 rmon statistics

Description

The **rmon statistics** command is used to configure the entries of SNMP-RMON statistics. To delete the corresponding entry, please use **no rmon statistics** command. The maximum supported entries are 1000.

Syntax

```
rmon statistics index interface gigabitEthernet port [ owner owner-name ]  
[ status { underCreation | valid } ]
```

```
no rmon statistics index
```

Parameter

index — The index number of the statistics entry, ranging from 1 to 65535, in the format of 1-3,5.

port — The statistics port number, in the format of 1/0/1.

owner-name — The creator of the event entry, ranging from 1 to 16 characters. By default, it is "monitor".

status — The status of the statistics entry, either "underCreation" or "valid". "underCreation" means this entry won't take effect until it is modified to "valid"; "valid" means this entry takes effect immediately after it is created.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the statistics entries 1-3 with the statistics port as 1/0/1, owner as owner1 and status as valid:

```
T2500G-10TS(config)#rmon statistics 1-3 interface gigabitEthernet 1/0/1  
owner owner1 status valid
```

33.17 show snmp-server

Description

The **show snmp-server** command is used to display SNMP configuration globally.

Syntax

```
show snmp-server
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display SNMP configuration globally:

```
T2500G-10TS# show snmp-server
```

33.18 show snmp-server view

Description

The **show snmp-server view** command is used to display the View table.

Syntax

```
show snmp-server view
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the View table:

```
T2500G-10TS# show snmp-server view
```

33.19 show snmp-server group

Description

The **show snmp-server group** command is used to display the Group table.

Syntax

```
show snmp-server group
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the Group table:

```
T2500G-10TS# show snmp-server group
```

33.20 show snmp-server user

Description

The **show snmp-server user** command is used to display the User table.

Syntax

```
show snmp-server user
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the User table:

```
T2500G-10TS# show snmp-server user
```

33.21 show snmp-server community

Description

The **show snmp-server community** command is used to display the Community table.

Syntax

```
show snmp-server community
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the Community table:

```
T2500G-10TS# show snmp-server community
```

33.22 show snmp-server host

Description

The **show snmp-server host** command is used to display the Host table.

Syntax

```
show snmp-server host
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the Host table:

```
T2500G-10TS# show snmp-server host
```

33.23 show snmp-server engineID

Description

The **show snmp-server engineID** command is used to display the engineID of the SNMP.

Syntax

```
show snmp-server engineID
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the engineID:

```
T2500G-10TS# show snmp-server engineID
```

33.24 show rmon history

Description

The **show rmon history** command is used to display the configuration of the history sample entry.

Syntax

```
show rmon history [ index ]
```

Parameter

index — The index number of the entry selected to display the configuration, ranging from 1 to 12, in the format of 1-3, 5. You can select more than one entry for each command. By default, the configuration of all history sample entries is displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the configuration of all history sample entries:

```
T2500G-10TS# show rmon history
```

33.25 show rmon event

Description

The **show rmon event** command is used to display the configuration of SNMP-RMON Event.

Syntax

```
show rmon event [index]
```

Parameter

index — The index number of the entry selected to display the configuration, ranging from 1 to 12, in the format of 1-3, 5. You can select more than one entry for each command. By default, the configuration of all SNMP-RMON enabled entries is displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the Event configuration of entry1-4:

```
T2500G-10TS# show rmon event 1-4
```

33.26 show rmon alarm

Description

The **show rmon alarm** command is used to display the configuration of the Alarm Management entry.

Syntax

```
show rmon alarm [ index ]
```

Parameter

index — The index number of the entry selected to display the configuration, ranging from 1 to 12, in the format of 1-3, 5. You can select more than one entry for each command. By default, the configuration of all Alarm Management entries is displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the configuration of the Alarm Management entry 1-2:

```
T2500G-10TS# show rmon alarm 1-2
```

33.27 show rmon statistics

Description

The **show rmon statistics** command is used to display the configuration of the specified statistics entry.

Syntax

```
show rmon statistics [ index ]
```

Parameter

index — The index number of the statistics entry selected to display the configuration, ranging from 1 to 65535. By default, the configuration of all statistics entries is displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the configuration of the statistics entry 1:

```
T2500G-10TS#show rmon statistics 1
```

Chapter 34 LLDP Commands

LLDP function enables network devices to advertise their own device information periodically to neighbors on the same LAN. The information of the LLDP devices in the LAN can be stored by its neighbor in a standard MIB, so it is possible for the information to be accessed by a Network Management System (NMS) using SNMP.

34.1 lldp

Description

The **lldp** command is used to enable LLDP function. To disable the LLDP function, please use **no lldp** command.

Syntax

lldp

no lldp

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable LLDP function globally:

```
T2500G-10TS(config)#lldp
```

34.2 lldp hold-multiplier

Description

The **lldp hold-multiplier** command is used to configure the Hold Multiplier parameter. The aging time of the local information in the neighbor device is determined by the actual TTL value used in the sending LLDPDU. $TTL = \text{Hold Multiplier} * \text{Transmit Interval}$. To return to the default configuration, please use **no lldp hold-multiplier** command.

Syntax

lldp hold-multiplier *multiplier*

no lldp hold-multiplier

Parameter

multiplier — Configure the Hold Multiplier parameter. It ranges from 2 to 10. By default, it is 4.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify Hold Multiplier as 5:

```
T2500G-10TS(config)#lldp hold-multiplier 5
```

34.3 lldp timer

Description

The **lldp timer** command is used to configure the parameters about transmission. To return to the default configuration, please use **no lldp timer** command.

Syntax

```
lldp timer { tx-interval tx-interval / tx-delay tx-delay / reinit-delay reinit-delay / notify-interval notify-interval / fast-count fast-count }
```

```
no lldp timer { tx-interval | tx-delay | reinit-delay | notify-interval | fast-count }
```

Parameter

tx-interval — Configure the interval for the local device to transmit LLDPDU to its neighbors. The value ranges from 5 to 32768 and the default value is 30 seconds.

tx-delay — Configure a value from 1 to 8192 in seconds to specify the time for the local device to transmit LLDPDU to its neighbors after changes occur so as to prevent LLDPDU being sent frequently. By default, it is 2 seconds.

reinit-delay — This parameter indicates the amount of delay from when LLDP status becomes "disable" until re-initialization will be attempted. The value ranges from 1 to 10 and the default value is 3.

notify-interval — Specify the interval of Trap message which will be sent from local device to network management system. The value ranges from 5 to 3600 and the default value is 5 seconds.

fast-count — When the port's LLDP state transforms from Disable (or Rx_Only) to Tx&Rx (or Tx_Only), the fast start mechanism will be enabled, that is, the transmit interval will be shorten to a second, and several LLDPDUs will be sent out (the number of LLDPDUs equals this parameter). The value ranges from 1 to 10 and the default value is 3.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the Transmit Interval of LLDPDU as 45 seconds and Trap message to NMS as 120 seconds:

```
T2500G-10TS(config)#lldp timer tx-interval 45
T2500G-10TS(config)#lldp timer notify-interval 120
```

34.4 Ildp receive

Description

The **lldp receive** command is used to enable the designated port to receive LLDPDU. To disable the function, please use **no lldp receive** command.

Syntax

```
lldp receive
no lldp receive
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable Gigabit Ethernet port 1/0/1 to receive LLDPDU:

```
T2500G-10TS(config)#interface gigabitEthernet 1/0/1
T2500G-10TS(config-if)#lldp receive
```

34.5 lldp transmit

Description

The **lldp transmit** command is used to enable the designated port to transmit LLDPDU. To disable the function, please use **no lldp transmit** command.

Syntax

lldp transmit
no lldp transmit

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable Gigabit Ethernet port 1/0/1 to transmit LLDPDU:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/1
T2500G-10TS(config-if)#lldp transmit
```

34.6 lldp snmp-trap

Description

The **lldp snmp-trap** command is used to enable the port's SNMP notification. If enabled, the port will notify the trap event to network management system. To disable the ports' SNMP notification, please use **no lldp snmp-trap** command.

Syntax

lldp snmp-trap
no lldp snmp-trap

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the SNMP notification for Gigabit Ethernet port 1/0/1:

```
T2500G-10TS(config)#interface gigabitEthernet 1/0/1
T2500G-10TS(config-if)#lldp snmp-trap
```

34.7 lldp tlv-select

Description

The **lldp tlv-select** command is used to configure TLVs to be included in outgoing LLDPDU. To exclude TLVs, please use **no lldp tlv-select** command. By default, All TLVs are included in outgoing LLDPDU.

Syntax

```
lldp tlv-select { [ port-description ] [ system-capability ] [ system-description ]
[ system-name ] [ management-address ] [ port-vlan ] [ protocol-vlan ]
[ vlan-name ] [ link-aggregation ] [ mac-phy-cfg ] [ max-frame-size ] [ power ]
[ all ] }
```

```
no lldp tlv-select { [ port-description ] [ system-capability ]
[ system-description ] [ system-name ] [ management-address ] [ port-vlan ]
[ protocol-vlan ] [ vlan-name ] [ link-aggregation ] [ mac-phy-cfg ]
[ max-frame-size ] [ power ] [ all ] }
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Exclude "management-address" and "port-vlan-id" TLVs in LLDPDU outgoing from Gigabit Ethernet port 1/0/1:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/1
T2500G-10TS(config-if)# no lldp tlv-select management-address port-vlan
```

34.8 lldp med-fast-count

Description

The **lldp med-fast-count** command is used to configure the number of the LLDP-MED frames that will be sent out. When LLDP-MED fast start mechanism is activated, multiple LLDP-MED frames will be transmitted based on this parameter. The default value is 4. To return to the default configuration, please use **no lldp med-fast-count** command.

Syntax

lldp med-fast-count *count*

no lldp med-fast-count

Parameter

count — Configure the Fast Start Count parameter. It ranges from 1 to 10. By default, it is 4.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify Fast Start Count as 5:

```
T2500G-10TS(config)# lldp med-fast-count 5
```

34.9 lldp med-status

Description

The **lldp med-status** command is used to enable the LLDP-MED feature for the corresponding port. After the LLDP-MED feature is enabled, the port's Admin Status will be changed to Tx&Rx. To disable the LLDP-MED feature for the corresponding port, please use **no lldp med-status** command.

Syntax

lldp med-status

no lldp med-status

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the LLDP-MED feature for port 1/0/2:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/2
T2500G-10TS(config-if)# lldp med-status
```

34.10 lldp med-tlv-select

Description

The **lldp med-tlv-select** command is used to configure LLDP-MED TLVs to be included in outgoing LLDPDU for the corresponding port. To exclude LLDP-MED TLVs, please use **no lldp med-tlv-select** command. By default, All TLVs are included in outgoing LLDPDU.

Syntax

```
lldp med-tlv-select { [inventory-management] [location] [network-policy]
[power-management] [all] }
```

```
no lldp med-tlv-select { [inventory-management] [location] [network-policy]
[power-management] [all] }
```

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Exclude "network policy" and "inventory" TLVs in LLDPDU outgoing from port 1/0/2:

```
T2500G-10TS(config)# interface gigabitEthernet 1/0/2
```

```
T2500G-10TS(config-if)# no lldp med-tlv-select network-policy inventory-  
management
```

34.11 lldp med-location

Description

The `lldp med-location` command is used to configure the Location Identification TLV's content in outgoing LLDPDU of the port.

Syntax

```
lldp med-location { emergency-number identifier | civic-address  
[[ language language ] [ province-state province-state ] [ county county ] [ city  
city ] [ street street ] [ house-number house-number ] [ name name ]  
[ postal-zipcode postal-zipcode ] [ room-number room-number ]  
[ post-office-box post-office-box ] [ additional additional ] [ country-code  
country-code ] [ what { dhcp-server | endpoint | switch } ] ] }
```

Parameter

`emergency-number` — Emergency Call Service ELIN identifier, which is used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. The length of this field ranges from 10 to 25 characters.

`civic-address` — The civic address is defined to reuse the relevant sub-fields of the DHCP option for civic Address based Location Configuration Information as specified by IETF.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure the civic address in the Location Identification TLV's content in outgoing LLDPDU of port 1/0/2. Configure the language as English and city as London:

```
T2700-28TQ (config)# interface gigabitEthernet 1/0/2  
T2700-28TQ(config-if)# lldp med-location civic-address language English  
city London
```

34.12 show lldp

Description

The **show lldp** command is used to display the global configuration of LLDP.

Syntax

```
show lldp
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of LLDP:

```
T2500G-10TS#show lldp
```

34.13 show lldp interface

Description

The **show lldp interface** command is used to display LLDP configuration of the corresponding port. By default, the LLDP configuration of all the ports will be displayed.

Syntax

```
show lldp interface [ gigabitEthernet port ]
```

Parameters

port— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the LLDP configuration of Gigabit Ethernet port 1/0/1:

```
T2500G-10TS#show lldp interface gigabitEthernet 1/0/1
```

34.14 show lldp local-information interface

Description

The **show lldp local-information interface** command is used to display the LLDP information of the corresponding port. By default, the LLDP information of all the ports will be displayed.

Syntax

```
show lldp local-information interface [ gigabitEthernet port]
```

Parameters

port— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the LLDP information of Gigabit Ethernet port 1/0/1:

```
T2500G-10TS#show lldp local-information interface gigabitEthernet 1/0/1
```

34.15 show lldp neighbor-information interface

Description

The **show lldp neighbor-information interface** command is used to display the neighbor information of the corresponding port. By default, the neighbor information of all the ports will be displayed.

Syntax

```
show lldp neighbor-information interface [ gigabitEthernet port]
```

Parameters

port— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the neighbor information of Gigabit Ethernet port 1/0/1:

```
T2500G-10TS#show lldp neighbor-information interface gigabitEthernet
1/0/1
```

34.16 show lldp traffic interface

Description

The **show lldp traffic interface** command is used to display the LLDP statistic information between the local device and neighbor device of the corresponding port. By default, the LLDP statistic information of all the ports will be displayed.

Syntax

```
show lldp traffic interface [ gigabitEthernet port ]
```

Parameters

port— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the LLDP statistic information of Gigabit Ethernet port 1/0/1:

```
T2500G-10TS#show lldp traffic interface gigabitEthernet 1/0/1
```

Chapter 35 AAA Commands

AAA stands for authentication, authorization and accounting. This feature is used to authenticate users trying to log in to the switch or trying to access the administrative level privilege.

➤ **Applicable Access Application**

The authentication can be applied on the following access applications: Console, Telnet, SSH and HTTP.

➤ **Authentication Method List**

A method list describes the authentication methods and their sequence to authenticate a user. The switch supports Login List for users to gain access to the switch, and Enable List for normal users to gain administrative privileges.

➤ **RADIUS/TACACS+ Server**

User can configure the RADIUS/TACACS+ servers for the connection between the switch and the server.

➤ **Server Group**

User can define the authentication server group with up to several servers running the same secure protocols, either RADIUS or TACACS+. Users can set these servers in a preferable order, which is called the server group list. When a user tries to access the switch, the switch will ask the first server in the server group list for authentication. If no response is received, the second server will be queried, and so on.

35.1 **aaa enable**

Description

The **aaa enable** command is used to enable the AAA function globally. To disable the AAA function globally, please use the **no aaa enable** command. The global AAA function is disabled by default.

Syntax

aaa enable
no aaa enable

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the AAA function globally:

```
T2500G-10TS(config)# aaa enable
```

35.2 enable admin password

Description

The **enable admin password** command is used to elevate the current logged-in user from guest to admin and gain administrator level privileges. The authentication password is possibly authenticated in RADIUS/TACACS+ servers, user-defined server groups or local on the switch.

To remove the password, please use **no enable admin password** command. This command uses the symmetric encryption.

Syntax

```
enable admin password {[ 0 ] password | 7 encrypted-password}
```

```
no enable admin password
```

Parameter

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

password — A string from 1 to 31 alphanumeric characters or symbols. The password is case sensitive, allows digits, English letters (case sensitive), underlines and sixteen special characters (!\$%()*,-./[]{}). By default, it is empty.

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

encrypted-password — A symmetric encrypted password with fixed length, which you can copy from another switch's configuration file. After the encrypted password is configured, you should use the corresponding unencrypted password to elevate the privilege.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

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

Example

Set the elevation password as 123 for the current logged-in user to gain administrator level privileges:

```
T2500G-10TS(config)#enable admin password 0 123
```

35.3 enable admin secret

Description

The **enable admin secret** command is used to elevate the current logged-in user from guest to admin and gain administrator level privileges. The authentication password is possibly authenticated in RADIUS/TACACS+ servers, user-defined server groups or local on the switch.

To remove the password, please use **no enable admin secret** command.

This command uses the MD5 encryption.

Syntax

```
enable secret {[ 0] password | 5 encrypted-password}
```

```
no enable secret
```

Parameter

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

password — Super password, a string from 1 to 31 alphanumeric characters or symbols. The password is case sensitive, allows digits, English letters (case sensitive), underlines and sixteen special characters (!\$%'()*,-./[]{}). By default, it is empty. The password in the configuration file will be displayed in the MD5 encrypted form.

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

encrypted-password — An MD5 encrypted password with fixed length, which you can copy from another switch's configuration file. After the encrypted password is configured, you should use the corresponding unencrypted password to elevate the privilege.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

If both the **enable admin password** and **enable admin secret** are defined, you must enter the password set in **enable admin secret**.

Example

Set the secret elevation password as 123 for the current logged-in user to gain administrator level privileges. The password will be displayed in the encrypted form:

```
T2500G-10TS(config)#enable admin secret 0 123
```

35.4 tacacs-server host

Description

The **tacacs-server host** command is used to configure a new TACACS+ server. To delete the specified TACACS+ server, please use **no tacacs-server host** command.

Syntax

```
tacacs-server host ip-address [ port port-id ] [ timeout time ] [ key { [ 0 ] string | 7 encrypted-string } ]
```

```
no tacacs-server host ip-address
```

Parameter

ip-address — Specify the IP address of the TACACS+ server.

port-id — Specify the server's port number for AAA. By default it is 49.

time — Specify the time in seconds the switch waits for the server's response before it times out. The time ranges from 1 to 9 seconds. The default is 5 seconds.

[0] *string* | 7 *encrypted-string* — 0 and 7 are the encryption type. 0 indicates that an unencrypted key will follow. 7 indicates that a symmetric encrypted key with a fixed length will follow. By default, the encryption type is

0. *string* is the shared key for the switch and the authentication servers to exchange messages which contains 31 characters at most. The question marks and spaces are not allowed. *encrypted-string* is a symmetric encrypted key with a fixed length, which you can copy from another switch's configuration file. The key or encrypted-key you configured here will be displayed in the encrypted form. Always configure the key as the last item of this command.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

The TACACS+ servers you configured are added in the server group "tacacs" by default.

Example

Configure a TACACS+ server with the IP address as 1.1.1.1, TCP port as 1500, timeout as 6 seconds, and the unencrypted key string as 12345.

```
T2500G-10TS(config)# tacacs-server host 1.1.1.1 port 1500 timeout 6 key  
12345
```

35.5 show tacacs-server

Description

This **show tacacs-server** command is used to display the summary information of the TACACS+ servers.

Syntax

```
show tacacs-server
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of all the TACACS+ servers:

```
T2500G-10TS(config)# show tacacs-server
```

35.6 radius-server host

Description

The **radius-server host** command is used to configure a new RADIUS server. To delete the specified RADIUS server, please use **no radius-server host** command.

Syntax

```
radius-server host ip-address [ auth-port port-id ] [ acct-port port-id ]  
[ timeout time ] [ retransmit number ] [ nas-id nas-id ] [ key { [ 0 ] string | 7  
encrypted-string } ]
```

```
no radius-server host ip-address
```

Parameter

ip-address — Specify the IP address of the RADIUS server.

auth-port *port-id* — Specify the UDP destination port for authentication requests. By default it is 1812.

acct-port *port-id* — Specify the UDP destination port for accounting requests. By default it is 1813.

time — Specify the time in seconds the switch waits for the server's response before it times out. The time ranges from 1 to 9 seconds. The default is 5 seconds.

number — Specify the number of times a RADIUS request is resent to a server if the server is not responding in time. By default it is 2 times.

nas-id — Specify the name of the NAS (Network Access Server) to be contained in RADIUS packets for identification. It ranges from 1 to 31 characters. The default value is the MAC address of the switch. Generally, the NAS indicates the switch itself.

[0] *string* | 7 *encrypted-string* — 0 and 7 are the encryption type. 0 indicates that an unencrypted key will follow. 7 indicates that a symmetric encrypted key with a fixed length will follow. By default, the encryption type is 0. "*string*" is the shared key for the switch and the authentication servers to exchange messages which contains 31 characters at most. The question marks and spaces are not allowed. "*encrypted-string*" is a symmetric

encrypted key with a fixed length, which you can copy from another switch's configuration file. The key or encrypted-key you configured here will be displayed in the encrypted form. Always configure the key as the last item of this command.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

The RADIUS servers you configured are added in the server group "radius" by default.

Example

Configure a RADIUS server with the IP address as 1.1.1.1, authentication port as 1200, timeout as 6 seconds, retransmit times as 3, and the unencrypted key string as 12345.

```
T2500G-10TS (config)# radius-server host 1.1.1.1 auth-port 1200 timeout  
6 retransmit 3 key 12345
```

35.7 show radius-server

Description

This **show radius-server** command is used to display the summary information of the RADIUS servers.

Syntax

```
show radius-server
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of all the RADIUS servers:

```
T2500G-10TS(config)# show radius-server
```


35.8 aaa group

Description

This **aaa group** command is used to create AAA server groups to group existing TACACS+/RADIUS servers for authentication. This command puts the switch in the server group subconfiguration mode.

To delete the corresponding AAA group, please use the **no aaa group** command.

Syntax

aaa group { radius | tacacs } *group-name*

no aaa group { radius | tacacs } *group-name*

Parameter

radius | tacacs — Specify the server group type as RADIUS or TACACS+.

group-name — Specify the server group name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Create a RADIUS server group with the name radius1:

```
T2500G-10TS(config)# aaa group radius radius1
```

35.9 server

Description

This **server** command is used to add the existing server in the defined server group. To remove the specified server from the server group, please use the **no server** command.

Syntax

```
server ip-address  
no server ip-address
```

Parameter

ip-address—— Specify the server's IP address.

Command Mode

Server Group Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Create the RADIUS server 1.1.1.1 to RADIUS server group "radius1":

```
T2500G-10TS(config)# aaa group radius radius1  
T2500G-10TS(aaa-group)# server 1.1.1.1
```

35.10 show aaa group

Description

This **show aaa group** command is used to display the summary information of the AAA groups. All the servers in this group will be listed if you specify the group name.

Syntax

```
show aaa group [ group-name ]
```

Parameter

group-name—— Specify the server group name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of all the server groups:

```
T2500G-10TS(config)# show aaa group
```

35.11 aaa authentication login

Description

This **aaa authentication login** command is used to configure a login authentication method list. A method list describes the authentication methods and their sequence to authenticate a user. To delete the specified authentication method list, please use the **no aaa authentication login** command.

Syntax

```
aaa authentication login { method-list } { method1 } [ method2 ] [ method3 ]  
[ method4 ]
```

```
no aaa authentication login method-list
```

Parameter

method-list — Specify the method list name.

method1, method2, method3, method4 — Specify the authentication methods in order. The next authentication method is tried only if the previous method does not respond, not if it fails.

The preset methods include radius, tacacs, local and none. "radius" means the RADIUS server group "radius"; "tacacs" means the RACACS+ server group "tacacs"; "local" means local username database are used; "none" means no authentication is used for login.

Users can also define new method with the [aaa group](#) command.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

By default the login authentication method list is "default" with "local" as method1.

Example

Configure a login authentication method list "list1" with the priority1 method as radius and priority2 method as local:

```
T2500G-10TS(config)# aaa authenticaiton login list1 radius local
```

35.12 aaa authentication enable

Description

This **aaa authentication enable** command is used to configure a privilege authentication method list. A method list describes the authentication methods and their sequence to elevate a user's privilege. To delete the specified authentication method list, please use the **no aaa authentication enable** command.

Syntax

```
aaa authentication enable { method-list } { method1 } [ method2 ] [ method3 ]  
[ method4 ]
```

```
no aaa authentication enable method-list
```

Parameter

method-list — Specify the method list name.

method1, method2, method3, method4 — Specify the authentication methods in order. The next authentication method is tried only if the previous method does not respond, not if it fails.

The preset methods include radius, tacacs, local and none. "radius" means the RADIUS server group "radius"; "tacacs" means the RACACS+ server group "tacacs"; "local" means local username database are used; "none" means no authentication is used for privilege elevation.

Users can also define new method with the [aaa group](#) command.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

By default the enable authentication method is "default" with "none" as method1.

Example

Configure a privilege authentication method list "list2" with the priority1 method as radius and priority2 method as local:

```
T2500G-10TS(config)# aaa authenticaion enable list2 radius local
```

35.13 aaa authentication dot1x default

Description

This **aaa authentication dot1x default** command is used to configure an 802.1X authentication method list. A method list describes the authentication methods for users' login in 802.1X. To delete the default authentication method list, please use the **no aaa authentication dot1x default** command.

Syntax

```
aaa authentication dot1x default { method }
```

```
no aaa authentication dot1x default
```

Parameter

method — Specify the method name. Only RADIUS server group is supported, and the default method is server group "radius".

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the default 802.1X authentication method as "radius1":

```
T2500G-10TS(config)# aaa authentication dot1x default radius1
```

35.14 aaa accounting dot1x default

Description

This **aaa accounting dot1x default** command is used to configure an 802.1X accounting method list. To delete the default accounting method list, please use the **no aaa accounting dot1x default** command.

Syntax

```
aaa accounting dot1x default { method }
```

```
no aaa accounting dot1x default
```

Parameter

method — Specify the method name. Only RADIUS server group is supported, and the default method is server group "radius".

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the default 802.1X accounting method as "radius1":

```
T2500G-10TS(config)# aaa accounting dot1x default radius1
```

35.15 show aaa authentication

Description

This **show aaa authentication** command is used to display the summary information of the authentication login, enable and dot1x method list.

Syntax

```
show aaa authentication [ login | enable | dot1x ]
```

Parameter

login | enable | dot1x — Specify the method list type.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of all the authentication method lists:

```
T2500G-10TS(config)# show aaa authentication
```

35.16 show aaa accounting

Description

This **show aaa accounting** command is used to display the summary information of the accounting method list.

Syntax

```
show aaa accounting [ dot1x ]
```

Parameter

dot1x — Specify the method list type.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of the default 802.1X accounting method list:

```
T2500G-10TS(config)# show aaa accounting
```

35.17 line console

Description

The **line console** command is used to enter the Line Configuration Mode configure the console port to which you want to apply the authentication list.

Syntax

```
line console { linenum }
```

Parameter

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

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

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

```
T2500G-10TS(config)#line console 0
```

35.18 login authentication(console)

Description

The **login authentication** command is used to apply the login authentication method list to the console port. To restore to the default authentication method list, please use the **no login authentication** command.

Syntax

```
login authentication { method-list }
```

```
no login authentication
```

Parameter

method-list — Specify the login method list on the console port. It is "default" by default, which contains the method "local".

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the login authentication method list on the console port as "list1":

```
T2500G-10TS(config)# line console 0
```

```
T2500G-10TS(config-line)# login authentication list1
```


35.19 enable authentication(console)

Description

The **enable authentication** command is used to apply the privilege authentication method list to the console port. To restore to the default authentication method list, please use the **no enable authentication** command.

Syntax

```
enable authentication { method-list }
```

```
no enable authentication
```

Parameter

method-list — Specify the enable method list on the console port. It is "default" by default, which contains the method "none".

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the enable authentication method list on the console port as "list2":

```
T2500G-10TS(config)# line console 0
T2500G-10TS(config-line)# enable authentication list2
```

35.20 line telnet

Description

The **line telnet** command is used to enter the Line Configuration Mode to configure the telnet terminal line to which you want to apply the authentication list.

Syntax

```
line telnet
```

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enter the telnet terminal line configuration mode:

```
T2500G-10TS(config)#line telnet
```

35.21 login authentication(telnet)

Description

The **login authentication** command is used to apply the login authentication method list to the telnet terminal line. To restore to the default authentication method list, please use the **no login authentication** command.

Syntax

login authentication { *method-list* }

no login authentication

Parameter

method-list — Specify the login method list on the telnet terminal line. It is "default" by default, which contains the method "local".

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the login authentication method list on the telnet terminal line as "list1":

```
T2500G-10TS(config)#line telnet
```

```
T2500G-10TS(config-line)# login authentication list1
```

35.22 line ssh

Description

The **line ssh** command is used to enter the Line Configuration Mode to configure the ssh terminal line to which you want to apply the authentication list.

Syntax

```
line ssh
```

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enter the ssh terminal line configuration mode:

```
T2500G-10TS(config)#line ssh
```

35.23 login authentication(ssh)

Description

The **login authentication** command is used to apply the login authentication method list to the ssh terminal line. To restore to the default authentication method list, please use the **no login authentication** command.

Syntax

```
login authentication { method-list }
```

```
no login authentication
```

Parameter

method-list — Specify the login method list on the ssh terminal line. It is "default" by default, which contains the method "local".

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the login authentication method list on the ssh terminal line as "list1":

```
T2500G-10TS(config)# line ssh
T2500G-10TS(config-line)# login authentication list1
```

35.24 enable authentication(telnet)

Description

The **enable authentication** command is used to apply the privilege authentication method list to the telnet terminal line. To restore to the default authentication method list, please use the **no enable authentication** command.

Syntax

enable authentication { *method-list* }

no enable authentication

Parameter

method-list—— Specify the enable method list on the telnet terminal line. It is "default" by default, which contains the method "none".

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the enable authentication method list on the telnet terminal line as "list2":

```
T2500G-10TS(config)#line telnet
T2500G-10TS(config-line)# enable authentication list2
```

35.25 enable authentication(ssh)

Description

The **enable authentication** command is used to apply the privilege authentication method list to the ssh terminal line. To restore to the default authentication method list, please use the **no enable authentication** command.

Syntax

```
enable authentication { method-list }
```

```
no enable authentication
```

Parameter

method-list — Specify the enable method list on the ssh terminal line. It is "default" by default, which contains the method "none".

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the enable authentication method list on the ssh terminal line as "list2":

```
T2500G-10TS(config)# line ssh
T2500G-10TS(config-line)# enable authentication list2
```

35.26 ip http login authentication

Description

The **ip http login authentication** command is used to apply the login authentication method list to users accessing through HTTP. To restore to the default authentication method list, please use the **no ip http login authentication** command.

Syntax

```
ip http login authentication { method-list }
```

no ip http login authentication

Parameter

method-list — Specify the login method list on the HTTP access. It is "default" by default, which contains the method "local".

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the login authentication method list on the HTTP access as "list1":

```
T2500G-10TS(config)# ip http login authentication list1
```

35.27 ip http enable authentication

Description

The **ip http enable authentication** command is used to apply the privilege authentication method list to users accessing through HTTP. To restore to the default authentication method list, please use the **no ip http enable authentication** command.

Syntax

```
ip http enable authentication { method-list }
```

```
no ip http enable authentication
```

Parameter

method-list — Specify the enable method list on the HTTP access. It is "default" by default, which contains the method "none".

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the enable authentication method list on the HTTP access as "list2":

```
T2500G-10TS(config)# ip http enable authentication list2
```

35.28 show aaa global

Description

This **show aaa global** command is used to display global status of AAA function and the login/enable method lists of different application modules: console, telnet, ssh and HTTP.

Syntax

```
show aaa global
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the AAA function's global status and each application's method list:

```
T2500G-10TS(config)# show aaa global
```

Chapter 36 DHCP Relay Commands

A DHCP Relay is a device that forwards DHCP packets between clients and servers. DHCP Relay forward requests and replies between clients and servers when they are not on the same physical subnet.

36.1 ip dhcp relay

Description

The **ip dhcp relay** command is used to enable DHCP Relay function globally. To disable DHCP Relay function, please use **no ip dhcp relay** command.

Syntax

ip dhcp relay
no ip dhcp relay

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable DHCP Relay function globally:

```
T2500G-10TS(config)# ip dhcp relay
```

36.2 ip dhcp relay information option

Description

The **ip dhcp relay information option** command is used to enable option 82 support in DHCP Relay. To disable this function, please use **no ip dhcp relay information option** command.

Syntax

ip dhcp relay information option
no ip dhcp relay information option

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable option 82 support in DHCP Relay:

```
T2500G-10TS(config)# ip dhcp relay information option
```

36.3 ip dhcp relay information strategy

Description

The **ip dhcp relay information strategy** command is used to specify the operation for the Option 82 field of the DHCP request packets from the Host. To restore to the default option, please use **no ip dhcp relay information strategy** command.

Syntax

```
ip dhcp relay information strategy { drop | keep | replace }  
no ip dhcp relay information strategy
```

Parameter

drop | keep | replace —The operations for Option 82 field of the DHCP request packets from the Host. The default operation is keep.

drop: Discard the packet with the Option 82 field.

keep: Keep the Option 82 field in the packet.

replace: Replace the option 82 field with the system option defined by the switch.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the option 82 policy as replace to replace the Option 82 field with the local parameter on receiving the DHCP request packet:

```
T2500G-10TS(config)# ip dhcp relay information strategy replace
```

36.4 ip dhcp relay information format

Description

The **ip dhcp relay information format** command is used to select the format of option 82 sub-option value field. To restore to the default option, please use **no ip dhcp relay information format** command.

Syntax

```
ip dhcp relay information format { normal | private }  
no ip dhcp relay information format
```

Parameter

normal | private — The format type of option 82 sub-option value field.

normal: Indicates that the format of sub-option value field is TLV (type-length-value).

private: Indicates that the format of sub-option value field is the value you configure for the related sub-option.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Select the format of option 82 sub-option value field as TLV (type-length-value):

```
T2500G-10TS (config)#ip dhcp relay information format normal
```

36.5 ip dhcp relay information circuit-id

Description

The **ip dhcp relay information circuit-id** command is used to specify the custom circuit ID when option 82 customization is enabled. To clear the circuit ID, please use **no ip dhcp relay information circuit-id** command.

Syntax

```
ip dhcp relay information circuit-id circuitID  
no ip dhcp relay information circuit-id
```

Parameter

circuitID— Specify the circuit ID, ranging from 1 to 63 characters.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the circuit ID as "TP-Link":

```
T2500G-10TS(config)# ip dhcp relay information circuit-id TP-Link
```

36.6 ip dhcp relay information remote-id

Description

The **ip dhcp relay information remote-id** command is used to specify the custom remote ID when option 82 customization is enabled. To clear the remote ID, please use **no ip dhcp relay information remote-id** command.

Syntax

```
ip dhcp relay information remote-id remoteID  
no ip dhcp relay information remote-id
```

Parameter

remoteID— Specify the remote ID, ranging from 1 to 63 characters.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the remote ID as "TP-Link":

```
T2500G-10TS(config)# ip dhcp relay information remote-id TP-Link
```

36.7 ip dhcp relay vlan

Description

The **ip dhcp relay vlan** command is used to add DHCP server address to specified VLAN. If there is an IP interface in the VLAN and it has configured a DHCP server address at the interface level, then the configuration at the interface level has higher priority. In this case, the DHCP server configured on the VLAN will not be used to forward the DHCP packets. To delete the DHCP server address use **no ip dhcp relay vlan**.

Syntax

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

Parameter

vid—— VLAN ID.

ip-address—— DHCP Server address.

Command mode

Global Configuration Mode

Privilege Requirement

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

Example

Add DHCP server address 192.168.2.1 to VLAN 1 :

```
T2500G-10TS (config)# ip dhcp relay vlan 1 helper-address 192.168.2.1
```

36.8 show ip dhcp relay

Description

The **show ip dhcp relay** command is used to display the global status and Option 82 configuration of DHCP Relay.

Syntax

```
show ip dhcp relay
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of DHCP Relay:

```
T2500G-10TS(config)# show ip dhcp relay
```