CLI Reference Guide

T1700X-16TS

1910012423 REV3.0.0

June 2018

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 © 2018 TP-Link Technologies Co., Ltd. All rights reserved.

https://www.tp-link.com

CONTENTS

Preface 1

Chapter 1 Using the CLI 5

1.1 Accessing the CLI 5

1.1.1 Logon by Telnet 5

1.1.2 Logon by SSH 6

1.2 CLI Command Modes 11

1.3 Privilege Restrictions 14

1.4 Conventions 14

1.4.1 Format Conventions 14

1.4.2 Special Characters 15

1.4.3 Parameter Format 15

Chapter 2 User Interface 16

2.1 enable 16

2.2 service password-encryption 16

2.3 enable password 17

2.4 enable secret 18

2.5 configure 19

2.6 exit 20

2.7 end 20

2.8 clipaging 21

2.9 history 21

2.10 history clear 22

Chapter 3 User Management Commands 23

3.1 user name (password) 23

3.2 user name (secret) 24

3.3 show user account-list 25

3.4 show user configuration 26

Chapter 4 System Configuration Commands 27

4.1 system-time manual 27

4.2 system-time ntp 27

4.3 system-time dst predefined 29

4.4 system-time dst date 30

4.5 system-time dst recurring 31

4.6 hostname 32
4.7 location 33
4.8 contact-info 33
4.9 ip address 34
4.10 ip address-alloc 35
4.11 reset 36
4.12 reboot 36
4.13 reboot-schedule 37
4.14 copy running-config startup-config 38
4.15 copy startup-config tftp 38
4.16 copy tftp startup-config 39
4.17 copy backup-config tftp 40
4.18 copy backup-config startup-config 40
4.19 copy running-config backup-config 41
4.20 copy tftp backup-config 41
4.21 boot application 42
4.22 boot config 43
4.23 remove backup-image 43
4.24 firmware upgrade 44
4.25 ping 45
4.26 tracert 46
4.27 show system-info 47
4.28 show image-info 47
4.29 show boot 48
4.30 show running-config 48
4.31 show startup-config 49
4.32 show system-time 49
4.33 show system-time dst 50
4.34 show system-time ntp 50
4.35 show cable-diagnostics interface 51
4.36 show cpu-utilization 51
4.37 show memory-utilization 52

Chapter 5 EEE Configuration Commands 53

5.1 eee 53
5.2 show interface eee 53

Chapter 6 SDM Template Commands 55

6.1 sdm prefer 55
6.2 show sdm prefer 56

Chapter 7 Time Range Commands 57

7.1 time-range 57
7.2 absolute 57
7.3 periodic 58
7.4 holiday (time-range mode) 59
7.5 holiday 60
7.6 show holiday 60
7.7 show time-range 61

Chapter 8 Port Configuration Commands 62

8.1 interface ten-gigabitEthernet 62
8.2 interface range ten-gigabitEthernet 62
8.3 description 63
8.4 shutdown 64
8.5 flow-control 65
8.6 duplex 65
8.7 jumbo-size 66
8.8 speed 66
8.9 clear counters 67
8.10 show interface status 68
8.11 show interface counters 68
8.12 show interface configuration 69

Chapter 9 Port Isolation Commands 70

9.1 port isolation 70
9.2 show port isolation interface 71

Chapter 10 Loopback Detection Commands 72

10.1 loopback-detection (global) 72
10.2 loopback-detection interval 72
10.3 loopback-detection recovery-time 73
10.4 loopback-detection (interface) 74
10.5 loopback-detection config process-mode 74
10.6 loopback-detection recover 75
10.7 show loopback-detection global 76

10.8 show loopback-detection interface 76

Chapter 11 Etherchannel Commands 78

11.1 channel-group 78
11.2 port-channel load-balance 79
11.3 lacp system-priority 80
11.4 lacp port-priority 81
11.5 show etherchannel 81
11.6 show etherchannel load-balance 82
11.7 show lacp 83
11.8 show lacp sys-id 83

Chapter 12 MAC Address Commands 85

12.1 mac address-table static 85
12.2 mac address-table aging-time 86
12.3 mac address-table filtering 86
12.4 mac address-table max-mac-count 87
12.5 show mac address-table 89
12.6 clear mac address-table 89
12.7 show mac address-table aging-time 90
12.8 show mac address-table max-mac-count 90
12.9 show mac address-table interface 91
12.10 show mac address-table count 91
12.11 show mac address-table address 92
12.12 show mac address-table vlan 93

Chapter 13 IEEE 802.1Q VLAN Commands 94

13.1 vlan 94
13.2 name 95
13.3 switchport general allowed vlan 95
13.4 switchport pvid 96
13.5 switchport check ingress 97
13.6 switchport acceptable frame 97
13.7 show vlan summary 98
13.8 show vlan brief 99
13.9 show vlan 99
13.10 show interface switchport 100

Chapter 14 MAC-based VLAN Commands 101

14.1 mac-vlan mac-address 101
14.2 mac-vlan 102
14.3 show mac-vlan 102
14.4 show mac-vlan interface 103

Chapter 15 Protocol-based VLAN Commands 104

15.1 protocol-vlan template 104
15.2 protocol-vlan vlan 105
15.3 protocol-vlan group 106
15.4 show protocol-vlan template 106
15.5 show protocol-vlan vlan 107

Chapter 16 GVRP Commands 108

16.1 gvrp 108
16.2 gvrp (interface) 108
16.3 gvrp registration 109
16.4 gvrp timer 110
16.5 show gvrp interface 111
16.6 show gvrp global 111

Chapter 17 IGMP Snooping Commands 113

17.1 ip igmp snooping (global) 113
17.2 ip igmp snooping version 113
17.3 ip igmp snooping drop-unknown 114
17.4 ip igmp snooping header-validation 115
17.5 ip igmp snooping vlan-config 115
17.6 ip igmp snooping vlan-config (immediate-leave) 117
17.7 ip igmp snooping vlan-config (report-suppression) 117
17.8 ip igmp snooping vlan-config (router-ports-forbidden) 118
17.9 ip igmp snooping vlan-config (rport interface) 119
17.10 ip igmp snooping vlan-config (static) 120
17.11 ip igmp snooping vlan-config (querier) 121
17.12 ip igmp snooping (interface) 122
17.13 ip igmp snooping max-groups 123
17.14 ip igmp snooping immediate-leave 124
17.15 ip igmp profile 124
17.16 deny 125

17.17 permit 125
17.18 range 126
17.19 ip igmp filter 127
17.20 clear ip igmp snooping statistics 127
17.21 show ip igmp snooping 128
17.22 show ip igmp snooping interface 128
17.23 show ip igmp snooping vlan 129
17.24 show ip igmp snooping groups 130
17.25 show ip igmp profile 131

Chapter 18 MLD Snooping Commands 132

18.1 ipv6 mld snooping (global) 132
18.2 ipv6 mld snooping drop-unknown 132
18.3 ipv6 mld snooping vlan-config 133
18.4 ipv6 mld snooping vlan-config (immediate-leave) 134
18.5 ipv6 mld snooping vlan-config (report-suppression) 135
18.6 ipv6 mld snooping vlan-config (router-ports-forbidden) 136
18.7 ipv6 mld snooping vlan-config (rport interface) 137
18.8 ipv6 mld snooping vlan-config (static) 137
18.9 ipv6 mld snooping vlan-config (querier) 138
18.10 ipv6 mld snooping (interface) 140
18.11 ipv6 mld snooping max-groups 140
18.12 ipv6 mld snooping immediate-leave 141
18.13 ipv6 mld profile 142
18.14 deny 143
18.15 permit 143
18.16 range 144
18.17 ipv6 mld filter 144
18.18 clear ipv6 mld snooping statistics 145
18.19 show ipv6 mld snooping 145
18.20 show ipv6 mld snooping interface 146
18.21 show ipv6 mld snooping vlan 147
18.22 show ipv6 mld snooping groups 147
18.23 show ipv6 mld profile 148

Chapter 19 MVR Commands 149

19.1 mvr (global) 149
19.2 mvr group 149

19.3 mvr mode 150
19.4 mvr querytime 151
19.5 mvr vlan 152
19.6 mvr (interface) 152
19.7 mvr type 153
19.8 mvr immediate 154
19.9 mvr vlan (group) 154
19.10 show mvr 155
19.11 show mvr interface 156
19.12 show mvr members 156
19.13 show mvr traffic 157

Chapter 20 MSTP Commands 158

20.1 debug spanning-tree 158
20.2 spanning-tree (global) 159
20.3 spanning-tree (interface) 159
20.4 spanning-tree common-config 160
20.5 spanning-tree mode 161
20.6 spanning-tree mst configuration 162
20.7 instance 162
20.8 name 163
20.9 revision 164
20.10 spanning-tree mst instance 165
20.11 spanning-tree mst 165
20.12 spanning-tree priority 166
20.13 spanning-tree timer 167
20.14 spanning-tree hold-count 168
20.15 spanning-tree max-hops 168
20.16 spanning-tree bpdufilter 169
20.17 spanning-tree bpduflood 170
20.18 spanning-tree bpduguard 170
20.19 spanning-tree guard loop 171
20.20 spanning-tree guard root 172
20.21 spanning-tree guard tc 172
20.22 spanning-tree mcheck 173
20.23 show spanning-tree active 173
20.24 show spanning-tree bridge 174
20.25 show spanning-tree interface 174

20.26 show spanning-tree interface-security 175
20.27 show spanning-tree mst 176

Chapter 21 LLDP Commands 178

21.1 lldp 178
21.2 lldp forward_message 178
21.3 lldp hold-multiplier 179
21.4 lldp timer 180
21.5 lldp receive 181
21.6 lldp transmit 181
21.7 lldp snmp-trap 182
21.8 lldp tlv-select 183
21.9 lldp management-address 183
21.10 lldp med-fast-count 184
21.11 lldp med-status 185
21.12 lldp med-tlv-select 185
21.13 lldp med-location 186
21.14 show lldp 187
21.15 show lldp interface 187
21.16 show lldp local-information interface 188
21.17 show lldp neighbor-information interface 189
21.18 show lldp traffic interface 189

Chapter 22 Static Routes Commands 191

22.1 ip routing 191
22.2 interface vlan 191
22.3 interface loopback 192
22.4 switchport 192
22.5 interface range port-channel 193
22.6 description 194
22.7 shutdown 194
22.8 interface port-channel 195
22.9 ip route 196
22.10 ipv6 routing 196
22.11 ipv6 route 197
22.12 show interface vlan 198
22.13 show ip interface 198
22.14 show ip interface brief 199

22.15 show ip route 199
22.16 show ip route specify 200
22.17 show ip route summary 201
22.18 show ipv6 interface 201
22.19 show ipv6 route 202
22.20 show ipv6 route summary 202

Chapter 23 IPv6 Address Configuration Commands 204

23.1 ipv6 enable 204
23.2 ipv6 address autoconfig 204
23.3 ipv6 address link-local 205
23.4 ipv6 address dhcp 206
23.5 ipv6 address ra 206
23.6 ipv6 address eui-64 207
23.7 ipv6 address 208
23.8 show ipv6 interface 209

Chapter 24 ARP Commands 210

24.1 arp 210
24.2 clear arp-cache 211
24.3 arp dynamicrenew 211
24.4 arp timeout 212
24.5 gratuitous-arp intf-status-up enable 212
24.6 gratuitous-arp dup-ip-detected enable 213
24.7 gratuitous-arp learning enable 213
24.8 gratuitous-arp send-interval 214
24.9 ip proxy-arp 215
24.10 ip local-proxy-arp 215
24.11 show arp 216
24.12 show ip arp (interface) 217
24.13 show ip arp summary 217
24.14 show gratuitous-arp 218
24.15 show ip proxy-arp 218

Chapter 25 DHCP Server Commands 220

25.1 service dhcp server 220
25.2 ip dhcp server extend-option capwap-ac-ip 220
25.3 ip dhcp server extend-option vendor-class-id 221
25.4 ip dhcp server exclude-address 222

25.5 ip dhcp server pool 222
25.6 ip dhcp server ping timeout 223
25.7 ip dhcp server ping packets 224
25.8 network 224
25.9 lease 225
25.10 address hardware-address 226
25.11 address client-identifier 226
25.12 default-gateway 227
25.13 dns-server 228
25.14 netbios-name-server 229
25.15 netbios-node-type 229
25.16 next-server 230
25.17 domain-name 231
25.18 bootfile 231
25.19 show ip dhcp server status 232
25.20 show ip dhcp server statistics 232
25.21 show ip dhcp server extend-option 233
25.22 show ip dhcp server pool 233
25.23 show ip dhcp server excluded-address 234
25.24 show ip dhcp server manual-binding 234
25.25 show ip dhcp server binding 235
25.26 clear ip dhcp server statistics 235
25.27 clear ip dhcp server binding 236

Chapter 26 DHCP Relay Commands 237

26.1 service dhcp relay 237
26.2 ip dhcp relay hops 237
26.3 ip dhcp relay time 238
26.4 ip helper-address 239
26.5 ip dhcp relay information 239
26.6 ip dhcp relay information strategy 240
26.7 ip dhcp relay information format 241
26.8 ip dhcp relay information circuit-id 242
26.9 ip dhcp relay information remote-id 242
26.10 ip dhcp relay default-interface 243
26.11 ip dhcp relay vlan 244
26.12 show ip dhcp relay 244

Chapter 27 DHCP L2 Relay Commands 246

27.1 ip dhcp l2relay 246
27.2 ip dhcp l2relay vlan 246
27.3 ip dhcp l2relay information 247
27.4 ip dhcp l2relay information strategy 247
27.5 ip dhcp l2relay information format 248
27.6 ip dhcp l2relay information circuit-id 249
27.7 ip dhcp l2relay information remote-id 250
27.8 show ip dhcp l2relay 250
27.9 show ip dhcp l2relay interface 251

Chapter 28 QoS Commands 252

28.1 qos trust mode 252
28.2 qos port-priority 253
28.3 qos cos-map 253
28.4 qos dot1p-remap 254
28.5 qos dscp-map 255
28.6 qos dscp-remap 256
28.7 qos queue bandwidth 256
28.8 qos queue mode 257
28.9 show qos cos-map 258
28.10 show qos dot1p-remap 259
28.11 show qos dscp-map 259
28.12 show qos dscp-remap 260
28.13 show qos port-priority interface 260
28.14 show qos trust interface 261
28.15 show qos queue interface 261

Chapter 29 Bandwidth Control Commands 263

29.1 storm-control rate-mode 263
29.2 storm-control 264
29.3 storm-control exceed 265
29.4 storm-control recover 265
29.5 bandwidth 266
29.6 show storm-control 267
29.7 show bandwidth 267

Chapter 30 Voice VLAN Commands 269

30.1 voice vlan 269
30.2 voice vlan (interface) 269
30.3 voice vlan priority 270
30.4 voice vlan oui 271
30.5 show voice vlan 271
30.6 show voice vlan oui-table 272
30.7 show voice vlan interface 272

Chapter 31 Auto VoIP Commands 274

31.1 auto-voip 274
31.2 auto-voip (interface) 274
31.3 auto-voip dot1p 275
31.4 auto-voip untagged 276
31.5 auto-voip none 276
31.6 no auto-voip (interface) 277
31.7 auto-voip dscp 277
31.8 auto-voip data priority 278
31.9 show auto-voip 278

Chapter 32 Access Control Commands 280

32.1 user access-control ip-based enable 280
32.2 user access-control ip-based 280
32.3 user access-control mac-based enable 281
32.4 user access-control mac-based 282
32.5 user access-control port-based enable 283
32.6 user access-control port-based 283

Chapter 33 HTTP and HTTPS Commands 285

33.1 ip http server 285
33.2 ip http port 285
33.3 ip http max-users 286
33.4 ip http session timeout 287
33.5 ip http secure-server 288
33.6 ip http secure-port 288
33.7 ip http secure-protocol 289
33.8 ip http secure-ciphersuite 290
33.9 ip http secure-max-users 290

33.10 ip http secure-session timeout 291
33.11 ip http secure-server download certificate 292
33.12 ip http secure-server download key 293
33.13 show ip http configuration 294
33.14 show ip http secure-server 294

Chapter 34 SSH Commands 296

34.1 ip ssh server 296
34.2 ip ssh port 296
34.3 ip ssh version 297
34.4 ip ssh algorithm 298
34.5 ip ssh timeout 298
34.6 ip ssh max-client 299
34.7 ip ssh download 300
34.8 remove public-key 300
34.9 show ip ssh 301

Chapter 35 Telnet Commands 302

35.1 telnet enable 302
35.2 telnet port 302
35.3 show telnet-status 303

Chapter 36 AAA Commands 304

36.1 tacacas-server host 304
36.2 show tacacs-server 305
36.3 radius-server host 306
36.4 show radius-server 307
36.5 aaa group 308
36.6 server 309
36.7 show aaa group 309
36.8 aaa authentication login 310
36.9 aaa authentication enable 311
36.10 aaa authentication dot1x default 312
36.11 aaa accounting dot1x default 313
36.12 show aaa authentication 313
36.13 show aaa accounting 314
36.14 line telnet 314
36.15 login authentication (telnet) 315
36.16 line ssh 316

36.17 login authentication (ssh) 316
36.18 enable authentication (telnet) 317
36.19 enable authentication (ssh) 318
36.20 ip http login authentication 318
36.21 ip http enable authentication 319
36.22 show aaa global 320
36.23 enable-admin 320

Chapter 37 IEEE 802.1x Commands 322

37.1 dot1x system-auth-control 322
37.2 dot1x handshake 323
37.3 dot1x auth-protocol 323
37.4 dot1x vlan-assignment 324
37.5 dot1x accounting 325
37.6 dot1x mab 326
37.7 dot1x guest-vlan 326
37.8 dot1x timeout quiet-period 327
37.9 dot1x timeout supp-timeout 328
37.10 dot1x max- req 329
37.11 dot1x 329
37.12 dot1x port-control 330
37.13 dot1x port-method 331
37.14 dot1x auth-init 332
37.15 dot1x auth-reauth 332
37.16 show dot1x global 333
37.17 show dot1x interface 334
37.18 show dot1x auth-state interface 334

Chapter 38 Port Security Commands 336

38.1 mac address-table max-mac count 336
38.2 show mac address-table max-mac-count 336

Chapter 39 Port Mirroring Commands 338

39.1 monitor session destination interface 338
39.2 monitor session source 339
39.3 show monitor session 340

Chapter 40 ACL Commands 342

40.1 access-list create 342

40.2 access-list resequence 342
40.3 access-list mac 343
40.4 access-list ip 345
40.5 access-list combined 347
40.6 access-list ipv6 349
40.7 access-list action 350
40.8 redirect interface 351
40.9 s-condition 352
40.10 s-mirror 353
40.11 qos-remark 353
40.12 access bind 354
40.13 show access-list 355
40.14 show access-list bind 356
40.15 show access-list status 356
40.16 show access-list counter 356
40.17 clear access-list 357

Chapter 41 IPv4 IMPB Commands 358

41.1 ip source binding 358
41.2 ip dhcp snooping 359
41.3 ip dhcp snooping vlan 360
41.4 ip dhcp snooping max-entries 360
41.5 show ip source binding 361
41.6 show ip dhcp snooping 362
41.7 show ip dhcp snooping interface 362

Chapter 42 IPv6 IMPB Commands 364

42.1 Ipv6 source binding 364
42.2 ipv6 dhcp snooping 365
42.3 ipv6 dhcp snooping vlan 366
42.4 ipv6 dhcp snooping max-entries 366
42.5 ipv6 nd snooping 367
42.6 ipv6 nd snooping vlan 368
42.7 ipv6 nd snooping max-entries 368
42.8 show ipv6 source binding 369
42.9 show ipv6 dhcp snooping 370
42.10 show ipv6 dhcp snooping interface 370
42.11 show ipv6 nd snooping 371

Chapter 43 IP Verify Source Commands 372

43.1 ip verify source 372
43.2 ip verify source logging 373
43.3 show ip verify source 373
43.4 show ip verify source interface 374

Chapter 44 IPv6 Verify Source Commands 375

44.1 ipv6 verify source 375
44.2 show ipv6 verify source 376
44.3 show ipv6 verify source interface 376

Chapter 45 DHCPv4 Filter Commands 378

45.1 ip dhcp filter 378
45.2 ip dhcp filter (interface) 378
45.3 ip dhcp filter mac-verify 379
45.4 ip dhcp filter limit rate 380
45.5 ip dhcp filter decline rate 381
45.6 ip dhcp filter server permit-entry 381
45.7 show ip dhcp filter 382
45.8 show ip dhcp filter interface 383
45.9 show ip dhcp filter server permit-entry 383

Chapter 46 DHCPv6 Filter Commands 385

46.1 ipv6 dhcp filter 385
46.2 ipv6 dhcp filter (interface) 385
46.3 ipv6 dhcp filter limit rate 386
46.4 ipv6 dhcp filter decline rate 387
46.5 ipv6 dhcp filter server permit-entry 388
46.6 show ipv6 dhcp filter 389
46.7 show ipv6 dhcp filter interface 389
46.8 show ip dhcp filter server permit-entry 390

Chapter 47 DoS Defend Commands 391

47.1 ip dos-prevent 391
47.2 ip dos-prevent type 391
47.3 show ip dos-prevent 393

Chapter 48 DLDP Commands 395

48.1 dldp (global) 395

48.2 dldp interval 395
48.3 dldp shut-mode 396
48.4 dldp(interface) 397
48.5 show dldp 397
48.6 show dldp interface 398

Chapter 49 SNMP Commands 399

49.1 snmp-server 399
49.2 snmp-server view 399
49.3 snmp-server group 400
49.4 snmp-server user 402
49.5 snmp-server community 403
49.6 snmp-server host 404
49.7 snmp-server engineID 406
49.8 snmp-server traps snmp 406
49.9 snmp-server traps 407
49.10 snmp-server traps ddm 409
49.11 snmp-server traps vlan 410
49.12 snmp-server traps security 411
49.13 snmp-server traps acl 412
49.14 snmp-server traps ip 412
49.15 snmp-server traps link-status 413
49.16 rmon history 413
49.17 rmon event 414
49.18 rmon alarm 415
49.19 rmon statistics 417
49.20 show snmp-server 418
49.21 show snmp-server view 418
49.22 show snmp-server group 419
49.23 show snmp-server user 419
49.24 show snmp-server community 420
49.25 show snmp-server host 420
49.26 show snmp-server engineID 420
49.27 show rmon history 421
49.28 show rmon event 421
49.29 show rmon alarm 422
49.30 show rmon statistics 423

Chapter 50 ARP Inspection Commands 424

50.1 ip arp inspection 424
50.2 ip arp inspection validate 424
50.3 ip arp inspection vlan 425
50.4 ip arp inspection vlan logging 426
50.5 ip arp inspection trust 427
50.6 ip arp inspection limit-rate 427
50.7 ip arp inspection burst-interval 428
50.8 ip arp inspection recover 429
50.9 show ip arp inspection 429
50.10 show ip arp inspection interface 430
50.11 show ip arp inspection vlan 431
50.12 show ip arp inspection statistics 431
50.13 clear ip arp inspection statistics 432

Chapter 51 ND Detection Commands 433

51.1 ipv6 nd detection 433
51.2 ipv6 nd detection vlan 433
51.3 ipv6 nd detection vlan logging 434
51.4 ipv6 nd detection trust 434
51.5 show ipv6 nd detection 435
51.6 show ipv6 nd detection interface 435
51.7 show ipv6 nd detection vlan 436

Chapter 52 System Log Commands 437

52.1 logging buffer 437
52.2 logging buffer level 437
52.3 logging file flash 438
52.4 logging file flash frequency 439
52.5 logging file flash level 440
52.6 logging host index 440
52.7 logging console 441
52.8 logging console level 442
52.9 logging monitor 443
52.10 logging monitor level 443
52.11 clear logging 444
52.12 show logging local-config 445
52.13 show logging loghost 445

52.14 show logging buffer 446
52.15 show logging flash 446

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 T1700X-16TS without any explanation. The commands in this guide apply to these models if not specially noted.
Some models featured in this guide may be unavailable in your country or region. For local sales information, visit https://www.tp-link.com.

Overview of this Guide

Chapter 1: Using the CLI

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

Chapter 2: User Interface

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

Chapter 3: User Management Commands

Provide information about the commands used for user management.

Chapter 4: 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 5: EEE Configuration Commands

Provide information about the commands used for configuring EEE.

Chapter 6: SDM Template Commands

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

Chapter 7: Time Range Commands

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

Chapter 8: Port Configuration Commands

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

Chapter 9: Port Isolation Commands

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

Chapter 10: Loopback Detection Commands

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

Chapter 11: Etherchannel Commands

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

Chapter 12: MAC Address Commands

Provide information about the commands used for Address configuration.

Chapter 13: IEEE 802.1Q VLAN Commands

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

Chapter 14: MAC-based VLAN Commands

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

Chapter 15: Protocol-based VLAN Commands

Provide information about the commands used for configuring Protocol VLAN.

Chapter 16: GVRP Commands

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

Chapter 17: IGMP Snooping Commands

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

Chapter 18: MLD Snooping Commands

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

Chapter 19: MVR Commands

Provide information about the commands used for configuring the MVR.

Chapter 20: MSTP Commands

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

Chapter 21: LLDP Commands

Provide information about the commands used for configuring LLDP function.

Chapter 22: Static Routes Commands

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

Chapter 23: IPv6 Address Configuration Commands

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

Chapter 24: ARP Commands

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

Chapter 25: DHCP Server Commands

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

Chapter 26: DHCP Relay Commands

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

Chapter 27: DHCP L2 Relay Commands

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

Chapter 28: QoS Commands

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

Chapter 29: Bandwidth Commands

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

Chapter 30: Voice VLAN Commands

Provide information about the commands used for configuring Voice VLAN.

Chapter 31 Auto VoIP Commands

Provide information about the commands used for configuring Auto VoIP.

Chapter 32: Access Control Commands

Provide information about the commands used for configuring Access Control.

Chapter 33: HTTP and HTTPS Commands

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

Chapter 34: SSH Commands

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

Chapter 35: Telnet Commands

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

Chapter 36: AAA Commands

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

Chapter 37: IEEE 802.1X Commands

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

Chapter 38 Port Security Commands

Provide information about the commands used for configuring Port Security.

Chapter 39: Port Mirroring Commands

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

Chapter 40: ACL Commands

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

Chapter 41: IPv4 IMPB Commands

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

Chapter 42: IPv6 IMPB Commands

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

Chapter 43: IP Verify Source Commands

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

Chapter 44: IPv6 Verify Source Commands

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

Chapter 45: DHCPv4 Filter Commands

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

Chapter 46: DHCPv6 Filter Commands

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

Chapter 47: DoS Defend Command

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

Chapter 48: DLDP Commands

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

Chapter 49: SNMP Commands

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

Chapter 50: ARP Inspection Commands

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

Chapter 51: ND Detection Commands

Provide information about the commands used for configuring ND detection.

Chapter 52: System Log Commands

Provide information about the commands used for configuring system log.

Chapter 1 Using the CLI

1.1 Accessing the CLI

You can log on to the switch and access the CLI by logging on to the switch remotely by a Telnet or SSH connection through an Ethernet port.

1.1.1 Logon by Telnet

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

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

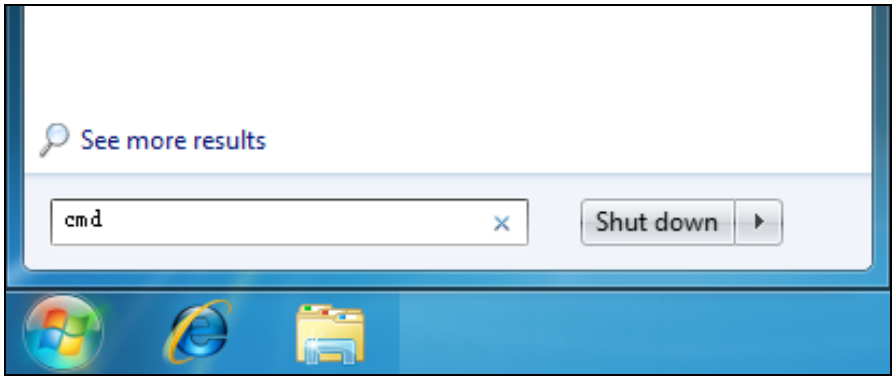

Figure 1-1 Run Window

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

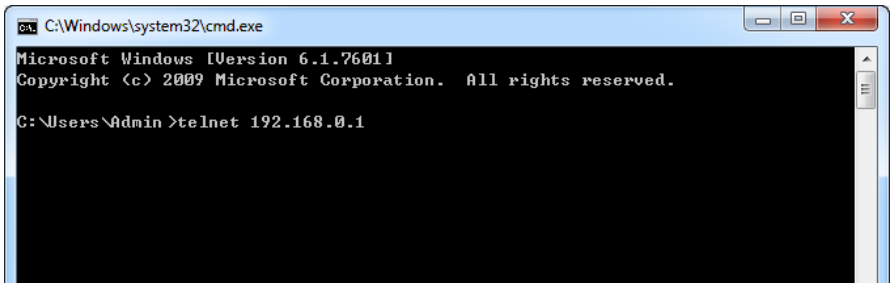

Figure 1-2 Type in the telnet command

3. Type in the login username and password (both **admin** by default). Press **Enter** and you will enter User EXEC Mode.

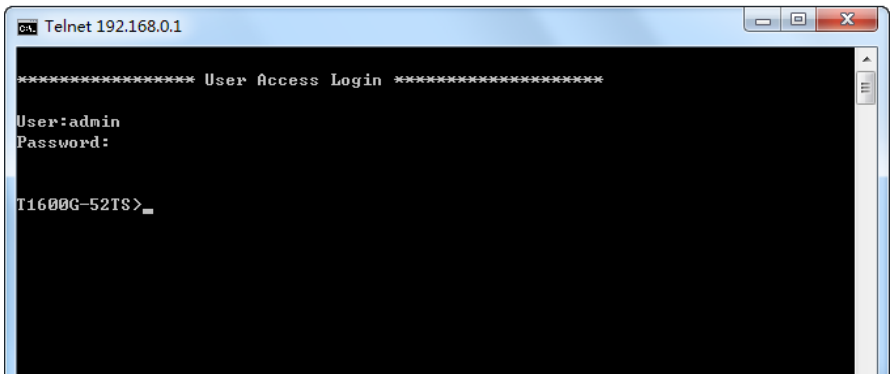

Figure 1-2 Log in the Switch

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

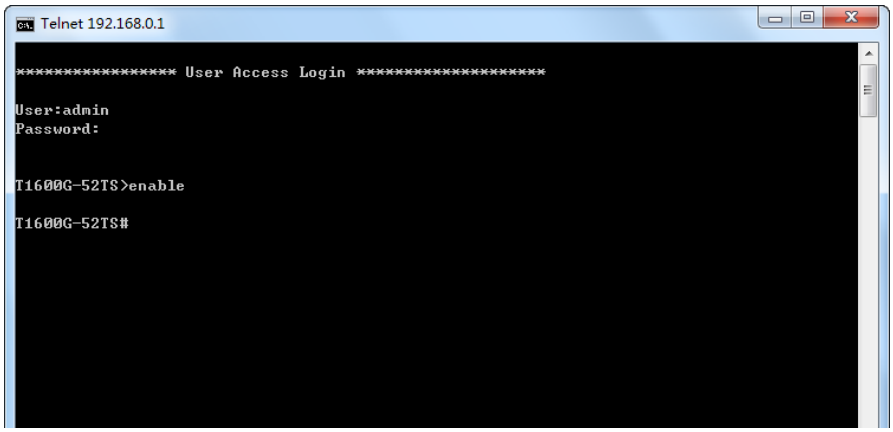

Figure 1-3 Enter into Priviledged EXEC Mode

1.1.2 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 1-4 to enable the SSH function through Telnet connection.

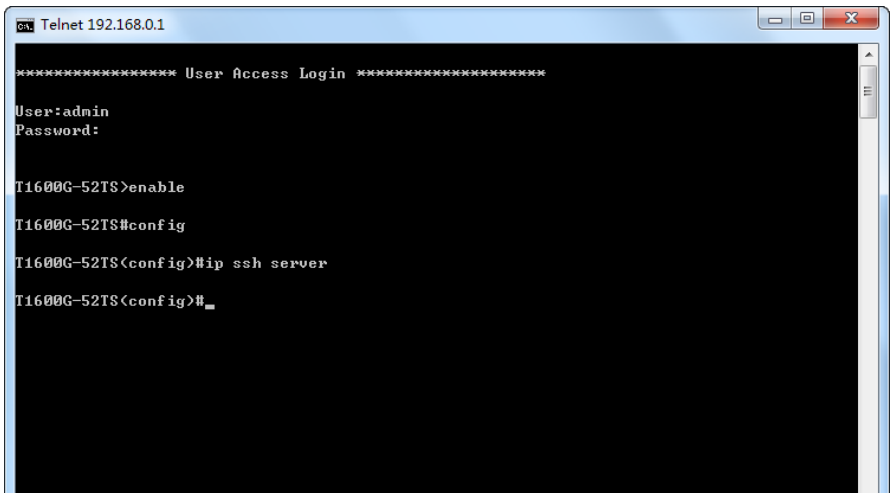

Figure 1-4 Enable SSH function

- **Password Authentication Mode**

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

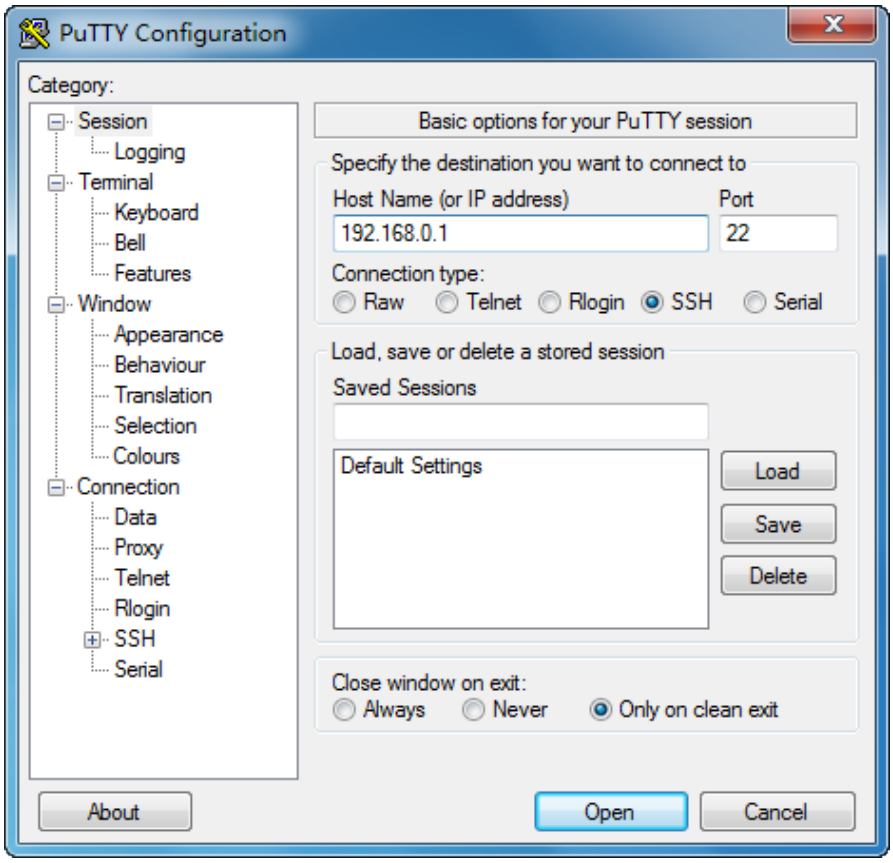

Figure 1-5 SSH Connection Config

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

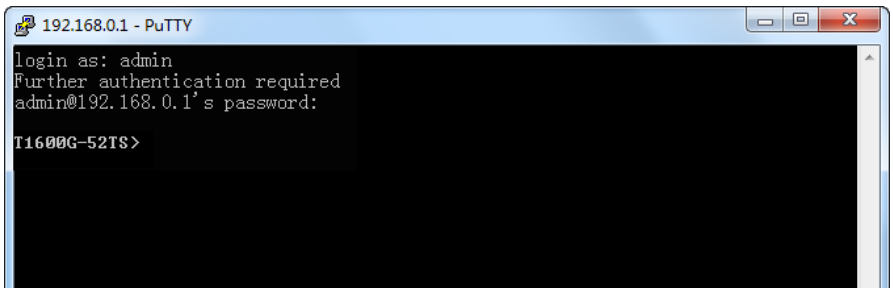

Figure 1-6 Log on the Switch

- **Key Authentication Mode**

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

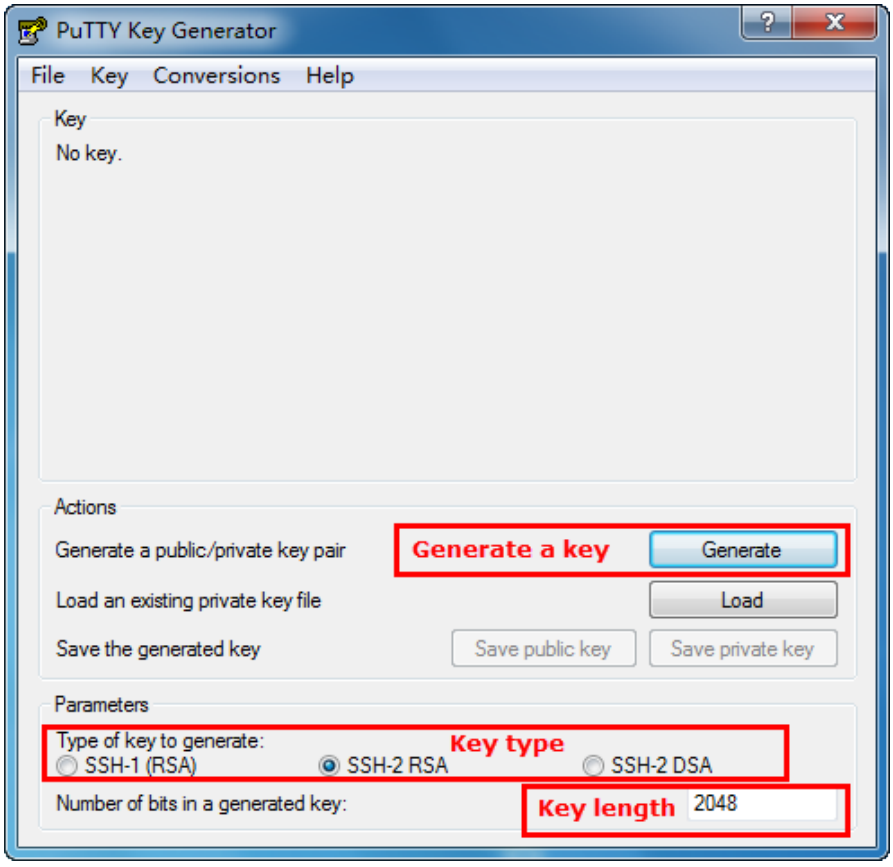

Figure 1-7 Generate SSH Key

Note:

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

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

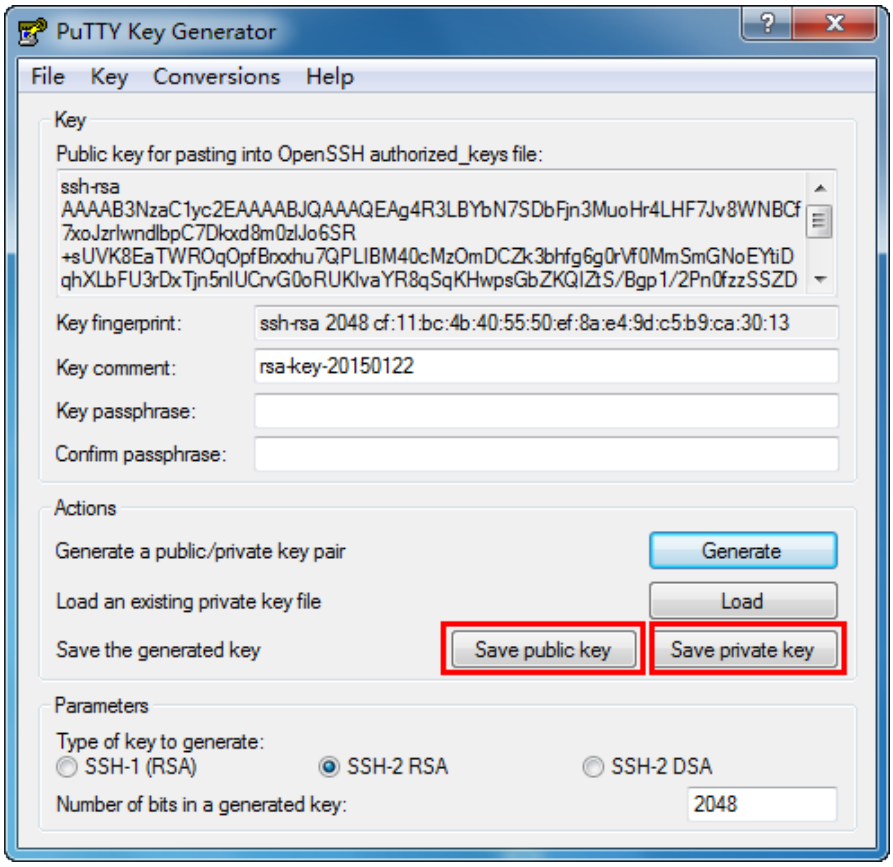

Figure 1-8 Save the Generated Key

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:

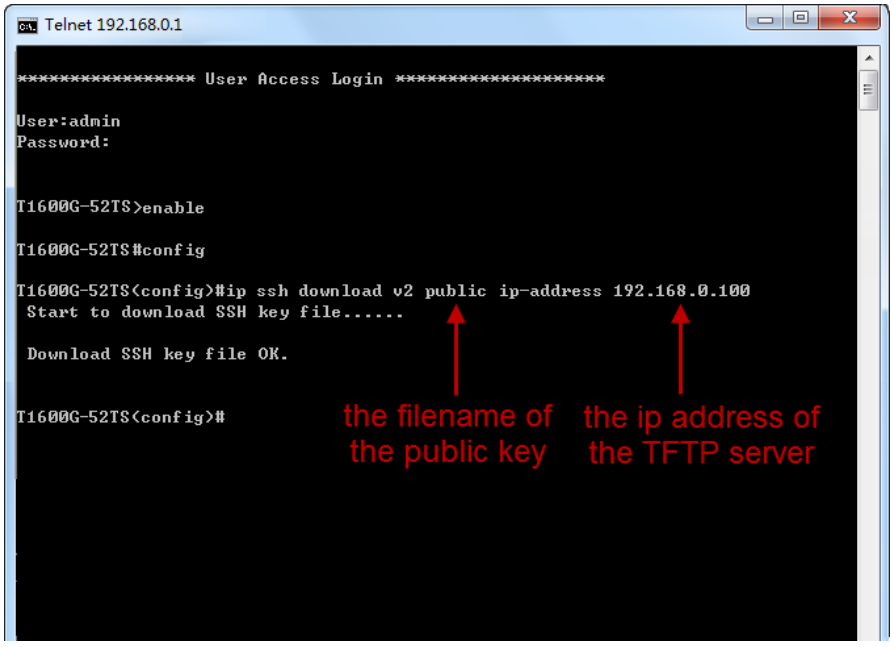

Figure 1-9 Download the Public Key

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.

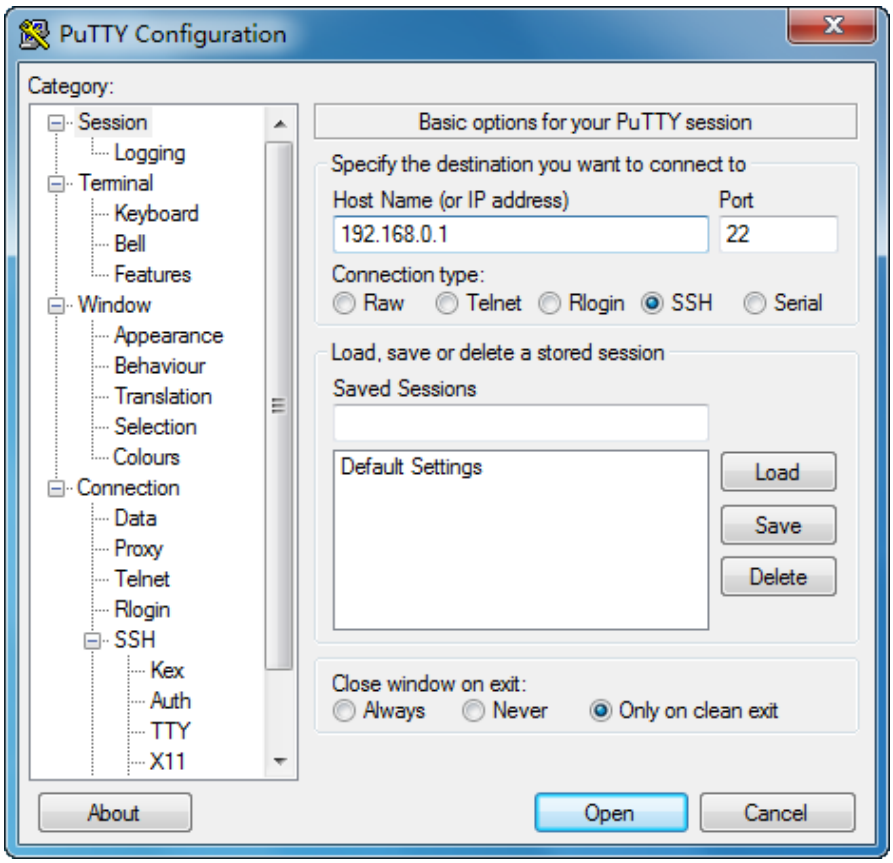

Figure 1-10 SSH Connection Config

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

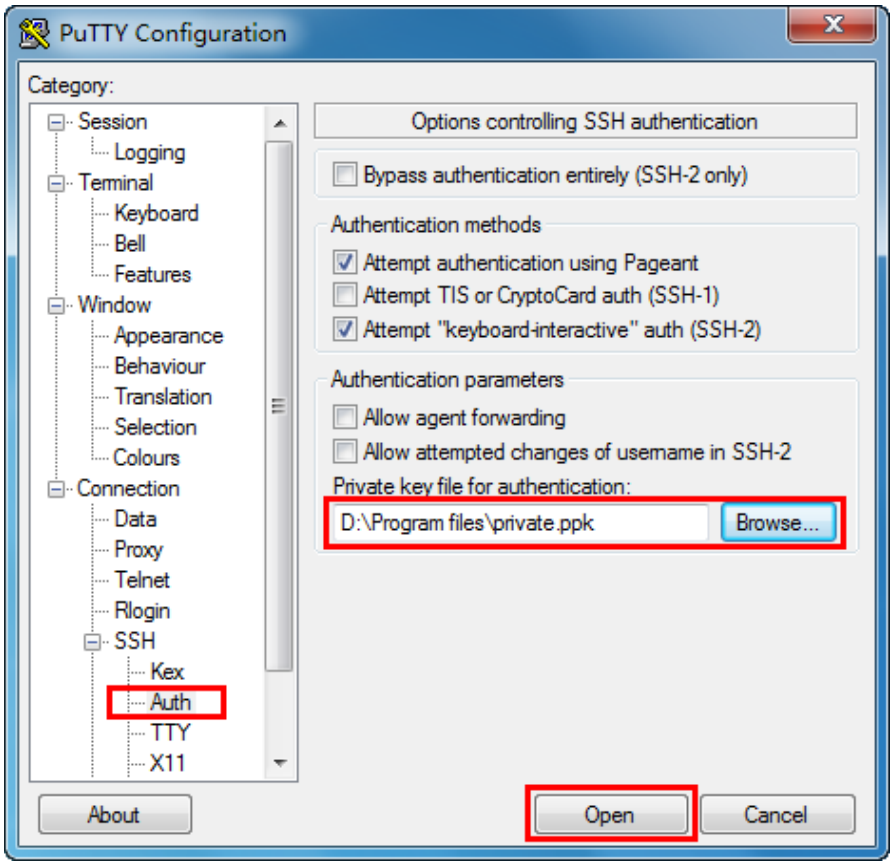

Figure 1-11 Download the Private Key

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.

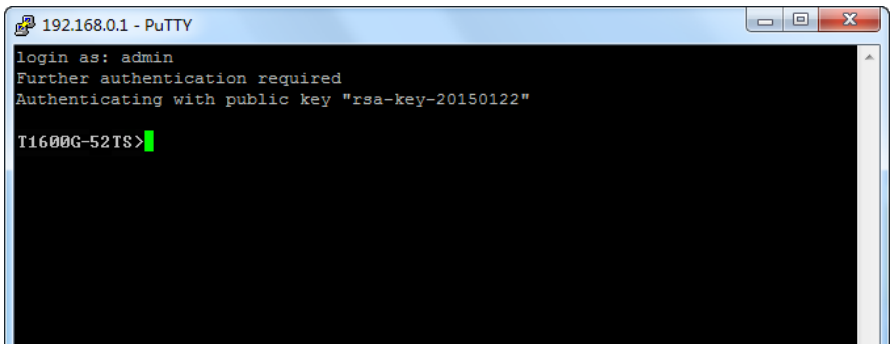

Figure 1-12 Log on the Switch

1.2 CLI Command Modes

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

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

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

Mode	Accessing Path	Prompt	Logout or Access the next mode
User EXEC Mode	Primary mode once it is connected with the switch.	**T1700X-16TS>**	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.	**T1700X-16TS#**	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.	**T1700X-16TS(config)#**	Use the **exit** or the **end** command or press **Ctrl+Z** to return to Privileged EXEC mode. Use the **interface ten-gigabitEthernet** *port* or **interface range ten-gigabitEthernet** *port-list* command to access interface Configuration mode. Use the **vlan** *vlan-list* to access VLAN Configuration mode.
Interface Configuration Mode	Layer 2 Interface: Use the **interface ten-gigabitEthernet** *port,* **interface port-channel** *port-channel-id* or **interface range ten-gigabitEthernet** *port-list* command to enter this mode from Global Configuration mode.	**T1700X-16TS (config-if)#** or **T1700X-16TS(config-if-range)#**	Use the **end** command or press **Ctrl+Z** to return to Privileged EXEC mode. Enter the **exit** or the **#** command to return to Global Configuration mode. A port number must be specified in the **interface** command.

Mode	Accessing Path	Prompt	Logout or Access the next mode
Interface Configuration Mode	Layer 3 Interface: Use the **no switchport** command to enter Routed Port mode from Interface Configuration mode. Use the **interface vlan** *vlan-id* command to enter VLAN Interface mode from Global Configuration mode. Use the **interface loopback** *id* command to enter Loopback Interface mode from Global Configuration mode.	**T1700X-16TS (config-if)#** or **T1700X-16TS(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** *vlan-list* command to enter this mode from Global Configuration mode.	**T1700X-16TS (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 ten-gigabitEthernet: Configure parameters for an Ethernet port, such as Duplex-mode, flow control status.
  b). Interface range ten-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.
- **history**: Display the commands history..

1.3 Privilege Restrictions

This switch's security is divided into four privilege levels: User level, Power User level, Operator level and Admin level. You can define username and password pairs, and assign a specific privilege level to each pair. Different privilege levels have access to specified commands, which is illustrated in the **Privilege Requirement** in each command. For details about how to configure usename 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 " < > , \ & cannot be input.
- If a blank is contained in a character string, single or double quotation marks should be used, for example 'hello world', "hello world", and the words in the quotation marks will be identified as a string. Otherwise, the words will be identified as several strings.

1.4.3 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:

```
T1700X-16TS>enable
Enter password:
T1700X-16TS#
```

2.2 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:

```
T1700X-16TS(config)# service password-encryption
```

2.3 enable password

Description

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

Syntax

enable password { [0] *password* | 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:

```
T1700X-16TS(config)#enable password 0 admin
```

2.4 enable secret

Description

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

Syntax

enable secret { [0] *password* **|** 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.

T1700X-16TS(config)#enable secret 0 admin

2.5 configure

Description

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

Syntax

configure

Command Mode

Privileged EXEC Mode

Privilege Requirement

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

Example

Access Global Configuration Mode from Privileged EXEC Mode:

T1700X-16TS# configure
T1700X-16TS(config)#

2.6 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:

```
T1700X-16TS(config-if)# exit
T1700X-16TS(config)#exit
T1700X-16TS#
```

2.7 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:

```
T1700X-16TS(config-if)#end
T1700X-16TS#
```

2.8 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:

```
T1700X-16TS(config)#no clipaging
```

2.9 history

Description

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

Syntax

history

Command Mode

Privileged EXEC Mode and any Configuration Mode

Privilege Requirement

None.

Example

Show the commands you have entered in the current mode:

```
T1700X-16TS (config)# history

    1 history
```

2.10 history clear

Description

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

Syntax

history clear

Command Mode

Privileged EXEC Mode and any Configuration Mode

Privilege Requirement

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

Example

Clear the commands you have entered in the current mode:

```
T1700X-16TS(config)#history clear
```

Chapter 3 User Management Commands

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

3.1 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:

T1700X-16TS(config)#user name tplink **privilege** admin **password** 0 admin

3.2 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.

T1700X-16TS(config)#user name tplink **privilege** admin **secret** 0 admin

3.3 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:

```
T1700X-16TS(config)# show user account-list
```

3.4 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:

```
T1700X-16TS(config)# show user configuration
```

Chapter 4 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.

4.1 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

T1700X-16TS(config)# system-time manual 12/20/2010-17:30:35

4.2 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 Novosibrisk, 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, Welington.

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:

T1700X-16TS(config)# system-time ntp UTC-12:00 133.100.9.2 139.79.100.163 11

4.3 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:

T1700X-16TS(config)#system-time dst predefined USA

4.4 system-time dst date

Description

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

Syntax

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

no system-time dst

Parameter

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

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

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

syear —— The start year of the daylight saving time.

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

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

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

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

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

T1700X-16TS(config)# system-time dst date Apr 1 00:00 2015 Oct 1 00:00 2015 30

4.5 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*} {*eweek*} {*eday*} {*emonth*} {*etime*} [*offset*]

no system-time dst

Parameter

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

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

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

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

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

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

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

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

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

T1700X-16TS(config)# system-time dst recurring first Sun May 02:00 last Sun Oct 02:00 45

4.6 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 “T1700X-16TS”.

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:

T1700X-16TS(config)# hostname TPLINK

4.7 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:

T1700X-16TS(config)# location SHENZHEN

4.8 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:

T1700X-16TS(config)# contact-info www.tp-link.com

4.9 ip address

Description

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

Syntax

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

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

Parameter

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

mask —— The subnet mask of the Layer 3 interface.

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

Command Mode

Interface Configuration Mode

Privilege Requirement

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

Example

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

T1700X-16TS(config)# interface vlan 2

T1700X-16TS(config-if)# ip address 192.168.1.1 255.255.255.0

T1700X-16TS(config-if)# ip address 192.168.2.1 255.255.255.0 **secondary**

4.10 ip address-alloc

Description

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

Syntax

ip address-alloc { dhcp | bootp }

no ip address

Parameter

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

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

Command Mode

Interface Configuration Mode

Privilege Requirement

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

Example

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

T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/1

T1700X-16TS(config-if)# no switchport

T1700X-16TS(config-if)# ip address-alloc dhcp

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

T1700X-16TS(config)# interface vlan 2

T1700X-16TS(config-if)# no ip address

4.11 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:

```
T1700X-16TS# reset
```

4.12 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:

```
T1700X-16TS# reboot
```

4.13 reboot-schedule

Description

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

Syntax

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

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

reboot-schedule cancel

Parameter

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

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

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

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

cancel —— Delete the reboot schedule settings.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

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

Example

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

T1700X-16TS(config)# reboot-schedule in 200 **save_before_reboot**

4.14 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:

```
T1700X-16TS# copy running-config startup-config
```

4.15 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:

T1700X-16TS# 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:

T1700X-16TS# copy startup-config tftp ip-address fe80::1234 **filename** config

4.16 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:

T1700X-16TS# 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

T1700X-16TS# copy tftp startup-config ip-address fe80::1234 **filename** config

4.17 copy backup-config tftp

Description

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

Syntax

copy backup-config tftp ip-address *ip-addr* **filename** *name*

Parameter

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

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

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Export the backup configuration file of the switch to the TFTP server with the IP 192.168.0.148 and name the file config.cfg:

T1700X-16TS# copy backup-config tftp ip-address 192.168.0.148 **filename** config

4.18 copy backup-config startup-config

Description

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

Syntax

copy backup-config startup-config

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

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

```
T1700X-16TS# copy backup-config startup-config
```

4.19 copy running-config backup-config

Description

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

Syntax

copy running-config backup-config

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Save the current running configuration as the backup configuration file.

```
T1700X-16TS# copy running-config backup-config
```

4.20 copy tftp backup-config

Description

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

Syntax

Copy tftp backup-config ip-address *ip-addr* **filename** *name*

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 config.cfg from the TFTP server with the IP 192.168.0.148:

T1700X-16TS# copy tftp backup-config ip-address 192.168.0.148 **filename** config

4.21 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:

T1700X-16TS(config)# boot application filename image2 startup

4.22 boot config

Description

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

Syntax

boot config filename { config1 | config 2 } { startup | backup }

no boot application

Parameter

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

startup | backup—— Specify the property of the configuration.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the config2.cfg as the startup image:

T1700X-16TS(config)# boot config filename config2 startup

4.23 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:

```
T1700X-16TS# remove backup-image
```

4.24 firmware upgrade

Description

The **firmware upgrade** command is used to upgrade the switch's backup iamge 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 iamge 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:

```
T1700X-16TS# 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 iamge file with the file firmware.bin in the TFTP server with the IP address fe80::1234, but do not reboot the switch:

T1700X-16TS# 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

4.25 ping

Description

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

Syntax

ping [ip | ipv6] { *ip_addr* } [**-n** *count*] [**-l** *size*] [**-i** *interval*]

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

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

Command Mode

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:

T1700X-16TS# ping 192.168.0.131 **–n** 8 **–l** 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:

T1700X-16TS# ping fe80::1234 **–n** 8 **–l** 512

4.26 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

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:

T1700X-16TS# 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:

T1700X-16TS# tracert fe80::1234 20

4.27 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:

T1700X-16TS# show system-info

4.28 show image-info

Description

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

Syntax

show image-info

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the system image files' information:

```
T1700X-16TS# show image-info
```

4.29 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:

```
T1700X-16TS# show boot
```

4.30 show running-config

Description

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

Syntax

show running-config

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the system current operating configuration:

```
T1700X-16TS# show running-config
```

4.31 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:

```
T1700X-16TS# show startup-config
```

4.32 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

```
T1700X-16TS# show system-time
```

4.33 show system-time dst

Description

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

Syntax

show system-time dst

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DST information of the switch

```
T1700X-16TS# show system-time dst
```

4.34 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:

```
T1700X-16TS# show system-time ntp
```

4.35 show cable-diagnostics interface

Description

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

Syntax

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

Parameter

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

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Show the cable-diagnostics of port 3:

```
T1700X-16TS# show cable-diagnostics interface ten-gigabitEthernet 1/0/3
```

4.36 show cpu-utilization

Description

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

Syntax

show cpu-utilization

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the CPU utilization information of the switch:

```
T1700X-16TS# show cpu-utilization
```

4.37 show memory-utilization

Description

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

Syntax

show memory-utilization

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the memory utilization information of the switch:

```
T1700X-16TS# show memory-utilization
```

Chapter 5 EEE Configuration Commands

EEE (Energy Efficient Ethernet) is used to save power consumption of the switch during periods of low data activity. You can simply enable this feature on ports to allow power reduction.

5.1 eee

Description

The **eee** command is used to enable EEE on the port. To disable EEE on the port, please use **no eee** command.

Syntax

eee

no eee

Command Mode

Interface Configuration Mode

Privilege Requirement

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

Example

Enable EEE on port 1/0/1:

```
T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/1
T1700X-16TS(config-if)#eee
```

5.2 show interface eee

Description

The **show interface eee** command is used to display the EEE configuration on each port.

Syntax

show interface eee [fastEthernet *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port***]**

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the EEE configuration of each port

```
T1700X-16TS# show interface eee
```

Chapter 6 SDM Template Commands

This chapter describes how to configure the Switch Database Management (SDM) templates to allocate hardware resources on the switch for different uses.

6.1 sdm prefer

Description

The **sdm prefer** command is used to configure the SDM template. The SDM template is used to allocate system resources to best support the features being used in your application. To return to use the default template, please use the **sdm prefer default** command. The template change will takes effect after a reboot.

Syntax

sdm prefer { default | enterpriseV4 | enterpriseV6 }

Parameter

default —— Specify the SDM template used in the switch as "default".

enterpriseV4 —— Specify the SDM template used in the switch as "enterpriseV4".

enterpriseV6 —— Specify the SDM template used in the switch as "enterpriseV6".

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Specify the SDM template as enterpriseV4:

```
T1700X-16TS(config)# sdm prefer enterpriseV4
```

6.2 show sdm prefer

Description

The **show sdm prefer** command is used to display resource allocation of the current SDM template in use, or the SDM templates that can be used.

Syntax

show sdm prefer { used | default | enterpriseV4 | enterpriseV6 }

Parameter

used —— Display the resource allocation of the template currently in use, and the template that will become active after a reboot.

default —— Display the resource allocation of the default template.

enterpriseV4 —— Display the resource allocation of the enterpriseV4 template. enterpriseV6 —— Display the resource allocation of the enterpriseV6 template.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the resource allocation of the template currently in use, and the template that will become active after a reboot:

```
T1700X-16TS(config)#show sdm prefer used
```

Chapter 7 Time Range Commands

With this feature, you can configure a time range and bind it to an ACL rule.

7.1 time-range

Description

The **time-range** command is used to create time-range entry for the switch and enter Time-range Create Configuration Mode. After a time-range entry is created, you need to specify the date and time. A time-range can implement multiple time-ranges simultaneously as long as they do not conflict with each other. To delete the corresponding time-range configuration, please use **no time-range** command.

Syntax

time-range *name*

no time-range *name*

Command Mode

Global Configuration Mode

Parameter

name —— The time-range name, ranging from 1 to 16 characters.

Privilege Requirement

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

Example

Create a time-range named "tRange1" for the switch:

```
T1700X-16TS(config)# time-range tRange1
```

7.2 absolute

Description

The **absolute** command is used to create an absolute time-range for the time-range of the switch. To delete the corresponding absolute time-range configuration, please use **no absolute** command.

Syntax

absolute from *start-date* **to** *end-date*

no absolute [*index*]

Parameter

start-date —— The start date in Absoluteness Mode, in the format of MM/DD/YYYY.

end-date —— The end date in Absoluteness Mode, in the format of MM/DD/YYYY.

Command Mode

Time-range Create Configuration Mode

Privilege Requirement

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

Example

Create an absolute time-range for the switch and specify the date extending from May 5th, 2017 through Oct. 5th, 2017:

T1700X-16TS(config)#time-range tRange1

T1700X-16TS(config-time-range)#absolute from 05/05/2017 **to** 10/05/2017

7.3 periodic

Description

The **periodic** command is used to create a periodic mode time-range for the time-range of the switch. To delete the corresponding periodic mode time-range configuration, please use **no periodic** command.

Syntax

periodic { [**start** *start-time*] [**end** *end-time*] [**day-of-the-week** *week-day*]}

no periodic [*index*]

Parameter

start-time——Specify the start time in the format of HH:MM

end-time——Specify the end time in the format of HH:MM

week-day ——Specify the days of a week in the format of 1-3, 7. The numbers 1-7 respectively represent Monday, Tuesday, Wednesday, Thursday, Friday, Saturday and Sunday.

Command Mode

Time-range Create Configuration Mode

Privilege Requirement

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

Example

Configure the time-range named "tRange2" as a periodic time-range and specify the date and time as 8:30 to 12:00 on weekends:

T1700X-16TS(config)#time-range tRange2

T1700X-16TS(config -time-range)#periodic start 08:30 **end** 12:00

day-of-the-week 6-7

7.4 holiday (time-range mode)

Description

The **holiday** command is used to create holiday mode time-range for the time-range of the switch. When the holiday which is excluded from time-range occurs, the switch will not supply power.

Syntax

holiday { exclude | include }

Parameter

exclude ——The time range will not take effect on holiday.

include —— The time range will take effect on holiday.

Command Mode

Time-range Create Configuration Mode

Privilege Requirement

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

Example

Create a time-range entry named "tRange3" and configure time-range to exclude the holiday:

T1700X-16TS(config)#time-range tRange3

T1700X-16TS(config-time-range)#holiday exclude

7.5 holiday

Description

The **holiday** command is used to create holiday for the switch. To delete the corresponding holiday configuration, please use **no holiday** command.

Syntax

holiday *name* **start-date** *start-date* **end-date** *end-date*

no holiday *name*

Parameter

name —— The holiday name, ranging from 1 to 16 characters.

start-date —— The start date of the holiday, in the format of MM/DD, for instance, 05/01.

end-date ——The end date of the holiday, in the format of MM/DD, for instance, 05/01.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create a holiday named "holiday1" and configure the start date as October 1st and the end date as October 3rd:

T1700X-16TS(config)# holiday holiday1 **start-date** 10/01 **end-date** 10/03

7.6 show holiday

Description

The **show holiday** command is used to display the defined holiday.

Syntax

show holiday

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the defined holiday:

```
T1700X-16TS# show holiday
```

7.7 show time-range

Description

The **show time-range** command is used to display the defined time-range.

Syntax

show time-range [*time-range-name*]

Parameter

time-range-name —— The time-range name, ranging from 1 to 16 characters.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the defined time-range:

```
T1700X-16TS# show time-range
```

Chapter 8 Port Configuration Commands

Ethernet Configuration Commands can be used to configure the Bandwidth Control, Negotiation Mode and Storm Control for Ethernet ports.

8.1 interface ten-gigabitEthernet

Description

The **interface ten-gigabitEthernet** command is used to enter the Interface ten-gigabitEthernet Configuration Mode and configure the corresponding Port.

Syntax

interface ten-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 ten-gigabitEthernet Configuration Mode and configure port 2:

T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/2

8.2 interface range ten-gigabitEthernet

Description

The **interface range ten-gigabitEthernet** command is used to enter the interface range ten-gigabitEthernet Configuration Mode and configure multiple Ports at the same time.

Syntax

interface range ten-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 ten-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 ten-gigabitEthernet Configuration Mode, and configure ports 1, 2, 3, 6, 7 and 9 at the same time by adding them to one port-list:

```
T1700X-16TS(config)# interface range ten-gigabitEthernet
1/0/1-3,1/0/6-7,1/0/9
```

8.3 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 ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

Add a description Port_5 to port 1/0/5:

T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/5

T1700X-16TS(config-if)# description Port_5

8.4 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 ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

Disable port 1/0/3:

T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/3

T1700X-16TS(config-if)# shutdown

8.5 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 ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

Enable the flow-control function for port 1/0/3:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/3
T1700X-16TS(config-if)# flow-control
```

8.6 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 Port is auto-negotiation mode.

Command Mode

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

Privilege Requirement

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

Example

Configure the Duplex Mode as full-duplex for port 1/0/3:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/3
T1700X-16TS(config-if)# duplex full
```

8.7 jumbo-size

Description

The **jumbo-size** command is used to specify the size of jumbo frames.

Syntax

jumbo-size *size*

Parameter

size —— The value of jumbo frames. It ranges from 1518 to 9216 bytes, and the default is 1518 bytes.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Globally configure the size of jumbo frames as 9216:

```
T1700X-16TS(config)# jumbo-size 9216
```

8.8 speed

Description

The **speed** command is used to configure the Speed Mode for an Ethernet port. To return to the default configuration, please use **no speed** command.

Syntax

speed { 10 | 100 | 1000 | 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 ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

Configure the Speed Mode as 100Mbps for port 1/0/3:

T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/3

T1700X-16TS(config-if)# speed 100

8.9 clear counters

Description

The **clear counters** command is used to clear the statistics information of all the Ethernet ports and port channels.

Syntax

clear counters

clear counters interface [**gigabitEthernet** *port*] [**port-channel** *port-channel-id*]

Parameter

port —— The Ethernet port number.

port-channel-id —— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

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

Example

Clear the statistic information of all ports and port channels:

T1700X-16TS(config)# clear counters

8.10 show interface status

Description

The **show interface status** command is used to display the connection status of the Ethernet port/port channel.

Syntax

show interface status [**gigabitEthernet** *port*] [**port-channel** *port-channel-id*]

Parameter

port—— The Ethernet port number.

port-channel-id—— The ID of the port channel..

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the connection status of all ports and port channels:

T1700X-16TS(config)# show interface status

Display the connection status of port 1/0/1:

T1700X-16TS(config)# show interface status gigabitEthernet 1/0/1

8.11 show interface counters

Description

The **show interface counters** command is used to display the statistics information of all ports/port channels.

Syntax

show interface counters [**gigabitEthernet** *port*] [**port-channel** *port-channel-id*]

Parameter

port—— The Ethernet port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the statistics information of all Ethernet ports and port channels:

```
T1700X-16TS(config)# show interface counters
```

Display the statistics information of port 1/0/2:

```
T1700X-16TS(config)# show interface counters gigabitEthernet 1/0/2
```

8.12 show interface configuration

Description

The **show interface configuration** command is used to display the configurations of all ports and port channels, including Port-status, Flow Control, Negotiation Mode and Port-description.

Syntax

show interface configuration [**gigabitEthernet** *port*] [**port-channel** *port-channel-id*]

Parameter

port—— The Ethernet port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configurations of all Ethernet ports and port channels:

```
T1700X-16TS(config)# show interface configuration
```

Display the configurations of port 1/0/2:

```
T1700X-16TS(config)# show interface configuration gigabitEthernet 1/0/2
```

Chapter 9 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.

9.1 port isolation

Description

The **port isolation** command is used to configure the forward port/port channel list of a port/port channel, so that this port/port channel can only communicate with the ports/port channels on its list. To delete the corresponding configuration, please use **no port isolation** command.

Syntax

port isolation { [**fa-forward-list** *fa-forward-list*] [**gi-forward-list** *gi-forward-list*] [**po-forward-list** *po-forward-list*] [**te-forward-list** *te-forward-list*] }

no port isolation

Parameter

fa-forward-list / *gi-forward-list* / *te-forward-list* —— The list of Ethernet ports.

po-forward-list —— The list of port channels.

Command Mode

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

Privilege Requirement

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

Example

Set port 1, 2, 4 and port channel 2 to the forward list of port 1/0/5:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/5
T1700X-16TS(config-if)# port isolation te-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:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/2
```

```
T1700X-16TS(config-if)# no port isolation
```

9.2 show port isolation interface

Description

The **show port isolation interface** command is used to display the forward port list of a port/port channel.

Syntax

show port isolation interface [**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port*| **port-channel** *port-channel-id*]

Parameter

port —— The number of Ethernet port you want to show its forward port list, in the format of 1/0/2.

port-channel-id —— The ID of port channel you want to show its forward port list, ranging from 1 to 6.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the forward-list of port 1/0/2:

```
T1700X-16TS# show port isolation interface ten-gigabitEthernet 1/0/2
```

Display the forward-list of all Ethernet ports and port channels:

```
T1700X-16TS# show port isolation interface
```

Chapter 10 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.

10.1 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:

```
T1700X-16TS(config)# loopback-detection
```

10.2 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:

```
T1700X-16TS(config)# loopback-detection interval 50
```

10.3 loopback-detection recovery-time

Description

The **loopback-detection recovery-time** command is used to configure the time after which the blocked port would automatically recover to normal status.

Syntax

loopback-detection recovery-time *recovery-time*

Parameter

recovery-time —— The time after which the blocked port would automatically recover to normal status, and the loopback detection would restart. It ranges from 2 to 1000000 seconds. By default, this value is 90.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the recovery-time as 70 seconds:

```
T1700X-16TS(config)# loopback-detection recovery-time 70
```

10.4 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 ten-gigabitEthernet | interface range ten-gigabitEthernet | interface port-channel | interface range port-channel)

Privilege Requirement

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

Example

Enable the loopback detection function of ports 1-3:

T1700X-16TS(config)# interface range ten-gigabitEthernet 1/0/1-3

T1700X-16TS(Config-if-range)# loopback-detection

10.5 loopback-detection config process-mode

Description

The **loopback-detection config process-mode** command is used to configure the process-mode for the ports by which the switch copes with the detected loops. You also need to configure the recovery mode to remove the block status of the port or VLAN when the process-mode is Port Based or VLAN Based.

Syntax

loopback-detection config process-mode { alert | port-based | vlan-based } **recovery-mode** { auto | manual }

Parameter

alert —— When a loop is detected, the switch will send a trap message and generate an entry on the log file. It is the default setting.

port-based —— When a loop is detected, the switch will send a trap message and generate an entry on the log file. In addition, the switch will block the port

on which the loop is detected and no packets can pass through the port.

vlan-based —— When a loop is detected, the switch will send a trap message and generate an entry on the log file. In addition, the switch will block the VLAN in which the loop is detected and only the packets of the blocked VLAN cannot pass through the port.

auto —— Block status can be automatically removed after recovery time.

manual —— Block status can only be removed manually.

Command Mode

Interface Configuration Mode (interface ten-gigabitEthernet | interface range ten-gigabitEthernet | interface port-channel | interface range port-channel)

Privilege Requirement

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

Example

Configure the loopback detection process-mode as port-based, and configure the recovery mode as manual for port 2:

T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/2

T1700X-16TS(config-if)# loopback-detection config process-mode

port-based **recovery-mode** manual

10.6 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 ten-gigabitEthernet | interface range ten-gigabitEthernet | interface port-channel | interface range port-channel)

Privilege Requirement

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

Example

Recover the blocked port 1/0/2 to normal status:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/2
T1700X-16TS(config-if)# loopback-detection recover
```

10.7 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:

```
T1700X-16TS# show loopback-detection global
```

10.8 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* | **port-channel** *lagid*] [**detail**]

Parameter

port—— The Ethernet port number.

lagid—— The number of LAG, ranging from 1 to 14.

detail —— Displays the loop status and block status of the VLAN which the specified port belongs to.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of loopback detection function and the status of all ports:

T1700X-16TS# show loopback-detection interface

Display the configuration of loopback detection function and the status of port 5:

T1700X-16TS# show loopback-detection interface ten-gigabitEthernet 1/0/5

Chapter 11 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.

11.1 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 ten-gigabitEthernet / interface range ten-gigabitEthernet)

Privilege Requirement

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

Example

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

T1700X-16TS(config)# interface range ten-gigabitEthernet 1/0/2-4

T1700X-16TS(config-if-range)# channel-group 1 **mode** on

11.2 port-channel load-balance

Description

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

Syntax

port-channel load-balance { src-mac | dst-mac | src-dst-mac | src-ip | dst-ip | src-dst-ip }

no port-channel load-balance

Parameter

src-mac —— The source MAC address. When this option is selected, the Aggregate Arithmetic will be based on the source MAC address of the packets.

dst-mac —— The destination MAC address. When this option is selected, the Aggregate Arithmetic will be based on the destination MAC address of the packets.

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

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

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

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

T1700X-16TS(config)# port-channel load-balance src-dst-ip

11.3 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:

T1700X-16TS(config)# lacp system-priority 1024

11.4 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 ten-gigabitEthernet / interface range ten-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:

T1700X-16TS(config)# interface range ten-gigabitEthernet 1/0/1-3

T1700X-16TS(config-if-range)# lacp port-priority 1024

Configure the LACP port priority as 2048 for port 4:

T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/4

T1700X-16TS(config-if)# lacp port-priority 2048

11.5 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:

```
T1700X-16TS(config)# show etherchannel 1 detail
```

11.6 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:

```
T1700X-16TS(config)# show etherchannel load-balance
```

11.7 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:

```
T1700X-16TS(config)# show lacp 1 internal
```

11.8 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:

```
T1700X-16TS(config)# show lacp sys-id
```

Chapter 12 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.

12.1 mac address-table static

Description

The **mac address-table static** command is used to add the static MAC address entry. To remove the corresponding entry, please use **no mac address-table static** command. The static address can be added or removed manually, independent of the aging time. In the stable networks, the static MAC address entries can facilitate the switch to reduce broadcast packets and enhance the efficiency of packets forwarding remarkably.

Syntax

mac address-table static *mac-addr* **vid** *vid* **interface** { **fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* }

no mac address-table static *mac-addr* **vid** *vid* **interface** { **fastEthernet** *port* | **gigabitEthernet** *port* | **ten-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:

```
T1700X-16TS(config)# mac address-table static 00:02:58:4f:6c:23 vid 1 interface ten-gigabitEthernet 1/0/1
```

12.2 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:

T1700X-16TS(config)# mac address-table aging-time 500

12.3 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:

```
T1700X-16TS(config)# mac address-table filtering 00:1e:4b:04:01:5d vid 1
```

12.4 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 cannot access to the network via this port.

Syntax

mac address-table max-mac-count { [**max-number** *num*] [**mode** { dynamic | static | permanent }] [**status** { forward | drop | disable }] [**exceed-max-learned** enable | disable] }

no mac address-table max-mac-count [max-number | mode | status]

Parameter

num —— The maximum number of MAC addresses that can be learned on the port. It ranges from 0 to 64. By default this value is 64.

dynamic | static | permanent —— Learn mode for MAC addresses. There are three modes, including Dynamic mode, Static mode and Permanent mode. When Dynamic mode is selected, the learned MAC address will be deleted automatically after the aging time. When Static mode is selected, the learned

MAC address will be out of the influence of the aging time and can only be deleted manually. The learned entries will be cleared after the switch is rebooted. When permanent mode is selected, the learned MAC address will be out of the influence of the aging time and can only be deleted manually too. However, the learned entries will be saved even the switch is rebooted.

status —— Select the action to be taken when the number of the MAC addresses reaches the maximum learning number on the port. By default this function is disabled.

- forward: The packets will be forward but not be learned when learned MAC number exceeds the maximum MAC address number on this port.
- drop: The packets will be dropped when learned MAC number exceeds the maximum MAC address number on this port.
- disable: The MAC address threshold on this port is disabled.

new-mac-learned enable | disable —— Enable/Disable the new-mac-learned notification on this port. With this feature enabled, a SNMP notification is generated and sent to the network management system (NMS) when the port learns a new MAC address.

Command Mode

Interface Configuration Mode (interface ten-gigabitEthernet / interface range ten-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:

T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/1

T1700X-16TS(config-if)# mac address-table max-mac-count max-number 30 **mode** static **status** drop

12.5 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 | filtering }

Parameter

dynamic | static | filtering —— The type of your desired entry. By default all the entries are displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of all address entries:

```
T1700X-16TS(config)# show mac address-table
```

12.6 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:

```
T1700X-16TS(config)# clear mac address-table static
```

12.7 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:

```
T1700X-16TS(config)# show mac address-table aging-time
```

12.8 show mac address-table max-mac-count

Description

The **show mac address-table max-mac-count interface ten-gigabitEthernet** command is used to display the security configuration of all ports or the specified port.

Syntax

show mac address-table max-mac-count { all | **interface ten-gigabitEthernet** *port*}

Parameter

all —— Displays the security information of all the Ethernet ports.

port —— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the security configuration of all ports:

T1700X-16TS(config)# show mac address-table max-mac-count all

Display the security configuration of port 1/0/1:

T1700X-16TS(config)# show mac address-table max-mac-count interface ten-gigabitEthernet 1/0/1

12.9 show mac address-table interface

Description

The **show mac address-table interface** command is used to display the address configuration of the specified port/port channel.

Syntax

show mac address-table interface { **gigabitEthernet** *port* | **port-channel** *port-channel-id*}

Parameter

port——The Ethernet port number.

port-channel-id——The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the address configuration of port 1/0/1:

T1700X-16TS(config)# show mac address-table interface ten-gigabitEthernet 1/0/1

12.10 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 [**vlan** *vlan-id*]

Parameter

vlan-id —— Specify the VLAN which the MAC entries belong to.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the total MAC entry information in different VLANs:

```
T1700X-16TS(config)# show mac address-table count
```

12.11 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* [**interface** { **gigabitEthernet** *port* | **port-channel** *port-channel-id*} | **vid** *vlan-id*]

Parameter

mac-addr——The specified MAC address.

port—— The Ethernet port number.

port-channel-id—— The ID of the port channel.

vlan-id—— Specify the VLAN which the entry belongs to.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of the MAC address 00:00:00:00:23:00 in VLAN 1:

```
T1700X-16TS(config)#show mac address-table address 00:00:00:00:23:00
vid 1
```

12.12 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:

```
T1700X-16TS(config)# show mac address-table vlan 1
```

Chapter 13 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.

13.1 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:

T1700X-16TS(config)# vlan 2-10,100

Delete VLAN 2:

T1700X-16TS(config)# no vlan 2

13.2 name

Description

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

Syntax

name *descript*

no name

Parameter

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

Command Mode

VLAN Configuration Mode(VLAN)

Privilege Requirement

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

Example

Specify the name of VLAN 2 as "group1":

T1700X-16TS(config)# vlan 2

T1700X-16TS(config-vlan)# name group1

13.3 switchport general allowed vlan

Description

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

Syntax

switchport general allowed vlan *vlan-list* { tagged | untagged }

no switchport general allowed vlan *vlan-list*

Parameter

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

tagged | untagged —— egress-rule.

Command Mode

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

Privilege Requirement

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

Example

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

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/4

T1700X-16TS(config-if)#switchport mode general

T1700X-16TS(config-if)#switchport general allowed vlan 2 tagged

13.4 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 ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

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

T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/2

T1700X-16TS(config-if)# switchport pvid 2

13.5 switchport check ingress

Description

The **switchport check ingress** command is used to enable the Ingress Checking function for the switch ports. With this function enabled, the port will accept the packet of which the VLAN ID is in the port's VLAN list and discard others. With this function disabled, the port will forward the packet directly. To disable this function, please use **no switchport check ingress** command.

Syntax

switchport check ingress

no switchport check ingress

Command Mode

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

Privilege Requirement

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

Example

Enable Ingress Checking on the port 1/0/2:

T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/2

T1700X-16TS(config-if)# switchport check ingress

13.6 switchport acceptable frame

Description

The **switchport acceptable frame** command is used to specify the acceptable frame type for the switch ports and the ports will perform this operation before Ingress Checking. To restore to the default setting, please use **no switchport acceptable frame** command.

Syntax

switchport acceptable frame { all | tagged }

no switchport acceptable frame

Parameter

all | tagged —— the acceptable frame type.

Command Mode

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

Privilege Requirement

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

Example

Specify the acceptable frame type of Port 1/0/4 as “tagged”:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/4

T1700X-16TS(config-if)#switchport acceptable frame general

13.7 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:

T1700X-16TS(config)# show vlan summary

13.8 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:

```
T1700X-16TS(config)# show vlan brief
```

13.9 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:

T1700X-16TS(config)# show vlan id 5

13.10 show interface switchport

Description

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

Syntax

show interface switchport [**fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id*]

Parameter

port—— The port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

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

T1700X-16TS(config)# show interface switchport

Chapter 14 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.

14.1 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":

T1700X-16TS(config)#mac-vlan mac-address 00:11:11:01:01:12 **vlan** 2 **description** TP

14.2 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 ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

Enable the Port 1/0/3 for the MAC-based VLAN feature:

```
T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/3
T1700X-16TS(config-if)#mac-vlan
```

14.3 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:

```
T1700X-16TS(config)#show mac-vlan all
```

14.4 show mac-vlan interface

Description

The **show mac-vlan interface** command is used to display the port state of MAC-based VLAN.

Syntax

show mac-vlan interface

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the enable state of all the ports:

```
T1700X-16TS(config)#show mac-vlan interface
```

Chapter 15 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.

15.1 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:

T1700X-16TS(config)#protocol-vlan template name TP **frame ether_2 ether-type** 2024

15.2 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* **priority** *priority* **template** *template-idx*

no protocol-vlan vlan *group-idx*

Parameter

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

priority—— Specify the 802.1p priority for the packets that belong to the protocol VLAN, ranging from 0-7. The switch will determine the forwarding sequence according this value. The packets with larger value of 802.1p priority have the higher priority.

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

group-idx ——The number of the Protocol-based VLAN entry. You can get the Protocol-based VLAN entry corresponding to the number by the **show protocol-vlan vlan** command.

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:

T1700X-16TS(config)#protocol-vlan vlan 2 **template** 3

15.3 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 ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

Add port 2 to protocol group 1:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/2

T1700X-16TS(config-if)#protocol-vlan group 1

15.4 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:

```
T1700X-16TS(config)#show protocol-vlan template
```

15.5 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:

```
T1700X-16TS(config)#show protocol-vlan vlan
```

Chapter 16 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.

16.1 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:

```
T1700X-16TS(config)#gvrp
```

16.2 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 ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

Enable the GVRP function for Ports 1/0/2-6:

```
T1700X-16TS(config)#interface range ten-gigabitEthernet 1/0/2-6
T1700X-16TS(config-if-range)#gvrp
```

16.3 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 ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

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

T1700X-16TS(config)#interface range ten-gigabitEthernet 1/0/2-6

T1700X-16TS(config-if-range)#gvrp registration fixed

16.4 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 ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

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

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/6

T1700X-16TS(config-if)#gvrp timer leaveall 2000

T1700X-16TS(config-if)#no gvrp timer join

16.5 show gvrp interface

Description

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

Syntax

show gvrp interface [**fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id*]

Parameter

port —— The port number.
port-channel-id —— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the GVRP configuration information of Port 1:

T1700X-16TS(config)#show gvrp interface ten-gigabitEthernet 1/0/1

Display the GVRP configuration information of all Ethernet ports:

T1700X-16TS(config)#show gvrp interface

16.6 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:

```
T1700X-16TS(config)#show gvrp global
```

Chapter 17 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.

17.1 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:

```
T1700X-16TS(config)# ip igmp snooping
```

17.2 ip igmp snooping version

Description

The **ip igmp snooping version** command is used to configure IGMP version globally. To return to the default configuration, please use **no ip igmp snooping version** command.

Syntax

ip igmp snooping version {v1 | v2 | v3 **}**

no ip igmp snooping version

Parameter

v1 | v2 | v3—— Specify the IGMP version. By default, it is IGMP v3.

v1: The switch works as an IGMPv1 Snooping switch. It can only process IGMPv1 messages from the host. Report messages of other versions are ignored.

v2: The switch works as an IGMPv2 Snooping switch. It can process both IGMPv1 and IGMPv2 messages from the host. IGMPv3 messages are ignored.

v3: The switch works as an IGMPv3 Snooping switch. It can process IGMPv1, IGMPv2 and IGMPv3 messages from the host.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the IGMP version as v2:

T1700X-16TS (config)# ip igmp snooping version v2

17.3 ip igmp snooping drop-unknown

Description

The **ip igmp snooping drop-unknown** command is used to configure the way how the switch processes multicast streams that are sent to unknown multicast groups as Discard. By default, it is Forward. To return to the default configuration, please use **no ip igmp snooping drop-unknown** command.

Syntax

ip igmp snooping drop-unknown

no ip igmp snooping drop-unknown

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the operation to process unknown multicast as discard:

```
T1700X-16TS(config)# ip igmp snooping drop-unknown
```

17.4 ip igmp snooping header-validation

Description

The **ip igmp snooping header-validation** command is used to enable IGMP Header Validation globally. To disable the IGMP Header Validation function, please use **no ip igmp snooping header-validation** command.

Generally, for IGMP packets, the TTL value should be 1, ToS field should be 0xC0, and Router Alert option should be 0x94040000. The fields to be validated depend on the IGMP version being used. IGMPv1 only checks the TTL field. IGMPv2 checks the TTL field and the Router Alert option. IGMPv3 checks TTL field, ToS field and Router Alert option. Packets that fail the validation process will be dropped.

Syntax

ip igmp snooping header-validation

no ip igmp snooping header-validation

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable IGMP Header Validation:

```
T1700X-16TS(config)# ip igmp snooping header-validation
```

17.5 ip igmp snooping vlan-config

Description

The **ip igmp snooping vlan-config** command is used to enable VLAN IGMP Snooping function or to modify IGMP Snooping parameters. To disable the VLAN IGMP Snooping function, please use **no ip igmp snooping vlan-config** command. To restore the default values, please use **no ip igmp snooping vlan-config** with specified parameters.

Syntax

ip igmp snooping vlan-config *vlan-id-list* [**rtime** *router-time* | **mtime** *member-time* | **ltime** *leave-time*]

no ip igmp snooping vlan-config *vlan-id-list* [**rtime** | **mtime** | **ltime**]

Parameter

vlan-id-list —— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

router-time —— The Router Port Aging Time. Within this time, if the switch does not receive IGMP query message from the router port, it will consider this port is not a router port any more. Valid values are from 60 to 600 in seconds, and the default value is 300 seconds.

member-time —— The Member Port Aging Time. Within this time, if the switch does not receive IGMP report message from the member port, it will consider this port is not a member port any more. Valid values are from 60 to 600 in seconds, and the default value is 260 seconds.

leave-time —— The Leave Time. Valid values are from 1 to 30 in seconds, and the default value is 1 second. When the switch receives a leave message from a port to leave a multicast group, it will wait for a Leave Time before removing the port from the multicast group. During the period, if the switch receives any report messages from the port, the port will not be removed from the multicast group. Exceptions are as follows:

- If the member port ages out before the Leave Time ends and no report messages are received, the port will be removed from the multicast group once its Member Port Aging Time ends.
- The Leave Time mechanism will not take effect when Fast Leave takes effect.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the IGMP Snooping function and modify Router Port Aging Time as 300 seconds, Member Port Aging Time as 200 seconds for VLAN 1-3:

T1700X-16TS(config)# ip igmp snooping vlan-config 1-3 **rtime** 300

T1700X-16TS(config)# ip igmp snooping vlan-config 1-3 **mtime** 200

17.6 ip igmp snooping vlan-config (immediate-leave)

Description

This command is used to enable the Fast Leave feature for specific VLANs. To disable Fast Leave on the VLANs, please use **no ip igmp snooping vlan-config** *vlan-id-list* **immediate-leave** command. This function is disabled by default.

Syntax

ip igmp snooping vlan-config *vlan-id-list* **immediate-leave**

no ip igmp snooping vlan-config *vlan-id-list* **immediate-leave**

Parameter

vlan-id-list —— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the Fast Leave for VLAN 1-3:

T1700X-16TS(config)# ip igmp snooping vlan-config 1-3 **immediate-leave**

17.7 ip igmp snooping vlan-config (report-suppression)

Description

This command is used to enable the IGMP Report Suppression function for specific VLANs. When enabled, the switch will only forward the first IGMP report message for each multicast group to the IGMP querier and suppress subsequent IGMP report messages for the same multicast group during one query interval. This feature prevents duplicate report messages from being sent to the IGMP querier. To disable the IGMP report suppression function and forward all the IGMP reports to the Layer 3 device in specific VLANs,

please use **no ip igmp snooping vlan-config** *vlan-id-list* **report-suppression** command. This function is disabled by default.

Syntax

ip igmp snooping vlan-config *vlan-id-list* **report-suppression**

no ip igmp snooping vlan-config *vlan-id-list* **report-suppression**

Parameter

vlan-id-list —— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the IGMP Report Suppression for VLAN 1-3:

```
T1700X-16TS(config)# ip igmp snooping vlan-config 1-3
report-suppression
```

17.8 ip igmp snooping vlan-config (router-ports-forbidden)

Description

This command is used to forbid the specified ports as being router ports in the specified VLAN(s). To delete the forbidden router ports, please use **no ip igmp snooping vlan-config** *vlan-id-list* **router-ports-forbidd** command.

Syntax

ip igmp snooping vlan-config *vlan-id-list* **router-ports-forbidd interface** { **gigabitEthernet** *port-list* | **port-channel** *port-channel-list* }

no ip igmp snooping vlan-config *vlan-id-list* **router-ports-forbidd interface** [**gigabitEthernet** *port-list* | **port-channel** *port-channel-list*]

Parameter

vlan-id-list —— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

port-list —— Forbid the specified ports as being router ports. Packets sent from multicast routers to these ports will be discarded.

port-channel-list —— Forbid the specified port-channels as being router ports. Packets sent from multicast routers to these port-channels will be discarded.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Forbid the Ethernet ports 1/0/1-3 as being router ports in VLAN 1 :

T1700X-16TS(config)# ip igmp snooping vlan-config 1

router-ports-forbidd interface ten-gigabitEthernet 1/0/1-3

17.9 ip igmp snooping vlan-config (rport interface)

Description

This command is used to specify the static router ports for specific VLANs. To delete the static router ports, please use **no ip igmp snooping vlan-config** *vlan-id-list* **rport interface** command.

Syntax

ip igmp snooping vlan-config *vlan-id-list* **rport interface** { **gigabitEthernet** *port-list* | **port-channel** *port-channel-list* }

no ip igmp snooping vlan-config *vlan-id-list* **rport interface** { **gigabitEthernet** *port-list* | **port-channel** *port-channel-list* }

Parameter

vlan-id-list —— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

port-list —— The list of Ethernet ports.

port-channel-list—— The ID of the port channels.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Set the router port as 1/0/1 for VLAN 1-2:

```
T1700X-16TS(config)# ip igmp snooping vlan-config 1-2 rport interface
ten-gigabitEthernet 1/0/1
```

17.10 ip igmp snooping vlan-config (static)

Description

This command is used to configure interfaces to statically join a multicast group. To remove interfaces from a static multicast group, please use **no ip igmp snooping vlan-config** *vlan-id-list* **static**command.

Syntax

ip igmp snooping vlan-config *vlan-id-list* **static** *ip* **interface** { **gigabitEthernet** *port-list* | **port-channel** *port-channel-list* }

no ip igmp snooping vlan-config *vlan-id-list* **static** *ip* **interface** { **gigabitEthernet** *port-list* | **port-channel** *port-channel-list* }

Parameter

vlan-id-list —— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

ip ——Specify the IP address of the multicast group that the hosts want to join.

port-list —— The list of Ethernet ports.

port-channel-list —— The ID of the port channels.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure port ports 1/0/1-3 in VLAN 2 to statically join multicast group 225.0.0.1:

```
T1700X-16TS(config)# ip igmp snooping vlan-config 2 static 225.0.0.1
interface ten-gigabitEthernet 1/0/1-3
```

17.11 ip igmp snooping vlan-config (querier)

Description

This command is used to enable the IGMP Snooping Querier feature for specific VLANs. To disable the IGMP Snooping Querier feature on the VLANs, please use **no ip igmp snooping vlan-config** *vlan-id-list* **querier** command without any parameters. To restore the default values, please use **no ip igmp snooping vlan-config** *vlan-id-list* **querier** command with specified parameters.

Syntax

ip igmp snooping vlan-config *vlan-id-list* **querier [max-response-time** *response-time* **| query-interval** *interval* **| general-query source-ip** *ip-addr* **| last-member-query-count** *count* **| last-member-query-interval** *interval* **]**

no ip igmp snooping vlan-config *vlan-id-list* **querier [max-response-time | query-interval | general-query source-ip | last-member-query-count]**

Parameter

vlan-id-list —— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

response-time—— The host's maximum response time to general query messages. Valid values are from 1 to 25 seconds, and the default value is 10 seconds.

query-interval *interval*—— The interval between general query messages sent by the switch. Valid values are from 10 to 300 seconds, and the default value is 60 seconds.

ip-addr—— The source IP address of the general query messages sent by the switch. It should be a unicast address. By default, it is 0.0.0.0.

count —— The number of group-specific queries to be sent. With IGMP Snooping Querier enabled, when the switch receives an IGMP leave message, it obtains the address of the multicast group that the host wants to leave from the message. Then the switch sends out group-specific queries to this multicast group through the port receiving the leave message. If specified count of group-specific queries are sent and no report message is received, the switch will delete the multicast address from the multicast forwarding table. Valid values are from 1 to 5, and the default value is 2.

last-member-query-interval *interval* —— The interval between group-specific queries.. Valid values are from 1 to 5 seconds, and the default value is 1 second.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the IGMP Snooping Querier for VLAN 3, and configure the query interval as 100 seconds:

```
T1700X-16TS(config)# ip igmp snooping vlan-config 3 querier
T1700X-16TS(config)# ip igmp snooping vlan-config 3 querier query
interval 100
```

17.12 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 ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

Enable IGMP Snooping function of port 1/0/3:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/3
T1700X-16TS(config-if)# ip igmp snooping
```

17.13 ip igmp snooping max-groups

Description

The **ip igmp snooping max-groups** command is used to configure the maximum number of groups that a port can join in. The **ip igmp snooping max-groups action** is used to configure the action that the port takes when it receives an IGMP report message and the maximum number of entries is in the forwarding table. To remove the maximum group limitation and return to the default of no limitation on the specified port, please use the **no ip igmp snooping max-groups** command. To return to the default action of dropping the report, please use the **no ip igmp snooping max-groups action** command. These commands only apply to the dynamic multicast groups.

Syntax

ip igmp snooping max-groups *maxgroup*

ip igmp snooping max-groups action { drop | replace }

no ip igmp snooping max-groups

no ip igmp snooping max-groups action

Parameter

maxgroup —— Specify the maximum numbers of groups that the port can join. It ranges from 0 to 1000 and the default value is 1000.

drop —— When the number of the dynamic multicast groups that a port joins has exceeded the max-group, the port will not join any new multicast group.

replace —— When the number of the dynamic multicast groups that a port joins has exceeded the max-group, the newly joined multicast group will replace an existing multicast group with the lowest multicast group address.

Command Mode

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

Privilege Requirement

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

Example

Specify the maximum numbers of groups that ports 1/0/2-5 can join as 10, and configure the throttling action as replace:

```
T1700X-16TS(config)#interface range ten-gigabitEthernet 1/0/2-5
```

T1700X-16TS(config-if-range)#ip igmp snooping max-groups 10

T1700X-16TS(config-if-range)#ip igmp snooping max-groups action replace

17.14 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 ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

Enable the Fast Leave function for port 1/0/3:

T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/3

T1700X-16TS(config-if)# ip igmp snooping immediate-leave

17.15 ip igmp profile

Description

The **ip igmp profile** command is used to create the configuration profile. To delete the corresponding profile, please use **no ip igmp profile** command.

Syntax

ip igmp profile *id*

no ip igmp profile *id*

Parameter

id —— Specify the id of the configuration profile, ranging from 1 to 999.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create the profile 1:

T1700X-16TS(config)# ip igmp profile 1

17.16 deny

Description

The **deny** command is used to configure the filtering mode of profile as deny.

Syntax

deny

Command Mode

Profile Configuration Mode

Privilege Requirement

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

Example

Configure the filtering mode of profile 1 as deny:

T1700X-16TS(config)# ip igmp profile 1

T1700X-16TS(config-igmp-profile)#deny

17.17 permit

Description

The **permit** command is used to configure the filtering mode of profile as permit.

Syntax

permit

Command Mode

Profile Configuration Mode

Privilege Requirement

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

Example

Configure the filtering mode of profile 1 as permit:

T1700X-16TS(config)# ip igmp profile 1
T1700X-16TS(config-igmp-profile)#permit

17.18 range

Description

The **range** command is used to configure the range of the profile's filtering multicast address. To delete the corresponding filtering multicast address, please use **no range** command. A profile contains 16 filtering IP-range entries at most.

Syntax

range *start-ip end-ip*

no range *start-ip end-ip*

Parameter

start-ip —— The start filtering multicast IP address.

end-ip —— The end filtering multicast IP address.

Command Mode

Profile Configuration Mode

Privilege Requirement

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

Example

Configure one of the filter multicast address entry as range 225.1.1.1 to 226.3.2.1 in profile 1:

T1700X-16TS(config)# ip igmp profile 1

T1700X-16TS(config-igmp-profile)#range 225.1.1.1 226.3.2.1

17.19 ip igmp filter

Description

The **ip igmp filter** command is used to bind the specified profile to the interface. To delete the binding, please use **no ip igmp filter** command.

Syntax

ip igmp filter *profile-id*

no ip igmp filter

Parameter

profile-id—— Specify the profile ID, ranging from 1 to 999.

Command Mode

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

Privilege Requirement

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

Example

Bind profile 1 to interface ten-gigabitEthernet 1/0/2:

T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/2

T1700X-16TS(config-if)# ip igmp filter 1

17.20 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:

```
T1700X-16TS(config)# clear ip igmp snooping statistics
```

17.21 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:

```
T1700X-16TS# show ip igmp snooping
```

17.22 show ip igmp snooping interface

Description

The **show ip igmp snooping interface** command is used to display the port configuration of IGMP snooping. If no interface is specified, it displays all interfaces' IGMP snooping configurations.

Syntax

show ip igmp snooping interface [**gigabitEthernet** [*port-list*] | **port-channel** [*port-channel-list*]] { basic-config | max-groups | packet-stat }

Parameter

port-list —— The list of Ethernet ports.

Port-channel-list —— The list of port channels.

basic-config | max-groups | packet-stat —— The related configuration information selected to display.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IGMP baisic configuration configuration of all ports and port channels:

T1700X-16TS# show ip igmp snooping interface basic-config

Display the IGMP basic configuration of port 1/0/2:

T1700X-16TS# show ip igmp snooping interface ten-gigabitEthernet 1/0/2 basic-config

Display the IGMP packet statistics of ports 1/0/1-4:

T1700X-16TS# show ip igmp snooping interface ten-gigabitEthernet 1/0/1-4 packet-stat

17.23 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:

T1700X-16TS# show ip igmp snooping vlan 2

17.24 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:

T1700X-16TS#show ip igmp snooping groups

Display all the multicast entries in VLAN 5:

T1700X-16TS(config)#show ip igmp snooping groups vlan 5

Display the count of multicast entries in VLAN 5:

T1700X-16TS(config)#show ip igmp snooping groups vlan 5 count

Display the dynamic multicast groups of VLAN 5

T1700X-16TS(config)#show ip igmp snooping groups vlan 5 dynamic

Display the static multicast groups of VLAN 5

T1700X-16TS(config)#show ip igmp snooping groups vlan 5 static

Display the count of dynamic multicast entries of VLAN 5

T1700X-16TS(config)#show ip igmp snooping groups vlan 5 dynamic count

Display the count of static multicast entries of VLAN 5

T1700X-16TS(config)#show ip igmp snooping groups vlan 5 static count

17.25 show ip igmp profile

Description

The **show ip igmp profile** command is used to display the configuration information of all the profiles or a specific profile.

Syntax

show ip igmp profile [*id*]

Parameter

id —— Specify the ID of the profile, ranging from 1 to 999.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration information of all profiles:

T1700X-16TS(config)# show ip igmp profile

Chapter 18 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.

18.1 ipv6 mld snooping (global)

Description

The **ipv6 mld snooping** command is used to enable MLD Snooping function globally. If this function is disabled, all related MLD Snooping function would not work. To disable this function, please use **no ipv6 mld snooping** command.

Syntax

ipv6 mld snooping

no ipv6 mld snooping

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable MLD Snooping:

```
T1700X-16TS(config)# ipv6 mld snooping
```

18.2 ipv6 mld snooping drop-unknown

Description

The **ipv6 mld snooping drop-unknown** command is used to enable the unknown multicast packets filter function. To disable this function, please use **no ipv6 mld snooping drop-unknown** command. By default, it is disabled.

Syntax

ipv6 mld snooping drop-unknown

no ipv6 mld snooping drop-unknown

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable unknown multicast filter function:

```
T1700X-16TS(config)# ipv6 mld snooping drop-unknown
```

18.3 ipv6 mld snooping vlan-config

Description

The **ipv6 mld snooping vlan-config** command is used to enable VLAN MLD Snooping function or to modify MLD Snooping parameters. To disable the VLAN MLD Snooping function, please use **no ipv6 mld snooping vlan-config** command.

Syntax

ipv6 mld snooping vlan-config *vlan-id-list* [**rtime** *router-time* | **mtime** *member-time* | **ltime** *leave-time*]

no ipv6 mld snooping vlan-config *vlan-id-list* [**rtime** | **mtime** | **ltime**]

Parameter

vlan-id-list —— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

router-time —— The Router Port Aging Time. Within this time, if the switch does not receive any MLD query messages from the router port, it will consider this port is not a router port any more. Valid values are from 60 to 600 in seconds, and the default value is 300 seconds.

member-time —— The Member Port Aging Time. Within this time, if the switch does not receive any MLD report messages from the member port, it will consider this port is not a member port any more. Valid values are from 60 to 600 in seconds, and the default value is 260 seconds.

leave-time —— The Leave Time. Valid values are from 1 to 30 in seconds, and the default value is 1 second. When the switch receives a done message from a port to leave a multicast group, it will wait for a Leave Time before removing the port from the multicast group. During the period, if the switch receives any report messages from the port, the port will not be removed from the multicast group. Exceptions are as follows:

- If the member port ages out before the Leave Time ends and no report messages are received, the port will be removed from the multicast group once its Member Port Aging Time ends.

- The Leave Time mechanism will not take effect when Fast Leave takes effect.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the MLD Snooping function and modify Router Port Time as 300 seconds, Member Port Time as 200 seconds for VLAN 1-3:

T1700X-16TS(config)# ipv6 mld snooping vlan-config 1-3 **rtime** 300

T1700X-16TS(config)# ipv6 mld snooping vlan-config 1-3 **mtime** 200

18.4 ipv6 mld snooping vlan-config (immediate-leave)

Description

This command is used to enable the Fast Leave feature for specific VLANs. To disable Fast Leave on the VLANs, please use **no ipv6 mld snooping vlan-config** *vlan-id-list* **immediate-leave** command. This function is disabled by default.

Syntax

ipv6 mld snooping vlan-config *vlan-id-list* **immediate-leave**

no ipv6 mld snooping vlan-config *vlan-id-list* **immediate-leave**

Parameter

vlan-id-list —— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the Fast Leave for VLAN 1-3:

```
T1700X-16TS(config)# ipv6 mld snooping vlan-config 1-3
immediate-leave
```

18.5 ipv6 mld snooping vlan-config (report-suppression)

Description

This command is used to enable the MLD Report Suppression function for specific VLANs. When enabled, the switch will only forward the first MLD report message for each multicast group to the MLD querier and suppress subsequent MLD report messages for the same multicast group during one query interval. This feature prevents duplicate report messages from being sent to the MLD querier. To disable the MLD report suppression function and forward all the MLD reports to the Layer 3 device in specific VLANs, please use **no ipv6 mld snooping vlan-config** *vlan-id-list* **report-suppression** command. This function is disabled by default.

Syntax

ipv6 mld snooping vlan-config *vlan-id-list* **report-suppression**

no ipv6 mld snooping vlan-config *vlan-id-list* **report-suppression**

Parameter

vlan-id-list —— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the MLD Report Suppression for VLAN 1-3:

```
T1700X-16TS(config)# ipv6 mld snooping vlan-config 1-3
report-suppression
```

18.6 ipv6 mld snooping vlan-config (router-ports-forbidden)

Description

This command is used to forbid the specified ports as being router ports in the specified VLAN(s). To delete the forbidden router ports, please use **no ipv6 mld snooping vlan-config** *vlan-id-list* **router-ports-forbidd** command.

Syntax

ipv6 mld snooping vlan-config *vlan-id-list* **router-ports-forbidd interface** { **gigabitEthernet** *port-list* | **port-channel** *port-channel-list* }

no ipv6 mld snooping vlan-config *vlan-id-list* **router-ports-forbidd interface** [**gigabitEthernet** *port-list* | **port-channel** *port-channel-list*]

Parameter

vlan-id-list —— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

port-list —— Forbid the specified ports as being router ports. Packets sent from multicast routers to these ports will be discarded.

port-channel-list —— Forbid the specified port-channels as being router ports. Packets sent from multicast routers to these port-channels will be discarded.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Forbid the Ethernet ports 1/0/1-3 as being router ports in VLAN 1:

```
T1700X-16TS(config)# ipv6 mld snooping vlan-config 1
router-ports-forbidd interface ten-gigabitEthernet 1/0/1-3
```

18.7 ipv6 mld snooping vlan-config (rport interface)

Description

This command is used to specify the static router ports for specific VLANs. To delete the static router ports, please use **no ipv6 mld snooping vlan-config** *vlan-id-list* **rport interface** command.

Syntax

ipv6 mld snooping vlan-config *vlan-id-list* **rport interface** { **gigabitEthernet** *port-list* | **port-channel** *port-channel-list* }

no ipv6 mld snooping vlan-config *vlan-id-list* **rport interface** { **gigabitEthernet** *port-list* | **port-channel** *port-channel-list* }

Parameter

vlan-id-list —— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

port-list —— The list of Ethernet ports.

port-channel-list—— The ID of the port channels.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Set the router port as 1/0/1 for VLAN 1-2:

```
T1700X-16TS(config)# ipv6 mld snooping vlan-config 1-2 rport interface
ten-gigabitEthernet 1/0/1
```

18.8 ipv6 mld snooping vlan-config (static)

Description

This command is used to configure interfaces to statically join a multicast group. To remove interfaces from a static multicast group, please use **no ipv6 mld snooping vlan-config** *vlan-id-list* **static**command.

Syntax

ipv6 mld snooping vlan-config *vlan-id-list* **static** *ip* **interface** { **gigabitEthernet** *port-list* | **port-channel** *port-channel-list* }

no ipv6 mld snooping vlan-config *vlan-id-list* **static** *ip* **interface** { **gigabitEthernet** *port-list* | **port-channel** *port-channel-list* }

Parameter

vlan-id-list —— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

ip ——Specify the IP address of the multicast group that the hosts want to join.

port-list —— The list of Ethernet ports.

port-channel-list —— The ID of the port channels.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure port ports 1/0/1-3 in VLAN 2 to statically join multicast group 225.0.0.1:

T1700X-16TS(config)# ipv6 mld snooping vlan-config 2 **static** 225.0.0.1 **interface ten-gigabitEthernet** 1/0/1-3

18.9 ipv6 mld snooping vlan-config (querier)

Description

This command is used to enable the MLD Snooping Querier feature for specific VLANs. To disable the MLD Snooping Querier feature on the VLANs, please use **no ipv6 mld snooping vlan-config** *vlan-id-list* **querier** command without any parameters. To restore the default values, please use **no ipv6 mld snooping vlan-config** *vlan-id-list* **querier** command with specified parameters.

Syntax

ipv6 mld snooping vlan-config *vlan-id-list* **querier [max-response-time** *response-time* **| query-interval** *interval* **| general-query source-ip** *ip-addr* **| last-listener-query-count** *count* **| last-listener-query-interval** *interval***]**

no ipv6 mld snooping vlan-config *vlan-id-list* **querier [max-response-time | query-interval | general-query source-ip | last-listener-query-count | last-listener-query-interval]**

Parameter

vlan-id-list —— The ID list of the VLAN desired to modify configuration, ranging from 1 to 4094, in the format of 1-3, 5.

response-time—— The host's maximum response time to general query messages. Valid values are from 1 to 25 seconds, and the default value is 10 seconds.

query-interval *interval*—— The interval between general query messages sent by the switch. Valid values are from 10 to 300 seconds, and the default value is 60 seconds.

ip-addr—— The source IP address of the general query messages sent by the switch. It should be a unicast address. By default, it is fe80::2ff:ffff:fe00:1.

count —— The number of group-specific queries to be sent. With MLD Snooping Querier enabled, when the switch receives an MLD done message, it obtains the address of the multicast group that the host wants to leave from the message. Then the switch sends out group-specific queries to this multicast group through the port receiving the done message. If specified count of group-specific queries are sent and no report message is received, the switch will delete the multicast address from the multicast forwarding table. Valid values are from 1 to 5, and the default value is 2.

last-member-query-interval *interval* —— The interval between group-specific queries. Valid values are from 1 to 5 seconds, and the default value is 1 second.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the MLD Snooping Querier for VLAN 3, and configure the query interval as 100 seconds:

T1700X-16TS(config)# ipv6 mld snooping vlan-config 3 **querier**

T1700X-16TS(config)# ipv6 mld snooping vlan-config 3 **querier query interval** 100

18.10 ipv6 mld snooping (interface)

Description

The **ipv6 mld snooping** command is used to enable MLD Snooping function on the desired port. To disable this function, please use **no ipv6 mld snooping** command.

Syntax

ipv6 mld snooping

no ipv6 mld snooping

Command Mode

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

Privilege Requirement

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

Example

Enable MLD Snooping on port 1/0/3:

T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/3

T1700X-16TS(config-if)# ipv6 mld snooping

18.11 ipv6 mld snooping max-groups

Description

The **ipv6 mld snooping max-groups** command is used to configure the maximum number of groups that a port can join in. The **ipv6 mld snooping max-groups action** is used to configure the action that the port takes when it receives an MLD report message and the maximum number of entries is in the forwarding table. To remove the maximum group limitation and return to the default of no limitation on the specified port, please use the **no ipv6 mld**

snooping max-groups command. To return to the default action of dropping the report, please use the **no ipv6 mld snooping max-groups action** command. These commands only apply to the dynamic multicast groups.

Syntax

ipv6 mld snooping max-groups *maxgroup*

ipv6 mld snooping max-groups action { drop | replace }

no ipv6 mld snooping max-groups

no ipv6 mld snooping max-groups action

Parameter

maxgroup —— Specify the maximum numbers of groups that the port can join. It ranges from 0 to 1000 and the default value is 1000.

drop —— When the number of the dynamic multicast groups that a port joins has exceeded the max-group, the port will not join any new multicast group.

replace —— When the number of the dynamic multicast groups that a port joins has exceeded the max-group, the newly joined multicast group will replace an existing multicast group with the lowest multicast group address.

Command Mode

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

Privilege Requirement

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

Example

Specify the maximum numbers of groups that ports 1/0/2-5 can join as 10, and configure the throttling action as replace:

```
T1700X-16TS(config)#interface range ten-gigabitEthernet 1/0/2-5
T1700X-16TS(config-if-range)#ipv6 mld snooping max-groups 10
T1700X-16TS(config-if-range)#ipv6 mld snooping max-groups action
replace
```

18.12 ipv6 mld snooping immediate-leave

Description

The **ipv6 mld snooping immediate-leave** command is used to configure the Fast Leave function for port. To disable the Fast Leave function, please use **no ipv6 mld snooping immediate-leave** command.

Syntax

ipv6 mld snooping immediate-leave

no ipv6 mld snooping immediate-leave

Command Mode

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

Privilege Requirement

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

Example

Enable the Fast Leave function for port 1/0/3:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/3
T1700X-16TS(config-if)# ipv6 mld snooping immediate-leave
```

18.13 ipv6 mld profile

Description

The **ipv6 mld profile** command is used to create the configuration profile. To delete the corresponding profile, please use **no ipv6 mld profile** command.

Syntax

ipv6 mld profile *id*

no ipv6 mld profile *id*

Parameter

id —— Specify the id of the configuration profile, ranging from 1 to 999.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create the profile 1:

```
T1700X-16TS(config)# ipv6 mld profile 1
```

18.14 deny

Description

The **deny** command is used to configure the filtering mode of profile as deny.

Syntax

deny

Command Mode

Profile Configuration Mode

Privilege Requirement

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

Example

Configure the filtering mode of profile 1 as deny:

```
T1700X-16TS(config)# ipv6 mld profile 1
T1700X-16TS(config-MLD-profile)#deny
```

18.15 permit

Description

The **permit** command is used to configure the filtering mode of profile as permit.

Syntax

permit

Command Mode

Profile Configuration Mode

Privilege Requirement

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

Example

Configure the filtering mode of profile 1 as permit:

```
T1700X-16TS(config)# ipv6 mld profile 1
T1700X-16TS(config-igmp-profile)#permit
```

18.16 range

Description

The **range** command is used to configure the range of the profile's filtering multicast address. To delete the corresponding filtering multicast address, please use **no range** command. A profile contains 16 filtering IP-range entries at most.

Syntax

range *start-ip end-ip*

no range *start-ip end-ip*

Parameter

start-ip —— Start IPv6 multicast address of the filter entry..

end-ip —— End IPv6 multicast address of the filter entry.

Command Mode

Profile Configuration Mode

Privilege Requirement

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

Example

Configure one of the filter multicast address entry as range ff80::1234 to ff80::1235 in profile 1:

T1700X-16TS(config)# ipv6 mld profile 1

T1700X-16TS(config-igmp-profile)#range ff80::1234 ff80::1235

18.17 ipv6 mld filter

Description

The **ipv6 mld filter** command is used to bind the specified profile to the interface. To delete the binding, please use **no ipv6 mld filter** command.

Syntax

ipv6 mld filter *profile-id*

no ipv6 mld filter

Parameter

profile-id —— Specify the profile ID, ranging from 1 to 999.

Command Mode

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

Privilege Requirement

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

Example

Bind profile 1 to interface ten-gigabitEthernet 1/0/2:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/2
T1700X-16TS(config-if)# ipv6 mld filter 1
```

18.18 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:

```
T1700X-16TS(config)# clear ipv6 mld snooping statistics
```

18.19 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:

T1700X-16TS(config)# show ipv6 mld snooping

18.20 show ipv6 mld snooping interface

Description

The **show ipv6 mld snooping interface** command is used to display the port configuration of MLD snooping.

Syntax

show ipv6 mld snooping interface [**gigabitEthernet** [*port* | *port-list*]] { basic-config | max-groups | packet-stat }

show ipv6 mld snooping interface [**port-channel** [*port-channel-list*]] { basic-config | max-groups }

Parameter

port —— The Ethernet port number.

port-list —— The list of Ethernet ports.

basic-config | max-groups | packet-stat —— The related configuration information selected to display.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the MLD baisic configuration configuration of all ports and port channels:

T1700X-16TS# show ipv6 mld snooping interface basic-config

Display the MLD basic configuration of port 1/0/2:

T1700X-16TS# show ipv6 mld snooping interface ten-gigabitEthernet 1/0/2 basic-config

Display the MLD packet statistics of ports 1/0/1-4:

T1700X-16TS# show ipv6 mld snooping interface ten-gigabitEthernet 1/0/1-4 packet-stat

18.21 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:

T1700X-16TS(config)# show ipv6 mld snooping vlan

18.22 show ipv6 mld snooping groups

Description

The **show ipv6 mld snooping groups** command is used to display multicast groups.

Syntax

show ipv6 mld snooping groups [**vlan** { *vlan-id* }] [*ipv6_multicast_addr* | count | dynamic | dynamic count | static | static count]

Parameter

vlan-id ——The VLAN ID selected to display the information of all multicast items.

ipv6_multicast_addr —— IPv6 address of the multicast group.

count—— The numbers of all multicast groups.

dynamic—— Display dynamic multicast groups.

dynamic count—— The numbers of all dynamic multicast groups.

static—— Display static multicast groups.

static count—— The numbers of all static multicast groups.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display all of the multicast groups:

```
T1700X-16TS(config)# show ipv6 mld snooping groups
```

18.23 show ipv6 mld profile

Description

The **show ipv6 mld profile** command is used to display the configuration information of all the profiles or a specific profile.

Syntax

show ipv6 mld profile [*id*]

Parameter

id —— Specify the ID of the profile, ranging from 1 to 999.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration information of all profiles:

```
T1700X-16TS(config)# show ipv6 mld profile
```

Chapter 19 MVR Commands

MVR (Multicast VLAN Registration) allows a single multicast VLAN to be shared for multicast member ports in different VLANs in IPv4 network. In IGMP Snooping, if member ports are in different VLANs, a copy of the multicast streams is sent to each VLAN that has member ports. While MVR provides a dedicated multicast VLAN to forward multicast traffic over the Layer 2 network, to avoid duplication of multicast streams for clients in different VLANs. Clients can dynamically join or leave the multicast VLAN without interfering with their relationships in other VLANs.

19.1 mvr (global)

Description

The **mvr** command is used to enable MVR globally. To disable MVR, please use **no mvr** command.

Syntax

mvr

no mvr

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable MVR globally:

```
T1700X-16TS(config)# mvr
```

19.2 mvr group

Description

The **mvr group** command is used to add multicast groups to MVR. To delete multicast groups from MVR, please use **no mvr group** command.

Syntax

mvr group *ip-addr* [*count*]

no mvr group *ip-addr* [*count*]

Parameter

ip-addr —— The start IP address of the contiguous series of multicast groups.

count —— The number of the multicast groups to be added to the MVR. Valid values are from 1 to 256, and the default value is 1.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Add multicast groups 225.1.2.3 -239.1.2.5 to MVR:

T1700X-16TS (config)# mvr group 225.1.2.3 3

19.3 mvr mode

Description

The **mvr mode** command is used to configure the MVR mode as compatible or dynamic. By default, it is compatible. To return to the default configuration, please use **no mvr mode** command.

Syntax

mvr mode { compatible | dynamic **}**

no mvr mode

Parameter

compatible —— In this mode, the switch does not forward report or leave messages from the hosts to the IGMP querier. So the IGMP querier cannot learn the multicast groups membership information from the switch. You have to statically configure the IGMP querier to transmit all the required multicast streams to the switch via the multicast VLAN.

dynamic —— In this mode, after receiving report or leave messages from the hosts, the switch will forward them to the IGMP querier via the multicast VLAN (with appropriate translation of the VLAN ID). So the IGMP querier can learn the multicast groups membership information through the report and leave messages, and transmit the multicast streams to the switch via the multicast VLAN according to the multicast forwarding table.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the MVR mode as dynamic:

```
T1700X-16TS(config)# mvr mode dynamic
```

19.4 mvr querytime

Description

The **mvr querytime** command is used to configure the maximum time to wait for IGMP report on a receiver port before removing the port from multicast group membership. To return to the default configuration, please use **no mvr querytime** command.

Syntax

mvr querytime *time*

no mvr querytime

Parameter

time —— The query response time. Valid values are from 1 to100 tenths of a second, and the default value is 5 tenths of a second.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the query response time of MVR as 1 second, that is 10 tenths of a second:

```
T1700X-16TS(config)# mvr querytime 10
```

19.5 mvr vlan

Description

The **mvr vlan** command is used to specify the multicast VLAN. By default, it is VLAN 1. To return to the default configuration, please use **no mvr vlan** command.

Syntax

mvr vlan *vlan-id*

no mvr vlan

Parameter

vlan-id—— The ID of the multicast VLAN. Valid values are from 1 to 4094.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the multicast VLAN as VLAN 10:

```
T1700X-16TS(config)# mvr vlan 10
```

19.6 mvr (interface)

Description

This command is used to enable MVR for specific interfaces. To disable MVR for the interfaces, please use **no mvr** command. By default, it is disabled.

Syntax

mvr

no mvr

Command Mode

Interface Configuration Mode (interface ten-gigabitEthernet / interface range ten-gigabitEthernet)

Privilege Requirement

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

Example

Enable MVR for port 1/0/1:

T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/1

T1700X-16TS(config-if)#mvr

19.7 mvr type

Description

The **mvr type** command is used to configure the MVR port type as receiver or source. By default, the port is a non-MVR port. If you attempt to configure a non-MVR port with MVR characteristics, the operation fails. To return to the default configuration, please use **no mvr type** command.

Syntax

mvr type { source | receiver **}**

no mvr type

Parameter

source —— Configure the uplink ports that receive and send multicast data on the multicast VLAN as source ports. Source ports should belong to the multicast VLAN.

receiver —— Configure the ports that are connecting to the hosts as receiver ports. A receiver port can only belong to one VLAN, and cannot belong to the multicast VLAN.

Command Mode

Interface Configuration Mode (interface ten-gigabitEthernet / interface range ten-gigabitEthernet)

Privilege Requirement

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

Example

Configure the port 1/0/3 as a receiver port:

T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/3

T1700X-16TS(config-if)#mvr type receiver

19.8 mvr immediate

Description

The **mvr immediate** command is used to enable the Fast Leave feature of MVR for specified port. To disable the Fast Leave feature of MVR for specific ports, please use **no mvr immediate** command.

Syntax

mvr immediate

no mvr immediate

Command Mode

Interface Configuration Mode (interface ten-gigabitEthernet / interface range ten-gigabitEthernet)

Privilege Requirement

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

User Guidelines

Only receiver ports support Fast Leave. Before enabling Fast Leave for a port, make sure there is only a single receiver device connecting to the port.

Example

Enable the Fast Leave feature of MVR for port 1/0/3:

T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/3

T1700X-16TS(config-if)#mvr immediate

19.9 mvr vlan (group)

Description

This command is used to statically add ports to an MVR group. Then the ports can receive multicast traffic sent to the IP multicast address via the multicast VLAN.

Syntax

mvr vlan *vlan-id* **group** *ip-addr*

Parameter

vlan-id—— The ID of the multicast VLAN. Valid values are from 1 to 4094.

ip-addr—— The IP address of the multicast group.

Command Mode

Interface Configuration Mode (interface ten-gigabitEthernet / interface range ten-gigabitEthernet)

Privilege Requirement

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

User Guidelines

This command applies to only receiver ports. The switch adds or removes the receiver ports to the corresponding multicast groups by snooping the report and leave messages from the hosts. You can also statically add a receiver port to an MVR group.

Example

Add port 1/0/3 to MVR group 225.1.2.3 statically. The multicast VLAN is VLAN 10:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/3
T1700X-16TS(config-if)#mvr vlan 10 group 225.1.2.3
```

19.10 show mvr

Description

The **show mvr** command is used to display the global configuration of MVR.

Syntax

show mvr

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of mvr:

```
T1700X-16TS# show mvr
```

19.11 show mvr interface

Description

The **show mvr interface** command is used to display the MVR configurations of specific interfaces.

Syntax

show mvr interface ten-gigabitEthernet [*port* | *port-list*]

Parameter

port——The Ethernet port number.

port-list—— The list of Ethernet ports.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the MVR configuration of port 1/0/3:

T1700X-16TS# show mvr interface ten-gigabitEthernet 1/0/3

19.12 show mvr members

Description

The **show mvr members** command is used to display the membership information of all MVR groups or the specified MVR group.

Syntax

show mvr members [*ip-addr*]

Parameter

ip-addr——The multicast IP address of the MVR group.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the membership information of all MVR groups:

```
T1700X-16TS# show mvr members
```

19.13 show mvr traffic

Description

The **show mvr traffic** command is used to display the statistics information of all MVR groups.

Syntax

show mvr traffic

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the statistics information of all MVR groups:

```
T1700X-16TS# show mvr traffic
```

Chapter 20 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.

20.1 debug spanning-tree

Description

The **debug spanning-tree** command is used to enable debuggning of spanning-tree activities. To disable the debugging function, please use **no debug spanning-tree** command.

Syntax

debug spanning-tree { all | bpdu receive | bpdu transmit | cmpmsg | errors | flush | init | migration | proposals | roles | state | tc }

no debug spanning-tree { all | bpdu receive | bpdu transmit | cmpmsg | errors | flush | init | migration | proposals | roles | state | tc }

Parameters

all —— Display all the spanning-tree debug messages.

bpdu receive —— Display the debug messages of the received spanning-tree bridge protocol data unit (BPDU).

bpdu transmit —— Display the debug messages of the sent spanning-tree BPDU.

cmpmsg —— Display the message priority debug messages.

errors —— Display the MSTP error debug messages.

flush —— Display the address table flushing debug messages.

init —— Display the data structure initialization debug messages.

migration —— Display the version migration debug messages.

proposals —— Display the MSTP handshake debug messages.

roles —— Display the MSTP interface role switchling debug messages.

state —— Display the MSTP interface state change debug messages.

tc —— Display the MSTP topology event debug messages.

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display all the spanning-tree debug messages:

```
T1700X-16TS# debug spanning-tree all
```

20.2 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:

```
T1700X-16TS(config)# spanning-tree
```

20.3 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 ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

Enable the STP function for port 1/0/2:

T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/2

T1700X-16TS(config-if)# spanning-tree

20.4 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 o 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 o to 2000000. By default, it is 0 which is mean auto.

portfast —— Enable/ Disable Edge Port. By default, it is disabled. The edge port can transit its state from blocking to forwarding rapidly without waiting for forward delay.

point-to-point —— The P2P link status, with auto, open and close options. By default, the option is auto. If the two ports in the P2P link are root port or designated port, they can transit their states to forwarding rapidly to reduce the unnecessary forward delay.

Command Mode

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

Privilege Requirement

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

Example

Enable the 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:

T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/1

T1700X-16TS(config-if)# spanning-tree common-config port-priority 64

ext-cost 100 **int-cost** 100 **portfast** enable **point-to-point** open

20.5 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:

```
T1700X-16TS(config)# spanning-tree mode mstp
```

20.6 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:

```
T1700X-16TS(config)# spanning-tree mst configuration
T1700X-16TS(Config-mst)#
```

20.7 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:

```
T1700X-16TS(config)# spanning-tree mst configuration
T1700X-16TS(config-mst)# instance 1 vlan 1-100
```

Disable Instance 1, namely remove all the mapping VLANs 1-100:

```
T1700X-16TS(config)# spanning-tree mst configuration
T1700X-16TS(config-mst)# no instance 1
```

Remove VLANs 1-50 in mapping VLANs 1-100 for Instance 1:

```
T1700X-16TS(config)# spanning-tree mst configuration
T1700X-16TS(config-mst)# no instance 1 vlan 1-50
```

20.8 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":

T1700X-16TS(config)# spanning-tree mst configuration

T1700X-16TS(config-mst)# name region1

20.9 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:

T1700X-16TS(config)# spanning-tree mst configuration

T1700X-16TS(config-mst)# revision 100

20.10 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:

T1700X-16TS(config)# spanning-tree mst instance 1 **priority** 4096

20.11 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 ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

Configure the priority of port 1 in MST Instance 1 as 64, and path cost as 2000:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/1
T1700X-16TS(config-if)# spanning-tree mst instance 1 port-priority 64
cost 2000
```

20.12 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:

T1700X-16TS(config)# spanning-tree priority 4096

20.13 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 * (Forward Delay - 1) >= 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 * (Hello Time + 1) <= 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:

T1700X-16TS(config)# spanning-tree timer forward-time 16 **hello-time** 3 **max-age** 22

20.14 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:

T1700X-16TS(config)# spanning-tree hold-count 8

20.15 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:

T1700X-16TS(config)# spanning-tree max-hops 30

20.16 spanning-tree bpdufilter

Description

The **spanning-tree bpdufilter** 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 bpdufilter** command.

Syntax

spanning-tree bpdufilter

no spanning-tree bpdufilter

Command Mode

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

Privilege Requirement

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

Example

Enable the BPDU filter function for port 1/0/2:

T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/2

T1700X-16TS(config-if)# spanning-tree bpdufilter

20.17 spanning-tree bpduflood

Description

The **spanning-tree bpduflood** command is used to enable the BPDU forward function for a port. With the function enabled, the port still can forward spanning tree BPDUs when the spanning tree function is disabled on this port. To disable the BPDU filter function, please use **no spanning-tree bpduflood** command.

Syntax

spanning-tree bpduflood

no spanning-tree bpduflood

Command Mode

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

Privilege Requirement

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

Example

Enable the BPDU forward function for port 1/0/2:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/2
T1700X-16TS(config-if)# spanning-tree bpduflood
```

20.18 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 ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

Enable the BPDU protect function for port 1/0/2:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/2
T1700X-16TS(config-if)# spanning-tree bpduguard
```

20.19 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 ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

Enable the Loop Protect function for port 2:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/2
T1700X-16TS(config-if)# spanning-tree guard loop
```

20.20 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 ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

Enable the Root Protect function for port 2:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/2
T1700X-16TS(config-if)# spanning-tree guard root
```

20.21 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 ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

Enable the TC Protect of Spanning Tree for port 2:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/2
T1700X-16TS(config-if)# spanning-tree guard tc
```

20.22 spanning-tree mcheck

Description

The **spanning-tree mcheck** command is used to enable mcheck.

Syntax

spanning-tree mcheck

Command Mode

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

Privilege Requirement

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

Example

Enable mcheck for port 2:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/2
T1700X-16TS(config-if)# spanning-tree mcheck
```

20.23 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:

```
T1700X-16TS(config)# show spanning-tree active
```

20.24 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:

```
T1700X-16TS(config)# show spanning-tree bridge
```

20.25 show spanning-tree interface

Description

The **show spanning-tree interface** command is used to display the spanning-tree information of all ports or a specified port.

Syntax

show spanning-tree interface [**gigabitEthernet** *port* | **port-channel** *port-channel-id*] [edge | ext-cost | int-cost | mode | p2p | priority | role | state | status]

Parameter

port—— The Ethernet port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the spanning-tree information of all ports:

T1700X-16TS(config)# show spanning-tree interface

Display the spanning-tree information of port 1/0/2:

T1700X-16TS(config)# show spanning-tree interface ten-gigabitEthernet 1/0/2

Display the spanning-tree mode information of port 1/0/2:

T1700X-16TS(config)# show spanning-tree interface ten-gigabitEthernet 1/0/2 mode

20.26 show spanning-tree interface-security

Description

The **show spanning-tree interface-security** command is used to display the protect information of all ports or a specified port.

Syntax

show spanning-tree interface-security [**gigabitEthernet** *port* | **port-channel** *port-channel-id*] [bpdufilter | bpduflood | bpduguard | loop | root | tc]

Parameter

port—— The Ethernet port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the protect information of all ports:

```
T1700X-16TS(config)# show spanning-tree interface-security
```

Display the protect information of port 1:

```
T1700X-16TS(config)# show spanning-tree interface-security
gigabitEthernet 1/0/1
```

Display the interface security bpdufilter information:

```
T1700X-16TS(config)# show spanning-tree interface-security bpdufilter
```

20.27 show spanning-tree mst

Description

The **show spanning-tree mst** command is used to display the related information of MST Instance.

Syntax

show spanning-tree mst { **configuration** [**digest**] | **instance** *instance-id* [**interface** [**gigabitEthernet** *port* | **port-channel** *port-channel-id*]] }

Parameter

instance-id—— Instance ID desired to show, ranging from 1 to 8.

port—— The Ethernet port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the region information and mapping information of VLAN and MST Instance:

```
T1700X-16TS(config)#show spanning-tree mst configuration
```

Display the related information of MST Instance 1:

T1700X-16TS(config)#show spanning-tree mst instance 1

Display all the ports information of MST Instance 1:

T1700X-16TS(config)#show spanning-tree mst instance 1 **interface**

Chapter 21 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.

21.1 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:

```
T1700X-16TS(config)#lldp
```

21.2 lldp forward_message

Description

The **lldp forward_message** command is used to enable the switch to forward LLDP messages when LLDP function is disabled. To disable the LLDP messages forwarding function, please use **no lldp forward_message** command.

Syntax

lldp forward_message

no lldp forward_message

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the switch to forward LLDP messages when LLDP function is disabled globally:

T1700X-16TS(config)#lldp forward_message

21.3 lldp hold-multiplier

Description

The **lldp hold-multiplier** command is used to configure the Hold Multiplier parameter. The aging time of the local information in the neighbor device is determined by the actual TTL value used in the sending LLDPDU. TTL = Hold Multiplier * 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:

T1700X-16TS(config)#lldp hold-multiplier 5

21.4 lldp timer

Description

The **lldp timer** command is used to configure the parameters about transmission. To return to the default configuration, please use **no lldp timer** command.

Syntax

lldp timer { **tx-interval** *tx-interval* /**tx-delay** *tx-delay* /**reinit-delay** *reinit-delay* /**notify-interval** *notify-interval* /**fast-count** *fast-count* }

no lldp timer { tx-interval | tx-delay | reinit-delay | notify-interval | fast-count }

Parameter

tx-interval —— Configure the interval for the local device to transmit LLDPDU to its neighbors. The value ranges from 5 to 32768 and the default value is 30 seconds.

tx-delay —— Configure a value from 1 to 8192 in seconds to specify the time for the local device to transmit LLDPDU to its neighbors after changes occur so as to prevent LLDPDU being sent frequently. By default, it is 2 seconds.

reinit-delay —— This parameter indicates the amount of delay from when LLDP status becomes "disable" until re-initialization will be attempted. The value ranges from 1 to 10 and the default value is 2.

notify-interval —— Specify the interval of Trap message which will be sent from local device to network management system. The value ranges from 5 to 3600 and the default value is 5 seconds.

fast-count —— When the port's LLDP state transforms from Disable (or Rx_Only) to Tx&Rx (or Tx_Only), the fast start mechanism will be enabled, that is, the transmit interval will be shorten to a second, and several LLDPDUs will be sent out (the number of LLDPDUs equals this parameter). The value ranges from 1 to 10 and the default value is 3.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the Transmit Interval of LLDPDU as 45 seconds and Trap message to NMS as 120 seconds:

T1700X-16TS(config)#lldp timer tx-interval 45

T1700X-16TS(config)#lldp timer notify-interval 120

21.5 lldp receive

Description

The **lldp receive** command is used to enable the designated port to receive LLDPDU. To disable the function, please use **no lldp receive** command.

Syntax

lldp receive

no lldp receive

Command Mode

Interface Configuration Mode (interface ten-gigabitEthernet / interface range ten-gigabitEthernet)

Privilege Requirement

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

Example

Enable port 1/0/1 to receive LLDPDU:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/1

T1700X-16TS(config-if)#lldp receive

21.6 lldp transmit

Description

The **lldp transmit** command is used to enable the designated port to transmit LLDPDU. To disable the function, please use **no lldp transmit** command.

Syntax

lldp transmit

no lldp transmit

Command Mode

Interface Configuration Mode (interface ten-gigabitEthernet / interface range ten-gigabitEthernet)

Privilege Requirement

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

Example

Enable Port 1/0/1 to transmit LLDPDU:

T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/1

T1700X-16TS(config-if)#lldp transmit

21.7 lldp snmp-trap

Description

The **lldp snmp-trap** command is used to enable the port's SNMP notification. If enabled, the port will notify the trap event to network management system. To disable the ports' SNMP notification, please use **no lldp snmp-trap** command.

Syntax

lldp snmp-trap

no lldp snmp-trap

Command Mode

Interface Configuration Mode (interface ten-gigabitEthernet / interface range ten-gigabitEthernet)

Privilege Requirement

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

Example

Enable the SNMP notification for Port 1/0/1:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/1

T1700X-16TS(config-if)#lldp snmp-trap

21.8 lldp tlv-select

Description

The **lldp tlv-select** command is used to configure TLVs to be included in outgoing LLDPDU. To exclude TLVs, please use **no lldp tlv-select** command. By default, All TLVs are included in outgoing LLDPDU.

Syntax

lldp tlv-select { [port-description] [system-capability] [system-description] [system-name] [management-address] [port-vlan] [protocol-vlan] [vlan-name] [link-aggregation] [mac-phy-cfg] [max-frame-size] [power] [all] }

no lldp tlv-select { [port-description] [system-capability] [system-description] [system-name] [management-address] [port-vlan] [protocol-vlan] [vlan-name] [link-aggregation] [mac-phy-cfg] [max-frame-size] [power] [all] }

Command Mode

Interface Configuration Mode (interface ten-gigabitEthernet / interface range ten-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 Port 1/0/1:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/1
T1700X-16TS(config-if)# no lldp tlv-select management-address port-vlan
```

21.9 lldp management-address

Description

The **lldp management-address** command is used to configure the port’s management address to be included in management address TLV. The NMS uses management addresses to identify the devices. To delete the port’s management address, please use **no lldp management address** command.

Syntax

lldp management-address { *ip-address* }

no lldp management-address

Command Mode

Interface Configuration Mode (interface ten-gigabitEthernet / interface range ten-gigabitEthernet)

Privilege Requirement

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

Example

Configure the port's management address as 192.168.1.100 for port 1/0/1:

T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/1

T1700X-16TS(config-if)# lldp management-address 192.168.0.100

21.10 lldp med-fast-count

Description

The **lldp med-fast-count** command is used to configure the number of the LLDP-MED frames that will be sent out. When LLDP-MED fast start mechanism is activated, multiple LLDP-MED frames will be transmitted based on this parameter. The default value is 4. To return to the default configuration, please use **no lldp med-fast-count** command.

Syntax

lldp med-fast-count *count*

no lldp med-fast-count

Parameter

count —— Configure the Fast Start Count parameter. It ranges from 1 to 10. By default, it is 4.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify Fast Start Count as 5:

T1700X-16TS(config)# lldp med-fast-count 5

21.11 lldp med-status

Description

The **lldp med-status** command is used to enable the LLDP-MED feature for the corresponding port. After the LLDP-MED feature is enabled, the port's Admin Status will be changed to Tx&Rx. To disable the LLDP-MED feature for the corresponding port, please use **no lldp med-status** command.

Syntax

lldp med-status

no lldp med-status

Command Mode

Interface Configuration Mode (interface ten-gigabitEthernet / interface range ten-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:

T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/2

T1700X-16TS(config-if)# lldp med-status

21.12 lldp med-tlv-select

Description

The **lldp med-tlv-select** command is used to configure LLDP-MED TLVs to be included in outgoing LLDPDU for the corresponding port. To exclude LLDP-MED TLVs, please use **no lldp med-tlv-select** command. By default, All TLVs are included in outgoing LLDPDU.

Syntax

lldp med-tlv-select { [inventory-management] [location] [network-policy] [power-management] [all] }

no lldp med-tlv-select { [inventory-management] [location] [network-policy] [power-management] [all] }

Command Mode

Interface Configuration Mode (interface ten-gigabitEthernet / interface range ten-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:

T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/2

T1700X-16TS(config-if)# no lldp med-tlv-select network-policy inventory-management

21.13 lldp med-location

Description

The lldp med-location command is used to configure the Location Identification TLV's content in outgoing LLDPDU of the port.

Syntax

lldp med-location { **emergency-number** *identifier* | **civic-address** [[language *language*] [province-state *province-state*] [lci-county-name *county-name*] [lci-city *city*] [street *street*] [house-number *house-number*] [name *name*] [postal-zipcode *postal-zipcode*] [room-number *room-number*] [post-office-box *post-office-box*] [additional *additional*] [country-code *country-code*] [what { dhcp-server | endpoint | switch }]] }

Parameter

emergency-number —— Emergency Call Service ELIN identifier, which is used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. The length of this field ranges from 10 to 25 characters.

civic-address —— The civic address is defined to reuse the relevant sub-fields of the DHCP option for civic Address based Location Configuration Information as specified by IETF.

Command Mode

Interface Configuration Mode (interface ten-gigabitEthernet / interface range ten-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:

T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/2

T1700X-16TS(config-if)# lldp med-location civic-address language English lci-city London

21.14 show lldp

Description

The **show lldp** command is used to display the global configuration of LLDP.

Syntax

show lldp

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of LLDP:

T1700X-16TS#show lldp

21.15 show lldp interface

Description

The **show lldp interface** command is used to display LLDP configuration of the corresponding port. By default, the LLDP configuration of all the ports will be displayed.

Syntax

show lldp interface [**gigabitEthernet** *port*]

Parameters

port—— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the LLDP configuration of Port 1/0/1:

T1700X-16TS#show lldp interface ten-gigabitEthernet 1/0/1

21.16 show lldp local-information interface

Description

The **show lldp local-information interface** command is used to display the LLDP information of the corresponding port. By default, the LLDP information of all the ports will be displayed.

Syntax

show lldp local-information interface [**gigabitEthernet** *port*]

Parameters

port—— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the LLDP information of 1/0/1:

T1700X-16TS#show lldp local-information interface ten-gigabitEthernet 1/0/1

21.17 show lldp neighbor-information interface

Description

The **show lldp neighbor-information interface** command is used to display the neighbor information of the corresponding port. By default, the neighbor information of all the ports will be displayed.

Syntax

show lldp neighbor-information interface [**gigabitEthernet** *port*]

Parameters

port —— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the neighbor information of Port 1/0/1:

```
T1700X-16TS#show lldp neighbor-information interface
ten-gigabitEthernet 1/0/1
```

21.18 show lldp traffic interface

Description

The **show lldp traffic interface** command is used to display the LLDP statistic information between the local device and neighbor device of the corresponding port. By default, the LLDP statistic information of all the ports will be displayed.

Syntax

show lldp traffic interface [**gigabitEthernet** *port*]

Parameters

port —— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the LLDP statistic information of Port 1/0/1:

T1700X-16TS#show lldp traffic interface ten-gigabitEthernet 1/0/1

Chapter 22 Static Routes Commands

22.1 ip routing

Description

This **ip routing** command is used to enable IPv4 routing globally. To disable IPv4 routing, please use the **no ip routing** command.

Syntax

ip routing

no ip routing

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable IPv4 routing feature for the switch:

```
T1700X-16TS(config)# ip routing
```

22.2 interface vlan

Description

This **interface vlan** command is used to create the VLAN interface. To delete the specified VLAN interface, please use the **no interface vlan** command.

Syntax

interface vlan { *vid*}

no interface vlan { *vid*}

Parameter

vid—— The ID of the VLAN.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create the VLAN interface 2:

T1700X-16TS(config)# interface vlan 2

22.3 interface loopback

Description

This **interface loopback** command is used to create the loopback interface. To delete the specified loopback interface, please use the **no interface loopback** command.

Syntax

interface loopback { *id*}

no interface loopback { *id*}

Parameter

id—— The ID of the loopback interface, ranging from 1 to 64.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create the loopback interface 1:

T1700X-16TS(config)# interface loopback 1

22.4 switchport

Description

This **switchport** command is used to switch the Layer 3 interface into the Layer 2 port. To switch the Layer 2 port into the Layer 3 routed port, please use the **no switchport** command.

Syntax

switchport

no switchport

Command Mode

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

Privilege Requirement

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

Example

Switch port 1/0/9 into the routed port:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/9
T1700X-16TS(config-if)# no switchport
```

22.5 interface range port-channel

Description

This **interface range port-channel** command is used to create multiple port-channel interfaces.

Syntax

interface range port-channel *port-channel-list*

Parameter

port-channel-list —— The list of the port-channel interface, ranging from 1 to 14, in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create the port-channel interfaces 1, 3, 4 and 5:

```
T1700X-16TS(config)# interface port-channel 1,3-5
```

22.6 description

Description

This **description** command is used to add a description to the Layer 3 interface, including routed port, port-channel interface, loopback interface and VLAN interface. To clear the description of the corresponding interface, please use the **no description** command.

Syntax

description *string*

no description

Parameter

string —— Content of an interface description, ranging from 1 to 32 characters.

Command Mode

Interface Configuration Mode

Privilege Requirement

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

Example

Add a description system-if to the routed port 1/0/9 :

T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/9
T1700X-16TS(config-if)# no switchport
T1700X-16TS(config-if)# description system-if

22.7 shutdown

Description

This **shutdown** command is used to shut down the specified interface. The interface type include: routed port, port-channel interface, loopback interface and VLAN interface. To enable the specified interface, please use the **no shutdown** command.

Syntax

shutdown

no shutdown

Command Mode

Interface Configuration Mode

Privilege Requirement

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

Example

Shut down the routed port 1/0/9:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/9
T1700X-16TS(config-if)# no switchport
T1700X-16TS(config-if)# shutdown
```

22.8 interface port-channel

Description

This **interface port-channel** command is used to create the port-channel interface. To delete the specified port-channel interface, please use the **no interface port-channel** command.

Syntax

interface port-channel { *port-channel-id* }

no interface port-channel { *port-channel-id* }

Parameter

port-channel-id —— The ID of the port-channel interface, ranging from 1 to 14.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create the port-channel interface 1:

```
T1700X-16TS(config)# interface port-channel 1
```

22.9 ip route

Description

This **ip route** command is configure the static route. To clear the corresponding entry, please use the **no ip route** command.

Syntax

ip route { *dest-address* } { *mask* } { *next-hop-address* } [*distance*]

no ip route { *dest-address* } { *mask* } { *next-hop-address* }

Parameter

dest-address —— The destination IP address.

mask —— The subnet mask.

next-hop-address —— The address of the next-hop.

distance —— The distance metric of this route, ranging from 1 to 255. The smaller the distance is, the higher the priority is.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create a static route with the destination IP address as 192.168.2.0, the subnet mask as 255.255.255.0 and the next-hop address as 192.168.0.2:

T1700X-16TS(config)# ip route 192.168.2.0 255.255.255.0 192.168.0.2

22.10 ipv6 routing

Description

This **ipv6 routing** command is enale the IPv6 routing feature globally. To diable IPv6 routing, please use the **no ipv6 routing** command.

Syntax

ipv6 routing

no ipv6 routing

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable IPv6 routing globally:

T1700X-16TS(config)# ipv6 routing

22.11 ipv6 route

Description

This **ipv6 route** command is configure the IPv6 static route. To clear the corresponding entry, please use the **no ipv6 route** command.

Syntax

ipv6 route { *ipv6-dest-address* } { *next-hop-address* } [*distance*]

no ipv6 route { *ipv6-dest-address* } { *next-hop-address* }

Parameter

ipv6-dest-address—— The IPv6 address of the destination network.

next-hop-address —— The IPv6 address of the next-hop.

distance —— The distance metric of this route, ranging from 1 to 255. The smaller the distance is, the higher the priority is.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create a static route with the destination network IP address as 3200::/64 and the next-hop address as 3100::1234:

T1700X-16TS(config)# ipv6 route 3200::/64 3100::1234

22.12 show interface vlan

Description

The **show interface vlan** command is used to display the information of the specified interface VLAN.

Syntax

show interface vlan *vid*

Parameter

vid—— The VLAN ID.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of VLAN 2:

```
T1700X-16TS(config)#show interface vlan 2
```

22.13 show ip interface

Description

This **show ip interface** command is used to display the detailed information of the specified Layer 3 interface.

Syntax

show ip interface [**gigabitEthernet** *port* / **port-channel** *port-channel-id* / **loopback** *id*| **vlan** *vlan-id*]

Parameter

port—— The port number.

port-channel-id —— The ID of the port channel. Member ports in this port channel should all be routed ports.

id—— The loopback interface ID.

vlan-id—— The VLAN interface ID.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the detailed information of the VLAN interface 2:

T1700X-16TS(config)# show ip interface vlan 2

22.14 show ip interface brief

Description

This **show ip interface brief** command is used to display the summary information of the Layer 3 interfaces.

Syntax

show ip interface brief

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the summary information of the Layer 3 interfaces:

T1700X-16TS(config)# show ip interface brief

22.15 show ip route

Description

This **show ip route** command is used to display the route entries of the specified type.

Syntax

show ip route [static | connected]

Parameter

static | connected —— Specify the route type. If not specified, all types of route entries will be displayed.

static: The static routes.

connected: The connected routes.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the static routes:

T1700X-16TS(config)# show ip route static

22.16 show ip route specify

Description

This **show ip route specify** command is used to display the valid routing information to the specified IP address or network segments.

Syntax

show ip route specify { *ip* } [*mask*] [**longer-prefixes**]

Parameter

ip —— Specify the destination IP address.

mask —— Specify the destination IP address together with the parameter *ip*.

longer-prefixes —— Specify the destination subnets that match the network segment determined by the ip and mask parameters.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the shortest route to 192.168.0.100:

T1700X-16TS(config)# show ip route specify 192.168.0.100

Look up the route entry with the destination as 192.168.0.0/24:

T1700X-16TS(config)# show ip route specify 192.168.0.0 255.255.255.0

Display the routes to all the subnets that belongs to 192.168.0.0/16:

T1700X-16TS(config)# show ip route specify 192.168.0.0 255.255.0.0 **longer-prefixes**

22.17 show ip route summary

Description

This **show ip route summary** command is used to display the summary information of the route entries classified by their sources.

Syntax

show ip route summary

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the summary information of route entries:

T1700X-16TS(config)# show ip route summary

22.18 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:

T1700X-16TS(config)# show ipv6 interface

22.19 show ipv6 route

Description

This **show ipv6 route** command is used to display the IPv6 route entries of the specified type.

Syntax

show ipv6 route [static | connected]

Parameter

static | connected —— Specify the route type. If not specified, all types of route entries will be displayed.

static: The static routes.

connected: The connected routes.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IPv6 static routes:

T1700X-16TS(config)# show ipv6 route static

22.20 show ipv6 route summary

Description

This **show ipv6 route summary** command is used to display the summary information of the IPv6 route entries classified by their sources.

Syntax

show ipv6 route summary

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the summary information of IPv6 route entries:

```
T1700X-16TS(config)# show ipv6 route summary
```

Chapter 23 IPv6 Address Configuration Commands

The IPv6 address configuration commands are provided in the Interface Configuration Mode, which includes the routed port, the port-channel interface and the VLAN interface. Enter the configuration mode of these Layer 3 interfaces and configure their IPv6 parameters.

23.1 ipv6 enable

Description

This command is used to enable the IPv6 function on the specified Layer 3 interface. IPv6 function should be enabled before the IPv6 address configuration management. By default it is enabled on VLAN interface 1. IPv6 function can only be enabled on one Layer 3 interface at a time.

If the IPv6 function is disabled, the corresponding IPv6-based modules will be invalid, for example SSHv6, SSLv6, TFTPv6 and more. To disable the IPv6 function, please use **no ipv6 enable** command.

Syntax

ipv6 enable

no ipv6 enable

Command Mode

Interface Configuration Mode

Privilege Requirement

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

Example

Enable the IPv6 function on the VLAN interface 1：

```
T1700X-16TS(config)# interface vlan 1
T1700X-16TS(config-if)# ipv6 enable
```

23.2 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 autu-configured ipv6 link-local address is in EUI-64 format. To verify the uniqueness of the link-local address, the manually configured ipv6 link-local address will be deleted when the auto-configured ipv6 link-local address takes effect.

Syntax

ipv6 address autoconfig

Configuration Mode

Interface Configuration Mode

Privilege Requirement

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

Example

Enable the automatic configuration of the ipv6 link-local address on VLAN interface 1:

T1700X-16TS(config)# interface vlan 1

T1700X-16TS(config-if)# ipv6 address autoconfig

23.3 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:

T1700X-16TS(config)# interface vlan 1

T1700X-16TS(config-if)# ipv6 address fe80::1234 **link-local**

23.4 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:

T1700X-16TS(config)# interface vlan 1

T1700X-16TS(config-if)# ipv6 address dhcp

23.5 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:

T1700X-16TS(config)# interface vlan 1

T1700X-16TS(config-if)# ipv6 address ra

23.6 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 a EUI-64 IPv6 address from the interface, please use the **no ipv6 address eui-64** command.

Syntax

ipv6 address *ipv6-addr* **eui-64**

no ipv6 address *ipv6-addr* **eui-64**

Parameter

ipv6-addr —— Global IPv6 address with 64 bits network prefix, for example 3ffe::/64.

Configuration Mode

Interface Configuration Mode

Privilege Requirement

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

Example

Configure an EUI-64 global address on the interface with the network prefix 3ffe::/64:

T1700X-16TS(config)# interface vlan 1

T1700X-16TS(config-if)# ipv6 address 3ffe::/64 **eui-64**

23.7 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:

T1700X-16TS(config)# interface vlan 1

T1700X-16TS(config-if)# ipv6 address 3001::1/64

23.8 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:

```
T1700X-16TS(config)# show ipv6 interface
```

Chapter 24 ARP Commands

Address Resolution Protocol (ARP) is used to resolve an IP address into an Ethernet MAC address. The switch maintains an ARP mapping table to record the IP-to-MAC mapping relations, which is used for forwarding packets. An ARP mapping table contains two types of ARP entries: dynamic and static. An ARP dynamic entry is automatically created and maintained by ARP. A static ARP entry is manually configured and maintained.

24.1 arp

Description

This **arp** command is used to add a static ARP entry. To delete the specified ARP entry, please use the **no arp** command.

Syntax

arp *ip mac type*

no arp *ip type*

Parameter

ip —— The IP address of the static ARP entry.

mac —— The MAC address of the static ARP entry.

type —— The ARP type. Configure it as "arpa".

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create a static ARP entry with the IP as 192.168.0.1 and the MAC as 00:11:22:33:44:55:

```
T1700X-16TS(config)# arp 192.168.0.1 00:11:22:33:44:55 arpa
```

24.2 clear arp-cache

Description

This **clear arp-cache** command is used to clear all the dynamic ARP entries.

Syntax

clear arp-cache

Command Mode

Privileged EXEC Mode

Privilege Requirement

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

Example

Clear all the dynamic ARP entries:

```
T1700X-16TS(config)# clear arp-cache
```

24.3 arp dynamicrenew

Description

This **arp dynamicrenew** command is used to automatically renew dynamic ARP entries. To disable the switch to automatically renew dynamic ARP entries, please use the **no arp dynamicremew** command. By default, it is enabled.

Syntax

arp dynamicremew

no arp dynamicremew

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the switch to automatically renew the dynamic ARP entries:

```
T1700X-16TS(config)# arp dynamicrenew
```

24.4 arp timeout

Description

This **arp timeout** command is used to configure the ARP aging time of the interface.

Syntax

arp timeout *timeout*

no arp timeout

Parameter

timeout —— Specify the aging time, ranging from 10 to 3000 seconds. The default value is 1200 seconds.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the ARP aging time as 60 seconds:

```
T1700X-16TS(config)# arp timeout 60
```

24.5 gratuitous-arp intf-status-up enable

Description

This **gratuitous-arp intf-status-up enable** command is used to enable the Layer 3 interface to send a gratuitous ARP packet when the interface's status becomes up.

Syntax

gratuitous-arp intf-status-up enable

no gratuitous-arp intf-status-up enable

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Enable the switch's Layer 3 interfaces to send gratuitous ARP packets when their status becomes up:

```
T1700X-16TS(config)# gratuitous-arp intf-status-up enable
```

24.6 gratuitous-arp dup-ip-detected enable

Description

This **gratuitous-arp dup-ip-detected enable** command is used to enable the Layer 3 interface to send a gratuitous ARP packet when receiving a gratuitous packets of which the IP address is the same as its own.

Syntax

gratuitous-arp dup-ip-detected enable

no gratuitous-arp dup-ip-detected enable

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Enable the switch's Layer 3 interface to send gratuitous ARP packets when receiving a gratuitous packets of which the IP address is the same as its own:

```
T1700X-16TS(config)# gratuitous-arp dup-ip-detected enable
```

24.7 gratuitous-arp learning enable

Description

This **gratuitous-arp learning enable** command is used to enable the Layer 3 interface to learn MAC addresses from the gratuitous ARP packets.

Syntax

gratuitous-arp learning enable

no gratuitous-arp learning enable

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Enable the Layer 3 interface to learn MAC addresses from the gratuitous ARP packets:

```
T1700X-16TS(config)# gratuitous-arp learning enable
```

24.8 gratuitous-arp send-interval

Description

This **gratuitous-arp send-interval** command is used to configure the interval at which the interface periodically send the gratuitous ARP packets.

Syntax

gratuitous-arp send-interval *interval*

Parameter

Interval —— Specify the interval at which the interface periodically send the gratuitous ARP packets. Value 0 means the interface will not send gratuitous ARP packets.

Command Mode

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

Privilege Requirement

None.

Example

Specify the interface VLAN 1 to send gratuitous ARP packets every 1 second:

```
T1700X-16TS(config)# interface vlan 1
T1700X-16TS(config-if)# gratuitous-arp send-interval 1
```

24.9 ip proxy-arp

Description

The **ip proxy-arp** command is used to enable Proxy ARP function on the specified VLAN interface or routed port. To disable Proxy ARP on this interface, please use **no ip proxy-arp** command.

Syntax

ip proxy-arp
no ip proxy-arp

Command Mode

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

Privilege Requirement

None

Example

Enable the Proxy ARP function on VLAN Interface 2:

```
T1700X-16TS(config)# interface vlan 2
T1700X-16TS(config-if)# ip proxy-arp
```

Enable the Proxy ARP function on routed port 1/0/2:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 2
T1700X-16TS(config-if)# no switchport
T1700X-16TS(config-if)# ip proxy-arp
```

24.10 ip local-proxy-arp

Description

The **ip local-proxy-arp** command is used to enable Local Proxy ARP function on the specified VLAN interface or routed port. To disable Local Proxy ARP function on this interface, please use **no ip local-proxy-arp** command.

Syntax

ip local-proxy-arp
no ip local-proxy-arp

Command Mode

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

Privilege Requirement

None

Example

Enable the Proxy ARP function on VLAN Interface 2:

```
T1700X-16TS(config)# interface vlan 2
T1700X-16TS(config-if)# ip local-proxy-arp
```

Enable the Proxy ARP function on routed port 1/0/2:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 2
T1700X-16TS(config-if)# no switchport
T1700X-16TS(config-if)# ip local-proxy-arp
```

24.11 show arp

Description

This **show arp** command is used to display the active ARP entries. If no parameter is speicified, all the active ARP entries will be displayed.

Syntax

show arp [*ip*] [*mac*]

Parameter

ip —— Specify the IP address of your desired ARP entry.

mac —— Specify the MAC address of your desired ARP entry.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the ARP entry with the IP as 192.168.0.2:

T1700X-16TS(config)# show arp 192.168.0.2

24.12 show ip arp (interface)

Description

This **show ip arp (interface)** command is used to display the active ARP entries associated with a specified Layer 3 interface.

Syntax

show ip arp { **gigabitEthernet** *port* | **port-channel** *port-channel-id* | **vlan** *id* }

Parameter

port —— Specify the number of the routed port.

port-channel-id —— Specify the ID of the port channel.

id —— Specify the VLAN interface ID.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the ARP entry associated with VLAN interface 2:

T1700X-16TS(config)# show ip arp vlan 2

24.13 show ip arp summary

Description

This **show ip arp summary** command is used to display the number of the active ARP entries.

Syntax

show ip arp summary

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the number of the ARP entries:

```
T1700X-16TS(config)# show ip arp summary
```

24.14 show gratuitous-arp

Description

This **show gratuitous arp** command is used to display the configuration of gratuitous ARP.

Syntax

show gratuitous-arp

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of gratuitous ARP:

```
T1700X-16TS(config)# show gratuitous-arp
```

24.15 show ip proxy-arp

Description

The **show ip proxy-arp** command is used to display the Proxy ARP status.

Syntax

show ip proxy-arp

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None

Example

Display the Proxy ARP status:

```
T1700X-16TS(config)# show ip proxy-arp
```

Chapter 25 DHCP Server Commands

DHCP (Dynamic Host Configuration Protocol) is a network configuration protocol for hosts on TCP/IP networks, and it provides a framework for distributing configuration information to hosts. DHCP server assigns IP addresses from specified address pools on a switch or router to DHCP clients and manages them.

25.1 service dhcp server

Description

The **service dhcp server** command is used to enable DHCP service globally. To disable DHCP server service, please use **no service dhcp server** command.

Syntax

service dhcp server

no service dhcp server

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable DHCP server service globally:

```
T1700X-16TS(config)# service dhcp server
```

25.2 ip dhcp server extend-option capwap-ac-ip

Description

The **ip dhcp server extend-option capwap-ac-ip** command is used to configure the IP address of the remote DHCP server. To delete the remote DHCP server's IP address, please use **no ip dhcp server extend-option capwap-ac-ip** command.

Syntax

ip dhcp server extend-option capwap-ac-ip *ip-address*

no ip dhcp server extend-option capwap-ac-ip

Parameter

ip-address —— Specify the IP address of the remote server.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Set the remote DHCP server's IP address as 192.168.3.1:

T1700X-16TS(config)# ip dhcp server extend-option capwap-ac-ip 192.168.3.1

25.3 ip dhcp server extend-option vendor-class-id

Description

The **ip dhcp server extend-option vendor-class-id** command is used to configure the class ID of the packets from DHCP server in a different network segment. To delete the class ID settings, please use **no ip dhcp server extend-option vendor-class-id** command.

Syntax

ip dhcp server extend-option vendor-class-id *class-id*

no ip dhcp server extend-option vendor-class-id

Parameter

class-id —— Specify the class ID of the DHCP packets from another network segment.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Set the class ID of the DHCP packets from another network segment as 34:

T1700X-16TS(config)# ip dhcp server extend-option vendor-class-id 34

25.4 ip dhcp server exclude-address

Description

The **ip dhcp server exclude-address** command is used to specify the reserved IP addresses which are forbidden to allocate, such as the gateway address, the network segment broadcast address, the server address etc. To delete the reserved IP addresses, please use **no ip dhcp server exclude-address** command.

Syntax

ip dhcp server exclude-address *start-ip-address end-ip-address*

no ip dhcp server exclude-address *start-ip-addr end-ip-address*

Parameter

start-ip-address —— Specify the start IP address of the reserved IP pool.

end-ip-address —— Specify the end IP address of the reserved IP pool. Only one IP address will be reserved if the end IP address and the start IP address are the same.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Set the reserved IP addresses from 192.168.1.1 to 192.168.1.9:

```
T1700X-16TS(config)# ip dhcp server exclude-address 192.168.1.1 192.168.1.9
```

25.5 ip dhcp server pool

Description

The **ip dhcp server pool** command is used to create the address pool of DHCP Server and enter the dhcp configuration mode. To delete the address pool, please use **no ip dhcp server pool** command.

Syntax

ip dhcp server pool *pool-name*

no ip dhcp server pool *pool-name*

Parameter

pool-name —— Specify the address pool name, ranging from 1 to 8 characters.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create the address pool of name POOL1:

T1700X-16TS(config)# ip dhcp server pool POOL1

25.6 ip dhcp server ping timeout

Description

The **ip dhcp server ping timeout** command is used to specify the timeout of PING process. To resume the default value, please use **no ip dhcp server ping timeout** command.

Syntax

ip dhcp server ping timeout *value*

no ip dhcp server ping timeout

Parameter

value —— Specify the timeout value, ranging from 100 to 10000ms. The default value is 100ms.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Set the timeout of PING as 200ms:

T1700X-16TS(config)# ip dhcp server ping timeout 200

25.7 ip dhcp server ping packets

Description

The **ip dhcp server ping packets** command is used to specify the number of PING packets sent. If this value is set to 0, the PING process will be disabled. To resume the default value, please use **no ip dhcp server ping packets** command.

Syntax

ip dhcp server ping packets *num*

Parameter

num —— Specify the PING packets' number, ranging from 0 to 10. By default it's 1.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the PING packets' number as 2:

T1700X-16TS(config)# ip dhcp server ping packets 2

25.8 network

Description

The **network** command is used to specify the address and subnet of the network pool.

Syntax

network *network-address subnet-mask*

Parameter

network-address —— Specify the network address of the pool, with the format A.B.C.D. All the IP addresses in the same subnet are allocatable except the reserved addresses and specific addresses.

subnet-mask —— Specify the subnet mask of the pool, with the format A.B.C.D.

Command Mode

DHCP Configuration Mode

Privilege Requirement

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

Example

Specify the address pool "product" as 192.168.1.0 255.255.255.0:

T1700X-16TS(config)# ip dhcp server pool product

T1700X-16TS(config-dhcp)# network 192.168.1.0 255.255.255.0

25.9 lease

Description

The **lease** command is used to specify the lease time of the address pool.

Syntax

lease *lease-time*

Parameter

lease-time —— Specify the lease time of the pool, ranging from 1 to 2880 minutes. The default value is 120 minutes.

Command Mode

DHCP Configuration Mode

Privilege Requirement

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

Example

Specify the lease time of address pool "product" as 10 minutes:

T1700X-16TS(config)# ip dhcp server pool product

T1700X-16TS(config-dhcp)# lease 10

25.10 address hardware-address

Description

The **address hardware-address** command is used to reserve the static address bound with hardware address in the address pool. To delete the binding, please use **no address hardware-address**.

Syntax

address *ip-address* **hardware-address** *hardware-address* **hardware-type** { ethernet | ieee802 }

no address *ip-address*

Parameter

ip-address —— Specify the static binding IP address.

hardware-address —— Specify the hardware address, in the format XX:XX:XX:XX:XX:XX.

ethernet | ieee802 —— Specify the hardware type.

Command Mode

DHCP Configuration Mode

Privilege Requirement

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

Example

Reserve the IP address 192.168.0.10 in the address pool "product" for the device with the MAC address as 5e:4c:a6:31:24:01 and the hardware type as ethernet:

T1700X-16TS(config)# ip dhcp server pool product

T1700X-16TS(config-dhcp)# address 192.168.0.10 **hardware-address** 5e:4c:a6:31:24:01 **hardware-type** ethernet

25.11 address client-identifier

Description

The **address client-identifier** command is used to specify the static address bound with client ID in the address pool. To delete the binding, please use **no address** command.

Syntax

address *ip-address* **client-identifier** *client-id* [**ascii**]

no address *ip-address*

Parameter

ip-address —— Specify the static binding IP address.

client-id —— Specify the client ID, in the format of hex value.

ascii —— The client ID is entered with ASCII characters.

Command Mode

DHCP Configuration Mode

Privilege Requirement

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

Example

Reserve the IP address 192.168.0.10 in the address pool "product" for the device with the client ID as abc in ASCII:

T1700X-16TS(config)# ip dhcp pool product

T1700X-16TS(dhcp-config)# address 192.168.0.10 **client-identifier** abc **ascii**

25.12 default-gateway

Description

The **default-gateway** command is used to specify the default gateway of the address pool. To delete the configuration, please use **no default-gateway**.

Syntax

default-gateway *gateway-list*

no default-gateway

Parameter

gateway-list —— Specify the gateway list, with the format of A.B.C.D,E.F.G.H. At most 8 gateways can be configured, separated by comma.

Command Mode

DHCP Configuration Mode

Privilege Requirement

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

Example

Specify the address pool product's default gateways as 192.168.0.1 and 192.168.1.1:

T1700X-16TS(config)# ip dhcp server pool product

T1700X-16TS(dhcp-config)# default-gateway 192.168.0.1,192.168.1.1

25.13 dns-server

Description

The **dns-server** command is used to specify the DNS server of the address pool. To delete this configuration, please use **no dns-server** command.

Syntax

dns-server *dns-list*

no dns-server

Parameter

dns-list —— Specify the DNS server list, with the format of A.B.C.D,E.F.G.H. At most 8 DNS servers can be configured, separated by comma.

Command Mode

DHCP Configuration Mode

Privilege Requirement

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

Example

Specify the address pool's DNS servers as 192.168.0.1 and 192.168.1.1:

T1700X-16TS(config)# ip dhcp server pool product

T1700X-16TS(config-dhcp)# dns-server 192.168.0.1,192.168.1.1

25.14 netbios-name-server

Description

The **netbios-name-server** command is used to specify the Netbios server's IP address. To delete the Netbios servers, please use **no netbios-name-server** command.

Syntax

netbios-name-server *NBNS-list*

no netbios-name-server

Parameter

NBNS-list —— Specify the Netbios server list, with the format of A.B.C.D,E.F.G.H. At most 8 Netbios servers can be configured, separated by comma.

Command Mode

DHCP Configuration Mode

Privilege Requirement

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

Example

Specify the address pool's Netbios servers as 192.168.0.1 and 192.168.1.1:

T1700X-16TS(config)# ip dhcp server pool product

T1700X-16TS(config-dhcp)# netbios-name-server 192.168.0.1,192.168.1.1

25.15 netbios-node-type

Description

The **netbios-node-type** command is used to specify the Netbios server's node type. To delete the node type setttings, please use **no netbios-node-type** command.

Syntax

netbios-node-type *type*

no netbios-node-type

Parameter

type —— Specify the node type as b-node, h-node, m-node or p-node.

Command Mode

DHCP Configuration Mode

Privilege Requirement

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

Example

Specify the address pool's Netbios server type as b-node:

T1700X-16TS(config)# ip dhcp server pool product

T1700X-16TS(config-dhcp)# netbios-node-type b-node

25.16 next-server

Description

The **next-server** command is used to specify the next DHCP server's address during the DHCP boot process. To delete the next server, please use **no next-server** command.

Syntax

next-server *ip-address*

next-server

Parameter

ip-address —— Specify the IP address of the next server.

Command Mode

DHCP Configuration Mode

Privilege Requirement

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

Example

Specify the next server's IP address as 192.168.2.1:

T1700X-16TS(config)# ip dhcp server pool product

T1700X-16TS(config-dhcp)# next-server 192.168.2.1

25.17 domain-name

Description

The **domain-name** command is used to specify the domain name for the DHCP client. To delete the domain name, please use **no domain-name** command.

Syntax

domain-name *domainname*

no domain-name

Parameter

domainname —— Specify the domain name for the DHCP client.

Command Mode

DHCP Configuration Mode

Privilege Requirement

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

Example

Specify the DHCP client's domain name as edu:

T1700X-16TS(config)# ip dhcp server pool product

T1700X-16TS(config-dhcp)# domain-name edu

25.18 bootfile

Description

The **bootfile**command is used to specify the name of the DHCP client's bootfile. To delete the bootfile, please use **no bootfile** command.

Syntax

bootfile *file-name*

no bootfile

Parameter

file-name —— Specify the name of the DHCP client's bootfile.

Command Mode

DHCP Configuration Mode

Privilege Requirement

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

Example

Specify the name of the DHCP client's bootfile as boot1:

T1700X-16TS(config)# ip dhcp server pool product

T1700X-16TS(config-dhcp)# bootfile boot1

25.19 show ip dhcp server status

Description

The **show ip dhcp server status** command is used to display the status of the DHCP service.

Syntax

show ip dhcp server status

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the status of DHCP service:

T1700X-16TS(config)# show ip dhcp server status

25.20 show ip dhcp server statistics

Description

The **show ip dhcp server statistics** command is used to display the DHCP packets received and sent by DHCP server.

Syntax

show ip dhcp server statistics

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the statistics of DHCP packets received and sent by the DHCP server:

```
T1700X-16TS(config)# show ip dhcp server statistics
```

25.21 show ip dhcp server extend-option

Description

The **show ip dhcp server extend-option** command is used to display the configuration of the remote DCHP servers.

Syntax

show ip dhcp server extend-option

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configurations of the remote DCHP servers:

```
T1700X-16TS(config)# show ip dhcp server extend-option
```

25.22 show ip dhcp server pool

Description

The **show ip dhcp server pool** command is used to display the configuration of the address pool.

Syntax

show ip dhcp server pool

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configured address pool:

```
T1700X-16TS(config)# show ip dhcp server pool
```

25.23 show ip dhcp server excluded-address

Description

The **show ip dhcp server excluded-address** command is used to display the configuration of reserved addresses.

Syntax

show ip dhcp server excluded-address

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configured reserved addresses:

```
T1700X-16TS(config)# show ip dhcp server excluded-address
```

25.24 show ip dhcp server manual-binding

Description

The **show ip dhcp server manual-binding** command is used to display the configuration of static binding address.

Syntax

show ip dhcp server manual-binding

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configured static binding address:

```
T1700X-16TS(config)# show ip dhcp server manual-binding
```

25.25 show ip dhcp server binding

Description

The **show ip dhcp server binding** command is used to display the binding entries.

Syntax

show ip dhcp server binding [**ip** *ip-address*]

Parameter

ip-address —— Specify the binding IP address.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the address binding entries:

```
T1700X-16TS(config)# show ip dhcp server binding
```

25.26 clear ip dhcp server statistics

Description

The **clear ip dhcp server statistics** command is used to clear the statistics information of DHCP packets.

Syntax

clear ip dhcp server statistics

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

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

Example

Clear the packet statistics:

```
T1700X-16TS(config)# clear ip dhcp server statistics
```

25.27 clear ip dhcp server binding

Description

The **clear ip dhcp server binding** command is used to clear the binding information.

Syntax

clear ip dhcp server binding [*ip-address*]

Parameter

ip-address —— Specify the binding IP address.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

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

Example

Clear all the binding addresses:

```
T1700X-16TS(config)# clear ip dhcp server binding
```

Chapter 26 DHCP Relay Commands

A DHCP Relay agent is a Layer 3 device that forwards DHCP packets between clients and servers. DHCP Relay forward requests and replies between clients and servers when they are not on the same physical subnet.

26.1 service dhcp relay

Description

The **service dhcp relay** command is used to enable DHCP Relay function globally. To disable DHCP Relay function, please use **no service dhcp relay** command.

Syntax

service dhcp relay

no service dhcp relay

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable DHCP Relay function globally:

```
T1700X-16TS(config)# service dhcp relay
```

26.2 ip dhcp relay hops

Description

The **ip dhcp relay hops** command is used to specify the maximum hops (DHCP Relay agent) that the DHCP packets can be relayed. To restore the default value, please use **no service dhcp relay hops** command.

Syntax

ip dhcp relay hops *hops*

no ip dhcp relay hops

Parameter

hops ——Specify the maximum hops (DHCP Relay agent) that the DHCP packets can be relayed. If a packet's hop count is more than the value you set here, the packet will be dropped. The valid value ranges from the 1 to 16, and the default value is 4.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the maximum number of relay hops as 6:

T1700X-16TS(config)# ip dhcp relay hops 6

26.3 ip dhcp relay time

Description

The **ip dhcp relay time** command is used to specify the DHCP relay time threshold. DHCP relay time is the time elapsed since client began address acquisition or renewal process. When the elapsed time of the DHCP packet is greater than the value set here, the DHCP packet will be dropped by the switch. To restore the default value, please use **no service dhcp relay time** command.

Syntax

ip dhcp relay time *time*

no ip dhcp relay time

Parameter

time ——Specify the DHCP relay time threshold. The valid value ranges from 1 to 65535. The default value is 0, which means the switch will not examine this field of the DHCP packets.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the DHCP Relay time as 30 seconds:

T1700X-16TS(config)# ip dhcp relay time 30

26.4 ip helper-address

Description

The **ip helper-address** command is used to add DHCP Server address to the Layer 3 interface. To delete the server address, please use **no ip helper-address** command.

Syntax

ip helper-address *ip-address*

no ip helper-address [*ip-address*]

Parameter

ip-address —— DHCP Server address.

Command Mode

Interface Configuration Mode

Privilege Requirement

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

Example

Add DHCP Server address 192.168.2.1 to interface VLAN 1:

T1700X-16TS(config)# interface vlan 1

T1700X-16TS(config-if)# ip helper-address 192.168.2.1

26.5 ip dhcp relay information

Description

The **ip dhcp relay information** command is used to enable option 82 support in DHCP Relay. To disable this function, please use **no ip dhcp relay information** command.

Syntax

ip dhcp relay information

no ip dhcp relay information

Command Mode

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

Privilege Requirement

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

Example

Enable option 82 support in DHCP Relay for port 2:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/2

T1700X-16TS(config-if)# ip dhcp relay information

26.6 ip dhcp relay information strategy

Description

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

Syntax

ip dhcp relay information strategy { drop | keep | replace }

no ip dhcp relay information strategy

Parameter

drop | keep | replace ——The operations for Option 82 field of the DHCP request packets from the Host. The default operation is keep.

drop: Discard the packet with the Option 82 field.

keep: Keep the Option 82 field in the packet.

replace: Replace the option 82 field with the system option defined by the switch.

Command Mode

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

Privilege Requirement

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

Example

Specify the option 82 strategy as replace to replace the Option 82 field with the local parameter on receiving the DHCP request packet for port 2:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/2

T1700X-16TS(config-if)# ip dhcp relay information strategy replace

26.7 ip dhcp relay information format

Description

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

Syntax

ip dhcp relay information format { normal | private }

no ip dhcp relay information format

Parameter

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

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

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

Command Mode

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

Privilege Requirement

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

Example

Select the format of option 82 sub-option value field as TLV (type-length-value) for port 2:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/2

T1700X-16TS(config-if)#ip dhcp relay information format normal

26.8 ip dhcp relay information circuit-id

Description

The **ip dhcp relay information circuit-id** command is used to specify the custom circuit ID when option 82 customization is enabled. To clear the circuit ID, please use **no ip dhcp relay information circuit-id** command.

Syntax

ip dhcp relay information circuit-id *circuitID*

no ip dhcp relay information circuit-id

Parameter

circuitID —— Specify the circuit ID, ranging from 1 to 64 characters.

Command Mode

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

Privilege Requirement

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

Example

Specify the circuit ID as "TP-Link" for port 2:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/2

T1700X-16TS(config-if)# ip dhcp relay information circuit-id TP-Link

26.9 ip dhcp relay information remote-id

Description

The **ip dhcp relay information remote-id** command is used to specify the custom remote ID when option 82 customization is enabled. To clear the remote ID, please use **no ip dhcp relay information remote-id** command.

Syntax

ip dhcp relay information remote-id *remoteID*

no ip dhcp relay information remote-id

Parameter

remoteID —— Specify the remote ID, ranging from 1 to 64 characters.

Command Mode

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

Privilege Requirement

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

Example

Specify the remote ID as "TP-Link" for port 2:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/2

T1700X-16TS(config-if)# ip dhcp relay information remote-id TP-Link

26.10 ip dhcp relay default-interface

Description

The **ip dhcp relay default-interface** command is used to configure default relay agent interface. When the switch works at DHCP VLAN Relay mode and there is no IP interface in the VLAN, the switch uses the IP of default relay agent interface to fill in the relay agent IP address field of DHCP packets. To delete the default relay agent interface use **no ip dhcp relay default-interface.**

Syntax

ip dhcp relay default-interface

no ip dhcp relay default-interface

Command mode

Interface Configuration Mode

Privilege Requirement

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

Example

Configure interface VLAN 1 as the default relay agent interface：

T1700X-16TS(config)# interface vlan 1

T1700X-16TS(config-if)# ip dhcp relay default-interface

26.11 ip dhcp relay vlan

Description

The **ip dhcp relay vlan** command is used to add DHCP server address to specified VLAN. If there is an IP interface in the VLAN and it has configured a DHCP server address at the interface level, then the configuration at the interface level has higher priority. In this case, the DHCP server configured on the VLAN will not be used to forward the DHCP packets. To delete the DHCP server address use **no ip dhcp relay vlan.**

Syntax

ip dhcp relay vlan *vid* **helper-address** *ip-address*

no ip dhcp relay vlan *vid* **helper-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：

```
T1700X-16TS(config)# ip dhcp relay vlan 1 helper-address 192.168.2.1
```

26.12 show ip dhcp relay

Description

The **show ip dhcp relay** command is used to display the global status and Option 82 configuration of DHCP Relay.

Syntax

show ip dhcp relay

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of DHCP Relay:

```
T1700X-16TS(config)# show ip dhcp relay
```

Chapter 27 DHCP L2 Relay Commands

27.1 ip dhcp l2relay

Description

The **ip dhcp l2relay** command is used to enable DHCP L2 Relay function globally. To disable DHCP L2 Relay function, please use **no ip dhcp l2relay** command.

Syntax

ip dhcp l2relay

no ip dhcp l2relay

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable DHCP L2 Relay function globally:

```
T1700X-16TS(config)# ip dhcp l2relay
```

27.2 ip dhcp l2relay vlan

Description

The **ip dhcp l2relay vlan** command is used to enable DHCP L2 relay in the specified VLAN. To disable DHCP L2 Relay in the specific vlan, please use **no ip dhcp l2relay vlan** command.

Syntax

ip dhcp l2relay vlan *vlan-range*

no ip dhcp l2relay vlan *vlan-range*

Parameter

vlan-range —— Specify the vlan to be enabled with DHCP L2 relay.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable DHCP L2 Relay for VLAN 2:

T1700X-16TS(config)# ip dhcp l2relay vlan 2

27.3 ip dhcp l2relay information

Description

The **ip dhcp l2relay information** command is used to enable option 82 support in DHCP Relay. To disable this function, please use **no ip dhcp l2relay information** command.

Syntax

ip dhcp l2relay information

no ip dhcp l2relay information

Command Mode

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

Privilege Requirement

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

Example

Enable option 82 support in DHCP Relay for port 2:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/2

T1700X-16TS(config-if)# ip dhcp l2relay information

27.4 ip dhcp l2relay information strategy

Description

The **ip dhcp l2relay information strategy** command is used to specify the operation for the Option 82 field of the DHCP request packets from the Host. To restore to the default option, please use **no ip dhcp l2relay information strategy** command.

Syntax

ip dhcp l2relay information strategy { drop | keep | replace }

no ip dhcp l2relay information strategy

Parameter

drop | keep | replace —— The operations for Option 82 field of the DHCP request packets from the Host. The default operation is keep.

drop: Discard the packet with the Option 82 field.

keep: Keep the Option 82 field in the packet.

replace: Replace the option 82 field with the system option defined by the switch.

Command Mode

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

Privilege Requirement

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

Example

Specify the option 82 strategy as replace to replace the Option 82 field with the local parameter on receiving the DHCP request packet for port 2:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/2

T1700X-16TS(config-if)# ip dhcp l2relay information strategy replace

27.5 ip dhcp l2relay information format

Description

The **ip dhcp l2relay information format** command is used to select the format of option 82 sub-option value field. To restore to the default option, please use **no ip dhcp l2relay information format** command.

Syntax

ip dhcp l2relay information format { normal | private }

no ip dhcp l2relay information format

Parameter

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

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

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

Command Mode

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

Privilege Requirement

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

Example

Select the format of option 82 sub-option value field as TLV (type-length-value) for port 2:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/2

T1700X-16TS(config-if)#ip dhcp l2relay information format normal

27.6 ip dhcp l2relay information circuit-id

Description

The **ip dhcp l2relay information circuit-id** command is used to specify the custom circuit ID when option 82 customization is enabled. To clear the circuit ID, please use **no ip dhcp l2relay information circuit-id** command.

Syntax

ip dhcp l2relay information circuit-id *circuitID*

no ip dhcp l2relay information circuit-id

Parameter

circuitID—— Specify the circuit ID, ranging from 1 to 64 characters.

Command Mode

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

Privilege Requirement

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

Example

Specify the circuit ID as “TP-Link” for port 2:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/2

T1700X-16TS(config-if)# ip dhcp l2relay information circuit-id TP-Link

27.7 ip dhcp l2relay information remote-id

Description

The **ip dhcp l2relay information remote-id** command is used to specify the custom remote ID when option 82 customization is enabled. To clear the remote ID, please use **no ip dhcp l2relay information remote-id** command.

Syntax

ip dhcp l2relay information remote-id *remoteID*

no ip dhcp l2relay information remote-id

Parameter

remoteID —— Specify the remote ID, ranging from 1 to 64 characters.

Command Mode

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

Privilege Requirement

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

Example

Specify the remote ID as “TP-Link” for port 2:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/2

T1700X-16TS(config-if)# ip dhcp l2relay information remote-id TP-Link

27.8 show ip dhcp l2relay

Description

The **show ip dhcp l2relay** command is used to display the global status and Option 82 configuration of DHCP Relay.

Syntax

show ip dhcp l2relay

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of DHCP Relay:

```
T1700X-16TS(config)# show ip dhcp l2relay
```

27.9 show ip dhcp l2relay interface

Description

The **show ip dhcp l2relay interface** command is used to display the DHCP L2 Relay status for the ports.

Syntax

show ip dhcp l2relay interface [**gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of DHCP L2 Relay:

```
T1700X-16TS(config)# show ip dhcp l2relay interface
```

Chapter 28 QoS Commands

QoS (Quality of Service) function is used to optimize the network performance. It provides you with network service experience of a better quality. The switch implements three priority modes based on port, on 802.1p and on DSCP.

28.1 qos trust mode

Description

The **qos trust mode** command is used to configure the trust mode of CoS (Class of Service) function for the ports. The default trust mode is trust port priority.

Syntax

qos trust mode { dot1p | dscp | untrust }

Parameter

dot1p—— Trust 802.1p mode. In this mode, data will be classified into different services based on the 802.1p priority.

dscp—— Trust dscp mode. In this mode, data will be classified into different services based on the dscp priority.

untrust—— Trust port mode. In this mode, data will be classified into different services based on the based on the port priority.

Command Mode

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

Privilege Requirement

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

Example

Set the trust mode of port 1/0/3 as dscp:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/3
T1700X-16TS(config-if)# qos trust mode dscp
```

28.2 qos port-priority

Description

The **qos port-priority** command is used to configure the port to 802.1p priority mapping for the desired port. To return to the default configuration, please use **no qos port-priority** command. When Port Priority is enabled, the packets will be mapped to different priority queues based on the ingress ports.

Syntax

qos port-priority { *dot1p-priority*}

no qos port-priority

Parameter

dot1p-priority —— The 802.1p priority that the packets will be mapped to from the desired port. It ranges from 0 to 7, which represent 802.1p priority 0-7 respectively. By default, the priority is 0.

Command Mode

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

Privilege Requirement

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

Example

Configure the priority of port 5 as 3:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/5
T1700X-16TS(config-if)# qos port-priority 3
```

28.3 qos cos-map

Description

The **qos cos-map** command is used to configure 802.1p to queue mapping globally. To return to the default configuration, please use **no qos cos-map** command. When 802.1P Priority is enabled, the packets with 802.1Q tag are mapped to different priority levels based on 802.1P priority.

Syntax

qos cos-map { *dot1p-priority* } { *tc-queue* }

no qos cos-map

Parameter

dot1p-priority —— The value of 802.1p priority. It ranges from 0 to 7, which represent 802.1p priority 0-7 respectively.

tc-queue—— The number of TC queue that the 80.1p priority will be mapped to. It ranges from 0 to 7.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Map the 802.1p priority 5 to TC-2:

```
T1700X-16TS (config)# qos cos-map 5 2
```

28.4 qos dot1p-remap

Description

The **qos dot1p-remap** command is used to configure the 802.1p to 802.1p mappings. To return to the default configuration, please use **no qos dot1p-remap** command. When 802.1p remap is configured, the packets with the specific 802.1p priority will tagged with the desired new 802.1p priority.

Syntax

qos dot1p-remap { *dot1p-priority* } { *new-dot1p-priority* }

no qos dot1p-remap

Parameter

dot1p-priority —— The original 802.1p priority. It ranges from 0 to 7, which represent 802.1p priority 0-7 respectively.

new-dot1p-priority—— The new 802.1p priority. It ranges from 0 to 7.

Command Mode

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

Privilege Requirement

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

Example

Remap 802.1p priority 5 to 802.1p priority 6:

T1700X-16TS(config)#qos dot1p-remap 5 6

28.5 qos dscp-map

Description

The **qos dscp-map** command is used to configure the DSCP to 802.1p mapping. To return to the default configuration, please use **no qos dscp-map** command. DSCP (DiffServ Code Point) is a new definition to IP ToS field given by IEEE. This field is used to divide IP datagram into 64 priorities. When DSCP Priority is enabled, IP datagram are mapped to different priority levels based on DSCP priority.

Syntax

qos dscp-map { *dscp-value-list*} { *dot1p-priority*}

no qos dscp-map

Parameter

dscp-value-list —— The DSCP value list in the format of "1-3,5,7". The valid values are from 0 to 63.

dot1p-priority ——The 802.1p priority to which the DSCP priority will be mapped. It ranges from 0 to 7, which represent 802.1p priority 0-7 respectively. By default, the priority is 0.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Map DSCP Priority 5 to 802.1p priority 2:

T1700X-16TS(config)#qos dscp-map 5 2

28.6 qos dscp-remap

Description

The **qos dscp-remap** command is used to configure the DSCP to DSCP mappings. To return to the default configuration, please use **no qos dscp-remap** command. When DSCP remap is configured, the packets with the specific DSCP priority will be changed to the desired new DSCP priority.

Syntax

qos queue dscp-map { *dscp-value-list* } { *dscp-remap-value* }

no qos queue dscp-map

Parameter

Dscp-value-list ——The original DSCP value list in the format of "1-3,5,7". The valid values are from 0 to 63.

Dscp-remap-value—— The new DSCP value, which ranges from 0 to 63.

Command Mode

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

Privilege Requirement

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

Example

Map DSCP values 10-12 to DSCP value 2:

T1700X-16TS(config)# qos dscp-remap 10-12 2

28.7 qos queue bandwidth

Description

The **qos queue bandwidth** command is used to configure the minimum guaranteed bandwidth allocated to the specified queue. A value of 0 means there is no guaranteed minimum bandwidth in effect (best-effort service). The default value is 0. The sum of all bandwidth values for the queues must not

exceed 100%. To return to the default configuration, please use **no qos bandwidth** command.

Syntax

qos queue { *tc-queue* } **bandwidth** { *rate* }

no qos queue { *tc-queue* } **bandwidth**

Parameter

tc-queue —— The egress queue ID. It ranges from 0 to 7, which represents TC queue from TC0 to TC7 respectively.

rate ——The minimum bandwidth percentage for queue, ranging from 1 to 100 in increments of 1. By default, it is 0.

Command Mode

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

Privilege Requirement

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

Example

Set the minimum bandwidth of TC5 as 10% for port 1/0/1:

T1700X-16TS (config)# interface ten-gigabitEthernet 1/0/1

T1700X-16TS (config-if)# qos queue 5 **bandwidth** 10

28.8 qos queue mode

Description

The **qos queue mode** command is used to configure the Scheduler Mode. When the network is congested, the program that many packets complete for resources must be solved, usually in the way of queue scheduling. The switch will control the forwarding sequence of the packets according to the priority queues and scheduling algorithms you set. On this switch, the priority levels are labeled as TC0, TC1, TC2 ... TC7.

Syntax

qos queue { *tc-queue* } **mode** { sp | wrr } [**weight** *weight*]

Parameter

tc-queue —— The egress queue ID. It ranges from 0 to 7, which represents TC queue from TC0 to TC7 respectively.

sp —— Strict-Priority Mode. In this mode, the queue with higher priority will occupy the whole bandwidth. Packets in the queue with lower priority are sent only when the queue with higher priority is empty.

wrr —— Weight Round Robin Mode. In this mode, packets in all the queues are sent in order based on the weight value for each queue. If you select this mode, you need to specify the queue weight at the same time.

weight —— Configure the weight value of the specified TC queue. When the scheduler mode is specified as WRR, the weight value ranges from 1 to 127. The 8 queues will take up the bandwidth according to their ratio.

Command Mode

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

Privilege Requirement

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

Example

Specify the Scheduler Mode of TC1 as WRR and set the queue weight as 10 for port 1/0/1:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/1
T1700X-16TS(config-if)# qos queue 1 mode wrr weight 10
```

28.9 show qos cos-map

Description

The **show qos cos-msp** command is used to display the 802.1p priority to TC queue mappings.

Syntax

show qos cos-map

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the 802.1p to queue mappings:

```
T1700X-16TS# show qos cos-map
```

28.10 show qos dot1p-remap

Description

The **show qos dot1p-remap interface** command is used to display the 802.1p priority to 802.1p priority mappings.

Syntax

show qos dot1p-remap

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IEEE 802.1P remap configuration:

```
T1700X-16TS# show qos dot1p-remap
```

28.11 show qos dscp-map

Description

The **show qos dscp-map** command is used to display the DSCP priority configuration.

Syntax

show qos dscp-map

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DSCP priority configuration:

```
T1700X-16TS# show qos dscp-map
```

28.12 show qos dscp-remap

Description

The **show qos dscp-remap** command is used to display the DSCP priority to DSCP priority mappingss.

Syntax

show qos dscp-remap

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DSCP to DSCP mappings:

```
T1700X-16TS# show qos dscp-remap
```

28.13 show qos port-priority interface

Description

The **show qos port-priority interface** command is used to display the port to 802.1p priority mappings for the ports.

Syntax

show qos port-priority interface [**fastEthernet** *port* **| gigabitEthernet** *port* | **ten-gigabitEthernet** *port* **| port-channel** *port-channel-id*]

Parameter

port —— The port number.

port-channel-id —— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the port to 802.1p priority mappings for all the ports:

```
T1700X-16TS# show qos port-priority interface
```

28.14 show qos trust interface

Description

The **show qos trust interface** command is used to display the trust mode of the ports.

Syntax

show qos trust interface [**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parameter

port—— The port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the trust mode of all the ports:

```
T1700X-16TS# show qos trust interface
```

28.15 show qos queue interface

Description

The **show qos queue interface** command is used to display the scheduler settings of the ports.

Syntax

show qos queue interface [**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parameter

port—— The port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the scheduler settings of all the ports:

```
T1700X-16TS# show qos queue interface
```

Chapter 29 Bandwidth Control Commands

Bandwidth Control functions to control the traffic rate and traffic threshold on each port to ensure network performance. Rate limit functions to limit the ingress/egress traffic rate on each port. Storm Control function allows the switch to monitor broadcast packets, multicast packets and Unknown unicast frames in the network.

29.1 storm-control rate-mode

Description

The **storm-control rate-mode** command is used to configure the storm control mode of the interface. To return to the default configuration, please use **no storm-control rate-mode** command.

Syntax

storm-control rate-mode { kbps | ratio | pps }

no storm-control rate-mode

Parameter

kbps —— The switch will limit the maximum speed of the specific kinds of traffic in kilo-bits per second.

ratio —— The switch will limit the percentage of bandwidth utilization for specific kinds of traffic.

pps —— The switch will limit the maximum number of packets per second for specific kinds of traffic.

Command Mode

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

Privilege Requirement

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

User Guidelines

This command should be used along with the **storm-control** command to enable the storm control function and specify the detailed parameters.

Example

Set the storm control mode as kbps on port 1/0/5:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/5
```

```
T1700X-16TS(config-if)# storm-control rate-mode kbps
```

29.2 storm-control

Description

The **storm-control** command is used to enable the broadcast, multicast, or unknown unicast strom control function and to set threshold levels on an interface. To return to the default configuration, please use **no storm-control** command.

Syntax

storm-control { broadcast | multicast | unicast } { *rate* }

no storm-control { broadcast | multicast | unicast }

Parameter

broadcast | multicast | unicast —— Select the mode of the storm control on the interface.

rate —— Specify the bandwidth for receiving packets on the port. The specified type of packet traffic exceeding the bandwidth will be processed according to the configuration of **storm-control exceed** command. For kbps, the rate ranges from 1 to 1000000 kbps; For ratio, the rate ranges from 1 to 100 percent; For pps, the rate ranges from 1 to 1488000 packets per second.

Command Mode

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

Privilege Requirement

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

User Guidelines

Before you configure the storm-control type as kbps or ratio, pelease ensure that the port is not in pps mode.

Example

Configure the broadcast storm control rate as 1024 kbps on port 1/0/5:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/5
T1700X-16TS(config-if)# storm-control rate-mode kbps
T1700X-16TS(config-if)# storm-control broadcast 1024
```

29.3 storm-control exceed

Description

The **storm-control exceed** command is used to configure the action that the switch will perform when the storm exceeds the defined limit on an interface.

Syntax

storm-control exceed { drop | shutdown } [**revocer-time** *time*]

Parameter

drop —— Set the Action as Drop. The port will drop the subsequent packets when the traffic exceeds the limit.

shutdown —— Set the Action as Shutdown. The port will be shutdown when the traffic exceeds the limit.

time ——Specify the recover time for the port. It takes effect only when the action is set as shutdown. The valid values are from 0 to 3600 and the default value is 0. When the port is shutdown, it can recover to its normal state after the recover time passed. If the recover time is specified as 0, which means the port will not recover to its normal state automatically and you can recover the port manually using **storm-control recover** command.

Command Mode

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

Privilege Requirement

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

Example

Configure the action as drop on port 1/0/5:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/5
T1700X-16TS(config-if)# storm-control exceed drop
```

29.4 storm-control recover

Description

The **storm-control recover** command is used to recover the port manually after the port is shutdown because of the storm. When the recover time is specified as 0, the port will not recover to its normal state automatically. In this condition, you need to use this command to recover the port manually.

Syntax

storm-control recover

Command Mode

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

Privilege Requirement

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

Example

Recover port 1/0/5 manually:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/5
T1700X-16TS(config-if)# storm-control recover
```

29.5 bandwidth

Description

The **bandwidth** command is used to configure the bandwidth limit for an Ethernet port. To disable the bandwidth limit, please use **no bandwidth** command.

Syntax

bandwidth {[**ingress** *ingress-rate*] [**egress** *egress-rate*]}

no bandwidth { all | ingress | egress }

Parameter

ingress-rate —— Specify the 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 ten-gigabitEthernet / interface range ten-gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

Configure the ingress-rate as 5120Kbps and egress-rate as 1024Kbps for port 1/0/5:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/5
T1700X-16TS(config-if)# bandwidth ingress 5120 egress 1024
```

29.6 show storm-control

Description

The **show storm-control** command is used to display the storm-control information of Ethernet ports.

Syntax

show storm-control interface [**fastEthernet** *port* **| gigabitEthernet** *port-list* ***ten-gigabitEthernet*** *port* **| port-channel** *port-channel-id-list*]

Parameter

port-list ——The list of Ethernet ports.

port-channel-id-list —— The list of port channels.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the storm-control information of port 4, 5, 6, and 7:

```
T1700X-16TS(config)# show storm-control interface ten-gigabitEthernet
1/0/4-7
```

29.7 show bandwidth

Description

The **show bandwidth** command is used to display the bandwidth-limit information of Ethernet ports.

Syntax

show bandwidth interface [**fastEthernet** *port* **| gigabitEthernet** *port-list* **ten-gigabitEthernet** *port* **| port-channel** *port-channel-id-list*]

Parameter

port-list ——The list of Ethernet ports.

port-channel-id-list —— The list of port channels.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the bandwidth-limit information of port 1/0/4:

T1700X-16TS(config)# show bandwidth interface ten-gigabitEthernet 1/0/4

Chapter 30 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.

30.1 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:

```
T1700X-16TS(config)# voice vlan 10
```

30.2 voice vlan (interface)

Description

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

Syntax

voice vlan

no voice vlan

Command Mode

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

Privilege Requirement

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

Example

Enable the Voice VLAN function for port 1/0/1:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/1
T1700X-16TS(config-if)#voice vlan
```

30.3 voice vlan priority

Description

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

Syntax

voice vlan priority *pri*

no voice vlan priority

Parameter

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the priority of the Voice VLAN as 5:

T1700X-16TS(config)# voice vlan priority 5

30.4 voice vlan oui

Description

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

Syntax

voice vlan oui *oui-prefix* **oui-desc** *string*

no voice vlan mac-address *oui-prefix*

Parameter

oui-prefix —— The OUI address of the voice device, in the format of XX:XX:XX.

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

T1700X-16TS(config)#voice vlan oui 00:11:11 **oui-desc** TP-Phone

30.5 show voice vlan

Description

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

Syntax

show voice vlan

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

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

Example

Display the configuration information of Voice VLAN globally:

```
T1700X-16TS(config)# show voice vlan
```

30.6 show voice vlan oui-table

Description

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

Syntax

show voice vlan oui

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

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

Example

Display the configuration information of Voice VLAN OUI:

```
T1700X-16TS(config)# show voice vlan oui-table
```

30.7 show voice vlan interface

Description

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

Syntax

show voice vlan interface

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

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

Example

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

```
T1700X-16TS(config)# show voice vlan interface
```

Chapter 31 Auto VoIP Commands

The Auto VoIP feature is used to prioritize the transmission of voice traffic. Voice over Internet Protocol (VoIP) enables telephone calls over a data network, and the Auto VoIP feature helps provide a classification mechanism for voice packets. When Auto VoIP is configured on a port that receives both voice and data traffic, this feature can help ensure that the sound quality of an IP phone does not deteriorate when data traffic on the port is heavy.

31.1 auto-voip

Description

The **auto-voip** command is used to enable the Auto VoIP function globally.

To disable the Auto VoIP function, use **no auto-voip** command.

Syntax

auto-voip

no auto-voip

Command Mode

Global Configuration Mode

Example

Enable the Auto VoIP function globally:

```
T1700X-16TS(config)# auto-voip
```

31.2 auto-voip (interface)

Description

The **auto-voip** command is used to specify the interface mode as VLAN ID for the ports. In this mode, the voice devices will send voice packets with desired VLAN tag.

Syntax

auto-voip *vlan-id*

Parameter

vlan-id ——Specify the Auto VoIP VLAN ID. The valid values are from 2 to 4094.

Command Mode

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

Example

Set Auto VoIP VLAN 3 for port 3:

T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/3

T1700X-16TS(config-if)# auto-voip 3

31.3 auto-voip dot1p

Description

The **auto-voip dot1p** command is used to specify the interface mode as dat1p for the ports. In this mode, the voice devices will send voice packets with desired 802.1p priority.

Syntax

auto-voip dot1p *dot1p*

Parameter

dot1p——Set the 802.1p priority of Auto VoIP on specified ports. It ranges from 0 to 7.

Command Mode

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

Example

Set the 802.1p priority as 5 for the port:

T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/3

T1700X-16TS(config-if)# auto-voip dot1p 5

31.4 auto-voip untagged

Description

The **auto-voip untagged** command is used to specify the interface mode as untagged for the ports. In this mode, the voice devices will send untagged voice packets.

Syntax

auto-voip untagged

Command Mode

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

Example

Set the interface mode as untagged for port 1/0/3:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/3
T1700X-16TS(config-if)# auto-voip untagged
```

31.5 auto-voip none

Description

The **auto-voip none** command is used to specify the interface mode as none for the ports. In this mode, the switch allows the voice devices to use its own configuration to send voice traffic.

Syntax

auto-voip none

Command Mode

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

Example

Instruct voice devices that are connected to port 3 to send the packets according to its own configuration:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/3
T1700X-16TS(config-if)# auto-voip none
```

31.6 no auto-voip (interface)

Description

The **no auto-voip** command is used to specify the interface mode as disabled for the ports, which means the Auto VoIP function is disabled on the corresponding port.

Syntax

no auto-voip

Command Mode

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

Example

Disable the Auto VoIP function on port 1/0/3:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/3
T1700X-16TS(config-if)# no auto-voip
```

31.7 auto-voip dscp

Description

The **auto-voip dscp** command is used to set the DSCP value of Auto VoIP on specified ports.

Syntax

auto-voip dscp *value*

Parameter

value——Set the DSCP value of Auto VoIP on specified ports. It ranges from 0 to 63. By default, it is 0.

Command Mode

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

Example

Set DSCP value of Auto VoIP on port 3 as 33:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/3
T1700X-16TS(config-if)# auto-voip dscp 33
```

31.8 auto-voip data priority

Description

The **auto-voip data priority** command is used to enable or disable the CoS Override Mode on specified ports.

Syntax

auto-voip data priority { trust | untrust }

Parameter

trust——In this mode, the switch will then put the voice packets in the corresponding TC queue according to the 802.1p priority of the packets.

untrust——In this mode, the switch will ignore the 802.1p priority in the voice packets and put the packets in TC-5 directly.

Command Mode

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

Example

Set the CoS Override Mode as trust for port 1/0/3:

```
T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/3
T1700X-16TS(config-if)# auto-voip data priority trust
```

31.9 show auto-voip

Description

The **show auto-voip** command is used to display the Auto VoIP configuration information.

Syntax

show auto-voip [interface]

Parameter

interface —— Displays the Auto VoIP configuration information of ports. When no parameter is entered, displays the global Auto VoIP configuration information.

Command Mode

Privileged EXEC Mode and any Configuration Mode

Example

Displays the global Auto VoIP configuration information:

```
T1700X-16TS (config)# show auto-voip
```

Chapter 32 Access Control Commands

32.1 user access-control ip-based enable

Description

The **user access-control ip-based enable** command is used to configure the access control mode IP-based. To disable the access control feature, please use **no user access-control** command.

Syntax

user access-control ip-based enable

no user access-control

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the access control mode as IP-based:

```
T1700X-16TS(config)# user access-control ip-based enable
```

32.2 user access-control ip-based

Description

The **user access-control ip-based** command is used to limit the IP-range of the users for login. Only the users within the IP-range you set here are allowed to login. You can add up to 30 IP-based entries. To cancel the user access limit, please use **no user access-control ip-based** command.

Syntax

user access-control ip-based { *ip-addr ip-mask* } [snmp] [telnet] [ssh] [http] [https] [ping] [all]

no user access-control ip-based index *id*

Parameter

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

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

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

id —— Delete the specified IP-based entry.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

T1700X-16TS(config)# user access-control ip-based 192.168.0.148 255.255.255.255

32.3 user access-control mac-based enable

Description

The **user access-control mac-based enable** command is used to configure the access control mode MAC-based. To disable the access control feature, please use **no user access-control** command.

Syntax

user access-control mac-based enable

no user access-control

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the access control mode as MAC-based:

T1700X-16TS(config)# user access-control mac-based enable

32.4 user access-control mac-based

Description

The **user access-control mac-based** command is used to limit the MAC address of the users for login. Only the user with this MAC address you set here is allowed to login. You can add up to 30 mac-based control entries. To delete the mac-based access control entry, please use **no user access-control mac-based** command.

Syntax

user access-control mac-based { *mac-addr* } [snmp] [telnet] [ssh] [http] [https] [ping] [all]

no user access-control mac-based index *id*

Parameter

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

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

id—— Specify the ID of the mac-based entry to be deleted.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

T1700X-16TS(config)# user access-control mac-based 00:00:13:0A:00:01

32.5 user access-control port-based enable

Description

The **user access-control port-based enable** command is used to configure the access control mode Port-based. To disable the access control feature, please use **no user access-control** command.

Syntax

user access-control port-based enable

no user access-control

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the access control mode as Port-based:

```
T1700X-16TS(config)# user access-control port-based enable
```

32.6 user access-control port-based

Description

The **user access-control port-based** command is used to limit the ports for login. Only the users connected to these ports you set here are allowed to login. You can add up to 30 port-based control entries. To delete the port-based access control entry, please use **no user access-control port-based** command.

Syntax

user access-control port-based interface { **gigabitEthernet** *port-list* } [snmp] [telnet] [ssh] [http] [https] [ping] [all]

no user access-control port-based index *id*

Parameter

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

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

id—— Specify the ID of the port-based entry to be deleted.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

T1700X-16TS(config)# user access-control port-based interface ten-gigabitEthernet 1/0/2-6

Chapter 33 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.

33.1 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:

```
T1700X-16TS(config)# no ip http server
```

33.2 ip http port

Description

The **ip http port** command is used to configure the port number of the HTTP server within the switch. To set the number to the default value, please use **no ip http port** command.

Syntax

ip http port *port-num*

no ip http port

Parameter

port-num —— Enter the port number. This value ranges from 1 to 65535.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Set the port number of HTTP server as 1800:

T1700X-16TS(config)# ip http port 1800

33.3 ip http max-users

Description

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

Syntax

ip http max-users *admin-num operator-num poweruser-num user-num*

no ip http max-users

Parameter

admin-num —— The maximum number of the users logging on to the HTTP server as Admin, ranging from 1 to 16. The total number of users should be no more than 16.

operator-num —— The maximum number of the users logging on to the HTTP server as operator, ranging from 0 to 15. The total number of users should be no more than 16.

poweruser-num —— The maximum number of the users logging on to the HTTP server as Power User, ranging from 0 to 15. The total number of users should be no more than 16.

user-num —— The maximum number of the users logging on to the HTTP server as User, ranging from 0 to 15. The total number of users should be no more than 16.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the maximum number of the Admin, Operator, Power User and User as 5, 1, 1, 1 for HTTP:

T1700X-16TS(config)# ip http max-users 5 1 1 1

33.4 ip http session timeout

Description

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

Syntax

ip http session timeout *time*

no ip http session timeout

Parameter

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

T1700X-16TS(config)# ip http session timeout 15

33.5 ip http secure-server

Description

The **ip http secure-server** command is used to enable the HTTPS server within the switch. To disable the HTTPS function, please use **no ip http secure-server** command. This function is enabled by default. The HTTP and HTTPS server function 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:

T1700X-16TS(config)# no ip http secure-server

33.6 ip http secure-port

Description

The **ip http secure-port** command is used to configure the port number of the HTTPS server within the switch. To set the number to the default value, please use **no ip http secure-port** command.

Syntax

ip http secure-port *port-num*

no ip http secure-port

Parameter

port-num —— Enter the port number. This value ranges from 1 to 65535.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Set the port number of HTTPS server as 2800:

T1700X-16TS(config)# ip http port 2800

33.7 ip http secure-protocol

Description

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

T1700X-16TS(config)# ip http secure-protocol ssl3

33.8 ip http secure-ciphersuite

Description

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

Syntax

ip http secure-ciphersuite { [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:

T1700X-16TS(config)# ip http secure-ciphersuite 3des-ede-cbc-sha

33.9 ip http secure-max-users

Description

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

Syntax

ip http secure-max-users *admin-num operator-num poweruser-num user-num*

no ip secure-max-users

Parameter

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

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

poweruser-num —— The maximum number of the users logging on to the HTTP server as Power User, ranging from 0 to 15. The total number of users should be less than 16.

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the maximum number of the Admin, Operator, Power User and User as 5, 1, 1, 1 for HTTPs:

```
T1700X-16TS(config)# ip http secure-max-users 5 1 1 1
```

33.10 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:

T1700X-16TS(config)# ip http secure-session timeout 15

33.11 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:

T1700X-16TS(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

T1700X-16TS(config)# ip http secure-server download certificate ssl-cert **ip-address** fe80::1234

33.12 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:

T1700X-16TS(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

T1700X-16TS(config)# ip http secure-server download key ssl-key **ip-address** fe80::1234

33.13 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:

T1700X-16TS(config)# show ip http configuration

33.14 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:

```
T1700X-16TS(config)# show ip http secure-server
```

Chapter 34 SSH Commands

SSH (Security Shell) can provide the unsecured remote management with security and powerful authentication to ensure the security of the management information.

34.1 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:

```
T1700X-16TS(config)# ip ssh server
```

34.2 ip ssh port

Description

The **ip ssh port** command is used to configure the port for SSH service. To set the value to the default, please use **no ip ssh port** command.

Syntax

ip ssh port *port*

no ip ssh port

Parameter

port —— Set the port number. It ranges from 1 to 65535. The default value is 22.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the SSH port number as 22:

```
T1700X-16TS(config)# ip ssh port 22
```

34.3 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:

```
T1700X-16TS(config)# ip ssh version v2
```

34.4 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:

T1700X-16TS(config)# ip ssh algorithm AES128-CBC

34.5 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:

```
T1700X-16TS(config)# ip ssh timeout 30
```

34.6 ip ssh max-client

Description

The **ip ssh max-client** command is used to specify the maximum number of the connections to the SSH server. To return to the default configuration, please use **no ip ssh max-client** command.

Syntax

ip ssh max-client *num*

no ip ssh max-client

Parameter

num —— The maximum number of the connections to the SSH server. It ranges from 1 to 5. By default, this value is 5.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the maximum number of the connections to the SSH server as 3:

```
T1700X-16TS(config)# ip ssh max-client 3
```

34.7 ip ssh download

Description

The **ip ssh download** command is used to download the SSH key file from TFTP server.

Syntax

ip ssh download { 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:

T1700X-16TS(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:

T1700X-16TS(config)# ip ssh download v1 ssh-key **ip-address** fe80::1234

34.8 remove public-key

Description

The **remove public-key** command is used to remove the SSH public key from the switch.

Syntax

remove public-key { 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:

```
T1700X-16TS# remove public-key v1
```

34.9 show ip ssh

Description

The **show ip ssh** command is used to display the global configuration of SSH.

Syntax

show ip ssh

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of SSH:

```
T1700X-16TS(config)# show ip ssh
```

Chapter 35 Telnet Commands

35.1 telnet enable

Description

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

Syntax

telnet enable

telnet disable

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Disable the Telnet function:

```
T1700X-16TS(config)# telnet disable
```

35.2 telnet port

Description

The **telnet port** command is used to configure the telent port number. To restore the setting, please use the **no telnet port** command.

Syntax

telnet port *port*

no telnet port

Parameter

port——The number of telnet port.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the telnet port number as 566:

```
T1700X-16TS(config)# telnet port 566
```

35.3 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:

```
T1700X-16TS(config)# show telnet-status
```

Chapter 36 AAA Commands

AAA stands for authentication, authorization and accounting. This feature is used to authenticate users trying to log in to the switch or trying to access the administrative level privilege.

- **Applicable Access Application**

The authentication can be applied on the following access applications: Telnet, SSH and HTTP.

- **Authentication Method List**

A method list describes the authentication methods and their sequence to authenticate a user. The switch supports Login List for users to gain access to the switch, and Enable List for normal users to gain administrative privileges.

- **RADIUS/TACACS+ Server**

User can configure the RADIUS/TACACS+ servers for the connection between the switch and the server.

- **Server Group**

User can define the authentication server group with up to several servers running the same secure protocols, either RADIUS or TACACS+. Users can set these servers in a preferable order, which is called the server group list. When a user tries to access the switch, the switch will ask the first server in the server group list for authentication. If no response is received, the second server will be queried, and so on.

36.1 tacacas-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 *encryped-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 32 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.

T1700X-16TS(config)# tacacs-server host 1.1.1.1 **port** 1500 **timeout** 6 **key** 12345

36.2 show tacacs-server

Description

This **show tacacs-server** command is used to display the summary information of the TACACS+ servers.

Syntax

show tacacs-server

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of all the TACACS+ servers:

T1700X-16TS(config)# show tacacs-server

36.3 radius-server host

Description

The **radius-server host** command is used to configure a new RADIUS server. To delete the specified RADIUS server, please use **no radius-server host** command.

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 accouting requests. By deault 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 32 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.

T1700X-16TS(config)# radius-server host 1.1.1.1 **auth-port** 1200 **timeout** 6 **retransmit** 3 **key** 12345

36.4 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:

T1700X-16TS(config)# show radius-server

36.5 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:

T1700X-16TS(config)# aaa group radius radius1

36.6 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":

T1700X-16TS(config)# aaa group radius radius1

T1700X-16TS(aaa-group)# server 1.1.1.1

36.7 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:

```
T1700X-16TS(config)# show aaa group
```

36.8 aaa authentication login

Description

This **aaa authentication login** command is used to configure a login authentication method list. A method list describes the authentication methods and their sequence to authenticate a user. To delete the specified authentication method list, please use the **no aaa authentication login** command.

Syntax

aaa authentication login { *method-list* } { *method1* } [*method2*] [*method3*] [*method4*]

no authentication login *method-list*

Parameter

method-list —— Specify the method list name.

method1, method2, method3, method4 —— Specify the authentication methods in order. The next authentication method is tried only if the previous method does not respond, not if it fails.

The preset methods include radius, tacacs, local and none. "radius" means the RADIUS server group "radius"; "tacacs" means the RACACS+ server group "tacacs"; "local" means local username database are used; "none" means no authentication is used for login.

Users can aslo 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:

T1700X-16TS(config)# aaa authenticaiton login list1 radius local

36.9 aaa authentication enable

Description

This **aaa authentication enable** command is used to configure a privilege authentication method list. A method list describes the authentication methods and their sequence to elevate a user’s privilege. To delete the specified authentication method list, please use the **no aaa authentication enable** command.

Syntax

aaa authentication enable { *method-list* } { *method1* } [*method2*] [*method3*] [*method4*]

no authentication enable *method-list*

Parameter

method-list —— Specify the method list name.

method1, method2, method3, method4 —— Specify the authentication methods in order. The next authentication method is tried only if the previous method does not respond, not if it fails.

The preset methods include radius, tacacs, local and none. “radius” means the RADIUS server group “radius”; “tacacs” means the RACACS+ server group “tacacs”; “local” means local username database are used; “none” means no authentication is used for privilege elevation.

Users can aslo 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:

T1700X-16TS(config)# aaa authenticaiton enable list2 radius local

36.10 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”:

T1700X-16TS(config)# aaa authentication dot1x default radius1

36.11 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 —— Sp+ecify 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”:

T1700X-16TS(config)# aaa accounting dot1x default radius1

36.12 show aaa authentication

Description

This **show aaa authentication** command is used to display the summary information of the authentication login, enable and dot1x metheod 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:

T1700X-16TS(config)# show aaa authentication

36.13 show aaa accounting

Description

This **show aaa accounting** command is used to display the summary information of the accounting metheod 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:

T1700X-16TS(config)# show aaa accounting

36.14 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:

```
T1700X-16TS(config)#line telnet
```

36.15 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":

```
T1700X-16TS(config)#line telnet
T1700X-16TS(config-line)# login authentication list1
```

36.16 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:

```
T1700X-16TS(config)#line ssh
```

36.17 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":

T1700X-16TS(config)# line ssh

T1700X-16TS(config-line)# login authentication list1

36.18 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":

T1700X-16TS(config)#line telnet

T1700X-16TS(config-line)# enable authentication list2

36.19 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":

T1700X-16TS(config)# line ssh

T1700X-16TS(config-line)# enable authentication list2

36.20 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":

T1700X-16TS(config)# ip http login authentication list1

36.21 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":

T1700X-16TS(config)# ip http enable authentication list2

36.22 show aaa global

Description

This **show aaa global** command is used to display global status of AAA function and the login/enable method lists of different application modules: telnet, ssh and HTTP.

Syntax

show aaa global

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the AAA function's global status and each application's method list:

T1700X-16TS(config)# show aaa global

36.23 enable-admin

Description

The **enable-admin** command is used to get the administrative privelges by a non-admin user.

Syntax

enable-admin

Command Mode

Privileged EXEC Mode

Privilege Requirement

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

Example

Get the administrative privelges (the Enable password is “123456”):

T1700X-16TS# enable-admin

Password: 123456

Chapter 37 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 enbable the AAA function and configure the RADIUS server. Go to Chapter 42 AAA Commands for more details.

37.1 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:

```
T1700X-16TS(config)#dot1x system-auth-control
```

37.2 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:

```
T1700X-16TS(config)# no dot1x handshake
```

37.3 dot1x auth-protocol

Description

The **dot1x auth-protocol** command is used to configure the authentication protocol of IEEE 802.1x and the default 802.1x authentication method is “eap”. To restore to the default 802.1x authentication protocol, please use **no dot1x auth-protocol** command.

Syntax

dot1x auth-protocol { pap | eap }

no dot1x auth-protocol

Parameter

pap | eap ——Authentication protocols.

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

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the Authentication protocol of IEEE 802.1x as "pap":

T1700X-16TS(config)#dot1x auth-protocol pap

37.4 dot1x vlan-assignment

Description

The **dot1x vlan-assignment** command is used to enable the VLAN assignment feature.To disable this feature, please use **no dot1x vlan-assignment** command.

802.1x VLAN assignment is a technology allowing the RADIUS server to send the VLAN assignment to the port when the port is authenticated.

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

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

If no VLAN is supplied by the RADIUS server or if 802.1x authentication is disabled, the port will be in its original VLAN after successful authentication.

Syntax

dot1x vlan-assignment

no dot1x vlan-assignment

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the VLAN assignment feature:

```
T1700X-16TS(config)#dot1x vlan-assignment
```

37.5 dot1x accounting

Description

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

Syntax

dot1x accounting

no dot1x accounting

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the enable the IEEE 802.1x accounting function globally:

```
T1700X-16TS(config)#dot1x accounting
```

37.6 dot1x mab

Description

The **dot1x mab** command is used to enable the MAB feature on the port.To disable this feature, please use **no dot1x mab** command.

With MAB (MAC-Based Authentication Bypass) feature enabled, the switch automatically sends the authentication server a RADIUS access request frame with the client's MAC address as the username and password. It is also necessary to configure the RADIUS server with the client's information for authentication. You can enable this feature on IEEE 802.1x ports connected to devices without 802.1x capability. For example, most printers, IP phones and fax machines do not have 802.1x capability.

Syntax

dot1x mab

no dot1x mab

Command Mode

Interface Configuration Mode

Privilege Requirement

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

Example

Enable the MAB feature on the Port 1/0/1:

```
T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/1
T1700X-16TS(config-if)#dot1x mab
```

37.7 dot1x guest-vlan

Description

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

Syntax

dot1x guest-vlan *vid*

no dot1x guest-vlan

Parameter

vid —— The VLAN ID needed to enable the Guest VLAN function, ranging from 0 to 4094. 0 means that Guest VLAN is disabled. The supplicants in the Guest VLAN can access the specified network source.

Command Mode

Interface Configuration Mode

Privilege Requirement

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

Example

Enable the Guest VLAN function for VLAN 5 and set the VLAN ID as 20 on the Port 1/0/1::

```
T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/1
T1700X-16TS(config-if)#dot1x guest-vlan 5
```

37.8 dot1x timeout quiet-period

Description

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

Syntax

dot1x timeout quiet-period [*time*]

no dot1x timeout quiet-period

Parameter

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

Command Mode

Interface Configuration Mode

Privilege Requirement

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

Example

Enable the quiet-period function and set the quiet-period as 5 seconds on the Port 1/0/1:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/1

T1700X-16TS(config-if)#dot1x quiet-period 5

37.9 dot1x timeout supp-timeout

Description

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

Syntax

dot1x timeout supp-timeout *time*

no dot1x timeout supp-timeout

Parameter

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

Command Mode

Interface Configuration Mode

Privilege Requirement

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

Example

Configure the supplicant timeout value as 5 seconds on the Gigabit Ethernet pot 1/0/1:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/1

T1700X-16TS(config-if)#dot1x timeout supp-timeout 5

37.10 dot1x max- req

Description

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

Syntax

dot1x max-req *times*

no dot1x max-req

Parameter

times —— The maximum transfer times of the repeated authentication request, ranging from 1 to 9 in times. By default, the value is 3.

Command Mode

Interface Configuration Mode

Privilege Requirement

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

Example

Configure the maximum transfer times of the repeated authentication request as 5 on the Port 1/0/1:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/1

T1700X-16TS(config-if)#dot1x max-req 5

37.11 dot1x

Description

The **dot1x** command is used to enable the IEEE 802.1x function for a specified port. To disable the IEEE 802.1x function for a specified port, please use **no dot1x** command.

Syntax

dot1x

no dot1x

Command Mode

Interface Configuration Mode (interface ten-gigabitEthernet / interface range ten-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 Port 1:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/1

T1700X-16TS(config-if)#dot1x

37.12 dot1x port-control

Description

The **dot1x port-control** command is used to configure the Control Mode of IEEE 802.1x for the specified port. By default, the control mode is “auto”. To restore to the default configuration, please use **no dot1x port-control** command.

Syntax

dot1x port-control {auto | authorized-force | unauthorized-force}

no dot1x port-control

Parameter

auto | authorized-force | unauthorized-force —— The Control Mode for the port.

auto: In this mode, the port will normally work only after passing the 802.1x Authentication.

authorized-force: In this mode, the port can work normally without passing the 802.1x Authentication.

unauthorized-force: In this mode, the port is forbidden working for its fixed unauthorized status.

Command Mode

Interface Configuration Mode (interface ten-gigabitEthernet / interface range ten-gigabitEthernet)

Privilege Requirement

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

Example

Configure the Control Mode for port 20 as “authorized-force”:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/2

T1700X-16TS(config-if)#dot1x port-control authorized-force

37.13 dot1x port-method

Description

The **dot1x port-method** command is used to configure the control type of IEEE 802.1x for the specified port. By default, the control type is “mac-based”. To restore to the default configuration, please use **no dot1x port-method** command.

Syntax

dot1x port-method { mac-based | port-based }

no dot1x port-method

Parameter

mac-based | port-based ——The control type for the port.

mac-based: Any client connected to the port should pass the 802.1x authentication for access.

port-based: All the clients connected to the port can access the network on the condition that any one of the clients has passed the 802.1x Authentication.

Command Mode

Interface Configuration Mode (interface ten-gigabitEthernet / interface range ten-gigabitEthernet)

Privilege Requirement

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

Example

Configure the Control Type for port 20 as “port-based”:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/2

T1700X-16TS(config-if)#dot1x port-method port-based

37.14 dot1x auth-init

Description

The **dot1x auth-init** command is used to initialize the specific client.

Syntax

dot1x auth-init [mac *mac-address* **]**

Parameter

mac-address: Enter the MAC address of the client that will be unauthorized.

Command Mode

Interface Configuration Mode (interface ten-gigabitEthernet / interface range ten-gigabitEthernet)

Privilege Requirement

None.

Example

Initialize the client whose MAC address is a 00:02:58:4f:6c:23 on port 1:

T1700X-16TS(Config)# interface ten-gigabitEthernet 1/0/1

T1700X-16TS(Config-if)#dot1x auth-init mac 00:02:58:4f:6c:23

37.15 dot1x auth-reauth

Description

The **dot1x auth-reauth** command is used to reauthenticate the specific client.

Syntax

dot1x auth-reauth [**mac** *mac-address*]

Parameter

mac-address: Enter the MAC address of the client that will be reauthenticated.

Command Mode

Interface Configuration Mode (interface ten-gigabitEthernet / interface range ten-gigabitEthernet)

Privilege Requirement

None.

Example

Reauthenticate the client whose MAC address is a 00:02:58:4f:6c:23 on port 1:

T1700X-16TS(Config)# interface ten-gigabitEthernet 1/0/1

T1700X-16TS(Config-if)#dot1x auth-reauth mac 00:02:58:4f:6c:23

37.16 show dot1x global

Description

The **show dot1x global** command is used to display the global configuration of 801.X.

Syntax

show dot1x global

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of 801.X globally:

T1700X-16TS(config)#show dot1x global

37.17 show dot1x interface

Description

The **show dot1x interface** command is used to display all ports or the specified port's configuration information of 801.X.

Syntax

show dot1x interface [**gigabitEthernet** *port*]

Parameter

port —— The Ethernet port number. If not specified, the information of all the ports will be displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration information of 801.X for port 20:

T1700X-16TS(config)#show dot1x interface ten-gigabitEthernet 1/0/2

Display the configuration information of 801.X for all Ethernet ports:

T1700X-16TS(config)#show dot1x interface

37.18 show dot1x auth-state interface

Description

The **show dot1x auth-state interface** command is used to display the authentication status of each port.

Syntax

show dot1x auth-state interface [**fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port*]

Parameter

port —— The Ethernet port number. If not specified, the information of all the ports will be displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the authentication status of each port:

```
T1700X-16TS(config)#show dot1x auth-state interface
```

Chapter 38 Port Security Commands

You can limit the number of MAC addresses that can be learned on each port on this page, thus preventing the MAC address table from being exhausted by the attack packets.

38.1 mac address-table max-mac count

Description

The **mac address-table max-mac-count** command is used to enable the port security feature of the port and configure the related parameters. To disable the feature and restore the parameters to defaults on the port, please use **no mac address-table max-mac-count** command.

Syntax

mac address-table max-mac-count { [max-number *num* **]**
[exceed-max-learned enable | disable **] [mode {** dynamic | static | permanent **}] [status {** forward | drop | disable **}] }**

no mac address-table max-mac-count [max-number | mode | status]

Command Mode

Interface Configuration Mode

Privilege Requirement

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

Example

Set the maximum number of MAC addresses that can be learned on port 1/0/1 as 30, enable exceed-max-leaned feature and configure the mode as permanent and the status as drop:

T1700X-16TS (config)#interface ten-gigabitEthernet 1/0/1

T1700X-16TS(config-if)#mac address-table max-mac-count max-number 30 **exceed-maxlearned** enable **mode** permanent **status** drop

38.2 show mac address-table max-mac-count

Description

The **show mac address-table max-mac-count** command is used to display the port security configuration on each port.

Syntax

show mac address-table max-mac-count interface { fastEthernet *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}**

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the port security configuration on port 1/0/1

T1700X-16TS# show mac address-table max-mac-count interface ten-gigabitEthernet 1/0/1

Chapter 39 Port Mirroring Commands

Port Mirroring allows the switch to send a copy of the traffic that passes through specified sources (ports, LAGs or the CPU) to a destination port. It does not affect the switching of network traffic on source ports, LAGs or the CPU. Usually, the monitoring port is connected to data diagnose device, which is used to analyze the monitored packets for monitoring and troubleshooting the network.

39.1 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 ten-gigabitEthernet** *port*

no monitor session *session_num* **destination interface ten-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:

T1700X-16TS(config)# monitor session 1 **destination interface ten-gigabitEthernet** 1/0/1

Delete the monitoring port 1/0/2 from monitor session 1：

T1700X-16TS(config)# no monitor session 1 **destination interface ten-gigabitEthernet** 1/0/2

Delete the monitor session 1:

T1700X-16TS(config)# no monitor session 1

39.2 monitor session source

Description

The **monitor session source** command is used to configure the monitored interface. To delete the corresponding monitored interface, please use **no monitor session source** command.

Syntax

monitor session *session_num* **source { cpu** *cpu_number* **| interface ten-gigabitEthernet** *port-list* | **interface port-channel** *port-channel-id* **}** *mode*

no monitor session *session_num* **source { cpu** *cpu_number* **| interface ten-gigabitEthernet** *port-list* | **interface port-channel** *port-channel-id* **}** *mode*

Parameter

session_num —— The monitor session number. It can only be specified as 1.

cpu_number —— The CPU number. It can only be specified as 1.

port-list —— List of the Ethernet port number. It is multi-optional.

lag-list —— List of LAG interfaces. It is multi-optional.

mode —— The monitor mode. There are three options: rx, tx and both. Rx (ingress monitoring mode), means the incoming packets received by the monitored interface will be copied to the monitoring port. Tx (egress monitoring mode), indicates the outgoing packets sent by the monitored interface will be copied to the monitoring port. Both (ingress and egress monitoring), presents the incoming packets received and the outgoing packets sent by the monitored interface will both be copied to the monitoring port.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin 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:

```
T1700X-16TS(config)# monitor session 1 source interface
ten-gigabitEthernet 1/0/4-5,1/0/7 rx
```

Delete port 4 in monitor session 1 and its configuration:

```
T1700X-16TS(config)# no monitor session 1 source interface
ten-gigabitEthernet 1/0/4 rx
```

39.3 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:

```
T1700X-16TS(config)# show monitor session 1
```

Chapter 40 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.

40.1 access-list create

Description

The **access-list create** command is used to create an ACL.

Syntax

access-list create *acl-id* [**name** *acl-name*]

no access-list create { *acl-id***}**

Parameter

acl-id ——Enter an ACL ID. The IDs for MAC ACL are from 0 to 499. The IDs for IP ACL are from 500 to 999. The IDs for Combined ACL are from 1000 to 1499.The IDs for IPv6 ACL are from 1500 to 1999.

acl-name —— Enter a name to identify the ACL.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create an IP ACL whose ID is 523:

```
T1700X-16TS(config)# access-list create 523
```

40.2 access-list resequence

Description

The **access-list resequence** command is used to resequence the rules by providing a Start Rule ID and Step value.

Syntax

access-list resequence *acl-id-or-name* **start** *start-rule-id* **step** *rule-id-step-value*

Parameter

acl-id-or-name —— The ACL ID or name.

start-rule-id —— The start rule ID.

rule-id-step-value —— The step value.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Resequence the rules of ACL 12 with the start ID as 1 and step value as 5:

```
T1700X-16TS(config)# access-list resequence 12 start 1 step 5
```

40.3 access-list mac

Description

The **access-list mac** command is used to create MAC ACL. To delete the MAC ACL, please use **no access-list mac**.

Syntax

access-list mac *acl-id-or-name* **rule {** auto | *rule-id***} {** deny | permit **} logging {**enable | disable**} [smac** *source-mac* **smask** *source-mac-mask* **] [dmac** *destination-mac* **dmask** *destination-mac-mask* **] [type** *ether-type***] [pri** *dot1p-priority***] [vid** *vlan-id***] [tseg** *time-range-name***]**

no access-list mac *acl-id-or-name* **rule** *rule-id*

Parameter

acl-id-or-name —— Enter the ID or name of the ACL that you want to add a rule for.

auto —— The rule ID will be assigned automatically and the interval between rule IDs is 5.

rule-id —— Assign an ID to the rule.

deny | permit —— Specify the action to be taken with the packets that match the rule. By default, it is set to permit. The packets will be discarded if “deny” is selected and forwarded if “permit” is selected.

enable | disable —— Enable or disable Logging function for the ACL rule. If "enable " is selected, the times that the rule is matched will be logged every 5 minutes. With ACL Counter trap enabled, a related trap will be generated if the matching times changes.

source-mac —— Enter the source MAC address. The format is FF:FF:FF:FF:FF:FF.

source-mac-mask —— Enter the mask of the source MAC address. This is required if a source MAC address is entered. The format is FF:FF:FF:FF:FF:FF.

destination-mac —— Enter the destination MAC address. The format is FF:FF:FF:FF:FF:FF.

destination-mac-mask —— Enter the mask of the destination MAC address. This is required if a destination MAC address is entered. The format is FF:FF:FF:FF:FF:FF.

ether-type —— Specify an Ethernet-type with 4 hexadecimal numbers.

dot1p-priority: The user priority ranges from 0 to 7. The default is No Limit.

vlan-id —— The VLAN ID ranges from 1 to 4094.

time-range-name —— The name of the time-range. The default is No Limit.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create MAC ACL 50 and configure Rule 5 to permit packets with source MAC address 00:34:a2:d4:34:b5:

T1700X-16TS (config)#access-list create 50

T1700X-16TS (config-mac-acl)#access-list mac 50 **rule** 5 **permit logging disable smac** 00:34:a2:d4:34:b5 **smask** ff:ff:ff:ff:ff:ff

40.4 access-list ip

Description

The **access-list ip** command is used to add IP ACL rule. To delete the corresponding rule, please use **no access-list ip** command. IP ACLs analyze and process data packets based on a series of match conditions, which can be the source IP addresses and destination IP addresses carried in the packets.

Syntax

access-list ip *acl-id-or-name* **rule {**auto **|** *rule-id***} {**deny | permit**} logging {**enable | disable**} [sip** *sip-address* **sip-mask** *sip-address-mask* **] [dip** *dip-address* **dip-mask** *dip-address-mask* **] [dscp** *dscp-value***] [tos** *tos-value***] [pre** *pre-value***] [frag** enable | disable**] [protocol** *protocol***/[s-port** *s-port-number***] [s-port-mask** *s-port-mask***] [d-port** *d-port-number***] [d-port-mask** *d-port-mask***] [tcpflag** *tcpflag***]] [tseg** *time-range-name***]**

no access-list ip *acl-id-or-name* **rule** *rule-id*

Parameter

acl-id-or-name —— Enter the ID or name of the ACL that you want to add a rule for.

auto —— The rule ID will be assigned automatically and the interval between rule IDs is 5.

rule-id —— Assign an ID to the rule.

deny | permit —— Specify the action to be taken with the packets that match the rule. By default, it is set to permit. The packets will be discarded if “deny” is selected and forwarded if “permit” is selected.

logging {enable | disable**}** —— Enable or disable Logging function for the ACL rule. If "enable" is selected, the times that the rule is matched will be logged every 5 minutes. With ACL Counter trap enabled, a related trap will be generated if the matching times changes.

sip-address —— Enter the source IP address.

sip-address-mask —— Enter the mask of the source IP address. This is required if a source IP address is entered.

dip-address —— Enter the destination IP address.

dip-address-mask —— Enter the mask of the destination IP address. This is required if a destination IP address is entered.

dscp-value —— Specify the DSCP value between 0 and 63.

tos-value ——Specify an IP ToS value to be matched between 0 and 15.

pre-value ——Specify an IP Precedence value to be matched between 0 and 7.

frag {enable | disable} —— Enable or disable matching of fragmented packets. The default is disable. When enabled, the rule will apply to all fragmented packets and always permit to forward the last fragment of a packet.

protocol —— Specify a protocol type.

s-port-number —— Specify the source port number.

s-port-mask —— Specify the source port mask with 4 hexadecimal numbers.

d-port-number —— Specify the destination port number.

d-port-mask —— Specify the destination port mask with 4 hexadacimal numbers.

tcpflag —— For TCP protocol, specify the flag value using either binary numbers or * (for example, 01*010*). The default is *, which indicates that the flag will not be matched. The flags are URG (Urgent flag), ACK (acknowledge flag), PSH(push flag), RST(reset flag),SYN(synchronize flag), and FIN(finish flag).

time-range-name —— The name of the time-range. The default is No Limit.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create IP ACL 600, and configure Rule 1 to permit packets with source IP address 192.168.1.100：

T1700X-16TS (config)#access-list create 600

T1700X-16TS (config)#access-list ip 600 **rule** 1 permit **logging** disable **sip** 192.168.1.100 **sip-mask** 255.255.255.255

40.5 access-list combined

Description

The **access-list combined** command is used to add Combined ACL rule. To delete the corresponding rule, please use **no access-list extended** command.

Syntax

access-list combined *acl-id-or-name* **rule** {auto | *rule-id*} {deny | permit} **logging** {enable | disable} [**smac** *source-mac-address* **smask** *source-mac-mask*] [**dmac** *dest-mac-address* **dmask** *dest-mac-mask*] [**vid** *vlan-id*] [**type** *ether-type*] [**pri** *priority*] [**sip** *source-ip-address* **sip-mask** *source-ip-mask*]] [**dip** *destination-ip-address* **dip-mask** *destination-ip-mask*] **[dscp** *dscp-value***] [tos** *tos-value***] [pre** *pre-value***] [protocol** *protocol***/[s-port** *s-port-number* **s-port-mask** *s-port-mask***] [d-port** *d-port-number* **d-port-mask** *d-port-mask***] [tcpflag** *tcpflag***]] [tseg** *time-range-name***]**

no access-list combined *acl-id-or-name* **rule** *rule-id*

Parameter

acl-id-or-name —— Enter the ID or name of the ACL that you want to add a rule for.

auto —— The rule ID will be assigned automatically and the interval between rule IDs is 5.

rule-id —— Assign an ID to the rule.

deny | permit —— Specify the action to be taken with the packets that match the rule. By default, it is set to permit. The packets will be discarded if “deny” is selected and forwarded if “permit” is selected.

logging {enable | disable} —— Enable or disable Logging function for the ACL rule. If "enable " is selected, the times that the rule is matched will be logged every 5 minutes. With ACL Counter trap enabled, a related trap will be generated if the matching times changes.

source-mac-address —— Enter the source MAC address.

source-mac-mask —— Enter the source MAC address mask.

dest-mac-address —— Enter the destination MAC address.

dest-mac-mask —— Enter the destination MAC address mask. This is required if a destination MAC address is entered.

vlan-id: The VLAN ID ranges from 1 to 4094.

ether-type —— Specify the Ethernet-type with 4 hexadecimal numbers.

priority —— The user priority ranges from 0 to 7. The default is No Limit.

source-ip: Enter the source IP address.

source-ip-mask —— Enter the mask of the source IP address. It is required if source IP address is entered.

destination-ip —— This is required if a source IP address is entered.

destination-ip-mask —— Enter the destination IP address mask. This is required if a destination IP address is entered.

dscp-value —— Specify the DSCP value between 0 and 63.

tos-value ——Specify an IP ToS value to be matched between 0 and 15.

pre-value ——Specify an IP Precedence value to be matched between 0 and 7.

protocol —— Specify a protocol type.

s-port-number —— Specify the source port number.

s-port-mask —— Specify the source port mask with 4 hexadecimal numbers.

d-port-number —— Specify the destination port number.

d-port-mask —— Specify the destination port mask with 4 hexadecimal numbers.

tcpflag —— For TCP protocol, specify the flag value using either binary numbers or * (for example, 01*010*). The default is *, which indicates that the flag will not be matched. The flags are URG (Urgent flag), ACK (acknowledge flag), PSH(push flag), RST(reset flag),SYN(synchronize flag), and FIN(finish flag).

time-range-name —— The name of the time-range. The default is No Limit.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create Combined ACL 1100 and configure Rule 1 to deny packets with source IP address 192.168.3.100 in VLAN 2:

T1700X-16TS(config)# access-list create 1100

T1700X-16TS(config)# access-list combined 1100 **logging** disable **rule** 1 permit **vid** 2 **sip** 192.168.3.100 **sip-mask** 255.255.255.255

40.6 access-list ipv6

Description

The **access-list ipv6** command is used to add IPv6 ACL rule. To delete the corresponding rule, please use **no access-list ipv6** command. IPv6 ACLs analyze and process data packets based on a series of match conditions, which can be the source IP addresses and destination IP addresses carried in the packets, the DSCP and flow-label value, etc.

Syntax

access-list ipv6 *acl-id-or-name* **rule** {auto | *rule-id* } {deny | permit} **logging** {enable | disable} [**class** *class-value*] [**flow-label** *flow-label-value*] [**sip** *source-ip-address* **sip-mask** *source-ip-mask*] [**dip** *destination-ip-address* **dip-mask** *destination-ip-mask*] [**s-port** *source-port-number*] [**d-port** *destination-port-number*] [**tseg** *time-range-name*]

no access-list ipv6 *acl-id-or-name* **rule** *rule-id*

Parameter

acl-id-or-name —— Enter the ID or name of the ACL that you want to add a rule for.

auto —— The rule ID will be assigned automatically and the interval between rule IDs is 5.

rule-id —— Assign an ID to the rule.

deny | permit —— Specify the action to be taken with the packets that match the rule. By default, it is set to permit. The packets will be discarded if “deny” is selected and forwarded if “permit” is selected.

logging {enable | disable} —— Enable or disable Logging function for the ACL rule. If "enable " is selected, the times that the rule is matched will be logged every 5 minutes. With ACL Counter trap enabled, a related trap will be generated if the matching times changes.

class-value —— Specify a class value to be matched. It ranges from 0 to 63.

flow-label-value —— Specify a Flow Label value to be matched.

source-ip-address —— Enter the source IP address. Enter the destination IPv6 address to be matched. All types of IPv6 address will be checked. You may enter a complete 128-bit IPv6 address but only the first 64 bits will be valid.

source-ip-mask —— Enter the source IP address mask. The mask is required if the source IPv6 address is entered. Enter the mask in complete format (for

example, ffff:ffff:0000:ffff). The mask specifies which bits in the source IPv6 address to match the rule.

destination-ip-address —— Enter the destination IPv6 address to be matched. All types of IPv6 address will be checked. You may enter a complete 128-bit IPv6 addresses but only the first 64 bits will be valid.

destination-ip-mask: Enter the source IP address mask. The mask is required if the source IPv6 address is entered. Enter the mask in complete format (for example, ffff:ffff:0000:ffff). The mask specifies which bits in the source IPv6 address to match the rule.

source-port-number —— Enter the TCP/UDP source port if TCP/UDP protocol is selected.

destination-port-number —— Enter the TCP/UDP destination port if TCP/UDP protocol is selected.

time-range-name —— The name of the time-range. The default is No Limit.

Command Mode

Global Configuration Mode

Privilege Requirement

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

User Guidelines

Before binding an IPv6 ACL to a VLAN or interface, you should configure the SDM template as "enterpriseV6" and save your configurations.

Example

Create IPv6 ACL 1600 and configure Rule 1 to deny packets with source IPv6 address CDCD:910A:2222:5498:8475:1111:3900:2020:

```
T1700X-16TS(config)# access-list create 1600
T1700X-16TS(config)# access-list ipv6 1600 rule 1 deny logging disable
sip CDCD:910A:2222:5498:8475:1111:3900:2020 sip-mask ffff:ffff:ffff:ffff
```

40.7 access-list action

Description

The **access-list action** command is used to specify a rule to be configured with policies and enter Action Configuration mode. To delete the corresponding policies, please use **no access-list action** command.

Syntax

access-list action *acl-id-or-name* **rule** *rule-id*

no access-list action *acl-id-or-name* **rule** *rule-id*

Parameter

acl-id-or-name —— Enter the ID or name of the ACL.

rule-id —— Enter the ID of the ACL rule.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the rule 1 of ACL 200 to be configured with policies:

T1700X-16TS(config)# access-list action 200 **rule** 1

40.8 redirect interface

Description

The **redirect interface** command is used to define the policy to redirect the matched packets to the desired port. To disable this policy, please use **no redirect interface** command.

Syntax

redirect interface { fastEthernet *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}**

no redirect interface { fastEthernet *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}**

Parameter

port —— The destination port to which the packets will be redirected. The default is All.

Command Mode

Action Configuration Mode

Privilege Requirement

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

Example

Define the policy to redirect the matched packets to port 1/0/1 for rule 1 of ACL 6:

T1700X-16TS(config)# access-list action 6 **rule** 1

T1700X-16TS(config-action)# redirect interface ten-gigabitEthernet 1/0/1

40.9 s-condition

Description

The **s-condition** command is used to limit the rate of the matched packets. To restore the settings to the defaults, please use **no s-condition**.

Syntax

s-condition rate *rate* **burst** *burst-size* **osd { none | discard }**

no s-condition

Parameter

rate —— Specify a rate, ranging from 0 to 1000000kbps.

burst-size —— Specify the number of bytes allowed in one second ranging from 1 to 128.

osd ——Select either "none" or "discard" as the action to be taken for the packets whose rate is beyond the specified rate. The default is None.

Command Mode

Action Configuration Mode

Privilege Requirement

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

Example

Configure a policy for rule 1 of ACL 6: limit the transmission rate of the matched packets as 1000 Kbps and if the number of bytes per second is beyond 100, the packets will be discarded by the switch:

T1700X-16TS(config)#access-list action 6 **rule** 1

T1700X-16TS(config-action)# s-condition rate 1000 **burst** 100 **osd** discard

40.10 s-mirror

Description

The **s-mirror** command is used to define the policy to mirror the matched packets to the desired port. To disable this policy, please use **no s-mirror** command.

Syntax

s-mirror interface { **fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* }

Parameter

port —— The destination port to which the packets will be mirrored.

Command Mode

Action Configuration Mode

Privilege Requirement

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

Example

Configure a policy for rule 1 of ACL 6: specify the mirror port as Port 1/0/2 for the data packets matching this rule:

```
T1700X-16TS(config)#access-list action 6 rule 1
T1700X-16TS(config-action)#s-mirror interface ten-gigabitEthernet 1/0/2
```

40.11 qos-remark

Description

The **qos-remark** command is used to configure QoS Remark function of policy action. To restore the settings to the default, please use no **qos-remark**.

Syntax

qos-remark [**dscp** *dscp*] [**priority** *pri*] [**dot1p** dot1p-pri]

no qos-remark

Parameter

dscp —— DSCP of QoS Remark. Specify the DSCP region for the data packets matching the corresponding ACL. DSCP ranges from 0 to 63. By default, it is not limited.

pri —— Local Priority of QoS Remark. Specify the local priority for the data packets matching the corresponding ACL. Local Priority ranges from 0 to 7.

dot1p-pri —— 802.1P priority of QoS Remark. This remark configuration will change the data packet's 802.1P priority field to the dot1p-pri you set. 802.1P priority ranges from 0 to 7.

Command Mode

Action Configuration Mode

Privilege Requirement

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

Example

Configure a policy for rule 1 of ACL 6: specify the DSCP region as 30 and local priority 2 for the packets matching this rule:

T1700X-16TS(config)#access-list action 6 **rule** 1

T1700X-16TS(config-action)# qos-remark dscp 30 **priority** 2

40.12 access bind

Description

The **access-list policy name** command is used to add Policy. To delete the corresponding Policy, please use **no access-list policy name** command. A Policy is used to control the data packets those match the corresponding ACL rules.

Syntax

access-list bind *acl-id-or-name* **interface { [vlan** *vlan-list* **] | [fastEthernet** *port-list* **] | [gigabitEthernet** *port-list* **] | [ten-gigabitEthernet** *port-list* **] }**

no access-list bind *acl-id-or-name* **interface { [vlan** *vlan-list* **] | [fastEthernet** *port-list* **] | [gigabitEthernet** *port-list* **] | [ten-gigabitEthernet** *port-list* **] }**

Parameter

acl-id-or-name —— Enter the ID or name of the ACL that you want to add a rule for.

vlan-list —— Specify the ID or the ID list of the VLAN(s) that you want to bind the ACL to. The valid values are from 1 to 4094, for example, 2-3,5.

port-list —— Specify the number or the list of the Ethernet port that you want to bind the ACL to.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Bind ACL 1 to port 3 and VLAN 4:

```
T1700X-16TS(config)#access-list bind 1 interface vlan 4 gigabitEthernet 1/0/3
```

40.13 show access-list

Description

The **show access-list** command is used to display configuration of ACL.

Syntax

show access-list *acl-id-or-name*

Parameter

acl-id-or-name —— The ID or name of the ACL selected to display the configuration.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of the MAC ACL whose ID is 20:

```
T1700X-16TS(config)# show access-list 20
```

40.14 show access-list bind

Description

The **show access-list bind** command is used to display the configuration of ACL binding.

Syntax

show access-list bind

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of Policy bind:

```
T1700X-16TS(config)# show access-list bind
```

40.15 show access-list status

Description

The **show access-list status** command is used to display usage status of ACL entry resource.

Syntax

show access-list status

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the usage status of ACL entry resource:

```
T1700X-16TS(config)# show access-list status
```

40.16 show access-list counter

Description

The **show access-list counter** command is used to display the packet counter of a specified ACL.

Syntax

show access-list *acl-id-or-name* **counter**

Parameter

acl-id-or-name —— The ID or name of the ACL to display.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the packet counter of ACL 100:

```
T1700X-16TS(config)# show access-list 100 counter
```

40.17 clear access-list

Description

The **clear access-list** command is used to clear the counter of matched packets of a specified ACL or rule.

Syntax

clear access-list *acl-id-or-name* **[rule** *rule-id***]**

Parameter

acl-id-or-name —— The ID or name of the ACL.

rule-id—— The ID of the rule.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Clear the packet counter of ACL 100:

```
T1700X-16TS(config)# clear access-list 100
```

Chapter 41 IPv4 IMPB Commands

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

41.1 ip source binding

Description

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

Syntax

ip source binding *hostname ip-addr mac-addr* **vlan** *vlan-id* **interface** { **fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id* } { none | arp-detection | ip-verify-source | both }

no ip source binding index *ip-addr*

Parameter

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

ip-addr—— The IP address of the Host.

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

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

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

none | arp-detection | ip-verify-source | both ——The protect type for the entry. “arp-detection” indicates ARP detection; “ip-verify-source” indicates IP source filter; “none” indicates applying none; “both” indicates applying both.

ip-addr—— The IP address of the entry to be deleted.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

T1700X-16TS(config)#ip source binding host1 192.168.0.1 00:00:00:00:00:01 **vlan** 2 **interface ten-gigabitEthernet** 1/0/5 arp-detection

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

T1700X-16TS(config)#no ip source binding index 5

41.2 ip dhcp snooping

Description

The **ip dhcp snooping** command is used to enable DHCP Snooping function globally. To disable DHCP Snooping function globally, please use **no ip dhcp snooping** command. DHCP Snooping functions to monitor the process of the Host obtaining the IP address from DHCP server, and record the IP address, MAC address, VLAN and the connected Port number of the Host for automatic binding.

Syntax

ip dhcp snooping

no ip dhcp snooping

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the DHCP Snooping function globally:

T1700X-16TS(config)#ip dhcp snooping

41.3 ip dhcp snooping vlan

Description

The **ip dhcp snooping vlan** command is used to enable DHCP Snooping function on a specified VLAN. To disable DHCP Snooping function on this VLAN, please use **no ip dhcp snooping vlan** command.

Syntax

ip dhcp snooping vlan *vlan-range*

no ip dhcp snooping vlan *vlan-range*

Parameter

vlan-range —— Specify the VLANs to enable the DHCP snooping function, in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the DHCP Snooping function on VLAN 1,4,6-7:

```
T1700X-16TS(config)#ip dhcp snooping vlan 1,4,6-7
```

41.4 ip dhcp snooping max-entries

Description

The **ip dhcp snooping max-entries** command is used to configure the maximum number of entries that can be learned on a port via DHCP Snooping. To restore to the default setting, please use **no ip dhcp snooping max-entries** command.

Syntax

ip dhcp snooping max-entries *value*

no ip dhcp snooping max-entries

Syntax

value —— Enter the value of maximum number of entries that can be learned on the port via DHCP Snooping.

Command Mode

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

Privilege Requirement

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

Example

Configure the maximum number of entries that can be learned on port 1 as 100:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/1

T1700X-16TS(config-if)#ip dhcp snooping max-entries 100

41.5 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:

T1700X-16TS(config)#show ip source binding

41.6 show ip dhcp snooping

Description

The **show ip dhcp snooping** command is used to display the running status of DHCP Snooping.

Syntax

show ip dhcp snooping

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the running status of DHCP Snooping:

```
T1700X-16TS#show ip dhcp snooping
```

41.7 show ip dhcp snooping interface

Description

The **show ip dhcp snooping interface** command is used to display the DHCP Snooping configuration of a desired Port/port channel or of all Ethernet ports/port channels.

Syntax

show ip dhcp snooping interface [**gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parameters

port—— The Ethernet port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DHCP Snooping configuration of all Ethernet ports and port channels:

T1700X-16TS#show ip dhcp snooping interface

Display the DHCP Snooping configuration of Port 1/0/5:

T1700X-16TS#show ip dhcp snooping interface ten-gigabitEthernet 1/0/5

Chapter 42 IPv6 IMPB Commands

You can bind the IPv6 address, MAC address, VLAN and the connected Port number of the Host together, which can be the condition for the ARP Inspection and IP verify source to filter the packets.

42.1 Ipv6 source binding

Description

The **ipv6 source binding** command is used to bind the IPv6 address, MAC address, VLAN ID and the Port number together manually. You can manually bind the IPv6 address, MAC address, VLAN ID and the Port number together in the condition that you have got the related information of the Hosts in the LAN. To delete the IPv6-MAC–VID-PORT entry from the binding table, please use **no ipv6 source binding index** command.

Syntax

Ipv6 source binding *hostname ipv6-addr mac-addr* **vlan** *vlan-id* **interface** { **fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id* } { none | nd-detection | ipv6-verify-source | both }

no ipv6 source binding index *ipv6-addr*

Parameter

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

Ipv6-addr—— The IP address of the Host.

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

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

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

none | nd-detection | ipv6-verify-source | both ——The protect type for the entry. “nd-detection” indicates ND detection; “ipv6-verify-source” indicates IPv6 source filter; “none” indicates applying none; “both” indicates applying both.

Ipv6-addr—— The IPv6 address of the entry to be deleted.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

The following example shows how to bind an entry with the hostname host1, IPv6 address 2001:0:9d38:90d5::34, MAC address AA-BB-CC-DD-EE-FF, VLAN ID 10, port number 1/0/5, and enable this entry for ND Detection.

T1700X-16TS(config)# ipv6 source binding host1 2001:0:9d38:90d5::34 aa:bb:cc:dd:ee:ff **vlan** 10 **interface ten-gigabitEthernet** 1/0/5 nd-detection

42.2 ipv6 dhcp snooping

Description

The **ipv6 dhcp snooping** command is used to enable DHCPv6 Snooping function globally. To disable DHCPv6 Snooping function globally, please use **no ipv6 dhcp snooping** command. DHCPv6 Snooping functions to monitor the process of the Host obtaining the IP address from DHCPv6 server, and record the IPv6 address, MAC address, VLAN and the connected Port number of the Host for automatic binding.

Syntax

Ipv6 dhcp snooping

no ipv6 dhcp snooping

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the DHCPv6 Snooping function globally:

T1700X-16TS(config)#ipv6 dhcp snooping

42.3 ipv6 dhcp snooping vlan

Description

The **ipv6 dhcp snooping vlan** command is used to enable DHCP Snooping function on a specified VLAN. To disable DHCP Snooping function on this VLAN, please use **no ipv6 dhcp snooping vlan** command.

Syntax

ipv6 dhcp snooping vlan *vlan-range*

no ipv6 dhcp snooping vlan *vlan-range*

Parameter

vlan-range —— Specify the VLANs to enable the DHCP snooping function, in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the DHCPv6 Snooping function on VLAN 1,4,6-7:

```
T1700X-16TS(config)#ipv6 dhcp snooping vlan 1,4,6-7
```

42.4 ipv6 dhcp snooping max-entries

Description

The **ipv6 dhcp snooping max-entries** command is used to configure the maximum number of entries that can be learned on a port via DHCPv6 Snooping. To restore to the default setting, please use **no ipv6 dhcp snooping max-entries** command.

Syntax

Ipv6 dhcp snooping max-entries *value*

no ipv6 dhcp snooping max-entries

Syntax

value: Enter the value of maximum number of entries that can be learned on the port via DHCPv6 Snooping.

Command Mode

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

Privilege Requirement

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

Example

Configure the maximum number of entries that can be learned on port 1 as 100:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/1

T1700X-16TS(config-if)#ipv6 dhcp snooping max-entries 100

42.5 ipv6 nd snooping

Description

The **ipv6 nd snooping** command is used to enable ND snooping function globally. To disable ND Snooping function globally, please use **no ipv6 nd snooping** command. ND Snooping functions to monitor the process of the duplication address detection, and record the IPv6 address, MAC address, VLAN and the connected Port number of the Host for automatic binding.

Syntax

ipv6 nd snooping

no ipv6 nd snooping

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the ND snooping function globally:

T1700X-16TS (config)#ipv6 nd snooping

42.6 ipv6 nd snooping vlan

Description

The **ipv6 nd snooping vlan** command is used to enable ND snooping function on a specified VLAN. To disable ND Snooping function on this VLAN, please use **no ipv6 nd snooping vlan** command.

Syntax

ipv6 nd snooping vlan *vlan-range*

no ipv6 nd snooping vlan *vlan-range*

Parameter

vlan-range —— Specify the VLANs to enable the ND snooping function, in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the ND snooping function on VLAN 1,4,6-7:

T1700X-16TS(config)#ipv6 nd snooping vlan 1,4,6-7

42.7 ipv6 nd snooping max-entries

Description

The **ipv6 nd snooping max-entries** command is used to specify the maximum number of binding entries that are allow to be bound to a port. To return the default, please use **no ipv6 nd snooping max-entries** command.

Syntax

ipv6 nd snooping max-entries *value*

no ipv6 nd snooping max-entries

Parameter

value —— Specify the maximum number of ND snooping entries on this interface.

Command Mode

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

Privilege Requirement

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

Example

Configure the maximum number of binding entries from ND Snooping of Port 1/0/2 is 100:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/2

T1700X-16TS(config-if)#ipv6 nd snooping max-entries 100

42.8 show ipv6 source binding

Description

The **show ipv6 source binding** command is used to display the IPv6-MAC-VID- PORT binding table.

Syntax

show ipv6 source binding

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IPv6-MAC-VID-PORT binding table:

T1700X-16TS(config)#show ipv6 source binding

42.9 show ipv6 dhcp snooping

Description

The **show ipv6 dhcp snooping** command is used to display the running status of DHCPv6 Snooping.

Syntax

show ipv6 dhcp snooping

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the running status of DHCPv6 Snooping:

```
T1700X-16TS#show ipv6 dhcp snooping
```

42.10 show ipv6 dhcp snooping interface

Description

The **show ipv6 dhcp snooping interface** command is used to display the DHCPv6 Snooping configuration of a desired Port/port channel or of all Ethernet ports/port channels.

Syntax

show ipv6 dhcp snooping interface [**gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parameters

port—— The Ethernet port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DHCPv6 Snooping configuration of all Ethernet ports and port channels:

T1700X-16TS#show ipv6 dhcp snooping interface

Display the DHCPv6 Snooping configuration of Port 1/0/5:

T1700X-16TS#show ipv6 dhcp snooping interface ten-gigabitEthernet 1/0/5

42.11 show ipv6 nd snooping

Description

The **show ipv6 nd snooping** command is used to display the running status of ND Snooping.

Syntax

show ipv6 nd snooping

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the running status of ND Snooping:

T1700X-16TS#show ipv6 nd snooping

Chapter 43 IP Verify Source Commands

IP Verify Source is to filter the IP packets based on the IP-MAC Binding entries. Only the packets matched to the IP-MAC Binding rules can be processed, which can enhance the bandwidth utility.

43.1 ip verify source

Description

The **ip verify source** command is used to configure the IP Verify Source mode for a specified port. To disable the IP Verify Source function, please use **no ip verify source** command.

Syntax

ip verify source sip+mac

no ip verify source

Parameter

sip+mac —— Security type. "sip+mac" indicates that only the packets with its source IP address, source MAC address and port number matched to the IP-MAC binding rules can be processed.

Command Mode

Interface Configuration Mode (interface ten-gigabitEthernet / interface range ten-gigabitEthernet)

Privilege Requirement

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

Example

Enable the IP Verify Source function for Ports 5-10. Configure that only the packets with its source IP address, source MAC address and port number matched to the IP-MAC binding rules can be processed:

T1700X-16TS(config)#interface range ten-gigabitEthernet 1/0/5-10

T1700X-16TS(config-if-range)#ip verify source sip+mac

43.2 ip verify source logging

Description

The **ip verify source logging** command is used to enable the log feature. With this feature enabled, the switch will generate a log when illegal packets are received. To disable the log feature, please use **no ip verify source logging** command.

Syntax

ip verify source logging

no ip verify source logging

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the log feature to make the switch generate logs when receiving illegal packets:

```
T1700X-16TS(config)#ip verify source logging
```

43.3 show ip verify source

Description

The **show ip verify source** command is used to display the IP Verify Source configuration information.

Syntax

show ip verify source

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IP Verify Source configuration information:

T1700X-16TS(config)#show ip verify source

43.4 show ip verify source interface

Description

The **show ip verify source interface** command is used to display the IP verify source configuration of a desired Port.

Syntax

show ip verify source interface [fastEthernet *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]**

Parameters

port —— The Ethernet port number.

port-channel-id —— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IP verify source configuration of Port 1/0/5:

T1700X-16TS#show ip verify source interface ten-gigabitEthernet 1/0/5

Chapter 44 IPv6 Verify Source Commands

IPv6 Verify Source is to filter the IPv6 packets based on the IPv6-MAC Binding entries. Only the packets matched to the IPv6-MAC Binding rules can be processed, which can enhance the bandwidth utility.

Before configuring IPv6 Verify Source feature, you should configure the SDM template as "enterpriseV6" and save your configurations.

44.1 ipv6 verify source

Description

The **ipv6 verify source** command is used to configure the IPv6 Verify Source mode for a specified port. To disable the IPv6 Verify Source function, please use **no ipv6 verify source** command.

Syntax

ipv6 verify source { sipv6+mac | sipv6 }

no ipv6 verify source

Parameter

sipv6+mac —— Security type. "sipv6+mac" indicates that only the packets with its source IPv6 address, source MAC address and port number matched to the IPv6-MAC binding rules can be processed.

sipv6 —— Security type. "sipv6" indicates that only the packets with its source IPv6 address and port number matched to the IPv6-MAC binding rules can be processed.

Command Mode

Interface Configuration Mode (interface ten-gigabitEthernet / interface range ten-gigabitEthernet)

Privilege Requirement

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

Example

Enable the IPv6 Verify Source function for Ports 5-10. Configure that only the packets with its source IPv6 address, source MAC address and port number matched to the IPv6-MAC binding rules can be processed:

T1700X-16TS(config)#interface range ten-gigabitEthernet 1/0/5-10

T1700X-16TS(config-if-range)#ipv6 verify source sipv6+mac

44.2 show ipv6 verify source

Description

The **show ipv6 verify source** command is used to display the IPv6 Verify Source configuration information.

Syntax

show ipv6 verify source

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IPv6 Verify Source configuration information:

T1700X-16TS(config)#show ipv6 verify source

44.3 show ipv6 verify source interface

Description

The **show ipv6 verify source interface** command is used to display the IPv6 verify source configuration of a desired Port.

Syntax

show ipv6 verify source interface ten-gigabitEthernet *port*

Parameters

port—— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IPv6 verify source configuration of Port 1/0/5:

```
T1700X-16TS#show ipv6 verify source interface ten-gigabitEthernet 1/0/5
```

Chapter 45 DHCPv4 Filter Commands

DHCPv4 Filter function allows the user to not only to restrict all DHCP Server packets but also to receive any specified DHCP server packet by any specified DHCP client, it is useful when one or more DHCP servers are present on the network and both provide DHCP services to different distinct groups of clients.

45.1 ip dhcp filter

Description

The **ip dhcp filter** command is used to enable DHCP Filter function globally. To disable DHCP Filter function globally, please use **no ip dhcp filter** command.

Syntax

ip dhcp filter

no ip dhcp filter

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the DHCP Filter function globally:

```
T1700X-16TS(config)#ip dhcp filter
```

45.2 ip dhcp filter (interface)

Description

The **ip dhcp filter (interface)** command is used to enable DHCP Filter function on a specified port. To disable DHCP Filter function on this port, please use **no ip dhcp filter (interface)** command.

Syntax

ip dhcp filter

no ip dhcp filter

Command Mode

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

Privilege Requirement

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

Example

Enable the DHCP Filter on port 1/0/1

```
T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/1
T1700X-16TS(Config-if)#ip dhcp filter
```

45.3 ip dhcp filter mac-verify

Description

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

Syntax

ip dhcp filter mac-verify

no ip dhcp filter mac-verify

Command Mode

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

Privilege Requirement

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

Example

Enable the MAC Verify feature for the Port 10/2:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/2

T1700X-16TS(config-if)#ip dhcp filter mac-verify

45.4 ip dhcp filter limit rate

Description

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

Syntax

ip dhcp filter limit rate *value*

no ip dhcp filter limit rate

Parameter

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

Command Mode

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

Privilege Requirement

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

Example

Set the Flow Control of GigabitEthernet port 2 as 20 pps:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/2

T1700X-16TS(config-if)#ip dhcp filter limit rate 20

45.5 ip dhcp filter decline rate

Description

The **ip dhcp filter decline rate** command is used to enable the Decline Protect feature and configure the rate limit on DHCP Decine packets. The excessive DHCP Decline packets will be discarded. To disable the Decline Protect feature, please use **no ip dhcp filter decline rate** command.

Syntax

ip dhcp filter decline rate *value*

no ip dhcp filter decline rate

Parameter

value —— Specify the rate limit of DHCP Decline packets, and the optional values are 0, 5, 10, 15, 20, 25 and 30 (units:packet/second). It default value is 0, which stands for "disable".

Command Mode

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

Privilege Requirement

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

Example

Configure the rate limit of DHCP Decline packets as 20 packets per second on Port 1/0/2:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/2

T1700X-16TS(config-if)#ip dhcp filter decline 20

45.6 ip dhcp filter server permit-entry

Description

The **ip dhcp filter server permit-entry** command is used to add entry for the legal DHCP server. To restore to the default option, please use **no ip dhcp snooping information strategy** command.

Syntax

ip dhcp filter server permit-entry server-ip *ipAddr* **client-mac** *macAddr* **interface { fastEthernet** *port* **| gigabitEthernet port | ten-gigabitEthernet** *port* **| interface port-channel** *port-channel-id***}**

no ip dhcp filter server permit-entry server-ip *ipAddr* **client-mac** *macAddr* **interface { fastEthernet** *port* **| gigabitEthernet port | ten-gigabitEthernet** *port* **| interface port-channel** *port-channel-id***}**

Parameter

ipAddr —— Specify the IP address of the legal DHCPv4 server.

macAddr —— Specify the MAC address of the DHCP Client. The value "all" means all client mac addresses.

port-list / *port-channel-id* —— Specify the port that the legal DHCPv4 server is connected to.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create an entry for the legal DHCPv4 server whose IP address is 192.168.0.100 and connected port number is 1/0/1 without client MAC address restricted:

T1700X-16TS(config)#ip dhcp filter server permit-entry server-ip 192.168.0.100 **client-mac** all **interface ten-gigabitEthernet** 1/0/1

45.7 show ip dhcp filter

Description

The **show ip dhcp filter** command is used to display the configuration of DHCP Filter.

Syntax

show ip dhcp filter

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DHCP Filter configuration:

```
T1700X-16TS#show ip dhcp filter
```

45.8 show ip dhcp filter interface

Description

The **show ip dhcp filter interface** command is used to display the configuration of DHCP Filter on ports.

Syntax

show ip dhcp filter interface [fastEthernet *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]**

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DHCP Filter configuration on port 1/0/3:

```
T1700X-16TS#show ip dhcp filter interface ten-gigabitEthernet 1/0/3
```

45.9 show ip dhcp filter server permit-entry

Description

The **show ip dhcp filter server permit-entry** command is used to display the legal server configuration.

Syntax

show ip dhcp filter server permit-entry

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the legal DHCP server configuration:

```
T1700X-16TS#show ip dhcp filter server permit-entry
```

Chapter 46 DHCPv6 Filter Commands

DHCPv6 Filter function allows the user to not only to restrict all DHCPv6 Server packets but also to receive any specified DHCPv6 server packet by any specified DHCPv6 client, it is useful when one or more DHCPv6 servers are present on the network and both provide DHCPv6 services to different distinct groups of clients.

46.1 ipv6 dhcp filter

Description

The **ipv6 dhcp filter** command is used to enable DHCP Filter function globally. To disable DHCPv6 Filter function globally, please use **no ipv6 dhcp filter** command.

Syntax

Ipv6 dhcp filter

no ipv6 dhcp filter

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the DHCPv6 Filter function globally:

```
T1700X-16TS(config)#ipv6 dhcp filter
```

46.2 ipv6 dhcp filter (interface)

Description

The **ipv6 dhcp filter (interface)** command is used to enable DHCPv6 Filter function on a specified port. To disable DHCPv6v Filter function on this port, please use **no ipv6 dhcp filter (interface)** command.

Syntax

ipv6 dhcp filter

no ipv6 dhcp filter

Command Mode

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

Privilege Requirement

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

Example

Enable the DHCPv6 Filter on port 1/0/1

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/1

T1700X-16TS(Config-if)#ipv6 dhcp filter

46.3 ipv6 dhcp filter limit rate

Description

The **ipv6 dhcp filter limit rate** command is used to enable the Flow Control feature for the DHCPv6 packets. The excessive DHCPv6 packets will be discarded. To restore to the default configuration, please use **no ipv6 dhcp filter limit rate** command.

Syntax

Ipv6 dhcp filter limit rate *value*

no ipv6 dhcp filter limit rate

Parameter

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

Command Mode

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

Privilege Requirement

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

Example

Set the Flow Control of GigabitEthernet port 2 as 20 pps:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/2

T1700X-16TS(config-if)#ipv6 dhcp filter limit rate 20

46.4 ipv6 dhcp filter decline rate

Description

The **ipv6 dhcp filter decline rate** command is used to enable the Decline Protect feature and configure the rate limit on DHCP Decine packets. The excessive DHCPv6 Decline packets will be discarded. To disable the Decline Protect feature, please use **no ipv6 dhcp filter decline rate** command.

Syntax

Ipv6 dhcp filter decline rate *value*

no ipv6 dhcp filter decline rate

Parameter

value —— Specify the rate limit of DHCPv6 Decline packets, and the optional values are 0, 5, 10, 15, 20, 25 and 30 (units:packet/second). It default value is 0, which stands for “disable”.

Command Mode

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

Privilege Requirement

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

Example

Configure the rate limit of DHCPv6 Decline packets as 20 packets per second on Port 1/0/2:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/2

T1700X-16TS(config-if)#ipv6 dhcp filter decline 20

46.5 ipv6 dhcp filter server permit-entry

Description

The **ipv6 dhcp filter server permit-entry** command is used to add entry for the legal DHCPv6 server. To restore to the default option, please use **no ipv6 dhcp snooping information strategy** command.

Syntax

Ipv6 dhcp filter server permit-entry server-ip *ipAddr* **interface { fastEthernet** *port* **| gigabitEthernet port | ten-gigabitEthernet** *port* **| interface port-channel** *port-channel-id***}**

no ipv6 dhcp filter server permit-entry server-ip *ipAddr* **interface { fastEthernet** *port* **| gigabitEthernet port | ten-gigabitEthernet** *port* **| interface port-channel** *port-channel-id***}**

Parameter

ipAddr —— Specify the IPv6 address of the legal DHCPv6 server.

port-list / *port-channel-id* —— Specify the port that the legal DHCPv6 server is connected to.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create an entry for the legal DHCPv6 server whose IP address is 192.168.0.100 and connected port number is 1/0/1:

T1700X-16TS(config)#ipv6 dhcp filter server permit-entry server-ip 2003::1 **interface ten-gigabitEthernet** 1/0/1

46.6 show ipv6 dhcp filter

Description

The **show ipv6 dhcp filter** command is used to display the configuration of DHCPv6 Filter.

Syntax

show ipv6 dhcp filter

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DHCPv6 Filter configuration:

T1700X-16TS#show ipv6 dhcp filter

46.7 show ipv6 dhcp filter interface

Description

The **show ipv6 dhcp filter interface** command is used to display the configuration of DHCPv6 Filter on ports.

Syntax

show ipv6 dhcp filter interface [fastEthernet *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]**

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DHCPv6 Filter configuration on port 1/0/3:

T1700X-16TS#show ipv6 dhcp filter interface ten-gigabitEthernet 1/0/3

46.8 show ip dhcp filter server permit-entry

Description

The **show ipv6 dhcp filter server permit-entry** command is used to display the legal server configuration.

Syntax

show ipv6 dhcp filter server permit-entry

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the legal DHCPv6 server configuration:

```
T1700X-16TS#show ipv6 dhcp filter server permit-entry
```

Chapter 47 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.

47.1 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:

```
T1700X-16TS(config)#ip dos-prevent
```

47.2 ip dos-prevent type

Description

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

Syntax

ip dos-prevent type { land | scan-synfin | xma-scan | null-scan | port-less-1024 | blat | ping-flood | syn-flood | win-nuke | ping-of-death | smurf }

no ip dos-prevent type { land | scan-synfin | xma-scan | null-scan | port-less-1024 | blat | ping-flood | syn-flood | win-nuke | ping-of-death | smurf }

Parameter

land ——The attacker sends a specific fake SYN (synchronous) packet to the destination host. Because both of the source IP address and the destination IP address of the SYN packet are set to be the IP address of the host, the host will be trapped in an endless circle of building the initial connection.

scan-synfin ——The attacker sends the packet with its SYN field and the FIN field set to 1. The SYN field is used to request initial connection whereas the FIN field is used to request disconnection. Therefore, the packet of this type is illegal.

xma-scan ——The attacker sends the illegal packet with its TCP index, FIN, URG and PSH field set to 1.

null-scan ——The attacker sends the illegal packet with its TCP index and all the control fields set to 0. During the TCP connection and data transmission, the packets with all control fields set to 0 are considered illegal.

port-less-1024 ——The attacker sends the illegal packet with its TCP SYN field set to 1 and source port smaller than 1024.

blat ——The attacker sends the illegal packet with the same source port and destination port on Layer 4 and with its URG field set to 1. Similar to the Land Attack, the system performance of the attacked host is reduced because the Host circularly attempts to build a connection with the attacker.

ping-flood ——The attacker floods the destination system with Ping packets, creating a broadcast storm that makes it impossible for the system to respond to legal communication.

syn-flood ——The attacker uses a fake IP address to send TCP request packets to the server. Upon receiving the request packets, the server responds with SYN-ACK packets. Since the IP address is fake, no response will be returned. The server will keep on sending SYN-ACK packets. If the attacker sends overflowing fake request packets, the network resource will be occupied maliciously and the requests of the legal clients will be denied.

win-nuke ——Because the Operation System with bugs cannot correctly process the URG (Urgent Pointer) of TCP packets, the attacker sends this

type of packets to the TCP port139 (NetBIOS) of the host with the Operation System bugs, which will cause the host with a blue screen.

ping-of-death ——Ping of Death attack means that the attacker sends abnormal ping packets larger than 65535 bytes to cause system crash on the target computer.

smurf ——Smurf attack is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic.

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:

T1700X-16TS(config)#ip dos-prevent type land

47.3 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:

```
T1700X-16TS(config)#show ip dos-prevent
```

Chapter 48 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).

48.1 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:

```
T1700X-16TS(config)# dldp
```

48.2 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:

T1700X-16TS(config)# dldp interval 10

48.3 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:

T1700X-16TS(config)# dldp shut-mode manual

48.4 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 ten-gigabitEthernet / interface range ten-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:

T1700X-16TS (config)# interface range ten-gigabitEthernet 1/0/2-4

T1700X-16TS (config-if-range)# dldp

48.5 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:

```
T1700X-16TS# show dldp
```

48.6 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 Port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration and state of all ports:

```
T1700X-16TS# show dldp interface
```

Display the configuration and state of port 1/0/5:

```
T1700X-16TS# show dldp interface ten-gigabitEthernet 1/0/5
```

Chapter 49 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.

49.1 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:

```
T1700X-16TS(config)# snmp-server
```

49.2 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:

```
T1700X-16TS(config)# snmp-server view view1 1.3.6.1.6.3.20 include
```

49.3 snmp-server group

Description

The **snmp-server group** command is used to manage and configure the SNMP group. To delete the corresponding SNMP group, please use **no snmp-server group** command. SNMP v3 provides the VACM (View-based Access Control Model) and USM (User-Based Security Model) mechanisms for authentication. The users in the SNMP Group can manage the device via the Read View, Write View and Notify View. And the authentication mode and the privacy mode guarantee the high security for the communication between the management station and the managed device.

Syntax

snmp-server group *name* [**smode** v3] [**slev** { noAuthNoPriv | authNoPriv | authPriv }] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*]

no snmp-server group *name* **smode** v3 **slev** { noAuthNoPriv | authNoPriv | authPriv }

Parameter

name ——The SNMP Group name, ranging from 1 to 16 characters. The Group Name, Security Model and Security Level compose the identifier of the

SNMP Group. These three items of the Users in one group should be the same.

v3 —— The security mode for the group, v3 indicates SNMPv3, the most secure level.

slev —— The Security Level of SNMP v3 Group. There are three options, including noAuthNoPriv (no 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:

T1700X-16TS(config)# snmp-server group group1 **smode** v3 **slev**

authNoPriv **read** viewDefault **write** viewDefault **notify** viewDefault

Delete group 1:

T1700X-16TS(config)# no snmp-server group group1 **smode** v3 **slev**

authNoPriv

49.4 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** 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. As the remote engine ID and user password are used to compute the authentication and privacy digests, before configuring a remote user, you need to set the remote engine ID first.

group-name —— The Group Name of the User. The User is classified to the corresponding Group according to its Group Name, Security Model and Security Level.

v3 ——The security mode for the user. v3 indicates SNMPv3, the most secure model.

slev —— The Security Level of SNMP v3 Group. There are three options, including noAuthNoPriv (no authorization and no encryption), authNoPriv (authorization and no encryption) and authPriv (authorization and encryption). The security level from highest to lowest is: noAuthNoPriv, authNoPriv, authPriv, and the default is noAuthNoPriv. The security level of the user should not be lower than the group it belongs to.

cmode —— The Authentication Mode of the SNMP v3 User, with none, MD5 and SHA options. None indicates no authentication method is used, MD5 indicates the port authentication is performed via HMAC-MD5 algorithm and SHA indicates the port authentication is performed via SHA (Secure Hash Algorithm). SHA authentication mode has a higher security than MD5 mode. By default, the Authentication Mode is “none”.

confirm-pwd—— Authentication Password, ranging from 1 to 16 characters. The question marks and spaces are not allowed. This password in the configuration file will be displayed in the symmetric encrypted form.

emode —— The Privacy Mode of the SNMP v3 User, with none 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:

T1700X-16TS(config)# snmp-server user admin local group2 **smode** v3 **slev** authPriv **cmode** MD5 **cpwd** 11111 **emode** DES **epwd** 22222

49.5 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:

T1700X-16TS(config)# snmp-server community public read-write viewDefault

49.6 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:

T1700X-16TS(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:

T1700X-16TS(config)# snmp-server host fe80::1234 162 admin **smode** v2c **type** inform **retries** 100 **timeout** 1000

49.7 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:

```
T1700X-16TS(config)# snmp-server engineID local 1234567890 remote
abcdef123456
```

49.8 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. The command without parameter enables all SNMP standard traps. All SNMP

standard traps are enabled by default. To disable the sending of SNMP standard traps, please use **no snmp-server traps snmp** command.

Syntax

snmp-server traps snmp [linkup | linkdown | warmstart | coldstart | auth-failure]

no snmp-server traps snmp [linkup | linkdown | warmstart | coldstart | auth-failure]

Parameter

linkup —— Indicates a port status changes from linkdown to linkup, and can be triggered when you connect a device to a port.

linkdown —— Indicates a port status changes from linkup to linkdown, and can be triggered when you disconnect a device to a port.

warmstart —— Indicates the SNMP feature on the switch is reinitialized with the physical configuration unchanged. The trap can be triggered if you disable and then enable SNMP after the SNMP is completely configured and enabled.

coldstart —— Indicates an SNMP initialization caused by the reinitialization of the switch system. The trap can be triggered when you reboot the switch.

auth-failure —— Triggered when a received SNMP request fails the authentication.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable SNMP standard linkup trap for the switch:

```
T1700X-16TS(config)# snmp-server traps snmp linkup
```

49.9 snmp-server traps

Description

The **snmp-server traps** command is used to enable SNMP extended traps. To disable the sending of SNMP extended traps, please use **no snmp-server traps** command. All SNMP extended traps are disabled by default.

Syntax

snmp-server traps { rate-limit | cpu | flash | lldp remtableschange | lldp topologychange | loopback-detection | storm-control | spanning-tree | memory }

no snmp-server traps { bandwidth-control | cpu | flash | lldp remtableschange | lldp topologychange | loopback-detection | storm-control | spanning-tree | memory }

Parameter

rate-limit ——Monitors whether the bandwidth has reached the limit you have set. The trap can be triggered when the Rate Limit feature is enabled and packets are sent to the port with a rate higher than what you have set.

cpu ——Monitors the load status of the switch CPU. The trap can be triggered when the utilization rate of the CPU has exceeded the limit that you have set. The limit of CPU utilization rate for the switch is 80% by default.

flash ——Triggered when flash is modified during operations such as backup, reset, firmware upgrade, configuration import, and so on.

lldp remtableschange ——An lldp RemTablesChange notification is sent when the value of lldp StatsRemTableLastChangeTime changes. It can be utilized by an NMS host to trigger LLDP remote systems table maintenance polls.

lldp topologychange ——A notification generated by the local device to sense the change in the topology that indicates a new remote device attached to a local port, or a remote device disconnected or moved from one port to another.

loopback-detection ——The feature is used to detect loopbacks. And the trap is disabled by default. The system will generate the trap when a loopback is detected or cleared.

storm-control ——The feature is used to monitor network storms. And the trap is disabled by default. The system will generate the trap when the rate of broadcast or multicast reaches the limit of storm control.

spanning-tree ——The feature is used to monitor the spanning tree status. And the trap is disabled by default. The system will generate the trap in the following situations: a port changes from non-forwarding state to forwarding state or the other way round; a port receives a packet with TC flag or a TCN packet.

memory ——The feature is used to monitor the memory. And the trap is disabled by default. The system will generate the trap when the memory utilization exceeds 80%.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable SNMP extended bandwidth-control trap for the switch:

T1700X-16TS(config)# snmp-server traps bandwidth-control

49.10 snmp-server traps ddm

Note: Only T1700X-16TS supports DDM traps.

Description

The **snmp-server traps ddm** command is used to enable the corresponding DDM traps. DDM function is used to monitor the status of the SFP modules inserted into the SFP ports on the switch. The command without parameter enables all SNMP DDM traps. To disable the sending of SNMP DDM traps, use **no snmp-server traps ddm** command. All DDM traps are disabled by default.

Syntax

snmp-server traps ddm [temperature | voltage | bias_current | tx_power | rx_power]

no snmp-server traps ddm [temperature | voltage | bias_current | tx_power | rx_power]

Parameter

temperature ——Monitors the temperature of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the temperature of any SFP module has reached the warning or alarm threshold.

voltage ——Monitors the voltage of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the voltage of any SFP module has reached the warning or alarm threshold.

bias_current ——Monitors the bias current of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the bias current of any SFP module has reached the warning or alarm threshold.

tx_power ——Monitors the TX Power of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the TX Power of any SFP module has reached the warning or alarm threshold.

rx_power ——Monitors the RX Power of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the RX Power of any SFP module has reached the warning or alarm threshold.

User guidelines

The **snmp-server traps ddm** command without any parameter is used to enable all the types of DDM traps. And the **no snmp-server traps ddm** command without any parameter is used to disable all the types of DDM traps.

For more instructions about the alarm threshold or warning threshold, refer to Chapter 11 DDM Commands.

Command Mode

Global Configuration Mode

Example

Enable all the SNMP DDM traps for the switch:

```
T1700X-16TS(config)# snmp-server traps ddm
```

49.11 snmp-server traps vlan

Description

The **snmp-server traps vlan** command is used to enable the corresponding VLAN traps. The command without parameter enables all SNMP VLAN traps. To disable this function, please use **no snmp-server traps vlan** command. All VLAN traps are disabled by default.

Syntax

snmp-server traps vlan [create | delete]

no snmp-server traps vlan [create | delete]

Parameter

create ——Triggered when certain VLANs are created successfully.

delete ——Triggered when certain VLANs are deleted successfully.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable all SNMP extended VLAN-related traps for the switch:

T1700X-16TS(config)# snmp-server traps vlan

Enable VLAN-created trap only for the switch:

T1700X-16TS(config)# snmp-server traps vlan create

49.12 snmp-server traps security

Description

The **snmp-server traps security** command is used to enable the corresponding security traps. To disable this feature, please use **no snmp-server traps security** command. All security traps are disabled by default.

Syntax

snmp-server traps security { dhcp-filter | ip-mac-binding | acl **}**

no snmp-server traps security { dhcp-filter | ip-mac-binding **}**

Parameter

dhcp-filter —— Triggered when the DHCPv4 Filter feature is enabled and the switch receives DHCP packets from an illegal DHCP server.

ip-mac-binding —— Triggered when the ARP Inspection feature is enabled and the switch receives an illegal ARP packet, or the IPv4 Source Guard feature is enabled and the switch receives an illegal IP packet.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the DHCP filter trap for the switch:

T1700X-16TS(config)# snmp-server traps security dhcp-filter

49.13 snmp-server traps acl

Description

The **snmp-server traps acl** command is used to enable the ACL trap. To disable this feature, please use **no snmp-server traps acl** command. It is disabled by default.

The trap monitors matched ACL information, including the matched ACL ID, rule ID and the number of the matched packets. With both this trap and the Logging feature in ACL rule settings enabled, the switch will check the matched ACL information every five minutes and send SNMP traps if there is any updated information.

Syntax

snmp-server traps acl

no snmp-server traps acl

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the ACL trap for the switch：

```
T1700X-16TS(config)# snmp-server traps acl
```

49.14 snmp-server traps ip

Description

The **snmp-server traps ip** command is used to enable IP traps. To disable this feature, please use **no snmp-server traps ip** command. All IP traps are disabled by default.

Syntax

snmp-server traps ip { change | duplicate **}**

no snmp-server traps ip { change | duplicate **}**

Parameter

change —— Enable SNMP IP change traps. The trap monitors the IP changed of each interface. The trap can be triggered when the IP address of any interface is changed.

duplicate —— Enable SNMP IP duplicate traps. The trap can be triggered when the switch detects an IP conflict event.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the IP-Change trap for the switch：

T1700X-16TS(config)# snmp-server traps ip change

49.15 snmp-server traps link-status

Description

The **snmp-server traps link-status** command is used to enable SNMP link status trap for the specified port. To disable the sending of SNMP link status trap, please use **no snmp-server traps link-status** command. By default, it is disabled.

Syntax

snmp-server traps link-status

no snmp-server traps link-status

Command Mode

Interface Configuration Mode (interface ten-gigabitEthernet / interface range ten-gigabitEthernet)

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable SNMP link status trap for port 3:

T1700X-16TS(config)# interface ten-gigabitEthernet 1/0/3

T1700X-16TS(config-if)# snmp-server traps link-status

49.16 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 ten-gigabitEthernet** *port* [**interval** *interval*] [**owner** *owner-name*] [**buckets** *number*]

no rmon history *index*

Parameter

index —— The index number of the entry, ranging from 1 to 12, in the format of 1-3,5.

port ——The Ethernet port number.

interval —— The interval to take samplings from the port, ranging from 10 to 3600 in seconds. By default, it is 1800.

owner-name —— The owner of the history sample entry, ranging from 1 to 16 characters. By default, it is "monitor".

number —— The maximum number of buckets desired for the RMON history group of statistics, ranging from 1 to 130. The default is 50 buckets.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the sample port as Te1/0/2 and the sample interval as 100 seconds for the entry 1-3:

```
T1700X-16TS(config)# rmon history 1-3 interface ten-gigabitEthernet
1/0/2 interval 100 owner owner1
```

49.17 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:

```
T1700X-16TS(config)# rmon event 1-4 user user1 description description1
type log owner owner1
```

49.18 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:

```
T1700X-16TS(config)#rmon alarm 1-3 stats-index 2 owner owner1 interval
100
```

49.19 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 ten-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:

T1700X-16TS(config)#rmon statistics 1-3 **interface ten-gigabitEthernet** 1/0/1 **owner** owner1 **status** valid

49.20 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:

T1700X-16TS# show snmp-server

49.21 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:

```
T1700X-16TS# show snmp-server view
```

49.22 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:

```
T1700X-16TS# show snmp-server group
```

49.23 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:

```
T1700X-16TS# show snmp-server user
```

49.24 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:

```
T1700X-16TS# show snmp-server community
```

49.25 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:

```
T1700X-16TS# show snmp-server host
```

49.26 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:

```
T1700X-16TS# show snmp-server engineID
```

49.27 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:

```
T1700X-16TS# show rmon history
```

49.28 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:

```
T1700X-16TS# show rmon event 1-4
```

49.29 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:

```
T1700X-16TS# show rmon alarm 1-2
```

49.30 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:

```
T1700X-16TS#show rmon statistics 1
```

Chapter 50 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.

50.1 ip arp inspection

Description

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

Syntax

ip arp inspection

no ip arp inspection

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the ARP Detection function globally:

```
T1700X-16TS(config)#ip arp inspection
```

50.2 ip arp inspection validate

Description

The **ip arp inspection validate** command is used to enable the switch to check whether the reveided ARP packet is illegal. To disable,the feature please use **no ip arp detection validate** command.

Syntax

ip arp inspection validate { src-mac | dst-mac | ip **}**

no ip arp inspection validate { src-mac | dst-mac | ip **}**

Syntax

src-mac —— Enable the switch to check whether the source MAC address and the sender MAC address are the same when receiving an ARP packet. If not, the ARP packet will be discarded.

dst-mac —— Enable the switch to check whether the sender IP address of all ARP packets and the target IP address of ARP reply packets are legal. The illegal packets will be discarded.

ip —— Enable or disable the switch to check whether the sender IP address of all ARP packets and the target IP address of ARP reply packets are legal. The illegal packets will be discarded.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the switch to check whether the source MAC address and the sender MAC address are the same when receiving an ARP packet

```
T1700X-16TS(config)#ip arp inspection validate src-mac
```

50.3 ip arp inspection vlan

Description

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

Syntax

ip arp inspection vlan *vlan-list*

no ip arp inspection vlan *vlan-list*

Syntax

vlan-list —— Enter the VLAN ID. The format is 1,5-9.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the ARP Detection function on VLAN 2:

T1700X-16TS(config)#ip arp inspection vlan 2

50.4 ip arp inspection vlan logging

Description

The **ip arp inspection vlan logging** command is used to enable the Log function on the specific VLAN. To disable the Log function on the VLAN, please use **no ip arp detection vlan logging** command.

Syntax

ip arp inspection vlan *vlan-list* **logging**

no ip arp inspection vlan *vlan-list* **logging**

Syntax

vlan-list —— Enter the VLAN ID. The format is 1,5-9.

logging —— Enable the Log feature to make the switch generate a log when an ARP packet is discarded.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the log feature on VLAN 2:

T1700X-16TS(config)#ip arp inspection vlan 2 **logging**

50.5 ip arp inspection trust

Description

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

Syntax

ip arp inspection trust

no ip arp inspection trust

Command Mode

Interface Configuration Mode (interface ten-gigabitEthernet / interface range ten-gigabitEthernet)

Privilege Requirement

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

Example

Configure the Ports 1/0/2-5 as the Trusted Port:

T1700X-16TS(config)#interface range ten-gigabitEthernet 1/0/2-5

T1700X-16TS(config-if-range)#ip arp inspection trust

50.6 ip arp inspection limit-rate

Description

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

Syntax

ip arp inspection limit-rate *value*

no ip arp inspection limit-rate

Parameter

value ——The value to specify the maximum amount of the received ARP packets per second, ranging from 1 to 300 in pps(packet/second). By default, the value is 100.

Command Mode

Interface Configuration Mode (interface ten-gigabitEthernet / interface range ten-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 Port 5:

T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/5

T1700X-16TS(config-if)#ip arp inspection limit-rate 50

50.7 ip arp inspection burst-interval

Description

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

Syntax

ip arp inspection burst-interval *value*

no ip arp inspection burst-interval

Parameter

value —— Specify a time range. If the speed of received ARP packets in this time range reaches the limit for this time range, the port will be shut down. The valid values are from 1 to 15 seconds, and the default value is 1 second.

Command Mode

Interface Configuration Mode (interface ten-gigabitEthernet / interface range ten-gigabitEthernet)

Privilege Requirement

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

Example

Configure the burst interval as 2 seconds for Port 5:

```
T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/5
T1700X-16TS(config-if)#ip arp inspection burst-interval 2
```

50.8 ip arp inspection recover

Description

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

Syntax

ip arp inspection recover

Command Mode

Interface Configuration Mode (interface ten-gigabitEthernet / interface range ten-gigabitEthernet)

Privilege Requirement

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

Example

Restore Port 1/0/5 to the ARP transmit status:

```
T1700X-16TS(config)#interface ten-gigabitEthernet 1/0/5
T1700X-16TS(config-if)#ip arp inspection recover
```

50.9 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:

```
T1700X-16TS(config)#show ip arp inspection
```

50.10 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 Port 1/0/1:

```
T1700X-16TS(config)#show ip arp inspection interface ten-gigabitEthernet 1/0/1
```

Display the configuration of all Ethernet ports:

```
T1700X-16TS(config)#show ip arp inspection interface
```

50.11 show ip arp inspection vlan

Description

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

Syntax

show ip arp inspection vlan

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the ARP Inspection configuration of VLAN:

```
T1700X-16TS(config)#show ip arp inspection vlan
```

50.12 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:

```
T1700X-16TS(config)#show ip arp inspection statistics
```

50.13 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:

```
T1700X-16TS(config)#clear ip arp inspection statistics
```

Chapter 51 ND Detection Commands

The ND Detection feature allows the switch to detect the ND packets based on the binding entries in the IPv6-MAC Binding Table and filter out the illegal ND packets. Before configuring ND Detection, complete IPv6-MAC Binding configuration. For details, refer to IPv6-MAC Binding Configurations.

51.1 ipv6 nd detection

Description

The **ipv6 nd detection** command is used to enable the ND Detection function globally. To disable the ND Detection function, please use **no ipv6 nd detection** command.

Syntax

ipv6 nd detection

no ipv6 nd detection

Command Mode

Global Configuration Mode

Example

Enable the ND Detection function globally:

```
T1700X-16TS(config)#ipv6 nd detection
```

51.2 ipv6 nd detection vlan

Description

The **ipv6 nd detection vlan** command is used to enable ND Detection function on a specified VLAN. To disable ND Detection function on this VLAN, please use **no ipv6 nd detection vlan** command.

Syntax

ipv6 nd detection vlan *vlan-range*

no ipv6 nd detection vlan *vlan-range*

Parameter

vlan-range ——Enter the vlan range in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Example

Enable the ND Detection function on VLAN 1,4,6-7:

T1700X-16TS(config)#ipv6 nd detection vlan 1,4,6-7

51.3 ipv6 nd detection vlan logging

Description

The **ipv6 nd detection vlan logging** command is used to enable Log function on a specified VLAN. To disable Log function on this VLAN, please use **no ipv6 nd detection vlan logging** command.

Syntax

ipv6 nd detection vlan *vlan-range* **logging**

no ipv6 nd detection vlan *vlan-range* **logging**

Parameter

vlan-range ——Enter the vlan range in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Example

Enable the Log function on VLAN 1,4,6-7:

T1700X-16TS(config)#ipv6 nd detection vlan 1,4,6-7 **logging**

51.4 ipv6 nd detection trust

Description

The **ipv6 nd detection trust** command is used to configure the port for which the ND Detection function is unnecessary as the Trusted Port. To clear the Trusted Port list, please use **no ipv6 nd detection trust** command .The specific port, such as up-linked port, routing port and LAG port, should be set

as Trusted Port. To ensure the normal communication of the switch, please configure the ND Detection Trusted Port before enabling the ND Detection function.

Syntax

Ipv6 nd detection trust

no ipv6 nd detection trust

Command Mode

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

Example

Configure the Ports 1/0/2-5 as the Trusted Port:

```
T1700X-16TS(config)#interface range ten-gigabitEthernet 1/0/2-5
T1700X-16TS(config-if-range)#ipv6 nd detection trust
```

51.5 show ipv6 nd detection

Description

The **show ipv6 nd detection** command is used to display the ND detection global configuration including the enable/disable status.

Syntax

show ipv6 nd detection

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the ND Detection configuration globally:

```
T1700X-16TS(config)#show ipv6 nd detection
```

51.6 show ipv6 nd detection interface

Description

The **show ipv6 nd detection interface** command is used to display the interface configuration of ND Detection.

Syntax

show ipv6 nd detection interface[**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parameter

port——The Ethernet port number.

port-channel-id—— The ID of the port channel.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the configuration of Port 1/0/1:

T1700X-16TS(config)#show ipv6 nd detection interface ten-gigabitEthernet 1/0/1

Display the configuration of all Ethernet ports:

T1700X-16TS(config)#show ipv6 nd detection interface

51.7 show ipv6 nd detection vlan

Description

The **show ipv6 nd detection vlan** command is used to display the VLAN configuration of ND Detection.

Syntax

show ipv6 nd detection vlan

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the ipv6 ND Detection configuration of VLAN.

T1700X-16TS(config)#show ipv6 nd detection vlan

Chapter 52 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.

52.1 logging buffer

Description

The **logging buffer** command is used to store the system log messages to an internal buffer. To disable the log buffer function, please use the **no logging buffer** command. Local Log is the system log information saved in the switch. It has two output channels, that is, it can be saved to two different positions, log buffer and log flash memory. The log buffer indicates the RAM for saving system log and the information in the log buffer can be got by **show logging buffer** command. It will be lost when the switch is restarted.

Syntax

logging buffer

no logging buffer

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the system log buffer:

```
T1700X-16TS(config)#logging buffer
```

52.2 logging buffer level

Description

The **logging buffer level** command is used to configure the severity level and the status of the configuration input to the log buffer. To return to the default configuration, please use **no logging buffer level** command.

Syntax

logging buffer level *level*

no logging buffer level

Parameter

level —— Severity level of the log information output to each channel. There are 8 severity levels marked with values 0-7. The smaller value has the higher priority. Only the log with the same or smaller severity level value will be output. By default, it is 6 indicating that the log information with level 0-6 will be saved in the log buffer.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Set the severity level as 5:

T1700X-16TS(config)#logging buffer level 5

52.3 logging file flash

Description

The **logging file flash** command is used to store the log messages in a file in the flash on the switch. To disable the log file flash function, please use **no logging file flash** command. This function is disabled by default. The log file flash indicates the flash sector for saving system log. The information in the log file of the flash will not be lost after the switch is restarted and can be got by the **show logging flash** command.

Syntax

logging file flash

no logging file flash

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the log file flash function:

```
T1700X-16TS(config)#logging file flash
```

52.4 logging file flash frequency

Description

The **logging file flash frequency** command is used to specify the frequency to synchronize the system log file in the log buffer to the flash. To resume the default synchronizing frequency, please use the **no logging file flash frequency** command.

Syntax

logging file flash frequency { **periodic** *periodic* | **immediate** }

no logging file flash frequency

Parameter

periodic —— The frequency to synchronize the system log file in the log buffer to the flash, ranging from 1 to 48 hours. By default, the synchronization process takes place every 24 hours.

immediate —— The system log file in the buffer will be synchronized to the flash immediately. This option will reduce the life of the flash and is not recommended.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the log file synchronization frequency as 10 hours:

```
T1700X-16TS(config)#logging file flash frequency periodic10
```

52.5 logging file flash level

Description

The **logging file flash level** command is used to specify the system log message severity level. Messages will a severity level equal to or higher than this value will be stored to the flash. To restore to the default level, please use **no logging file flash level** command.

Syntax

logging file flash level *level*

no logging file flash level

Parameter

level —— Severity level of the log message. There are 8 severity levels marked with values 0-7. The smaller value has the higher priority. Only the log with the same or smaller severity level value will be saved to the flash. By default, it is 3 indicating that the log message marked with 0~3 will be saved in the log flash.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin 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 :

```
T1700X-16TS(config)#logging file flash level 7
```

52.6 logging host index

Description

The **logging host index** command is used to configure the Log Host. To clear the configuration of the specified Log Host, please use **no logging host index** command. Log Host is to receive the system log from other devices. You can remotely monitor the settings and operation status of other devices through the log host.

Syntax

logging host index *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:

T1700X-16TS(config)# logging host index 2 192.168.0.148 5

52.7 logging console

Description

The **logging console** command is used to send the system logs to the console port. To disable logging to the console, please use **no logging console** command. This function is enabled by default.

Syntax

logging console

no logging console

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable logging to the console port:

```
T1700X-16TS(config)# logging console
```

52.8 logging console level

Description

The **logging console level** command is used to limit messages logged to the console port. System logs no higher than the set threshold level will be displayed on the console port. To restore the threshold level to default value, please use **no logging console level** command.

Syntax

logging console level *level*

no logging monitor level

Parameter

level —— Severity level of the log information output to the console port. There are 8 severity levels marked with values 0-7. The smaller value has the higher priority. Only the log with the same or smaller severity level value will be output to the terminal devices. By default, it is 5 indicating that all the log information between level 0-5 will be output to the terminal devices.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Output the log information with severity levels between 0-7 to the console port:

```
T1700X-16TS(config)# logging console level 7
```

52.9 logging monitor

Description

The **logging monitor** command is used to display the system logs on the terminal devices. To disable logging to the terminal, please use **no logging monitor** command. This function is enabled by default.

Syntax

logging monitor

no logging monitor

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Disable logging to the terminal devices:

```
T1700X-16TS(config)# no logging monitor
```

52.10 logging monitor level

Description

The **logging monitor level** command is used to limit messages logged to the terminal devices. System logs no higher than the set threshold level will be displayed on the terminal devices. To restore the threshold level to default value, please use **no logging monitor level** command.

Syntax

logging monitor level *level*

no logging monitor level

Parameter

level—— Severity level of the log information output to the terminal devices. There are 8 severity levels marked with values 0-7. The smaller value has the higher priority. Only the log with the same or smaller severity level value will

be output to the terminal devices. By default, it is 5 indicating that all the log information between level 0-5 will be output to the terminal devices.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Output the log information with severity levels between 0-7 to the terminal devices:

```
T1700X-16TS(config)# logging monitor level 7
```

52.11 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:

```
T1700X-16TS(config)# clear logging buffer
```

52.12 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:

```
T1700X-16TS(config)# show logging local-config
```

52.13 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:

```
T1700X-16TS(config)# show logging loghost 2
```

52.14 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:

```
T1700X-16TS(config)# show logging buffer level 5
```

52.15 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:

T1700X-16TS(config)# show logging flash level 3