




CLI Reference Guide

T1500-28TC (TL-SL2428)/T1500-28PCT (TL-SL2428P)

1910012116 REV 2.0.0

March 2017

COPYRIGHT & TRADEMARKS

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

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

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

CONTENTS

Preface	1
Chapter 1 Using the CLI	4
1.1 Accessing the CLI	4
1.1.1 Logon by Telnet	4
1.1.2 Logon by SSH	5
1.2 CLI Command Modes	10
1.3 Privilege Restrictions	13
1.4 Conventions	13
1.4.1 Format Conventions	13
1.4.2 Special Characters	13
1.4.3 Parameter Format	14
Chapter 2 User Interface	15
2.1 enable	15
2.2 enable-admin	15
2.3 service password-encryption	16
2.4 enable password	17
2.5 enable secret	18
2.6 configure	19
2.7 exit	19
2.8 end	20
2.9 history	20
2.10 history clear	21
Chapter 3 IEEE 802.1Q VLAN Commands	22
3.1 vlan	22
3.2 interface vlan	23
3.3 name	23
3.4 switchport general allowed vlan	24
3.5 switchport pvid	25
3.6 show vlan summary	25
3.7 show vlan brief	26
3.8 show vlan	26
3.9 show interface switchport	27
Chapter 4 Voice VLAN Commands	28
4.1 voice vlan	28

4.2	voice vlan aging	28
4.3	voice vlan priority	29
4.4	voice vlan mac-address	30
4.5	switchport voice vlan mode	31
4.6	switchport voice vlan security	31
4.7	show voice vlan	32
4.8	show voice vlan oui	33
4.9	show voice vlan switchport	33
Chapter 5	Etherchannel Commands.....	35
5.1	channel-group	35
5.2	port-channel load-balance	36
5.3	lacp system-priority	37
5.4	lacp port-priority	38
5.5	show etherchannel	38
5.6	show etherchannel load-balance	39
5.7	show lacp	40
5.8	show lacp sys-id	40
Chapter 6	User Management Commands	42
6.1	user name (password)	42
6.2	user name (secret)	43
6.3	user access-control ip-based	44
6.4	user access-control mac-based	45
6.5	user access-control port-based	46
6.6	telnet	47
6.7	show user account-list	47
6.8	show user configuration	48
6.9	show telnet-status	48
Chapter 7	HTTP and HTTPS Commands	50
7.1	ip http server	50
7.2	ip http max-users	51
7.3	ip http session timeout	52
7.4	ip http secure-server	52
7.5	ip http secure-protocol	53
7.6	ip http secure-ciphersuite	54
7.7	ip http secure-max-users	54
7.8	ip http secure-session timeout	55
7.9	ip http secure-server download certificate	56

7.10	ip http secure-server download key	57
7.11	show ip http configuration.....	58
7.12	show ip http secure-server	58
Chapter 8	Binding Table Commands	60
8.1	ip source binding	60
8.2	ip dhcp snooping	61
8.3	ip dhcp snooping vlan.....	62
8.4	ip dhcp snooping information option	63
8.5	ip dhcp snooping information strategy	63
8.6	ip dhcp snooping information remote-id.....	64
8.7	ip dhcp snooping information circuit-id.....	65
8.8	ip dhcp snooping trust	66
8.9	ip dhcp snooping mac-verify.....	67
8.10	ip dhcp snooping limit rate.....	67
8.11	ip dhcp snooping decline rate.....	68
8.12	show ip source binding.....	69
8.13	show ip dhcp snooping.....	70
8.14	show ip dhcp snooping interface.....	70
8.15	show ip dhcp snooping information interface.....	71
Chapter 9	ARP Inspection Commands	72
9.1	ip arp inspection(global)	72
9.2	ip arp inspection trust	72
9.3	ip arp inspection(interface)	73
9.4	ip arp inspection limit-rate	74
9.5	ip arp inspection recover	75
9.6	show ip arp inspection.....	75
9.7	show ip arp inspection interface.....	76
9.8	show ip arp inspection statistics.....	77
9.9	clear ip arp inspection statistics.....	77
Chapter 10	DoS Defend Commands.....	78
10.1	ip dos-prevent.....	78
10.2	ip dos-prevent type.....	78
10.3	show ip dos-prevent	80
Chapter 11	System Log Commands	81
11.1	logging buffer	81
11.2	logging buffer level	81

11.3	logging file flash	82
11.4	logging file flash frequency	83
11.5	logging file flash level	84
11.6	logging host index.....	84
11.7	logging monitor	85
11.8	logging monitor level.....	86
11.9	clear logging	87
11.10	show logging local-config	87
11.11	show logging loghost.....	88
11.12	show logging buffer	88
11.13	show logging flash.....	89
Chapter 12 SSH Commands		90
12.1	ip ssh server	90
12.2	ip ssh version.....	90
12.3	ip ssh algorithm	91
12.4	ip ssh timeout.....	92
12.5	ip ssh max-client.....	92
12.6	ip ssh download.....	93
12.7	remove public-key	94
12.8	show ip ssh.....	94
Chapter 13 IEEE 802.1X Commands		95
13.1	dot1x system-auth-control.....	95
13.2	dot1x handshake	96
13.3	dot1x auth-method.....	96
13.4	dot1x accounting	97
13.5	dot1x guest-vlan(global).....	98
13.6	dot1x quiet-period.....	99
13.7	dot1x timeout.....	99
13.8	dot1x max-reauth-req	100
13.9	dot1x	101
13.10	dot1x guest-vlan(interface).....	102
13.11	dot1x port-control.....	102
13.12	dot1x port-method	103
13.13	show dot1x global.....	104
13.14	show dot1x interface.....	105
Chapter 14 MAC Address Commands		106
14.1	mac address-table static.....	106

14.2	mac address-table aging-time	107
14.3	mac address-table filtering	107
14.4	mac address-table notification.....	108
14.5	mac address-table notification (interface)	109
14.6	mac address-table max-mac-count	110
14.7	mac address-table security	112
14.8	show mac address-table.....	112
14.9	clear mac address-table	113
14.10	show mac address-table aging-time.....	114
14.11	show mac address-table max-mac-count	114
14.12	show mac address-table interface.....	115
14.13	show mac address-table count.....	115
14.14	show mac address-table address.....	116
14.15	show mac address-table vlan	117
14.16	show mac address-table notification	117
14.17	show mac address-table security	118
Chapter 15 System Configuration Commands		119
15.1	system-time manual	119
15.2	system-time ntp	119
15.3	system-time dst predefined	121
15.4	system-time dst date	122
15.5	system-time dst recurring	123
15.6	hostname	124
15.7	location	125
15.8	contact-info	125
15.9	ip address	126
15.10	ip management-vlan	127
15.11	ip address-alloc	127
15.12	reset.....	128
15.13	reboot.....	128
15.14	copy running-config startup-config	129
15.15	copy startup-config tftp	129
15.16	copy tftp startup-config	130
15.17	boot application	131
15.18	remove backup-image.....	132
15.19	firmware upgrade.....	132
15.20	ping	133
15.21	tracert.....	134

15.22	show system-info	135
15.23	show image-info	136
15.24	show running-config	136
15.25	show startup-config	137
15.26	show system-time	137
15.27	show system-time dst	138
15.28	show system-time ntp	138
15.29	show cable-diagnostics interface gigabitEthernet	139
15.30	show cpu-utilization	139
15.31	show memory-utilization	140
Chapter 16 Ethernet Configuration Commands		141
16.1	interface gigabitEthernet	141
16.2	interface range fastEthernet gigabitEthernet	141
16.3	description	142
16.4	shutdown	143
16.5	flow-control	143
16.6	duplex	144
16.7	jumbo-size	145
16.8	speed	145
16.9	storm-control	146
16.10	bandwidth	147
16.11	clear counters	148
16.12	show interface status	148
16.13	show interface counters	149
16.14	show interface configuration	149
16.15	show storm-control	150
16.16	show bandwidth	151
Chapter 17 QoS Commands		152
17.1	qos	152
17.2	qos cos	152
17.3	qos dscp	153
17.4	qos queue cos-map	154
17.5	qos queue dscp-map	155
17.6	qos queue mode	156
17.7	show qos interface	157
17.8	show qos cos-map	157
17.9	show qos dscp-map	158
17.10	show qos queue mode	158

17.11	show qos status	159
Chapter 18 Port Mirror Commands		160
18.1	monitor session destination interface	160
18.2	monitor session source interface.....	161
18.3	show monitor session	162
Chapter 19 Port Isolation Commands		163
19.1	port isolation	163
19.2	show port isolation interface.....	164
Chapter 20 Loopback Detection Commands.....		165
20.1	loopback-detection(global)	165
20.2	loopback-detection interval.....	165
20.3	loopback-detection recovery-time	166
20.4	loopback-detection(interface).....	167
20.5	loopback-detection config.....	167
20.6	loopback-detection recover	168
20.7	show loopback-detection global	169
20.8	show loopback-detection interface.....	169
Chapter 21 ACL Commands		171
21.1	access-list create	171
21.2	mac access-list	171
21.3	access-list standard	172
21.4	access-list extended	173
21.5	rule	174
21.6	access-list policy name.....	175
21.7	access-list policy action.....	176
21.8	access-list bind acl(interface)	176
21.9	access-list bind acl(vlan)	177
21.10	access-list bind(interface).....	177
21.11	access-list bind(vlan).....	178
21.12	show access-list	179
21.13	show access-list policy	179
21.14	show access-list bind.....	180
Chapter 22 PoE Commands.....		181
22.1	power inline consumption (global).....	181
22.2	power profile	182
22.3	power time-range.....	183

22.4	absolute	183
22.5	periodic	184
22.6	power holiday.....	186
22.7	holiday	186
22.8	power inline consumption (interface)	187
22.9	power inline priority.....	188
22.10	power inline supply	189
22.11	power inline profile.....	189
22.12	power inline time-range	190
22.13	show power inline	191
22.14	show power inline configuration interface	191
22.15	show power inline information interface	192
22.16	show power profile.....	192
22.17	show power holiday	193
22.18	show power time-range	193
Chapter 23 MSTP Commands		194
23.1	debug spanning-tree.....	194
23.2	spanning-tree(global).....	195
23.3	spanning-tree(interface)	195
23.4	spanning-tree common-config.....	196
23.5	spanning-tree mode.....	197
23.6	spanning-tree mst configuration	198
23.7	instance	199
23.8	name	199
23.9	revision	200
23.10	spanning-tree mst instance	201
23.11	spanning-tree mst.....	201
23.12	spanning-tree priority.....	202
23.13	spanning-tree timer.....	203
23.14	spanning-tree hold-count.....	204
23.15	spanning-tree max-hops.....	204
23.16	spanning-tree bpdudfilter.....	205
23.17	spanning-tree bpduguard	206
23.18	spanning-tree guard loop.....	206
23.19	spanning-tree guard root.....	207
23.20	spanning-tree guard tc.....	208
23.21	spanning-tree mcheck	208
23.22	show spanning-tree active.....	209

23.23	show spanning-tree bridge	209
23.24	show spanning-tree interface	210
23.25	show spanning-tree interface-security	211
23.26	show spanning-tree mst	211
Chapter 24 IGMP Snooping Commands		213
24.1	ip igmp snooping(global)	213
24.2	ip igmp snooping(interface)	213
24.3	ip igmp snooping rtime	214
24.4	ip igmp snooping mtime.....	215
24.5	ip igmp snooping report-suppression	215
24.6	ip igmp snooping immediate-leave.....	216
24.7	ip igmp snooping drop-unknown	216
24.8	ip igmp snooping last-listener query-inteval.....	217
24.9	ip igmp snooping last-listener query-count.....	218
24.10	ip igmp snooping vlan-config.....	218
24.11	ip igmp snooping vlan-config (router-ports-forbidden)	220
24.12	ip igmp snooping multi-vlan-config.....	221
24.13	ip igmp snooping multi-vlan-config (router-ports-forbidden)	222
24.14	ip igmp snooping multi-vlan-config (source-ip-replace)	223
24.15	ip igmp snooping querier vlan	223
24.16	ip igmp snooping querier vlan (general query).....	224
24.17	ip igmp snooping max-groups	225
24.18	ip igmp profile	226
24.19	deny	227
24.20	permit.....	227
24.21	range.....	228
24.22	ip igmp filter	229
24.23	clear ip igmp snooping statistics.....	229
24.24	show ip igmp snooping	230
24.25	show ip igmp snooping interface	230
24.26	show ip igmp snooping vlan	231
24.27	show ip igmp snooping multi-vlan	232
24.28	show ip igmp snooping groups vlan	232
24.29	show ip igmp snooping groups.....	233
24.30	show ip igmp snooping querier.....	234
24.31	show ip igmp profile.....	234
Chapter 25 SNMP Commands		236
25.1	snmp-server.....	236

25.2	snmp-server view	236
25.3	snmp-server group	237
25.4	snmp-server user.....	239
25.5	snmp-server community	240
25.6	snmp-server host.....	241
25.7	snmp-server engineID	243
25.8	snmp-server traps snmp.....	243
25.9	snmp-server traps link-status	244
25.10	snmp-server traps.....	245
25.11	snmp-server traps vlan	246
25.12	rmon history	247
25.13	rmon event.....	248
25.14	rmon alarm.....	249
25.15	rmon statistics.....	250
25.16	show snmp-server	251
25.17	show snmp-server view	252
25.18	show snmp-server group.....	252
25.19	show snmp-server user	253
25.20	show snmp-server community.....	253
25.21	show snmp-server host	253
25.22	show snmp-server engineID.....	254
25.23	show rmon history	254
25.24	show rmon event	255
25.25	show rmon alarm	256
25.26	show rmon statistics	256
Chapter 26 LLDP Commands		258
26.1	lldp	258
26.2	lldp hold-multiplier.....	258
26.3	lldp timer	259
26.4	lldp receive.....	260
26.5	lldp transmit	261
26.6	lldp snmp-trap	261
26.7	lldp tlv-select	262
26.8	lldp med-fast-count	263
26.9	lldp med-status	263
26.10	lldp med-tnv-select.....	264
26.11	lldp med-location.....	265
26.12	show lldp.....	266

26.13	show lldp interface	266
26.14	show lldp local-information interface	267
26.15	show lldp neighbor-information interface	267
26.16	show lldp traffic interface	268
Chapter 27 AAA Commands.....		269
27.1	aaa enable	269
27.2	enable admin password.....	270
27.3	enable admin secret	271
27.4	tacacs-server host	272
27.5	show tacacs-server.....	273
27.6	radius-server host.....	274
27.7	show radius-server	275
27.8	aaa group.....	276
27.9	server	276
27.10	show aaa group	277
27.11	aaa authentication login.....	278
27.12	aaa authentication enable	279
27.13	aaa authentication dot1x default	280
27.14	aaa accounting dot1x default	280
27.15	show aaa authentication.....	281
27.16	show aaa accounting.....	282
27.17	line telnet	282
27.18	login authentication(telnet)	283
27.19	line ssh.....	283
27.20	login authentication(ssh)	284
27.21	enable authentication(telnet).....	285
27.22	enable authentication(ssh)	285
27.23	ip http login authentication.....	286
27.24	ip http enable authentication	287
27.25	show aaa global.....	288

Preface

Some models featured in this guide may be unavailable in your country or region. For local sales information, visit <http://www.tp-link.com>

This Guide is intended for network administrator to provide referenced information about CLI (Command Line Interface). The device mentioned in this Guide stands for T1500-28TC (TL-SL2428)/T1500-28PCT (TL-SL2428P) JetStream Smart Switch without any explanation. The commands in this guide apply to these models if not specially noted, and T1500-28PCT is taken as an example model in the example commands.

Overview of this Guide

Chapter 1: Using the CLI

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

Chapter 2: User Interface

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

Chapter 3: IEEE 802.1Q VLAN Commands

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

Chapter 4: Voice VLAN Commands

Provide information about the commands used for configuring Voice VLAN.

Chapter 5: Etherchannel Commands

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

Chapter 6: User Management Commands

Provide information about the commands used for user management.

Chapter 7: HTTP and HTTPS Commands

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

Chapter 8: Binding Table Commands

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

Chapter 9: ARP Inspection Commands

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

Chapter 10: DoS Defend Command

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

Chapter 11: System Log Commands

Provide information about the commands used for configuring system log.

Chapter 12: SSH Commands

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

Chapter 13: IEEE 802.1X Commands

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

Chapter 14: MAC Address Commands

Provide information about the commands used for Address configuration.

Chapter 15: 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 16: Ethernet Configuration Commands

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

Chapter 17: QoS Commands

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

Chapter 18: Port Mirror Commands

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

Chapter 19: Port Isolation Commands

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

Chapter 20: Loopback Detection Commands

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

Chapter 21: ACL Commands

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

Chapter 22: PoE Commands

Provide information about the commands used for configuring PoE function.

Chapter 23: MSTP Commands

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

Chapter 24: IGMP Snooping Commands

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

Chapter 25: SNMP Commands

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

Chapter 26: LLDP Commands

Provide information about the commands used for configuring LLDP function.

Chapter 27: AAA Commands

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

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.

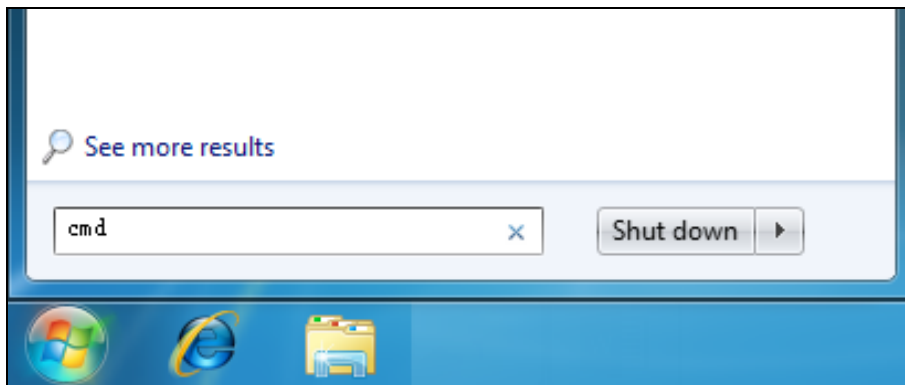


Figure 1-1 Run Window

2. Telnet the switch's IP address (factory setting is 192.168.0.1) in the prompt cmd window and press **Enter**.

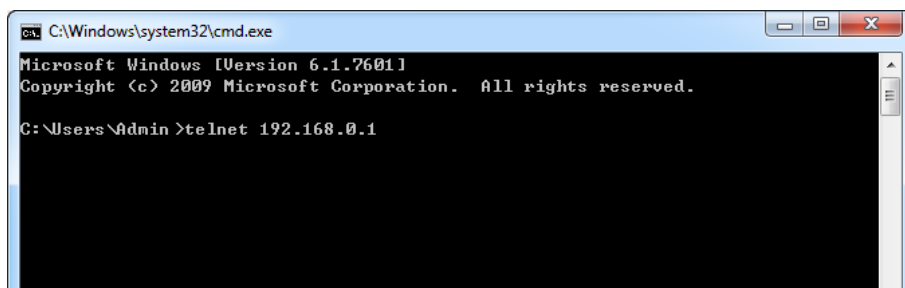
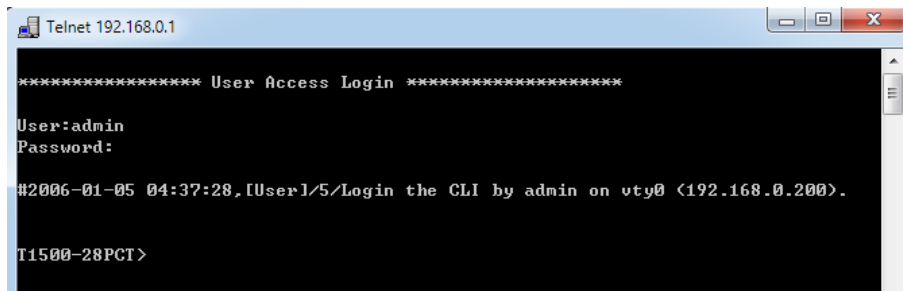


Figure 1-2 Type in the telnet command

3. Type in the User name and Password (the factory default value for both of them are admin) and press the **Enter** button to enter User EXEC Mode , which is shown as Figure 1-3.



```
Telnet 192.168.0.1

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

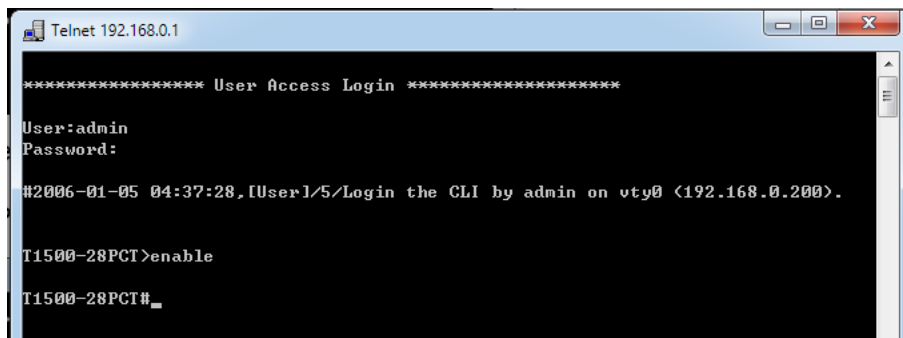
User:admin
Password:

#2006-01-05 04:37:28,[User1/5/Login the CLI by admin on vty0 <192.168.0.200>.

T1500-28PCT>
```

Figure 1-3 Log in the Switch

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



```
Telnet 192.168.0.1

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

User:admin
Password:

#2006-01-05 04:37:28,[User1/5/Login the CLI by admin on vty0 <192.168.0.200>.

T1500-28PCT>enable
T1500-28PCT#_
```


Figure 1-4 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 1-5 to enable the SSH function through Telnet connection.

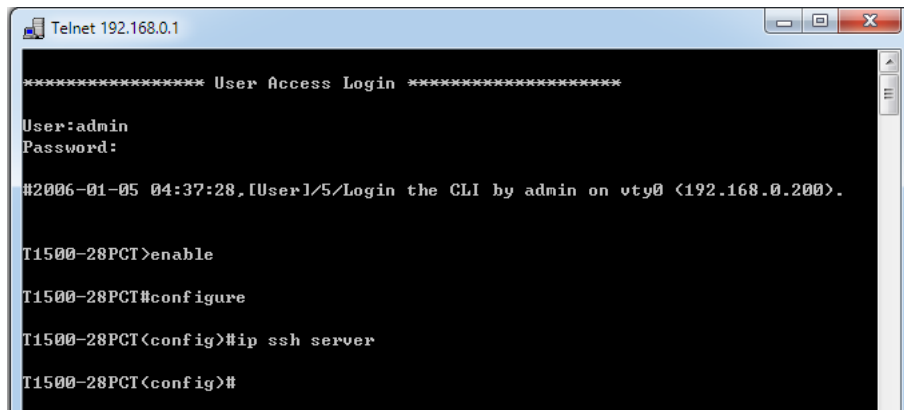


Figure 1-5 Enable SSH function

➤ **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.

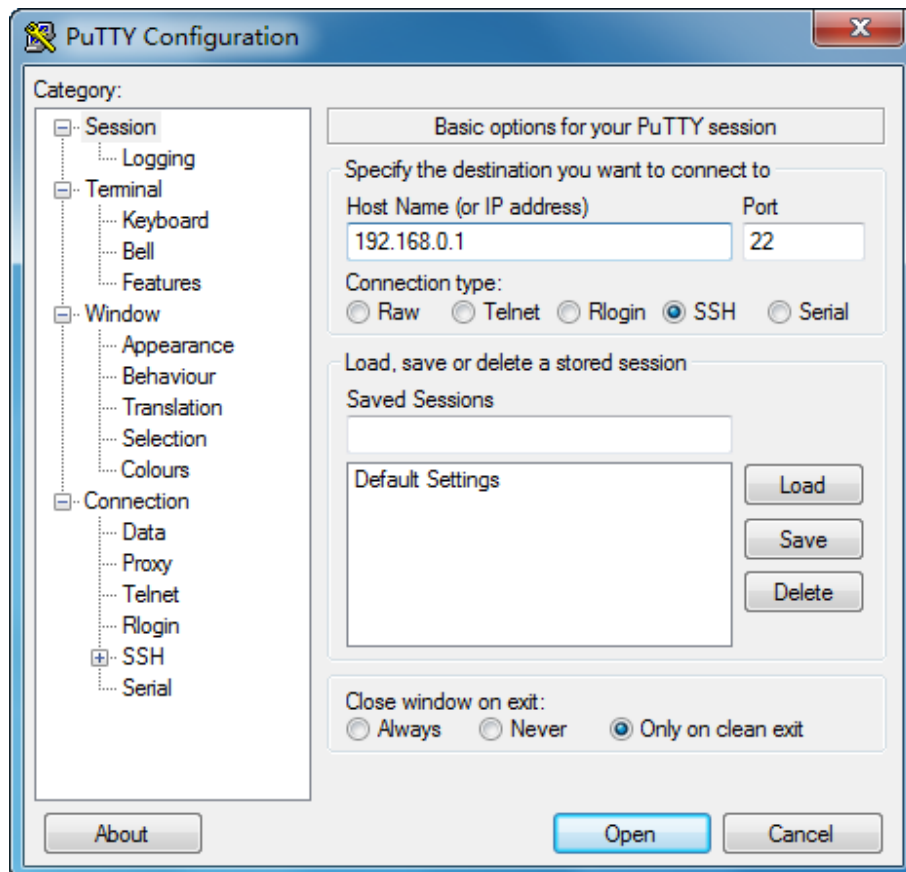


Figure 1-6 SSH Connection Config

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.

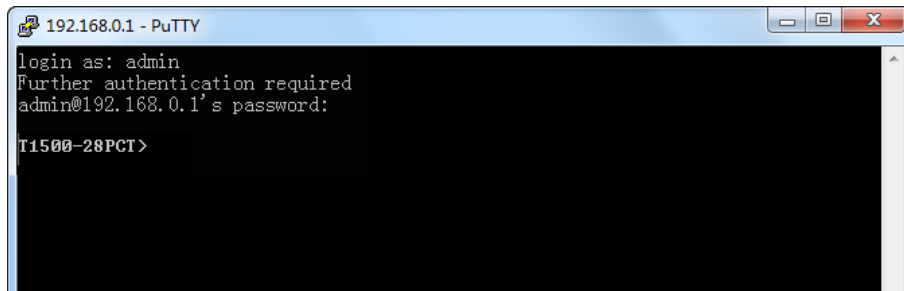


Figure 1-7 Log on the Switch

➤ Key Authentication Mode

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

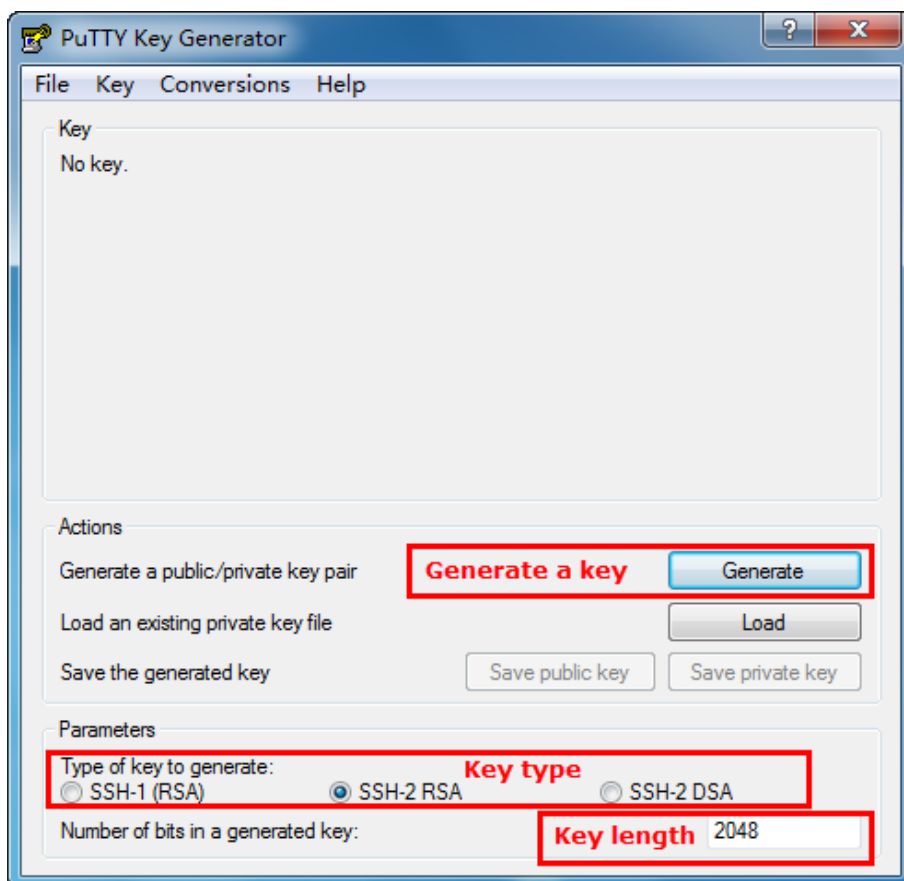


Figure 1-8 Generate SSH Key

⚠ 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.

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

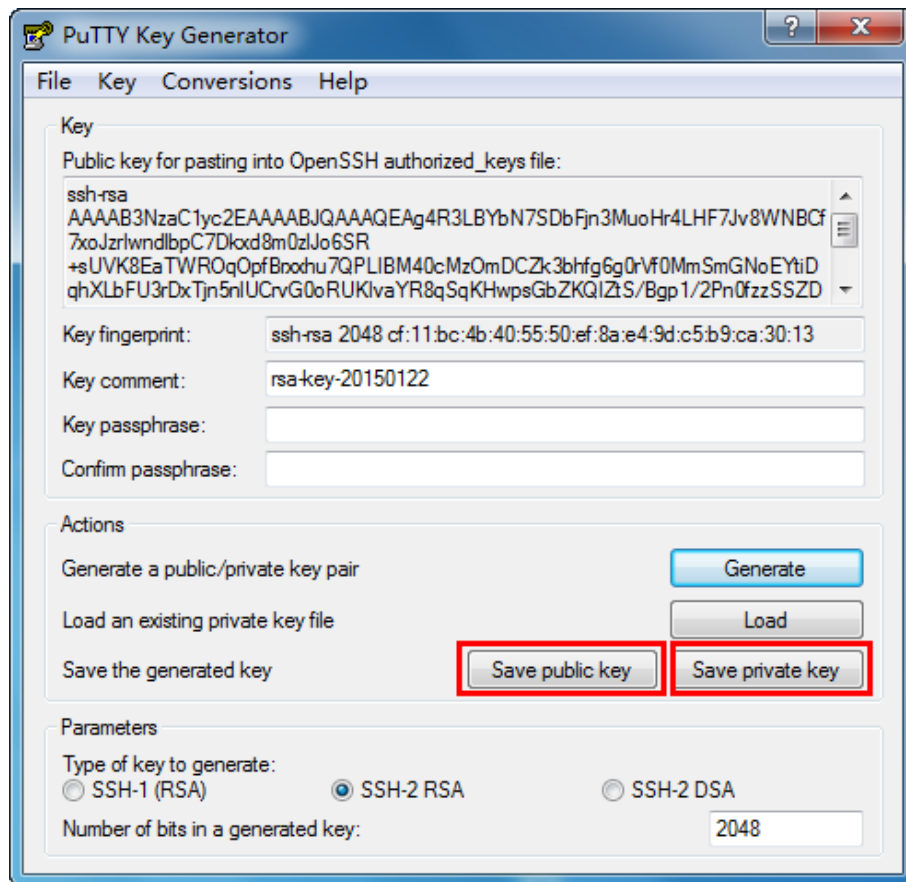


Figure 1-9 Save the Generated Key

- 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:

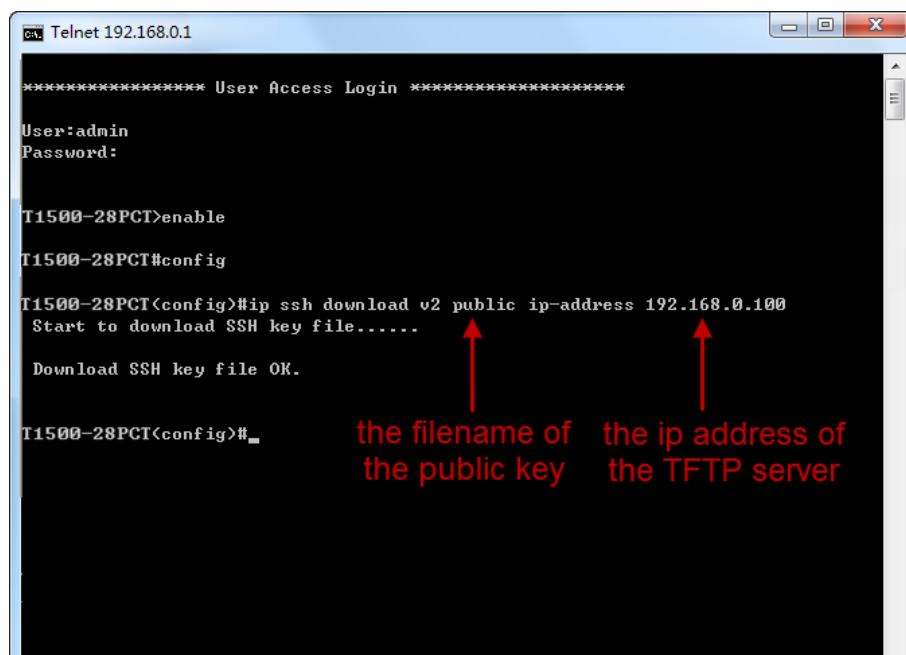


Figure 1-10 Download the Public Key

 **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.

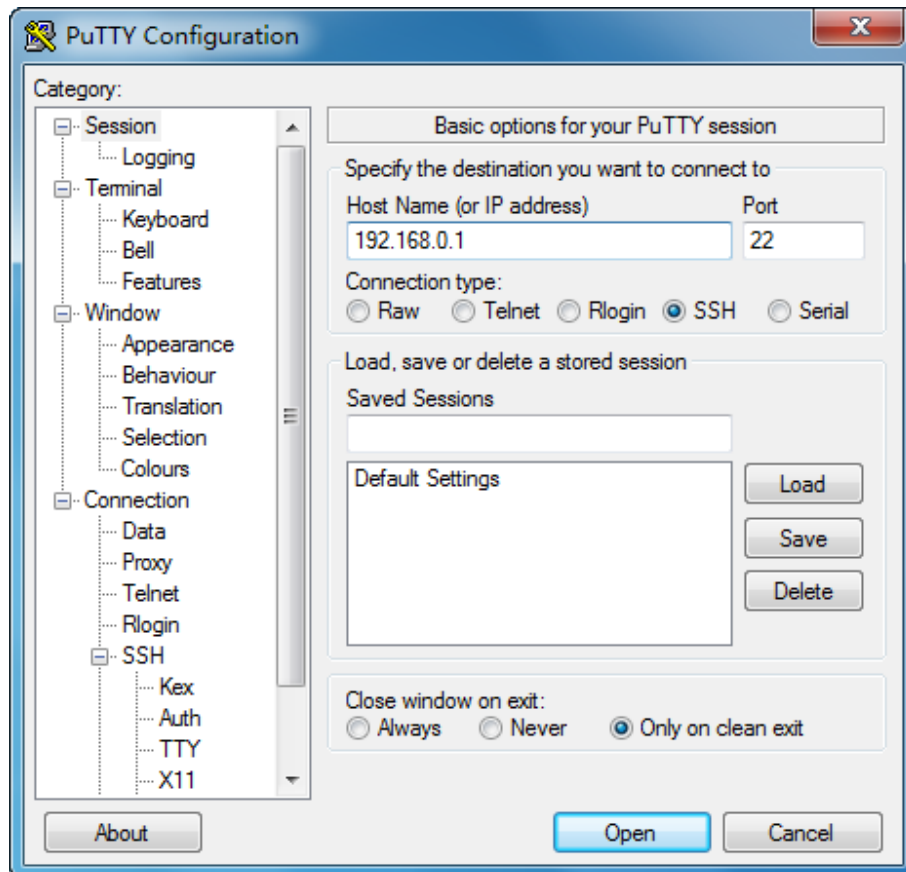


Figure 1-11 SSH Connection Config

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

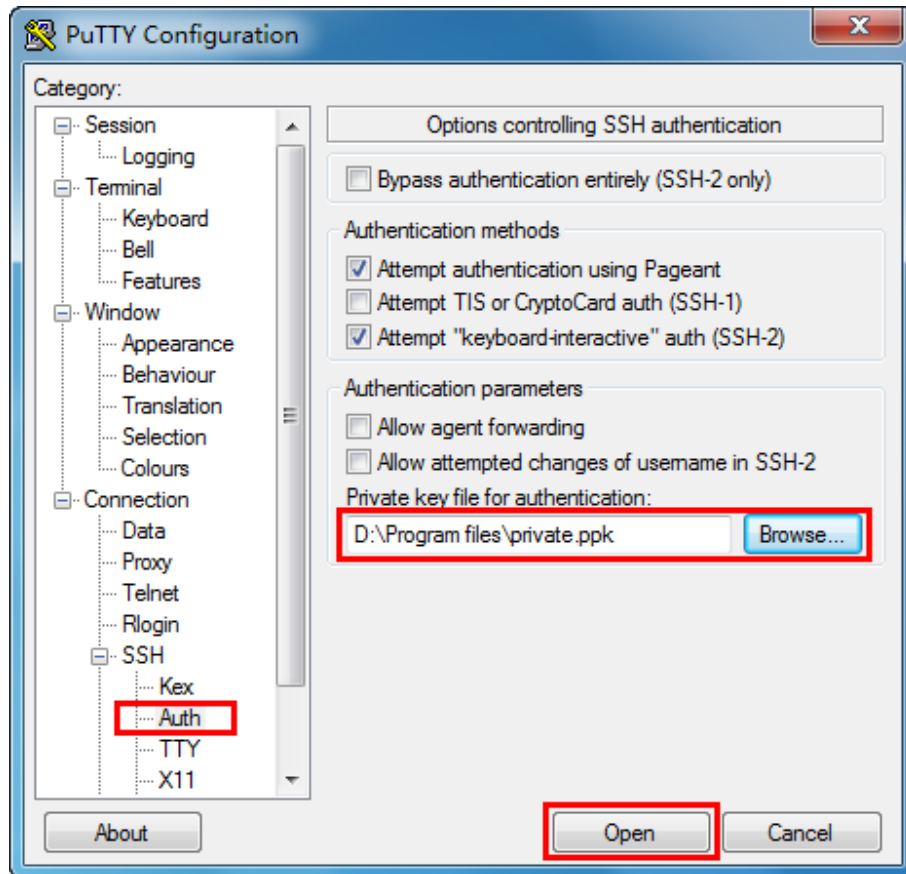


Figure 1-12 Download the Private Key

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.

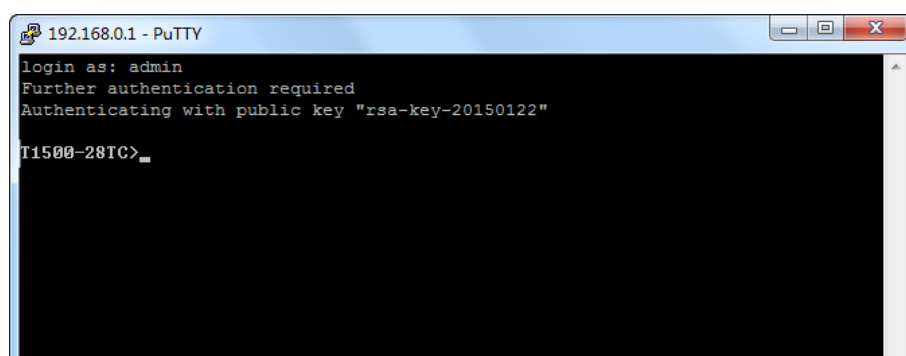


Figure 1-13 Log on the Switch

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.	T1500-28PCT>	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.	T1500-28PCT#	Enter 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.	T1500-28PCT(config)#	Use the exit or the end command or press Ctrl+Z to return to Privileged EXEC mode. Use the interface gigabitEthernet port or interface range fastEthernet port-list gigabitEthernet port-list command to access interface Configuration mode. Use the vlan vlan-list to access VLAN Configuration mode.
Interface Configuration Mode	Layer 2 Interface: Use the interface gigabitEthernet port , interface port-channel lagid or interface range fastEthernet port-list gigabitEthernet port-list command to enter this mode from Global Configuration mode.	T1500-28PCT(config-if)# or T1500-28PCT(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	Use the interface <i>vlan-id</i> command to enter VLAN Interface mode from Global Configuration mode. Use the interface <i>loopback id</i> command to enter Loopback Interface mode from Global Configuration mode.	T1500-28PCT(config-if)# or T1500-28PCT(config-if-range)#	Use the switchport command to switch to the Layer 2 interface mode. Use the end command or press Ctrl+Z to return to Privileged EXEC mode. Enter the exit or the # command to return to Global Configuration mode.
VLAN Configuration Mode	Use the vlan <i>vlan-list</i> command to enter this mode from Global Configuration mode.	T1500-28PCT(config-vlan)#	Use the end command or press Ctrl+Z to return to Privileged EXEC mode. Enter the exit command or the # command to return to Global configuration mode.



Note:

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

- **Global Configuration Mode:** In this mode, global commands are provided, such as the Spanning Tree, Schedule Mode and so on.
- **Interface Configuration Mode:** In this mode, users can configure one or several ports, different ports corresponds to different commands
 - a). Interface gigabitEthernet: Configure parameters for an Ethernet port, such as Duplex-mode, flow control status.
 - b). Interface range gigabitEthernet: Configure parameters for several Ethernet ports.
 - c). Interface link-aggregation: Configure parameters for a link-aggregation, such as broadcast storm.
 - d). Interface range link-aggregation: Configure parameters for multi-trunks.
 - e). Interface vlan: Configure parameters for the vlan-port.
- **VLAN Configuration Mode:** In this mode, users can create a VLAN and add a specified port to the VLAN.

3. Some commands are global, that means they can be performed in all modes:
 - **show**: Display all information of switch, for example: statistic information, port information, VLAN information.
 - **history**: Display the commands history.

1.3 Privilege Restrictions

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

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

1.4 Conventions

1.4.1 Format Conventions

The following conventions are used in this Guide:

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

1.4.2 Special Characters

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

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

1.4.3 Parameter Format

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

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

Chapter 2 User Interface

2.1 enable

Description

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

Syntax

enable

Command Mode

User EXEC Mode

Privilege Requirement

None.

Example

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

```
T1500-28PCT>enable
Enter password:
T1500-28PCT#
```

2.2 enable-admin

Description

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

Syntax

enable-admin

Command Mode

Privileged Configuration Mode

Privilege Requirement

None.

User Guidelines

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

Example

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

```
T1500-28PCT#enable-admin
Password:123
T1500-28PCT#
```

2.3 service password-encryption

Description

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

Syntax

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

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the global encryption function:

```
T1500-28PCT(config)# service password-encryption
```

2.4 enable password

Description

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

Syntax

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

no enable password

Parameter

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

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

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

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

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

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

Example

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

```
T1500-28PCT(config)#enable password 0 admin
```

2.5 enable secret

Description

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

Syntax

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

Parameter

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

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

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

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

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

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

Example

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

```
T1500-28PCT(config)#enable secret 0 admin
```

2.6 configure

Description

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

Syntax

```
configure
```

Command Mode

Privileged EXEC Mode

Privilege Requirement

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

Example

Access Global Configuration Mode from Privileged EXEC Mode:

```
T1500-28PCT#configure  
T1500-28PCT(config)#
```

2.7 exit

Description

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

Syntax

```
exit
```


Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

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

```
T1500-28PCT(config-if)# exit
T1500-28PCT(config)#exit
T1500-28PCT#
```

2.8 end

Description

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

Syntax

```
end
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Return to Privileged EXEC Mode from Interface Configuration Mode:

```
T1500-28PCT(config-if)#end
T1500-28PCT#
```

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:

```
T1500-28PCT (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:

```
T1500-28PCT(config)#history clear
```

Chapter 3 IEEE 802.1Q VLAN Commands

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

3.1 vlan

Description

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

Syntax

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

Parameter

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create VLAN 2-10 and VLAN 100:

```
T1500-28PCT(config)# vlan 2-10,100
```

Delete VLAN 2:

```
T1500-28PCT(config)# no vlan 2
```

3.2 interface vlan

Description

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

Syntax

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

Parameter

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create VLAN Interface 2:

```
T1500-28PCT(config)# interface vlan 2
```

3.3 name

Description

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

Syntax

```
name descript  
no name
```

Parameter

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

Command Mode

VLAN Configuration Mode(VLAN)

Privilege Requirement

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

Example

Specify the name of VLAN 2 as "group1":

```
T1500-28PCT(config)# vlan 2
T1500-28PCT(config-vlan)# name group1
```

3.4 switchport general allowed vlan

Description

The **switchport general allowed vlan** command is used to add the desired General port to IEEE 802.1Q VLAN and specify the port's type. To delete the corresponding VLAN(s), please use **no switchport general allowed vlan** command.

Syntax

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

tagged | untagged — Egress rule, untagged or tagged. Tagged: All packets forwarded by the port are tagged. The packets contain VLAN information. Untagged: Packets forwarded by the port are untagged.

Command Mode

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

Privilege Requirement

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

Example

Add port 4 it to VLAN 2 and configure the type of port 1/0/4 as tagged:

```
T1500-28PCT(config)#interface fastEthernet 1/0/4
```

3.5 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 fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)#interface fastEthernet 1/0/2
```

```
T1500-28PCT(config-if)# switchport pvid 2
```

3.6 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:

```
T1500-28PCT(config)# show vlan summary
```

3.7 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:

```
T1500-28PCT(config)# show vlan brief
```

3.8 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:

```
T1500-28PCT(config)# show vlan id 5
```

3.9 show interface switchport

Description

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

Syntax

```
show interface switchport [ gigabitEthernet port | port-channel lagid ]
```

Parameter

port — The port number.

lagid — The ID of the LAG.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the VLAN configuration information of all ports and LAGs:

```
T1500-28PCT(config)# show interface switchport
```


Chapter 4 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.

4.1 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:

```
T1500-28PCT(config)# voice vlan 10
```

4.2 voice vlan aging

Description

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

Syntax

voice vlan aging *time*

no voice vlan aging

Parameter

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)# voice vlan aging 1
```

4.3 voice vlan priority

Description

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

Syntax

voice vlan priority *pri*

no voice vlan priority

Parameter

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the priority of the Voice VLAN as 5:

```
T1500-28PCT(config)# voice vlan priority 5
```

4.4 voice vlan mac-address

Description

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

Syntax

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

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

Parameter

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

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

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)#voice vlan mac-address 00:11:11:11:11:11 mask  
FF:FF:FF:00:00:00 description TP-Phone
```

4.5 switchport voice vlan mode

Description

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

Syntax

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

Parameter

manual | auto — Port mode.

Command Mode

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

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)#interface fastEthernet 1/0/3  
T1500-28PCT(config-if)# switchport voice vlan mode auto
```

4.6 switchport voice vlan security

Description

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

Syntax

```
switchport voice vlan security
```

```
no switchport voice vlan security
```

Command Mode

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

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)#interface fastEthernet 1/0/3
T1500-28PCT(config-if)# switchport voice vlan security
```

4.7 show voice vlan

Description

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

Syntax

```
show voice vlan
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

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

Example

Display the configuration information of Voice VLAN globally:

```
T1500-28PCT(config)# show voice vlan
```

4.8 show voice vlan oui

Description

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

Syntax

```
show voice vlan oui
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

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

Example

Display the configuration information of Voice VLAN OUI:

```
T1500-28PCT(config)# show voice vlan oui
```

4.9 show voice vlan switchport

Description

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

Syntax

```
show voice vlan switchport [ gigabitEthernet port | port-channel lagid ]
```

Parameter

port—— The Ethernet port number.

lagid—— The ID of the LAG.

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 LAGs:

```
T1500-28PCT(config)# show voice vlan switchport
```

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

```
T1500-28PCT(config)# show voice vlan switchport fastEthernet 1/0/2
```

Chapter 5 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.

5.1 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 6.

on — Enable the static LAG.

active — Enable the active LACP mode.

passive — Enable the passive LACP mode.

Command Mode

Interface Configuration Mode (interface fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)# interface range fastEthernet 1/0/2-4
T1500-28PCT(config-if-range)# channel-group 1 mode on
```

5.2 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":

```
T1500-28PCT(config)# port-channel load-balance src-dst-ip
```

5.3 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:

```
T1500-28PCT(config)# lacp system-priority 1024
```

5.4 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 fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)# interface range fastEthernet 1/0/1-3  
T1500-28PCT(config-if-range)# lacp port-priority 1024
```

Configure the LACP port priority as 2048 for port 4:

```
T1500-28PCT(config)#interface fastEthernet 1/0/4  
T1500-28PCT(config-if)# lacp port-priority 2048
```

5.5 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 6. 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:

```
T1500-28PCT(config)# show etherchannel 1 detail
```

5.6 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:

```
T1500-28PCT(config)# show etherchannel load-balance
```

5.7 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 6. 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:

```
T1500-28PCT(config)# show lacp 1 internal
```

5.8 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:

```
T1500-28PCT(config)# show lacp sys-id
```

Chapter 6 User Management Commands

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

6.1 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:

```
T1500-28PCT(config)#user name tplink privilege admin password 0 admin
```

6.2 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.

```
T1500-28PCT(config)#user name tplink privilege admin secret 0 admin
```

6.3 user access-control ip-based

Description

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

Syntax

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

Parameter

ip-addr — The source IP address. Only the users within the IP-range you set here are allowed to access the switch.

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.

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:

```
T1500-28PCT(config)# user access-control ip-based 192.168.0.148  
255.255.255.255
```

6.4 user access-control mac-based

Description

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

Syntax

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

Parameter

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

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)# user access-control mac-based 00:00:13:0A:00:01
```

6.5 user access-control port-based

Description

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

Syntax

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

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.

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 access the switch:

```
T1500-28PCT(config)# user access-control port-based interface  
fastEthernet 1/0/2-6
```

6.6 telnet

Description

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

Syntax

```
telnet enable
```

```
telnet disable
```

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Disable the Telnet function:

```
T1500-28PCT(config)# telnet disable
```

6.7 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:

```
T1500-28PCT(config)# show user account-list
```

6.8 show user configuration

Description

The **show user configuration** command is used to display the security configuration information of the user authentication information and the access interface.

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:

```
T1500-28PCT(config)# show user configuration
```

6.9 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:

```
T1500-28PCT(config)# show telnet-status
```

Chapter 7 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.

7.1 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:

```
T1500-28PCT(config)# no ip http server
```

7.2 ip http max-users

Description

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

Syntax

ip http max-users *admin-num operator-num power-user-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.

power-user-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 logging on to the HTTP server as 5, 2, 2, and 1:

```
T1500-28PCT(config)# ip http max-users 5 2 2 1
```


7.3 ip http session timeout

Description

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

Syntax

```
ip http session timeout minutes  
no ip http session timeout
```

Parameter

minutes——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 server connection as 15 minutes:

```
T1500-28PCT(config)# ip http session timeout 15
```

7.4 ip http secure-server

Description

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

Syntax

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Disable the HTTPS function:

```
T1500-28PCT(config)# no ip http secure-server
```

7.5 ip http secure-protocol

Description

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

Syntax

```
ip http secure-protocol [[ssl3][tls1]]
```

```
no ip http secure-protocol
```

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:

```
T1500-28PCT(config)# ip http secure-protocol ssl3
```

7.6 ip http secure-ciphersuite

Description

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

Syntax

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

Parameter

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)# ip http secure-ciphersuite 3des-ede-cbc-sha
```

7.7 ip http secure-max-users

Description

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

Syntax

```
ip http secure-max-users admin-num operator-num power-user-num  
user-num
```

```
no ip http 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 no more 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 no more than 16.

power-user-num — The maximum number of the users logging on to the HTTPS 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 HTTPS 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, Operator and Power User level users have access to these commands.

Example

Configure the maximum number of the Admin, Operator, Power User and User logging on to the HTTPS server as 5, 2, 2, and 1:

```
T1500-28PCT(config)# ip http secure-max-users 5 2 2 1
```

7.8 ip http secure-session timeout

Description

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

Syntax

ip http secure-session timeout *minutes*

no ip http secure-session timeout

Parameter

minutes — 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 server connection as 15 minutes:

```
T1500-28PCT(config)# ip http secure-session timeout 15
```

7.9 ip http secure-server download certificate

Description

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

Syntax

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

Parameter

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

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

```
T1500-28PCT(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

```
T1500-28PCT(config)# ip http secure-server download certificate ssl-cert  
ip-address fe80::1234
```

7.10 ip http secure-server download key

Description

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

Syntax

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

Parameter

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

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

```
T1500-28PCT(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

```
T1500-28PCT(config)# ip http secure-server download key ssl-key
ip-address fe80::1234
```

7.11 show ip http configuration

Description

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

Syntax

```
show ip http configuration
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration information of the HTTP server:

```
T1500-28PCT(config)# show ip http configuration
```

7.12 show ip http secure-server

Description

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

Syntax

show ip http secure-server

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of SSL:

```
T1500-28PCT(config)# show ip http secure-server
```


Chapter 8 Binding Table Commands

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

8.1 ip source binding

Description

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

Syntax

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

Parameter

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

ip-addr — The IP address of the Host.

mac-addr — The MAC address of the Host.

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

port — The number of port connected to the Host.

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

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

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)#ip source binding host1 192.168.0.1  
00:00:00:00:00:01 vlan 2 interface fastEthernet 1/0/5 arp-detection
```

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

```
T1500-28PCT(config)#no ip source binding index 5
```

8.2 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. The switch can also propagate the control information and the network parameters via the Option 82 field to provide more information for the Host.

Syntax

ip dhcp snooping

no ip dhcp snooping

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the DHCP Snooping function globally:

```
T1500-28PCT(config)#ip dhcp snooping
```

8.3 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:

```
T1500-28PCT(config)#ip dhcp snooping vlan 1,4,6-7
```

8.4 ip dhcp snooping information option

Description

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

Syntax

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

Command Mode

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

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)#interface fastEthernet 1/0/1  
T1500-28PCT(config-if)#ip dhcp snooping information option
```

8.5 ip dhcp snooping information strategy

Description

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

Syntax

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

Parameter

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

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

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

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

Command Mode

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

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)#interface fastEthernet 1/0/1
```

```
T1500-28PCT(config-if)#ip dhcp snooping information strategy replace
```

8.6 ip dhcp snooping information remote-id

Description

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

Syntax

```
ip dhcp snooping information remote-id string
```

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

Parameter

string — Enter the sub-option Remote ID, which contains 64 characters at most.

Command Mode

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

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)#interface fastEthernet 1/0/1
T1500-28PCT(config-if)#ip dhcp snooping information remote-id tplink
```

8.7 ip dhcp snooping information circuit-id

Description

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

Syntax

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

Parameter

string — Enter the sub-option Circuit ID, which contains 64 characters at most.

Command Mode

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

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)#interface fastEthernet 1/0/1
T1500-28PCT(config-if)#ip dhcp snooping information circuit-id tplink
```

8.8 ip dhcp snooping trust

Description

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

Syntax

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

Command Mode

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

Privilege Requirement

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

Example

Configure the port 1/0/2 to be a Trusted Port:

```
T1500-28PCT(config)#interface fastEthernet 1/0/2
T1500-28PCT(config-if)#ip dhcp snooping trust
```

8.9 ip dhcp snooping mac-verify

Description

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

Syntax

ip dhcp snooping mac-verify

no ip dhcp snooping mac-verify

Command Mode

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

Privilege Requirement

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

Example

Enable the MAC Verify feature for the port 10/2:

```
T1500-28PCT(config)#interface fastEthernet 1/0/2
T1500-28PCT(config-if)#ip dhcp snooping mac-verify
```

8.10 ip dhcp snooping limit rate

Description

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

Syntax

ip dhcp snooping limit rate *value*

no ip dhcp snooping limit rate

Parameter

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

Command Mode

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

Privilege Requirement

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

Example

Set the Flow Control of port 1/0/2 as 20 pps:

```
T1500-28PCT(config)#interface fastEthernet 1/0/2
T1500-28PCT(config-if)#ip dhcp snooping limit rate 20
```

8.11 ip dhcp snooping decline rate

Description

The **ip dhcp snooping decline rate** command is used to enable the Decline Protect feature and configure the rate limit on DHCP Decline packets. The excessive DHCP Decline packets will be discarded. To disable the Decline Protect feature, please use **no ip dhcp snooping decline rate** command.

Syntax

ip dhcp snooping decline rate *value*
no ip dhcp snooping decline rate

Parameter

value — Specify the rate limit of DHCP Decline packets, and the optional values are 0, 5, 10, 15, 20, 25 and 30 (units:packet/second). Its default value is 0, which stands for "disable".

Command Mode

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

Privilege Requirement

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

Example

Configure the rate limit of DHCP Decline packets as 20 packets per second on port 1/0/2:

```
T1500-28PCT(config)#interface fastEthernet 1/0/2
T1500-28PCT(config-if)#ip dhcp snooping decline 20
```

8.12 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:

```
T1500-28PCT(config)#show ip source binding
```

8.13 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:

```
T1500-28PCT#show ip dhcp snooping
```

8.14 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/LAG or of all Ethernet ports/LAGs.

Syntax

```
show ip dhcp snooping interface [ gigabitEthernet port | port-channel lagid]
```

Parameters

port— The Ethernet port number.

lagid— The ID of the LAG.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DHCP Snooping configuration of all Ethernet ports and LAGs:

```
T1500-28PCT#show ip dhcp snooping interface
```

Display the DHCP Snooping configuration of port 1/0/5:

```
T1500-28PCT#show ip dhcp snooping interface fastEthernet 1/0/5
```

8.15 show ip dhcp snooping information interface

Description

The **show ip dhcp snooping information interface** command is used to display the DHCP snooping option 82 configuration of a desired port/port channel or of all Ethernet ports/port channels.

Syntax

```
show ip dhcp snooping information 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 option 82 configuration of all Ethernet ports and port channels:

```
T1500-28PCT#show ip dhcp snooping information interface
```

Chapter 9 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.

9.1 ip arp inspection(global)

Description

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

Syntax

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the ARP Detection function globally:

```
T1500-28PCT(config)#ip arp inspection
```

9.2 ip arp inspection trust

Description

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

Syntax

ip arp inspection trust

no ip arp inspection trust

Command Mode

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

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)#interface range fastEthernet 1/0/2-5
```

```
T1500-28PCT(config-if-range)#ip arp inspection trust
```

9.3 ip arp inspection(interface)

Description

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

Syntax

ip arp inspection

no ip arp inspection

Command Mode

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

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)#interface range fastEthernet 1/0/2-6
T1500-28PCT(config-if-range)#ip arp inspection
```

9.4 ip arp inspection limit-rate

Description

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

Syntax

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

Parameter

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

Command Mode

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

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)#interface fastEthernet 1/0/5
```

```
T1500-28PCT(config-if)#ip arp inspection limit-rate 50
```

9.5 ip arp inspection recover

Description

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

Syntax

```
ip arp inspection recover
```

Command Mode

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

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)#interface fastEthernet 1/0/5
```

```
T1500-28PCT(config-if)#ip arp inspection recover
```

9.6 show ip arp inspection

Description

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

Syntax

```
show ip arp inspection
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the ARP detection configuration globally:

```
T1500-28PCT(config)#show ip arp inspection
```

9.7 show ip arp inspection interface

Description

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

Syntax

```
show ip arp inspection interface [ gigabitEthernet port | port-channel  
lagid]
```

Parameter

port—The Ethernet port number.

lagid—The ID of the LAG.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of port 1/0/1:

```
T1500-28PCT(config)#show ip arp inspection interface fastEthernet 1/0/1
```

Display the configuration of all Ethernet ports:

```
T1500-28PCT(config)#show ip arp inspection interface
```

9.8 show ip arp inspection statistics

Description

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

Syntax

```
show ip arp inspection statistics
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the number of the illegal ARP packets received:

```
T1500-28PCT(config)#show ip arp inspection statistics
```

9.9 clear ip arp inspection statistics

Description

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

Syntax

```
clear ip arp inspection statistics
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

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

Example

Clear the statistic of the illegal ARP packets received:

```
T1500-28PCT(config)#clear ip arp inspection statistics
```

Chapter 10 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.

10.1 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:

```
T1500-28PCT(config)#ip dos-prevent
```

10.2 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 | smurf |  
ping-of-death }
```

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

Parameter

land — Land attack.

scan-synfin — Scan SYNFIN attack.

xma-scan — Xma Scan attack.

null-scan — NULL Scan attack.

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

blat — Blat attack.

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

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

win-nuke — winNuke attack.

smurf — Smurf attack.

ping-of-death — Ping of Death attack.

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:

```
T1500-28PCT(config)#ip dos-prevent type land
```

10.3 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:

```
T1500-28PCT(config)#show ip dos-prevent
```

Chapter 11 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.

11.1 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:

```
T1500-28PCT(config)#logging buffer
```

11.2 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:

```
T1500-28PCT(config)#logging buffer level 5
```

11.3 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:

```
T1500-28PCT(config)#logging file flash
```

11.4 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:

```
T1500-28PCT(config)#logging file flash frequency periodic 10
```


11.5 logging file flash level

Description

The **logging file flash level** command is used to specify the system log message severity level. Messages with a severity level equal to or higher than this value will be stored to the flash. To restore to the default level, please use **no logging file flash level** command.

Syntax

logging file flash level *level*

no logging file flash level

Parameter

level — Severity level of the log message. There are 8 severity levels marked with values 0-7. The smaller value has the higher priority. Only the log with the same or smaller severity level value will be saved to the flash. By default, it is 3 indicating that the log message marked with 0~3 will be saved in the log flash.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin 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 :

```
T1500-28PCT(config)#logging file flash level 7
```

11.6 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:

```
T1500-28PCT(config)# logging host index 2 192.168.0.148 5
```

11.7 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:

```
T1500-28PCT(config)# no logging monitor
```

11.8 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

Set the severity level as 7:

```
T1500-28PCT(config)# logging monitor level 7
```

11.9 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:

```
T1500-28PCT(config)# clear logging buffer
```

11.10 show logging local-config

Description

The **show logging local-config** command is used to display the configuration of the Local Log output to 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:

```
T1500-28PCT(config)# show logging local-config
```

11.11 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:

```
T1500-28PCT(config)# show logging loghost 2
```

11.12 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:

```
T1500-28PCT(config)# show logging buffer level 5
```

11.13 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:

```
T1500-28PCT(config)# show logging flash level 3
```

Chapter 12 SSH Commands

SSH (Security Shell) can provide the unsecured remote management with security and powerful authentication to ensure the security of the management information.

12.1 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:

```
T1500-28PCT(config)# ip ssh server
```

12.2 ip ssh version

Description

The **ip ssh version** command is used to enable the SSH protocol version. To disable the protocol version, please use **no ip ssh version** command.

Syntax

ip ssh version {v1 | v2}
no ip ssh version {v1 | v2}

Parameter

v1 | v2 — The SSH protocol version to be enabled. They represent SSH v1 and SSH v2 respectively.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable SSH v2:

```
T1500-28PCT(config)# ip ssh version v2
```

12.3 ip ssh algorithm

Description

The **ip ssh algorithm** command is used to configure the algorithm in SSH function. To disable the specified algorithm, please use **no ip ssh algorithm** command.

Syntax

```
ip ssh algorithm { AES128-CBC | AES192-CBC | AES256-CBC | Blowfish-CBC  
| Cast128-CBC | 3DES-CBC | HMAC-SHA1 | HMAC-MD5 }
```

```
no ip ssh algorithm
```

Parameter

AES128-CBC | AES192-CBC | AES256-CBC | Blowfish-CBC | Cast128-CBC | 3DES-CBC | HMAC-SHA1 | HMAC-MD5 — Specify the SSH algorithm.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the SSH algorithm as AES128-CBC:

```
T1500-28PCT(config)# ip ssh algorithm AES128-CBC
```


12.4 ip ssh timeout

Description

The **ip ssh timeout** command is used to specify the idle-timeout time of SSH. To restore to the factory defaults, please use **no 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:

```
T1500-28PCT(config)# ip ssh timeout 30
```

12.5 ip ssh max-client

Description

The **ip ssh max-client** command is used to specify the maximum number of the connections to the SSH server. To return to the default configuration, please use **no ip ssh max-client** command.

Syntax

ip ssh max-client *num*

no ip ssh max-client

Parameter

num — The maximum number of the connections to the SSH server. It ranges from 1 to 5. By default, this value is 5.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the maximum number of the connections to the SSH server as 3:

```
T1500-28PCT(config)# ip ssh max-client 3
```

12.6 ip ssh download

Description

The **ip ssh download** command is used to download the SSH key file from TFTP server.

Syntax

```
ip ssh download {v1 | v2} key-file ip-address ip-addr
```

Parameter

v1 | v2 — Select the type of SSH key to download, v1 represents SSH-1, v2 represents SSH-2.

key-file — The name of the key-file which is selected to download. The length of the name ranges from 1 to 25 characters. The key length of the downloaded file must be in the range of 512 to 3072 bits.

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Download an SSH-1 type key file named ssh-key from TFTP server with the IP address 192.168.0.148:

```
T1500-28PCT(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:

```
T1500-28PCT(config)# ip ssh download v1 ssh-key ip-address fe80::1234
```

12.7 remove public-key

Description

The **remove public-key** command is used to remove the SSH public key from the switch.

Syntax

```
remove public-key { v1 | v2 }
```

Parameter

v1 | v2 — Select the type of SSH public key, v1 represents SSH-1, v2 represents SSH-2.

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Remove the SSH-1 type public key from the switch:

```
T1500-28PCT# remove public-key v1
```

12.8 show ip ssh

Description

The **show ip ssh** command is used to display the global configuration of SSH.

Syntax

```
show ip ssh
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of SSH:

```
T1500-28PCT(config)# show ip ssh
```

Chapter 13 IEEE 802.1X Commands

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

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

This chapter handles with the authentication process between the supplicant and the switch. To realize the authentication and accounting function, you should also enable the AAA function and configure the RADIUS server. Go to [Chapter 34 AAA Commands](#) for more details.

13.1 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:

13.2 dot1x handshake

Description

The **dot1x handshake** command is used to 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:

```
T1500-28PCT(config)# no dot1x handshake
```

13.3 dot1x auth-method

Description

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

Syntax

```
dot1x auth-method { pap | eap }
```

```
no dot1x auth-method
```

Parameter

pap | eap —Authentication Methods.

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

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)#dot1x auth-method pap
```

13.4 dot1x accounting

Description

The **dot1x accounting** command is used to enable the IEEE 802.1X accounting function globally. To disable the enable 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:

```
T1500-28PCT(config)#dot1x accounting
```

13.5 dot1x guest-vlan(global)

Description

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

Syntax

```
dot1x guest-vlan vid
```

```
no dot1x guest-vlan
```

Parameter

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the Guest VLAN function for VLAN 5:

```
T1500-28PCT(config)#dot1x guest-vlan 5
```

13.6 dot1x quiet-period

Description

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

Syntax

```
dot1x quiet-period [ time ]
```

```
no dot1x quiet-period
```

Parameter

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the quiet-period function:

```
T1500-28PCT(config)#dot1x quiet-period
```

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

```
T1500-28PCT(config)#dot1x quiet-period 5
```

13.7 dot1x timeout

Description

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

Syntax

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


no dot1x timeout supplicant-timeout

Parameter

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the supplicant's timeout value as 5 seconds:

```
T1500-28PCT(config)#dot1x timeout supplicant-timeout 5
```

13.8 dot1x max-reauth-req

Description

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

Syntax

dot1x max-reauth-req *times*

no dot1x max-reauth-req

Parameter

times —— The maximum transfer times of the repeated authentication request, ranging from 1 to 9 in times. By default, the value is 3.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the maximum transfer times of the repeated authentication request as 5:

```
T1500-28PCT(config)#dot1x max-reauth-req 5
```

13.9 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 fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the IEEE 802.1X function for the port 1/0/1:

```
T1500-28PCT(config)#interface fastEthernet 1/0/1
```

```
T1500-28PCT(config-if)#dot1x
```

13.10 dot1x guest-vlan(interface)

Description

The **dot1x guest-vlan** command is used to enable the guest VLAN function for a specified port. To disable the Guest VLAN function for a specified port, please use **no dot1x guest-vlan** command. Please ensure that the Control Type of the corresponding port is port-based before enabling the guest VLAN function for it.

Syntax

dot1x guest-vlan

no dot1x guest-vlan

Command Mode

Interface Configuration Mode (interface fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the Guest VLAN function for port 1/0/2:

```
T1500-28PCT(config)#interface fastEthernet 1/0/2
T1500-28PCT(config-if)#dot1x guest-vlan
```

13.11 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 fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure the Control Mode for port 1/0/20 as "authorized-force":

```
T1500-28PCT(config)#interface fastEthernet 1/0/20
T1500-28PCT(config-if)#dot1x port-control authorized-force
```

13.12 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 fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure the Control Type for port 1/0/20 as "port-based":

```
T1500-28PCT(config)#interface fastEthernet 1/0/20
T1500-28PCT(config-if)#dot1x port-method port-based
```

13.13 show dot1x global

Description

The **show dot1x global** command is used to display the global configuration of 802.1X.

Syntax

```
show dot1x global
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of 802.1X globally:

```
T1500-28PCT(config)#show dot1x global
```

13.14 show dot1x interface

Description

The **show dot1x interface** command is used to display all ports or the specified port's configuration information of 802.1X.

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 802.1X for port 1/0/2:

```
T1500-28PCT(config)#show dot1x interface fastEthernet 1/0/2
```

Display the configuration information of 802.1X for all Ethernet ports:

```
T1500-28PCT(config)#show dot1x interface
```

Chapter 14 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.

14.1 mac address-table static

Description

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

Syntax

```
mac address-table static mac-addr vid vid interface gigabitEthernet port  
no mac address-table static { mac-addr | vid vid | mac-addr vid vid |  
interface gigabitEthernet port}
```

Parameter

mac-addr——The MAC address of the entry you desire to add.

vid—— The VLAN ID number of your desired entry. It ranges from 1 to 4094.

port—— The Ethernet port number of your desired entry.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Add a static Mac address entry to bind the MAC address 00:02:58:4f:6c:23, VLAN1 and port 1 together:

```
T1500-28PCT(config)# mac address-table static 00:02:58:4f:6c:23 vid 1  
interface fastEthernet 1/0/1
```

14.2 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:

```
T1500-28PCT(config)# mac address-table aging-time 500
```

14.3 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:

```
T1500-28PCT(config)# mac address-table filtering 00:1e:4b:04:01:5d vid 1
```

14.4 mac address-table notification

Description

The **mac address-table notification** command is used to configure global settings of MAC address table notification.

Syntax

```
mac address-table notification { [ global-status enable | disable ]  
[ table-full-status enable | disable ] [ interval time ] }
```

Parameter

global-status enable | disable — Enable/Disable the notification function globally.

table-full-status enable | disable — Enable/Disable the MAC threshold notification. With this feature enabled, a SNMP notification is generated and sent to the network management system (NMS) when the threshold of the switch's MAC address table is reached or exceeded.

interval *time* — Specify the notification trap interval between each set of traps that are generated to the NMS. The interval ranges from 1 to 1000 seconds and it's 1 second by default.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the global MAC address notification and table full notification, specify the notification sending interval as 2 seconds:

```
T1500-28PCT(config)# mac address-table notification global-status
enable table-full-status enable interval 2
```

14.5 mac address-table notification (interface)

Description

The **mac address-table notification** command is used to configure the MAC change notification on port.

Syntax

```
mac address-table notification { [ learn-mode-change enable | disable ]
[ exceed-max-learned enable | disable ] [ new-mac-learned enable |
disable ] }
```

Parameter

learn-mode-change enable | disable — Enable/Disable the learn-mode-change notification. With this feature enabled, a SNMP notification is generated and sent to the network management system (NMS) when the learning mode of this port changes. To configure the learning mode configuration, please refer to [mac address-table max-mac-count](#).

exceed-max-learned enable | disable — Enable/Disable the MAC address threshold notification on this port. With this feature enabled, a SNMP notification is generated and sent to the network management system (NMS) when the MAC address threshold limit on this port is reached or exceeded. To configure the port's MAC address threshold, please refer to [mac address-table max-mac-count](#).

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

Command Mode

Interface Configuration Mode (interface fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the learn-mode-change notification on port 1/0/2:

```
T1500-28PCT(config)# mac address-table notification global-status
enable

T1500-28PCT(config)#interface fastEthernet 1/0/2

T1500-28PCT(config-if)#      mac      address-table      notification
learn-mode-change enable
```

14.6 mac address-table max-mac-count

Description

The **mac address-table max-mac-count** command is used to configure the Port Security. To return to the default configurations, please use **no mac address-table max-mac-count** command. Port Security is to protect the switch from the malicious MAC address attack by limiting the maximum number of the MAC addresses that can be learned on the port. The port with Port Security feature enabled will learned the MAC address dynamically. When the learned MAC address number reaches the maximum, the port will stop learning. Therefore, the other devices with the MAC address unlearned can not access to the network via this port.

Syntax

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

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

Parameter

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

dynamic | static | permanent — Learn mode for MAC addresses. There are three modes, including Dynamic mode, Static mode and Permanent mode. When Dynamic mode is selected, the learned MAC address will be deleted automatically after the aging time. When Static mode is selected, the learned MAC address will be out of the influence of the aging time and can only be deleted manually. The learned entries will be cleared after the switch is rebooted. When permanent mode is selected, the learned MAC address will be out of the influence of the aging time and can only be deleted manually too. However, the learned entries will be saved even the switch is rebooted.

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

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

Command Mode

Interface Configuration Mode (interface fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable Port Security function for port 1, select Static mode as the learn mode, and specify the maximum number of MAC addresses that can be learned on this port as 30:

```
T1500-28PCT(config)#interface fastEthernet 1/0/1
T1500-28PCT(config-if)# mac address-table max-mac-count max-number
30 mode static status enable
```

14.7 mac address-table security

Description

The **mac address-table security** command is used to configure security of the MAC address table in a specified VLAN.

Syntax

```
mac address-table security vid vid max-learn number { forward | drop | disable }
```

Parameter

vid—— Specify the VLAN ID to configure its MAC address table.

number—— Configure the threshold of the MAC address table in this VLAN. It ranges from 0 to 16383.

forward | drop | disable —— Choose the mode when learned MAC number exceeds the threshold of the MAC address table in this VLAN.

- Drop: The packets will be dropped when learned MAC number exceeds the threshold of the MAC address table in this VLAN..
- Forward: The packets will be forward but not be learned when learned MAC number exceeds the threshold of the MAC address table in this VLAN..
- Disable: The threshold of the MAC address table is disabled.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the max learned MAC address number is VLAN 2 as 1000, and drop the packets that have no match in the MAC address table:

```
T1500-28PCT(config)# mac address-table security vid 2 max-learn 1000  
drop
```

14.8 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:

```
T1500-28PCT(config)# show mac address-table
```

14.9 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:

```
T1500-28PCT(config)# clear mac address-table static
```

14.10 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:

```
T1500-28PCT(config)# show mac address-table aging-time
```

14.11 show mac address-table max-mac-count

Description

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

Syntax

```
show mac address-table max-mac-count { all | interface 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:

```
T1500-28PCT(config)# show mac address-table max-mac-count
```

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

```
T1500-28PCT(config)# show mac address-table max-mac-count interface
fastEthernet 1/0/1
```

14.12 show mac address-table interface

Description

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

Syntax

```
show mac address-table interface { gigabitEthernet port | port-channel
lagid}
```

Parameter

port—— The Ethernet port number.

lagid—— The ID of the LAG.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

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

```
T1500-28PCT(config)# show mac address-table interface fastEthernet
1/0/1
```

14.13 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:

```
T1500-28PCT(config)# show mac address-table count
```

14.14 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 lagid } | vid vlan-id ]
```

Parameter

mac-addr——The specified MAC address.

port—— The Ethernet port number.

lagid—— The ID of the LAG.

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:

```
T1500-28PCT(config)#show mac address-table address 00:00:00:00:23:00  
vid 1
```

14.15 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:

```
T1500-28PCT(config)# show mac address-table vlan 1
```

14.16 show mac address-table notification

Description

The **show mac address-table notification** command is used to display the MAC notification configuration globally or on the specified port.

Syntax

```
show mac address-table notification { all | interface gigabitEthernet port }
```

Parameter

all —— Displays the notification information globally and of all the Ethernet ports.

port—— Displays the notification information on the specified port.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the notification configuration of all the ports:

```
T1500-28PCT(config)# show mac address-table notification all
```

14.17 show mac address-table security

Description

The **show mac address-table vlan** command is used to display the MAC address security configuration of the specified vlan.

Syntax

```
show mac address-table security [ vid vid]
```

Parameter

vid——The specified VLAN id.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the MAC address security configuration of vlan 1:

```
T1500-28PCT(config)# show mac address-table security vid 1
```

Chapter 15 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.

15.1 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

```
T1500-28PCT(config)# system-time manual 12/20/2010-17:30:35
```

15.2 system-time ntp

Description

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

Syntax

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

Parameter

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

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

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

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

UTC-10:00 — TimeZone for Hawaii.

UTC-09:00 — TimeZone for Alaska.

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

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

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

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

UTC-04:30 — TimeZone for Caracas.

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

UTC-03:30 — TimeZone for Newfoundland.

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

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

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

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

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

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

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

UTC+03:30 — TimeZone for Tehran.

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

UTC+04:30 — TimeZone for Kabul.

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

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

UTC+05:45 — TimeZone for Kathmandu.

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

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

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

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

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

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

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

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

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

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

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

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

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)# system-time ntp UTC-12:00 133.100.9.2
139.79.100.163 11
```

15.3 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:

```
T1500-28PCT(config)#system-time dst predefined USA
```

15.4 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:

```
T1500-28PCT(config)# system-time dst date Apr 1 00:00 2015 Oct 1 00:00
2015 30
```

15.5 system-time dst recurring

Description

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

Syntax

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

```
no system-time dst
```

Parameter

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

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

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

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

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

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

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

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

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)# system-time dst recurring first Sun May 02:00 last  
Sun Oct 02:00 45
```

15.6 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 "T1500-28PCT".

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:

```
T1500-28PCT(config)# hostname TPLINK
```

15.7 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:

```
T1500-28PCT(config)# location SHENZHEN
```

15.8 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:

```
T1500-28PCT(config)# contact-info www.tp-link.com
```

15.9 ip address

Description

This **ip address** command is used to configure the IP address, IP subnet mask and default gateway 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 } [ gateway ip-addr ]  
no ip address [ ip-addr ] [ mask ] [ gateway ip-addr ]
```

Parameter

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

mask — The subnet mask of the Layer 3 interface.

gateway — Specify the interface's default gateway.

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 IP address as 192.168.1.1/24 and default gateway as 0.0.0.0:

```
T1500-28PCT(config)# interface vlan 2  
T1500-28PCT(config-if)# ip address 192.168.1.1 255.255.255.0  
T1500-28PCT(config-if)# ip address 192.168.2.1 255.255.255.0 gateway  
0.0.0.0
```

15.10 ip management-vlan

Description

This **ip management-vlan** command is used to specify the management vlan. Only the user in the specified vlan can access to the switch

Syntax

```
ip management-vlan vlan  
no management-vlan vlan
```

Parameter

vlan—— The ID of the management VLAN.

Command Mode

Global Configuration Mode

Example

Set VLAN 2 as the management vlan:

```
T1500-28PCT(config)# ip management-vlan 2
```

15.11 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

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

```
T1500-28PCT(config)# interface vlan 2
T1500-28PCT(config-if)# no ip address
```

15.12 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:

```
T1500-28PCT# reset
```

15.13 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:

```
T1500-28PCT# reboot
```

15.14 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:

```
T1500-28PCT# copy running-config startup-config
```

15.15 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:

```
T1500-28PCT# 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:

```
T1500-28PCT# copy startup-config tftp ip-address fe80::1234 filename
config
```

15.16 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:

```
T1500-28PCT# 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

```
T1500-28PCT# copy tftp startup-config ip-address fe80::1234 filename
config
```

15.17 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:

```
T1500-28PCT(config)# boot application filename image2 startup
```


15.18 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:

```
T1500-28PCT# remove backup-image
```

15.19 firmware upgrade

Description

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

Syntax

```
firmware upgrade ip-address ip-addr filename name
```

Parameter

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

name — Specify the name for the firmware file.

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

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

```
T1500-28PCT# firmware upgrade ip-address 192.168.0.148 filename
firmware.bin

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

Operation OK!

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

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

```
T1500-28PCT# 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
```

15.20 ping

Description

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

Syntax

```
ping [ ip | ipv6 ] { ip_addr } [ -n count ] [ -l count ] [ -i count ]
```

Parameter

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

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

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

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

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

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

Command Mode

User EXEC Mode and Privileged EXEC Mode

Privilege Requirement

None.

Example

To test the connectivity between the switch and the network device with the IP 192.168.0.131, please specify the *count* (-l) as 512 bytes and *count* (-i) as 1000 milliseconds. If there is not any response after 8 times' Ping test, the connection between the switch and the network device is failed to establish:

```
T1500-28PCT# 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:

```
T1500-28PCT# ping fe80::1234 -n 8 -l 512
```

15.21 tracert

Description

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

Syntax

```
tracert [ ip | ipv6 ] ip_addr [ maxHops ]
```

Parameter

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

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

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

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

Command Mode

User EXEC Mode and Privileged EXEC Mode

Privilege Requirement

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

Example

Test the connectivity between the switch and the network device with the IP 192.168.0.131. If the destination device has not been found after 20 *maxHops*, the connection between the switch and the destination device is failed to establish:

```
T1500-28PCT# 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:

```
T1500-28PCT# tracert fe80::1234 20
```

15.22 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:

```
T1500-28PCT# show system-info
```

15.23 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:

```
T1500-28PCT# show image-info
```

15.24 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:

```
T1500-28PCT# show running-config
```

15.25 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:

```
T1500-28PCT# show startup-config
```

15.26 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

```
T1500-28PCT# show system-time
```

15.27 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

```
T1500-28PCT# show system-time dst
```

15.28 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:

```
T1500-28PCT# show system-time ntp
```

15.29 show cable-diagnostics interface gigabitEthernet

Description

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

Syntax

show cable-diagnostics interface gigabitEthernet *port*

Parameter

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

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Show the cable-diagnostics of port 3:

```
T1500-28PCT# show cable-diagnostics interface fastEthernet 1/0/3
```

15.30 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:

```
T1500-28PCT# show cpu-utilization
```

15.31 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:

```
T1500-28PCT# show memory-utilization
```

Chapter 16 Ethernet Configuration Commands

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

16.1 interface gigabitEthernet

Description

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

Syntax

```
interface gigabitEthernet port
```

Parameter

port—— The Ethernet port number.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

To enter the Interface gigabitEthernet Configuration Mode and configure port 1/0/2:

```
T1500-28PCT(config)#interface fastEthernet 1/0/2
```

16.2 interface range fastEthernet | gigabitEthernet

Description

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

Syntax

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

```
T1500-28PCT(config)# interface range fastEthernet 1/0/1-3,1/0/6-7,1/0/9
```

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

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)#interface fastEthernet 1/0/5
```

```
T1500-28PCT(config-if)# description Port_5
```

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

Privilege Requirement

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

Example

Disable port 1/0/3:

```
T1500-28PCT(config)#interface fastEthernet 1/0/3  
T1500-28PCT(config-if)# shutdown
```

16.5 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 fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)#interface fastEthernet 1/0/3
T1500-28PCT(config-if)# flow-control
```

16.6 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 fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)#interface fastEthernet 1/0/3
T1500-28PCT(config-if)# duplex full
```

16.7 jumbo-size

Description

The **jumbo-size** command is used to configure the size of the jumbo frame which is allowed to pass through the switch.

Syntax

jumbo-size *size*

Parameter

size — Specify the global jumbo frame size, ranging from 1518 to 9216 bytes. By default it's 1518 bytes.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the size of the jumbo frame which is allowed to pass through the switch as 1600 bytes:

```
T1500-28PCT(config)# jumbo-size 1600
```

16.8 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 fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)#interface fastEthernet 1/0/3
T1500-28PCT(config-if)# speed 100
```

16.9 storm-control

Description

The **storm-control** command is used to enable the broadcast, multicast, or unicast storm control function and to set threshold levels on an interface. To disable the storm control function, please use **no storm-control** command.

Syntax

```
storm-control { broadcast | multicast | unicast } { kbps | ratio } { rate }
no storm-control { broadcast | multicast | unicast }
```

Parameter

broadcast | multicast | unicast — Enable broadcast/multicast/unicast storm control on the interface.

kbps | ratio — Specify the storm control type.

kbps: Specify the threshold in kbits per second.

ratio: Specify the threshold as a percentage of the bandwidth.

rate — Specify the bandwidth for receiving packets on the port. The specified type of packet traffic exceeding the bandwidth will be discarded.

For kbps, the rate ranges from 1 to 1000000 kbps. For ratio, the rate ranges from 1 to 100 percent.

Command Mode

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

Privilege Requirement

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

Example

Configure the broadcast storm control rate as 1000 kbps on port 1/0/5:

```
T1500-28PCT(config)#interface fastEthernet 1/0/5
T1500-28PCT(config-if)# storm-control broadcast kbps 1000
```

16.10 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 fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

Configure the ingress-rate as 5120Kbps and egress-rate as 1024Kbps for port 1/0/5:

```
T1500-28PCT(config)#interface fastEthernet 1/0/5
T1500-28PCT(config-if)# bandwidth ingress 5120 egress 1024
```


16.11 clear counters

Description

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

Syntax

clear counters

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

Parameter

port—— The Ethernet port number.

lagid—— The ID of the LAG.

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 LAGs:

```
T1500-28PCT(config)# clear counters
```

16.12 show interface status

Description

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

Syntax

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

Parameter

port—— The Ethernet port number.

lagid—— The ID of the LAG..

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the connection status of all ports and LAGs:

```
T1500-28PCT(config)# show interface status
```

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

```
T1500-28PCT(config)# show interface status fastEthernet 1/0/1
```

16.13 show interface counters

Description

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

Syntax

```
show interface counters [ gigabitEthernet port] [ port-channel lagid]
```

Parameter

port—— The Ethernet port number.

lagid—— The ID of the LAG.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the statistics information of all Ethernet ports and LAGs:

```
T1500-28PCT(config)# show interface counters
```

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

```
T1500-28PCT(config)# show interface counters fastEthernet 1/0/2
```

16.14 show interface configuration

Description

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

Syntax

```
show interface configuration [ gigabitEthernet port] [ port-channel lagid]
```

Parameter

port—— The Ethernet port number.

lagid—— The ID of the LAG.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configurations of all Ethernet ports and LAGs:

```
T1500-28PCT(config)# show interface configuration
```

Display the configurations of port 1/0/2:

```
T1500-28PCT(config)# show interface configuration fastEthernet 1/0/2
```

16.15 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-list | gigabitEthernet port-list] [port-channel lagid-list]
```

Parameter

port-list——The list of Ethernet ports.

lagid-list—— The list of LAGs.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the storm-control information of port 1/0/4-7:

```
T1500-28PCT(config)# show storm-control interface fastEthernet 1/0/4-7
```

16.16 show bandwidth

Description

The **show bandwidth** command is used to display the bandwidth-limit information of Ethernet ports.

Syntax

```
show bandwidth interface [ fastEthernet port-list | gigabitEthernet port-list ]  
[ port-channel lagid-list ]
```

Parameter

port-list——The list of Ethernet ports.

lagid-list—— The list of LAGs.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the bandwidth-limit information of port 1/0/4:

```
T1500-28PCT(config)# show bandwidth interface fastEthernet 1/0/4
```

Chapter 17 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.

17.1 qos

Description

The **qos** command is used to configure the priority level of packets from the port. To return to the default configuration, please use **no qos** command.

Syntax

qos *pri*

no qos

Parameter

pri — The priority level of port. The port priorities are labeled as TC0,TC1,TC2 and TC3. By default, the priority is TC0.

Command Mode

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

Privilege Requirement

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

Example

Configure the priority of port 1/0/5 as TC3:

```
T1500-28PCT(config)#interface fastEthernet 1/0/5
T1500-28PCT(config-if)# qos 3
```

17.2 qos cos

Description

The **qos cos** command is used to enable the mapping relation between IEEE802.1P Priority and TC egress queue. To disable the mapping relation, please use **no qos cos** command.

Syntax

qos cos

no qos cos

Command Mode

Global Configuration Mode

Privilege Requirement

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

User Guidelines

IEEE 802.1P gives the Pri field in IEEE 802.1Q tag a recommended definition. When the mapping relation between IEEE 802.1P Priority and TC egress queue is enabled, the data will be classified into the egress queue based on this mapping relation.

Example

Enable the mapping relation between IEEE 802.1P Priority and egress queue:

```
T1500-28PCT (config)# qos cos
```

17.3 qos dscp

Description

The **qos dscp** command is used to enable the mapping relation between DSCP Priority and CoS value. To disable the mapping relation, please use **no qos dscp** command.

Syntax

qos dscp

no qos dscp

Command Mode

Global Configuration Mode

Privilege Requirement

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

User Guidelines

DSCP (DiffServ Code Point) is a new definition to IP ToS field given by IEEE. DSCP priorities are mapped to the corresponding 802.1p priorities. IP

datagram will be classified into the egress queue based on the mapping relation between DSCP priority and CoS value.

Example

Enable the mapping relation between DSCP Priority and CoS value:

```
T1500-28PCT(config)# qos dscp
```

17.4 qos queue cos-map

Description

The **qos queue cos-map** command is used to configure the mapping relation between IEEE 802.1P priority tag/IEEE 802.1Q tag, CoS value and the TC egress queue. To return to the default configuration, please use **no qos queue cos-map** command. When 802.1P Priority is enabled, the packets with 802.1Q tag are mapped to different priority levels based on 802.1P priority mode. The untagged packets are mapped based on port priority mode.

Syntax

```
qos queue cos-map { tag/cos-id } { tc-id }
```

```
no qos queue cos-map
```

Parameter

tag/cos-id — The 8 priority levels defined by IEEE 802.1P or the priority level the packets with tag are mapped to, which ranges from CoS 0 to CoS 7.

tc-id — The egress queue the packets with tag are mapped to. It ranges from 0 to 3, which represents TC0 to TC3 respectively.

Command Mode

Global Configuration Mode

Privilege Requirement

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

User Guidelines

1. By default, the mapping relation between tag/cos and the egress queue is:
0/CoS 0-TC1, 1/CoS 1-TC0, 2/CoS 2-TC0, 3/CoS 3-TC1, 4/CoS 4-TC2, 5/CoS 5-TC2, 6/CoS 6-TC3, 7/CoS 7-TC3
2. Among the priority levels TC0-TC3, the bigger value, the higher priority.

Example

Map CoS 5 to TC 2:

```
T1500-28PCT(config)# qos queue cos-map 5 2
```

17.5 qos queue dscp-map

Description

The **qos queue dscp-map** command is used to configure the mapping relation between DSCP Priority and the TC queue. To return to the default configuration, please use **no qos queue dscp-map** command. DSCP (DiffServ Code Point) is a new definition to IP ToS field given by IEEE. This field is used to divide IP datagram into 64 priorities. When DSCP Priority is enabled, IP datagram are mapped to different priority levels based on DSCP priority mode; non-IP datagram with IEEE 802.1Q tag are mapped to different priority levels based on IEEE 802.1P priority mode if IEEE 802.1P Priority is enabled; the untagged non-IP datagram are mapped based on port priority mode.

Syntax

```
qos queue dscp-map { dscp-list } { tc-id }
```

```
no qos queue dscp-map
```

Parameter

dscp-list — List of DSCP value. One or several DSCP values can be typed using comma to separate. Use a hyphen to designate a range of values, for instance, 1,4-7,11 indicates choosing 1,4,5,6,7,11. The DSCP value ranges from 0 to 63.

tc-id — The TC queue ID, which ranges from 0 to 3.

Command Mode

Global Configuration Mode

Privilege Requirement

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

User Guidelines

By default, the mapping relation between DSCP value and the egress queue is: (0-15)-TC 0, (16-31)-TC 1, (32-47)-TC 2, (48-63)-TC 3.

Example

Map DSCP values 10-12 to TC 2:

17.6 qos queue mode

Description

The **qos queue mode** command is used to configure the Schedule Mode. To return to the default Equal-Mode, please use **no qos queue mode** command. When the network is congested, the program that many packets complete for resources must be solved, usually in the way of queue scheduling. The switch will control the forwarding sequence of the packets according to the priority queues and scheduling algorithms you set. On this switch, the priority levels are labeled as TC0, TC1... TC3.

Syntax

```
qos queue mode { sp | wrr | spwrr | equ }
```

```
no qos queue mode
```

Parameter

sp — Strict-Priority Mode. In this mode, the queue with higher priority will occupy the whole bandwidth. Packets in the queue with lower priority are sent only when the queue with higher priority is empty.

wrr —Weight Round Robin Mode. In this mode, packets in all the queues are sent in order based on the weight value for each queue. The weight value ratio of TC0, TC1, TC2 and TC3 is 1:2:4:8.

spwrr —Strict-Priority + Weight Round Robin Mode. In this mode, the switch provides two scheduling groups, SP group and WRR group. Queues in SP group and WRR group are scheduled strictly based on Strict-Priority mode while the queues inside WRR group follow the WRR mode. In SP + WRR mode, TC3 is the SP group; TC0, TC1 and TC2 belong to the WRR group and the weight value ratio of TC0, TC1 and TC2 is 1:2:4. In this way, when scheduling queues, the switch allows TC3 to occupy the whole bandwidth following the SP mode and the TC0, TC1 and TC2 in the WRR group will take up the bandwidth according to their ratio 1:2:4.

equ — Equal-Mode. In this mode, all the queues occupy the bandwidth equally. The weight value ratio of all the queues is 1:1:1:1.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the Schedule Mode as Weight Round Robin Mode:

```
T1500-28PCT(config)# qos queue mode wrr
```

17.7 show qos interface

Description

The **show qos interface** command is used to display the configuration of QoS based on port priority.

Syntax

```
show qos interface [ fastEthernet port-list | fastEthernet port-list | gigabitEthernet port-list] [port-channel lagid-list]
```

Parameter

port-list——The list of Ethernet ports.

lagid-list—— The list of LAGs.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of QoS for all ports and LAGs:

```
T1500-28PCT# show qos interface
```

Display the configuration of QoS for ports 1/0/1-4:

```
T1500-28PCT# show qos interface fastEthernet 1/0/1-4
```

17.8 show qos cos-map

Description

The **show qos cos-map** command is used to display the configuration of IEEE 802.1P Priority and the mapping relation between cos-id and tc-id.

Syntax

```
show qos cos-map
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of IEEE 802.1P Priority and the mapping relation between cos-id and tc-id:

```
T1500-28PCT# show qos cos-map
```

17.9 show qos dscp-map

Description

The **show qos dscp-map** command is used to display the configuration of DSCP Priority.

Syntax

```
show qos dscp-map
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of DSCP Priority:

```
T1500-28PCT# show qos dscp-map
```

17.10 show qos queue mode

Description

The **show qos queue mode** command is used to display the schedule rule of the egress queues.

Syntax

```
show qos queue mode
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the schedule rule of the egress queues:

```
T1500-28PCT# show qos queue mode
```

17.11 show qos status

Description

The **show qos status** command is used to display the status of IEEE 802.1P priority and DSCP priority.

Syntax

```
show qos status
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the status of IEEE 802.1P priority and DSCP priority:

```
T1500-28PCT# show qos status
```

Chapter 18 Port Mirror Commands

Port Mirror refers to the process of forwarding copies of packets from one or multiple ports to a monitoring port. Usually, the monitoring port is connected to data diagnose device, which is used to analyze the monitored packets for monitoring and troubleshooting the network.

18.1 monitor session destination interface

Description

The **monitor session destination interface** command is used to configure the monitoring port. Each monitor session has only one monitoring port. To change the monitoring port, please use the **monitor session destination interface** command by changing the port value. The **no monitor session** command is used to delete the corresponding monitoring port or monitor session.

Syntax

```
monitor session session_num destination interface gigabitEthernet port  
no monitor session session_num destination interface gigabitEthernet port  
no monitor session session_num
```

Parameter

session_num — The monitor session number, can only be specified as 1.
port — The monitoring port number.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create monitor session 1 and configure port 1/0/1 as the monitoring port:

```
T1500-28PCT(config)# monitor session 1 destination interface  
fastEthernet 1/0/1
```

Delete the monitoring port 1/0/2 from monitor session 1:

```
T1500-28PCT(config)# no monitor session 1 destination interface
fastEthernet 1/0/2
```

Delete the monitor session 1:

```
T1500-28PCT(config)# no monitor session 1
```

18.2 monitor session source interface

Description

The **monitor session source interface** command is used to configure the monitored port/ LAG. To delete the corresponding monitored port, please use **no monitor session source interface** command.

Syntax

```
monitor session session_num source interface { fastEthernet port-list |
gigabitEthernet port-list / port-channel lagid-list } mode
no monitor session session_num source interface { fastEthernet port-list |
gigabitEthernet port-list / port-channel lagid-list } mode
```

Parameter

session_num—— The monitor session number, can only be specified as 1.

port-list—— The list of monitored port. It is multi-optional.

lagid-list——The list of monitored LAG.

mode —— The monitor mode. There are three options: rx, tx and both. Rx (ingress monitoring mode), means the incoming packets received by the monitored port will be copied to the monitoring port. Tx (egress monitoring mode), indicates the outgoing packets sent by the monitored port will be copied to the monitoring port. Both (ingress and egress monitoring), presents the incoming packets received and the outgoing packets sent by the monitored port will both be copied to the monitoring port.

Command Mode

Global Configuration Mode

Privilege Requirement

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

User Guidelines

1. The monitoring port is corresponding to current interface configuration mode.

2. Monitored ports number is not limited, but it can't be the monitoring port at the same time.
3. Whether the monitoring port and monitored ports are in the same VLAN or not is not demanded strictly.
4. The monitoring port cannot be link-aggregation member.

Example

Create monitor session 1, then configure port 4, 5, 7 as monitored port and enable ingress monitoring:

```
T1500-28PCT(config)# monitor session 1 source interface fastEthernet  
1/0/4-5,1/0/7 rx
```

Delete port 4 in monitor session 1 and its configuration:

```
T1500-28PCT(config)# no monitor session 1 source interface  
fastEthernet 1/0/4 rx
```

18.3 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:

```
T1500-28PCT(config)# show monitor session 1
```

Chapter 19 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.

19.1 port isolation

Description

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

Syntax

```
port isolation { [ gi-forward-list gi-forward-list ] [ po-forward-list  
po-forward-list] }
```

```
no port isolation
```

Parameter

gi-forward-list — The list of Ethernet ports.

po-forward-list — The list of LAGs.

Command Mode

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

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)#interface fastEthernet 1/0/5  
T1500-28PCT(config-if)# port isolation gi-forward-list 1/0/1-2,1/0/4  
po-forward-list 2
```

Set all Ethernet ports and LAGs to forward list of port 1/0/2, namely restore to the default setting:

```
T1500-28PCT(config)#interface fastEthernet 1/0/2
```


19.2 show port isolation interface

Description

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

Syntax

```
show port isolation interface [ gigabitEthernet port | port-channel lagid ]
```

Parameter

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

lagid — The ID of LAG 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:

```
T1500-28PCT# show port isolation interface fastEthernet 1/0/2
```

Display the forward-list of all Ethernet ports and LAGs:

```
T1500-28PCT# show port isolation interface
```

Chapter 20 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.

20.1 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:

```
T1500-28PCT(config)# loopback-detection
```

20.2 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:

```
T1500-28PCT(config)# loopback-detection interval 50
```

20.3 loopback-detection recovery-time

Description

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

Syntax

```
loopback-detection recovery-time recovery-time
```

Parameter

recovery-time — The time after which the blocked port would automatically recover to normal status, and the loopback detection would restart. It is integral times of detection interval, ranging from 1 to 100 and the default value is 3.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the recovery-time as 3 times of detection interval:

```
T1500-28PCT(config)# loopback-detection recovery-time 3
```

20.4 loopback-detection(interface)

Description

The **loopback-detection** command is used to enable the loopback detection function of the specified port/LAG. To disable it, please use **no loopback-detection** command.

Syntax

loopback-detection
no loopback-detection

Command Mode

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

Privilege Requirement

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

Example

Enable the loopback detection function of ports 1/0/1-3:

```
T1500-28PCT(config)# interface range fastEthernet 1/0/1-3
T1500-28PCT(Config-if-range)# loopback-detection
```

20.5 loopback-detection config

Description

The **loopback-detection config** command is used to configure the process-mode and recovery-mode for the ports/LAGs by which the switch copes with the detected loops.

Syntax

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

Parameter

process-mode — The mode how the switch processes the detected loops.

Alert: When a loop is detected, display an alert.

Port based: When a loop is detected, display an alert and block the port.

recovery-mode — The mode how the blocked port recovers to normal status. **Auto:** Block status can be automatically removed after recovery time.

Manual: Block status can only be removed manually.

Command Mode

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

Privilege Requirement

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

Example

Configure the loopback detection process-mode as port-based and recovery-mode as manual for port 1/0/2:

```
T1500-28PCT(config)#interface fastEthernet 1/0/2
T1500-28PCT(config-if)# loopback-detection config process-mode
port-based recovery-mode manual
```

20.6 loopback-detection recover

Description

The **loopback-detection recover** command is used to remove the block status of selected ports/LAGs, recovering the blocked ports to normal status,

Syntax

loopback-detection recover

Command Mode

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

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)#interface fastEthernet 1/0/2
```

```
T1500-28PCT(config-if)# loopback-detection recover
```

20.7 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:

```
T1500-28PCT# show loopback-detection global
```

20.8 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/LAG.

Syntax

```
show loopback-detection interface [gigabitEthernet port | port-channel  
lagid]
```

Parameter

port—— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

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

```
T1500-28PCT# show loopback-detection interface
```

Display the configuration of loopback detection function and the status of port 1/0/5:

```
T1500-28PCT# show loopback-detection interface fastEthernet 1/0/5
```

Chapter 21 ACL Commands

21.1 access-list create

Description

The **access-list create** command is used to create standard-IP ACL and extend-IP ACL.

Syntax

access-list create *access-list-num*

Parameter

access-list-num — ACL ID, ranging from 500 to 2499. The ID range of Standard-IP ACL ranges is 500-1499 and the Extend-IP ACL is 1500-2499.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create a standard-IP ACL whose ID is 523:

```
T1500-28PCT(config)# access-list create 523
```

21.2 mac access-list

Description

The **mac access-list** command is used to create MAC ACL. To set the detailed configurations for a specified MAC ACL, please use **mac access-list** command to access Mac Access-list Configuration Mode. To delete the MAC ACL, please use **no mac access-list**.

Syntax

mac access-list *access-list-num*

no mac access-list *access-list-num*

Parameter

access-list-num — ACL ID, ranging from 0 to 499.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create a MAC ACL whose ID is 23:

```
T1500-28PCT(config)# mac access-list 23
```

21.3 access-list standard

Description

The **access-list standard** command is used to add Standard-IP ACL rule. To delete the corresponding rule, please use **no access-list standard** command. Standard-IP ACLs analyze and process data packets based on a series of match conditions, which can be the source IP addresses and destination IP addresses carried in the packets.

Syntax

```
access-list standard acl-id rule rule-id { deny / permit } [[ sip source-ip ]  
smask source-ip-mask] [[ dip destination-ip ] dmask destination-ip-mask ]  
no access-list standard acl-id rule rule-id
```

Parameter

acl-id—— The desired Standard-IP ACL for configuration.

rule-id—— The rule ID.

deny —— The operation to discard packets.

permit ——The operation to forward packets. It is the default value.

source-ip—— The source IP address contained in the rule.

source-ip-mask —— The source IP address mask. It is required if you typed the source IP address.

destination-ip—— The destination IP address contained in the rule.

destination-ip-mask —— The destination IP address mask. It is required if you typed the destination IP address.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create a Standard-IP ACL whose ID is 520, and add Rule 10 for it. In the rule, the source IP address is 192.168.0.100, the source IP address mask is 255.255.255.0, and the packets match this rule will be forwarded by the switch:

```
T1500-28PCT(config)# access-list create 520
T1500-28PCT(config)# access-list standard 520 rule 10 permit sip
192.168.0.100 smask 255.255.255.0
```

21.4 access-list extended

Description

The **access-list extended** command is used to add Extended-IP ACL rule. To delete the corresponding rule, please use **no access-list extended** command.

Syntax

```
access-list extended acl-id rule rule-id { deny / permit } [[ sip source-ip ]
smask source-ip-mask ] [[ dip destination-ip] dmask destination-ip-mask ]
[ s-port s-port] [ d-port d-port] [ protocol protocol]
no access-list extended acl-id rule rule-id
```

Parameter

acl-id—The desired Extended-IP ACL for configuration.

rule-id— The rule ID.

deny — The operation to discard packets.

permit —The operation to forward packets. It is the default value.

source-ip— The source IP address contained in the rule.

source-ip-mask — The source IP address mask. It is required if you typed the source IP address.

destination-ip— The destination IP address contained in the rule.

destination-ip-mask — The destination IP address mask. It is required if you typed the destination IP address.

s-port— The source port number.

d-port—— The destination port number.

protocol—— Configure the value of the matching protocol.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create an Extended-IP ACL whose ID is 2220, and add Rule 10 for it. In the rule, the source IP address is 192.168.0.100, the source IP address mask is 255.255.255.0, and the packets match this rule will be forwarded by the switch:

```
T1500-28PCT(config)# access-list create 2220
T1500-28PCT(config)# access-list extended 2220 rule 10 permit sip
192.168.0.100 smask 255.255.255.0
```

21.5 rule

Description

The **rule** command is used to configure MAC ACL rule. To delete the corresponding rule, please use **no rule** command.

Syntax

```
rule rule-id { deny | permit } [[ smac source-mac ] smask source-mac-mask ]
[[ dmac destination-mac ] dmask destination-mac-mask ]
```

```
no rule rule-id
```

Parameter

rule-id—— The rule ID.

deny —— The operation to discard packets.

permit ——The operation to forward packets. It is the default value.

source-mac—— The source MAC address contained in the rule.

source-mac-mask —— The source MAC address mask. It is required if you typed the source MAC address.

destination-mac—— The destination MAC address contained in the rule.

destination-mac-mask —— The destination MAC address mask. It is required if you typed the destination MAC address.

Command Mode

Mac Access-list Configuration Mode

Privilege Requirement

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

Example

Create a MAC ACL whose ID is 20, and add Rule 10 for it. In the rule, the source MAC address is 00:01:3F:48:16:23, the source MAC address mask is 11:11:11:11:11:00, and the packets match this rule will be forwarded by the switch:

```
T1500-28PCT(config)# mac access-list 20
T1500-28PCT(config-mac-acl)# rule 10 permit smac 00:01:3F:48:16:23
smask 11:11:11:11:11:00
```

21.6 access-list policy name

Description

The **access-list policy name** command is used to add Policy. To delete the corresponding Policy, please use **no access-list policy name** command. A Policy is used to control the data packets those match the corresponding ACL rules.

Syntax

```
access-list policy name name
no access-list policy name name
```

Parameter

name — The Policy Name, ranging from 1 to 16 characters.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Add a Policy named policy1:

```
T1500-28PCT(config)# access-list policy name policy1
```

21.7 access-list policy action

Description

The **access-list policy action** command is used to add ACLs for the policy. To delete the corresponding actions, please use **no access-list policy action** command.

Syntax

access-list policy action *policy-name acl-id*

no access-list policy action *policy-name acl-id*

Parameter

policy-name—— The Policy Name, ranging from 1 to 16 characters.

acl-id—— The ID of the ACL to which the above policy is applied.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Add ACL whose ID is 120 for policy1:

```
T1500-28PCT(config)# access-list policy action policy1 120
```

21.8 access-list bind acl(interface)

Description

The **access-list bind acl** command is used to bind an ACL to the specified port. To cancel the bind relation, please use **no access-list bind acl** command.

Syntax

access-list bind acl *acl-id*

no access-list bind acl *acl-id*

Parameter

acl-id—— The ID of the ACL desired to bind.

Command Mode

Interface Configuration Mode (interface fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Bind ACL 100 to port 1/0/2:

```
T1500-28PCT(config)#interface fastEthernet 1/0/2
T1500-28PCT(config-if)# access-list bind acl 100
```

21.9 access-list bind acl(vlan)

Description

The **access-list bind acl** command is used to bind an ACL to the specified VLAN. To cancel the bind relation, please use **no access-list bind acl** command.

Syntax

```
access-list bind acl acl-id
no access-list bind acl acl-id
```

Parameter

acl-id—— The ID of the ACL desired to bind.

Command Mode

Interface VLAN Mode

Privilege Requirement

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

Example

Bind ACL 100 to VLAN 2:

```
T1500-28PCT(config)# interface vlan 2
T1500-28PCT(config-if)# access-list bind acl 100
```

21.10 access-list bind(interface)

Description

The **access-list bind** command is used to bind a policy to a specified port. To cancel the bind relation, please use **no access-list bind** command.

Syntax

access-list bind *policy-name*

no access-list bind *policy-name*

Parameter

policy-name—— The name of the policy desired to bind.

Command Mode

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

Privilege Requirement

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

Example

Bind policy1 to port 1/0/2:

```
T1500-28PCT(config)#interface fastEthernet 1/0/2
```

```
T1500-28PCT(config-if)# access-list bind policy1
```

21.11 access-list bind(vlan)

Description

The **access-list bind** command is used to bind a policy to a VLAN. To cancel the bind relation, please use **no access-list bind** command.

Syntax

access-list bind *policy-name*

no access-list bind *policy-name*

Parameter

policy-name—— The name of the policy desired to bind.

Command Mode

Interface VLAN Mode

Privilege Requirement

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

Example

Bind policy1 to VLAN 2:

```
T1500-28PCT(config)# interface vlan 2
T1500-28PCT(config-if)# access-list bind policy1
```

21.12 show access-list

Description

The **show access-list** command is used to display configuration of ACL.

Syntax

```
show access-list acl-id
```

Parameter

acl-id—— The ID of the ACL selected to display the configuration.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of the MAC ACL whose ID is 20:

```
T1500-28PCT(config)# show access-list 20
```

21.13 show access-list policy

Description

The **show access-list policy** command is used to display the information of a specified policy.

Syntax

```
show access-list policy name
```

Parameter

name—— The Policy Name desired to show.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of a policy named policy1:


```
T1500-28PCT(config)# show access-list policy policy1
```

21.14 show access-list bind

Description

The **show access-list bind** command is used to display the configuration of Policy bind.

Syntax

```
show access-list bind
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of Policy bind:

```
T1500-28PCT(config)# show access-list bind
```

Chapter 22 PoE Commands



Note:

Only T1500-28PCT supports PoE function.

PoE (Power over Ethernet) technology describes a system to transmit electrical power along with data to remote devices over standard twisted-pair cable in an Ethernet network. It is especially useful for supplying power to IP telephones, wireless LAN access points, cameras and so on.

A time-range based PoE enables you to implement PoE power supply by differentiating the time-ranges.

22.1 power inline consumption (global)

Description

The **power inline consumption** command is used to configure the max power the PoE switch can supply globally.

Syntax

power inline consumption *power-limit*

Parameter

power-limit —The max power the PoE switch can supply. It ranges from 1 to 192W.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the max power the PoE switch can supply as 100W:

```
T1500-28PCT(config)# power inline consumption 100
```

22.2 power profile

Description

The **power profile** command is used to create a PoE profile for the switch. To delete the configured PoE profile configuration, please use **no power profile** command. PoE Profile is a short cut for the configuration of the PoE port. In a PoE profile, the PoE status, PoE priority and power limit are configured. You can specify a PoE profile for each PoE port individually.

Syntax

```
power profile name [ supply { enable | disable } [ priority { low | middle | high }  
[ consumption { power-limit | auto | class1 | class2 | class3 | class4 } ] ] ]  
no power profile name
```

Parameter

name — The PoE profile name, ranging from 1 to 16 characters. If the name being assigned contains spaces then put it inside double quotes.

supply — The PoE status of the port in the profile. By default, the PoE status is "enable".

priority — The PoE priority of the port in the profile. The priority levels include "high", "middle" and "low" in descending order. When the supply power exceeds the system power limit, the PD linked to the port with lower priority will be disconnected. By default, the PoE priority is "low".

consumption — The max power the port in the profile can supply. There are six options: "power-limit", "auto", "class1", "class2", "class3" and "class4". "power-limit" indicates you can manually enter a value. It ranges from 1 to 300. The value is in the unit of 0.1 watt. For instance, if you want to configure the max power as 5w, you should enter 50. "auto" indicates the value is assigned automatically by the PoE switch. "class1" represents 4w. "class2" represents 7w. "class3" represents 15.4w. "class4" represents 30w.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create a PoE profile named "IP Camera" whose PoE status is "enable", PoE priority is "low" and the power limit is "5w":

```
T1500-28PCT(config)# power profile "IP Camera" supply enable priority
low consumption 50
```

22.3 power time-range

Description

The **power time-range** command is used to create PoE time-range for the switch and enter Power Time-range Configuration Mode. After a PoE time-range is created, you need to specify the date and time which has three mode options: absolute, periodic and holiday. A PoE time-range is the intersection of absolute time-range and periodic time-range with holiday included or excluded. To delete the corresponding PoE time-range configuration, please use **no power time-range** command. The PoE time-range determines the power supply time of the switch. You can specify a PoE time-range for each PoE port individually.

Syntax

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

Parameter

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)# power time-range tRange1
```

22.4 absolute

Description

The **absolute** command is used to create an absolute mode time-range for the Time-range of the switch. The Time-range takes affect only when both Absolute Time and Periodic Time are in effect.

Repeat this command to create multiple absolute time-ranges. Up to 7 absolute time-ranges can be created in one Time-range, and their union is the Absolute Time-range.

If no absolute time range is configured, the absolute time range takes effect from January 1, 2000 00:00 to December 31, 2099 24:00.

To delete the corresponding absolute time-range, please use **no absolute** command.

Syntax

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

no absolute [*index*]

Parameter

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

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

index — Specify the index of the absolute time-range to delete. If not specified, all absolute time-ranges will be deleted.

Command Mode

Power Time-range Configuration Mode

Privilege Requirement

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

Example

Create an absolute mode time-range for the PoE of the switch and specify the date extending from 08:00 on May 5th, 2012 to 22:00 on Oct. 5th, 2012:

```
T1500-28PCT(config)# power time-range tRange1
T1500-28PCT(config-time-range)# absolute from 05/05/2012-08:00 to
10/05/2012-22:00
```

22.5 periodic

Description

The **periodic** command is used to create a periodic mode time-range for the PoE time-range of the switch. The periodic time-range recurs every week.

The Time-range takes effect only when both Absolute Time and Periodic Time are in effect.

Repeat this command to create multiple periodic time-ranges. Up to 7 periodic time-ranges can be created in one Time-range, and their union is the Periodic Time-range.

If no periodic time range is configured, the periodic time range takes effect all the time from Monday to Sunday.

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** *day-of-the-week*

no periodic [*index*]

Parameter

start-date — The start time in the day in periodic mode, in the format of HH:MM.

end-date — The end time in the day in periodic mode, in the format of HH:MM.

day-of-the-week — Specify the days included in a week, ranging from 1-7, in the format as 1,3-4.

index — Specify the index of the periodic time-range to delete. If not specified, all periodic time-ranges will be deleted.

Command Mode

Power Time-range Configuration Mode

Privilege Requirement

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

Example

Configure the Time-range named "tRange2" with two periodic time-ranges: one is from 08:00 to 18:00 during Monday to Friday, the other is from 10:00 to 16:00 during the weekends:

```
T1500-28PCT(config)# power time-range tRange2
```

```
T1500-28PCT(config-time-range)# periodic start 08:00 end 18:00
```

```
day-of-the-week 1-5
```

```
T1500-28PCT(config-time-range)# periodic start 10:00 end 16:00
day-of-the-week 6-7
```

22.6 power holiday

Description

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

Syntax

```
power holiday name start-date start-date end-date end-date
no power holiday name
```

Parameter

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

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

end-date — The end date of the PoE holiday, in the format of MM/DD, for instance, 05/03.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)# power holiday LaborDay start-date 05/01 end-date
05/03
```

22.7 holiday

Description

The **holiday** command is used to configure holiday mode for the Time-range of the switch. The holiday will be excluded from the Time-range you created if the Holiday mode is Exclude.

Syntax

holiday { exclude | include }

Parameter

exclude — The final Time range will be the intersection of the Absolute Time and the Periodic Time, with Holiday excluded.

include — The Holiday has no effect on the Time-range, which means the final Time-range will be the intersection of the Absolute Time and Periodic Time.

Command Mode

Power Time-range Configuration Mode

Privilege Requirement

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

Example

Create a holiday mode time-range for the PoE time-range named "tRange3" and configure PoE time-range of the switch excludes the PoE holiday:

```
T1500-28PCT(config)# power time-range tRange3
T1500-28PCT(config-time-range)# holiday exclude
```

22.8 power inline consumption (interface)

Description

The **power inline consumption** command is used to configure the power limit the corresponding port can supply.

Syntax

power inline consumption { *power-limit* | auto | class1 | class2 | class3 | class4 }

Parameter

consumption — The max power the port in the profile can supply. There are six options: "power-limit", "auto", "class1", "class2", "class3" and "class4". "power-limit" indicates you can manually enter a value. It ranges from 1 to 300. The value is in the unit of 0.1 watt. For instance, if you want to configure the max power as 5w, you should enter 50. "auto" indicates the value is assigned automatically by the PoE switch. "class1" represents 4w. "class2" represents 7w. "class3" represents 15.4w. "class4" represents 30w.

Command Mode

Interface Configuration Mode (interface fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure the power limit as "5w" for port 1/0/2:

```
T1500-28PCT(config)#interface fastEthernet 1/0/2
T1500-28PCT(config-if)# power inline consumption 50
```

22.9 power inline priority

Description

The **power inline priority** command is used to configure the PoE priority for the corresponding port

Syntax

```
power inline priority { low | middle | high }
```

Parameter

priority —The PoE priority of the port. The priority levels include "high", "middle" and "low" in descending order. When the supply power exceeds the system power limit, the PD linked to the port with lower priority will be disconnected. By default, the priority level is "low".

Command Mode

Interface Configuration Mode (interface fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure the PoE priority as "low" for port 1/0/2:

```
T1500-28PCT(config)#interface fastEthernet 1/0/2
T1500-28PCT(config-if)# power inline priority low
```

22.10 power inline supply

Description

The **power inline supply** command is used to configure the PoE status of the corresponding port.

Syntax

```
power inline supply { enable | disable }
```

Parameter

enable | disable — The PoE status of the port. By default, the PoE status is "enable".

Command Mode

Interface Configuration Mode (interface fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the PoE feature for port 1/0/2:

```
T1500-28PCT(config)#interface fastEthernet 1/0/2
T1500-28PCT(config-if)# power inline supply enable
```

22.11 power inline profile

Description

The **power inline profile** command is used to bind a PoE profile to the corresponding port. To cancel the bind relation, please use **no power inline profile** command.

Syntax

```
power inline profile name
no power inline profile
```

Parameter

name — The name of the PoE profile to be bound to the port. If the name being assigned contains spaces then put it inside double quotes.

Command Mode

Interface Configuration Mode (interface fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Bind the PoE profile named "IP Camera" to port 1/0/2:

```
T1500-28PCT(config)#interface fastEthernet 1/0/2
T1500-28PCT(config-if)# power inline profile "IP Camera"
```

22.12 power inline time-range

Description

The **power inline time-range** command is used to bind a PoE time-range to the corresponding port. To cancel the bind relation, please use **no power inline time-range** command.

Syntax

```
power inline time-range name
no power inline time-range
```

Parameter

name — The name of the PoE time-range to be bound to the port.

Command Mode

Interface Configuration Mode

Privilege Requirement

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

Example

Bind the PoE time-range named "tRange2" to port 1/0/2:

```
T1500-28PCT(config)#interface fastEthernet 1/0/2
T1500-28PCT(config-if)# power inline time-range tRange2
```

22.13 show power inline

Description

The **show power inline** command is used to display the global PoE information of the system.

Syntax

```
show power inline
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the PoE information of the system:

```
T1500-28PCT# show power inline
```

22.14 show power inline configuration interface

Description

The **show power inline configuration interface** command is used to display the PoE configuration of the certain port.

Syntax

```
show power inline configuration interface [ gigabitEthernet port ]
```

Parameter

port—— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the PoE configuration of all ports:

```
T1500-28PCT# show power inline configuration interface
```

22.15 show power inline information interface

Description

The **show power inline information** command is used to display the PoE information of the certain port.

Syntax

show power inline information interface [gigabitEthernet port]

Parameter

port—— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the PoE information of all ports:

```
T1500-28PCT# show power inline information interface
```

22.16 show power profile

Description

The **show power profile** command is used to display the defined PoE profile.

Syntax

show power profile

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the defined PoE profile:

```
T1500-28PCT# show power profile
```

22.17 show power holiday

Description

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

Syntax

```
show power holiday
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the defined PoE holiday:

```
T1500-28PCT# show power holiday
```

22.18 show power time-range

Description

The **show power time-range** command is used to display the configuration of PoE time-range.

Syntax

```
show power time-range [ name ]
```

Parameter

name — The PoE time-range name, ranging from 1 to 16 characters. All PoE time-range configurations will be displayed if not specified.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of PoE time-range:

```
T1500-28PCT# show power time-range
```

Chapter 23 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.

23.1 debug spanning-tree

Description

The **debug spanning-tree** command is used to enable debugging of spanning-tree activities. To disable the debugging function, please use **no debug spanning-tree** command.

Syntax

debug spanning-tree { all | bpdu receive | bpdu transmit | cmpmsg | errors | flush | init | migration | proposals | roles | state | tc }

no debug spanning-tree { all | bpdu receive | bpdu transmit | cmpmsg | errors | flush | init | migration | proposals | roles | state | tc }

Parameters

all — Display all the spanning-tree debug messages.

bpdu receive — Display the debug messages of the received spanning-tree bridge protocol data unit (BPDU).

bpdu transmit — Display the debug messages of the sent spanning-tree BPDU.

cmpmsg — Display the message priority debug messages.

errors — Display the MSTP error debug messages.

flush — Display the address table flushing debug messages.

init — Display the data structure initialization debug messages.

migration — Display the version migration debug messages.

proposals — Display the MSTP handshake debug messages.

roles — Display the MSTP interface role switchling debug messages.

state — Display the MSTP interface state change debug messages.

tc — Display the MSTP topology event debug messages.

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display all the spanning-tree debug messages:

```
T1500-28PCT# debug spanning-tree all
```

23.2 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:

```
T1500-28PCT(config)# spanning-tree
```

23.3 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 fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

Enable the STP function for port 1/0/2:

```
T1500-28PCT(config)#interface fastEthernet 1/0/2
```

```
T1500-28PCT(config-if)# spanning-tree
```

23.4 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 0 to 2000000. By default, it is 0 which is mean auto.

int-cost — Internal Path Cost, which is used to choose the path and calculate the path costs of ports in an MST region. It is an important criterion on determining the root port. The lower value has the higher priority. By default, it is automatic. It ranges from 0 to 2000000. By default, it is 0 which means auto.

portfast — Enable/ Disable Edge Port. By default, it is disabled. The edge port can transit its state from blocking to forwarding rapidly without waiting for forward delay.

point-to-point — The P2P link status, with auto, open and close options. By default, the option is auto. If the two ports in the P2P link are root port or designated port, they can transit their states to forwarding rapidly to reduce the unnecessary forward delay.

Command Mode

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

Privilege Requirement

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

Example

Enable the 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:

```
T1500-28PCT(config)#interface fastEthernet 1/0/1
T1500-28PCT(config-if)# spanning-tree common-config port-priority 64
ext-cost 100 int-cost 100 portfast enable point-to-point open
```

23.5 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:

```
T1500-28PCT(config)# spanning-tree mode mstp
```

23.6 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:

```
T1500-28PCT(config)# spanning-tree mst configuration
```

```
T1500-28PCT(config-mst)#
```

23.7 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:

```
T1500-28PCT(config)# spanning-tree mst configuration  
T1500-28PCT(config-mst)# instance 1 vlan 1-100
```

Disable Instance 1, namely remove all the mapping VLANs 1-100:

```
T1500-28PCT(config)# spanning-tree mst configuration  
T1500-28PCT(config-mst)# no instance 1
```

Remove VLANs 1-50 in mapping VLANs 1-100 for Instance 1:

```
T1500-28PCT(config)# spanning-tree mst configuration  
T1500-28PCT(config-mst)# no instance 1 vlan 1-50
```

23.8 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":

```
T1500-28PCT(config)# spanning-tree mst configuration
T1500-28PCT(config-mst)# name region1
```

23.9 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:

```
T1500-28PCT(config)# spanning-tree mst configuration
T1500-28PCT(config-mst)# revision 100
```

23.10 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:

```
T1500-28PCT(config)# spanning-tree mst instance 1 priority 4096
```

23.11 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 fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

Configure the priority of port 1 in MST Instance 1 as 64, and path cost as 2000:

```
T1500-28PCT(config)#interface fastEthernet 1/0/1
T1500-28PCT(config-if)# spanning-tree mst instance 1 port-priority 64
cost 2000
```

23.12 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:

```
T1500-28PCT(config)# spanning-tree priority 4096
```

23.13 spanning-tree timer

Description

The **spanning-tree timer** command is used to configure forward-time, hello-time and max-age of Spanning Tree. To return to the default configurations, please use **no spanning-tree timer** command.

Syntax

```
spanning-tree timer {[ forward-time forward-time ] [ hello-time hello-time ]  
[ max-age max-age ]}
```

```
no spanning-tree timer
```

Parameter

forward-time — Forward Delay, which is the time for the port to transit its state after the network topology is changed. Forward Delay ranges from 4 to 30 in seconds and it is 15 by default. Otherwise, $2 * (\text{Forward Delay} - 1) \geq \text{Max Age}$.

hello-time — Hello Time, which is the interval to send BPDU packets, and used to test the links. Hello Time ranges from 1 to 10 in seconds and it is 2 by default. Otherwise, $2 * (\text{Hello Time} + 1) \leq \text{Max Age}$.

max-age — The maximum time the switch can wait without receiving a BPDU before attempting to reconfigure, ranging from 6 to 40 in seconds. By default, it is 20.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure forward-time, hello-time and max-age for Spanning Tree as 16 seconds, 3 seconds and 22 seconds respectively:


```
T1500-28PCT(config)# spanning-tree timer forward-time 16 hello-time 3
max-age 22
```

23.14 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:

```
T1500-28PCT(config)# spanning-tree hold-count 8
```

23.15 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:

```
T1500-28PCT(config)# spanning-tree max-hops 30
```

23.16 spanning-tree bpdudfilter

Description

The **spanning-tree bpdudfilter** command is used to enable the BPDU filter function for a port. With the function enabled, the port can be prevented from receiving and sending any BPDU packets. To disable the BPDU filter function, please use **no spanning-tree bpdudfilter** command.

Syntax

```
spanning-tree bpdudfilter  
no spanning-tree bpdudfilter
```

Command Mode

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

Privilege Requirement

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

Example

Enable the BPDU filter function for port 1/0/2:

```
T1500-28PCT(config)#interface fastEthernet 1/0/2  
T1500-28PCT(config-if)# spanning-tree bpdudfilter
```

23.17 spanning-tree bpduguard

Description

The **spanning-tree bpduguard** command is used to enable the BPDU protect function for a port. With the BPDU protect function enabled, the port will set itself automatically as ERROR-PORT when it receives BPDU packets, and the port will disable the forwarding function for a while. To disable the BPDU protect function, please use **no spanning-tree bpduguard** command.

Syntax

spanning-tree bpduguard

no spanning-tree bpduguard

Command Mode

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

Privilege Requirement

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

Example

Enable the BPDU protect function for port 1/0/2:

```
T1500-28PCT(config)#interface fastEthernet 1/0/2
```

```
T1500-28PCT(config-if)# spanning-tree bpduguard
```

23.18 spanning-tree guard loop

Description

The **spanning-tree guard loop** command is used to enable the Loop Protect function for a port. Loop Protect is to prevent the loops in the network brought by recalculating STP because of link failures and network congestions. To disable the Loop Protect function, please use **no spanning-tree guard loop** command.

Syntax

spanning-tree guard loop

no spanning-tree guard loop

Command Mode

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

Privilege Requirement

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

Example

Enable the Loop Protect function for port 1/0/2:

```
T1500-28PCT(config)#interface fastEthernet 1/0/2
T1500-28PCT(config-if)# spanning-tree guard loop
```

23.19 spanning-tree guard root

Description

The **spanning-tree guard root** command is used to enable the Root Protect function for a port. With the Root Protect function enabled, the root bridge will set itself automatically as ERROR-PORT when receiving BPDU packets with higher priority, in order to maintain the role of root ridge. To disable the Root Protect function, please use **no spanning-tree guard root** command.

Syntax

```
spanning-tree guard root
no spanning-tree guard root
```

Command Mode

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

Privilege Requirement

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

Example

Enable the Root Protect function for port 1/0/2:

```
T1500-28PCT(config)#interface fastEthernet 1/0/2
T1500-28PCT(config-if)# spanning-tree guard root
```

23.20 spanning-tree guard tc

Description

The **spanning-tree guard tc** command is used to enable the TC Protect of Spanning Tree function for a port. To disable the TC Protect of Spanning Tree function, please use **no spanning-tree guard tc** command. A switch removes MAC address entries upon receiving TC-BPDUs. If a malicious user continuously sends TC-BPDUs to a switch, the switch will be busy with removing MAC address entries, which may decrease the performance and stability of the network. With the Protect of Spanning Tree function enabled, you can configure the number of TC-BPDUs in a required time, so as to avoid the process of removing MAC addresses frequently.

Syntax

spanning-tree guard tc

no spanning-tree guard tc

Command Mode

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

Privilege Requirement

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

Example

Enable the TC Protect of Spanning Tree for port 1/0/2:

```
T1500-28PCT(config)#interface fastEthernet 1/0/2
```

```
T1500-28PCT(config-if)# spanning-tree guard tc
```

23.21 spanning-tree mcheck

Description

The **spanning-tree mcheck** command is used to enable mcheck.

Syntax

spanning-tree mcheck

Command Mode

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

Privilege Requirement

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

Example

Enable mcheck for port 1/0/2:

```
T1500-28PCT(config)#interface fastEthernet 1/0/2
T1500-28PCT(config-if)# spanning-tree mcheck
```

23.22 show spanning-tree active

Description

The **show spanning-tree active** command is used to display the active information of spanning-tree.

Syntax

```
show spanning-tree active
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the active information of spanning-tree:

```
T1500-28PCT(config)# show spanning-tree active
```

23.23 show spanning-tree bridge

Description

The **show spanning-tree bridge** command is used to display the bridge parameters.

Syntax

```
show spanning-tree bridge [ forward-time | hello-time | hold-count | max-age  
| max-hops | mode | priority | state ]
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the bridge parameters:

```
T1500-28PCT(config)# show spanning-tree bridge
```

23.24 show spanning-tree interface

Description

The **show spanning-tree interface** command is used to display the spanning-tree information of all ports or a specified port.

Syntax

```
show spanning-tree interface [ gigabitEthernet port | port-channel lagid ]  
[ edge | ext-cost | int-cost | mode | p2p | priority | role | state | status ]
```

Parameter

port— The Ethernet port number.

lagid— The ID of the LAG.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the spanning-tree information of all ports:

```
T1500-28PCT(config)# show spanning-tree interface
```

Display the spanning-tree information of port 1/0/2:

```
T1500-28PCT(config)# show spanning-tree interface fastEthernet 1/0/2
```

Display the spanning-tree mode information of port 1/0/2:

```
T1500-28PCT(config)# show spanning-tree interface fastEthernet 1/0/2
mode
```

23.25 show spanning-tree interface-security

Description

The **show spanning-tree interface-security** command is used to display the protect information of all ports or a specified port.

Syntax

```
show spanning-tree interface-security [ gigabitEthernet port |
port-channel lagid] [ bpdufilter | bpduguard | loop | root | tc | tc-defend ]
```

Parameter

port— The Ethernet port number.

lagid— The ID of the LAG.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the protect information of all ports:

```
T1500-28PCT(config)# show spanning-tree interface-security
```

Display the protect information of port 1:

```
T1500-28PCT(config)# show spanning-tree interface-security
fastEthernet 1/0/1
```

Display the interface security bpdufilter information:

```
T1500-28PCT(config)# show spanning-tree interface-security bpdufilter
```

23.26 show spanning-tree mst

Description

The **show spanning-tree mst** command is used to display the related information of MST Instance.

Syntax

```
show spanning-tree mst { configuration [ digest ] | instance instance-id
[ interface [ gigabitEthernet port | port-channel lagid ] ] }
```

Parameter

instance-id— Instance ID desired to show, ranging from 1 to 8.

port— The Ethernet port number.

lagid— The ID of the LAG.

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:

```
T1500-28PCT(config)#show spanning-tree mst configuration
```

Display the related information of MST Instance 1:

```
T1500-28PCT(config)#show spanning-tree mst instance 1
```

Display all the ports information of MST Instance 1:

```
T1500-28PCT(config)#show spanning-tree mst instance 1 interface
```

Chapter 24 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.

24.1 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:

```
T1500-28PCT(config)# ip igmp snooping
```

24.2 ip igmp snooping(interface)

Description

The **ip igmp snooping** command is used to enable the IGMP Snooping function for the desired port. To disable the IGMP Snooping function, please use **no ip igmp snooping** command.

Syntax

ip igmp snooping

no ip igmp snooping

Command Mode

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

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)#interface fastEthernet 1/0/3
T1500-28PCT(config-if)# ip igmp snooping
```

24.3 ip igmp snooping rtime

Description

The **ip igmp snooping rtime** command is used to specify router port aging time globally. To restore the default timer, please use **no ip igmp snooping rtime** command.

Syntax

```
ip igmp snooping rtime rtime
no ip igmp snooping rtime
```

Parameter

rtime — Specify the aging time in seconds, ranging from 60 to 600. The default aging time is 300 seconds.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify IGMP Snooping router port aging time as 100 seconds globally:

```
T1500-28PCT(config)# ip igmp snooping rtime 100
```

24.4 ip igmp snooping mtime

Description

The **ip igmp snooping mtime** command is used to specify member port aging time globally. The default aging time is 260 seconds. To restore the default timer, please use **no ip igmp snooping mtime** command.

Syntax

```
ip igmp snooping mtime mtime  
no ip igmp snooping mtime
```

Parameter

mtime — Specify the aging time in seconds, ranging from 60 to 600. The default aging time is 260 seconds.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify IGMP Snooping member port aging time as 100 seconds globally:

```
T1500-28PCT(config)# ip igmp snooping mtime 100
```

24.5 ip igmp snooping report-suppression

Description

The **ip igmp snooping report-suppression** command is used enable the IGMP report suppression function. When it is enabled, the switch forwards only the first IGMP report message per mulicast group to the Layer 3 device, and the subsequent IGMP reports from the same multicast group are discarded. To disable the IGMP report suppression function and forward all the IGMP reports to the Layer 3 device, please use **no ip igmp snooping report-suppression** command. This function is disabled by default.

Syntax

```
ip igmp snooping report-suppression  
no ip igmp snooping report-suppression
```

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the IGMP report suppression function:

```
T1500-28PCT(config)# ip igmp snooping report-suppression
```

24.6 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 fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)#interface fastEthernet 1/0/3
```

```
T1500-28PCT(config-if)# ip igmp snooping immediate-leave
```

24.7 ip igmp snooping drop-unknown

Description

The **ip igmp snooping drop-unknown** command is used to process the unknown multicast as discard. To disable the operation of processing the unknown multicast as discard, please use **no ip igmp snooping drop-unknown** command.

Syntax

ip igmp snooping drop-unknown

no ip igmp snooping drop-unknown

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the operation to process unknown multicast as discard:

```
T1500-28PCT(config)# ip igmp snooping drop-unknown
```

24.8 ip igmp snooping last-listener query-inteval

Description

The **ip igmp snooping last-listener query-inteval** command is used to specify the interval to send Specific Query Message. The default value is 1 second. To restore the default interval, please use **no ip igmp snooping last-listener query-inteval** command.

Syntax

ip igmp snooping last-listener query-inteval *interval*

no ip igmp snooping last-listener query-inteval

Parameter

interval—— Specify the interval to send Specific Query Message in seconds, ranging from 1 to 5.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the interval of Specific Query Message to 3 seconds:

```
T1500-28PCT(config)# ip igmp snooping last-listener query-inteval 3
```

24.9 ip igmp snooping last-listener query-count

Description

The **ip igmp snooping last-listener query-count** command is used to specify the numbers of Specific Query Message to be sent. The default value is 2. To restore the default number, please use **no ip igmp snooping last-listener query-count** command.

Syntax

```
ip igmp snooping last-listener query-count num  
no ip igmp snooping last-listener query-count
```

Parameter

num—— Specify the numbers of Specific Query Message to be sent, ranging from 1 to 5.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the number of Specific Query Message to 3:

```
T1500-28PCT(config)# ip igmp snooping last-listener query-count 3
```

24.10 ip igmp snooping vlan-config

Description

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

Syntax

```
ip igmp snooping vlan-config vlan-id-list [ rtime router-time | mtime member-time | rport interface { fastEthernet port-list | gigabitEthernet port-list | port-channel lagid } ]  
ip igmp snooping vlan-config vlan-id-list static ip interface { fastEthernet port-list | gigabitEthernet port-list | port-channel lagid }
```

```
no ip igmp snooping vlan-config vlan-id-list [ rtime router-time | mtime member-time | rport interface { fastEthernet port-list | gigabitEthernet port-list | port-channel lagid } ]
```

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

Parameter

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

router-time — Router Port Time. Within this time, if the switch does not receive IGMP query message from the router port, it will consider this port is not a router port any more. Router Port Time ranges from 60 to 600 in seconds. By default, it is 0 and the global router-time will be used.

member-time — Member Port Time. Within this time, if the switch does not receive IGMP report message from the member port, it will consider this port is not a member port any more. Member Port Time ranges from 60 to 600 in seconds. By default, it is 0 and the global member-time will be used.

port-list — The list of Ethernet ports.

lagid — The ID of the LAGs.

ip — The static multicast IP address.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the IGMP Snooping function and modify Router Port Time as 300 seconds, Member Port Time as 200 seconds for VLAN 1-3, and set the router port as 1/0/1 for VLAN 1-2:

```
T1500-28PCT(config)# ip igmp snooping vlan-config 1-3 rtime 300
T1500-28PCT(config)# ip igmp snooping vlan-config 1-3 mtime 200
T1500-28PCT(config)# ip igmp snooping vlan-config 1-2 rport interface
fastEthernet 1/0/1
```

Add static multicast IP address 225.0.0.1, which corresponds to VLAN 2, and configure the forward ports as ports 1/0/1-3:


```
T1500-28PCT(config)# ip igmp snooping vlan-config 2 static 225.0.0.1
interface fastEthernet 1/0/1-3
```

24.11 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-forbidden** command.

Syntax

```
ip igmp snooping vlan-config vlan-id-list router-ports-forbidden interface
{ fastEthernet port-list | gigabitEthernet port-list | port-channel
port-channel-id}
no ip igmp snooping vlan-config vlan-id-list router-ports-forbidden
interface [ fastEthernet port-list | gigabitEthernet port-list | port-channel
port-channel-id]
```

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-id — 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 :

```
T1500-28PCT(config)# ip igmp snooping vlan-config 1
router-ports-forbidden interface fastEthernet 1/0/1-3
```

24.12 ip igmp snooping multi-vlan-config

Description

The **ip igmp snooping multi-vlan-config** command is used to create Multicast VLAN. To delete the corresponding Multicast VLAN, please use **no ip igmp snooping multi-vlan-config** command. To restore the default values, please use **no ip igmp snooping multi-vlan-config** with specified parameters.

Syntax

```
ip igmp snooping multi-vlan-config [ vlan-id ] [ rtime router-time | mtime member-time | rport interface { fastEthernet port-list | gigabitEthernet port-list | port-channel lagid } ]
```

```
no ip igmp snooping multi-vlan-config [ rtime router-time | mtime member-time | rport interface { fastEthernet port-list | gigabitEthernet port-list | port-channel lagid } ]
```

Parameter

vlan-id— The ID of the multicast VLAN desired to create or modify, ranging from 2 to 4094. If not specified, the default multicast VLAN will be selected.

router-time — Router Port Time. Within this time, if the switch does not receive IGMP query message from the router port, it will consider this port is not a router port any more. Router Port Time ranges from 60 to 600 in seconds. By default, it is 0 and the global router-time will be used.

member-time — Member Port Time. Within this time, if the switch does not receive IGMP report message from the member port, it will consider this port is not a member port any more. Member Port Time ranges from 60 to 600 in seconds. By default, it is 0 and the global member-time will be used.

port-list — The list of Ethernet ports.

lagid — The ID of the LAGs.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable Multicast VLAN 3, and configure Router Port Time as 100 seconds, Member Port Time 100 seconds, and Static Router Port port 1/0/3:

```
T1500-28PCT(config)# ip igmp snooping multi-vlan-config 3 rtime 100
T1500-28PCT(config)# ip igmp snooping multi-vlan-config 3 mtime 100
T1500-28PCT(config)# ip igmp snooping multi-vlan-config 3 rport
interface fastEthernet1/0/3
```

24.13 ip igmp snooping multi-vlan-config (router-ports-forbidden)

Description

This command is used to forbid the specified ports as being router ports in the specified multicast VLAN. To delete the forbidden router ports, please use **no ip igmp snooping multi-vlan-config router-ports-forbidden** command.

Syntax

```
ip igmp snooping multi-vlan-config [ vlan-id ] router-ports-forbidden  
interface { fastEthernet port-list | gigabitEthernet port-list | port-channel  
port-channel-id}
```

```
no ip igmp snooping multi-vlan-config router-ports-forbidden [ interface  
{ fastEthernet port-list | gigabitEthernet port-list | port-channel  
port-channel-id}]
```

Parameter

vlan-id— The ID of the multicast VLAN, ranging from 2 to 4094.

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

port-channel-id— 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 level users have access to these commands.

Example

Forbid the Ethernet ports 1/0/1-3 as being router ports in multicast VLAN 2 :

```
T1500-28PCT(config)# ip igmp snooping multi-vlan-config 2
router-ports-forbidden interface fastEthernet1/0/1-3
```

24.14 ip igmp snooping multi-vlan-config (source-ip-replace)

Description

This command is used to replace the multicast source IP address of the IGMP packets in the specified multicast VLAN. To delete the forbidden router ports, please use **no ip igmp snooping multi-vlan-config replace-sourceip** command.

Syntax

```
ip igmp snooping multi-vlan-config [ vlan-id ] replace-sourceip ip
no ip igmp snooping multi-vlan-config replace-sourceip
```

Parameter

vlan-id—The ID of the multicast VLAN, ranging from 2 to 4094.

ip — Specify the IP address. The switch will use this IP address to replace the source IP address of the IGMP packets.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Replace the source IP address of the IGMP packets in multicast VLAN 2 as 192.168.0.112:

```
T1500-28PCT(config)# ip igmp snooping multi-vlan-config 2
replace-sourceip 192.168.0.112
```

24.15 ip igmp snooping querier vlan

Description

The **ip igmp snooping querier vlan** command is used to enable the IGMP Snooping Querier function of the VLAN(s). To disable the IGMP Snooping

Querier function of certain VLANs, please use **no ip igmp snooping querier vlan** command.

Syntax

```
ip igmp snooping querier vlan vlan-id  
no ip igmp snooping querier vlan vlan-id
```

Parameter

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the IGMP Snooping Querier function of VLAN 1:

```
T1500-28PCT(config)#ip igmp snooping querier vlan 1
```

24.16 ip igmp snooping querier vlan (general query)

Description

The **ip igmp snooping querier vlan** command is used to configure the parameters for IGMP Snooping Querier to send a general query frame. To return to the default configuration, please use **no ip igmp snooping querier vlan** command.

Syntax

```
ip igmp snooping querier vlan vlan-id { query-interval interval /  
max-response-time response-time /general-query source-ip ip-addr }  
no ip igmp snooping querier vlan vlan-id { query-interval /  
max-response-time /general-query source-ip }
```

Parameter

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

interval — The time interval to send a general query frame by IGMP Snooping Querier, ranging from 10 to 300 (Seconds). By default, it is 60 seconds.

response-time — The maximal time for the host to respond to a general query frame, ranging from 1 to 25 (Seconds). By default, it is 10 Seconds.

ip-addr — The source IP of the general query frame sent by IGMP Snooping Querier. It should not be a multicast IP or a broadcast IP. By default, it is 192.168.0.1.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

For VLAN 2, specify its query-interval as 200 seconds, and the response-time as 20 seconds:

```
T1500-28PCT(config)#ip igmp snooping querier vlan 2 query-interval 200
T1500-28PCT(config)#ip igmp snooping querier vlan 2
max-response-time 20
```

24.17 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 fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

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

```
T1500-28PCT(config)#interface range fastEthernet 1/0/2-5
T1500-28PCT(config-if-range)#ip igmp snooping max-groups 10
T1500-28PCT(config-if-range)#ip igmp snooping max-groups action
replace
```

24.18 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:

```
T1500-28PCT(config)# ip igmp profile 1
```

24.19 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:

```
T1500-28PCT(config)# ip igmp profile 1  
T1500-28PCT(config-igmp-profile)#deny
```

24.20 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:

```
T1500-28PCT(config)# ip igmp profile 1
T1500-28PCT(config-igmp-profile)#permit
```

24.21 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:

```
T1500-28PCT(config)# ip igmp profile 1
T1500-28PCT(config-igmp-profile)#range 225.1.1.1 226.3.2.1
```

24.22 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 fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel)

Privilege Requirement

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

Example

Bind profile 1 to interface fastEthernet 1/0/2:

```
T1500-28PCT(config)#interface fastEthernet 1/0/2  
T1500-28PCT(config-if)# ip igmp filter 1
```

24.23 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:

```
T1500-28PCT(config)# clear ip igmp snooping statistics
```

24.24 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:

```
T1500-28PCT# show ip igmp snooping
```

24.25 show ip igmp snooping interface

Description

The **show ip igmp snooping interface** command is used to display the port configuration of IGMP snooping.

Syntax

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

```
show ip igmp snooping interface [ port-channel [ lagid ] ] { 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 IGMP basic configuration configuration of all ports and LAGs:

```
T1500-28PCT# show ip igmp snooping interface basic-config
```

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

```
T1500-28PCT# show ip igmp snooping interface fastEthernet 1/0/2
basic-config
```

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

```
T1500-28PCT# show ip igmp snooping interface fastEthernet 1/0/1-4
packet-stat
```

24.26 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:

```
T1500-28PCT# show ip igmp snooping vlan 2
```

24.27 show ip igmp snooping multi-vlan

Description

The **show ip igmp snooping multi-vlan** command is used to display the Multicast VLAN configuration.

Syntax

```
show ip igmp snooping multi-vlan
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the Multicast VLAN configuration:

```
T1500-28PCT# show ip igmp snooping multi-vlan
```

24.28 show ip igmp snooping groups vlan

Description

The **show ip igmp snooping groups vlan** command is used to display the information of the multicast groups of a selected VLAN.

Syntax

```
show ip igmp snooping groups vlan vlan-id [ multicast_addr ]
```

Parameter

vlan-id—The VLAN ID selected to display.

multicast_addr— IP address of the multicast group.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display all the multicast entries in VLAN 5:

```
T1500-28PCT#show ip igmp snooping groups vlan 5
```

Display information of the multicast group with the IP address 225.1.1.1 in VLAN 5:

```
T1500-28PCT#show ip igmp snooping groups vlan 5 225.1.1.1
```

24.29 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 ] [ count | dynamic | dynamic count | static | static count ]
```

Parameter

vlan-id —The VLAN ID selected to display the information of all multicast items.

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:

```
T1500-28PCT#show ip igmp snooping groups
```

Display all the multicast entries in VLAN 5:

```
T1500-28PCT(config)#show ip igmp snooping groups vlan 5
```

Display the count of multicast entries in VLAN 5:

```
T1500-28PCT(config)#show ip igmp snooping groups vlan 5 count
```

Display the dynamic multicast groups of VLAN 5:

```
T1500-28PCT(config)#show ip igmp snooping groups vlan 5 dynamic
```

Display the static multicast groups of VLAN 5:

```
T1500-28PCT(config)#show ip igmp snooping groups vlan 5 static
```

Display the count of dynamic multicast entries of VLAN 5:

```
T1500-28PCT(config)#show ip igmp snooping groups vlan 5 dynamic  
count
```

Display the count of static multicast entries of VLAN 5:

```
T1500-28PCT(config)#show ip igmp snooping groups vlan 5 static count
```

24.30 show ip igmp snooping querier

Description

The **show ip igmp snooping querier** command is used to display the Querier configuration of VLAN.

Syntax

```
show ip igmp snooping querier [ vlan vlan-id]
```

Parameter

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

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display all Querier information:

```
T1500-28PCT(config)# show ip igmp snooping querier
```

24.31 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:

```
T1500-28PCT(config)# show ip igmp profile
```


Chapter 25 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.

25.1 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:

```
T1500-28PCT(config)# snmp-server
```

25.2 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:

```
T1500-28PCT(config)# snmp-server view view1 1.3.6.1.6.3.20 include
```

25.3 snmp-server group

Description

The **snmp-server group** command is used to manage and configure the SNMP group. To delete the corresponding SNMP group, please use **no snmp-server group** command. SNMP v3 provides the VACM (View-based Access Control Model) and USM (User-Based Security Model) mechanisms for authentication. The users in the SNMP Group can manage the device via the Read View, Write View and Notify View. And the authentication mode and the privacy mode guarantee the high security for the communication between the management station and the managed device.

Syntax

```
snmp-server group name [ smode { v1 | v2c | v3 } ] [ slev { noAuthNoPriv | authNoPriv | authPriv } ] [ read read-view ] [ write write-view ] [ notify notify-view ]
```

```
no snmp-server group name smode { v1 | v2c | v3 } slev { noAuthNoPriv | authNoPriv | authPriv }
```

Parameter

name — The SNMP Group name, ranging from 1 to 16 characters. The Group Name, Security Model and Security Level compose the identifier of the SNMP Group. These three items of the Users in one group should be the same.

smode — Security Model, with v1、v2c and v3 options. They represent SNMP v1, SNMP v2c and SNMP v3.

slev — The Security Level of SNMP v3 Group. There are three options, including noAuthNoPriv (no authorization and no encryption)、authNoPriv (authorization and no encryption) and authPriv (authorization and encryption) . By default, the Security Level is noAuthNoPriv. There is no need to configure this in SNMP v1 Mode and SNMP v2c Mode.

read-view — Select the View to be the Read View. The management access is restricted to read-only, and changes cannot be made to the assigned SNMP View.

write-view — Select the View to be the Write View. The management access is writing only and changes can be made to the assigned SNMP View. The View defined both as the Read View and the Write View can be read and modified.

notify-view — Select the View to be the Notify View. The management station can receive notification messages of the assigned SNMP view generated by the switch's SNMP agent.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Add a group, and configure the name as group 1, the Security Model as SNMP v3, the security level as authNoPriv, the management access to the assigned View viewDefault as read-write, besides the notification messages sent by View viewDefault can be received by Management station:

```
T1500-28PCT(config)# snmp-server group group1 smode v3 slev  
authNoPriv read viewDefault write viewDefault notify viewDefault
```

Delete group 1:

```
T1500-28PCT(config)# no snmp-server group group1 smode v3 slev  
authNoPriv
```

25.4 snmp-server user

Description

The **snmp-server user** command is used to add User. To delete the corresponding User, please use **no snmp-server user** command. The User in an SNMP Group can manage the switch via the management station software. The User and its Group have the same security level and access right.

Syntax

```
snmp-server user name { local | remote } group-name [ smode { v1 | v2c | v3 } ]  
[ slev { noAuthNoPriv | authNoPriv | authPriv } ] [ cmode { none | MD5 | SHA } ]  
[ cpwd confirm-pwd ] [ emode { none | DES } ] [ epwd encrypt-pwd ]  
no snmp-server user name
```

Parameter

name — User Name, ranging from 1 to 16 characters.

local | remote — User Type, with local and remote options. Local indicates that the user is connected to a local SNMP engine, while remote means that the user is connected to a remote SNMP engine.

group-name — The Group Name of the User. The User is classified to the corresponding Group according to its Group Name, Security Model and Security Level.

smode — The Security Model of the User, with v1, v2c and v3 options. By default, the option is v1. The Security Model of the User must be the same with that of the Group which the User belongs to.

slev — The Security Level of SNMP v3 Group. There are three options, including noAuthNoPriv (no authorization and no encryption), authNoPriv (authorization and no encryption) and authPriv (authorization and encryption). By default, the option is "noAuthNoPriv". The Security Level of the User must be the same with that of the Group which the User belongs to.

cmode — The Authentication Mode of the SNMP v3 User, with none, MD5 and SHA options. None indicates no authentication method is used, MD5 indicates the port authentication is performed via HMAC-MD5 algorithm and SHA indicates the port authentication is performed via SHA (Secure Hash Algorithm). SHA authentication mode has a higher security than MD5 mode. By default, the Authentication Mode is "none".

confirm-pwd — Authentication Password, ranging from 1 to 16 characters. The question marks and spaces are not allowed. This password in the configuration file will be displayed in the symmetric encrypted form.

emode — The Privacy Mode of the SNMP v3 User, with none and DES options. None indicates no privacy method is used, and DES indicates DES encryption method is used. By default, the Privacy Mode is “none”.

encrypt-pwd — Privacy Password, ranging from 1 to 16 characters. The question marks and spaces are not allowed. This password in the configuration file will be displayed in the symmetric encrypted form.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Add Local User admin to Group group2, and configure the Security Model of the user as v3, the Security Level of the group as authPriv, the Authentication Mode of the user as MD5, the Authentication Password as 11111, the Privacy Mode as DES, and the Privacy Password as 22222:

```
T1500-28PCT(config)# snmp-server user admin local group2 smode v3
slev authPriv cmode MD5 cpwd 11111 emode DES epwd 22222
```

25.5 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:

```
T1500-28PCT(config)# snmp-server community public read-write  
viewDefault
```

25.6 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:

```
T1500-28PCT(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:

```
T1500-28PCT(config)# snmp-server host fe80::1234 162 admin smode v2c type inform retries 100 timeout 1000
```

25.7 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:

```
T1500-28PCT(config)# snmp-server engineID local 1234567890 remote  
abcdef123456
```

25.8 snmp-server traps snmp

Description

The **snmp-server traps snmp** command is used to enable SNMP standard traps which include four types: linkup, linkdown, warmstart and coldstart. To

disable the sending of SNMP standard traps, please use **no snmp-server traps snmp** command.

Syntax

snmp-server traps snmp [linkup | linkdown | warmstart | coldstart | auth-failure]

no snmp-server traps snmp [linkup | linkdown | warmstart | coldstart | auth-failure]

Parameter

linkup — Enable linkup trap. It is sent when port status changes from linkdown to linkup. By default, it is enabled.

linkdown — Enable linkdown trap. It is sent when port status changes from linkup to linkdown. By default, it is enabled.

warmstart — Enable warmstart trap. It is sent upon SNMP function reboot. By default, it is enabled.

coldstart — Enable coldstart trap. It is sent upon switch reboot. By default, it is enabled.

auth-failure — Enable the auth-failure trap. It is sent when a received SNMP request fails the authentication. By default, it is enabled.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable SNMP standard linkup trap for the switch:

```
T1500-28PCT(config)# snmp-server traps snmp linkup
```

25.9 snmp-server traps link-status

Description

The **snmp-server traps link-status** command is used to enable SNMP link status trap for the specified port. To disable the sending of SNMP link status trap, please use **no snmp-server traps link-status** command.

Syntax

snmp-server traps link-status

no snmp-server traps link-status

Command Mode

Interface Configuration Mode (interface fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable SNMP link status trap for port 3:

```
T1500-28PCT(config)#interface fastEthernet 1/0/3
T1500-28PCT(config-if)# snmp-server traps link-status
```

25.10 snmp-server traps

Description

The **snmp-server traps** command is used to enable SNMP extended traps. To disable the sending of SNMP extended traps, please use **no snmp-server traps** command.

Syntax

```
snmp-server traps { bandwidth-control | cpu | flash | lldp |
loopback-detection | storm-control | spanning-tree | memory }
```

```
no snmp-server traps { bandwidth-control | cpu | flash | lldp |
loopback-detection | storm-control | spanning-tree | memory }
```

Parameter

bandwidth-control — Enable bandwidth-control trap. It is sent when the rate limit function is enabled and the bandwidth exceeds the predefined value.

cpu — Allow CPU-related trap. It is sent when CPU usage exceeds the predefined threshold. By default, the CPU usage threshold of the switch is 80%.

flash — Enable flash trap. It is sent when flash is modified during operations such as backup, reset, firmware upgrade, configuration import, etc.

lldp — Enable lldp trap. It is sent when the port's neighbor changes.

loopback-detection — Enable loopback-detection trap. It is sent when the switch detects loopback or loopback is cleared.

storm-control — Enable storm-control trap. It is sent when the multicast or broadcast rate exceeds the predefined value.

spanning-tree — Enable spanning-tree trap. It is sent when the port forwarding status changes or the port receives TCN packet or packet with TC fport-channel-.

memory — Enable memory trap. It is sent when memory usage exceeds 80%.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable SNMP extended bandwidth-control trap for the switch:

```
T1500-28PCT(config)# snmp-server traps bandwidth-control
```

25.11 snmp-server traps vlan

Description

The **snmp-server traps vlan** command is used to enable SNMP extended VLAN-related traps which include two types: create and delete. To disable this function, please use **no snmp-server traps vlan** command.

Syntax

```
snmp-server traps vlan [ create | delete ]
```

```
no snmp-server traps vlan [create | delete ]
```

Parameter

create — Enable VLAN-created trap. It is sent when new VLAN is created successfully.

delete — Enable VLAN-deleted traps. It is sent when VLAN is deleted successfully.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable all SNMP extended VLAN-related traps for the switch:

```
T1500-28PCT(config)# snmp-server traps vlan
```

Enable VLAN-created trap only for the switch:

```
T1500-28PCT(config)# snmp-server traps vlan create
```

25.12 rmon history

Description

The **rmon history** command is used to configure the history sample entry. To return to the default configuration, please use **no rmon history** command. RMON (Remote Monitoring), basing on SNMP architecture, functions to monitor the network. History Group is one of the commonly used RMON Groups. After a history group is configured, the switch collects network statistics information periodically, based on which the management station can monitor network effectively.

Syntax

```
rmon history index interface gigabitEthernet port [ interval seconds ]  
[ owner owner-name ] [ buckets number ]  
no rmon history index
```

Parameter

index — The index number of the entry, ranging from 1 to 12, in the format of 1-3,5.

port — The Ethernet port number.

seconds — The interval to take samplings from the port, ranging from 10 to 3600 in seconds. By default, it is 1800.

owner-name — The owner of the history sample entry, ranging from 1 to 16 characters. By default, it is "monitor".

number — The maximum number of buckets desired for the RMON history group of statistics, ranging from 1 to 130. The default is 50 buckets.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the sample port as port 1/0/2 and the sample interval as 100 seconds for the entry 1-3:

```
T1500-28PCT(config)# rmon history 1-3 interface fastEthernet 1/0/2
interval 100 owner owner1
```

25.13 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:

```
T1500-28PCT(config)# rmon event 1-4 user user1 description description1
type log owner owner1
```

25.14 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:

```
T1500-28PCT(config)#rmon alarm 1-3 stats-index 2 owner owner1 interval
100
```

25.15 rmon statistics

Description

The **rmon statistics** command is used to configure the entries of SNMP-RMON statistics. To delete the corresponding entry, please use **no rmon statistics** command. The maximum supported entries are 1000.

Syntax

```
rmon statistics index interface gigabitEthernet port [ owner owner-name ]  
[ status { underCreation | valid } ]
```

```
no rmon statistics index
```

Parameter

index — The index number of the statistics entry, ranging from 1 to 65535, in the format of 1-3,5.

port — The statistics port number, in the format of 1/0/1.

owner-name — The creator of the event entry, ranging from 1 to 16 characters. By default, it is "monitor".

status — The status of the statistics entry, either "underCreation" or "valid". "underCreation" means this entry won't take effect until it is modified to "valid"; "valid" means this entry takes effect immediately after it is created.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the statistics entries 1-3 with the statistics port as 1/0/1, owner as owner1 and status as valid:

```
T1500-28PCT(config)#rmon statistics 1-3 interface fastEthernet 1/0/1  
owner owner1 status valid
```

25.16 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:

```
T1500-28PCT# show snmp-server
```

25.17 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:

```
T1500-28PCT# show snmp-server view
```

25.18 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:

```
T1500-28PCT# show snmp-server group
```

25.19 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:

```
T1500-28PCT# show snmp-server user
```

25.20 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:

```
T1500-28PCT# show snmp-server community
```

25.21 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:

```
T1500-28PCT# show snmp-server host
```

25.22 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:

```
T1500-28PCT# show snmp-server engineID
```

25.23 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:

```
T1500-28PCT# show rmon history
```

25.24 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:

```
T1500-28PCT# show rmon event 1-4
```

25.25 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:

```
T1500-28PCT# show rmon alarm 1-2
```

25.26 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:

```
T1500-28PCT#show rmon statistics 1
```

Chapter 26 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) such as SNMP.

26.1 Ildp

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:

```
T1500-28PCT(config)#lldp
```

26.2 Ildp hold-multiplier

Description

The **lldp hold-multiplier** command is used to configure the Hold Multiplier parameter. The aging time of the local information in the neighbor device is determined by the actual TTL value used in the sending LLDPDU. $TTL = \text{Hold Multiplier} * \text{Transmit Interval}$. To return to the default configuration, please use **no lldp hold-multiplier** command.

Syntax

lldp hold-multiplier *multiplier*

no lldp hold-multiplier

Parameter

multiplier — Configure the Hold Multiplier parameter. It ranges from 2 to 10. By default, it is 4.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify Hold Multiplier as 5:

```
T1500-28PCT(config)#lldp hold-multiplier 5
```

26.3 lldp timer

Description

The **lldp timer** command is used to configure the parameters about transmission. To return to the default configuration, please use **no lldp timer** command.

Syntax

```
lldp timer { tx-interval tx-interval / tx-delay tx-delay / reinit-delay reinit-delay / notify-interval notify-interval / fast-count fast-count }
```

```
no lldp timer { tx-interval | tx-delay | reinit-delay | notify-interval | fast-count }
```

Parameter

tx-interval — Configure the interval for the local device to transmit LLDPDU to its neighbors. The value ranges from 5 to 32768 and the default value is 30 seconds.

tx-delay — Configure a value from 1 to 8192 in seconds to specify the time for the local device to transmit LLDPDU to its neighbors after changes occur so as to prevent LLDPDU being sent frequently. By default, it is 2 seconds.

reinit-delay — This parameter indicates the amount of delay from when LLDP status becomes "disable" until re-initialization will be attempted. The value ranges from 1 to 10 and the default value is 3.

notify-interval — Specify the interval of Trap message which will be sent from local device to network management system. The value ranges from 5 to 3600 and the default value is 5 seconds.

fast-count — When the port's LLDP state transforms from Disable (or Rx_Only) to Tx&Rx (or Tx_Only), the fast start mechanism will be enabled, that is, the transmit interval will be shorten to a second, and several LLDPDUs will be sent out (the number of LLDPDUs equals this parameter). The value ranges from 1 to 10 and the default value is 3.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the Transmit Interval of LLDPDU as 45 seconds and Trap message to NMS as 120 seconds:

```
T1500-28PCT(config)#lldp timer tx-interval 45
T1500-28PCT(config)#lldp timer notify-interval 120
```

26.4 Ildp receive

Description

The **lldp receive** command is used to enable the designated port to receive LLDPDU. To disable the function, please use **no lldp receive** command.

Syntax

```
lldp receive
no lldp receive
```

Command Mode

Interface Configuration Mode (interface fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable port 1/0/1 to receive LLDPDU:

```
T1500-28PCT(config)#interface fastEthernet 1/0/1
T1500-28PCT(config-if)#lldp receive
```

26.5 lldp transmit

Description

The **lldp transmit** command is used to enable the designated port to transmit LLDPDU. To disable the function, please use **no lldp transmit** command.

Syntax

lldp transmit
no lldp transmit

Command Mode

Interface Configuration Mode (interface fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable port 1/0/1 to transmit LLDPDU:

```
T1500-28PCT(config)#interface fastEthernet 1/0/1
T1500-28PCT(config-if)#lldp transmit
```

26.6 lldp snmp-trap

Description

The **lldp snmp-trap** command is used to enable the port's SNMP notification. If enabled, the port will notify the trap event to network management system. To disable the ports' SNMP notification, please use **no lldp snmp-trap** command.

Syntax

lldp snmp-trap
no lldp snmp-trap

Command Mode

Interface Configuration Mode (interface fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the SNMP notification for port 1/0/1:

```
T1500-28PCT(config)#interface fastEthernet 1/0/1
T1500-28PCT(config-if)#lldp snmp-trap
```

26.7 lldp tlv-select

Description

The **lldp tlv-select** command is used to configure TLVs to be included in outgoing LLDPDU. To exclude TLVs, please use **no lldp tlv-select** command. By default, All TLVs are included in outgoing LLDPDU.

Syntax

```
lldp tlv-select { [ port-description ] [ system-capability ] [ system-description ]
[ system-name ] [ management-address ] [ port-vlan ] [ protocol-vlan ]
[ vlan-name ] [ link-aggregation ] [ mac-phy-cfg ] [ max-frame-size ] [ power ]
[ all ] }

no lldp tlv-select { [ port-description ] [ system-capability ]
[ system-description ] [ system-name ] [ management-address ] [ port-vlan ]
[ protocol-vlan ] [ vlan-name ] [ link-aggregation ] [ mac-phy-cfg ]
[ max-frame-size ] [ power ] [ all ] }
```

Command Mode

Interface Configuration Mode (interface fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Exclude "management-address" and "port-vlan-id" TLVs in LLDPDU outgoing from port 1/0/1:

```
T1500-28PCT(config)#interface fastEthernet 1/0/1
T1500-28PCT(config-if)# no lldp tlv-select management-address port-vlan
```

26.8 Ildp med-fast-count

Description

The **ildp 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 ildp med-fast-count** command.

Syntax

ildp med-fast-count *count*

no ildp 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:

```
T1500-28PCT(config)# ildp med-fast-count 5
```

26.9 Ildp med-status

Description

The **ildp 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 ildp med-status** command.

Syntax

ildp med-status

no ildp med-status

Command Mode

Interface Configuration Mode (interface fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the LLDP-MED feature for port 1/0/2:

```
T1500-28PCT(config)#interface fastEthernet 1/0/2
T1500-28PCT(config-if)#lldp med-status
```

26.10 lldp med-tlv-select

Description

The **lldp med-tlv-select** command is used to configure LLDP-MED TLVs to be included in outgoing LLDPDU for the corresponding port. To exclude LLDP-MED TLVs, please use **no lldp med-tlv-select** command. By default, All TLVs are included in outgoing LLDPDU.

Syntax

```
lldp med-tlv-select { [inventory-management] [location] [network-policy]
[power-management] [all] }
```

```
no lldp med-tlv-select { [inventory-management] [location] [network-policy]
[power-management] [all] }
```

Command Mode

Interface Configuration Mode (interface fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Exclude "network policy" and "inventory" TLVs in LLDPDU outgoing from port 1/0/2:

```
T1500-28PCT(config)#interface fastEthernet 1/0/2
```

```
T1500-28PCT(config-if)# no lldp med-tlv-select network-policy inventory-  
management
```

26.11 lldp med-location

Description

The lldp med-location command is used to configure the Location Identification TLV's content in outgoing LLDPDU of the port.

Syntax

```
lldp med-location { emergency-number identifier | civic-address  
[ [ language language ] [ province-state province-state ] [ county county ] [ city  
city ] [ street street ] [ house-number house-number ] [ name name ]  
[ postal-zipcode postal-zipcode ] [ room-number room-number ]  
[ post-office-box post-office-box ] [ additional additional ] [ country-code  
country-code ] [ what { dhcp-server | endpoint | switch } ] }
```

Parameter

emergency-number — Emergency Call Service ELIN identifier, which is used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. The length of this field ranges from 10 to 25 characters.

civic-address — The civic address is defined to reuse the relevant sub-fields of the DHCP option for civic Address based Location Configuration Information as specified by IETF.

Command Mode

Interface Configuration Mode (interface fastEthernet / interface range fastEthernet / interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure the civic address in the Location Identification TLV's content in outgoing LLDPDU of port 1/0/2. Configure the language as English and city as London:

```
T2700-28TQ (config)#interface fastEthernet 1/0/2  
T2700-28TQ(config-if)# lldp med-location civic-address language English  
city London
```

26.12 show lldp

Description

The **show lldp** command is used to display the global configuration of LLDP.

Syntax

```
show lldp
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of LLDP:

```
T1500-28PCT#show lldp
```

26.13 show lldp interface

Description

The **show lldp interface** command is used to display LLDP configuration of the corresponding port. By default, the LLDP configuration of all the ports will be displayed.

Syntax

```
show lldp interface [ gigabitEthernet port ]
```

Parameters

port— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

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

```
T1500-28PCT#show lldp interface fastEthernet 1/0/1
```

26.14 show lldp local-information interface

Description

The **show lldp local-information interface** command is used to display the LLDP information of the corresponding port. By default, the LLDP information of all the ports will be displayed.

Syntax

```
show lldp local-information interface [ gigabitEthernet port]
```

Parameters

port— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the LLDP information of port 1/0/1:

```
T1500-28PCT#show lldp local-information interface fastEthernet 1/0/1
```

26.15 show lldp neighbor-information interface

Description

The **show lldp neighbor-information interface** command is used to display the neighbor information of the corresponding port. By default, the neighbor information of all the ports will be displayed.

Syntax

```
show lldp neighbor-information interface [ gigabitEthernet port]
```

Parameters

port— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the neighbor information of port 1/0/1:

```
T1500-28PCT#show lldp neighbor-information interface fastEthernet  
1/0/1
```

26.16 show lldp traffic interface

Description

The **show lldp traffic interface** command is used to display the LLDP statistic information between the local device and neighbor device of the corresponding port. By default, the LLDP statistic information of all the ports will be displayed.

Syntax

```
show lldp traffic interface [ gigabitEthernet port ]
```

Parameters

port— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the LLDP statistic information of port 1/0/1:

```
T1500-28PCT#show lldp traffic interface fastEthernet 1/0/1
```

Chapter 27 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.

27.1 aaa enable

Description

The **aaa enable** command is used to enable the AAA function globally. To disable the AAA function globally, please use the **no aaa enable** command. The global AAA function is disabled by default.

Syntax

aaa enable

no aaa enable

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the AAA function globally:

```
T1500-28PCT(config)# aaa enable
```

27.2 enable admin password

Description

The **enable admin password** command is used to elevate the current logged-in user from guest to admin and gain administrator level privileges. The authentication password is possibly authenticated in RADIUS/TACACS+ servers, user-defined server groups or local on the switch.

To remove the password, please use **no enable admin password** command. This command uses the symmetric encryption.

Syntax

```
enable admin password {[ 0 ] password | 7 encrypted-password }  
no enable admin password
```

Parameter

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

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

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

encrypted-password — A symmetric encrypted password with fixed length, which you can copy from another switch's configuration file. After the encrypted password is configured, you should use the corresponding unencrypted password to elevate the privilege.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

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

Example

Set the elevation password as 123 for the current logged-in user to gain administrator level privileges:

```
T1500-28PCT(config)#enable admin password 0 123
```

27.3 enable admin secret

Description

The **enable admin secret** command is used to elevate the current logged-in user from guest to admin and gain administrator level privileges. The authentication password is possibly authenticated in RADIUS/TACACS+ servers, user-defined server groups or local on the switch.

To remove the password, please use **no enable admin secret** command.

This command uses the MD5 encryption.

Syntax

```
enable secret {[ 0] password | 5 encrypted-password}
```

```
no enable secret
```

Parameter

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

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

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

encrypted-password — An MD5 encrypted password with fixed length, which you can copy from another switch's configuration file. After the encrypted password is configured, you should use the corresponding unencrypted password to elevate the privilege.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

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

Example

Set the secret elevation password as 123 for the current logged-in user to gain administrator level privileges. The password will be displayed in the encrypted form:

```
T1500-28PCT (config)#enable admin secret 0 123
```

27.4 tacacs-server host

Description

The **tacacs-server host** command is used to configure a new TACACS+ server. To delete the specified TACACS+ server, please use **no tacacs-server host** command.

Syntax

```
tacacs-server host ip-address [ port port-id ] [ timeout time ] [ key { [ 0 ] string | 7 encrypted-string } ]
```

```
no tacacs-server host ip-address
```

Parameter

ip-address — Specify the IP address of the TACACS+ server.

port-id — Specify the server's port number for AAA. By default it is 49.

time — Specify the time in seconds the switch waits for the server's response before it times out. The time ranges from 1 to 9 seconds. The default is 5 seconds.

[0] *string* | 7 *encrypted-string* — 0 and 7 are the encryption type. 0 indicates that an unencrypted key will follow. 7 indicates that a symmetric encrypted key with a fixed length will follow. By default, the encryption type is 0. "*string*" is the shared key for the switch and the authentication servers to

exchange messages which contains 31 characters at most. The question marks and spaces are not allowed. "*encrypted-string*" is a symmetric encrypted key with a fixed length, which you can copy from another switch's configuration file. The key or encrypted-key you configured here will be displayed in the encrypted form. Always configure the key as the last item of this command.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

The TACACS+ servers you configured are added in the server group "tacacs" by default.

Example

Configure a TACACS+ server with the IP address as 1.1.1.1, TCP port as 1500, timeout as 6 seconds, and the unencrypted key string as 12345.

```
T1500-28PCT(config)# tacacs-server host 1.1.1.1 port 1500 timeout 6 key
12345
```

27.5 show tacacs-server

Description

This **show tacacs-server** command is used to display the summary information of the TACACS+ servers.

Syntax

```
show tacacs-server
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of all the TACACS+ servers:

27.6 radius-server host

Description

The **radius-server host** command is used to configure a new RADIUS server. To delete the specified RADIUS server, please use **no radius-server host** command.

Syntax

```
radius-server host ip-address [ auth-port port-id ] [ acct-port port-id ]
[ timeout time ] [ retransmit number ] [ key { [ 0 ] string | 7 encrypted-string } ]
no radius-server host ip-address
```

Parameter

ip-address — Specify the IP address of the RADIUS server.

auth-port *port-id* — Specify the UDP destination port for authentication requests. By default it is 1812.

acct-port *port-id* — Specify the UDP destination port for accounting requests. By default it is 1813.

time — Specify the time in seconds the switch waits for the server's response before it times out. The time ranges from 1 to 9 seconds. The default is 5 seconds.

number — Specify the number of times a RADIUS request is resent to a server if the server is not responding in time. By default it is 2 times.

[0] *string* | 7 *encrypted-string* — 0 and 7 are the encryption type. 0 indicates that an unencrypted key will follow. 7 indicates that a symmetric encrypted key with a fixed length will follow. By default, the encryption type is 0. "*string*" is the shared key for the switch and the authentication servers to exchange messages which contains 31 characters at most. The question marks and spaces are not allowed. "*encrypted-string*" is a symmetric encrypted key with a fixed length, which you can copy from another switch's configuration file. The key or encrypted-key you configured here will be displayed in the encrypted form. Always configure the key as the last item of this command.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

The RADIUS servers you configured are added in the server group "radius" by default.

Example

Configure a RADIUS server with the IP address as 1.1.1.1, authentication port as 1200, timeout as 6 seconds, retransmit times as 3, and the unencrypted key string as 12345.

```
T1500-28PCT(config)# radius-server host 1.1.1.1 auth-port 1200 timeout 6  
retransmit 3 key 12345
```

27.7 show radius-server

Description

This **show radius-server** command is used to display the summary information of the RADIUS servers.

Syntax

```
show radius-server
```

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of all the RADIUS servers:

```
T1500-28PCT(config)# show radius-server
```


27.8 aaa group

Description

This **aaa group** command is used to create AAA server groups to group existing TACACS+/RADIUS servers for authentication. This command puts the switch in the server group subconfiguration mode.

To delete the corresponding AAA group, please use the **no aaa group** command.

Syntax

aaa group { radius | tacacs } *group-name*

no aaa group { radius | tacacs } *group-name*

Parameter

radius | tacacs — Specify the server group type as RADIUS or TACACS+.

group-name — Specify the server group name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Create a RADIUS server group with the name radius1:

```
T1500-28PCT(config)# aaa group radius radius1
```

27.9 server

Description

This **server** command is used to add the existing server in the defined server group. To remove the specified server from the server group, please use the **no server** command.

Syntax

```
server ip-address  
no server ip-address
```

Parameter

ip-address—— Specify the server's IP address.

Command Mode

Server Group Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Create the RADIUS server 1.1.1.1 to RADIUS server group "radius1":

```
T1500-28PCT(config)# aaa group radius radius1  
T1500-28PCT(aaa-group)# server 1.1.1.1
```

27.10 show aaa group

Description

This **show aaa group** command is used to display the summary information of the AAA groups. All the servers in this group will be listed if you specify the group name.

Syntax

```
show aaa group [ group-name ]
```

Parameter

group-name—— Specify the server group name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of all the server groups:

```
T1500-28PCT(config)# show aaa group
```

27.11 aaa authentication login

Description

This **aaa authentication login** command is used to configure a login authentication method list. A method list describes the authentication methods and their sequence to authenticate a user. To delete the specified authentication method list, please use the **no aaa authentication login** command.

Syntax

```
aaa authentication login { method-list } { method1 } [ method2 ] [ method3 ]  
[ method4 ]  
no authentication login method-list
```

Parameter

method-list — Specify the method list name.

method1, method2, method3, method4 — Specify the authentication methods in order. The next authentication method is tried only if the previous method does not respond, not if it fails.

The preset methods include radius, tacacs, local and none. "radius" means the RADIUS server group "radius"; "tacacs" means the RACACS+ server group "tacacs"; "local" means local username database are used; "none" means no authentication is used for login.

Users can also define new method with the [aaa group](#) command.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

By default the login authentication method list is "default" with "local" as method1.

Example

Configure a login authentication method list "list1" with the priority1 method as radius and priority2 method as local:

```
T1500-28PCT(config)# aaa authentication login list1 radius local
```

27.12 aaa authentication enable

Description

This **aaa authentication enable** command is used to configure a privilege authentication method list. A method list describes the authentication methods and their sequence to elevate a user's privilege. To delete the specified authentication method list, please use the **no aaa authentication enable** command.

Syntax

```
aaa authentication enable { method-list } { method1 } [ method2 ] [ method3 ]  
[ method4 ]
```

```
no authentication enable method-list
```

Parameter

method-list — Specify the method list name.

method1, method2, method3, method4 — Specify the authentication methods in order. The next authentication method is tried only if the previous method does not respond, not if it fails.

The preset methods include radius, tacacs, local and none. "radius" means the RADIUS server group "radius"; "tacacs" means the RACACS+ server group "tacacs"; "local" means local username database are used; "none" means no authentication is used for privilege elevation.

Users can also define new method with the [aaa group](#) command.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

By default the enable authentication method is "default" with "none" as method1.

Example

Configure a privilege authentication method list "list2" with the priority1 method as radius and priority2 method as local:

```
T1500-28PCT(config)# aaa authenticaiton enable list2 radius local
```

27.13 aaa authentication dot1x default

Description

This **aaa authentication dot1x default** command is used to configure an 802.1X authentication method list. A method list describes the authentication methods for users' login in 802.1X. To delete the default authentication method list, please use the **no aaa authentication dot1x default** command.

Syntax

```
aaa authentication dot1x default { method }
```

```
no aaa authentication dot1x default
```

Parameter

method — Specify the method name. Only RADIUS server group is supported, and the default method is server group "radius".

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the default 802.1X authentication method as "radius1":

```
T1500-28PCT(config)# aaa authentication dot1x default radius1
```

27.14 aaa accounting dot1x default

Description

This **aaa accounting dot1x default** command is used to configure an 802.1X accounting method list. To delete the default accounting method list, please use the **no aaa accounting dot1x default** command.

Syntax

```
aaa accounting dot1x default { method }
```

```
no aaa accounting dot1x default
```

Parameter

method — Specify the method name. Only RADIUS server group is supported, and the default method is server group "radius".

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the default 802.1X accounting method as "radius1":

```
T1500-28PCT(config)# aaa accounting dot1x default radius1
```

27.15 show aaa authentication

Description

This **show aaa authentication** command is used to display the summary information of the authentication login, enable and dot1x method list.

Syntax

```
show aaa authentication [ login | enable | dot1x ]
```

Parameter

login | enable | dot1x — Specify the method list type.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of all the authentication method lists:

```
T1500-28PCT(config)# show aaa authentication
```

27.16 show aaa accounting

Description

This **show aaa accounting** command is used to display the summary information of the accounting method list.

Syntax

```
show aaa accounting [ dot1x ]
```

Parameter

dot1x — Specify the method list type.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of the default 802.1X accounting method list:

```
T1500-28PCT(config)# show aaa accounting
```

27.17 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:

```
T1500-28PCT(config)#line telnet
```

27.18 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":

```
T1500-28PCT(config)#line telnet
```

```
T1500-28PCT(config-line)# login authentication list1
```

27.19 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:

```
T1500-28PCT(config)#line ssh
```

27.20 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":

```
T1500-28PCT(config)# line ssh
```

27.21 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":

```
T1500-28PCT(config)#line telnet  
T1500-28PCT(config-line)# enable authentication list2
```

27.22 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":

```
T1500-28PCT(config)# line ssh
```

```
T1500-28PCT(config-line)# enable authentication list2
```

27.23 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":

```
T1500-28PCT(config)# ip http login authentication list1
```

27.24 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":

```
T1500-28PCT(config)# ip http enable authentication list2
```

27.25 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:

```
T1500-28PCT(config)# show aaa global
```