CLI Reference Guide

Managed Switches

1910013605 REV6.0.0

January 2024

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. tp-link is a registered trademark of TP-Link Corporation Limited. 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 Corporation Limited. Copyright © 2024 TP-Link Corporation Limited. All rights reserved.

https://www.tp-link.com

CONTENTS

Preface 1

Chapter 1 Using the CLI 7

1.1 Accessing the CLI 7

1.1.1 Logon by a console port 7

1.1.2 Logon by Telnet 10

1.1.3 Logon by SSH 11

1.2 CLI Command Modes 19

1.3 Privilege Restrictions 23

1.4 Conventions 23

1.4.1 PoE Disclaimer 23

1.4.2 Format Conventions 23

1.4.3 Special Characters 23

1.4.4 Parameter Format 24

Chapter 2 Line Commands (Only for Certain Devices) 25

2.1 line 25

2.2 media-type rj45 26

Chapter 3 User Interface 27

3.1 enable 27

3.2 service password-encryption 27

3.3 enable password 28

3.4 enable secret 29

3.5 configure 30

3.6 exit 31

3.7 end 31

3.8 clipaging 32

3.9 history 32

3.10 history clear 33

Chapter 4 User Management Commands 34

4.1 user name (password) 34

4.2 user name (secret) 35

4.3 service password-recovery 36

4.4 show user account-list 37

4.5 show user configuration 38

Chapter 5 System Configuration Commands 39

5.1 system-time manual 39
5.2 system-time ntp 39
5.3 system-time dst predefined 41
5.4 system-time dst date 42
5.5 system-time dst recurring 43
5.6 hostname 44
5.7 location 45
5.8 contact-info 45
5.9 led 46
5.10 ip address 46
5.11 ip address-alloc 47
5.12 controller cloud-based (Only for Certain Devices) 48
5.13 controller inform-url (Only for Certain Devices) 49
5.14 reset 50
5.15 service reset-disable 50
5.16 reboot 51
5.17 reboot-schedule 51
5.18 copy running-config startup-config 52
5.19 copy startup-config tftp 53
5.20 copy tftp startup-config 53
5.21 copy backup-config tftp 54
5.22 copy backup-config startup-config 55
5.23 copy running-config backup-config 55
5.24 copy tftp backup-config 56
5.25 boot application 56
5.26 boot config 57
5.27 remove backup-image 58
5.28 firmware upgrade 58
5.29 mcu-firmware unit upgrade (Only for Certain Devices) 59
5.30 mcu-firmware type (Only for Certain Devices) 60
5.31 boot autoinstall start 60
5.32 boot autoinstall persistent-mode 61
5.33 boot autoinstall auto-save 61
5.34 boot autoinstall auto-reboot 62
5.35 boot autoinstall retry-count 63
5.36 show boot autoinstall 63

5.37 show boot autoinstall downloaded-config 64
5.38 ping 64
5.39 tracert 65
5.40 show system-info 66
5.41 show image-info 67
5.42 show boot 67
5.43 show running-config 68
5.44 show startup-config 69
5.45 show system-time 69
5.46 show system-time dst 70
5.47 show system-time ntp 70
5.48 show cable-diagnostics interface 71
5.49 show cpu-utilization 71
5.50 show memory-utilization 72
5.51 show controller 72
5.52 show temperature 73
5.53 show voltage 73
5.54 clear config interace 74
5.55 power backup unit (Only for Certain Devices) 74
5.56 show power (Only for Certain Devices) 75

Chapter 6 File System Configuration Commands (Only for Certain Devices) 76

6.1 copy 76
6.2 cd 76
6.3 dir 77
6.4 pwd 77
6.5 rename 78
6.6 delete 78
6.7 ftp 79
6.8 open 80
6.9 put 80
6.10 get 81
6.11 close 81

Chapter 7 Management Port Configuration Commands (Only for Certain Devices) 83

7.1 management-port protocol 83
7.2 management-port ip 83

7.3 management-port ipv6 enable 84
7.4 management-port ipv6 address 85
7.5 show management-port 85

Chapter 8 EEE Configuration Commands 87

8.1 eee 87
8.2 show interface eee 87

Chapter 9 SDM Template Commands 89

9.1 sdm prefer 89
9.2 show sdm prefer 90

Chapter 10 Time Range Commands 92

10.1 time-range 92
10.2 absolute 92
10.3 periodic 93
10.4 holiday (time-range mode) 94
10.5 holiday 95
10.6 show holiday 95
10.7 show time-range 96

Chapter 11 Port Configuration Commands 97

11.1 interface 97
11.2 interface range 98
11.3 description 99
11.4 shutdown 99
11.5 flow-control 100
11.6 duplex 101
11.7 jumbo-size 101
11.8 speed 102
11.9 clear counters 103
11.10 show fiber-ports 103
11.11 show interface status 104
11.12 show interface counters 104
11.13 show interface configuration 105

Chapter 12 Port Isolation Commands 107

12.1 port isolation 107
12.2 show port isolation interface 108

Chapter 13 Loopback Detection Commands 109

13.1 loopback-detection (global) 109
13.2 loopback-detection interval 109
13.3 loopback-detection recovery-time 110
13.4 loopback-detection (interface) 111
13.5 loopback-detection config process-mode 111
13.6 loopback-detection recover 112
13.7 show loopback-detection global 113
13.8 show loopback-detection interface 114

Chapter 14 Stack Commands (Only for Certain Devices) 115

14.1 switch stack-name 115
14.2 switch stack-group 116
14.3 group-info 116
14.4 interface port 117
14.5 switch priority 117
14.6 switch renumber 118
14.7 switch provision 119
14.8 show switch stack-ports 119
14.9 show switch 120
14.10 show switch unitid 120
14.11 show switch neighbors 121

Chapter 15 DDM Commands (Only for Certain Devices) 122

15.1 ddm state enable 122
15.2 ddm shutdown 123
15.3 ddm temperature_threshold 123
15.4 ddm voltage_threshold 124
15.5 ddm bias_current_threshold 125
15.6 ddm tx_power_threshold 126
15.7 ddm rx_power_threshold 127
15.8 show ddm configuration 128
15.9 show ddm status 129
15.10 show fiber-ports 129

Chapter 16 Etherchannel Commands 131

16.1 channel-group 131
16.2 port-channel load-balance 132

16.3 lacp system-priority 133
16.4 lacp port-priority 134
16.5 show etherchannel 134
16.6 show etherchannel load-balance 135
16.7 show lacp 136
16.8 show lacp sys-id 136

Chapter 17 MAC Address Commands 138

17.1 mac address-table static 138
17.2 no mac address-table dynamic 139
17.3 mac address-table aging-time 139
17.4 mac address-table filtering 140
17.5 mac address-table notification 141
17.6 mac address-table max-mac-count 142
17.7 mac address-table notification (interface) 143
17.8 mac address-table security 144
17.9 mac address-table vlan-security 145
17.10 show mac address-table 146
17.11 clear mac address-table 147
17.12 show mac address-table aging-time 147
17.13 show mac address-table max-mac-count 148
17.14 show mac address-table interface 149
17.15 show mac address-table count 149

58.18 line console 547
58.19 login authentication (console) 547
58.20 enable authentication (telnet) 548
58.21 enable authentication (ssh) 549
58.22 enable authentication (console) 550
58.23 ip http login authentication 550
58.24 ip http enable authentication 551
58.25 show aaa global 552
58.26 enable admin password 552
58.27 enable admin secret 554
58.28 enable-admin 555

Chapter 59 IEEE 802.1x Commands 556

59.1 dot1x system-auth-control 556
59.2 dot1x handshake 557
59.3 dot1x auth-protocol 557
59.4 dot1x vlan-assignment 558
59.5 dot1x accounting 559
59.6 dot1x mab 560
59.7 dot1x guest-vlan 560
59.8 dot1x timeout quiet-period 561
59.9 dot1x timeout supp-timeout 562
59.10 dot1x max- req 563
59.11 dot1x 563
59.12 dot1x port-control 564
59.13 dot1x port-method 565
59.14 dot1x auth-init 566
59.15 dot1x auth-reauth 566
59.16 show dot1x global 567
59.17 show dot1x interface 568
59.18 show dot1x auth-state interface 568

Chapter 60 Port Security Commands 570

60.1 mac address-table max-mac count 570
60.2 show mac address-table max-mac-count 571

Chapter 61 Port Mirroring Commands 572

61.1 monitor session destination interface 572
61.2 monitor session source 573

61.3 monitor session 1 destination remote vlan 574
61.4 monitor session 1 source remote vlan 575
61.5 show monitor session 576

Chapter 62 ACL Commands 577

62.1 access-list create 577
62.2 access-list packet-content profile 577
62.3 access-list resequence 578
62.4 access-list mac 579
62.5 access-list ip 580
62.6 access-list combined 582
62.7 access-list ipv6 584
62.8 access-list packet-content config 586
62.9 access-list action 587
62.10 redirect 588
62.11 s-condition 589
62.12 s-mirror 590
62.13 qos-remark 590
62.14 access bind 591
62.15 show access-list 592
62.16 show access-list bind 592
62.17 show access-list status 593
62.18 show access-list counter 593
62.19 clear access-list 594

Chapter 63 IPv4 IMPB Commands 595

63.1 ip source binding 595
63.2 ip dhcp snooping 596
63.3 ip dhcp snooping vlan 597
63.4 ip dhcp snooping max-entries 597
63.5 ip dhcp snooping trust 598
63.6 show ip source binding 599
63.7 show ip dhcp snooping 599
63.8 show ip dhcp snooping interface 600

Chapter 64 IPv6 IMPB Commands 601

64.1 ipv6 source binding 601
64.2 ipv6 dhcp snooping 602
64.3 ipv6 dhcp snooping vlan 603

64.4 ipv6 dhcp snooping max-entries 603
64.5 ipv6 nd snooping 604
64.6 ipv6 nd snooping vlan 605
64.7 ipv6 nd snooping max-entries 605
64.8 show ipv6 source binding 606
64.9 show ipv6 dhcp snooping 607
64.10 show ipv6 dhcp snooping interface 607
64.11 show ipv6 nd snooping 608
64.12 show ipv6 nd snooping interface 608

Chapter 65 IP Verify Source Commands 610

65.1 ip verify source 610
65.2 ip verify source logging 611
65.3 show ip verify source 611
65.4 show ip verify source interface 612

Chapter 66 IPv6 Verify Source Commands 613

66.1 ipv6 verify source 613
66.2 show ipv6 verify source 614
66.3 show ipv6 verify source interface 614

Chapter 67 DHCPv4 Filter Commands 616

67.1 ip dhcp filter 616
67.2 ip dhcp filter (interface) 616
67.3 ip dhcp filter mac-verify 617
67.4 ip dhcp filter limit rate 618
67.5 ip dhcp filter decline rate 619
67.6 ip dhcp filter server permit-entry 620
67.7 show ip dhcp filter 621
67.8 show ip dhcp filter interface 621
67.9 show ip dhcp filter server permit-entry 622

Chapter 68 DHCPv6 Filter Commands 623

68.1 ipv6 dhcp filter 623
68.2 ipv6 dhcp filter (interface) 623
68.3 ipv6 dhcp filter limit rate 624
68.4 ipv6 dhcp filter decline rate 625
68.5 ipv6 dhcp filter server permit-entry 626
68.6 show ipv6 dhcp filter 627

68.7 show ipv6 dhcp filter interface 627
68.8 show ip dhcp filter server permit-entry 628

Chapter 69 DoS Defend Commands 629

69.1 ip dos-prevent 629
69.2 ip dos-prevent type 629
69.3 show ip dos-prevent 631

Chapter 70 sFlow Commands (Only for Certain Devices) 633

70.1 sflow address 633
70.2 sflow enable 634
70.3 sflow collector collector-ID 634
70.4 sflow sampler 635
70.5 show sflow global 636
70.6 show sflow collector 637
70.7 show sflow sampler 637

Chapter 71 Ethernet OAM Commands (Only for Certain Devices) 638

71.1 ethernet-oam 638
71.2 ethernet-oam mode 639
71.3 ethernet-oam link-monitor symbol-period 639
71.4 ethernet-oam link-monitor frame 640
71.5 ethernet-oam link-monitor frame-period 641
71.6 ethernet-oam link-monitor frame-seconds 643
71.7 ethernet-oam remote-failure 644
71.8 ethernet-oam remote-loopback received-remote- loopback 645
71.9 ethernet-oam remote-loopback 646
71.10 clear ethernet-oam statistics 646
71.11 clear ethernet-oam event-log 647
71.12 show ethernet-oam configuration 648
71.13 show ethernet-oam event-log 649
71.14 show ethernet-oam statistics 649
71.15 show ethernet-oam status 650

Chapter 72 DLDP Commands (Only for Certain Devices) 651

72.1 dldp (global) 651
72.2 dldp interval 651
72.3 dldp shut-mode 652
72.4 dldp reset (global) 653

72.5 dldp(interface) 653
72.6 dldp reset (interface) 654
72.7 show dldp 654
72.8 show dldp interface 655

Chapter 73 SNMP Commands 656

73.1 snmp-server 656
73.2 snmp-server view 656
73.3 snmp-server group 657
73.4 snmp-server user 659
73.5 snmp-server community 661
73.6 snmp-server host 661
73.7 snmp-server engineID 663
73.8 snmp-server traps snmp 664
73.9 snmp-server traps 665
73.10 snmp-server traps ddm 667
73.11 snmp-server traps vlan 668
73.12 snmp-server traps security 669
73.13 snmp-server traps security dhcp6-filter 669
73.14 snmp-server traps acl 670
73.15 snmp-server traps ip 670
73.16 snmp-server traps power (Only for Certain Devices) 671
73.17 snmp-server traps link-status 672
73.18 rmon history 673
73.19 rmon event 674
73.20 rmon alarm 675
73.21 rmon statistics 677
73.22 show snmp-server 677
73.23 show snmp-server view 678
73.24 show snmp-server group 678
73.25 show snmp-server user 679
73.26 show snmp-server community 679
73.27 show snmp-server host 680
73.28 show snmp-server engineID 680
73.29 show rmon history 680
73.30 show rmon event 681
73.31 show rmon alarm 682
73.32 show rmon statistics 682

Chapter 74 PoE Commands (Only for Certain Devices) 684

74.1 power inline consumption (global) 684
74.2 power profile 684
74.3 power inline consumption (interface) 686
74.4 power inline consumption (unit) 686
74.5 power inline priority 687
74.6 power inline supply 688
74.7 power inline profile 688
74.8 power inline time-range 689
74.9 show power inline 690
74.10 show power inline configuration interface 690
74.11 show power inline information interface 691
74.12 show power profile 691
74.13 power recovery ststus enable 692
74.14 power recovery status 692
74.15 show power recovery 693
74.16 show power recovery interface 694

Chapter 75 ARP Inspection Commands 695

75.1 ip arp inspection 695
75.2 ip arp inspection validate 695
75.3 ip arp inspection vlan 696
75.4 ip arp inspection vlan logging 697
75.5 ip arp inspection trust 698
75.6 ip arp inspection limit-rate 698
75.7 ip arp inspection burst-interval 699
75.8 ip arp inspection recover 700
75.9 ip arp inspection exceed 701
75.10 show ip arp inspection 701
75.11 show ip arp inspection interface 702
75.12 show ip arp inspection vlan 703
75.13 show ip arp inspection statistics 703
75.14 clear ip arp inspection statistics 704

Chapter 76 ND Detection Commands 705

76.1 ipv6 nd detection 705
76.2 ipv6 nd detection vlan 705
76.3 ipv6 nd detection vlan logging 706

76.4 ipv6 nd detection trust 706
76.5 show ipv6 nd detection 707
76.6 show ipv6 nd detection interface 708
76.7 show ipv6 nd detection statistics 708
76.8 show ipv6 nd detection vlan 709

Chapter 77 System Log Commands 710

77.1 logging buffer 710
77.2 logging buffer level 710
77.3 logging file flash 711
77.4 logging file flash frequency 712
77.5 logging file flash level 713
77.6 logging host index 713
77.7 logging console 714
77.8 logging console level 715
77.9 logging monitor 716
77.10 logging monitor level 716
77.11 clear logging 717
77.12 show logging local-config 718
77.13 show logging loghost 718
77.14 show logging buffer 719
77.15 show logging flash 719

Preface

This Guide is intended for network administrator to provide referenced information about CLI (Command Line Interface). The device mentioned in this Guide stands for Managed Switch without any explanation. Some models featured in this guide may be unavailable in your country or region. For local sales information, visit https://www.tp-link.com.

Overview of this Guide

Chapter 1: Using the CLI

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

Chapter 2: Line Commands (Only for Certain Devices)

Provide information about the commands used to make related configurations for the desired users and set the priority of the console media type.

Chapter 3: User Interface

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

Chapter 4: User Management Commands

Provide information about the commands used for user management.

Chapter 5: 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 6: File System Configuration Commands

Provide information about the commands used for configuring the File System.

Chapter 7: Management Port Configuration Commands

Provide information about the commands used for configuring the Management Port.

Chapter 8: EEE Configuration Commands

Provide information about the commands used for configuring EEE.

Chapter 9: SDM Template Commands

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

Chapter 10: Time Range Commands

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

Chapter 11: Port Configuration Commands

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

Chapter 12: Port Isolation Commands

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

Chapter 13: Loopback Detection Commands

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

Chapter 14: Stack Commands

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

Chapter 15: DDM Commands (Only for Certain Devices)

Provide information about the commands used for DDM (Digital Diagnostic Monitoring) function.

Chapter 16: Etherchannel Commands

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

Chapter 17: MAC Address Commands

Provide information about the commands used for Address configuration.

Chapter 18: IEEE 802.1Q VLAN Commands

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

Chapter 19: MAC-based VLAN Commands

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

Chapter 20: Protocol-based VLAN Commands

Provide information about the commands used for configuring Protocol VLAN.

Chapter 21: Private VLAN Commands (Only for Certain Devices)

Provide information about the commands used for configuring Private VLAN.

Chapter 22: VLAN-VPN Commands (Only for Certain Devices)

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

Chapter 23: ERPS Commands

Provide information about the commands used for configuring ERPS (Ethernet Ring Protection Switching) function.

Chapter 24: GVRP Commands

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

Chapter 25: IGMP Snooping Commands

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

Chapter 26: Layer 3 IGMP Commands (Only for Certain Devices)

Provide information about the commands used for configuring the layer 3 IGMP Snooping (Internet Group Management Protocol Snooping).

Chapter 27: PIM Commands (Only for Certain Devices)

Provide information about the commands used for configuring the PIM (Protocol Independent Multicast) function.

Chapter 28: Static Multicast Routing Commands (Only for Certain Devices)

Provide information about the commands used for configuring the Static Multicast Routing function.

Chapter 29: MLD Snooping Commands

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

Chapter 30: MVR Commands

Provide information about the commands used for configuring the MVR.

Chapter 31: MSTP Commands

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

Chapter 32: Debug Commands

Provide information about the commands used for configuring the debug funtion.

Chapter 33: LLDP Commands

Provide information about the commands used for configuring LLDP function.

Chapter 34: L2PT Commands (Only for Certain Devices)

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

Chapter 35: PPPoE ID-Insertion Commands (Only for Certain Devices)

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

Chapter 36: Static Routes Commands

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

Chapter 37: RIP Configuration Commands

Provide information about the commands used for configuring the RIP (Routing Information Protocol).

Chapter 38: RIPng Configuration Commands

Provide information about the commands used for configuring the RIP (RIP next generation).

Chapter 39: OSPF Configuration Commands

Provide information about the commands used for configuring the OSPF (Open Shortest Path First).

Chapter 40: OSPFv3 Configuration Commands

Provide information about the commands used for configuring the OSPFv3 (Open Shortest Path First version 3).

Chapter 41: IPv6 Address Configuration Commands

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

Chapter 42: ARP Commands

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

Chapter 43: VRRP Commands (Only for Certain Devices)

Provide information about the commands used for configuring VRRP (Virtual Router Redundancy Protocol).

Chapter 44: DHCP Server Commands

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

Chapter 45: DHCP Relay Commands

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

Chapter 46: DHCPV6 Relay Commands

Provide information about the commands used for configuring the DHCPV6 Relay function.

Chapter 47: DHCP L2 Relay Commands

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

Chapter 48: DHCPV6 L2 Relay Commands

Provide information about the commands used for configuring the DHCPV6 L2 Relay function.

Chapter 49: QoS Commands

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

Chapter 50: Bandwidth Control Commands

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

Chapter 51: Voice VLAN Commands

Provide information about the commands used for configuring Voice VLAN.

Chapter 52 Auto VoIP Commands

Provide information about the commands used for configuring Auto VoIP.

Chapter 53: Access Control Commands

Provide information about the commands used for configuring Access Control.

Chapter 54: HTTP and HTTPS Commands

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

Chapter 55: SSH Commands

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

Chapter 56: Telnet Commands

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

Chapter 57: Serial Port Commands (Only for Certain Devices)

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

Chapter 58: AAA Commands

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

Chapter 59: IEEE 802.1X Commands

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

Chapter 60: Port Security Commands

Provide information about the commands used for configuring Port Security.

Chapter 61: Port Mirroring Commands

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

Chapter 62: ACL Commands

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

Chapter 63: IPv4 IMPB Commands

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

Chapter 64: IPv6 IMPB Commands

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

Chapter 65: IP Verify Source Commands

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

Chapter 66: IPv6 Verify Source Commands

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

Chapter 67: DHCPv4 Filter Commands

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

Chapter 68: DHCPv6 Filter Commands

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

Chapter 69: DoS Defend Command

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

Chapter 70: sFlow Commands (Only for Certain Devices)

Provide information about the commands used for configuring the Sampled Flow function.

Chapter 71: Ethernet OAM Commands (Only for Certain Devices)

Provide information about the commands used for configuring the Ethernet OAM (Operation, Administration, and Maintenance) function.

Chapter 72: DLDP Commands (Only for Certain Devices)

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

Chapter 73: SNMP Commands

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

Chapter 74: PoE Commands (Only for Certain Devices)

Provide information about the commands used for configuring PoE function.

Chapter 75: ARP Inspection Commands

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

Chapter 76: ND Detection Commands

Provide information about the commands used for configuring ND detection.

Chapter 77: System Log Commands

Provide information about the commands used for configuring system log.

Chapter 1 Using the CLI

1.1 Accessing the CLI

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

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

1.1.1 Logon by a console port

Note: Console port is only available on certain devices.

- Console Port

The switch has two console ports: an RJ-45 console port and a Micro-USB console port. Console output is active on devices connected to both console ports, but console input is only active on one console port at a time.

The Micro-USB connector takes precedence over the RJ-45 connector. When the switch detects a valid connection on the Micro-USB console port, input from the RJ-45 console port is immediately disabled, and input from the Micro-USB console port is enabled. Removing the Micro-USB connection immediately reenables input from the RJ-45 console connection.

- USB Console Driver

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

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

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

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

- 64-bit Windows 7
- 32-bit Windows 8
- 64-bit Windows 8
- 32-bit Windows 8.1
- 64-bit Windows 8.1
- 32-bit Windows 10
- 64-bit Windows 10

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

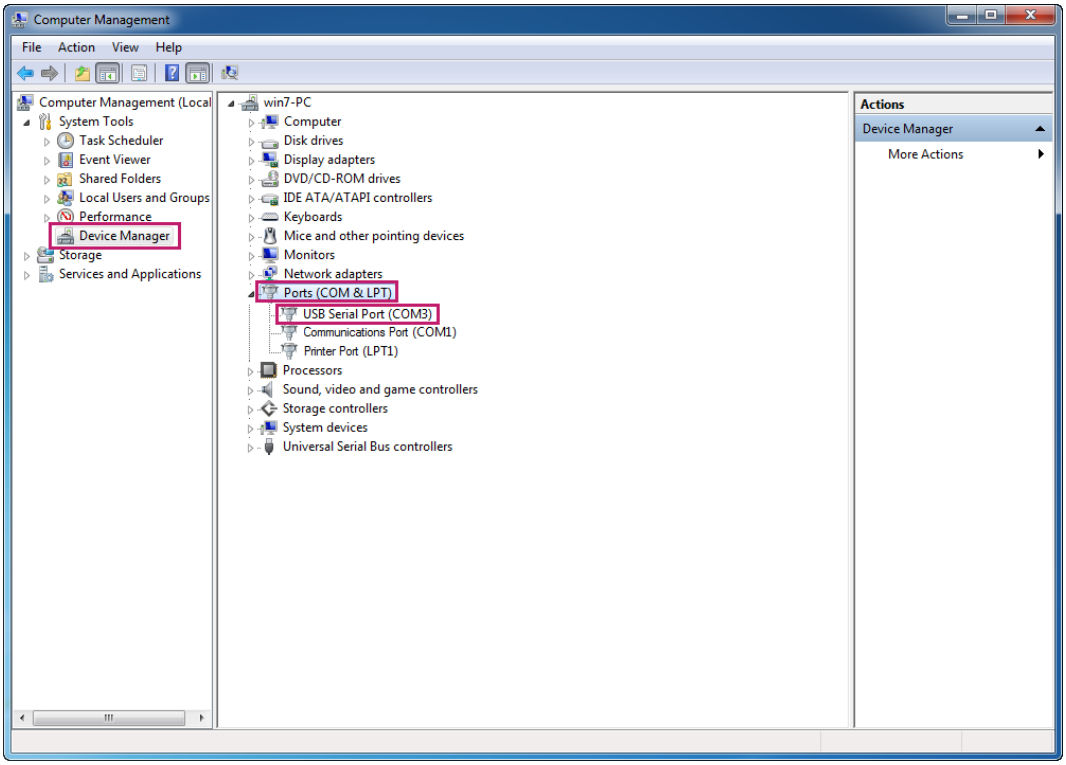
- Logon

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

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

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

Figure 1-1 USB Serial Port Number

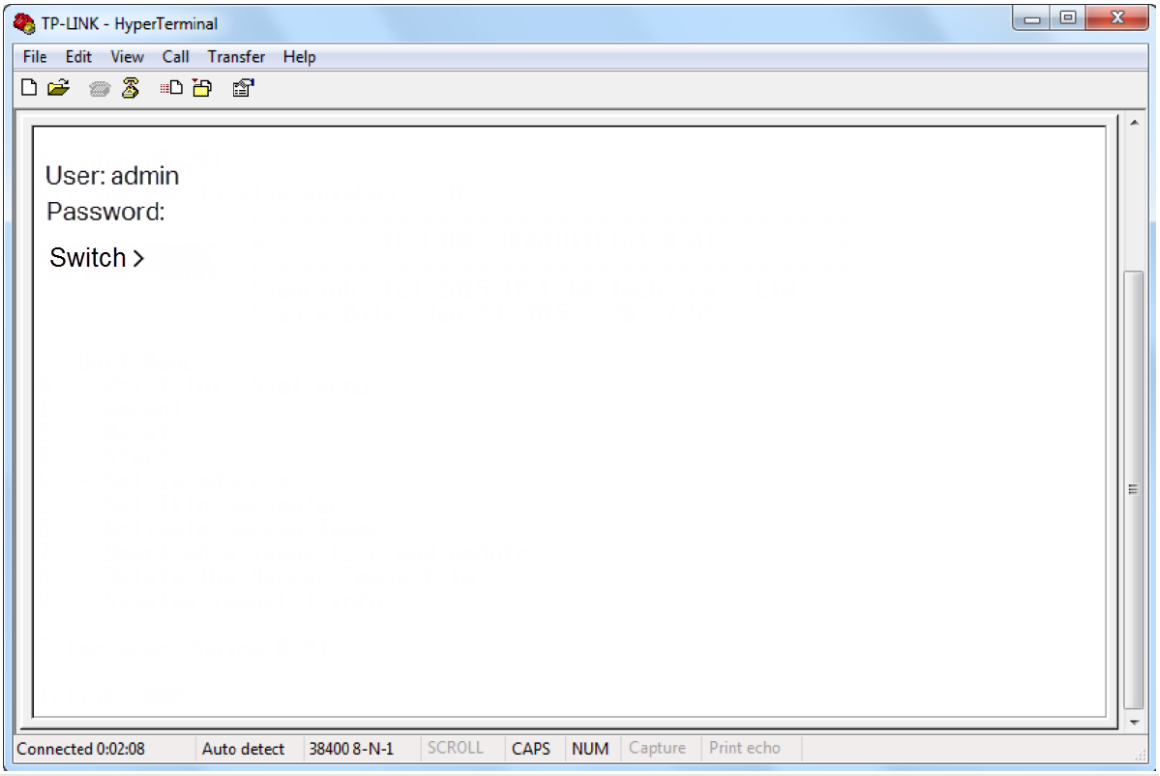


4. Configure the terminal emulation program or the terminal to use the following settings:

- Baud rate: 38400 bps
- Data bits: 8
- Parity: none
- Stop bits: 1
- Flow control: none

5. Type the Username and Password in the Hyper Terminal window. The default value for both of them are **admin**. Press **Enter** in the main window and "Switch>" will appear indicating that you have successfully logged in to the switch and you can use the CLI now.

Figure 1-2 Log in to the Switch



Note: The first time you log in, change the password to better protect your network and devices.

1.1.2 Logon by Telnet

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

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

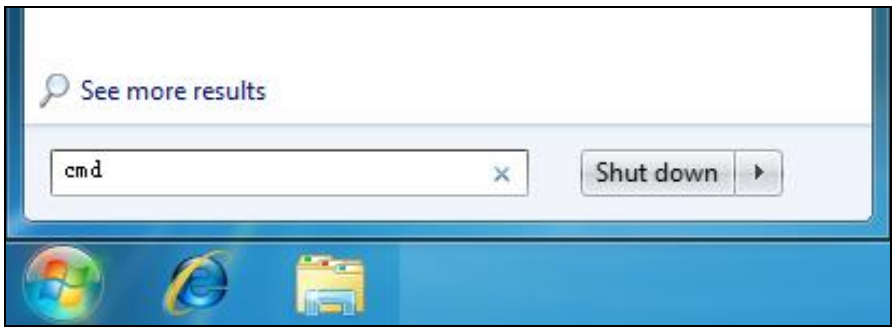


Figure 1-1 Run Window

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

Figure 1-2 Type in the telnet command

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

Figure 1-2 Log in the Switch

Note: The first time you log in, change the password to better protect your network and devices.

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

Figure 1-3 Enter into Priviledged EXEC Mode

1.1.3 Logon by SSH

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

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

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

Note:

1. Before SSH login, please follow the steps shown in Figure 1-4 to enable the SSH function through Telnet connection, which is enabled by default for some models.
2. The first time you log in, change the password to better protect your network and devices.

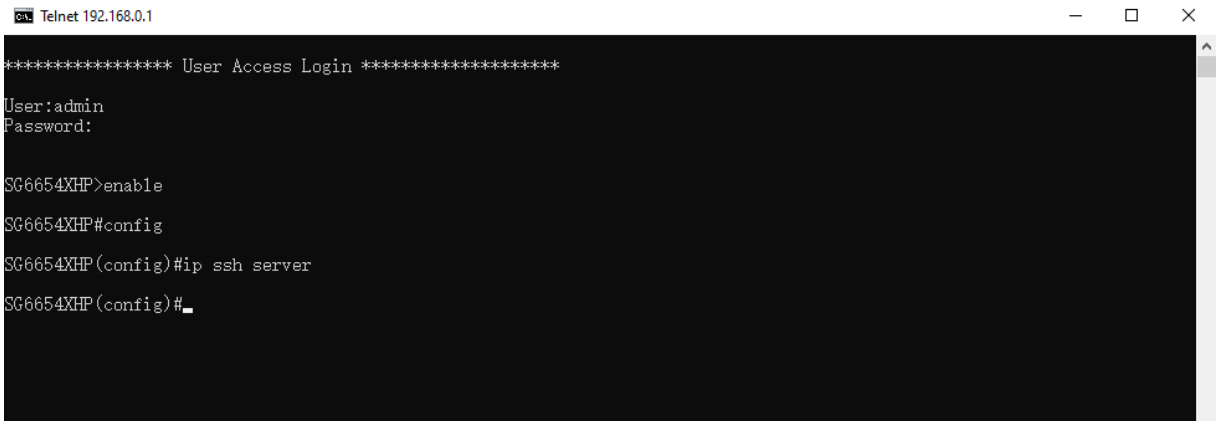


Figure 1-4 Enable SSH function

■ **Password Authentication Mode**

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

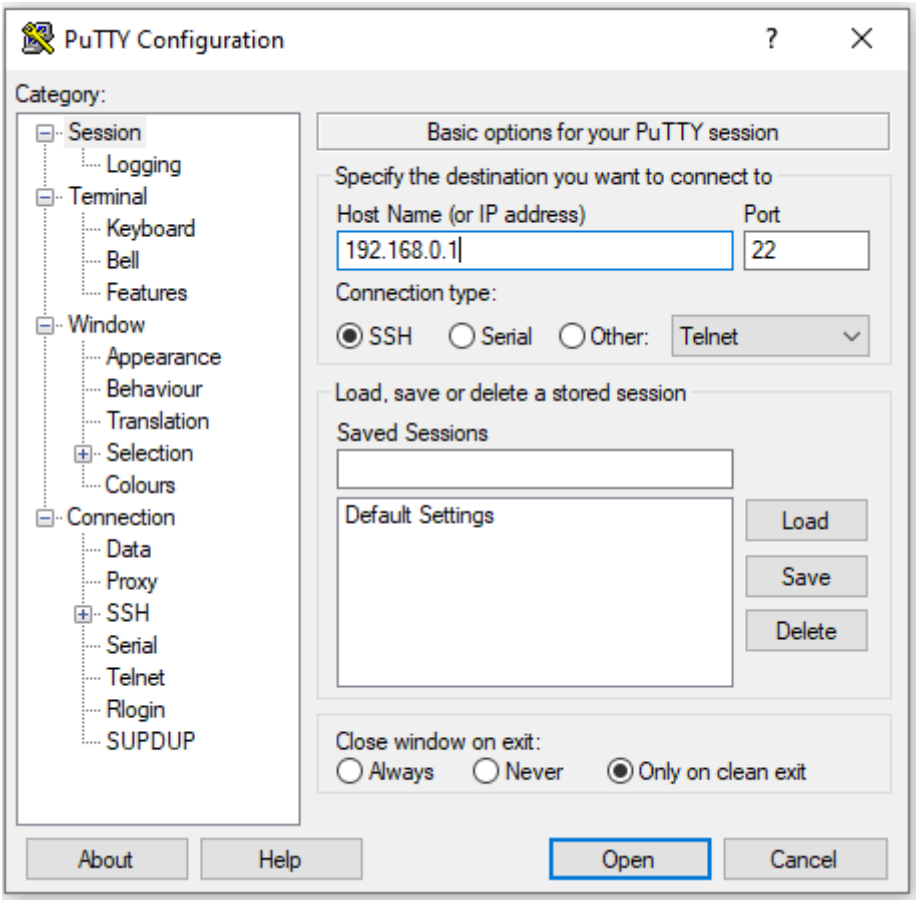


Figure 1-5 SSH Connection Config

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

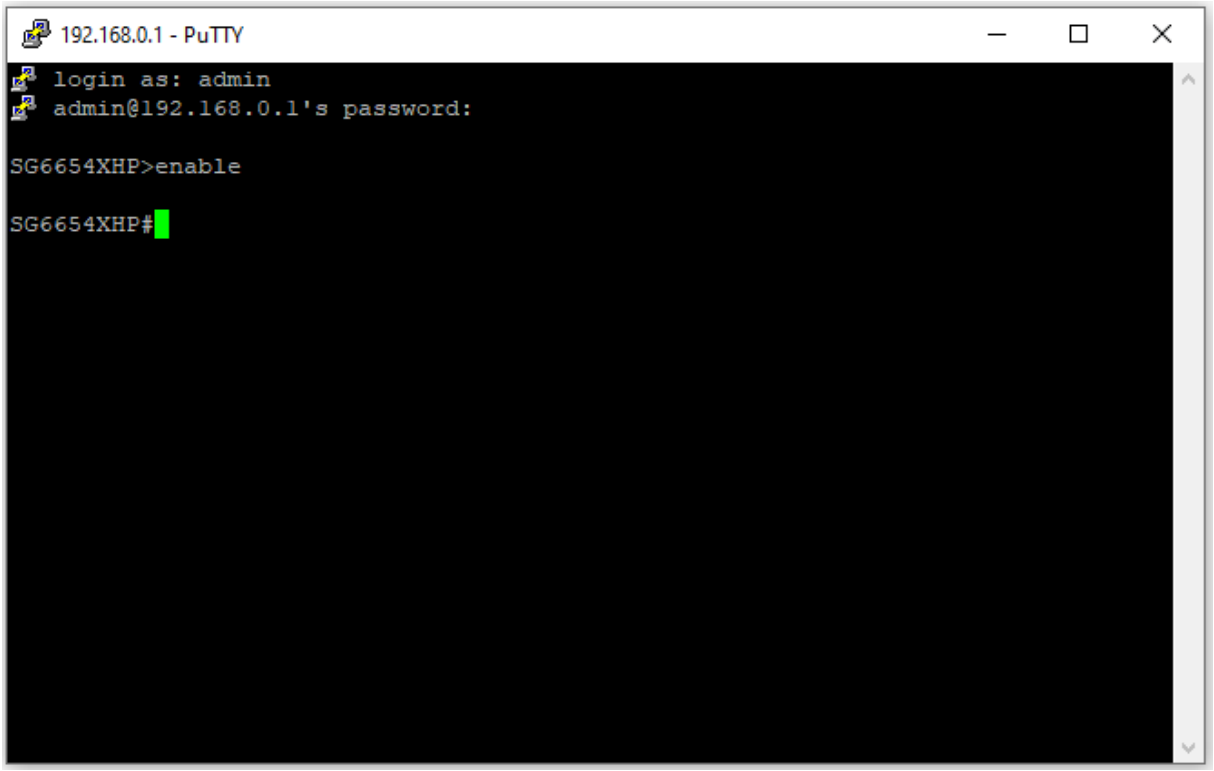


Figure 1-6 Log on the Switch

■ **Key Authentication Mode**

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

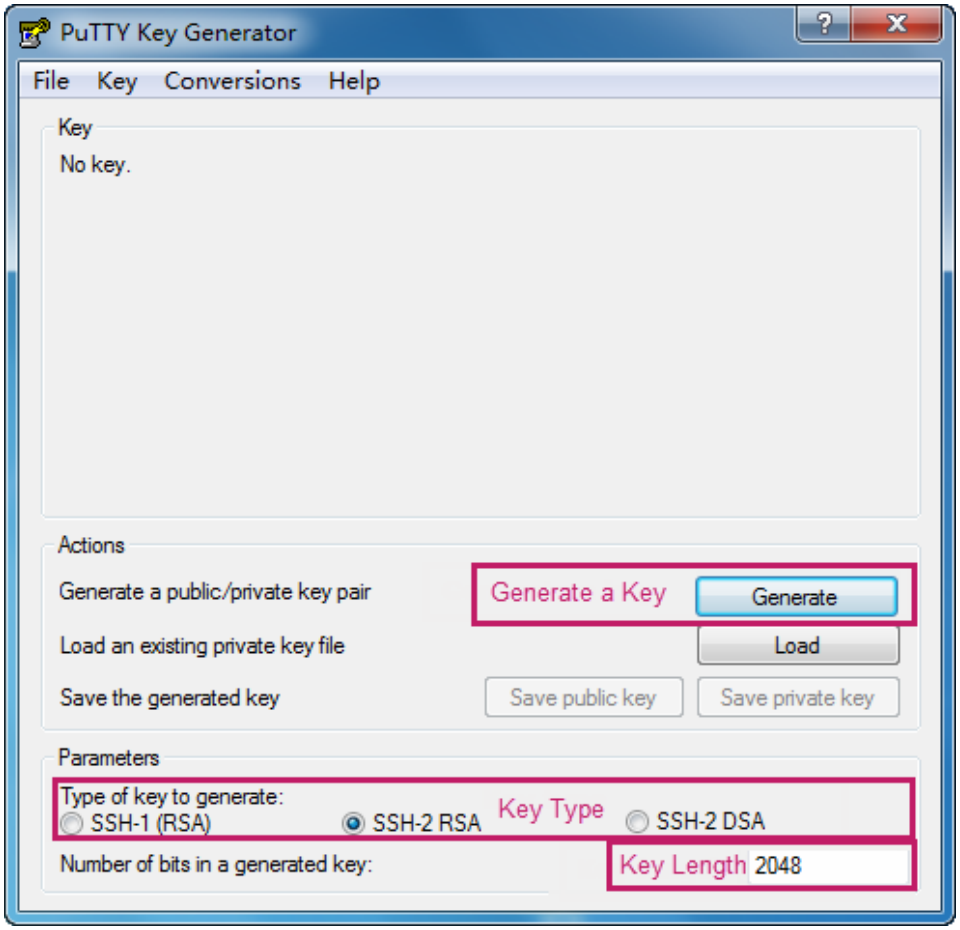


Figure 1-7 Generate SSH Key

Note:

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

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

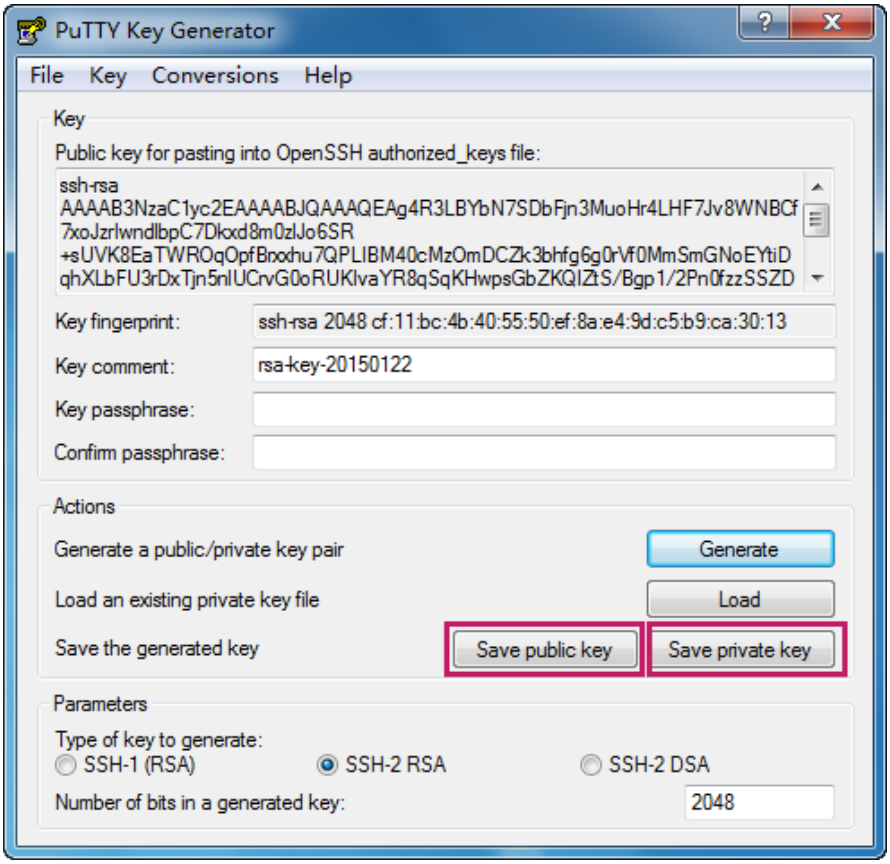


Figure 1-8 Save the Generated Key

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

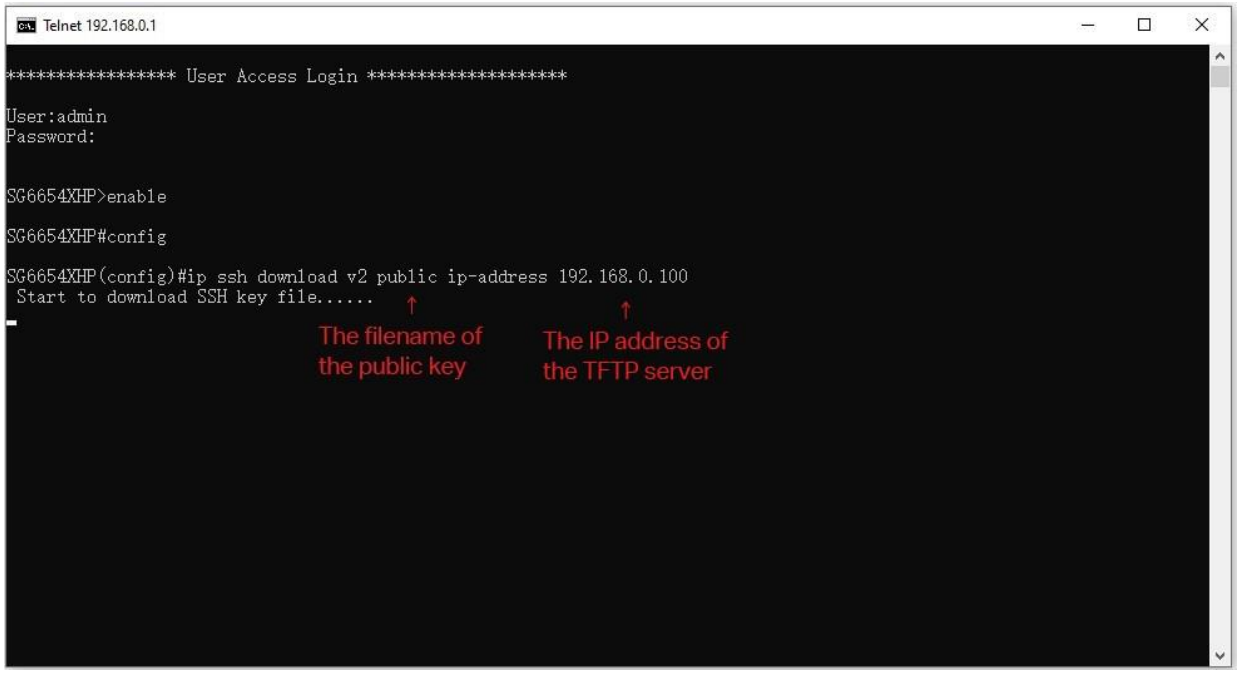


Figure 1-9 Download the Public Key

Note:

1. The key type should accord with the type of the key file.
2. The SSH key downloading cannot be interrupted.

5. After the public key is downloaded, please log on to the interface of PuTTY and enter the IP address for login.

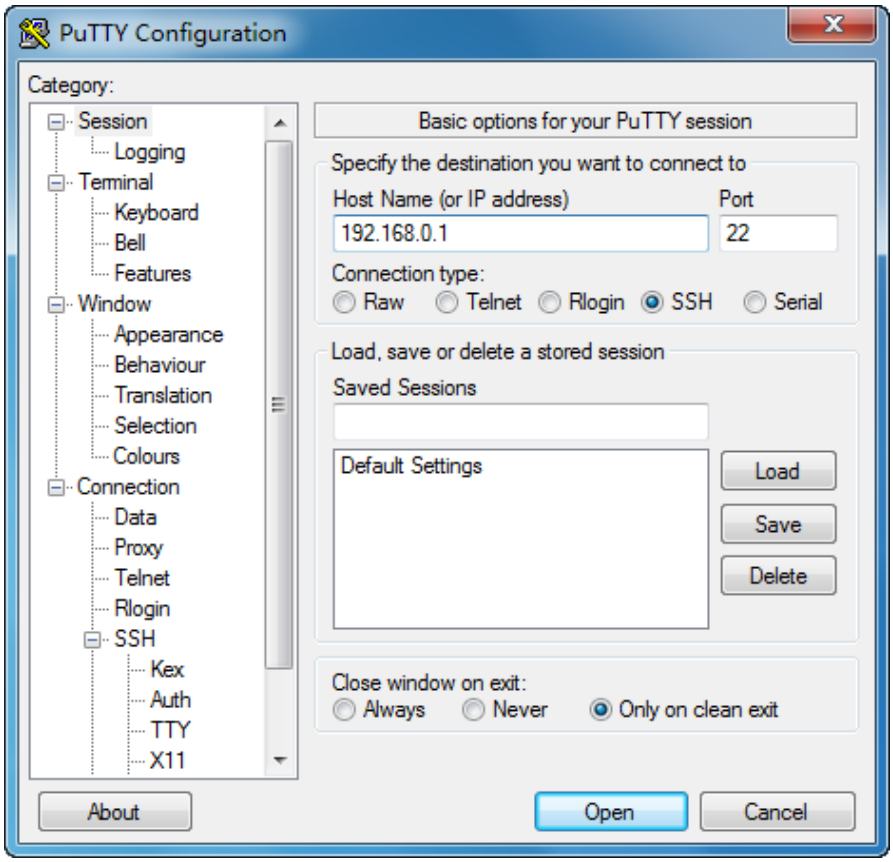


Figure 1-10 SSH Connection Config

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

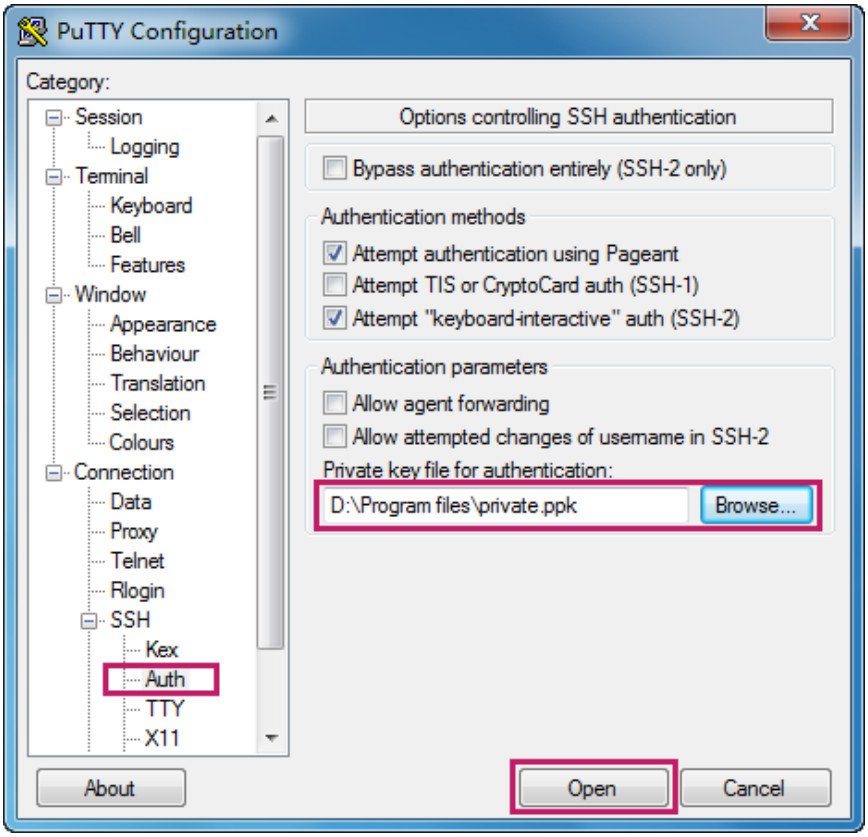


Figure 1-11 Download the Private Key

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

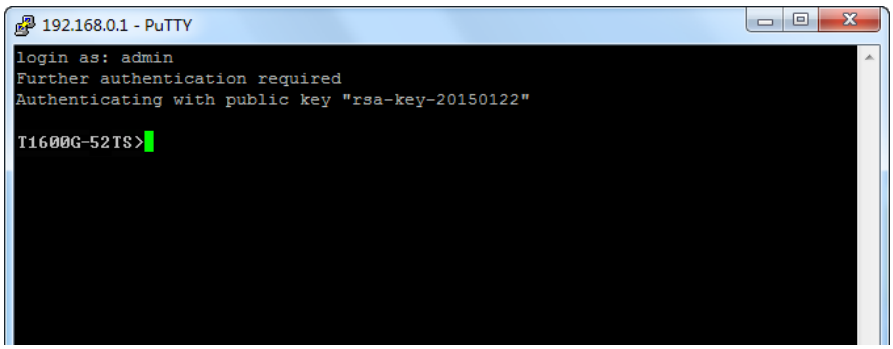


Figure 1-12 Log on the Switch

1.2 CLI Command Modes

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

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

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

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

Mode	Accessing Path	Prompt	Logout or Access the next mode
Interface Configuration Mode	Layer 3 Interface: Use the **no switchport** command to enter Routed Port mode from Interface Configuration mode. Use the **interface vlan** *vlan-id* command to enter VLAN Interface mode from Global Configuration mode. Use the **interface loopback** *id* command to enter Loopback Interface mode from Global Configuration mode.	**Switch (config-if)#** or **Switch(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.
Router Configuration Mode	Layer 3 Interface: Use the **router rip** or **router ripng** command to enter this mode from Global Configuration mode.	**Switch (config-router)**	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.
VLAN Configuration Mode	Use the **vlan** *vlan-list* command to enter this mode from Global Configuration mode.	**Switch (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. Global Configuration Mode/Interface Configuration Mode/VLAN Configuration Mode is only available in standalone mode.
3. 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 fastEthernet/gigabitEthernet/two-gigabitEthernet/ten-gigabitEthernet: Configure parameters for a fastEthernet/gigabitEthernet/two-gigabitEthernet/ten-gigabitEthernet port, such as Duplex-mode, flow control status.

  b). Interface range fastEthernet/gigabitEthernet/two-gigabitEthernet/ten-gigabitEthernet: Configure parameters for several fastEthernet/gigabitEthernet/two-gigabitEthernet/ten-gigabitEthernet 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.

4. Some commands are global, that means they can be performed in all modes:

   - **show**: Display all information of switch, for example: statistic information, port information, VLAN information.
   - **history**: Display the commands history.

1.3 Privilege Restrictions

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

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

1.4 Conventions

1.4.1 PoE Disclaimer

PoE budget calculations are based on laboratory testing. Actual PoE power budget is not guaranteed and will vary as a result of client limitations and environmental factors.

1.4.2 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*

1.4.3 Special Characters

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

- These six characters " < > , \ & cannot be input.

- If a blank is contained in a character string, single or double quotation marks should be used, for example 'hello world', "hello world", and the words in the quotation marks will be identified as a string. Otherwise, the words will be identified as several strings.

1.4.4 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 Line Commands (Only for Certain Devices)

Note: Line Commands are only available on certain devices.

2.1 line

Description

The line command is used to enter the Line Configuration Mode and make related configurations for the desired user(s).

Syntax

line { console linenum | vty startlinenum endlinenum }

Parameter

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

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

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

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

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

```
Switch(config)#line console 0
```

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

```
Switch(config)#line vty 0 5
```

2.2 media-type rj45

Description

The media-type rj45 command is used to configure the console media type as RJ-45 for input. The switch has two console ports available —— an RJ-45 console port and a micro-USB console port. Console input is active on only one console port at a time. By default, the micro-USB connector takes precedence over the RJ-45 connector, which means that, when both the RJ-45 console connection and micro-USB console connection are valid, input from the RJ-45 console is disabled, and input from the micro-USB console is enabled. To return to the default configuration, please use no media-type rj45 command.

Syntax

media-type rj45

no media-type rj45

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the RJ-45 console input:

```
Switch(config)# line console 0
Switch(config-line)# media-type rj45
```

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

```
Switch(config)# line console 0
Switch(config-line)# no media-type rj45
```

Chapter 3 User Interface

3.1 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:

```
Switch>enable
Enter password:
Switch#
```

3.2 service password-encryption

Description

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

Syntax

service password-encryption

no service password-encryption

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the global encryption function:

Switch(config)# service password-encryption

3.3 enable password

Description

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

Syntax

enable password { [0] *password* | 7 *encrypted-password* }
no enable password

Parameter

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

password —— A string with 31 characters at most, which can contain only English letters (case-sensitive), digits and 17 kinds of special characters. The special characters are **!$%'()*,-./[]_{|}**. 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.

If both the **enable password** and **enable secret** are defined, only the latest configured password will take effect.

Example

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

Switch(config)#enable password 0 admin

3.4 enable secret

Description

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

Syntax

enable secret { [0] *password* **|** 5 *encrypted-password*}

no enable secret

Parameter

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

password —— A string with 31 characters at most, which can contain only English letters (case-sensitive), digits and 17 kinds of special characters. The special characters are **!$%'()*,-./[]_{|}**. 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, only the latest configured password will take effect.

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.

Switch(config)#enable secret 0 admin

3.5 configure

Description

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

Syntax

configure

Command Mode

Privileged EXEC Mode

Privilege Requirement

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

Example

Access Global Configuration Mode from Privileged EXEC Mode:

Switch# configure
Switch (config)#

3.6 exit

Description

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

Syntax

exit

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

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

```
Switch (config-if)# exit
Switch (config)#exit
Switch#
```

3.7 end

Description

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

Syntax

end

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Return to Privileged EXEC Mode from Interface Configuration Mode:

```
Switch (config-if)#end
Switch #
```

3.8 clipaging

Description

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

Syntax

clipaging

no clipaging

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Disable the pause function for the screen display:

```
Switch (config)#no clipaging
```

3.9 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:

```
Switch (config)# history
    1 history
```

3.10 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:

```
Switch (config)#history clear
```

Chapter 4 User Management Commands

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

4.1 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. It contains 16 characters at most, composed of digits, English letters and symbols. No spaces, question marks and double quotation marks are allowed.

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 with 6–31 alphanumeric characters (case-sensitive) and symbols. No spaces are allowed.

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.

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" and unencrypted:

Switch(config)#user name tplink **privilege** admin **password** 0 admin

4.2 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. It contains 16 characters at most, composed of digits, English letters and symbols. No spaces, question marks and double quotation marks are allowed.

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.

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 with 6–31 alphanumeric characters (case-sensitive) and symbols. No spaces are allowed.

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.

Switch (config)#user name tplink **privilege** admin **secret** 0 admin

4.3 service password-recovery

Note: This command is only available on certain devices.

Description

The **service password-recovery** command is used to enable the password-recovery feature. To disable the password-recovery feature, please use **no service password-recovery** command.

With password-recovery enabled, you can connect to the switch’s console port and delete all your previous set accounts. You can use the default

username and password (which are both admin) to login the switch after its startup.

Syntax

service password-recovery

no service password-recovery

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the switch's password-recovery feature:

```
Switch(config)# service password-recovery
```

4.4 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:

```
Switch (config)# show user account-list
```

4.5 show user configuration

Description

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

Syntax

show user configuration

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the security configuration information of the users:

```
Switch (config)# show user configuration
```

Chapter 5 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.

5.1 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

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

5.2 system-time ntp

Description

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

Syntax

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

Parameter

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

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

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

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

UTC-10:00 —— TimeZone for Hawaii.

UTC-09:00 —— TimeZone for Alaska.

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

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

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

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

UTC-04:30 —— TimeZone for Caracas.

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

UTC-03:30 —— TimeZone for Newfoundland.

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

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

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

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

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

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

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

UTC+03:30 —— TimeZone for Tehran.

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

UTC+04:30 —— TimeZone for Kabul.

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

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

UTC+05:45 —— TimeZone for Kathmandu.

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

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

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

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

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

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

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

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

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

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

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

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

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

Switch(config)# system-time ntp UTC-12:00 133.100.9.2 139.79.100.163 11

5.3 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:

Switch(config)#system-time dst predefined USA

5.4 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:

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

5.5 system-time dst recurring

Description

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

Syntax

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

no system-time dst

Parameter

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

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

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

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

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

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

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

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

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

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

5.6 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 "SG6654XHP".

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the system name as TP-Link

Switch(config)# hostname TP-Link

5.7 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 "Hong Kong" 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 Hong Kong:

Switch(config)# location Hong Kong

5.8 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:

Switch(config)# contact-info www.tp-link.com

5.9 led

Note: This command is only available on certain devices.

Description

The **led** command is used to control the LEDs.

Syntax

led {on | off}

Parameter

on | off—— The LEDs are configured as on or off. By default, they are on.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the LED as off:

Switch(config)# led off

5.10 ip address

Description

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

Syntax

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

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

Parameter

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

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

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

Command Mode

Interface Configuration Mode

Privilege Requirement

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

Example

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

Switch (config)# interface vlan 2
Switch (config-if)# ip address 192.168.1.1 255.255.255.0
Switch (config-if)# ip address 192.168.2.1 255.255.255.0 **secondary**

5.11 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

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

Switch (config)# interface gigabitEthernet 1/0/1

Switch (config-if)# no switchport

Switch (config-if)# ip address-alloc dhcp

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

Switch (config)# interface vlan 2

Switch (config-if)# no ip address

5.12 controller cloud-based (Only for Certain Devices)

Note: This command is only available on certain devices

Description

The **controller cloud-based** command is used to enable Cloud-Based Controller managment. When this feature is enabled, you can further add your devices to your Omada Cloud-Based Controller. To disable the feature, use the **no controller cloud-based** command.

Syntax

controller cloud-based

no controller cloud-based

Command Mode

Global Configuration Mode

Privilege Requirement

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

5.13 controller inform-url (Only for Certain Devices)

Note: This command is only available on certain devices

Description

If your switch and Omada SDN Controller are not located on the same subnet, the **controller inform-url** command is used to inform the switch of the controller's URL/IP address. To disable the feature, use the **no controller inform-url** command.

Syntax

controller inform-url { controller-url | controller-ip }

no controller inform-url

Parameter

controller-url —— Specify the URL of Omada SDN Controller.

controller-ip —— Specify the IP address of Omada SDN Controller.

Command Mode

Gloabal Configuration Mode

Privilege Requirement

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

Example

Inform the switch of the controller whose IP address is 192.168.1.1:

Switch (config)# controller inform-url 192.168.1.1

5.14 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 [**except-ip**]

Parameter

except-ip ——Maintain the IP address when resetting the switch.

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Reset all settings of the switch except its IP address:

Switch # reset except-ip

5.15 service reset-disable

Description

The **service reset-disable** command is used to disable the reset function of the console port or reset button. To enable the reset function, use **no service reset-disable** command. By default, the reset function is enabled.

Syntax

service reset-disable

no service reset-disable

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Disable the reset function of console port or reset button:

```
Switch (config)# service reset-disable
```

5.16 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:

```
Switch # reboot
```

5.17 reboot-schedule

Description

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

Syntax

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

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

reboot-schedule cancel

Parameter

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

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

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

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

cancel —— Delete the reboot schedule settings.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

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

Example

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

Switch (config)# reboot-schedule in 200 **save_before_reboot**

5.18 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:

Switch # copy running-config startup-config

5.19 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:

Switch # 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:

Switch # copy startup-config tftp ip-address fe80::1234 **filename** config

5.20 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:

Switch # 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

Switch # copy tftp startup-config ip-address fe80::1234 **filename** config

5.21 copy backup-config tftp

Description

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

Syntax

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

Parameter

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

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

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

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

Switch # copy backup-config tftp ip-address 192.168.0.148 **filename** config

5.22 copy backup-config startup-config

Description

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

Syntax

copy backup-config startup-config

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

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

```
Switch # copy backup-config startup-config
```

5.23 copy running-config backup-config

Description

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

Syntax

copy running-config backup-config

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Save the current running configuration as the backup configuration file.

```
Switch # copy running-config backup-config
```

5.24 copy tftp backup-config

Description

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

Syntax

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

Parameter

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

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

Command Mode

Privileged EXEC Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Download the configuration file named config.cfg from the TFTP server with the IP 192.168.0.148:

Switch # copy tftp backup-config ip-address 192.168.0.148 **filename** config

5.25 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:

Switch (config)# boot application filename image2 startup

5.26 boot config

Description

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

Syntax

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

no boot application

Parameter

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

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

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the config2.cfg as the startup image:

Switch (config)# boot config filename config2 startup

5.27 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:

Switch # remove backup-image

5.28 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 choose whether to reboot the switch with the Backup Image.

Syntax

firmware upgrade 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 of the desired 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:

Switch # firmware upgrade tftp 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:

Switch # firmware upgrade tftp 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

5.29 mcu-firmware unit upgrade

(Only for Certain Devices)

Description

The **mcu-firmware unit upgrade** command is used to upgrade the switch's MCU-firmware online.

Syntax

mcu-firmware unit {*unit id***} type** {*mcu-type*} **upgrade**

Parameter

unit id —— Stack unit ID, ranging from 1 to 4.

mcu-type —— MCU device type, which can be pse, crps, fan, monitor.

Command Mode

None

Privilege Requirement

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

Example

Upgrade the switch's MCU-firmware online:

Switch#mcu-firmware unit 1 type pse upgrade

5.30 mcu-firmware type (Only for Certain Devices)

Description

The **mcu-firmware type** command is used to display the MCU version information.

Syntax

mcu-firmware type {*mcu-type*} **version**

Parameter

mcu-type —— MCU device type, which can be pse, crps, fan, monitor.

Command Mode

None

Privilege Requirement

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

Example

Upgrade the switch's MCU-firmware online:

Switch#mcu-firmware unit 1 type pse upgrade

5.31 boot autoinstall start

Note: This command is only available on certain devices.

Description

The **boot autoinstall start** command is used to start Auto Install function. To stop the Auto Install function, use **no boot autoinstall start**.

Syntax

boot autoinstall start

no boot autoinstall start

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Start Auto Install function:

```
Switch(config)# boot autoinstall start
```

5.32 boot autoinstall persistent-mode

Note: This command is only available on certain devices.

Description

The **boot autoinstall persistent-mode** command is used to start Auto Install function to next reboot cycle. To disable persistent mode, use **no boot autoinstall persistent-mode**.

Syntax

boot autoinstall persistent-mode

no boot autoinstall persistent-mode

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Start Auto Install function:

```
Switch(config)# boot autoinstall persistent-mode
```

5.33 boot autoinstall auto-save

Note: This command is only available on certain devices.

Description

The **boot autoinstall auto-save** command is used to automatically save the new configuration file that was downloaded by Auto Install function to start-up configuration file Auto Install. To disable auto-save configuration feature use **no boot autoinstall auto-save**.

Syntax

boot autoinstall auto-save

no boot autoinstall auto-save

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure Auto Install function to auto-save new configuration file to start-up configuration file:

```
Switch(config)# boot autoinstall auto-save
```

5.34 boot autoinstall auto-reboot

Note: This command is only available on certain devices.

Description

The **boot autoinstall auto-reboot** command is used to automatically reboot the switch after Auto Install function is completed successfully. To disable auto-reboot feature use **no boot autoinstall auto-reboot**.

Syntax

boot autoinstall auto-reboot

no boot autoinstall auto-reboot

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the switch to auto reboot after Auto Install function completed successfully:

```
Switch(config)# boot autoinstall auto-reboot
```

5.35 boot autoinstall retry-count

Note: This command is only available on certain devices.

Description

The **boot autoinstall retry-count** command is used to configure retry count when Auto Install function uses TFTP to download configuration files in a cycle of Auto Install process. To set retry count to default value use **no boot autoinstall retry-count**.

Syntax

boot autoinstall retry-count *count*

no boot autoinstall retry-count

Parameter

count —— The count of retrying auto install. The value ranges from 1 to 3.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure TFTP retry 2 times when download files failed:

Switch(config)# boot autoinstall retry-count 2

5.36 show boot autoinstall

Note: This command is only available on certain devices.

Description

The **show boot autoinstall** command is used to display the configuration of Auto Install function.

Syntax

show boot autoinstall

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of Auto Install function:

Switch# show boot autoinstall

5.37 show boot autoinstall downloaded-config

Note: This command is only available on certain devices.

Description

The **show boot autoinstall downloaded-config** command is used to display the configuration file which downloaded by Auto Install.

Syntax

show boot autoinstall downloaded-config

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration file which downloaded by Auto Install:

Switch# show boot autoinstall downloaded-config

5.38 ping

Description

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

Syntax

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

Parameter

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

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

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

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

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

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

Command Mode

Privileged EXEC Mode

Privilege Requirement

None.

Example

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

Switch # 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:

Switch # ping fe80::1234 **–n** 8 **–l** 512

5.39 tracert

Description

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

Syntax

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

Parameter

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

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

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

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

Command Mode

Privileged EXEC Mode

Privilege Requirement

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

Example

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

Switch # 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:

Switch # tracert fe80::1234 20

5.40 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:

```
Switch # show system-info
```

5.41 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:

```
Switch# show image-info
```

5.42 show boot

Description

The **show boot** command is used to display the boot configuration of the system.

Syntax

show boot

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the system boot configuration information:

Switch# show boot

5.43 show running-config

Description

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

Syntax

show running-config [*unit* {**all** | **|** [**exclude** *keyword*] [**include** *keyword*] | **interface** {**fastEthernet** |**gigabitEthernet** | **ten-gigabitEthernet**} *port*}]

show running-config [**all** | **|** [**exclude** *keyword*] [**include** *keyword*] | **interface** {**fastEthernet** |**gigabitEthernet** | **ten-gigabitEthernet**} *port*]

Parameter

unit—— Specify the unit number of a switch to show the unit's operating configurations. By default, it is 1.

all—— Display all the operating configurations of the whole system or a specified unit.

|—— Enable filter to filtrate the configurations. You can use **exclude** and **include** to set the filter rule.

keyword—— The filter conditions, such as interface, vlan, and user.

port —— Specify the number of the port to show the port's operating configurations.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the current operating configurations only related to the user:

Switch# show running-config | include user

5.44 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:

```
Switch# show startup-config
```

5.45 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

```
Switch# show system-time
```

5.46 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

```
Switch# show system-time dst
```

5.47 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:

```
Switch# show system-time ntp
```

5.48 show cable-diagnostics interface

Description

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

Syntax

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

Parameter

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

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Show the cable-diagnostics of port 3:

Switch# show cable-diagnostics interface gigabitEthernet 1/0/3

5.49 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:

Switch# show cpu-utilization

5.50 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:

Switch# show memory-utilization

5.51 show controller

Note: This command is only available on certain devices.

Description

The **show controller** command is used to display the current controller settings and status.

Syntax

show controller

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the current controller settings and status:

Switch# show controller

5.52 show temperature

Note: This command is only available on certain devices.

Description

The **show temperature** command is used to display the temperature of switch.

Syntax

show temperature

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the temperature information of the switch:

Switch-DC# show temperature

5.53 show voltage

Note: This command is only available on certain devices.

Description

The **show voltage** command is used to display the voltage of DC power board.

Syntax

show voltage

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the voltage information of the switch:

Switch # show voltage

5.54 clear config interace

Description

The **clear config interace** command is used to clear all configurations of a specified port.

Syntax

clear config interace [**fastEthernet | gigabitEthernet | two-gigabitEthernet | ten-gigabitEthernet | port-channel**] *port*

Parameter

port —— The port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Clear all configurations of gigabitEthernet port 1/0/3:

Switch(config)# clear config interace gigabitEthernet 1/0/3

5.55 power backup unit (Only for Certain Devices)

Description

The **power backup unit** command is used to configure the power backup mode.

Syntax

power backup unit {*unit id*} {*power*} **mode** {*mode*}

Parameter

unit id —— Stack unit ID, ranging from 1-4.

power—— power supply module number.

mode—— Power backup mode

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the power backup mode of stack unit 1:

```
Switch(config)#power backup unit 1 pwr1 mode enable
```

5.56 show power (Only for Certain Devices)

Description

The **show power** command is used to display the power details.

Syntax

show power [detail**]**

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the power details:

```
Switch#show power
```

Chapter 6 File System Configuration Commands

(Only for Certain Devices)

File System Commands can be used to configure the File System.

6.1 copy

Description

The **copy** command is used to copy the specified file.

Syntax

copy {flash|usbflash1|usbflash2} {filename} {destination}

Parameter

flash|usbflash1|usbflash2 —— The flash type of the source file.

filename —— File name.

destination —— Copied file path.

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

Copy the specified file:

```
Switch#copy flash test.txt usbflash1
```

6.2 cd

Description

The **cd** command is used to change the current file path.

Syntax

cd {filename|flash|usbflash1|usbflash2} [filename]

Parameter

filename|flash|usbflash1|usbflash2 —— The path that needs to be switched. If you enter filename, the file will be found in the current path by default.

filename —— Specify the file in the corresponding flash.

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

Change the current file path:

```
Switch# cd usbflash1 test
```

6.3 dir

Description

The **dir** command is used to list files and subdirectories contained in the specified working directory.

Syntax

dir [flash|usbflash1|usbflash2] [filename]

Parameter

flash|usbflash1|usbflash2 —— Specify path.

filename —— Specify the file in the corresponding flash.

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

List files and subdirectories contained in the specified working directory:

```
Switch#dir flash
```

6.4 pwd

Description

The **pwd** command is used to display the absolute path name of the current working directory.

Syntax

pwd

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 absolute path name of the current working directory:

```
Switch#pwd
```

6.5 rename

Description

The **rename** command is used to rename a file.

Syntax

rename {srcFilename} {dstFilename}

Parameter

srcFilename —— Source file name.

dstFilename —— Renamed file name.

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

Rename a file:

```
Switch#rename test1 test2
```

6.6 delete

Description

The **delete** command is used to delete a file.

Syntax

delete {filename|flash|usbflash1|usbflash2} [filename]

Parameter

filename|flash|usbflash1|usbflash2 —— The file that needs to be deleted. If you enter filename, the file will be found in the current working path by default.

filename —— Specify the file in the corresponding flash.

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

Delete a file:

```
Switch# delete text.txt
```

6.7 ftp

Description

The **ftp** command is used to enter the FTP (File Transfer Protocol) view.

Syntax

ftp

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

Enter the FTP view:

```
Switch#ftp
```

6.8 open

Description

The **open** command is used to connect to FTP server.

Syntax

open [ipv6] {hostIp}

Parameter

ipv6—— Specify the FTP server type as IPv6.

hostIp —— FTP server IP.

Command Mode

FTP Configuration Mode

Privilege Requirement

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

Example

Connect to FTP server:

```
Switch(ftp)#open 192.168.0.146
```

6.9 put

Description

The **put** command is used to upload files to FTP server.

Syntax

put {srcFilename} {dstFilename}

Parameter

srcFilename —— Source file name.

dstFilename —— Destination file name.

Command Mode

FTP Configuration Mode

Privilege Requirement

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

Example

Upload files to FTP server:

```
Switch(ftp)#put src.c dst.c
```

6.10 get

Description

The **get** command is used to download files from FTP server.

Syntax

get {srcFilename} {dstFilename}

Parameter

srcFilename —— Source file name.

dstFilename —— Destination file name.

Command Mode

FTP Configuration Mode

Privilege Requirement

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

Example

Download files from FTP server:

```
Switch(ftp)#get src.c dst.c
```

6.11 close

Description

The **close** command is used to close current FTP connection.

Syntax

close

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

Close current FTP connection:

```
Switch#close
```

Chapter 7 Management Port Configuration Commands (Only for Certain Devices)

7.1 management-port protocol

Description

The **management-port protocol** command is used to enable or disable the IPv4 DHCP funtion on the management port.

Syntax

management-port protocol {*dhcp*|*none*}

Parameter

dhcp——Enable the DHCP function

none—— Disable the DHCP function

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the IPv4 DHCP funtion on the management port:

```
Switch(config)#management-port protocol dhcp
```

7.2 management-port ip

Description

The **management-port ip** command is used to configure the IPv4 address of the management port. To delete the address, please use the **no management-port ip** command.

Syntax

management-port ip {*ip-addr*}{*mask*}

no management-port ip

Parameter

ip-addr—— IPv4 address

mask—— IP mask

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the IPv4 address of the management port:

Switch(config)#management-port ip 192.168.10.1 255.255.255.0

7.3 management-port ipv6 enable

Description

The **management-port ipv6 enable** command is used to enable the management-port ipv6 funtion. To disable the function, please use the **no management-port ipv6 enable** command.

Syntax

management-port ipv6 enable

no management-port ipv6 enable

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the management-port ipv6 funtion:

Switch(config)#management-port ipv6 enable

7.4 management-port ipv6 address

Description

The **management-port ipv6 address** command is used to configure the IPv6 address of the management port. To delete the address, please use the **no management-port ipv6 address** command.

Syntax

management-port ipv6 address {*ipv6-addr*} [*eui64*]

no management-port ipv6 address {*ipv6-addr*} [*eui64*]

Parameter

ipv6-addr —— IPv6 address, you need to specify the prefix length.

eui64 —— Create the address in eui64 mode.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the IPv6 address of the management port:

```
Switch(config)#management-port ipv6 address 2001::1/64 eui64
```

7.5 show management-port

Description

The **show management-port** command is used to display the configuration information of the management port.

Syntax

show management-port

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration information of the management port:

```
Switch# show management-port
```

Chapter 8 EEE Configuration Commands

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

8.1 eee

Description

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

Syntax

eee

no eee

Command Mode

Interface Configuration Mode

Privilege Requirement

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

Example

Enable EEE on port 1/0/1:

```
Switch(config)#interface gigabitEthernet 1/0/1
Switch(config-if)#eee
```

8.2 show interface eee

Description

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

Syntax

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

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the EEE configuration of each port

```
Switch# show interface eee
```

Chapter 9 SDM Template Commands

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

9.1 sdm prefer

Description

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

Syntax

sdm prefer { default | enterpriseV4 | enterpriseV6 | enterpriseMix | pca-default }

Parameter

default —— Specify the SDM template used in the switch as “default”.

enterpriseV4 —— Specify the SDM template used in the switch as “enterpriseV4”.

enterpriseV6 —— Specify the SDM template used in the switch as “enterpriseV6”.

enterpriseMix —— Specify the SDM template used in the switch as “enterpriseMix”, which provides both IPv4/IPv6-ACL support and IMPBv4/v6 support.

pca-default —— Specify the SDM template used in the switch as “pca-default”, which provides packet-content-ACL support.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

Some models may not support **pca-default** template. Changes to the SDM preferences cannot take effect until reboot the switch.

Example

Specify the SDM template as enterpriseV4:

Switch(config)# sdm prefer enterpriseV4

9.2 show sdm prefer

Description

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

Syntax

show sdm prefer { used | default | enterpriseV4 | enterpriseV6 | enterpriseMix | pca-default}

Parameter

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

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

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

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

enterpriseMix —— Specify the SDM template used in the switch as "enterpriseMix", which provides both IPv4/IPv6-ACL support and IMPBv4/v6 support.

pca-default —— Specify the SDM template used in the switch as "pca-default", which provides packet-content-ACL support.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

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

```
Switch(config)#show sdm prefer used
```

Chapter 10 Time Range Commands

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

10.1 time-range

Description

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

Syntax

time-range *name*

no time-range *name*

Command Mode

Global Configuration Mode

Parameter

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

Privilege Requirement

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

Example

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

Switch(config)# time-range tRange1

10.2 absolute

Description

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

Syntax

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

no absolute [*index*]

Parameter

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

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

Command Mode

Time-Range Create Configuration Mode

Privilege Requirement

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

Example

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

Switch(config)#time-range tRange1

Switch(config-time-range)#absolute from 05/05/2017 **to** 10/05/2017

10.3 periodic

Description

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

Syntax

periodic start *start-time* **end** *end-time* **day-of-the-week** *week-day*

no periodic [*index*]

Parameter

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

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

week-day ——In the format of 1-3, 6, daily, off-day, or working-day. For example, 1-3,6 represents Monday, Tuesday, Wednesday and Saturday; daily represents every day; off-day represents the weekends; working-day represents the working days.

Command Mode

Time-Range Create Configuration Mode

Privilege Requirement

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

Example

Configure the time-range tSeg1 with time from 8:30 to 12:00 at weekends:

Switch(config)#time-range tSeg1

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

day-of-the-week 6-7

10.4 holiday (time-range mode)

Description

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

Syntax

holiday { exclude | include }

Parameter

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

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

Command Mode

Time-Range Create Configuration Mode

Privilege Requirement

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

Example

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

Switch(config)#time-range tRange3

Switch(config-time-range)#holiday exclude

10.5 holiday

Description

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

Syntax

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

no holiday *name*

Parameter

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

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

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

Switch(config)# holiday holiday1 **start-date** 10/01 **end-date** 10/03

10.6 show holiday

Description

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

Syntax

show holiday

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the defined holiday:

```
Switch# show holiday
```

10.7 show time-range

Description

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

Syntax

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

Parameter

time-range-name —— Specify the time range name with 1 to 16 characters.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the defined time-range:

```
Switch# show time-range
```

Chapter 11 Port Configuration Commands

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

11.1 interface

Description

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

Syntax

interface ***fastEthernet / gigabitEthernet / two-gigabitEthernet / ten-gigabitEthernet****port***Parameter**

fastEthernet port——— The 100M Ethernet port number.

gigabitEthernet port——— The Gigabit Ethernet port number.

ten-gigabitEthernet port——— The 10-Gigabit Ethernet port number.

two-gigabitEthernet port——— The 2.5-Gigabit Ethernet port number.

port-channel num——— The Ethernet channel number.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

Switch(config)# interface gigabitEthernet 1/0/2

11.2 interface range

Description

The **interface range** command is used to enter the interface rangeConfiguration Mode and configure multipleEthernet ports at the same time.

Syntax

interface range fastEthernet | gigabitEthernet | two-gigabitEthernet | ten-gigabitEthernet *port-list*

Parameter

fastEthernet port —— The 100M Ethernet port number.

gigabitEthernet port —— The Gigabit Ethernet port number.

ten-gigabitEthernet port —— The 10-Gigabit Ethernet port number.

two-gigabitEthernet port —— The 2.5-Gigabit Ethernet port number.

port-list —— The list of Ethernet ports.

Command Mode

Global Configuration Mode

Privilege Requirement

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

User Guidelines

Command in the **Interface Range gigabitEthernet** Mode is executed independently on all ports in the range. It does not affect the execution on the other ports at all if the command results in an error on one port.

Example

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

Switch(config)# interface range gigabitEthernet 1/0/1-3,1/0/6-7,1/0/9

11.3 description

Description

The **description** command is used to add a description to the Ethernet port. To clear the description of the corresponding port, please use **no description** command.

Syntax

description *string*

no description

Parameter

string —— Content of a port description, ranging from 1 to 16 characters.

Command Mode

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

Switch(config)# interface gigabitEthernet 1/0/5

Switch(config-if)# description Port_5

11.4 shutdown

Description

The **shutdown** command is used to disable an Ethernet port. To enable this port again, please use **no shutdown** command.

Syntax

shutdown

no shutdown

Command Mode

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

```
Switch(config)# interface gigabitEthernet 1/0/3
Switch(config-if)# shutdown
```

11.5 flow-control

Description

The **flow-control** command is used to enable the flow-control function for a port. To disable the flow-control function for this corresponding port, please use **no flow-control** command. With the flow-control function enabled, the Ingress Rate and Egress Rate can be synchronized to avoid packet loss in the network.

Syntax

flow-control

no flow-control

Command Mode

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

```
Switch(config)# interface gigabitEthernet 1/0/3
Switch(config-if)# flow-control
```

11.6 duplex

Description

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

Syntax

duplex { auto | full | half }

no duplex

Parameter

auto | full | half —— The duplex mode of the Ethernet port. There are three options: auto-negotiation mode, full-duplex mode and half-duplex mode. By default, the Gigabit Ethernet port is auto-negotiation mode.

Command Mode

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

Switch(config)# interface gigabitEthernet 1/0/3

Switch(config-if)# duplex full

11.7 jumbo-size

Description

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

Syntax

jumbo-size *size*

Parameter

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Globally configure the size of jumbo frames as 9216:

Switch(config)# jumbo-size 9216

11.8 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 | 2500 | 5000 | 10000 | auto }

no speed

Parameter

10 | 100 | 1000 | 2500 | 5000 | 10000 | auto —— The speed mode of the Ethernet port. There are seven options: 10Mbps, 100Mbps, 1000Mbps, 2500Mbps, 5000Mbps, 10000Mbps and Auto negotiation mode (default).

Command Mode

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

Privilege Requirement

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

Example

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

Switch(config)# interface gigabitEthernet 1/0/3

Switch(config-if)# speed 100

11.9 clear counters

Description

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

Syntax

clear counters

clear counters interface [**fastEthernet** | **gigabitEthernet** | **two-gigabitEthernet** | **ten-gigabitEthernet** *port*] [**port-channel** *port-channel-id*]

Parameter

port——— The Ethernet port number.

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

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

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

Example

Clear the statistic information of all ports and port channels:

```
Switch(config)# clear counters
```

11.10 show fiber-ports

Note: This command is only available on certain devices.

Description

The **show fiber-ports** command is used to display the information of all optical modules.

Syntax

show fiber-ports

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of all fiber ports:

Switch(config)# show fiber-ports

11.11 show interface status

Description

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

Syntax

show interface status [**fastEthernet** *port*] [**gigabitEthernet** *port*] [**two-gigabitEthernet** *port*] [**ten-gigabitEthernet** *port*] [**port-channel** *port-channel-id*]

Parameter

port——— The Ethernet port number.

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

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the connection status of all ports and port channels:

Switch(config)# show interface status

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

Switch(config)# show interface status gigabitEthernet 1/0/1

11.12 show interface counters

Description

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

Syntax

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

Parameter

port —— The Ethernet port number.

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

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

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

Switch(config)# show interface counters

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

Switch(config)# show interface counters gigabitEthernet 1/0/2

11.13 show interface configuration

Description

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

Syntax

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

Parameter

port —— The Ethernet port number.

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

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configurations of all Ethernet ports and port channels:

```
Switch(config)# show interface configuration
```

Display the configurations of port 1/0/2:

```
Switch(config)# show interface configuration gigabitEthernet 1/0/2
```

Chapter 12 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.

12.1 port isolation

Description

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

Syntax

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

no port isolation

Parameter

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

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

Command Mode

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

Privilege Requirement

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

Example

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

Switch(config)# interface gigabitEthernet 1/0/5

Switch(config-if)# port isolation gi-forward-list 1/0/1-2,1/0/4 **po-forward-list** 2

Set all Ethernet ports and port channels to forward list of port 1/0/2, namely restore to the default setting:

Switch(config)# interface gigabitEthernet 1/0/2

Switch(config-if)# no port isolation

12.2 show port isolation interface

Description

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

Syntax

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

Parameter

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

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

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

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

Switch# show port isolation interface gigabitEthernet 1/0/2

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

Switch# show port isolation interface

Chapter 13 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.

13.1 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:

```
Switch(config)# loopback-detection
```

13.2 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:

Switch(config)# loopback-detection interval 50

13.3 loopback-detection recovery-time

Description

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

Syntax

loopback-detection recovery-time *recovery-time*

Parameter

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the recovery-time as 70 seconds:

Switch(config)# loopback-detection recovery-time 70

13.4 loopback-detection (interface)

Description

The **loopback-detection** command is used to enable the loopback detection function of the specified port. To disable it, please use **no loopback-detection** command.

Syntax

loopback-detection

no loopback-detection

Command Mode

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

Privilege Requirement

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

Example

Enable the loopback detection function of ports 1-3:

Switch(config)# interface range gigabitEthernet 1/0/1-3

Switch(Config-if-range)# loopback-detection

13.5 loopback-detection config process-mode

Description

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

Syntax

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

Parameter

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

port-based —— When a loop is detected, the switch will send a trap message and generate an entry on the log file. In addition, the switch will block the port on which the loop is detected and no packets can pass through the port.

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

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

manual —— Block status can only be removed manually.

Command Mode

Interface Configuration Mode (interface 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 configure the recovery mode as manual for port 2:

Switch(config)# interface gigabitEthernet 1/0/2

Switch(config-if)# loopback-detection config process-mode port-based **recovery-mode** manual

13.6 loopback-detection recover

Description

The **loopback-detection recover** command is used to remove the block status of selected ports, recovering the blocked ports to normal status,

Syntax

loopback-detection recover

Command Mode

Interface Configuration Mode (interface gigabitEthernet | interface range gigabitEthernet | 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:

```
Switch(config)# interface gigabitEthernet 1/0/2
Switch(config-if)# loopback-detection recover
```

13.7 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:

```
Switch# show loopback-detection global
```

13.8 show loopback-detection interface

Description

The **show loopback-detection interface** command is used to display the configuration of loopback detection function and the status of the specified Ethernet port.

Syntax

show loopback-detection interface [**fastEthernet** *port* | **gigabitEthernet** *port* | **two-gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **port-channel** *lagid*] [**detail**]

Parameter

port —— The Ethernet port number.

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

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

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

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

Switch# show loopback-detection interface

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

Switch# show loopback-detection interface gigabitEthernet 1/0/5

Chapter 14 Stack Commands (Only for Certain Devices)

Stack is a device virtualization technology that connects two and above switches supporting stack features via cables through their stack ports, which logically virtualize them to one device as a whole to forward data in the network in Layer 2 and Layer 3 protocols. Through this feature, switches can be stacked to improve reliablity, expand port numbers, increase bandwidth, simplify networking, and etc.

In a stack system, the switches can be categorized mainly into two roles: Master Switch and Member Switch. The master switch manages and controls devices in the whole stack system while the member switch only forwards data as a standby device of the master switch.

As the following figure shows, the switches are connected to form a stack which works as a unified system that enables multiple devices to collaborate under the management of the master switch as a whole.

14.1 switch stack-name

Description

The **switch stack-name** command is used to specify the name of the stack system.

Syntax

switch stack-name {*name*}

Parameter

name —— Specify the name of the stack system.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the name of the stack system:

```
Switch(config)#switch stack-name "test"
```

14.2 switch stack-group

Description

The **switch stack-group** command is used to access the viewing page of a specified stack port group configuration of the specified device.

Syntax

switch {*unitid*} stack-group {*groupid*}

Parameter

unitid—— Device ID in the stack system, ranging from 1-4.

groupid—— ID of the stack port group, ranging from 1-4.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enter the viewing page of a stack port group 1 on switch 1:

```
Switch(config)#switch 1 stack-group 1
```

14.3 group-info

Description

The **group-info** command is used to view the specified stack port group configuration of the specified device.

Syntax

group-info

Parameter

group-info—— Display the information of the stack group.

Command Mode

Stack-Group Mode

Privilege Requirement

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

Example

View the inforamtion of the stack port group 1 on switch 2.

```
Switch(config)# switch 2 stack-group 1
Switch(stack-group)#group-info
```

14.4 interface port

Description

The **interface port** command is used to enable the stack function for a specified slot. To disable this function, please use the **no interface port** command.

Syntax

interface *port*

no interface *port*

Parameter

port—— Port which the stack function to be enabled/disabled on

Command Mode

Stack-Group Mode

Privilege Requirement

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

Example

Configure 1/0/28 as a stack port and join stack-group 1 of uinit 2:

```
Switch(stack-group)# interface 1/0/28
```

14.5 switch priority

Description

The **switch priority** command is used to configure the stack priority of the device with specified unit ID.

Syntax

switch {*unitid***} priority {***priority***}**

Parameter

unitid—— Device ID in the stack system, ranging from 1 to 4.

Priority—— Stack priority. The higher the priority, the more likely the device is to become the master device. The value ranges from 1 to 255.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the stack priority of unit 1 as 5:

Switch(config)#switch 1 priority 5

14.6 switch renumber

Description

The **switch renumber** command is used to modify the stack unit ID of a specified device, which will take effect after the switch reboots.

Syntax

switch {*unitid***} renumber {***new-unitid***}**

Parameter

unitid—— ID in the stack system, ranging from 1 to 4.

new-unitid—— New device ID to be configured, ranging from 1 to 4.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Renumber the stack unit ID of unit 1 as 2:

Switch(config)# switch 1 renumber 2

WARNING: Changing the Unit number may result in a configuration change for that unit. The interface configuration associated with the old unit number will remain as a provisioned configuration. Do you want to continue?[Y/N] **y**

```
Changing Unit Number 1 to Unid Number 1. New Unit Number will be effective
after next reboot
```

14.7 switch provision

Description

The **switch provision** command is used to create a preconfigured entry specifying unitid and device-type. After creation, you can use other configuration commands to configure the unit. The configuration will take effect after the stack is connected. To delete the entry, please use the **no switch provision** command.

Syntax

switch {*unitid***} provision {***device-type***}**

no switch {*unitid***} provision {***device-type***}**

Parameter

unitid —— Device ID, which should be less than 32 characters and range from 1 to 4.

device-type —— Device type. The provision device needs to be of the same type as the connected device.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure provision entries:

```
Switch(config)#switch 1 provision 3
```

14.8 show switch stack-ports

Description

The **show switch stack-ports** command is used to display the stack port information of all members of the stack group.

Syntax

show switch stack-ports

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

View the stack port information of all members of the stack group:

```
Switch(config)#show switch stack-ports
```

14.9 show switch

Description

The **show switch** command is used to display the information of all devices in the stack system.

Syntax

show switch

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

View the information of all devices in the stack system:

```
Switch(config)#show switch
```

14.10 show switch unitid

Description

The **show switch unitid** command is used to display the information about specified stack member devices.

Syntax

show switch {*unitid***}**

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

View the information about unit 1:

```
Switch(config)#show switch 1
```

14.11 show switch neighbors

Description

The **show switch neighbors** command is used to display the group ID of the stack port and the unit ID of its neighboring member device in the current stack system.

Syntax

show switch neighbors

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

View the the group ID of the stack port and the unit ID of its neighboring member device in the current stack system:

```
Switch(config)#show switch neighbors
```

Chapter 15 DDM Commands (Only for Certain Devices)

Note: DDM commands are only available on certain devices.

The DDM (Digital Diagnostic Monitoring) function allows the user to monitor the status of the SFP modules inserted into the SFP ports on the switch. The user can choose to shut down the monitoring SFP port automatically when specified parameter exceeds the alarm threshold or warning threshold. The monitoring parameters include: Temperature, Voltage, Bias Current, Tx Power and Rx Power.

15.1 ddm state enable

Description

The **ddm state enable** command is used to enable the DDM function on the specified SFP port.

Use the **no ddm state enable** command to disable the DDM function on this port.

Syntax

ddm state enable

no ddm state enable

Default Setting

Enabled on all the SFP ports.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Example

Enable DDM function on port 1/0/25:

Switch(config)#interface gigabitEthernet 1/0/25

Switch(config-if)#ddm state enable

15.2 ddm shutdown

Description

The **ddm shutdown** command is used to configure whether to shut down the port when an exceeding alarm threshold or warning threshold event is encountered.

Syntax

ddm shutdown { none | warning | alarm }

Parameter

none —— The port will never be shut down regardless of the exceeding alarm threshold and warning threshold events.

warning —— Shut down the port when an exceeding warning threshold event is encountered.

alarm —— Shut down the port when an exceeding alarm threshold event is encountered.

Default Setting

none, which means the port will never be shut down regardless of the exceeding alarm threshold and warning threshold events.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Example

Shut down the port 1/0/25 when an exceeding warning threshold event is encountered:

Switch(config)#interface gigabitEthernet 1/0/25

Switch(config-if)#ddm shutdown warning

15.3 ddm temperature_threshold

Description

The **ddm temperature_threshold** command is used to configure the threshold of the DDM temperature value.

Syntax

ddm temperature_threshold { high_alarm | high_warning | low_alarm | low_warning } *value*

Parameter

high_alarm —— Specify the highest threshold for the alarm. When the operating parameter rises above the value hereinafter, action associated with the alarm will be taken.

high_warning ——Specify the highest threshold for the warning. When the operating parameter rises above the value hereinafter, action associated with the warning will be taken.

low_alarm ——Specify the lowest threshold for the alarm. When the operating parameter falls below the value hereinafter, action associated with the alarm will be taken.

low_warning —— Specify the lowest threshold for the warning. When the operating parameter falls below the value hereinafter, action associated with the warning will be taken.

value —— Enter the threshold value in Celsius.

Default Setting

None.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Example

Configure the high_alarm threshold of DDM temperature on the port 1/0/25 as 5:

```
Switch(config)#interface gigabitEthernet 1/0/25
Switch(config-if)#ddm temperature_threshold high_alarm 5
```

15.4 ddm voltage_threshold

Description

The **ddm voltage_threshold** command is used to configure the threshold of the DDM voltage value.

Syntax

ddm voltage_threshold { high_alarm | high_warning | low_alarm | low_warning } *value*

Parameter

high_alarm —— Specify the highest threshold for the alarm. When the operating parameter rises above the value hereinafter, action associated with the alarm will be taken.

high_warning ——Specify the highest threshold for the warning. When the operating parameter rises above the value hereinafter, action associated with the warning will be taken.

low_alarm ——Specify the lowest threshold for the alarm. When the operating parameter falls below the value hereinafter, action associated with the alarm will be taken.

low_warning —— Specify the lowest threshold for the warning. When the operating parameter falls below the value hereinafter, action associated with the warning will be taken.

value —— Enter the threshold value in Volt.

Default Setting

None.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Example

Configure the high_alarm threshold of DDM voltage on the port 1/0/25 as 5:

Switch(config)#interface gigabitEthernet 1/0/25

Switch(config-if)#ddm voltage_threshold high_alarm 5

15.5 ddm bias_current_threshold

Description

The **ddm bias_current_threshold** command is used to configure the threshold of the DDM Bias Current value.

Syntax

ddm bias_current_threshold { high_alarm | high_warning | low_alarm | low_warning } *value*

Parameter

high_alarm —— Specify the highest threshold for the alarm. When the operating parameter rises above the value hereinafter, action associated with the alarm will be taken.

high_warning ——Specify the highest threshold for the warning. When the operating parameter rises above the value hereinafter, action associated with the warning will be taken.

low_alarm ——Specify the lowest threshold for the alarm. When the operating parameter falls below the value hereinafter, action associated with the alarm will be taken.

low_warning —— Specify the lowest threshold for the warning. When the operating parameter falls below the value hereinafter, action associated with the warning will be taken.

value —— Enter the threshold value in mA.

Default Setting

None.

Command Mode

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

Example

Configure the high_alarm threshold of DDM Bias Current on the port 1/0/25 as 5:

Switch(config)#interface gigabitEthernet 1/0/25

Switch(config-if)#ddm bias_current_threshold high_alarm 5

15.6 ddm tx_power_threshold

Description

The **ddm tx_power_threshold** command is used to configure the threshold of the DDM Tx Power value.

Syntax

ddm tx_power_threshold { high_alarm | high_warning | low_alarm | low_warning } *value*

Parameter

high_alarm —— Specify the highest threshold for the alarm. When the operating parameter rises above the value hereinafter, action associated with the alarm will be taken.

high_warning ——Specify the highest threshold for the warning. When the operating parameter rises above the value hereinafter, action associated with the warning will be taken.

low_alarm ——Specify the lowest threshold for the alarm. When the operating parameter falls below the value hereinafter, action associated with the alarm will be taken.

low_warning —— Specify the lowest threshold for the warning. When the operating parameter falls below the value hereinafter, action associated with the warning will be taken.

value —— Enter the threshold value in mW.

Default Setting

None.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Example

Configure the high_alarm threshold of DDM Tx Power on the port 1/0/25 as 5:

Switch(config)#interface gigabitEthernet 1/0/25

Switch(config-if)#ddm tx_power_threshold high_alarm 5

15.7 ddm rx_power_threshold

Description

The **ddm rx_power_threshold** command is used to configure the threshold of the DDM Rx Power value.

Syntax

ddm rx_power_threshold { high_alarm | high_warning | low_alarm | low_warning } *value*

Parameter

high_alarm —— Specify the highest threshold for the alarm. When the operating parameter rises above the value hereinafter, action associated with the alarm will be taken.

high_warning ——Specify the highest threshold for the warning. When the operating parameter rises above the value hereinafter, action associated with the warning will be taken.

low_alarm ——Specify the lowest threshold for the alarm. When the operating parameter falls below the value hereinafter, action associated with the alarm will be taken.

low_warning —— Specify the lowest threshold for the warning. When the operating parameter falls below the value hereinafter, action associated with the warning will be taken.

value —— Enter the threshold value in mW.

Default Setting

None.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Example

Configure the high_alarm threshold of DDM Rx Power on the port 1/0/25 as 5:

Switch(config)#interface gigabitEthernet 1/0/25

Switch(config-if)#ddm rx_power_threshold high_alarm 5

15.8 show ddm configuration

Description

The **show ddm configuration** command is used to display the DDM configuration.

Syntax

show ddm configuration { state | temperature | voltage | bias_current | tx_power | rx_power }

Parameter

state —— Display the DDM configuration state.

temperature —— Displays the threshold of the DDM temperature value.

voltage —— Displays the threshold of the DDM Voltage value.

bias_current —— Displays the threshold of the DDM Bias Current value.

tx_power —— Displays the threshold of the DDM Tx Power value.

rx_power —— Displays the threshold of the DDM Rx Power value.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

View the DDM configuration state:

Switch(config)#show ddm configuration state

View the threshold of the DDM Voltage value:

Switch(config)#show ddm configuration voltage

15.9 show ddm status

Description

The **show ddm status** command is used to display the DDM status, which is the digital diagnostic monitoring status of SFP modules inserting into the switch's SFP ports.

Syntax

show ddm status

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

View the DDM status:

Switch(config)#show ddm status

15.10 show fiber-ports

Note: This command is only available on certain devices.

Description

The **show fiber-ports** command is used to display the information of all fiber ports.

Syntax

show fiber-ports

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the information of all fiber ports:

```
Switch(config)# show fiber-ports
```

Chapter 16 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.

16.1 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, which ranges from 1 to 8 for L2/L2+ switches, 1 to 64 for L3 access switches, and 1 to 120 for L3 aggregation switches.

on —— Enable the static LAG.

active —— Enable the active LACP mode.

passive —— Enable the passive LACP mode.

Command Mode

Interface Configuration Mode (interface fastEthernet | gigabitEthernet | two-gigabitEthernet | ten-gigabitEthernet / interface range fastEthernet | gigabitEthernet | two-gigabitEthernet | ten-gigabitEthernet)

Privilege Requirement

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

Example

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

Switch(config)# interface range gigabitEthernet 1/0/2-4

Switch(config-if-range)# channel-group 1 **mode** on

16.2 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.

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:

Switch# remove public-key v1

55.9 show ip ssh

Description

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

Syntax

show ip ssh

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of SSH:

Switch(config)# show ip ssh

Chapter 56 Telnet Commands

56.1 telnet

Description

The **telnet** command is used to log in and manage other devices via telnet.

Syntax

telnet *ip-addr*

Parameter

ip-addr——The IP address of the device you want to log in.

Command Mode

Privileged EXEC Mode

Privilege Requirement

None.

User Guidelines

Make sure the switch can access the device, and the device can be logged in via telnet.

Example

Log in to a device with the IP address of 192.168.0.10:

Switch# telnet 192.168.0.10

56.2 telnet enable

Description

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

Syntax

telnet enable

telnet disable

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Disable the Telnet function:

Switch(config)# telnet disable

56.3 telnet port

Description

The **telnet port** command is used to configure the telent port number. To restore the setting, please use the **no telnet port** command.

Syntax

telnet port *port*

no telnet port

Parameter

port——The number of telnet port.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the telnet port number as 566:

Switch(config)# telnet port 566

56.4 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:

```
Switch(config)# show telnet-status
```

Chapter 57 Serial Port Commands

Note: Serial Port commands are only available on certain devices.

57.1 serial_port baud-rate

Description

The **serial_port baud-rate** command is used to configure the communication baud rate on the console port. To return to the default baud rate, please use **no serial_port** command.

Syntax

serial_port baud-rate { 9600 | 19200 | 38400 | 57600 | 115200 }

no serial_port

Parameter

9600 | 19200 | 38400 | 57600 | 115200 ——Specify the communication baud rate on the console port. The default baul rate is 38400 bps.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the communication baud rate on the console port to the default value:

Switch(config)# no serial_port

Chapter 58 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.

58.1 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 *encryped-string* }]

no tacacs-server host *ip-address*

Parameter

ip-address —— Specify the IP address of the TACACS+ server.

port-id —— Specify the server's port number for AAA. By default it is 49.

time —— Specify the time in seconds the switch waits for the server's response before it times out. The time ranges from 1 to 9 seconds. The default is 5 seconds.

[0] *string* | 7 *encrypted-string* —— 0 and 7 are the encryption type. 0 indicates that an unencrypted key will follow. 7 indicates that a symmetric encrypted key with a fixed length will follow. By default, the encryption type is 0. "*string*" is the shared key for the switch and the authentication servers to exchange messages. "*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.

Switch(config)# tacacs-server host 1.1.1.1 **port** 1500 **timeout** 6 **key** 12345

58.2 show tacacs-server

Description

This **show tacacs-server** command is used to display the summary information of the TACACS+ servers.

Syntax

show tacacs-server

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of all the TACACS+ servers:

Switch(config)# show tacacs-server

58.3 radius-server host

Description

The **radius-server host** command is used to configure a new RADIUS server. To delete the specified RADIUS server, please use **no radius-server host** command.

Syntax

radius-server host *ip-address* [**auth-port** *port-id*] [**acct-port** *port-id*] [**timeout** *time*] [**retransmit** *number*] [**nas-id** *nas-id*] [**key** { [0] *string* | 7 *encrypted-string* }]

no radius-server host *ip-address*

Parameter

ip-address —— Specify the IP address of the RADIUS server.

auth-port *port-id* —— Specify the UDP destination port for authentication requests. By default it is 1812.

acct-port *port-id* —— Specify the UDP destination port for accouting requests. By deault it is 1813.

time —— Specify the time in seconds the switch waits for the server's response before it times out. The time ranges from 1 to 9 seconds. The default is 5 seconds.

number —— Specify the number of times a RADIUS request is resent to a server if the server is not responding in time. By default it is 2 times.

nas-id ——Specify the name of the NAS (Network Access Server) to be contained in RADIUS packets for identification. It ranges from 1 to 31 characters. The default value is the MAC address of the switch. Generally, the NAS indicates the switch itself.

[0] *string* | 7 *encrypted-string* —— 0 and 7 are the encryption type. 0 indicates that an unencrypted key will follow. 7 indicates that a symmetric

encrypted key with a fixed length will follow. By default, the encryption type is 0. "*string*" is the shared key for the switch and the authentication servers to exchange messages. "*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.

Switch(config)# radius-server host 1.1.1.1 **auth-port** 1200 **timeout** 6 **retransmit** 3 **key** 12345

58.4 show radius-server

Description

This **show radius-server** command is used to display the summary information of the RADIUS servers.

Syntax

show radius-server

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of all the RADIUS servers:

Switch(config)# show radius-server

58.5 aaa group

Description

This **aaa group** command is used to create AAA server groups to group existing TACACS+/RADIUS servers for authentication. This command puts the switch in the server group subconfiguration mode.

To delete the corresponding AAA group, please use the **no aaa group** command.

Syntax

aaa group { radius | tacacs } *group-name*
no aaa group { radius | tacacs } *group-name*

Parameter

radius | tacacs —— Specify the server group type as RADIUS or TACACS+.

group-name —— Specify the server group name.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Create a RADIUS server group with the name radius1:

Switch(config)# aaa group radius radius1

58.6 server

Description

This **server** command is used to add the existing server in the defined server group. To remove the specified server from the server group, please use the **no server** command.

Syntax

server *ip-address*

no server *ip-address*

Parameter

ip-address —— Specify the server's IP address.

Command Mode

Server Group Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Create the RADIUS server 1.1.1.1 to RADIUS server group "radius1":

```
Switch(config)# aaa group radius radius1
Switch(aaa-group)# server 1.1.1.1
```

58.7 show aaa group

Description

This **show aaa group** command is used to display the summary information of the AAA groups. All the servers in this group will be listed if you specify the group name.

Syntax

show aaa group [*group-name*]

Parameter

group-name —— Specify the server group name.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of all the server groups:

```
Switch(config)# show aaa group
```

58.8 aaa authentication login

Description

This **aaa authentication login** command is used to configure a login authentication method list. A method list describes the authentication methods and their sequence to authenticate a user. To delete the specified authentication method list, please use the **no aaa authentication login** command.

Syntax

aaa authentication login { *method-list* } { *method1* } [*method2*] [*method3*] [*method4*]

no authentication login *method-list*

Parameter

method-list —— Specify the method list name.

method1, method2, method3, method4 —— Specify the authentication methods in order. The next authentication method is tried only if the previous method does not respond, not if it fails.

The preset methods include radius, tacacs, local and none. "radius" means the RADIUS server group "radius"; "tacacs" means the RACACS+ server group "tacacs"; "local" means local username database are used; "none" means no authentication is used for login.

Users can aslo define new method with the aaa group command.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

By default the login authentication method list is "default" with "local" as method1.

Example

Configure a login authentication method list "list1" with the priority1 method as radius and priority2 method as local:

Switch(config)# aaa authenticaiton login list1 radius local

58.9 aaa authentication enable

Description

This **aaa authentication enable** command is used to configure a privilege authentication method list. A method list describes the authentication methods and their sequence to elevate a user's privilege. To delete the specified authentication method list, please use the **no aaa authentication enable** command.

Syntax

aaa authentication enable { *method-list* } { *method1* } [*method2*] [*method3*] [*method4*]

no authentication enable *method-list*

Parameter

method-list —— Specify the method list name.

method1, method2, method3, method4 —— Specify the authentication methods in order. The next authentication method is tried only if the previous method does not respond, not if it fails.

The preset methods include radius, tacacs, local and none. "radius" means the RADIUS server group "radius"; "tacacs" means the RACACS+ server group "tacacs"; "local" means local username database are used; "none" means no authentication is used for privilege elevation.

Users can aslo define new method with the aaa group command.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

User Guidelines

By default the enable authentication method is "default" with "none" as method1.

Example

Configure a privilege authentication method list "list2" with the priority1 method as radius and priority2 method as local:

Switch(config)# aaa authenticaiton enable list2 radius local

58.10 aaa authentication dot1x default

Description

This **aaa authentication dot1x default** command is used to configure an 802.1x authentication method list. A method list describes the authentication methods for users' login in 802.1x. To delete the default authentication method list, please use the **no aaa authentication dot1x default** command.

Syntax

aaa authentication dot1x default { *method*}

no aaa authentication dot1x default

Parameter

method —— Specify the method name. Only RADIUS server group is supported, and the default method is server group "radius".

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the default 802.1x authentication method as "radius1":

Switch(config)# aaa authentication dot1x default radius1

58.11 aaa accounting dot1x default

Description

This **aaa accounting dot1x default** command is used to configure an 802.1x accounting method list. To delete the default accounting method list, please use the **no aaa accounting dot1x default** command.

Syntax

aaa accounting dot1x default { *method*}

no aaa accounting dot1x default

Parameter

method —— Sp+ecify the method name. Only RADIUS server group is supported, and the default method is server group “radius”.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the default 802.1x accounting method as “radius1”:

Switch(config)# aaa accounting dot1x default radius1

58.12 show aaa authentication

Description

This **show aaa authentication** command is used to display the summary information of the authentication login, enable and dot1x metheod list.

Syntax

show aaa authentication [login | enable | dot1x]

Parameter

login | enable | dot1x —— Specify the method list type.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of all the authentication method lists:

Switch(config)# show aaa authentication

58.13 show aaa accounting

Description

This **show aaa accounting** command is used to display the summary information of the accounting metheod list.

Syntax

show aaa accounting [dot1x]

Parameter

dot1x —— Specify the method list type.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Display the information of the default 802.1x accounting method list:

```
Switch(config)# show aaa accounting
```

58.14 line telnet

Description

The **line telnet** command is used to enter the Line Configuration Mode to configure the telnet terminal line to which you want to apply the authentication list.

Syntax

line telnet

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enter the telnet terminal line configuration mode:

Switch(config)#line telnet

58.15 login authentication (telnet)

Description

The **login authentication** command is used to apply the login authentication method list to the telnet terminal line. To restore to the default authentication method list, please use the **no login authentication** command.

Syntax

login authentication { *method-list* }

no login authentication

Parameter

method-list —— Specify the login method list on the telnet terminal line. It is "default" by default, which contains the method "local".

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the login authentication method list on the telnet terminal line as "list1":

Switch(config)#line telnet

Switch(config-line)# login authentication list1

58.16 line ssh

Description

The **line ssh** command is used to enter the Line Configuration Mode to configure the ssh terminal line to which you want to apply the authentication list.

Syntax

line ssh

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enter the ssh terminal line configuration mode:

```
Switch(config)#line ssh
```

58.17 login authentication (ssh)

Description

The **login authentication** command is used to apply the login authentication method list to the ssh terminal line. To restore to the default authentication method list, please use the **no login authentication** command.

Syntax

login authentication { *method-list* }

no login authentication

Parameter

method-list —— Specify the login method list on the ssh terminal line. It is "default" by default, which contains the method "local".

Command Mode

Line Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the login authentication method list on the ssh terminal line as "list1":

```
Switch(config)# line ssh
```

```
Switch(config-line)# login authentication list1
```

58.18 line console

Note: This command is only available on certain devices.

Description

The **line console** command is used to enter the Line Configuration Mode to configure the console terminal line to which you want to apply the authentication list.

Syntax

line console *line-number*

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enter the console 0 terminal line configuration mode:

```
Switch(config)#line console 0
```

58.19 login authentication (console)

Note: This command is only available on certain devices.

Description

The **login authentication** command is used to apply the login authentication method list to the console 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 console 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 console 0 terminal line as “list1”:

Switch(config)# line console 0

Switch(config-line)# login authentication list1

58.20 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":

Switch(config)#line telnet

Switch(config-line)# enable authentication list2

58.21 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":

Switch(config)# line ssh

Switch(config-line)# enable authentication list2

58.22 enable authentication (console)

Note: This command is only available on certain devices.

Description

The **enable authentication** command is used to apply the privilege authentication method list to the console 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 console 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 console 0 terminal line as "list2":

Switch(config)# line console 0

Switch(config-line)# enable authentication list2

58.23 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":

Switch(config)# ip http login authentication list1

58.24 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":

Switch(config)# ip http enable authentication list2

58.25 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:

Switch(config)# show aaa global

58.26 enable admin password

Description

The **enable admin password** command is used to set or change the Enable password for users to change the access level to admin. To remove the Enable password, please use **no enable admin** command. This command uses the symmetric encryption.

Syntax

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

no enable admin

Parameter

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

password —— Enable password, a string with 31 characters at most, which can contain only English letters (case-sensitive), digits and 17 kinds of special characters. The special characters are **!$%'()*,-./[]_{|}**. By default, it is empty. 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.

If both the **enable admin password** and **enable admin secret** are defined, only the latest configured password will take effect.

Example

Set the Enable password as "abc123" and unencrypted for users to change the access level to admin:

Switch(config)#enable admin password 0 abc123

58.27 enable admin secret

Description

The **enable admin secret** command is used to set or change the Enable password for users to change the access level to admin. To remove the Enable password, please use **no enable admin** command. This command uses the MD5 encryption.

Syntax

enable admin secret { [0] *password* | 5 *encrypted-password* }

no enable admin

Parameter

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

password —— Enable password, a string with 31 characters at most, which can contain only English letters (case-sensitive), digits and 17 kinds of special characters. The special characters are **!$%'()*,-./[]_{|}**. By default, it is empty. 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 admin password** and **enable admin secret** are defined, only the latest configured password will take effect.

Example

Set the Enable password as “abc123” and unencrypted for users to change the access level to admin. The password will be displayed in the encrypted form.

Switch(config)#enable admin secret 0 abc123

58.28 enable-admin

Description

The **enable-admin** command is used to get the administrative privelges by a non-admin user.

Syntax

enable-admin

Command Mode

Privileged EXEC Mode

Privilege Requirement

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

Example

Get the administrative privelges (the Enable password is “123456”):

Switch# enable-admin

Password: 123456

Chapter 59 IEEE 802.1x Commands

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

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

This chapter handles with the authentication process between the supplicant and the switch. To realize the authentication and accounting function, you should also enbable the AAA function and configure the RADIUS server. Go to Chapter 42 AAA Commands for more details.

59.1 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:

```
Switch(config)#dot1x system-auth-control
```

59.2 dot1x handshake

Description

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

Syntax

dot1x handshake

no dot1x handshake

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Disable the 802.1x handshake function:

```
Switch(config)# no dot1x handshake
```

59.3 dot1x auth-protocol

Description

The **dot1x auth-protocol** command is used to configure the authentication protocol of IEEE 802.1x and the default 802.1x authentication method is “eap”. To restore to the default 802.1x authentication protocol, please use **no dot1x auth-protocol** command.

Syntax

dot1x auth-protocol { pap | eap }

no dot1x auth-protocol

Parameter

pap | eap ——Authentication protocols.

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

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the Authentication protocol of IEEE 802.1x as “pap”:

Switch(config)#dot1x auth-protocol pap

59.4 dot1x vlan-assignment

Description

The **dot1x vlan-assignment** command is used to enable the VLAN assignment feature.To disable this feature, please use **no dot1x vlan-assignment** command.

802.1x VLAN assignment is a technology allowing the RADIUS server to send the VLAN assignment to the port when the port is authenticated.

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

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

If no VLAN is supplied by the RADIUS server or if 802.1x authentication is disabled, the port will be in its original VLAN after successful authentication.

Syntax

dot1x vlan-assignment

no dot1x vlan-assignment

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the VLAN assignment feature:

```
Switch(config)#dot1x vlan-assignment
```

59.5 dot1x accounting

Description

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

Syntax

dot1x accounting

no dot1x accounting

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the enable the IEEE 802.1x accounting function globally:

```
Switch(config)#dot1x accounting
```

59.6 dot1x mab

Description

The **dot1x mab** command is used to enable the MAB feature on the port.To disable this feature, please use **no dot1x mab** command.

With MAB (MAC-Based Authentication Bypass) feature enabled, the switch automatically sends the authentication server a RADIUS access request frame with the client's MAC address as the username and password. It is also necessary to configure the RADIUS server with the client's information for authentication. You can enable this feature on IEEE 802.1x ports connected to devices without 802.1x capability. For example, most printers, IP phones and fax machines do not have 802.1x capability.

Syntax

dot1x mab

no dot1x mab

Command Mode

Interface Configuration Mode

Privilege Requirement

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

Example

Enable the MAB feature on the Gigabit Ethernet port 1/0/1:

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#dot1x mab

59.7 dot1x guest-vlan

Description

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

Syntax

dot1x guest-vlan *vid*

no dot1x guest-vlan

Parameter

vid —— The VLAN ID needed to enable the Guest VLAN function, ranging from 0 to 4094. 0 means that Guest VLAN is disabled. The supplicants in the Guest VLAN can access the specified network source.

Command Mode

Interface Configuration Mode

Privilege Requirement

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

Example

Enable the Guest VLAN function for VLAN 5 and set the VLAN ID as 20 on the Gigabit Ethernet port 1/0/1::

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#dot1x guest-vlan 5

59.8 dot1x timeout quiet-period

Description

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

Syntax

dot1x timeout quiet-period [*time*]

no dot1x timeout quiet-period

Parameter

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

Command Mode

Interface Configuration Mode

Privilege Requirement

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

Example

Enable the quiet-period function and set the quiet-period as 5 seconds on the Gigabit Ethernet port 1/0/1:

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#dot1x quiet-period 5

59.9 dot1x timeout supp-timeout

Description

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

Syntax

dot1x timeout supp-timeout *time*

no dot1x timeout supp-timeout

Parameter

time ——The maximum time for the switch to wait for the response from supplicant before resending a request to the supplicant, ranging from 1 to 60 in second. By default, it is 30 seconds.

Command Mode

Interface Configuration Mode

Privilege Requirement

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

Example

Configure the supplicant timeout value as 5 seconds on the Gigabit Ethernet pot 1/0/1:

```
Switch(config)#interface gigabitEthernet 1/0/1
Switch(config-if)#dot1x timeout supp-timeout 5
```

59.10 dot1x max- req

Description

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

Syntax

dot1x max-req *times*

no dot1x max-req

Parameter

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

Command Mode

Interface Configuration Mode

Privilege Requirement

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

Example

Configure the maximum transfer times of the repeated authentication request as 5 on the Gigabit Ethernet port 1/0/1:

```
Switch(config)#interface gigabitEthernet 1/0/1
Switch(config-if)#dot1x max-req 5
```

59.11 dot1x

Description

The **dot1x** command is used to enable the IEEE 802.1x function for a specified port. To disable the IEEE 802.1x function for a specified port, please use **no dot1x** command.

Syntax

dot1x

no dot1x

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the IEEE 802.1x function for the Gigabit Ethernet port 1:

```
Switch(config)#interface gigabitEthernet 1/0/1
Switch(config-if)#dot1x
```

59.12 dot1x port-control

Description

The **dot1x port-control** command is used to configure the Control Mode of IEEE 802.1x for the specified port. By default, the control mode is “auto”. To restore to the default configuration, please use **no dot1x port-control** command.

Syntax

dot1x port-control {auto | authorized-force | unauthorized-force}

no dot1x port-control

Parameter

auto | authorized-force | unauthorized-force —— The Control Mode for the port.

auto: In this mode, the port will normally work only after passing the 802.1x Authentication.

authorized-force: In this mode, the port can work normally without passing the 802.1x Authentication.

unauthorized-force: In this mode, the port is forbidden working for its fixed unauthorized status.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure the Control Mode for Gigabit Ethernet port 20 as "authorized-force":

Switch(config)#interface gigabitEthernet 1/0/20

Switch(config-if)#dot1x port-control authorized-force

59.13 dot1x port-method

Description

The **dot1x port-method** command is used to configure the control type of IEEE 802.1x for the specified port. By default, the control type is "mac-based". To restore to the default configuration, please use **no dot1x port-method** command.

Syntax

dot1x port-method { mac-based | port-based }

no dot1x port-method

Parameter

mac-based | port-based ——The control type for the port.

mac-based: Any client connected to the port should pass the 802.1x authentication for access.

port-based: All the clients connected to the port can access the network on the condition that any one of the clients has passed the 802.1x Authentication.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure the Control Type for Gigabit Ethernet port 20 as “port-based”:

Switch(config)#interface gigabitEthernet 1/0/20

Switch(config-if)#dot1x port-method port-based

59.14 dot1x auth-init

Description

The **dot1x auth-init** command is used to initialize the specific client.

Syntax

dot1x auth-init [mac *mac-address* **]**

Parameter

mac-address: Enter the MAC address of the client that will be unauthorized.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

None.

Example

Initialize the client whose MAC address is a 00:02:58:4f:6c:23 on port 1:

Switch(Config)# interface gigabitEthernet 1/0/1

Switch(Config-if)#dot1x auth-init mac 00:02:58:4f:6c:23

59.15 dot1x auth-reauth

Description

The **dot1x auth-reauth** command is used to reauthenticate the specific client.

Syntax

dot1x auth-reauth [**mac** *mac-address*]

Parameter

mac-address: Enter the MAC address of the client that will be reauthenticated.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

None.

Example

Reauthenticate the client whose MAC address is a 00:02:58:4f:6c:23 on port 1:

Switch(Config)# interface gigabitEthernet 1/0/1

Switch(Config-if)#dot1x auth-reauth mac 00:02:58:4f:6c:23

59.16 show dot1x global

Description

The **show dot1x global** command is used to display the global configuration of 801.X.

Syntax

show dot1x global

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of 801.X globally:

Switch(config)#show dot1x global

59.17 show dot1x interface

Description

The **show dot1x interface** command is used to display all ports or the specified port's configuration information of 801.X.

Syntax

show dot1x interface [**gigabitEthernet** *port*]

Parameter

port —— The Ethernet port number. If not specified, the information of all the ports will be displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration information of 801.X for Gigabit Ethernet port 20:

Switch(config)#show dot1x interface gigabitEthernet 1/0/20

Display the configuration information of 801.X for all Ethernet ports:

Switch(config)#show dot1x interface

59.18 show dot1x auth-state interface

Description

The **show dot1x auth-state interface** command is used to display the authentication status of each port.

Syntax

show dot1x auth-state interface [**fastEthernet** *port* **| gigabitEthernet** ***port*** **| ten-gigabitEthernet** *port*]

Parameter

port —— The Ethernet port number. If not specified, the information of all the ports will be displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the authentication status of each port:

```
Switch(config)#show dot1x auth-state interface
```

Chapter 60 Port Security Commands

You can limit the number of MAC addresses that can be learned on each port on this page, thus preventing the MAC address table from being exhausted by the attack packets.

60.1 mac address-table max-mac count

Description

The **mac address-table max-mac-count** command is used to enable the port security feature of the port and configure the related parameters. To disable the feature and restore the parameters to defaults on the port, please use **no mac address-table max-mac-count** command.

Syntax

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

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

Command Mode

Interface Configuration Mode

Privilege Requirement

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

Example

Set the maximum number of MAC addresses that can be learned on port 1/0/1 as 30, enable exceed-max-leaned feature and configure the mode as permanent and the status as drop:

Switch (config)#interface gigabitEthernet 1/0/1

Switch(config-if)#mac address-table max-mac-count max-number 30

exceed-maxlearned enable **mode** permanent **status** drop

60.2 show mac address-table max-mac-count

Description

The **show mac address-table max-mac-count** command is used to display the port security configuration on each port.

Syntax

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

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the port security configuration on port 1/0/1

Switch# show mac address-table max-mac-count interface gigabitEthernet 1/0/1

Chapter 61 Port Mirroring Commands

Port Mirroring allows the switch to send a copy of the traffic that passes through specified sources (ports, LAGs or the CPU) to a destination port. It does not affect the switching of network traffic on source ports, LAGs or the CPU. Usually, the monitoring port is connected to data diagnose device, which is used to analyze the monitored packets for monitoring and troubleshooting the network.

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

Example

Create monitor session 1 and configure port 1/0/1 as the monitoring port:

Switch(config)# monitor session 1 **destination interface gigabitEthernet** 1/0/1

Delete the monitoring port 1/0/2 from monitor session 1:

Switch(config)# no monitor session 1 **destination interface gigabitEthernet** 1/0/2

Delete the monitor session 1:

Switch(config)# no monitor session 1

61.2 monitor session source

Description

The **monitor session source** command is used to configure the monitored interface. To delete the corresponding monitored interface, please use **no monitor session source** command.

Syntax

monitor session *session_num* **source { cpu** *cpu_number* **| interface gigabitEthernet** *port-list* **| interface port-channel** *port-channel-id***}** *mode*

no monitor session *session_num* **source { cpu** *cpu_number* **| interface gigabitEthernet** *port-list* **| interface port-channel** *port-channel-id***}** *mode*

Parameter

session_num —— The monitor session number. It can only be specified as 1.

cpu_number —— The CPU number. It can only be specified as 1.

port-list —— List of the Ethernet port number. It is multi-optional.

lag-list —— List of LAG interfaces. It is multi-optional.

mode —— The monitor mode. There are three options: rx, tx and both. Rx (ingress monitoring mode), means the incoming packets received by the monitored interface will be copied to the monitoring port. Tx (egress monitoring mode), indicates the outgoing packets sent by the monitored interface will be copied to the monitoring port. Both (ingress and egress monitoring), presents the incoming packets received and the outgoing packets sent by the monitored interface will both be copied to the monitoring port.

Command Mode

Global Configuration Mode

Privilege Requirement

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

User Guidelines

1. The monitoring port is corresponding to current interface configuration mode.
2. Monitored ports number is not limited, but it can't be the monitoring port at the same time.
3. Whether the monitoring port and monitored ports are in the same VLAN or not is not demanded strictly.
4. The monitoring port and monitored ports cannot be link-aggregation member.

Example

Create monitor session 1, then configure port 4, 5, 7 as monitored port and enable ingress monitoring:

Switch(config)# monitor session 1 **source interface gigabitEthernet** 1/0/4-5,1/0/7 rx

Delete port 4 in monitor session 1 and its configuration:

Switch(config)# no monitor session 1 **source interface gigabitEthernet** 1/0/4 rx

61.3 monitor session 1 destination remote vlan

Description

The **monitor session 1 destination remote vlan** command is used to configure the RSPAN VLAN for remote port monitoring of egress packets. Please set the destination port before using this command. To disable this function, please use the **no monitor session 1 destination remote vlan** command.

Syntax

monitor session 1 destination remote vlan vlanid

no monitor session 1 destination remote vlan vlanid

Parameter

vlanid —— Remote port monitoring export message VLAN. The value ranges from 2 to 4094 and is mutually exclusive with voice VLAN and internal VLAN.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the RSPAN VLAN for remote port monitoring of egress packets:

```
Switch(config)#monitor session 1 destination remote vlan 4094
```

61.4 monitor session 1 source remote vlan

Description

The **monitor session 1 source remote vlan** command is used to monitor the packets added to the RSPAN VLAN port. To disable this function, use the **no monitor session 1 source remote vlan** command.

Syntax

monitor session 1 source remote vlan vlanid

no monitor session 1 source remote vlan vlanid

Parameter

vlanid —— Remote port monitoring export message VLAN. The value ranges from 2 to 4094 and is mutually exclusive with voice VLAN and internal VLAN.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Monitor the packets added to the RSPAN VLAN port:

```
Switch(config)#monitor session 1 source remote vlan 4094
```

61.5 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:

```
Switch(config)# show monitor session 1
```

Chapter 62 ACL Commands

ACL (Access Control List) is used to filter data packets by configuring a series of match conditions, operations and time ranges. It provides a flexible and secured access control policy and facilitates you to control the network security.

62.1 access-list create

Description

The **access-list create** command is used to create an ACL.

Syntax

access-list create *acl-id* [**name** *acl-name*]

no access-list create { *acl-id* **}**

Parameter

acl-id ——Enter an ACL ID. The IDs for MAC ACL are from 0 to 499. The IDs for IP ACL are from 500 to 999. The IDs for Combined ACL are from 1000 to 1499. The IDs for IPv6 ACL are from 1500 to 1999. The IDs for Packet Content ACL are from 2000 to 2499.

Note: Packet Content ACL is only available on certain devices.

acl-name —— Enter a name to identify the ACL.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create an IP ACL whose ID is 523:

Switch(config)# access-list create 523

62.2 access-list packet-content profile

Note: This command is only available on certain devices.

Description

The **access-list packet-content profile** command is used to specify the offset of each chunk. There are four chunks to be configured. They must be configured before you configure the chunk value&mask.

Syntax

access-list packet-content profile chunk-offset0 *offset0* **chunk-offset1** *offset1* **chunk-offset2** *offset2* **chunk-offset3** *offset3*

Parameter

offset0 -offset3: Specify the offset of each chunk. The value ranges from 0 to 31. When the offset is set as 31, it matches the first 127,128, 1, 2 bytes of the packet; when the offset is set as 0, it matches the 3, 4, 5, 6 bytes, and so on, for the rest of the offset value.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure a packet content profile with offset 0,1,2,3:

Switch(config)# access-list packet-content profile chunk-offset0 0 **chunk-offset1** 1 **chunk-offset2** 2 **chunk-offset3** 3

62.3 access-list resequence

Description

The **access-list resequence** command is used to resequence the rules by providing a Start Rule ID and Step value.

Syntax

access-list resequence *acl-id-or-name* **start** *start-rule-id* **step** *rule-id-step-value*

Parameter

acl-id-or-name —— The ACL ID or name.

start-rule-id —— The start rule ID.

rule-id-step-value —— The step value.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Resequence the rules of ACL 12 with the start ID as 1 and step value as 5:

Switch(config)# access-list resequence 12 **start** 1 **step** 5

62.4 access-list mac

Description

The **access-list mac** command is used to create MAC ACL. To delete the MAC ACL, please use **no access-list mac**.

Syntax

access-list mac *acl-id-or-name* **rule {** auto | *rule-id* **} {** deny | permit **} logging {**enable | disable**} [smac** *source-mac* **smask** *source-mac-mask* **] [dmac** *destination-mac* **dmask** *destination-mac-mask* **] [type** *ether-type***] [pri** *dot1p-priority***] [vid** *vlan-id***] [tseg** *time-range-name***]**

no access-list mac *acl-id-or-name* **rule** *rule-id*

Parameter

acl-id-or-name —— Enter the ID or name of the ACL that you want to add a rule for.

auto —— The rule ID will be assigned automatically and the interval between rule IDs is 5.

rule-id —— Assign an ID to the rule.

deny | permit —— Specify the action to be taken with the packets that match the rule. By default, it is set to permit. The packets will be discarded if “deny” is selected and forwarded if “permit” is selected.

enable | disable —— Enable or disable Logging function for the ACL rule. If "enable " is selected, the times that the rule is matched will be logged every 5 minutes. With ACL Counter trap enabled, a related trap will be generated if the matching times changes.

source-mac —— Enter the source MAC address. The format is FF:FF:FF:FF:FF:FF.

source-mac-mask —— Enter the mask of the source MAC address. This is required if a source MAC address is entered. The format is FF:FF:FF:FF:FF:FF.

destination-mac —— Enter the destination MAC address. The format is FF:FF:FF:FF:FF:FF.

destination-mac-mask —— Enter the mask of the destination MAC address. This is required if a destination MAC address is entered. The format is FF:FF:FF:FF:FF:FF.

ether-type —— Specify an Ethernet-type with 4 hexadecimal numbers.

dot1p-priority: The user priority ranges from 0 to 7. The default is No Limit.

vlan-id —— The VLAN ID ranges from 1 to 4094.

time-range-name —— The name of the time-range. The default is No Limit.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create MAC ACL 50 and configure Rule 5 to permit packets with source MAC address 00:34:a2:d4:34:b5:

Switch (config)#access-list create 50

Switch (config-mac-acl)#access-list mac 50 **rule** 5 **permit logging disable**

smac 00:34:a2:d4:34:b5 **smask** ff:ff:ff:ff:ff:ff

62.5 access-list ip

Description

The **access-list ip** command is used to add IP ACL rule. To delete the corresponding rule, please use **no access-list ip** command. IP ACLs analyze and process data packets based on a series of match conditions, which can be the source IP addresses and destination IP addresses carried in the packets.

Syntax

access-list ip *acl-id-or-name* **rule {**auto **|** *rule-id***} {**deny | permit**} logging {**enable | disable**} [sip** *sip-address* **sip-mask** *sip-address-mask* **] [dip** *dip-address* **dip-mask** *dip-address-mask* **] [dscp** *dscp-value***] [tos** *tos-value***]**

[pre *pre-value***] [frag** enable | disable**] [protocol** *protocol***[s-port** *s-port-number***] [s-port-mask** *s-port-mask***] [d-port** *d-port-number***] [d-port-mask** *d-port-mask***] [tcpflag** *tcpflag***]] [tseg** *time-range-name***]**

no access-list ip *acl-id-or-name* **rule** *rule-id*

Parameter

acl-id-or-name —— Enter the ID or name of the ACL that you want to add a rule for.

auto —— The rule ID will be assigned automatically and the interval between rule IDs is 5.

rule-id —— Assign an ID to the rule.

deny | permit —— Specify the action to be taken with the packets that match the rule. By default, it is set to permit. The packets will be discarded if "deny" is selected and forwarded if "permit" is selected.

logging {enable | disable**}** —— Enable or disable Logging function for the ACL rule. If "enable " is selected, the times that the rule is matched will be logged every 5 minutes. With ACL Counter trap enabled, a related trap will be generated if the matching times changes.

sip-address —— Enter the source IP address.

sip-address-mask —— Enter the mask of the source IP address. This is required if a source IP address is entered.

dip-address —— Enter the destination IP address.

dip-address-mask —— Enter the mask of the destination IP address. This is required if a destination IP address is entered.

dscp-value —— Specify the DSCP value between 0 and 63.

tos-value ——Specify an IP ToS value to be matched between 0 and 15.

pre-value ——Specify an IP Precedence value to be matched between 0 and 7.

frag {enable | disable} —— Enable or disable matching of fragmented packets. The default is disable. When enabled, the rule will apply to all fragmented packets and always permit to forward the last fragment of a packet.

Note: frag {enable | disable} is only available on certain devices.

protocol —— Specify a protocol type.

s-port-number —— Specify the source port number.

s-port-mask —— Specify the source port mask with 4 hexadecimal numbers.

d-port-number —— Specify the destination port number.

d-port-mask —— Specify the destination port mask with 4 hexadacimal numbers.

tcpflag —— For TCP protocol, specify the flag value using either binary numbers or * (for example, 01*010*). The default is *, which indicates that the flag will not be matched. The flags are URG (Urgent flag), ACK (acknowledge flag), PSH(push flag), RST(reset flag),SYN(synchronize flag), and FIN(finish flag).

time-range-name —— The name of the time-range. The default is No Limit.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create IP ACL 600, and configure Rule 1 to permit packets with source IP address 192.168.1.100:

Switch (config)#access-list create 600

Switch (config)#access-list ip 600 **rule** 1 permit **logging** disable **sip** 192.168.1.100 **sip-mask** 255.255.255.255

62.6 access-list combined

Description

The **access-list combined** command is used to add Combined ACL rule. To delete the corresponding rule, please use **no access-list extended** command.

Syntax

access-list combined *acl-id-or-name* **rule** {auto | *rule-id*} {deny | permit} **logging** {enable | disable} [**smac** *source-mac-address* **smask** *source-mac-mask*] [**dmac** *dest-mac-address* **dmask** *dest-mac-mask*] [**vid** *vlan-id*] [**type** *ether-type*] [**pri** *priority*] [**sip** *source-ip-address* **sip-mask** *source-ip-mask*]] [**dip** *destination-ip-address* **dip-mask** *destination-ip-mask*] **[dscp** *dscp-value***] [tos** *tos-value***] [pre** *pre-value***] [protocol** *protocol***[s-port** *s-port-number* **s-port-mask** *s-port-mask***] [d-port** *d-port-number* **d-port-mask** *d-port-mask***] [tcpflag** *tcpflag***]] [tseg** *time-range-name***]**

no access-list combined *acl-id-or-name* **rule** *rule-id*

Parameter

acl-id-or-name —— Enter the ID or name of the ACL that you want to add a rule for.

auto —— The rule ID will be assigned automatically and the interval between rule IDs is 5.

rule-id —— Assign an ID to the rule.

deny | permit —— Specify the action to be taken with the packets that match the rule. By default, it is set to permit. The packets will be discarded if “deny” is selected and forwarded if “permit” is selected.

logging {enable | disable} —— Enable or disable Logging function for the ACL rule. If "enable " is selected, the times that the rule is matched will be logged every 5 minutes. With ACL Counter trap enabled, a related trap will be generated if the matching times changes.

source-mac-address —— Enter the source MAC address.

source-mac-mask —— Enter the source MAC address mask.

dest-mac-address —— Enter the destination MAC address.

dest-mac-mask —— Enter the destination MAC address mask. This is required if a destination MAC address is entered.

vlan-id: The VLAN ID ranges from 1 to 4094.

ether-type —— Specify the Ethernet-type with 4 hexadecimal numbers.

priority —— The user priority ranges from 0 to 7. The default is No Limit.

source-ip: Enter the source IP address.

source-ip-mask —— Enter the mask of the source IP address. It is required if source IP address is entered.

destination-ip —— This is required if a source IP address is entered.

destination-ip-mask —— Enter the destination IP address mask. This is required if a destination IP address is entered.

dscp-value —— Specify the DSCP value between 0 and 63.

tos-value ——Specify an IP ToS value to be matched between 0 and 15.

pre-value ——Specify an IP Precedence value to be matched between 0 and 7.

protocol —— Specify a protocol type.

s-port-number —— Specify the source port number.

s-port-mask —— Specify the source port mask with 4 hexadecimal numbers.

d-port-number —— Specify the destination port number.

d-port-mask —— Specify the destination port mask with 4 hexadecimal numbers.

tcpflag —— For TCP protocol, specify the flag value using either binary numbers or * (for example, 01*010*). The default is *, which indicates that the flag will not be matched. The flags are URG (Urgent flag), ACK (acknowledge flag), PSH(push flag), RST(reset flag),SYN(synchronize flag), and FIN(finish flag).

time-range-name —— The name of the time-range. The default is No Limit.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create Combined ACL 1100 and configure Rule 1 to deny packets with source IP address 192.168.3.100 in VLAN 2:

Switch(config)# access-list create 1100

Switch(config)# access-list combined 1100 **logging** disable **rule** 1 permit **vid** 2 **sip** 192.168.3.100 **sip-mask** 255.255.255.255

62.7 access-list ipv6

Description

The **access-list ipv6** command is used to add IPv6 ACL rule. To delete the corresponding rule, please use **no access-list ipv6** command. IPv6 ACLs analyze and process data packets based on a series of match conditions, which can be the source IP addresses and destination IP addresses carried in the packets, the DSCP and flow-label value, etc.

Syntax

access-list ipv6 *acl-id-or-name* **rule** {auto | *rule-id* } {deny | permit} **logging** {enable | disable} [**class** *class-value*] [**flow-label** *flow-label-value*] [**sip** *source-ip-address* **sip-mask** *source-ip-mask*] [**dip** *destination-ip-address* **dip-mask** *destination-ip-mask*] [**s-port** *source-port-number*] [**d-port** *destination-port-number*] [**tseg** *time-range-name*]

no access-list ipv6 *acl-id-or-name* **rule** *rule-id*

Parameter

acl-id-or-name —— Enter the ID or name of the ACL that you want to add a rule for.

auto —— The rule ID will be assigned automatically and the interval between rule IDs is 5.

rule-id —— Assign an ID to the rule.

deny | permit —— Specify the action to be taken with the packets that match the rule. By default, it is set to permit. The packets will be discarded if “deny” is selected and forwarded if “permit” is selected.

logging {enable | disable} —— Enable or disable Logging function for the ACL rule. If "enable " is selected, the times that the rule is matched will be logged every 5 minutes. With ACL Counter trap enabled, a related trap will be generated if the matching times changes.

class-value —— Specify a class value to be matched. It ranges from 0 to 63.

flow-label-value —— Specify a Flow Label value to be matched.

source-ip-address —— Enter the source IP address. Enter the destination IPv6 address to be matched. All types of IPv6 address will be checked. You may enter a complete 128-bit IPv6 address but only the first 64 bits will be valid.

source-ip-mask —— Enter the source IP address mask. The mask is required if the source IPv6 address is entered. Enter the mask in complete format (for example, ffff:ffff:0000:ffff). The mask specifies which bits in the source IPv6 address to match the rule.

destination-ip-address —— Enter the destination IPv6 address to be matched. All types of IPv6 address will be checked. You may enter a complete 128-bit IPv6 addresses but only the first 64 bits will be valid.

destination-ip-mask: Enter the source IP address mask. The mask is required if the source IPv6 address is entered. Enter the mask in complete format (for example, ffff:ffff:0000:ffff). The mask specifies which bits in the source IPv6 address to match the rule.

source-port-number —— Enter the TCP/UDP source port if TCP/UDP protocol is selected.

destination-port-number —— Enter the TCP/UDP destination port if TCP/UDP protocol is selected.

time-range-name —— The name of the time-range. The default is No Limit.

Command Mode

Global Configuration Mode

Privilege Requirement

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

User Guidelines

Before binding an IPv6 ACL to a VLAN or interface, you should configure the SDM template as “enterpriseV6” and save your configurations.

Example

Create IPv6 ACL 1600 and configure Rule 1 to deny packets with source IPv6 address CDCD:910A:2222:5498:8475:1111:3900:2020:

Switch(config)# access-list create 1600

Switch(config)# access-list ipv6 1600 rule 1 deny **logging** disable **sip** CDCD:910A:2222:5498:8475:1111:3900:2020 **sip-mask** ffff:ffff:ffff:ffff

62.8 access-list packet-content config

Note: This command is only available on certain devices.

Description

The **access-list packet-content config** command is used to add Packet Content ACL rule. To delete the corresponding rule, please use **no access-list packet-content config** command. Packet content ACLs analyze and process data packets based on 4 chunk match conditions, each chunk can specify a user-defined 4-byte segment carried in the packet's first 128 bytes.

Syntax

access-list packet-content config *acl-id-or-name* **rule {**auto / *rule-id***} {**deny | permit**} logging {**enable | disable**}** [**chunk0** *value* **mask0** *mask*] [**chunk1** *value* **mask1** *mask*] [**chunk2** *value* **mask2** *mask*] [**chunk3** *value* **mask3** *mask*] [**tseg** *time-segment*]

no access-list packet-content config *acl-id-or-name* **rule** *rule-id*

Parameter

acl-id-or-name —— Enter the ID or name of the ACL that you want to add a rule for.

auto —— The rule ID will be assigned automatically and the interval between rule IDs is 5.

rule-id —— Assign an ID to the rule.

deny | permit —— Specify the action to be taken with the packets that match the rule. Deny means to discard; permit means to forward. By default, it is set to permit.

logging {enable | disable} —— Enable or disable Logging function for the ACL rule. If "enable" is selected, the times that the rule is matched will be logged every 5 minutes. With ACL Counter trap enabled, a related trap will be generated if the matching times changes.

value —— Specify the chunk value, ranging from 0-ffffffff.

mask ——Specify the chunk mask, ranging from 0-ffffffff. Chunk mask here must be written completely in 4-byte hex mode, like '0000ffff'.

time-segment —— The name of the time-range. The default is No Limit.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create a packet-content ACL rule with all 4 chunks configured, the rule id is 1 and the default action is permit:

SwitchSwitch(config)# access-list packet-content config rule 1 permit **logging** disable **chunk0** 45ea **mask0** 0000ffff **chunk1** 1111ffff **mask1** ffffffff **chunk2** ee34 **mask2** ffff0000 **chunk3** 7878 **mask3** 000ffae3

62.9 access-list action

Description

The **access-list action** command is used to specify a rule to be configured with policies and enter Action Configuration mode. To delete the corresponding policies, please use **no access-list action** command.

Syntax

access-list action *acl-id-or-name* **rule** *rule-id*

no access-list action *acl-id-or-name* **rule** *rule-id*

Parameter

acl-id-or-name —— Enter the ID or name of the ACL.

rule-id —— Enter the ID of the ACL rule.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the rule 1 of ACL 200 to be configured with policies:

Switch(config)# access-list action 200 **rule** 1

62.10 redirect

Description

The **redirect interface** command is used to define the policy to redirect the matched packets to the desired port. To disable this policy, please use **no redirect interface** command.

Syntax

redirect interface { fastEthernet *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}**

no redirect interface { fastEthernet *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}**

Parameter

port —— The destination port to which the packets will be redirected. The default is All.

Command Mode

Action Configuration Mode

Privilege Requirement

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

Example

Define the policy to redirect the matched packets to port 1/0/1 for rule 1 of ACL 6:

Switch(config)# access-list action 6 **rule** 1

Switch(config-action)# redirect interface gigabitEthernet 1/0/1

62.11 s-condition

Description

The **s-condition** command is used to limit the rate of the matched packets. To restore the settings to the defaults, please use **no s-condition**.

Syntax

s-condition rate *rate* **burst** *burst-size* **osd { none | discard | remark dscp** *dscp* **}**

no s-condition

Parameter

rate —— Specify a rate, ranging from 0 to 1000000kbps.

burst-size —— Specify the number of bytes allowed in one second ranging from 1 to 128.

osd ——Select either "none" or "discard" as the action to be taken for the packets whose rate is beyond the specified rate. The default is None. When "remark dscp" is selected, you also need to specify the DSCP value for the matched packets. The DSCP value ranges from 0 to 63.

Note: Remark DSCP is only available on certain devices.

Command Mode

Action Configuration Mode

Privilege Requirement

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

Example

Configure a policy for rule 1 of ACL 6: limit the transmission rate of the matched packets as 1000 Kbps and if the number of bytes per second is beyond 100, the packets will be discarded by the switch:

Switch(config)#access-list action 6 **rule** 1

Switch(config-action)# s-condition rate 1000 **burst** 100 **osd** discard

62.12 s-mirror

Description

The **s-mirror** command is used to define the policy to mirror the matched packets to the desired port. To disable this policy, please use **no s-mirror** command.

Syntax

s-mirror interface { **fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* }

Parameter

port —— The destination port to which the packets will be mirrored.

Command Mode

Action Configuration Mode

Privilege Requirement

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

Example

Configure a policy for rule 1 of ACL 6: specify the mirror port as Gigabit Ethernet port 1/0/2 for the data packets matching this rule:

Switch(config)#access-list action 6 **rule** 1

Switch(config-action)#s-mirror interface gigabitEthernet 1/0/2

62.13 qos-remark

Description

The **qos-remark** command is used to configure QoS Remark function of policy action. To restore the settings to the default, please use no **qos-remark**.

Syntax

qos-remark [**dscp** *dscp*] [**priority** *pri*] [**dot1p** dot1p-pri]

no qos-remark

Parameter

dscp —— DSCP of QoS Remark. Specify the DSCP region for the data packets matching the corresponding ACL. DSCP ranges from 0 to 63. By default, it is not limited.

pri —— Local Priority of QoS Remark. Specify the local priority for the data packets matching the corresponding ACL. Local Priority ranges from 0 to 7.

dot1p-pri —— 802.1P priority of QoS Remark. This remark configuration will change the data packet's 802.1P priority field to the dot1p-pri you set. 802.1P priority ranges from 0 to 7.

Note: The DSCP and dot1p cannot be configured at the same time.

Command Mode

Action Configuration Mode

Privilege Requirement

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

Example

Configure a policy for rule 1 of ACL 6: specify the DSCP region as 30 and local priority 2 for the packets matching this rule:

Switch(config)#access-list action 6 **rule** 1

Switch(config-action)# qos-remark dscp 30 **priority** 2

62.14 access bind

Description

The **access-list policy name** command is used to add Policy. To delete the corresponding Policy, please use **no access-list policy name** command. A Policy is used to control the data packets those match the corresponding ACL rules.

Syntax

access-list bind *acl-id-or-name* **interface { [vlan** *vlan-list* **] | [fastEthernet** *port-list* **] | [gigabitEthernet** *port-list* **] | [ten-gigabitEthernet** *port-list* **] }**

no access-list bind *acl-id-or-name* **interface { [vlan** *vlan-list* **] | [fastEthernet** *port-list* **] | [gigabitEthernet** *port-list* **] | [ten-gigabitEthernet** *port-list* **] }**

Parameter

acl-id-or-name —— Enter the ID or name of the ACL that you want to add a rule for.

vlan-list —— Specify the ID or the ID list of the VLAN(s) that you want to bind the ACL to. The valid values are from 1 to 4094, for example, 2-3,5.

port-list —— Specify the number or the list of the Ethernet port that you want to bind the ACL to.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Bind ACL 1 to port 3 and VLAN 4:

Switch(config)#access-list bind 1 **interface vlan** 4 **gigabitEthernet** 1/0/3

62.15 show access-list

Description

The **show access-list** command is used to display configuration of ACL.

Syntax

show access-list *acl-id-or-name*

Parameter

acl-id-or-name —— The ID or name of the ACL selected to display the configuration.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of the MAC ACL whose ID is 20:

Switch(config)# show access-list 20

62.16 show access-list bind

Description

The **show access-list bind** command is used to display the configuration of ACL binding.

Syntax

show access-list bind

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of Policy bind:

```
Switch(config)# show access-list bind
```

62.17 show access-list status

Description

The **show access-list status** command is used to display usage status of ACL entry resource.

Syntax

show access-list status

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the usage status of ACL entry resource:

```
Switch(config)# show access-list status
```

62.18 show access-list counter

Description

The **show access-list counter** command is used to display the packet counter of a specified ACL.

Syntax

show access-list *acl-id-or-name* **counter**

Parameter

acl-id-or-name —— The ID or name of the ACL to display.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the packet counter of ACL 100:

Switch(config)# show access-list 100 **counter**

62.19 clear access-list

Description

The **clear access-list** command is used to clear the counter of matched packets of a specified ACL or rule.

Syntax

clear access-list *acl-id-or-name* **[rule** *rule-id***]**

Parameter

acl-id-or-name —— The ID or name of the ACL.

rule-id—— The ID of the rule.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Clear the packet counter of ACL 100:

Switch(config)# clear access-list 100

Chapter 63 IPv4 IMPB Commands

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

63.1 ip source binding

Description

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

Syntax

ip source binding *hostname ip-addr mac-addr* **vlan** *vlan-id* **interface** { **fastEthernet** *port* **|** **gigabitEthernet** *port* **|** **ten-gigabitEthernet** *port* **|** **port-channel** *port-channel-id* } { none | arp-detection | ip-verify-source | both }

no ip source binding index *ip-addr*

Parameter

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

ip-addr—— The IP address of the Host.

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

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

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

none | arp-detection | ip-verify-source | both ——The protect type for the entry. “arp-detection” indicates ARP detection; “ip-verify-source” indicates IP source filter; “none” indicates applying none; “both” indicates applying both.

ip-addr—— The IP address of the entry to be deleted.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

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

Switch(config)#ip source binding host1 192.168.0.1 00:00:00:00:00:01 **vlan** 2 **interface gigabitEthernet** 1/0/5 arp-detection

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

Switch(config)#no ip source binding index 5

63.2 ip dhcp snooping

Description

The **ip dhcp snooping** command is used to enable DHCP Snooping function globally. To disable DHCP Snooping function globally, please use **no ip dhcp snooping** command. DHCP Snooping functions to monitor the process of the Host obtaining the IP address from DHCP server, and record the IP address, MAC address, VLAN and the connected Port number of the Host for automatic binding.

Syntax

ip dhcp snooping

no ip dhcp snooping

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the DHCP Snooping function globally:

Switch(config)#ip dhcp snooping

63.3 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:

Switch(config)#ip dhcp snooping vlan 1,4,6-7

63.4 ip dhcp snooping max-entries

Description

The **ip dhcp snooping max-entries** command is used to configure the maximum number of entries that can be learned on a port via DHCP Snooping. To restore to the default setting, please use **no ip dhcp snooping max-entries** command.

Syntax

ip dhcp snooping max-entries *value*

no ip dhcp snooping max-entries

Syntax

value —— Enter the value of maximum number of entries that can be learned on the port via DHCP Snooping.

Command Mode

Interface Configuration Mode (interface 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 number of entries that can be learned on port 1 as 100:

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#ip dhcp snooping max-entries 100

63.5 ip dhcp snooping trust

Description

The **ip dhcp snooping trust** command is used to configure the trust status of a specified interface, and only DHCP Server connected to a trusted port can assign packets to clients. To delete the status, please use **no ip dhcp snooping trust** command.

Syntax

ip dhcp snooping trust

no ip dhcp snooping trust

Command Mode

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

Privilege Requirement

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

Example

Enable DHCP Snooping trust function for port 1/0/3:

```
Switch(config)#interface gigabitEthernet 1/0/3
Switch(config-if)#ip dhcp snooping trust
```

63.6 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:

```
Switch(config)#show ip source binding
```

63.7 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:

Switch#show ip dhcp snooping

63.8 show ip dhcp snooping interface

Description

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

Syntax

show ip dhcp snooping interface [**gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parameters

port—— The Ethernet port number.

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

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DHCP Snooping configuration of all Ethernet ports and port channels:

Switch#show ip dhcp snooping interface

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

Switch#show ip dhcp snooping interface gigabitEthernet 1/0/5

Chapter 64 IPv6 IMPB Commands

You can bind the IPv6 address, MAC address, VLAN and the connected Port number of the Host together, which can be the condition for the ARP Inspection and IP verify source to filter the packets.

64.1 ipv6 source binding

Description

The **ipv6 source binding** command is used to bind the IPv6 address, MAC address, VLAN ID and the Port number together manually. You can manually bind the IPv6 address, MAC address, VLAN ID and the Port number together in the condition that you have got the related information of the Hosts in the LAN. To delete the IPv6-MAC–VID-PORT entry from the binding table, please use **no ipv6 source binding index** command.

Syntax

ipv6 source binding *hostname ipv6-addr mac-addr* **vlan** *vlan-id* **interface** { **fastEthernet** *port* **|** **gigabitEthernet** *port* **|** **ten-gigabitEthernet** *port* **|** **port-channel** *port-channel-id* } { none | nd-detection | ipv6-verify-source | both }

no ipv6 source binding index *ipv6-addr*

Parameter

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

Ipv6-addr—— The IP address of the Host.

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

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

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

none | nd-detection | ipv6-verify-source | both ——The protect type for the entry. “nd-detection” indicates ND detection; “ipv6-verify-source” indicates IPv6 source filter; “none” indicates applying none; “both” indicates applying both.

Ipv6-addr—— The IPv6 address of the entry to be deleted.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

The following example shows how to bind an entry with the hostname host1, IPv6 address 2001:0:9d38:90d5::34, MAC address AA-BB-CC-DD-EE-FF, VLAN ID 10, port number 1/0/5, and enable this entry for ND Detection.

Switch(config)# ipv6 source binding host1 2001:0:9d38:90d5::34 aa:bb:cc:dd:ee:ff **vlan** 10 **interface gigabitEthernet** 1/0/5 nd-detection

64.2 ipv6 dhcp snooping

Description

The **ipv6 dhcp snooping** command is used to enable DHCPv6 Snooping function globally. To disable DHCPv6 Snooping function globally, please use **no ipv6 dhcp snooping** command. DHCPv6 Snooping functions to monitor the process of the Host obtaining the IP address from DHCPv6 server, and record the IPv6 address, MAC address, VLAN and the connected Port number of the Host for automatic binding.

Syntax

ipv6 dhcp snooping

no ipv6 dhcp snooping

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the DHCPv6 Snooping function globally:

Switch(config)#ipv6 dhcp snooping

64.3 ipv6 dhcp snooping vlan

Description

The **ipv6 dhcp snooping vlan** command is used to enable DHCP Snooping function on a specified VLAN. To disable DHCP Snooping function on this VLAN, please use **no ipv6 dhcp snooping vlan** command.

Syntax

ipv6 dhcp snooping vlan *vlan-range*

no ipv6 dhcp snooping vlan *vlan-range*

Parameter

vlan-range —— Specify the VLANs to enable the DHCP snooping function, in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the DHCPv6 Snooping function on VLAN 1,4,6-7:

Switch(config)#ipv6 dhcp snooping vlan 1,4,6-7

64.4 ipv6 dhcp snooping max-entries

Description

The **ipv6 dhcp snooping max-entries** command is used to configure the maximum number of entries that can be learned on a port via DHCPv6 Snooping. To restore to the default setting, please use **no ipv6 dhcp snooping max-entries** command.

Syntax

Ipv6 dhcp snooping max-entries *value*

no ipv6 dhcp snooping max-entries

Syntax

value: Enter the value of maximum number of entries that can be learned on the port via DHCPv6 Snooping.

Command Mode

Interface Configuration Mode (interface 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 number of entries that can be learned on port 1 as 100:

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#ipv6 dhcp snooping max-entries 100

64.5 ipv6 nd snooping

Description

The **ipv6 nd snooping** command is used to enable ND snooping function globally. To disable ND Snooping function globally, please use **no ipv6 nd snooping** command. ND Snooping functions to monitor the process of the duplication address detection, and record the IPv6 address, MAC address, VLAN and the connected Port number of the Host for automatic binding.

Syntax

ipv6 nd snooping

no ipv6 nd snooping

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the ND snooping function globally:

T160G-28TS(config)#ipv6 nd snooping

64.6 ipv6 nd snooping vlan

Description

The **ipv6 nd snooping vlan** command is used to enable ND snooping function on a specified VLAN. To disable ND Snooping function on this VLAN, please use **no ipv6 nd snooping vlan** command.

Syntax

ipv6 nd snooping vlan *vlan-range*

no ipv6 nd snooping vlan *vlan-range*

Parameter

vlan-range —— Specify the VLANs to enable the ND snooping function, in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the ND snooping function on VLAN 1,4,6-7:

Switch(config)#ipv6 nd snooping vlan 1,4,6-7

64.7 ipv6 nd snooping max-entries

Description

The **ipv6 nd snooping max-entries** command is used to specify the maximum number of binding entries that are allow to be bound to a port. To return the default, please use **no ipv6 nd snooping max-entries** command.

Syntax

ipv6 nd snooping max-entries *value*

no ipv6 nd snooping max-entries

Parameter

value —— Specify the maximum number of ND snooping entries on this interface.

Command Mode

Interface Configuration Mode (interface 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 number of binding entries from ND Snooping of Gigabit Ethernet port 1/0/2 is 100:

Switch(config)#interface gigabitEthernet 1/0/2

Switch(config-if)#ipv6 nd snooping max-entries 100

64.8 show ipv6 source binding

Description

The **show ipv6 source binding** command is used to display the IPv6-MAC-VID- PORT binding table.

Syntax

show ipv6 source binding

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IPv6-MAC-VID-PORT binding table:

```
Switch(config)#show ipv6 source binding
```

64.9 show ipv6 dhcp snooping

Description

The **show ipv6 dhcp snooping** command is used to display the running status of DHCPv6 Snooping.

Syntax

show ipv6 dhcp snooping

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the running status of DHCPv6 Snooping:

```
Switch#show ipv6 dhcp snooping
```

64.10 show ipv6 dhcp snooping interface

Description

The **show ipv6 dhcp snooping interface** command is used to display the DHCPv6 Snooping configuration of a desired Gigabit Ethernet port/port channel or of all Ethernet ports/port channels.

Syntax

show ipv6 dhcp snooping interface [**gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parameters

port —— The Ethernet port number.

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

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DHCPv6 Snooping configuration of all Ethernet ports and port channels:

Switch#show ipv6 dhcp snooping interface

Display the DHCPv6 Snooping configuration of Gigabit Ethernet port 1/0/5:

Switch#show ipv6 dhcp snooping interface gigabitEthernet 1/0/5

64.11 show ipv6 nd snooping

Description

The **show ipv6 nd snooping** command is used to display the running status of ND Snooping.

Syntax

show ipv6 nd snooping

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the running status of ND Snooping:

Switch#show ipv6 nd snooping

64.12 show ipv6 nd snooping interface

Note: This command is only available on certain devices.

Description

The **show ipv6 nd snooping interface** command is used to display the ND Snooping configuration of a desired Gigabit Ethernet port/port channel or of all Ethernet ports/port channels.

Syntax

show ipv6 nd snooping interface [**gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parameters

port —— The Ethernet port number.

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

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the ND Snooping configuration of all Ethernet ports and port channels:

Switch#show ipv6 nd snooping interface

Display the ND Snooping configuration of Gigabit Ethernet port 1/0/5:

Switch#show ipv6 nd snooping interface gigabitEthernet 1/0/5

Chapter 65 IP Verify Source Commands

IP Verify Source is to filter the IP packets based on the IP-MAC Binding entries. Only the packets matched to the IP-MAC Binding rules can be processed, which can enhance the bandwidth utility.

65.1 ip verify source

Description

The **ip verify source** command is used to configure the IP Verify Source mode for a specified port. To disable the IP Verify Source function, please use **no ip verify source** command.

Syntax

ip verify source { sip+mac | sip }

no ip verify source

Parameter

sip+mac —— Security type. "sip+mac" indicates that only the packets with its source IP address, source MAC address and port number matched to the IP-MAC binding rules can be processed.

sip —— Security type. "sip" indicates that only the packets with its source IP address and port number matched to the IP-MAC binding rules can be processed.

Note: sip is only available on certain devices.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the IP Verify Source function for Gigabit Ethernet ports 5-10. Configure that only the packets with its source IP address, source MAC

address and port number matched to the IP-MAC binding rules can be processed:

Switch(config)#interface range gigabitEthernet 1/0/5-10

Switch(config-if-range)#ip verify source sip+mac

65.2 ip verify source logging

Description

The **ip verify source logging** command is used to enable the log feature. With this feature enabled, the switch will generate a log when illegal packets are received. To disable the log feature, please use **no ip verify source logging** command.

Syntax

ip verify source logging

no ip verify source logging

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the log feature to make the switch generate logs when receiving illegal packets:

Switch(config)#ip verify source logging

65.3 show ip verify source

Description

The **show ip verify source** command is used to display the IP Verify Source configuration information.

Syntax

show ip verify source

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IP Verify Source configuration information:

Switch(config)#show ip verify source

65.4 show ip verify source interface

Description

The **show ip verify source interface** command is used to display the IP verify source configuration of a desired Gigabit Ethernet port.

Syntax

show ip verify source interface [fastEthernet *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]**

Parameters

port —— The Ethernet port number.

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

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IP verify source configuration of Gigabit Ethernet port 1/0/5:

Switch#show ip verify source interface gigabitEthernet 1/0/5

Chapter 66 IPv6 Verify Source Commands

IPv6 Verify Source is to filter the IPv6 packets based on the IPv6-MAC Binding entries. Only the packets matched to the IPv6-MAC Binding rules can be processed, which can enhance the bandwidth utility.

Before configuring IPv6 Verify Source feature, you should configure the SDM template as "enterpriseV6" and save your configurations.

66.1 ipv6 verify source

Description

The **ipv6 verify source** command is used to configure the IPv6 Verify Source mode for a specified port. To disable the IPv6 Verify Source function, please use **no ipv6 verify source** command.

Syntax

ipv6 verify source { sipv6+mac | sipv6 }

no ipv6 verify source

Parameter

sipv6+mac —— Security type. "sipv6+mac" indicates that only the packets with its source IPv6 address, source MAC address and port number matched to the IPv6-MAC binding rules can be processed.

sipv6 —— Security type. "sipv6" indicates that only the packets with its source IPv6 address and port number matched to the IPv6-MAC binding rules can be processed.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the IPv6 Verify Source function for Gigabit Ethernet ports 5-10. Configure that only the packets with its source IPv6 address, source MAC

address and port number matched to the IPv6-MAC binding rules can be processed:

```
Switch(config)#interface range gigabitEthernet 1/0/5-10
Switch(config-if-range)#ipv6 verify source sipv6+mac
```

66.2 show ipv6 verify source

Description

The **show ipv6 verify source** command is used to display the IPv6 Verify Source configuration information.

Syntax

show ipv6 verify source

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IPv6 Verify Source configuration information:

```
Switch(config)#show ipv6 verify source
```

66.3 show ipv6 verify source interface

Description

The **show ipv6 verify source interface** command is used to display the IPv6 verify source configuration of a desired Gigabit Ethernet port.

Syntax

show ipv6 verify source interface gigabitEthernet *port*

Parameters

port—— The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the IPv6 verify source configuration of Gigabit Ethernet port 1/0/5:

Switch#show ipv6 verify source interface gigabitEthernet 1/0/5

Chapter 67 DHCPv4 Filter Commands

DHCPv4 Filter function allows the user to not only to restrict all DHCP Server packets but also to receive any specified DHCP server packet by any specified DHCP client, it is useful when one or more DHCP servers are present on the network and both provide DHCP services to different distinct groups of clients.

67.1 ip dhcp filter

Description

The **ip dhcp filter** command is used to enable DHCP Filter function globally. To disable DHCP Filter function globally, please use **no ip dhcp filter** command.

Syntax

ip dhcp filter

no ip dhcp filter

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the DHCP Filter function globally:

```
Switch(config)#ip dhcp filter
```

67.2 ip dhcp filter (interface)

Description

The **ip dhcp filter (interface)** command is used to enable DHCP Filter function on a specified port. To disable DHCP Filter function on this port, please use **no ip dhcp filter (interface)** command.

Syntax

ip dhcp filter

no ip dhcp filter

Command Mode

Interface Configuration Mode (interface 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 DHCP Filter on port 1/0/1

```
Switch(config)#interface gigabitEthernet 1/0/1
Switch(Config-if)#ip dhcp filter
```

67.3 ip dhcp filter mac-verify

Description

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

Syntax

ip dhcp filter mac-verify

no ip dhcp filter mac-verify

Command Mode

Interface Configuration Mode (interface 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 Gigabit Ethernet port 10/2:

Switch(config)#interface gigabitEthernet 1/0/2

Switch(config-if)#ip dhcp filter mac-verify

67.4 ip dhcp filter limit rate

Description

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

Syntax

ip dhcp filter limit rate *value*

no ip dhcp filter limit rate

Parameter

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

Command Mode

Interface Configuration Mode (interface 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 GigabitEthernet port 2 as 20 pps:

Switch(config)#interface gigabitEthernet 1/0/2

Switch(config-if)#ip dhcp filter limit rate 20

67.5 ip dhcp filter decline rate

Description

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

Syntax

ip dhcp filter decline rate *value*

no ip dhcp filter decline rate

Parameter

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

Command Mode

Interface Configuration Mode (interface 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 Gigabit Ethernet port 1/0/2:

Switch(config)#interface gigabitEthernet 1/0/2

Switch(config-if)#ip dhcp filter decline rate 20

67.6 ip dhcp filter server permit-entry

Description

The **ip dhcp filter server permit-entry** command is used to add entry for the legal DHCP server. To restore to the default option, please use **no ip dhcp snooping information strategy** command.

Syntax

ip dhcp filter server permit-entry server-ip *ipAddr* **client-mac** *macAddr* **interface { fastEthernet** *port* **| gigabitEthernet port | ten-gigabitEthernet** *port* **| interface port-channel** *port-channel-id***}**

no ip dhcp filter server permit-entry server-ip *ipAddr* **client-mac** *macAddr* **interface { fastEthernet** *port* **| gigabitEthernet port | ten-gigabitEthernet** *port* **| interface port-channel** *port-channel-id***}**

Parameter

ipAddr —— Specify the IP address of the legal DHCPv4 server.

macAddr —— Specify the MAC address of the DHCP Client. The value "all" means all client mac addresses.

port-list / *port-channel-id* —— Specify the port that the legal DHCPv4 server is connected to.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create an entry for the legal DHCPv4 server whose IP address is 192.168.0.100 and connected port number is 1/0/1 without client MAC address restricted:

Switch(config)#ip dhcp filter server permit-entry server-ip 192.168.0.100 **client-mac** all **interface gigabitEthernet** 1/0/1

67.7 show ip dhcp filter

Description

The **show ip dhcp filter** command is used to display the configuration of DHCP Filter.

Syntax

show ip dhcp filter

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DHCP Filter configuration:

Switch#show ip dhcp filter

67.8 show ip dhcp filter interface

Description

The **show ip dhcp filter interface** command is used to display the configuration of DHCP Filter on ports.

Syntax

show ip dhcp filter interface [fastEthernet *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]**

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DHCP Filter configuration on port 1/0/3:

Switch#show ip dhcp filter interface gigabitEthernet 1/0/3

67.9 show ip dhcp filter server permit-entry

Description

The **show ip dhcp filter server permit-entry** command is used to display the legal server configuration.

Syntax

show ip dhcp filter server permit-entry

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the legal DHCP server configuration:

```
Switch#show ip dhcp filter server permit-entry
```

Chapter 68 DHCPv6 Filter Commands

DHCPv6 Filter function allows the user to not only to restrict all DHCPv6 Server packets but also to receive any specified DHCPv6 server packet by any specified DHCPv6 client, it is useful when one or more DHCPv6 servers are present on the network and both provide DHCPv6 services to different distinct groups of clients.

68.1 ipv6 dhcp filter

Description

The **ipv6 dhcp filter** command is used to enable DHCP Filter function globally. To disable DHCPv6 Filter function globally, please use **no ipv6 dhcp filter** command.

Syntax

ipv6 dhcp filter

no ipv6 dhcp filter

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the DHCPv6 Filter function globally:

```
Switch(config)#ipv6 dhcp filter
```

68.2 ipv6 dhcp filter (interface)

Description

The **ipv6 dhcp filter (interface)** command is used to enable DHCPv6 Filter function on a specified port. To disable DHCPv6v Filter function on this port, please use **no ipv6 dhcp filter (interface)** command.

Syntax

ipv6 dhcp filter

no ipv6 dhcp filter

Command Mode

Interface Configuration Mode (interface 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 DHCPv6 Filter on port 1/0/1

```
Switch(config)#interface gigabitEthernet 1/0/1
Switch(Config-if)#ipv6 dhcp filter
```

68.3 ipv6 dhcp filter limit rate

Description

The **ipv6 dhcp filter limit rate** command is used to enable the Flow Control feature for the DHCPv6 packets. The excessive DHCPv6 packets will be discarded. To restore to the default configuration, please use **no ipv6 dhcp filter limit rate** command.

Syntax

ipv6 dhcp filter limit rate *value*

no ipv6 dhcp filter limit rate

Parameter

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

Command Mode

Interface Configuration Mode (interface 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 GigabitEthernet port 2 as 20 pps:

Switch(config)#interface gigabitEthernet 1/0/2

Switch(config-if)#ipv6 dhcp filter limit rate 20

68.4 ipv6 dhcp filter decline rate

Description

The **ipv6 dhcp filter decline rate** command is used to enable the Decline Protect feature and configure the rate limit on DHCP Decine packets. The excessive DHCPv6 Decline packets will be discarded. To disable the Decline Protect feature, please use **no ipv6 dhcp filter decline rate** command.

Syntax

ipv6 dhcp filter decline rate *value*

no ipv6 dhcp filter decline rate

Parameter

value —— Specify the rate limit of DHCPv6 Decline packets, and the optional values are 0, 5, 10, 15, 20, 25 and 30 (units:packet/second). It default value is 0, which stands for “disable”.

Command Mode

Interface Configuration Mode (interface 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 DHCPv6 Decline packets as 20 packets per second on Gigabit Ethernet port 1/0/2:

Switch(config)#interface gigabitEthernet 1/0/2

Switch(config-if)#ipv6 dhcp filter decline 20

68.5 ipv6 dhcp filter server permit-entry

Description

The **ipv6 dhcp filter server permit-entry** command is used to add entry for the legal DHCPv6 server. To restore to the default option, please use **no ipv6 dhcp snooping information strategy** command.

Syntax

ipv6 dhcp filter server permit-entry server-ip *ipAddr* **interface { fastEthernet** *port* **| gigabitEthernet port | ten-gigabitEthernet** *port* **| interface port-channel** *port-channel-id***}**

no ipv6 dhcp filter server permit-entry server-ip *ipAddr* **interface { fastEthernet** *port* **| gigabitEthernet port | ten-gigabitEthernet** *port* **| interface port-channel** *port-channel-id***}**

Parameter

ipAddr —— Specify the IPv6 address of the legal DHCPv6 server.

port-list / *port-channel-id* —— Specify the port that the legal DHCPv6 server is connected to.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Create an entry for the legal DHCPv6 server whose IP address is 192.168.0.100 and connected port number is 1/0/1:

```
Switch(config)#ipv6 dhcp filter server permit-entry server-ip 2003::1
interface gigabitEthernet 1/0/1
```

68.6 show ipv6 dhcp filter

Description

The **show ipv6 dhcp filter** command is used to display the configuration of DHCPv6 Filter.

Syntax

show ipv6 dhcp filter

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DHCPv6 Filter configuration:

```
Switch#show ipv6 dhcp filter
```

68.7 show ipv6 dhcp filter interface

Description

The **show ipv6 dhcp filter interface** command is used to display the configuration of DHCPv6 Filter on ports.

Syntax

show ipv6 dhcp filter interface [fastEthernet *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]**

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the DHCPv6 Filter configuration on port 1/0/3:

Switch#show ipv6 dhcp filter interface gigabitEthernet 1/0/3

68.8 show ip dhcp filter server permit-entry

Description

The **show ipv6 dhcp filter server permit-entry** command is used to display the legal server configuration.

Syntax

show ipv6 dhcp filter server permit-entry

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the legal DHCPv6 server configuration:

Switch#show ipv6 dhcp filter server permit-entry

Chapter 69 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.

69.1 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:

```
Switch(config)#ip dos-prevent
```

69.2 ip dos-prevent type

Description

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

Syntax

ip dos-prevent type { land | scan-synfin | xma-scan | null-scan | port-less-1024 | blat | ping-flood | syn-flood | win-nuke | ping-of-death | smurf }

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

Parameter

land ——The attacker sends a specific fake SYN (synchronous) packet to the destination host. Because both of the source IP address and the destination IP address of the SYN packet are set to be the IP address of the host, the host will be trapped in an endless circle of building the initial connection.

scan-synfin ——The attacker sends the packet with its SYN field and the FIN field set to 1. The SYN field is used to request initial connection whereas the FIN field is used to request disconnection. Therefore, the packet of this type is illegal.

xma-scan ——The attacker sends the illegal packet with its TCP index, FIN, URG and PSH field set to 1.

null-scan ——The attacker sends the illegal packet with its TCP index and all the control fields set to 0. During the TCP connection and data transmission, the packets with all control fields set to 0 are considered illegal.

port-less-1024 ——The attacker sends the illegal packet with its TCP SYN field set to 1 and source port smaller than 1024.

blat ——The attacker sends the illegal packet with the same source port and destination port on Layer 4 and with its URG field set to 1. Similar to the Land Attack, the system performance of the attacked host is reduced because the Host circularly attempts to build a connection with the attacker.

ping-flood ——The attacker floods the destination system with Ping packets, creating a broadcast storm that makes it impossible for the system to respond to legal communication.

syn-flood ——The attacker uses a fake IP address to send TCP request packets to the server. Upon receiving the request packets, the server responds with SYN-ACK packets. Since the IP address is fake, no response will be returned. The server will keep on sending SYN-ACK packets. If the attacker sends overflowing fake request packets, the network resource will be occupied maliciously and the requests of the legal clients will be denied.

win-nuke ——Because the Operation System with bugs cannot correctly process the URG (Urgent Pointer) of TCP packets, the attacker sends this

type of packets to the TCP port139 (NetBIOS) of the host with the Operation System bugs, which will cause the host with a blue screen.

ping-of-death ——Ping of Death attack means that the attacker sends abnormal ping packets larger than 65535 bytes to cause system crash on the target computer.

Note: ping-of-death is only available on certain devices.

smurf ——Smurf attack is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic.

Note: smurf is only available on certain devices.

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:

Switch(config)#ip dos-prevent type land

69.3 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:

```
Switch(config)#show ip dos-prevent
```

Chapter 70 sFlow Commands (Only for Certain Devices)

Note: sFlow commands are only available on certain devices.

sFlow (Sampled Flow) is a technology for accurately monitoring network traffic at high speeds. The sFlow monitoring system consists of a sFlow agent (embedded in a switch or router or in a standalone probe) and a central sFlow collector. The sFlow agent is a virtual entity using sampling technology to capture traffic statistics from the device it is monitoring. The sFlow collector can be a host receiving sFlow datagrams from the sFlow agent.

The sFlow feature is implemented as follows: the sFlow sampler take samples of traffic statistics and send sFlow datagrams to the sFlow agent for processing. The sFlow agent will forward sFlow datagrams to the sFlow collector for analysis. The analytic results can be displayed on the sFlow collector.

70.1 sflow address

Description

The **sflow address** command is used to configure the sFlow agent's IP address. To delete the configured address, please use **no sflow address** command.

Syntax

sflow address { *ipv4-addr* }

no sflow address { *ipv4-addr* }

Parameter

ipv4-addr ——The IP address of the sFlow agent. The type of the IP address should be IPv4. For example, you can set the switch's management IP as the IP address of the sFlow agent.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the sFlow agent with the IP address as 192.168.0.1:

Switch(config)#sflow address 192.168.0.1

70.2 sflow enable

Description

The **sflow enable** command is used to enable sFlow function. To disable the sFlow function, please use **no sflow enable** command.

Syntax

sflow enable

no sflow enable

Command Mode

Global Configuration Mode

Privilege Requirement

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

User Guidelines

A valid agent address should be assigned to the sFlow agent embedded in the switch before you enable the sFlow function.

Example

Enable sFlow function globally:

```
Switch(config)#sflow enable
```

70.3 sflow collector collector-ID

Description

The **sflow collector collector-ID** command is used to configure the parameters about the sFlow collector.

Syntax

sflow collector collector-ID *value* { [**descript** *descript*] | [**ip** *ip*] | [**port** *port*] | [**maxData** *maxData*] | [**timeout** *timeout*] }

Parameter

value —— The ID of the sFlow collector you desire to configure. The value ranges from 1 to 4.

descript ——Give a Description to the sFlow collector, which contains 16 characters at most.

ip ——The IP address of the sFlow collector. The type of the IP address should be IPv4, for example 192.168.0.100.

port ——The number of the udp port which is selected for the sFlow collector.

maxData ——Specify the maximum number of data bytes that can be sent in a single sample datagram. The value ranges from 300 to 1400 and the default value is 300 bytes.

timeout ——Specify the aging time of the sFlow collector, ranging from 0 to 2000000 seconds. When the timeout is set to 0, it means the life cycle of the collector is infinite.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the ip of the sFlow collector 1 as 192.168.0.100, the port as 3000:

Switch(config)# sflow collector collector-ID 1 **ip** 192.168.0.100

Switch(config)# sflow collector collector-ID 1 **port** 3000

70.4 sflow sampler

Description

The **sflow sampler** command is used to configure the parameters about the sFlow sampler.

Syntax

sflow sampler { [**collector-ID** *value*] | [**ingRate** *ingress-rate*] [**egRate** *egress-rate*] | [**maxHeader** *maxHeader*] }

Parameter

value —— The ID of the sFlow collector which the sFlow sampler will send sFlow datagrams to. The value ranges from 0 to 4. When the value is zero, it means no collector is selected.

ingress-rate ——Specify the ingress sampling frequency of the sFlow sampler. When a sample is taken, the value indicates how many packets to skip before the next sample is taken. The value ranges from 1024 to 65535 and the default value is 0 which means no packets will be sampled.

egress-rate ——Specify the egress sampling frequency of the sFlow sampler. When a sample is taken, the value indicates how many packets to skip before

the next sample is taken. The value ranges from 1024 to 65535 and the default value is 0 which means no packets will be sampled.

maxHeader——Specify the maximum number of bytes that should be copied from a sampled packet. The value ranges from 18 to 256 and the default value is 128 bytes.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure Gigabit Ethernet port 1 as the sFlow sampler: specify the Collector-ID as 1, the ingress rate as 1024:

Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#sflow sampler collector-ID 1

For L2/L2+ switches:

Switch(config-if)#sflow sampler ingRate 1024

For L3 switches:

Switch(config)#sflow sampler ingRate 1024

70.5 show sflow global

Description

The **show sflow global** command is used to display the global configuration of sFlow.

Syntax

show sflow global

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of sFlow:

```
Switch#show sflow global
```

70.6 show sflow collector

Description

The **show sflow collector** command is used to display the global configuration of the sFlow collector.

Syntax

show sflow collector

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of the sFlow collector:

```
Switch#show sflow collector
```

70.7 show sflow sampler

Description

The **show sflow sampler** command is used to display the global configuration of the sFlow sampler.

Syntax

show sflow sampler

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of the sFlow sampler:

```
Switch#show sflow sampler
```

Chapter 71 Ethernet OAM Commands (Only for Certain Devices)

Note: Ethernet OAM commands are only available on certain devices.

Ethernet OAM (standing for Operation, Administration, and Maintenance) is Layer 2 protocol that is used for monitoring and troubleshooting Ethernet networks. It can report the network status to network administrators through the OAMPDUs exchanged between two OAM entities. The operation of OAM on an Ethernet interface does not adversely affect data traffic as OAM is a slow protocol with very limited bandwidth potential.

71.1 ethernet-oam

Description

The **ethernet-oam** command is used to enable the Ethernet OAM function for the desired port. To disable the Ethernet OAM function, please use **no ethernet-oam** command.

Syntax

ethernet-oam

no ethernet-oam

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the Ethernet OAM function for Gigabit Ethernet port 1/0/2:

Switch(config)# interface gigabitEthernet 1/0/2

Switch(config-if)#ethernet-oam

71.2 ethernet-oam mode

Description

The **ethernet-oam mode** command is used to configure the OAM mode for the desired port. To return to the default configurations, please use **no ethernet-oam mode** command. The default mode is active.

Syntax

ethernet-oam mode { passive | active }

no ethernet-oam mode

Parameter

passive —— Specify the OAM mode as passive.

active ——Specify the OAM mode as active.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure Ethernet OAM client to operate in passive mode for Gigabit Ethernet port 2:

Switch(config)# interface gigabitEthernet 1/0/2

Switch(config-if)#ethernet-oam mode passive

71.3 ethernet-oam link-monitor symbol-period

Description

The **ethernet-oam link-monitor symbol-period** command is used to configure the parameters about one of the link events, error symbol period event. To return to the default configurations, please use **no ethernet-oam link-monitor symbol-period** command.

Syntax

ethernet-oam link-monitor symbol-period { **threshold** *threshold* | **window** *window* | **notify** { disable | enable }}

no ethernet-oam link-monitor symbol-period { threshold | window | notify }

Parameter

threshold —— Configure the error threshold for generating error symbol-period event. The range is from 1 to 4294967295 and the default value is 1.

window —— Configure the error symbol-period event detection interval. The range is from 10 to 600, in terms of 100 ms intervals. The default value is 10.

notify —— Enable/Disable the event notification. By default, it is enabled.

threshold | window | notify —— The parameter that you want to return to the default configuration.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

For error symbol-period event, configure the error threshold as 5 and the event detection interval as 3 seconds on Gigabit Ethernet port 1/0/2:

Switch(config)# interface gigabitEthernet 1/0/2

Switch(config-if)# ethernet-oam link-monitor symbol-period threshold 5 **window** 30

71.4 ethernet-oam link-monitor frame

Description

The **ethernet-oam link-monitor frame** command is used to configure the parameters about one of the link events, error frame event. To return to the

default configurations, please use **no ethernet-oam link-monitor frame** command.

Syntax

ethernet-oam link-monitor frame { [**threshold** *threshold*] [**window** *window*] [**notify** { disable | enable }] }

no ethernet-oam link-monitor frame { threshold | window | notify }

Parameter

threshold —— Configure the error threshold for generating error frame event. The range is from 1 to 4294967295 and the default value is 1.

window —— Configure the error symbol-period event detection interval. The range is from 10 to 600, in terms of 100 ms intervals. The default value is 10.

notify —— Enable/Disable the event notification. By default, it is enabled.

threshold | window | notify —— The parameter that you want to return to the default configuration.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

For error frame event, configure the error threshold as 6 and the event detection interval as 9 seconds on Gigabit Ethernet port 1/0/3:

Switch(config)# interface gigabitEthernet 1/0/3

Switch(config-if)# ethernet-oam link-monitor frame threshold 6 **window** 90

71.5 ethernet-oam link-monitor frame-period

Description

The **ethernet-oam link-monitor frame-period** command is used to configure the parameters about one of the link events, error frame period

event. To return to the default configurations, please use **no ethernet-oam link-monitor frame-period** command.

Syntax

ethernet-oam link-monitor frame-period { [**threshold** *threshold*] [**window** *window*] [**notify** { disable | enable }] }

no ethernet-oam link-monitor frame-period { threshold | window | notify }

Parameter

threshold —— Configure the error threshold for generating error frame period event. The range is from 1 to 4294967295 and the default value is 1.

window —— Configure the error frame period event detection interval. The range is from 148810 to 89286000. The default value is 148810 for Fast Ethernet port and 1488100 for Gigabit Ethernet port.

notify —— Enable/Disable the event notification. By default, it is enabled.

threshold | window | notify —— The parameter that you want to return to the default configuration.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

For error frame period event, configure the error threshold as 6 and the event detection interval as 150000 frames on Gigabit Ethernet port 1/0/4:

Switch(config)# interface gigabitEthernet 1/0/4

Switch(config-if)# ethernet-oam link-monitor frame-period threshold 6 **window** 150000

71.6 ethernet-oam link-monitor frame-seconds

Description

The **ethernet-oam link-monitor frame-seconds** command is used to configure the parameters about one of the link events, error frame seconds event. To return to the default configurations, please use **no ethernet-oam link-monitor frame-seconds** command.

Syntax

ethernet-oam link-monitor frame-seconds { [**threshold** *threshold*] [**window** *window*] [**notify** { disable | enable }] }

no ethernet-oam link-monitor frame-seconds { threshold | window | notify }

Parameter

threshold —— Configure the error threshold for generating error frame seconds event. The range is from 1 to 900 and the default value is 1.

window —— Configure the error frame seconds event detection interval. The range is from 100 to 9000, in terms of 100 ms intervals. The default value is 600.

notify —— Enable/Disable the event notification. By default, it is enabled.

threshold | window | notify —— The parameter that you want to return to the default configuration.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

For error frame seconds event, configure the error threshold as 8 and the event detection interval as 30 seconds on Gigabit Ethernet port 5:

Switch(config)# interface gigabitEthernet 1/0/5

Switch(config-if)# ethernet-oam link-monitor frame-seconds threshold 8 **window** 300

71.7 ethernet-oam remote-failure

Description

The ethernet-oam remote-failure command is used to configure whether to notify the link faults or not. The link faults include dying gasp and critical event. To return to the default configurations, please use **no ethernet-oam remote-failure** command.

Syntax

ethernet-oam remote-failure { dying-gasp | critical-event } **notify** { disable | enable }

no ethernet-oam remote-failure { dying-gasp | critical-event } **notify**

Parameter

dying-gasp —— Dying Gasp link event. Dying gasp means an unrecoverable fault, such as power failure, occurs.

critical-event —— Critical Event. Critical-event means unspecified critical event occurs.

notify ——Enable/Disable the event notification. By default, it is enabled.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Disable the Dying Gasp link event notification on Gigabit Ethernet port 1/0/7:

Switch(config)# interface gigabitEthernet 1/0/7

Switch(config-if)# ethernet-oam remote-failure dying-gasp **notify** disable

71.8 ethernet-oam remote-loopback received-remote- loopback

Description

The **ethernet-oam remote-loopback received-remote-loopback** command is used to configure the client to process or to ignore the received remote loopback request. To return to the default configurations, please use **no ethernet-oam remote-loopback received-remote-loopback** command.

Syntax

ethernet-oam remote-loopback received-remote-loopback { process | ignore }

no ethernet-oam remote-loopback received-remote-loopback

Parameter

process —— Process the received remote loopback request.

ignore —— Ignore the received remote loopback request.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure the client to process the received remote loopback request on Gigabit Ethernet port 1:

Switch(config)# interface gigabitEthernet 1/0/1

Switch(config-if)# ethernet-oam remote-loopback received -remote-loopback process

71.9 ethernet-oam remote-loopback

Description

The **ethernet-oam remote-loopback** command is used to request the remote peer to start or stop the Ethernet OAM remote loopback mode.

Syntax

ethernet-oam remote-loopback { start | stop }

Parameter

start —— Request the remote peer to start the Ethernet OAM remote loopback mode.

stop —— Request the remote peer to stop the Ethernet OAM remote loopback mode.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Request the remote peer to start the Ethernet OAM remote loopback mode on Gigabit Ethernet port 1/0/3:

Switch(config)# interface gigabitEthernet 1/0/3

Switch(config-if)# ethernet-oam remote-loopback start

71.10 clear ethernet-oam statistics

Description

The **clear ethernet-oam statistics** command is used to clear Ethernet OAM statistics.

Syntax

clear ethernet-oam statistics [**interface gigabitEthernet** *port*]

Parameter

port —— The Gigabit Ethernet port number. By default, the Ethernet OAM statistics of all ports are cleared.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Clear Ethernet OAM statistics of Gigabit Ethernet port 1/0/3:

Switch(config)# clear ethernet-oam statistics interface gigabit Ethernet 1/0/3

71.11 clear ethernet-oam event-log

Description

The **clear ethernet-oam event-log** command is used to clear the Ethernet OAM event log.

Syntax

clear ethernet-oam event-log [**interface gigabitEthernet** *port*]

Parameter

port ——The Gigabit Ethernet port number. By default, the Ethernet OAM event logs of all ports are cleared.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Clear Ethernet OAM event log of Gigabit Ethernet port 1/0/3:

Switch(config)# clear ethernet-oam event-log interface gigabitEthernet 1/0/3

71.12 show ethernet-oam configuration

Description

The **show ethernet-oam configuration** command is used to display Ethernet OAM configuration information.

Syntax

show ethernet-oam configuration [**interface gigabitEthernet** *port*]

Parameter

port —— The Gigabit Ethernet port number. By default, the Ethernet OAM configuration information of all ports is displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

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

Example

Display Ethernet OAM configuration information of Gigabit Ethernet port 1/0/2:

Switch(config)# show ethernet-oam configuration interface gigabitEthernet 1/0/2

71.13 show ethernet-oam event-log

Description

The **show ethernet-oam event-log** command is used to display the Ethernet OAM event log.

Syntax

show ethernet-oam event-log [**interface gigabitEthernet** *port*]

Parameter

port —— The Gigabit Ethernet port number. By default, the Ethernet OAM event logs of all ports are displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

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

Example

Display Ethernet OAM event log of Gigabit Ethernet port 1/0/2:

Switch(config)# show ethernet-oam event-log interface gigabitEthernet 1/0/2

71.14 show ethernet-oam statistics

Description

The **show ethernet-oam statistics** command is used to display the Ethernet OAM statistics.

Syntax

show ethernet-oam statistics [**interface gigabitEthernet** *port*]

Parameter

port —— The Gigabit Ethernet port number. By default, the Ethernet OAM statistics of all ports are displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

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

Example

Display Ethernet OAM statistics of Gigabit Ethernet port 1/0/2:

Switch(config)# show ethernet-oam statistics interface gigabitEthernet 1/0/2

71.15 show ethernet-oam status

Description

The **show ethernet-oam status** command is used to display the Ethernet OAM status of both the local and the remote client.

Syntax

show ethernet-oam status [**interface gigabitEthernet** *port*]

Parameter

port —— The Gigabit Ethernet port number. By default, the Ethernet OAM status of all ports is displayed.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

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

Example

Display Ethernet OAM status of Gigabit Ethernet port 1/0/2:

Switch(config)# show ethernet-oam status interface gigabitEthernet 1/0/2

Chapter 72 DLDP Commands (Only for Certain Devices)

DLDP (Device Link Detection Protocol) is used to monitor the link state of fiber-optic or twisted-pair Ethernet cables. When a unidirectional link is detected, the corresponding port will be shut down automatically or manually (depending on the shut mode configured).

72.1 dldp (global)

Description

The **dldp** command is used to enable the DLDP function globally. To disable it, please use **no dldp** command.

Syntax

dldp

no dldp

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the DLDP function globally:

```
Switch(config)# dldp
```

72.2 dldp interval

Description

The **dldp interval** command is used to define the interval of sending advertisement packets on ports that are in the advertisement state.

Syntax

dldp interval *interval-time*

Parameter

interval-time —— The interval of sending advertisement packets. It ranges from 1 to 30 seconds. By default, it is 5 seconds.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the interval of sending advertisement packets as 10 seconds:

Switch(config)# dldp interval 10

72.3 dldp shut-mode

Description

The **dldp shut-mode** command is used to configure the shutdown mode when a unidirectional link is detected.

Syntax

dldp shut-mode { auto /manual }

Parameter

auto —— The switch automatically shuts down ports when a unidirectional link is detected. By default, the shut-mode is auto.

manual ——The switch displays an alert when a unidirectional link is detected. The operation to shut down the unidirectional link ports is accomplished by the users.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Configure the shut-mode as manual:

Switch(config)# dldp shut-mode manual

72.4 dldp reset (global)

Note: This command is only available on certain devices

Description

The **dldp reset** command is used to reset all the unidirectional links and restart the link detect process.

Syntax

dldp reset

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Reset the DLDP function globally:

Switch(config)# dldp reset

72.5 dldp(interface)

Description

The **dldp** command is used to enable the DLDP function of the specified port. To disable it, please use **no dldp** command.

Syntax

dldp

no dldp

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the DLDP function of ports 1/0/2-4:

Switch (config)# interface range gigabitEthernet 1/0/2-4

Switch (config-if-range)# dldp

72.6 dldp reset (interface)

Note: This command is only available on certain devices

Description

The **dldp reset** command is used to reset the specified port and restart the link detect process.

Syntax

dldp reset

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Reset the DLDP function of ports 2-4:

Switch (config)# interface range gigabitEthernet 1/0/2-4

Switch (config-if-range)# dldp reset

72.7 show dldp

Description

The **show dldp** command is used to display the global configuration of DLDP function such as DLDP global state, DLDP interval and shut mode.

Syntax

show dldp

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the global configuration of DLDP function:

```
Switch# show dldp
```

72.8 show dldp interface

Description

The **show dldp interface** command is used to display the configuration and state of all ports. By default, the configuration and state of all the ports will be displayed.

Syntax

show dldp interface

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration and state of all ports:

```
Switch# show dldp interface
```

Chapter 73 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.

73.1 snmp-server

Description

The **snmp-server** command is used to enable the SNMP function. By default, it is disabled (For L3 switches, it is enabled by default). 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:

```
Switch(config)# snmp-server
```

73.2 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:

Switch(config)# snmp-server view view1 1.3.6.1.6.3.20 include

73.3 snmp-server group

Description

The **snmp-server group** command is used to manage and configure the SNMP group. To delete the corresponding SNMP group, please use **no snmp-server group** command. SNMP v3 provides the VACM (View-based Access Control Model) and USM (User-Based Security Model) mechanisms for authentication. The users in the SNMP Group can manage the device via the Read View, Write View and Notify View. And the authentication mode and the privacy mode guarantee the high security for the communication between the management station and the managed device.

Syntax

snmp-server group *name* [**smode** v3] [**slev** { noAuthNoPriv | authNoPriv | authPriv }] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*]

no snmp-server group *name* **smode** v3 **slev** { noAuthNoPriv | authNoPriv | authPriv }

Parameter

name ——The SNMP Group name, ranging from 1 to 16 characters. The Group Name, Security Model and Security Level compose the identifier of the

SNMP Group. These three items of the Users in one group should be the same.

v3 —— The security mode for the group, v3 indicates SNMPv3, the most secure level.

slev —— The Security Level of SNMP v3 Group. There are three options, including noAuthNoPriv (No authentication algorithm but a user name match is applied to check packets, and no privacy algorithm is applied to encrypt them), authNoPriv (An authentication algorithm is applied to check packets, but no privacy algorithm is applied to encrypt them) and authPriv (An authentication algorithm and a privacy algorithm are applied to check and encrypt packets). 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:

Switch(config)# snmp-server group group1 **smode** v3 **slev** authNoPriv **read** viewDefault **write** viewDefault **notify** viewDefault

Delete group 1:

Switch(config)# no snmp-server group group1 **smode** v3 **slev** authNoPriv

73.4 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

For L2/L2+ switches:

snmp-server user *name* **{** local | remote **}** *group-name* **[smode** v3 **] [slev** noAuthNoPriv **] [cmode** none **] [cpwd** *confirm-pwd* **] [emode** none **] [epwd** *encrypt-pwd* **]**

snmp-server user *name* **{** local | remote **}** *group-name* **[smode** v3 **] slev** authNoPriv **cmode {** MD5 | SHA **} cpwd** *confirm-pwd* **[emode** none**] [epwd** *encrypt-pwd* **]**

snmp-server user *name* **{** local | remote **}** *group-name* **[smode** v3 **] slev** authPriv **cmode {** MD5 | SHA **} cpwd** *confirm-pwd* **emode** DES **epwd** *encrypt-pwd*

no snmp-server user *name*

For L3 switches:

snmp-server user *name* **{** local | remote **}** *group-name* **[smode** v3 **] [slev** noAuthNoPriv **]**

snmp-server user *name* **{** local | remote **}** *group-name* **[smode** v3 **] slev** authNoPriv **cmode {** MD5 | SHA **} cpwd** *confirm-pwd*

snmp-server user *name* **{** local | remote **}** *group-name* **[smode** v3 **] slev** authPriv **cmode {** MD5 | SHA **} cpwd** *confirm-pwd* **emode** DES **epwd** *encrypt-pwd*

no snmp-server user *name*

Parameter

name —— User Name, ranging from 1 to 16 characters.

local | remote —— User Type, with local and remote options. Local indicates that the user is connected to a local SNMP engine, while remote means that the user is connected to a remote SNMP engine. As the remote engine ID and user password are used to compute the authentication and privacy digests, before configuring a remote user, you need to set the remote engine ID first.

group-name —— The Group Name of the User. The User is classified to the corresponding Group according to its Group Name, Security Model and Security Level.

v3 ——The security mode for the user. v3 indicates SNMPv3, the most secure model.

slev —— The Security Level of SNMP v3 User. There are three options, including noAuthNoPriv (No authentication algorithm but a user name match is applied to check packets, and no privacy algorithm is applied to encrypt them), authNoPriv (An authentication algorithm is applied to check packets, but no privacy algorithm is applied to encrypt them) and authPriv (An authentication algorithm and a privacy algorithm are applied to check and encrypt packets). The security level from lowest to highest is: noAuthNoPriv, authNoPriv, authPriv, and the default is noAuthNoPriv. The security level of the user should not be lower than the group it belongs to.

cmode —— The Authentication Mode of the SNMP v3 User, with none, MD5 and SHA options. None indicates no authentication method is used, MD5 indicates the port authentication is performed via HMAC-MD5 algorithm and SHA indicates the port authentication is performed via SHA (Secure Hash Algorithm). SHA authentication mode has a higher security than MD5 mode. By default, the Authentication Mode is “none”.

confirm-pwd —— Authentication Password, ranging from 1 to 16 characters. The question marks and spaces are not allowed. This password in the configuration file will be displayed in the symmetric encrypted form.

emode —— The Privacy Mode of the SNMP v3 User, with none and DES options. None indicates no privacy method is used, and DES indicates DES encryption method is used. By default, the Privacy Mode is “none”.

encrypt-pwd —— Privacy Password, ranging from 1 to 16 characters. The question marks and spaces are not allowed. This password in the configuration file will be displayed in the symmetric encrypted form.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Add Local User admin to Group group2, and configure the Security Model of the user as v3, the Security Level of the group as authPriv, the Authentication

Mode of the user as MD5, the Authentication Password as 11111, the Privacy Mode as DES, and the Privacy Password as 22222:

Switch(config)# snmp-server user admin local group2 **smode** v3 **slev** authPriv **cmode** MD5 **cpwd** 11111 **emode** DES **epwd** 22222

73.5 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:

Switch(config)# snmp-server community public read-write viewDefault

73.6 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 User. There are three options, including noAuthNoPriv (No authentication algorithm but a user name match is applied to check packets, and no privacy algorithm is applied to encrypt them), authNoPriv (An authentication algorithm is applied to check packets, but no privacy algorithm is applied to encrypt them) and authPriv (An authentication algorithm and a privacy algorithm are applied to check and encrypt packets). By default, the Security Level 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:

For L2/L2+ switches:

Switch(config)#snmp-server host 192.168.0.146 162 admin **smode** v2c **type** inform **retries** 100 **timeout** 1000

For L3 switches:

Switch(config)#snmp-server host 192.168.0.146 162 admin **smode** v2c **slev** noAuthNoPriv **type** inform retries 100 **timeout** 1000

Switch(config)#snmp-server host fe80::1234 162 admin **smode** v2c **slev** noAuthNoPriv **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:

Switch(config)# snmp-server host fe80::1234 162 admin **smode** v2c **type** inform **retries** 100 **timeout** 1000

73.7 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:

Switch(config)# snmp-server engineID local 1234567890

Switch(config)# snmp-server engineID remote abcdef123456

73.8 snmp-server traps snmp

Description

The **snmp-server traps snmp** command is used to enable SNMP standard traps which include four types: linkup, linkdown, warmstart and coldstart. The command without parameter enables all SNMP standard traps. All SNMP standard traps are enabled by default. To disable the sending of SNMP standard traps, please use **no snmp-server traps snmp** command.

Syntax

snmp-server traps snmp [linkup | linkdown | warmstart | coldstart | auth-failure]

no snmp-server traps snmp [linkup | linkdown | warmstart | coldstart | auth-failure]

Parameter

linkup —— Indicates a port status changes from linkdown to linkup, and can be triggered when you connect a device to a port.

linkdown —— Indicates a port status changes from linkup to linkdown, and can be triggered when you disconnect a device to a port.

warmstart —— Indicates the SNMP feature on the switch is reinitialized with the physical configuration unchanged. The trap can be triggered if you disable and then enable SNMP after the SNMP is completely configured and enabled.

coldstart —— Indicates an SNMP initialization caused by the reinitialization of the switch system. The trap can be triggered when you reboot the switch.

auth-failure —— Triggered when a received SNMP request fails the authentication.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable SNMP standard linkup trap for the switch:

Switch(config)# snmp-server traps snmp linkup

73.9 snmp-server traps

Description

The **snmp-server traps** command is used to enable SNMP extended traps. To disable the sending of SNMP extended traps, please use **no snmp-server traps** command. All SNMP extended traps are disabled by default.

Syntax

snmp-server traps { rate-limit | cpu | flash | lldp remtableschange | lldp topologychange | loopback-detection | storm-control | spanning-tree | memory }

no snmp-server traps { rate-limit | cpu | flash | lldp remtableschange | lldp topologychange | loopback-detection | storm-control | spanning-tree | memory }

Parameter

rate-limit ——Monitors whether the bandwidth has reached the limit you have set. The trap can be triggered when the Rate Limit feature is enabled and packets are sent to the port with a rate higher than what you have set.

cpu ——Monitors the load status of the switch CPU. The trap can be triggered when the utilization rate of the CPU has exceeded the limit that you have set. The limit of CPU utilization rate for the switch is 80% by default.

flash ——Triggered when flash is modified during operations such as backup, reset, firmware upgrade, configuration import, and so on.

lldp remtableschange ——An lldp RemTablesChange notification is sent when the value of lldp StatsRemTableLastChangeTime changes. It can be utilized by an NMS host to trigger LLDP remote systems table maintenance polls.

lldp topologychange ——A notification generated by the local device to sense the change in the topology that indicates a new remote device attached to a local port, or a remote device disconnected or moved from one port to another.

loopback-detection ——The feature is used to detect loopbacks. And the trap is disabled by default. The system will generate the trap when a loopback is detected or cleared.

storm-control ——The feature is used to monitor network storms. And the trap is disabled by default. The system will generate the trap when the rate of broadcast or multicast reaches the limit of storm control.

spanning-tree ——The feature is used to monitor the spanning tree status. And the trap is disabled by default. The system will generate the trap in the following situations: a port changes from non-forwarding state to forwarding state or the other way round; a port receives a packet with TC flag or a TCN packet.

memory ——The feature is used to monitor the memory. And the trap is disabled by default. The system will generate the trap when the memory utilization exceeds 80%.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable SNMP extended rate-limit trap for the switch:

Switch(config)# snmp-server traps rate-limit

73.10 snmp-server traps ddm

Note: This command is only available on certain devices.

Description

The **snmp-server traps ddm** command is used to enable the corresponding DDM traps. DDM function is used to monitor the status of the SFP modules inserted into the SFP ports on the switch. The command without parameter enables all SNMP DDM traps. To disable the sending of SNMP DDM traps, use **no snmp-server traps ddm** command. All DDM traps are disabled by default.

Syntax

snmp-server traps ddm [temperature | voltage | bias_current | tx_power | rx_power]

no snmp-server traps ddm [temperature | voltage | bias_current | tx_power | rx_power]

Parameter

temperature ——Monitors the temperature of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the temperature of any SFP module has reached the warning or alarm threshold.

voltage ——Monitors the voltage of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the voltage of any SFP module has reached the warning or alarm threshold.

bias_current ——Monitors the bias current of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the bias current of any SFP module has reached the warning or alarm threshold.

tx_power ——Monitors the TX Power of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the TX Power of any SFP module has reached the warning or alarm threshold.

rx_power ——Monitors the RX Power of SFP modules inserted into the SFP ports on the switch. The trap can be triggered when the RX Power of any SFP module has reached the warning or alarm threshold.

User guidelines

The **snmp-server traps ddm** command without any parameter is used to enable all the types of DDM traps. And the **no snmp-server traps ddm** command without any parameter is used to disable all the types of DDM traps.

For more instructions about the alarm threshold or warning threshold, refer to Chapter 11 DDM Commands.

Command Mode

Global Configuration Mode

Example

Enable all the SNMP DDM traps for the switch:

```
Switch(config)# snmp-server traps ddm
```

73.11 snmp-server traps vlan

Description

The **snmp-server traps vlan** command is used to enable the corresponding VLAN traps. The command without parameter enables all SNMP VLAN traps. To disable this function, please use **no snmp-server traps vlan** command. All VLAN traps are disabled by default.

Syntax

snmp-server traps vlan [create | delete]

no snmp-server traps vlan [create | delete]

Parameter

create ——Triggered when certain VLANs are created successfully.

delete ——Triggered when certain VLANs are deleted successfully.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable all SNMP extended VLAN-related traps for the switch:

```
Switch(config)# snmp-server traps vlan
```

Enable VLAN-created trap only for the switch:

Switch(config)# snmp-server traps vlan create

73.12 snmp-server traps security

Description

The **snmp-server traps security** command is used to enable the corresponding security traps. To disable this feature, please use **no snmp-server traps security** command. All security traps are disabled by default.

Syntax

snmp-server traps security { dhcp-filter | ip-mac-binding **}**

no snmp-server traps security { dhcp-filter | ip-mac-binding **}**

Parameter

dhcp-filter —— Triggered when the DHCPv4 Filter feature is enabled and the switch receives DHCP packets from an illegal DHCP server.

ip-mac-binding —— Triggered when the ARP Inspection feature is enabled and the switch receives an illegal ARP packet, or the IPv4 Source Guard feature is enabled and the switch receives an illegal IP packet.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the DHCP filter trap for the switch:

Switch(config)# snmp-server traps security dhcp-filter

73.13 snmp-server traps security dhcp6-filter

Description

The **snmp-server traps security dhcp6-filter** command is used to enable the IPv6 DHCP Filter illegal message snmp trap and log function. To disable this function, please use **no snmp-server traps security dhcp6-filter** command. All security traps are disabled by default.

Syntax

snmp-server traps security dhcp6-filter

no snmp-server traps security dhcp6-filter

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the IPv6 DHCP Filter illegal message snmp trap and log function:

```
Switch(config)# snmp-server traps security dhcp6-filter
```

73.14 snmp-server traps acl

Description

The **snmp-server traps acl** command is used to enable the ACL trap. To disable this feature, please use **no snmp-server traps acl** command. It is disabled by default.

The trap monitors matched ACL information, including the matched ACL ID, rule ID and the number of the matched packets. With both this trap and the Logging feature in ACL rule settings enabled, the switch will check the matched ACL information every five minutes and send SNMP traps if there is any updated information.

Syntax

snmp-server traps acl

no snmp-server traps acl

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the ACL trap for the switch:

```
Switch(config)# snmp-server traps acl
```

73.15 snmp-server traps ip

Description

The **snmp-server traps ip** command is used to enable IP traps. To disable this feature, please use **no snmp-server traps ip** command. All IP traps are

disabled by default.

Syntax

snmp-server traps ip { change | duplicate **}**

no snmp-server traps ip { change | duplicate **}**

Parameter

change —— Enable SNMP IP change traps. The trap monitors the IP changed of each interface. The trap can be triggered when the IP address of any interface is changed.

duplicate —— Enable SNMP IP duplicate traps. The trap can be triggered when the switch detects an IP conflict event.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable the IP-Change trap for the switch:

Switch(config)# snmp-server traps ip change

73.16 snmp-server traps power

(Only for Certain Devices)

Note: This command is only available on certain devices

Description

The **snmp-server traps power** command is used to enable PoE traps. The command without parameter enables all PoE traps. To disable this feature, please use **no snmp-server traps power** command. All PoE traps are disabled by default.

Syntax

snmp-server traps power [over-max-pwr-budget | port-pwr-change | port-pwr-deny | port-pwr-over-30w | port-pwr-overload | port-short-circuit | thermal-shutdown **]**

no snmp-server traps power [over-max-pwr-budget | port-pwr-change | port-pwr-deny | port-pwr-over-30w | port-pwr-overload | port-short-circuit | thermal-shutdown **]**

Parameter

over-max-pwr-budget ——Triggered when the total power required by the connected PDs exceeds the maximum power the PoE switch can supply.

port-pwr-change ——Triggered when the total power required by the connected PDs exceeds the maximum power the PoE switch can supply.

port-pwr-deny ——Triggered when the switch powers off PDs on low-priority PoE ports. When the total power required by the connected PDs exceeds the system power limit, the switch will power off PDs on low-priority PoE ports to ensure stable running of the other PDs.

port-pwr-over-30w ——Triggered when the power required by the connected PD exceeds 30 watts.

port-pwr-overload ——Triggered when the power required by the connected PD exceeds the maximum power the port can supply.

port-short-circuit ——Triggered when a short circuit is detected on a port.

thermal-shutdown ——Triggered when the PSE chip overheats. The switch will stop supplying power in this case.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable all PoE traps for the switch:

```
Switch(config)# snmp-server traps power
```

73.17 snmp-server traps link-status

Description

The **snmp-server traps link-status** command is used to enable SNMP link status trap for the specified port. To disable the sending of SNMP link status trap, please use **no snmp-server traps link-status** command. By default, it is enabled.

Syntax

snmp-server traps link-status

no snmp-server traps link-status

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

Only Admin level users have access to these commands.

Example

Enable SNMP link status trap for port 3:

Switch(config)# interface gigabitEthernet 1/0/3

Switch(config-if)# snmp-server traps link-status

73.18 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** *interval*] [**owner** *owner-name*] [**buckets** *number*]

no rmon history *index*

Parameter

index —— The index number of the entry, ranging from 1 to 12, in the format of 1-3,5.

port ——The Ethernet port number.

interval —— The interval to take samplings from the port, ranging from 10 to 3600 in seconds. By default, it is 1800.

owner-name —— The owner of the history sample entry, ranging from 1 to 16 characters. By default, it is “monitor”.

number —— The maximum number of buckets desired for the RMON history group of statistics, ranging from 1 to 130. The default is 50 buckets.

Command Mode

Global Configuration Mode

Privilege Requirement

Only Admin level users have access to these commands.

Example

Configure the sample port as Gi1/0/2 and the sample interval as 100 seconds for the entry 1-3:

Switch(config)# rmon history 1-3 **interface gigabitEthernet** 1/0/2 **interval** 100 **owner** owner1

73.19 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:

Switch(config)# rmon event 1-4 **user** user1 **description** description1 **type** log **owner** owner1

73.20 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:

Switch(config)#rmon alarm 1-3 **stats-index** 2 **owner** owner1 **interval** 100

73.21 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:

Switch(config)#rmon statistics 1-3 **interface gigabitEthernet** 1/0/1 **owner** owner1 **status** valid

73.22 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:

```
Switch# show snmp-server
```

73.23 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:

```
Switch# show snmp-server view
```

73.24 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:

```
Switch# show snmp-server group
```

73.25 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:

```
Switch# show snmp-server user
```

73.26 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:

```
Switch# show snmp-server community
```

73.27 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:

```
Switch# show snmp-server host
```

73.28 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:

```
Switch# show snmp-server engineID
```

73.29 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:

Switch# show rmon history

73.30 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:

Switch# show rmon event 1-4

73.31 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:

Switch# show rmon alarm 1-2

73.32 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:

```
Switch#show rmon statistics 1
```

Chapter 74 PoE Commands (Only for Certain Devices)

Note: PoE commands are only available on certain devices.

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.

74.1 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.

Command Mode

Global Configuration Mode

Privilege Requirement

None.

Example

Configure the max power the PoE switch can supply as 160 W:

Switch(config)# power inline consumption 160

74.2 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, with five options: "power-limit", "auto", "class1", "class2", "class3" and "class4". "Power-limit" indicates you can manually enter a value ranging 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

None.

Example

Create a PoE profile named "IP Camera" whose PoE status is "enable", PoE priority is "low" and the power limit is "5w":

Switch(config)# power profile "IP Camera" **supply** enable **priority** low **consumption** 50

74.3 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

power-limit —— The max power the port in the profile can supply, with five options: "power-limit", "auto", "class1", "class2", "class3" and "class4". "Power-limit" indicates you can manually enter a value ranging 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 gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

None.

Example

Configure the power limit as "5w" for port 2:

Switch(config)# interface gigabitEthernet 1/0/2

Switch(config-if)# power inline consumption 50

74.4 power inline consumption (unit)

Description

The **power inline unit consumption** command is used to specify the maximum power a stack unit can supply.

Syntax

power inline unit {*unit id*} **consumption** {power-limit}

Parameter

unit id —— Stack unit ID, ranging from 1-4

power-limit —— Specify the maximum power the PoE switch can supply, which depends on actual power usage.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Specify the maximum power unit 1 can supply to 402W:

```
Switch(config)#power inline unit 1 consumption 402
```

74.5 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 gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

None.

Example

Configure the PoE priority as “low” for port 2:

```
Switch(config)# interface gigabitEthernet 1/0/2
Switch(config-if)# power inline priority low
```

74.6 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 gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

None.

Example

Enable the PoE feature for port 2:

```
Switch(config)# interface gigabitEthernet 1/0/2
Switch(config-if)# power inline supply enable
```

74.7 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 gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

None.

Example

Bind the PoE profile named “IP Camera” to port 2:

Switch(config)# interface gigabitEthernet 1/0/2

Switch(config-if)# power inline profile “IP Camera”

74.8 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

None.

Example

Bind the PoE time-range named “tRange2" to port 2:

Switch(config)# interface gigabitEthernet 1/0/2

Switch(config-if)# power inline time-range tRange2

74.9 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:

```
Switch# show power inline
```

74.10 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 [**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-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:

```
Switch# show power inline configuration interface
```

74.11 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 [**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-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:

```
Switch# show power inline information interface
```

74.12 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:

```
Switch# show power profile
```

74.13 power recovery ststus enable

Description

The **power recovery ststus enable** command is used to enable the power auto recovery function globally. To disable this function, please use **power recovery ststus disable** command

Syntax

power recovery ststus enable

power recovery ststus disable

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the power auto recovery function globally:

```
Switch(config)# power recovery ststus enable
```

74.14 power recovery status

Description

The **power recovery ststus** command is used to configure the power recovery status and parameters of a specified port..

Syntax

power recovery ststus {disable|enable} ip *ipv4_addr* **startup** *startup delay* **interval** *ping interval* **retry** *failure threshold* **break** *break time*

Parameter

ipv4_addr —— Ipv4 address, in string format, for example, 192.168.0.1.

startup delay —— Feature startup delay(S), ranging from 30 to 600.

ping interval —— Ping package interval(S), ranging from 10 to 120.

failure threshold —— Number of ping failures, ranging from 1 to 10.

break time —— Break time after detecting abnormal POE status(S), ranging from 3 to 120.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Enable the power recovery status of port 2 and configure relevant parameters:

Switch(config)# interface gigabitEthernet 1/0/2

Switch(config-if)# power recovery status enable ip 192.168.0.1 **startup** 60 **interval** 60 **retry** 5 **break** 60

74.15 show power recovery

Description

The **show power recovery** command is used to display all POE auto recovery configurations.

Syntax

show power recovery

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 all POE auto recovery configurations:

Switch(config)#show power recovery

74.16 show power recovery interface

Description

The **show power recovery interface** command is used to display power auto recovery configurations of the selected port.

Syntax

show power recovery ***interface*** [**fastEthernet | gigabitEthernet | two-gigabitEthernet | ten-gigabitEthernet**] *port list*

Parameter

interface —— Port type.

port list—— Port number list.

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 power auto recovery configurations of:

```
Switch(config)#show power recovery
```

Chapter 75 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.

75.1 ip arp inspection

Description

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

Syntax

ip arp inspection

no ip arp inspection

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the ARP Detection function globally:

```
Switch(config)#ip arp inspection
```

75.2 ip arp inspection validate

Description

The **ip arp inspection validate** command is used to enable the switch to check whether the reveided ARP packet is illegal. To disable,the feature please use **no ip arp detection validate** command.

Syntax

ip arp inspection validate { src-mac | dst-mac | ip **}**

no ip arp inspection validate { src-mac | dst-mac | ip **}**

Syntax

src-mac —— Enable the switch to check whether the source MAC address and the sender MAC address are the same when receiving an ARP packet. If not, the ARP packet will be discarded.

dst-mac —— Enable the switch to check whether the sender IP address of all ARP packets and the target IP address of ARP reply packets are legal. The illegal packets will be discarded.

ip —— Enable or disable the switch to check whether the sender IP address of all ARP packets and the target IP address of ARP reply packets are legal. The illegal packets will be discarded.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the switch to check whether the source MAC address and the sender MAC address are the same when receiving an ARP packet

Switch(config)#ip arp inspection validate src-mac

75.3 ip arp inspection vlan

Description

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

Syntax

ip arp inspection vlan *vlan-list*

no ip arp inspection vlan *vlan-list*

Syntax

vlan-list —— Enter the VLAN ID. The format is 1,5-9.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the ARP Detection function on VLAN 2:

Switch(config)#ip arp inspection vlan 2

75.4 ip arp inspection vlan logging

Description

The **ip arp inspection vlan logging** command is used to enable the Log function on the specific VLAN. To disable the Log function on the VLAN, please use **no ip arp detection vlan logging** command.

Syntax

ip arp inspection vlan *vlan-list* **logging**

no ip arp inspection vlan *vlan-list* **logging**

Syntax

vlan-list —— Enter the VLAN ID. The format is 1,5-9.

logging —— Enable the Log feature to make the switch generate a log when an ARP packet is discarded.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable the log feature on VLAN 2:

Switch(config)#ip arp inspection vlan 2 **logging**

75.5 ip arp inspection trust

Description

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

Syntax

ip arp inspection trust

no ip arp inspection trust

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

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

Switch(config)#interface range gigabitEthernet 1/0/2-5

Switch(config-if-range)#ip arp inspection trust

75.6 ip arp inspection limit-rate

Description

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

Syntax

ip arp inspection limit-rate *value*

no ip arp inspection limit-rate

Parameter

value ——The value to specify the maximum amount of the received ARP packets per second, ranging from 1 to 300 in pps(packet/second). By default, the value is 100.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

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

Switch(config)#interface gigabitEthernet 1/0/5

Switch(config-if)#ip arp inspection limit-rate 50

75.7 ip arp inspection burst-interval

Description

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

Syntax

ip arp inspection burst-interval *value*

no ip arp inspection burst-interval

Parameter

value —— Specify a time range. If the speed of received ARP packets in this time range reaches the limit for this time range, the port will be shut down. The valid values are from 1 to 15 seconds, and the default value is 1 second.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure the burst interval as 2 seconds for Gigabit Ethernet port 5:

Switch(config)#interface gigabitEthernet 1/0/5

Switch(config-if)#ip arp inspection burst-interval 2

75.8 ip arp inspection recover

Description

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

Syntax

ip arp inspection recover

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

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

Switch(config)#interface gigabitEthernet 1/0/5

Switch(config-if)#ip arp inspection recover

75.9 ip arp inspection exceed

Description

The **ip arp inspection exceed** command is used to configure the overspeed action. To delete this action, please use **no ip arp inspection exceed** command.

Syntax

ip arp inspection exceed [**drop | shutdown**] *recover-time*

no ip arp inspection exceed

Parameter

drop —— Drop messages when speeding.

shutdown —— Shut ports down when speeding.

recover-time —— Configure self-recovery time.

Command Mode

Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet)

Privilege Requirement

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

Example

Configure the overspeed action as dropping messages when speeding and self-recovery time as 2 seconds for Gigabit Ethernet port 5:

Switch(config)#interface gigabitEthernet 1/0/5

Switch(config-if)#ip arp inspection exceed drop 2

75.10 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:

Switch(config)#show ip arp inspection

75.11 show ip arp inspection interface

Description

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

Syntax

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

Parameter

port——The Ethernet port number.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

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

Switch(config)#show ip arp inspection interface gigabitEthernet 1/0/1

Display the configuration of all Ethernet ports:

Switch(config)#show ip arp inspection interface

75.12 show ip arp inspection vlan

Description

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

Syntax

show ip arp inspection vlan

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the ARP Inspection configuration of VLAN:

```
Switch(config)#show ip arp inspection vlan
```

75.13 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:

```
Switch(config)#show ip arp inspection statistics
```

75.14 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:

```
Switch(config)#clear ip arp inspection statistics
```

Chapter 76 ND Detection Commands

The ND Detection feature allows the switch to detect the ND packets based on the binding entries in the IPv6-MAC Binding Table and filter out the illegal ND packets. Before configuring ND Detection, complete IPv6-MAC Binding configuration. For details, refer to IPv6-MAC Binding Configurations.

76.1 ipv6 nd detection

Description

The **ipv6 nd detection** command is used to enable the ND Detection function globally. To disable the ND Detection function, please use **no ipv6 nd detection** command.

Syntax

ipv6 nd detection

no ipv6 nd detection

Command Mode

Global Configuration Mode

Example

Enable the ND Detection function globally:

```
Switch(config)#ipv6 nd detection
```

76.2 ipv6 nd detection vlan

Description

The **ipv6 nd detection vlan** command is used to enable ND Detection function on a specified VLAN. To disable ND Detection function on this VLAN, please use **no ipv6 nd detection vlan** command.

Syntax

ipv6 nd detection vlan *vlan-range*

no ipv6 nd detection vlan *vlan-range*

Parameter

vlan-range——Enter the vlan range in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Example

Enable the ND Detection function on VLAN 1,4,6-7:

Switch(config)#ipv6 nd detection vlan 1,4,6-7

76.3 ipv6 nd detection vlan logging

Description

The **ipv6 nd detection vlan logging** command is used to enable Log function on a specified VLAN. To disable Log function on this VLAN, please use **no ipv6 nd detection vlan logging** command.

Syntax

ipv6 nd detection vlan *vlan-range* **logging**

no ipv6 nd detection vlan *vlan-range* **logging**

Parameter

vlan-range——Enter the vlan range in the format of 1-3, 5.

Command Mode

Global Configuration Mode

Example

Enable the Log function on VLAN 1,4,6-7:

Switch(config)#ipv6 nd detection vlan 1,4,6-7 **logging**

76.4 ipv6 nd detection trust

Description

The **ipv6 nd detection trust** command is used to configure the port for which the ND Detection function is unnecessary as the Trusted Port. To clear the

Trusted Port list, please use **no ipv6 nd detection trust** command .The specific port, such as up-linked port, routing port and LAG port, should be set as Trusted Port. To ensure the normal communication of the switch, please configure the ND Detection Trusted Port before enabling the ND Detection function.

Syntax

Ipv6 nd detection trust

no ipv6 nd detection trust

Command Mode

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

Example

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

Switch(config)#interface range gigabitEthernet 1/0/2-5

Switch(config-if-range)#ipv6 nd detection trust

76.5 show ipv6 nd detection

Description

The **show ipv6 nd detection** command is used to display the ND detection global configuration including the enable/disable status.

Syntax

show ipv6 nd detection

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the ND Detection configuration globally:

Switch(config)#show ipv6 nd detection

76.6 show ipv6 nd detection interface

Description

The **show ipv6 nd detection interface** command is used to display the interface configuration of ND Detection.

Syntax

show ipv6 nd detection interface[**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parameter

port——The Ethernet port number.

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

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

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

Switch(config)#show ipv6 nd detection interface gigabitEthernet 1/0/1

Display the configuration of all Ethernet ports:

Switch(config)#show ipv6 nd detection interface

76.7 show ipv6 nd detection statistics

Note: This command is only available on certain devices.

Description

The **show ipv6 nd detection statistics** command is used to display the ND statistics of each VLAN, including the number of forwarded and dropped ND packets.

Syntax

show ipv6 nd detection statistics

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the ipv6 ND Detection statistics of each VLAN.

```
Switch(config)#show ipv6 nd detection statistics
```

76.8 show ipv6 nd detection vlan

Description

The **show ipv6 nd detection vlan** command is used to display the VLAN configuration of ND Detection.

Syntax

show ipv6 nd detection vlan

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Example

Display the ipv6 ND Detection configuration of VLAN.

```
Switch(config)#show ipv6 nd detection vlan
```

Chapter 77 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.

77.1 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:

```
Switch(config)#logging buffer
```

77.2 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:

Switch(config)#logging buffer level 5

77.3 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:

```
Switch(config)#logging file flash
```

77.4 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:

```
Switch(config)#logging file flash frequency periodic10
```

77.5 logging file flash level

Description

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

Syntax

logging file flash level *level*

no logging file flash level

Parameter

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

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Save the log messages with their severities equal or higher than 7 to the flash :

Switch(config)#logging file flash level 7

77.6 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:

Switch(config)# logging host index 2 192.168.0.148 5

77.7 logging console

Description

The **logging console** command is used to send the system logs to the console port. To disable logging to the console, please use **no logging console** command. This function is enabled by default.

Syntax

logging console

no logging console

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Enable logging to the console port:

Switch(config)# logging console

77.8 logging console level

Description

The **logging console level** command is used to limit messages logged to the console port. System logs no higher than the set threshold level will be displayed on the console port. To restore the threshold level to default value, please use **no logging console level** command.

Syntax

logging console level *level*

no logging monitor level

Parameter

level —— Severity level of the log information output to the console port. There are 8 severity levels marked with values 0–7. The smaller value has the higher priority. Only the log with the same or smaller severity level value will be output to the terminal devices. By default, it is 5 indicating that all the log information between level 0–5 will be output to the terminal devices.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Output the log information with severity levels between 0–7 to the console port:

Switch(config)# logging console level 7

77.9 logging monitor

Description

The **logging monitor** command is used to display the system logs on the terminal devices. To disable logging to the terminal, please use **no logging monitor** command. This function is enabled by default.

Syntax

logging monitor

no logging monitor

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Disable logging to the terminal devices:

```
Switch(config)# no logging monitor
```

77.10 logging monitor level

Description

The **logging monitor level** command is used to limit messages logged to the terminal devices. System logs no higher than the set threshold level will be displayed on the terminal devices. To restore the threshold level to default value, please use **no logging monitor level** command.

Syntax

logging monitor level *level*

no logging monitor level

Parameter

level—— Severity level of the log information output to the terminal devices. There are 8 severity levels marked with values 0–7. The smaller value has the higher priority. Only the log with the same or smaller severity level value will

be output to the terminal devices. By default, it is 5 indicating that all the log information between level 0–5 will be output to the terminal devices.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Output the log information with severity levels between 0–7 to the terminal devices:

Switch(config)# logging monitor level 7

77.11 clear logging

Description

The **clear logging** command is used to clear the information in the log buffer and log file.

Syntax

clear logging [buffer | flash]

Parameter

buffer | flash —The output channels: buffer and flash. Clear the information of the two channels, by default.

Command Mode

Global Configuration Mode

Privilege Requirement

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

Example

Clear the information in the log file:

Switch(config)# clear logging buffer

77.12 show logging local-config

Description

The **show logging local-config** command is used to display the configuration of the Local Log output to the console, the terminal, the log buffer and the log file.

Syntax

show logging local-config

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of the Local Log:

Switch(config)# show logging local-config

77.13 show logging loghost

Description

The **show logging loghost** command is used to display the configuration of the log host.

Syntax

show logging loghost [*index*]

Parameter

index ——The index of the log host whose configuration will be displayed, ranging from 1 to 4. Display the configuration of all the log hosts by default.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the configuration of the log host 2:

Switch(config)# show logging loghost 2

77.14 show logging buffer

Description

The **show logging buffer** command is used to display the log information in the log buffer according to the severity level.

Syntax

show logging buffer [**level** *level*]

Parameter

level —— Severity level. There are 8 severity levels marked with values 0–7. The information of levels with priority not lower than the select level will display. Display all the log information in the log buffer by default.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the log information from level 0 to level 5 in the log buffer:

Switch(config)# show logging buffer level 5

77.15 show logging flash

Description

The **show logging flash** command is used to display the log information in the log file according to the severity level.

Syntax

show logging flash [**level** *level*]

Parameter

level —— Severity level. There are 8 severity levels marked with values 0–7. The information of levels with priority not lower than the select level will display. Display all the log information in the log file by default.

Command Mode

Privileged EXEC Mode and Any Configuration Mode

Privilege Requirement

None.

Example

Display the log information with the level marked 0-3 in the log file:

Switch(config)# show logging flash level 3