User Guide

T2600G Series Switches

T2600G-28TS (TL-SG3424) / T2600G-28MPS (TL-SG3424P)

1910012382 REV2.1.3

March 2018

COPYRIGHT & TRADEMARKS

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

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-Link Technologies Co., Ltd. Copyright © 2018 TP-Link Technologies Co., Ltd. All rights reserved.

https://www.tp-link.com

FCC STATEMENT

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1) This device may not cause harmful interference.
2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

CE Mark Warning

CE

This is a class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Industry Canada Statement

CAN ICES-3 (A)/NMB-3(A)

BSMI Notice

安全諮詢及注意事項

- 請使用原裝電源供應器或只能按照本產品注明的電源類型使用本產品。
- 清潔本產品之前請先拔掉電源線。請勿使用液體、噴霧清潔劑或濕布進行清潔。
- 注意防潮，請勿將水或其他液體潑灑到本產品上。
- 插槽與開口供通風使用，以確保本產品的操作可靠並防止過熱，請勿堵塞或覆蓋開口。
- 請勿將本產品置放於靠近熱源的地方。除非有正常的通風，否則不可放在密閉位置中。
- 請不要私自打開機殼，不要嘗試自行維修本產品，請由授權的專業人士進行此項工作。

此為甲類資訊技術設備，于居住環境中使用時，可能會造成射頻擾動，在此種情況下，使用者會被要求採取某些適當的對策。

限用物質含有情況標示聲明書

產品元件名稱	限用物質及其化學符號					
	鉛 Pb	鎘 Cd	汞 Hg	六價鉻 CrVI	多溴聯苯 PBB	多溴二苯醚 PBDE
PCB	○	○	○	○	○	○
外殼	○	○	○	○	○	○
電源供應板	—	○	○	○	○	○
電源適配器	—	○	○	○	○	○

備考 1. “超出 0.1 wt %”及“超出 0.01 wt %”系指限用物質之百分比含量超出百分比含量基準值。

備考 2. “○”系指該項限用物質之百分比含量未超出百分比含量基準值。

備考 3. “—”系指該項限用物質為排除項目。

Продукт сертифіковано згідно с правилами системи УкрСЕПРО на відповідність вимогам нормативних документів та вимогам, що передбачені чинними законодавчими актами України.

Safety Information

- When product has power button, the power button is one of the way to shut off the product; When there is no power button, the only way to completely shut off power is to disconnect the product or the power adapter from the power source.
- Don't disassemble the product, or make repairs yourself. You run the risk of electric shock and voiding the limited warranty. If you need service, please contact us.
- Avoid water and wet locations.

Please read and follow the above safety information when operating the device. We cannot guarantee that no accidents or damage will occur due to improper use of the device. Please use this product with care and operate at your own risk.

Explanation of the symbols on the product label

Symbol	Explanation
	AC voltage
	Indoor use only
	RECYCLING This product bears the selective sorting symbol for Waste electrical and electronic equipment (WEEE). This means that this product must be handled pursuant to European directive 2012/19/EU in order to be recycled or dismantled to minimize its impact on the environment. User has the choice to give his product to a competent recycling organization or to the retailer when he buys a new electrical or electronic equipment.

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

CONTENTS

About This Guide

Intended Readers 1
Conventions 1
More Information 2

Accessing the Switch

Overview 4
Web Interface Access 5
- Login 5
- Save Config Function 6
- Disable the Web Server 7
- Configure the Switch's IP Address and Default Gateway 8

Command Line Interface Access 11
- Console Login (only for switch with console port) 11
- Telnet Login 13
- SSH Login 14
- Disable Telnet login 18
- Disable SSH login 19
- Copy running-config startup-config 19
- Change the Switch's IP Address and Default Gateway 20

Managing System

System 22
- Overview 22
- Supported Features 22

System Info Configurations 24
- Using the GUI 24
  - Viewing the System Summary 24
  - Specifying the Device Description 26
  - Setting the System Time 26
  - Setting the Daylight Saving Time 28
  - Specifying the Serial Port Parameter 29
- Using the CLI 30
  - Viewing the System Summary 30

Specifying the Device Description....31
Setting the System Time....32
Setting the Daylight Saving Time....34
Specifying the Serial Port Parameter....36
User Management Configurations....38
Using the GUI....38
Creating Admin Accounts....38
Creating Accounts of Other Types....39
Using the CLI....41
Creating Admin Accounts....41
Creating Accounts of Other Types....42
System Tools Configurations....46
Using the GUI....46
Configuring the Boot File....46
Restoring the Configuration of the Switch....47
Backing up the Configuration File....48
Upgrading the Firmware....48
Configuring Auto Install Function....49
Rebooting the switch....50
Configuring the Reboot Schedule....50
Reseting the Switch....51
Using the CLI....51
Configuring the Boot File....51
Restoring the Configuration of the Switch....52
Backing up the Configuration File....53
Upgrading the firmware....53
Configuring Auto Install Function....54
Rebooting the switch....55
Configuring the Reboot Schedule....56
Reseting the Switch....57
Access Security Configurations....58
Using the GUI....58
Configuring the Access Control Feature....58
Configuring the HTTP Function....60
Configuring the HTTPS Function....61
Configuring the SSH Feature....63
Enabling the Telnet Function....64
Using the CLI....64

Configuring the Access Control....64
Configuring the HTTP Function....66
Configuring the HTTPS Function....67
Configuring the SSH Feature....69
Enabling the Telnet Function....72
SDM Template Configuration....73
Using the GUI....73
Using the CLI....74
Appendix: Default Parameters....76

Managing Physical Interfaces

Physical Interface....80
Overview....80
Supported Features....80
Basic Parameters Configurations....81
Using the GUI....81
Using the CLI....82
Port Mirror Configuration....85
Using the GUI....85
Using the CLI....87
Port Security Configuration....89
Using the GUI....89
Using the CLI....90
Port Isolation Configurations....93
Using the GUI....93
Using the CLI....94
Loopback Detection Configuration....96
Using the GUI....96
Using the CLI....98
Configuration Examples....100
Example for Port Mirror....100
Network Requirements....100
Configuration Scheme....100
Using the GUI....100
Using the CLI....102
Example for Port Isolation....102
Network Requirements....102

Configuration Scheme 103
Using the GUI 103
Using the CLI 104
Example for Loopback Detection 105
Network Requirements 105
Configuration Scheme 105
Using the GUI 105
Using the CLI 106
Appendix: Default Parameters 108

Configuring LAG

LAG 111
Overview 111
Supported Features 111
LAG Configuration 112
Using the GUI 113
Configuring Load-balancing Algorithm 113
Configuring Static LAG or LACP 114
Using the CLI 116
Configuring Load-balancing Algorithm 116
Configuring Static LAG or LACP 117
Configuration Example 121
Network Requirements 121
Configuration Scheme 121
Using the GUI 122
Using the CLI 123
Appendix: Default Parameters 125

Monitoring Traffic

Traffic Monitor 127
Using the GUI 127
Viewing the Traffic Summary 127
Viewing the Traffic Statistics in Detail 128
Using the CLI 130
Appendix: Default Parameters 131

Managing MAC Address Table

MAC Address Table 133
Overview 133
Supported Features 133
Address Configurations 135
Using the GUI 135
Adding Static MAC Address Entries 135
Modifying the Aging Time of Dynamic Address Entries 137
Adding MAC Filtering Address Entries 138
Viewing Address Table Entries 138
Using the CLI 139
Adding Static MAC Address Entries 139
Modifying the Aging Time of Dynamic Address Entries 140
Adding MAC Filtering Address Entries 141
Security Configurations 143
Using the GUI 143
Configuring MAC Notification Traps 143
Limiting the Number of MAC Addresses in VLANs 145
Using the CLI 146
Configuring MAC Notification Traps 146
Limiting the Number of MAC Addresses in VLANs 147
Example for Security Configurations 149
Network Requirements 149
Configuration Scheme 149
Using the GUI 150
Using the CLI 151
Appendix: Default Parameters 152

Configuring DDM

Overview 154
DDM Configuration 155
Using the GUI 155
Configuring DDM Globally 155
Configuring the Temperature Threshold 156
Configuring the Voltage Threshold 156
Configuring the Bias Current Threshold 157
Configuring the Tx Power Threshold 158

Configuring the Rx Power Threshold 159
Viewing DDM Status 159
Using the CLI 160
Configuring DDM Globally 160
Configuring DDM Shutdown 161
Configuring Temperature Threshold 162
Configuring Voltage Threshold 163
Configuring Bias Current Threshold 164
Configuring Tx Power Threshold 166
Configuring Rx Power Threshold 167
Viewing DDM Configuration 168
Viewing DDM Status 169
Appendix: Default Parameters 170

Configuring L2PT

Overview 172
L2PT Configuration 174
Using the GUI 174
Using the CLI 175
Configuration Example 178
Network Requirements 178
Configuration Scheme 178
Using the GUI 178
Using the CLI 179
Appendix: Default Parameters 181

Configuring 802.1Q VLAN

Overview 183
802.1Q VLAN Configuration 184
Using the GUI 184
Configuring the PVID of the Port 184
Configuring the VLAN 186
Using the CLI 187
Creating a VLAN 187
Configuring the Port 188
Adding the Port to the Specified VLAN 189
Configuration Example 191

Network Requirements....191
Configuration Scheme....191
Network Topology....192
Using the GUI....192
Using the CLI....195
Appendix: Default Parameters....197

Configuring MAC VLAN

Overview....199
MAC VLAN Configuration....200
Using the GUI....200
Configuring 802.1Q VLAN....200
Binding the MAC Address to the VLAN....201
Enabling MAC VLAN for the Port....201
Using the CLI....202
Configuring 802.1Q VLAN....202
Binding the MAC Address to the VLAN....202
Enabling MAC VLAN for the Port....203
Configuration Example....205
Network Requirements....205
Configuration Scheme....205
Using the GUI....206
Using the CLI....210
Appendix: Default Parameters....213

Configuring Protocol VLAN

Overview....215
Protocol VLAN Configuration....216
Using the GUI....216
Configuring 802.1Q VLAN....216
Creating Protocol Template....217
Configuring Protocol VLAN....218
Using the CLI....218
Configuring 802.1Q VLAN....218
Creating a Protocol Template....219
Configuring Protocol VLAN....220
Configuration Example....222

Network Requirements....222
Configuration Scheme....222
Using the GUI....223
Using the CLI....229
Appendix: Default Parameters....234

Configuring VLAN-VPN

VLAN-VPN....236
Overview....236
Supported Features....237
Basic VLAN-VPN Configuration....238
Using the GUI....238
Configuring 802.1Q VLAN....238
Configuring Global VLAN-VPN and Up-link Ports....239
Configuring VPN Ports....240
Using the CLI....240
Configuring 802.1Q VLAN....240
Configuring Basic VLAN-VPN....241
Flexible VLAN-VPN Configuration....243
Using the GUI....243
Using the CLI....244
Configuration Example....246
Network Requirements....246
Configuration Scheme....246
Using the GUI....247
Using the CLI....251
Appendix: Default Parameters....254

Configuring GVRP

Overview....256
GVRP Configuration....257
Using the GUI....257
Using the CLI....259
Configuration Example....262
Network Requirements....262
Configuration Scheme....262
Using the GUI....263

Using the CLI 266
Appendix: Default Parameters 270

Configuring Private VLAN

Overview 272
Private VLAN Configurations 274
Using the GUI 274
Creating Private VLAN 274
Configuring the Up-link Port 275
Configuring the Down-link Port 276
Using the CLI 277
Creating Private VLAN 277
Configuring the Up-link Port 279
Configuring the Down-link Port 280
Configuration Example 282
Network Requirements 282
Configuration Scheme 282
Network Topology 282
Using the GUI 283
Using the CLI 285
Appendix: Default Parameters 288

Configuring Spanning Tree

Spanning Tree 290
Overview 290
Basic Concepts 290
STP/RSTP Concepts 290
MSTP Concepts 294
STP Security 295
STP/RSTP Configurations 298
Using the GUI 298
Configuring STP/RSTP Parameters on Ports 298
Configuring STP/RSTP Globally 300
Verifying the STP/RSTP Configurations 302
Using the CLI 303
Configuring STP/RSTP Parameters on Ports 303
Configuring Global STP/RSTP Parameters 305

Enabling STP/RSTP Globally....306
MSTP Configurations....308
Using the GUI....308
Configuring Parameters on Ports in CIST....308
Configuring the MSTP Region....310
Configuring MSTP Globally....315
Verifying the MSTP Configurations....317
Using the CLI....318
Configuring Parameters on Ports in CIST....318
Configuring the MSTP Region....320
Configuring Global MSTP Parameters....323
Enabling Spanning Tree Globally....325
STP Security Configurations....328
Using the GUI....328
Using the CLI....329
Configuration Example for MSTP....332
Network Requirements....332
Configuration Scheme....332
Using the GUI....333
Using the CLI....344
Appendix: Default Parameters....351

Configuring OAM

Ethernet OAM....354
Overview....354
Supported Features....355
Ethernet OAM Configurations....358
Using the GUI....358
Enabling OAM and Configuring OAM Mode....358
Configuring Link Monitoring....359
Configuring RFI....361
Configuring Remote Loopback....362
Viewing OAM Status....363
Using the CLI....365
Enabling OAM and Configuring OAM Mode....365
Configuring Link Monitoring....366
Configuring Remote Failure Indication....372

Configuring Remote Loopback....373
Verifying OAM Connection....374
Viewing OAM Statistics....377
Using the GUI....377
Viewing OAMPDUs....377
Viewing Event Logs....379
Using the CLI....380
Viewing OAMPDUs....380
Viewing Event Logs....382
Configuration Example....384
Network Requirements....384
Configuration Scheme....384
Using the GUI....384
Using the CLI....389
Appendix: Default Parameters....394

Configuring Layer 2 Multicast

Layer 2 Multicast....396
Overview....396
Supported Layer 2 Multicast Protocols....397
IGMP Snooping Configurations....398
Using the GUI....398
Configuring IGMP Snooping Globally....398
Enabling IGMP Snooping Globally....398
(Optional) Configuring Unknown Multicast....398
(Optional) Configuring Report Message Suppression....399
Configuring Router Port Time and Member Port Time....399
Configuring IGMP Snooping Last Listener Query....400
Verifying IGMP Snooping Status....400
Configuring the Port's Basic IGMP Snooping Features....401
Enabling IGMP Snooping on the Port....401
(Optional) Configuring Fast Leave....401
Configuring IGMP Snooping in the VLAN....402
Configuring IGMP Snooping Globally in the VLAN....402
(Optional) Configuring the Static Router Ports in the VLAN....403
(Optional) Configuring the Forbidden Router Ports in the VLAN....403
Configuring the Multicast VLAN....403

Creating Multicast VLAN and Configuring Basic Settings....404
(Optional) Creating Replace Source IP....405
Viewing Dynamic Router Ports in the Multicast VLAN....405
(Optional) Configuring the Static Router Ports....405
(Optional) Configuring the Forbidden Router Ports....405
(Optional) Configuring the Querier....406
Configuring the Querier....406
Viewing Settings of IGMP Querier....406
Configuring IGMP Profile....407
Creating Profile....407
Searching Profile....407
Editing IP Range of the Profile....408
Binding Profile and Member Ports....408
Binding Profile and Member Ports....409
Configuring Max Groups a Port Can Join....409
Viewing IGMP Statistics on Each Port....410
Configuring Auto Refresh....410
Viewing IGMP Statistics....411
Enabling IGMP Accounting and Authentication....411
Configuring IGMP Accounting Globally....412
Configuring IGMP Authentication on the Port....412
Configuring Static Member Port....412
Configuring Static Member Port....413
Viewing IGMP Static Multicast Groups....413
Using the CLI....414
Enabling IGMP Snooping Globally....414
Enabling IGMP Snooping on the Port....414
Configuring IGMP Snooping Parameters Globally....415
Configuring Report Message Suppression....415
Configuring Unknown Multicast....416
Configuring IGMP Snooping Parameters on the Port....417
Configuring Router Port Time and Member Port Time....417
Configuring Fast Leave....418
Configuring Max Group and Overflow Action on the Port....419
Configuring IGMP Snooping Last Listener Query....420
Configuring IGMP Snooping Parameters in the VLAN....422
Configuring Router Port Time and Member Port Time....422
Configuring Static Router Port....423

Configuring Forbidden Router Port 424
Configuring Static Multicast (Multicast IP and Forward Port) 425
Configuring IGMP Snooping Parameters in the Multicast VLAN 425
Configuring Router Port Time and Member Port Time 425
Configuring Static Router Port 426
Configuring Forbidden Router Port 427
Configuring Replace Source IP 428
Configuring the Querier 429
Enabling IGMP Querier 429
Configuring Query Interval, Max Response Time and General Query Source IP 430
Configuring Multicast Filtering 431
Creating Profile 431
Binding Profile to the Port 432
Enabling IGMP Accounting and Authentication 434
Enabling IGMP Authentication on the Port 434
Enabling IGMP Accounting Globally 435
Configuring MLD Snooping 436
Using the GUI 436
Configuring MLD Snooping Globally 436
Enabling MLD Snooping Globally 436
(Optional) Configuring Unknown Multicast 436
(Optional) Configuring Report Message Suppression 437
Configuring Router Port Time and Member Port Time 437
Configuring MLD Snooping Last Listener Query 438
Verifying MLD Snooping Status 438
Configuring the Port's Basic MLD Snooping Features 439
Enabling MLD Snooping on the Port 439
(Optional) Configuring Fast Leave 439
Configuring MLD Snooping in the VLAN 440
Configuring MLD Snooping Globally in the VLAN 440
(Optional) Configuring the Static Router Ports in the VLAN 441
(Optional) Configuring the Forbidden Router Ports in the VLAN 441
Configuring the Multicast VLAN 441
Creating Multicast VLAN and Configuring Basic Settings 442
(Optional) Creating Replace Source IP 443
Viewing Dynamic Router Ports in the Multicast VLAN 443
(Optional) Configuring the Static Router Ports 443
(Optional) Configuring the Forbidden Router Ports 443

(Optional) Configuring the Querier....444
Configuring the Querier....444
Viewing Settings of MLD Querier....444
Configuring MLD Profile....445
Creating Profile....445
Searching Profile....445
Editing IP Range of the Profile....446
Binding Profile and Member Ports....447
Binding Profile and Member Ports....447
Configuring Max Groups a Port Can Join....448
Viewing MLD Statistics on Each Port....449
Configuring Auto Refresh....449
Viewing MLD Statistics....449
Configuring Static Member Port....450
Configuring Static Member Port....450
Viewing MLD Static Multicast Groups....450
Using the CLI....451
Enabling MLD Snooping Globally....451
Enabling MLD Snooping on the Port....451
Configuring MLD Snooping Parameters Globally....452
Configuring Report Message Suppression....452
Configuring Unknown Multicast....453
Configuring MLD Snooping Parameters on the Port....454
Configuring Router Port Time and Member Port Time....454
Configuring Fast Leave....455
Configuring Max Group and Overflow Action on the Port....456
Configuring MLD Snooping Last Listener Query....457
Configuring MLD Snooping Parameters in the VLAN....458
Configuring Router Port Time and Member Port Time....458
Configuring Static Router Port....459
Configuring Forbidden Router Port....460
Configuring Static Multicast (Multicast IP and Forward Port)....461
Configuring MLD Snooping Parameters in the Multicast VLAN....462
Configuring Router Port Time and Member Port Time....462
Configuring Static Router Port....463
Configuring Forbidden Router Port....464
Configuring Replace Source IP....465
Configuring the Querier....466

Enabling MLD Querier 466
Configuring Query Interval, Max Response Time and General Query Source IP 467
Configuring Multicast Filtering 468
Creating Profile 468
Binding Profile to the Port 469
Viewing Multicast Snooping Configurations 471
Using the GUI 471
Viewing IPv4 Multicast Snooping Configurations 471
Viewing IPv6 Multicast Snooping Configurations 472
Using the CLI 472
Viewing IPv4 Multicast Snooping Configurations 472
Viewing IPv6 Multicast Snooping Configurations 473
Configuration Examples 475
Example for Configuring Basic IGMP Snooping 475
Network Requirements 475
Configuration Scheme 475
Using the GUI 476
Using the CLI 479
Example for Configuring Multicast VLAN 481
Network Requirements 481
Configuration Scheme 481
Network Topology 481
Using the GUI 482
Using the CLI 485
Example for Configuring Unknown Multicast and Fast Leave 487
Network Requirement 487
Configuration Scheme 488
Using the GUI 488
Using the CLI 491
Example for Configuring Multicast Filtering 492
Network Requirements 492
Configuration Scheme 492
Network Topology 492
Using the GUI 493
Using the CLI 500
Appendix: Default Parameters 503
Default Parameters for IGMP Snooping 503
Default Parameters for MLD Snooping 504

Configuring Logical Interfaces

Overview 507
Logical Interfaces Configurations 508
Using the GUI 508
Creating a Layer 3 Interface 508
Configuring IPv4 Parameters of the Interface 509
Configuring IPv6 Parameters of the Interface 510
Viewing Detail Information of the Interface 513
Using the CLI 513
Creating a Layer 3 Interface 513
Configuring IPv4 Parameters of the Interface 515
Configuring IPv6 Parameters of the Interface 516
Appendix: Default Parameters 519

Configuring Static Routing

Overview 521
IPv4 Static Routing Configuration 522
Using the GUI 522
Using the CLI 523
IPv6 Static Routing Configuration 524
Using the GUI 524
Using the CLI 525
Viewing Routing Table 526
Using the GUI 526
Viewing IPv4 Routing Table 526
Viewing IPv6 Routing Table 527
Using the CLI 527
Viewing IPv4 Routing Table 527
Viewing IPv6 Routing Table 528
Example for Static Routing 529
Network Requirements 529
Configuration Scheme 529
Using the GUI 529
Using the CLI 530
Appendix: Default Parameter 533

Configuring DHCP

DHCP 535
Overview 535
Supported Features 535
DHCP Server Configuration 539
Using the GUI 539
Enabling DHCP Server 539
Configuring DHCP Server Pool 541
Configuring Manual Binding 542
Using the CLI 544
Enabling DHCP Server 544
Configuring DHCP Server Pool 546
Configuring Manual Binding 549
DHCP Client Configuration 551
Using the GUI 551
Using the CLI 552
DHCP Relay Configuration 554
Using the GUI 554
Enabling DHCP Relay globally and Configuring Option 82 554
Enabling DHCP Relay for ports 556
Specifying DHCP Server for the Interface or VLAN 557
Using the CLI 559
Enabling DHCP Relay globally 559
(Optional) Configuring Option 82 559
Enabling DHCP Relay for ports 561
Specifying DHCP Server for Interface or VLAN 562
DHCP L2 Relay Configuration 566
Using the GUI 566
Enabling DHCP L2 Relay 566
Configuring Option 82 for Ports 567
Using the CLI 568
Enabling DHCP L2 Relay 568
Configuring Option 82 for Ports 569
Configuration Examples 571
Example for DHCP Server 571
Network Requirements 571
Configuration Scheme 571

Using the GUI....571
Using the CLI....574
Example for DHCP Interface Relay....575
Network Requirements....575
Configuration Scheme....575
Using the GUI....576
Using the CLI....577
Appendix: Default Parameters....579

Configuring ARP

Overview....583
ARP Configurations....584
Using the GUI....584
Viewing the ARP Entries....584
Adding Static ARP Entries Manually....585
Using the CLI....585
Configuring ARP Function....585

Configuring QoS

QoS....590
Overview....590
Supported Features....590
DiffServ Configuration....591
Using the GUI....592
Configuring Port Priority....592
Configuring 802.1P Priority....594
Configuring DSCP Priority....597
Configuring Schedule Mode....600
Using CLI....601
Configuring Port Priority....601
Configuring 802.1P Priority....603
Configuring DSCP Priority....606
Configuring Schedule Mode....610
Bandwidth Control Configuration....613
Using the GUI....613
Configuring Rate Limit....613
Configuring Storm Control....614

Using the CLI 616
Configuring Rate Limit on Port 616
Configuring Storm Control 617
Configuration Examples 620
Example for Configuring SP Mode 620
Network Requirements 620
Configuration Scheme 620
Using the GUI 621
Using the CLI 622
Example for Configuring WRR Mode 624
Network Requirements 624
Configuration Scheme 624
Using the GUI 625
Using the CLI 632
Appendix: Default Parameters 637

Configuring Voice VLAN

Overview 640
Voice VLAN Configuration 642
Using the GUI 643
Configuring OUI Addresses 643
Configuring Voice VLAN Globally 644
Configuring Voice VLAN Mode on Ports 645
Using the CLI 646
Configuration Example 649
Network Requirements 649
Configuration Scheme 649
Network Topology 649
Using the GUI 651
Using the CLI 661
Appendix: Default Parameters 666

Configuring PoE

PoE 668
Overview 668
Supported Features 668
PoE Power Management Configurations 669

Using the GUI 669
Configuring the PoE Parameters Manually 669
Configuring the PoE Parameters Using the Profile 671
Using the CLI 673
Configuring the PoE Parameters Manually 673
Configuring the PoE Parameters Using the Profile 675
Time-Range Function Configurations 677
Using the GUI 677
Creating a Time-Range 677
Configuring the Holiday Parameters 679
Viewing the Time-Range Table 679
Using the CLI 680
Configuring a Time-Range 680
Configuring the Holiday Parameters 682
Viewing the Time-Range Table 683
Example for PoE Configurations 684
Network Requirements 684
Configuring Scheme 684
Using the GUI 684
Using the CLI 686
Appendix: Default Parameters 688

Configuring ACL

Overview 690
Introduction 690
Supported Features 690
ACL Configuration 691
Using the GUI 692
Configuring Time-Range 692
(Optional) Configuring Holiday 693
Creating an ACL 693
Configuring ACL Rules 695
Configuring Policy 703
Configuring the ACL Binding and Policy Binding 706
Using the CLI 711
Configuring Time Range 711
Configuring ACL 713

Configuring Policy....722
ACL Binding and Policy Binding....724
Configuration Example for ACL....727
Network Requirements....727
Network Topology....727
Configuration Scheme....727
Using the GUI....728
Using the CLI....733
Appendix: Default Parameters....735

Configuring Network Security

Network Security....738
Overview....738
Supported Features....738
IP-MAC Binding Configurations....745
Using the GUI....745
Binding Entries Manually....745
Binding Entries Dynamically....746
Viewing the Binding Entries....748
Using the CLI....749
Binding Entries Manually....750
Viewing Binding Entries....751
IPv6-MAC Binding Configurations....751
Using the GUI....752
Binding Entries Manually....752
Binding Entries Dynamically....753
Viewing the Binding Entries....755
Using the CLI....757
Binding Entries Manually....757
Binding Entries via ND Snooping....758
Viewing Binding Entries....759
DHCP Snooping Configuration....760
Using the GUI....760
Enabling DHCP Snooping on VLAN....760
Configuring DHCP Snooping on Ports....762
Using the CLI....763
Enabling DHCP Snooping on VLAN....763

Configuring DHCP Snooping on Ports 764
DHCPv6 Snooping Configuration 765
Using the GUI 766
Using the CLI 766
ARP Inspection Configurations 768
Using the GUI 768
Configuring ARP Detection 768
Configuring ARP Defend 769
Viewing ARP Statistics 771
Using the CLI 772
Configuring ARP Detection 772
Configuring ARP Defend 773
Viewing ARP Statistics 775
ND Detection Configuration 775
Using the GUI 775
Using the CLI 776
IP Source Guard Configuration 777
Using the GUI 777
Using the CLI 779
DoS Defend Configuration 780
Using the GUI 780
Using the CLI 781
802.1X Configuration 783
Using the GUI 783
Configuring the RADIUS Server 783
Configuring 802.1X Globally 787
Configuring 802.1X on Ports 789
Using the CLI 790
Configuring the RADIUS Server 790
Configuring 802.1X Globally 792
Configuring 802.1X on Ports 795
PPPoE ID-Insertion Configuration 797
Using the GUI 797
Using the CLI 798
AAA Configuration 800
Using the GUI 801
Globally Enabling AAA 801
Adding Servers 801

Configuring Server Groups....803
Configuring the Method List....805
Configuring the AAA Application List....806
Configuring Login Account and Enable Password....807
Using the CLI....808
Globally Enabling AAA....808
Adding Servers....808
Configuring Server Groups....811
Configuring the Method List....812
Configuring the AAA Application List....813
Configuring Login Account and Enable Password....818
DHCP Server Filter Configuration....820
Using the GUI....820
Enabling DHCP Server Filter....820
Configuring the DHCP Server Permit Entry....821
Using the CLI....822
Enabling DHCP Server Filter globally....822
Enabling DHCP Server Filter for ports....823
Configuring the DHCP Server Permit Entry....824
NetBIOS Filtering Configuration....825
Using the GUI....825
Using the CLI....826
Configuration Examples....827
Example for DHCP Snooping and ARP Detection....827
Network Requirements....827
Configuration Scheme....827
Using the GUI....828
Using the CLI....831
Example for DHCPv6 Snooping and ND Detection....833
Network Requirements....833
Configuration Scheme....834
Using the GUI....834
Using the CLI....836
Example for IP Source Guard....838
Network Requirements....838
Configuration Scheme....838

Using the GUI 839
Using the CLI 840
Example for 802.1X 841
Network Requirements 841
Configuration Scheme 841
Network Topology 842
Using the GUI 842
Using the CLI 845
Example for AAA 847
Network Requirements 847
Configuration Scheme 848
Using the GUI 848
Using the CLI 851
Appendix: Default Parameters 854

Configuring LLDP

LLDP 866
Overview 866
Supported Features 866
LLDP Configurations 867
Using the GUI 867
Global Config 867
Port Config 869
Using the CLI 870
Global Config 870
Port Config 872
LLDP-MED Configurations 875
Using the GUI 875
Global Config 875
Port Config 876
Using the CLI 878
Global Config 878
Port Config 879
Viewing LLDP Settings 882
Using GUI 882
Viewing LLDP Device Info 882
Viewing LLDP Statistics 885

Using CLI 886
Viewing LLDP-MED Settings 887
Using GUI 887
Using CLI 889
Configuration Example 890
Example for Configuring LLDP 890
Network Requirements 890
Network Topology 890
Configuration Scheme 890
Using the GUI 890
Using CLI 891
Example for Configuring LLDP-MED 897
Network Requirements 897
Configuration Scheme 897
Network Topology 897
Using the GUI 898
Using the CLI 902
Appendix: Default Parameters 909

Configuring Maintenance

Maintenance 911
Overview 911
Supported Features 911
Monitoring the System 912
Using the GUI 912
Monitoring the CPU 912
Monitoring the Memory 913
Using the CLI 914
Monitoring the CPU 914
Monitoring the Memory 914
SFlow Configuration 915
Using the GUI 915
Configuring the SFlow Collector 915
Configuring the SFlow Sampler 916
Using the CLI 917
System Log Configurations 920
Using the GUI 921

Configuring the Local Log....921
Configuring the Remote Log....922
Backing up the Log File....922
Viewing the Log Table....923
Using the CLI....923
Configuring the Local Log....923
Configuring the Remote Log....925
Diagnosing the Device....927
Using the GUI....927
Using the CLI....928
Diagnosing the Network....929
Using the GUI....929
Configuring the Ping Test....929
Configuring the Tracert Test....930
Using the CLI....931
Configuring the Ping Test....931
Configuring the Tracert Test....932
DLDP Configuration....933
Using the GUI....933
Using the CLI....935
Configuration Examples....937
Example for Configuring SFlow....937
Network Requirements....937
Configuration Scheme....937
Using the GUI....937
Using the CLI....938
Example for Configuring Remote Log....940
Network Requirements....940
Configuration Scheme....940
Using the GUI....940
Using the CLI....940
Appendix: Default Parameters....942

Configuring SNMP & RMON

SNMP Overview....945
SNMP Configurations....946
Using the GUI....947

Enabling SNMP....947
Creating an SNMP View....947
Creating an SNMP Group....948
Creating SNMP Users....950
Creating SNMP Communities....951
Using the CLI....952
Enabling SNMP....952
Creating an SNMP View....954
Creating an SNMP Group....955
Creating SNMP Users....957
Creating SNMP Communities....958
Notification Configurations....960
Using the GUI....960
Using the CLI....962
Configuring the Host....962
Enabling SNMP Notification....963
RMON Overview....969
RMON Configurations....970
Using the GUI....970
Configuring Statistics....970
Configuring History....971
Configuring Event....972
Configuring Alarm....973
Using the CLI....975
Configuring Statistics....975
Configuring History....976
Configuring Event....977
Configuring Alarm....979
Configuration Example....981
Network Requirements....981
Configuration Scheme....981
Network Topology....982
Using the GUI....982
Using the CLI....987
Appendix: Default Parameters....993

About This Guide

This Configuration Guide provides information for managing T2600G Series Switches. Please read this guide carefully before operation.

Intended Readers

This Guide is intended for network managers familiar with IT concepts and network terminologies.

Conventions

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

When using this guide, please notice that features of the switch may vary slightly depending on the model and software version you have. All screenshots, images, parameters and descriptions documented in this guide are used for demonstration only.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied. Users must take full responsibility for their application of any products.

In this Guide, the following conventions are used:

The symbol  stands for *Note*. Notes contains suggestions or references that helps you make better use of your device.

- For GUI:

Menu Name > Submenu Name > Tab page indicates the menu structure. **System > System Info > System Summary** means the System Summary page under the System Info menu option that is located under the System menu.

Bold font indicates a button, a toolbar icon, menu or menu item.

- For CLI:

Bold Font	An unalterable keyword. For example: **show logging**

Normal Font	A constant (several options are enumerated and only one can be selected). For example: **no bandwidth** {all | ingress | egress}
{}	Items in braces { } are required.
[]	Items in square brackets [ ] are optional.
|	Alternative items are grouped in braces and separated by vertical bars |. For example: **speed** {10 | 100 | 1000}
Italic Font	A variable (an actual value must be assigned). For example: **bridge aging-time** *aging-time*

Common combination:

{[ ][ ][ ]}	A least one item in the square brackets must be selected. For example: **bandwidth** {[**ingress** *ingress-rate*] [**egress** *egress-rate*]} This command can be used on three occasions: **bandwidth ingress** *ingress-rate* is used to restrict ingress bandwidth. **bandwidth egress** *egress-rate* is used to restrict egress bandwidth. **bandwidth ingress** *ingress-rate* **egress** *egress-rate* is used to restrict ingress and egress bandwidth.

More Information

- The latest software and documentations can be found at Download Center at https://www.tp-link.com/support.
- The Installation Guide (IG) can be found where you find this guide or inside the package of the switch.
- Specifications can be found on the product page at https://www.tp-link.com.
- A Technical Support Forum is provided for you to discuss our products at https://forum.tp-link.com.
- Our Technical Support contact information can be found at the Contact Technical Support page at https://www.tp-link.com/support.

Part 1

Accessing the Switch

CHAPTERS

1. Overview
2. Web Interface Access
3. Command Line Interface Access

1 Overview

You can access and manage the switch using the GUI (Graphical User Interface, also called web interface in this text) or using the CLI (Command Line Interface). There are equivalent functions in the web interface and the command line interface, while web configuration is easier and more visual than the CLI configuration. You can choose the method according to their available applications and preference.

2 Web Interface Access

You can access the switch's web interface through the web-based authentication. The switch uses two built-in web servers, HTTP server and HTTPS server, for user authentication.

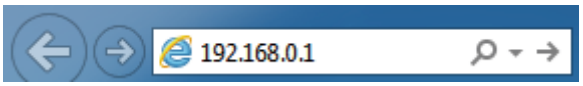
The following example shows how to login via the HTTP server.

2.1 Login

To manage your switch through a web browser in the host PC:

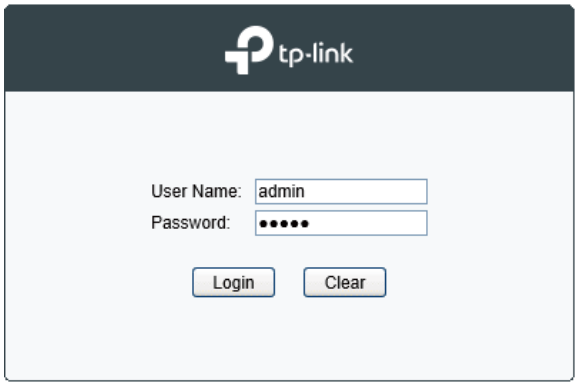
1) Make sure that the route between the host PC and the switch is available.
2) Launch a web browser. The supported web browsers include, but are not limited to, the following types:
   - IE 8.0, 9.0, 10.0, 11.0
   - Firefox 26.0, 27.0
   - Chrome 32.0, 33.0
3) Enter the switch's IP address in the web browser's address bar. The switch's default IP address is 192.168.0.1.

   Figure 2-1 Enter the switch's IP addresss in the browser



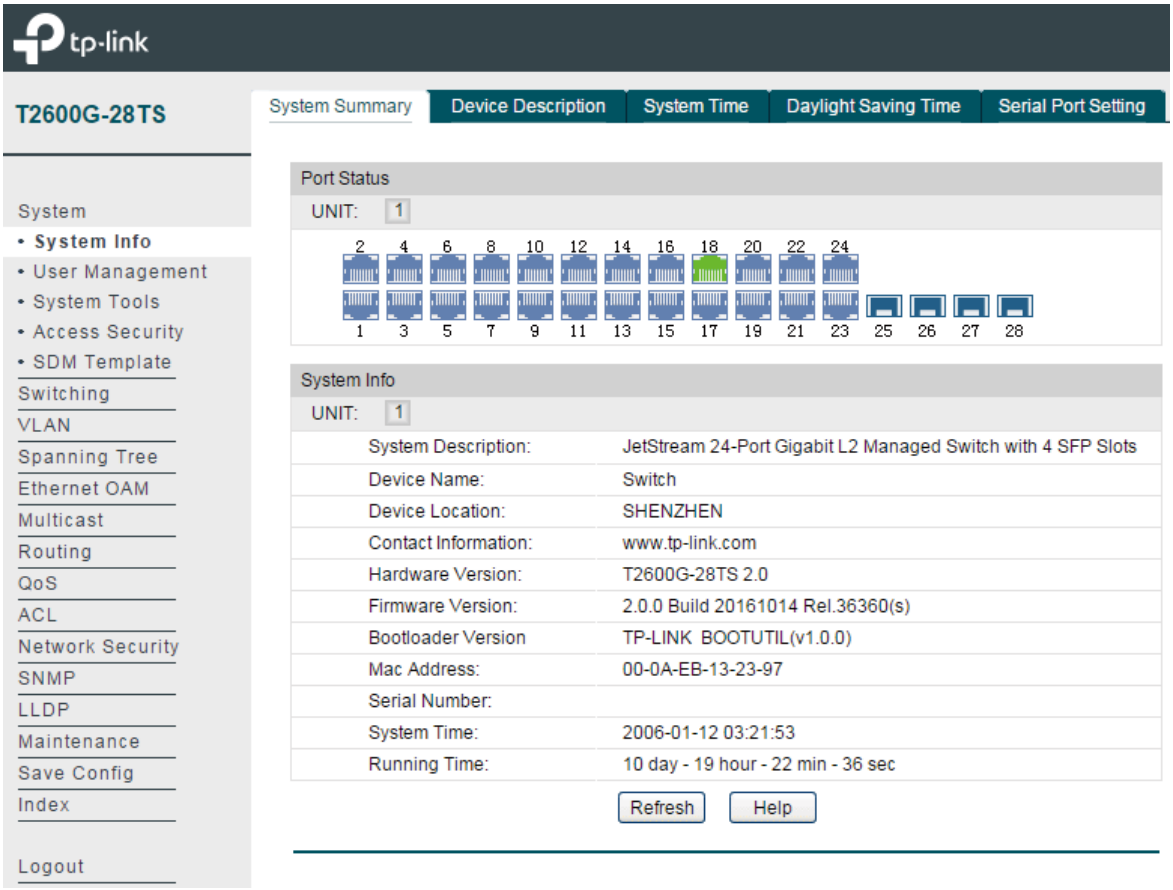
4) Enter the username and password in the pop-up login window. Use **admin** for both username and password in lower case letters.

   Figure 2-2 Login authentication



5) The typical web interface displays below. You can view the switch's running status and configure the switch on this interface.

Figure 2-3 Web interface



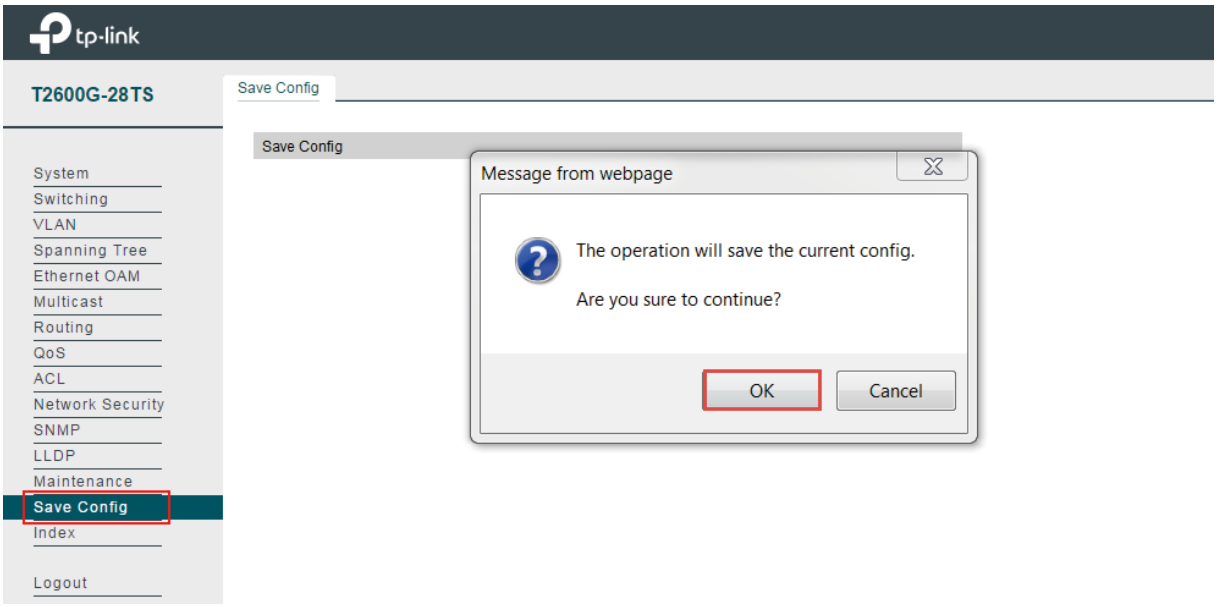
2.2 Save Config Function

The switch's configuration files fall into two types: the running configuration file and the start-up configuration file.

After you perform configurations on the sub-interfaces and click **Apply**, the modifications will be saved in the running configuration file. The configurations will be lost when the switch reboots.

If you need to keep the configurations after the switch reboots, please use the Save Config function on the main interface to save the configurations in the start-up configuration file.

Figure 2-4 Save Config

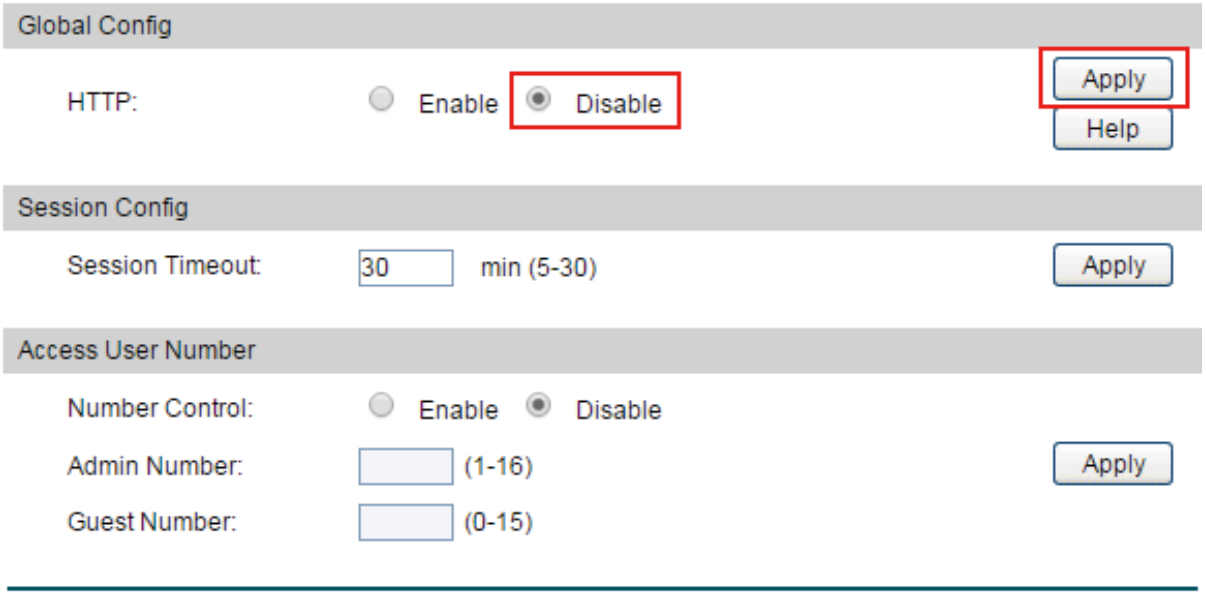


2.3 Disable the Web Server

You can shut down the HTTP server or HTTPS server to block any access to the web interface.

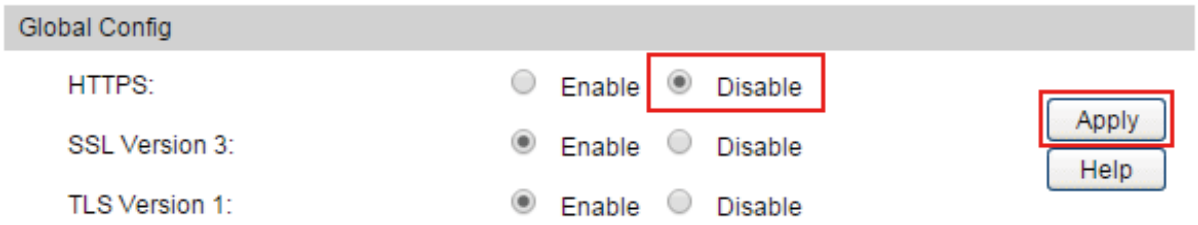
Go to **System > Access Security > HTTP Config**, disable the HTTP server and click **Apply**.

Figure 2-5 Shut down HTTP server



Go to **System > Access Security > HTTPS Config**, disable the HTTPS server and click **Apply**.

Figure 2-6 Disbale the HTTPS Server



2.4 Configure the Switch's IP Address and Default Gateway

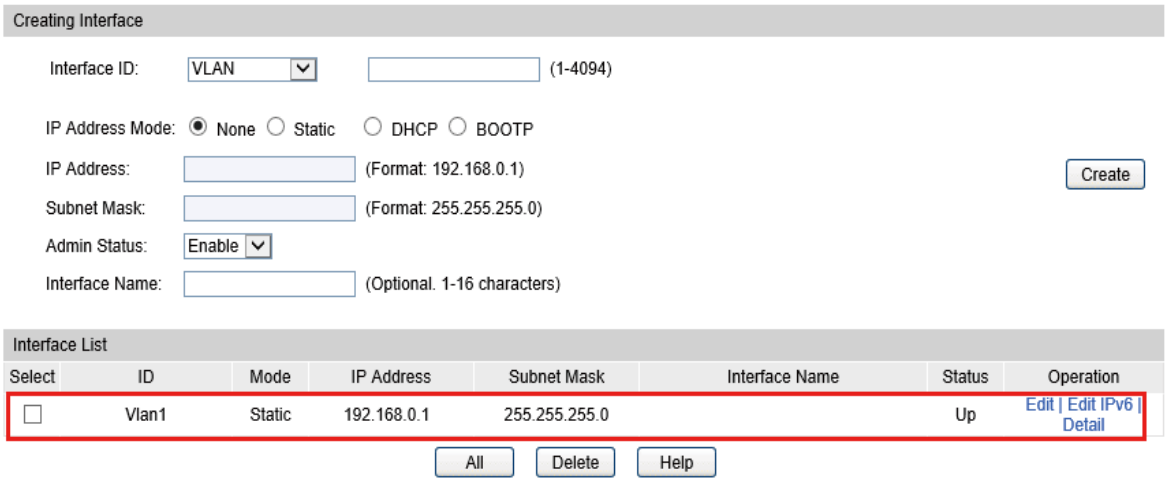
If you want to access the switch via a specified port (hereafter referred to as the access port), you can configure the port as a routed port and specify its IP address, or configure the IP address of the VLAN which the access port belongs to.

- Change the IP Address

By default, all the ports belong to VLAN 1 with the VLAN interface IP 192.168.0.1. The following example shows how to change the switch's default access IP address 192.168.0.1.

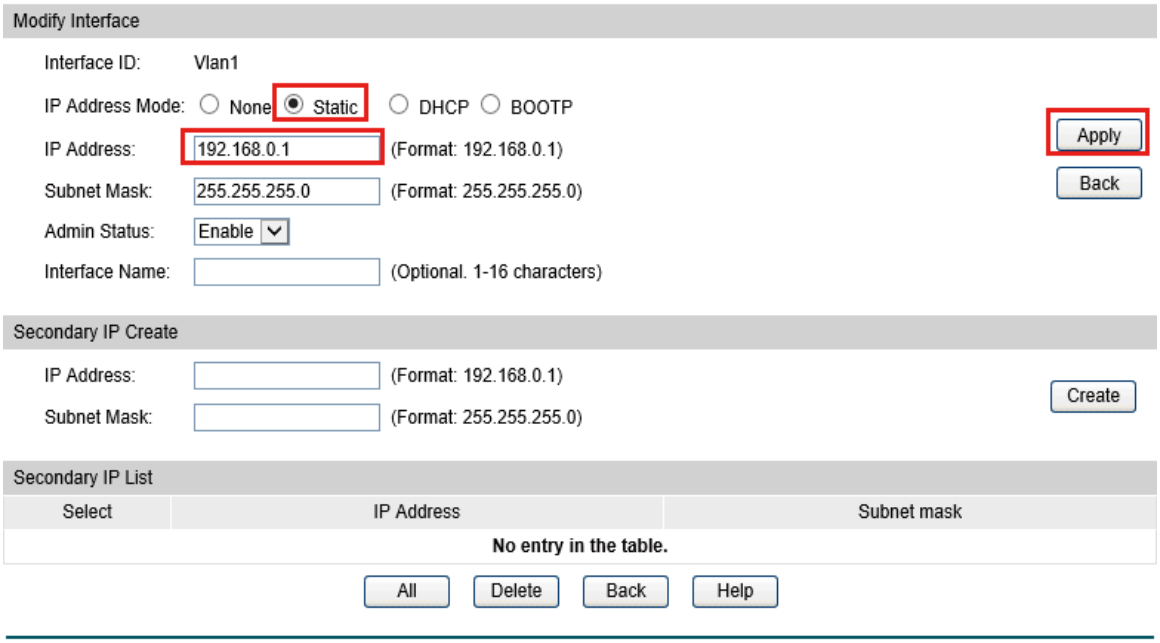
1) Go to **Routing > Interface > Interface Config**. The default access IP address in VLAN 1 in the Interface List. Click **Edit** to modify the VLAN1's IP address.

Figure 2-7 Change VLAN1's IP address



2) Choose the **IP Address Mode** as **Static**. Enter the new access address in the **IP Address** field and click **Apply**. Make sure that the route between the host PC and the switch's new IP address is available.

Figure 2-8 Specify the IP address



3) Enter the new IP address in the web browser to access the switch.

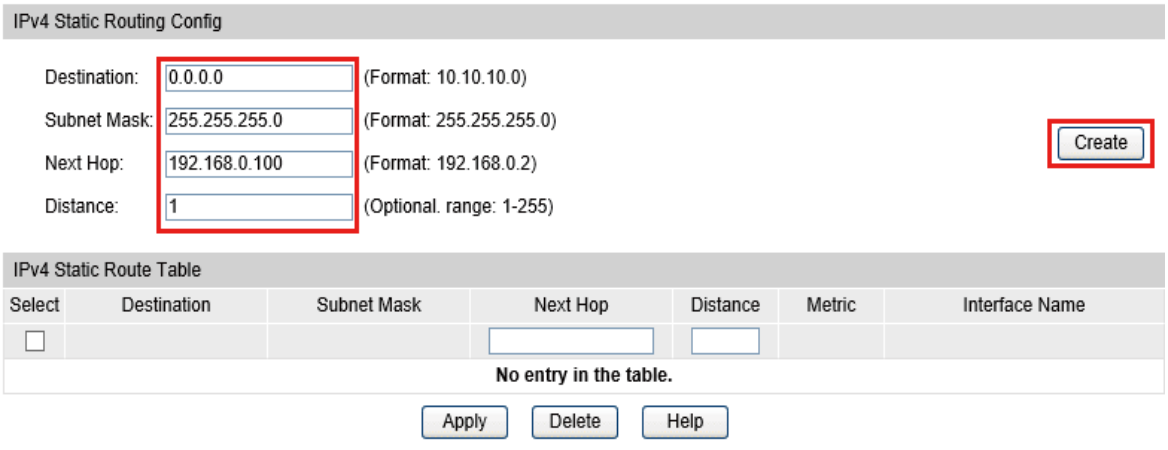
4) Click **Save Config** to save the settings.

- Configure the Default Gateway

The following example shows how to configure the switch's gateway. By default, the switch has no default gateway.

1) Go to page **Routing > Static Routing > IPv4 Static Routing Config**. Configure the parameters related to the switch's gateway and click **Create**.

Figure 2-9 Configure the default gateway



Destination	Specify the destination as 0.0.0.0.
Subnet Mask	Specify the subnet mask as 255.255.255.0.
Next Hop	Configure your desired default gateway as the next hop's IP address.

Distance	Specify the distance as 1.

2) Click **Save Config** to save the settings.

3) Check the routing table to verify the default gateway you configured. The entry marked in red box displays the valid default gateway.

Figure 2-10 View the default gateway

IPv4 Routing Information Summary

Protocol	Destination Network	Next Hop	Distance	Metric	Interface Name
static	0.0.0.0/24	192.168.0.100	1	0	
connected	192.168.0.0/24	192.168.0.16	0	1	

Refresh

3 Command Line Interface Access

Users can access the switch's command line interface through the console (only for switch with console port), Telnet or SSH connection, and manage the switch with the command lines.

Console connection requires the host PC connecting to the switch's console port directly, while Telnet and SSH connection support both local and remote access.

The following table shows the typical applications used in the CLI access.

Table 3-1 Method list

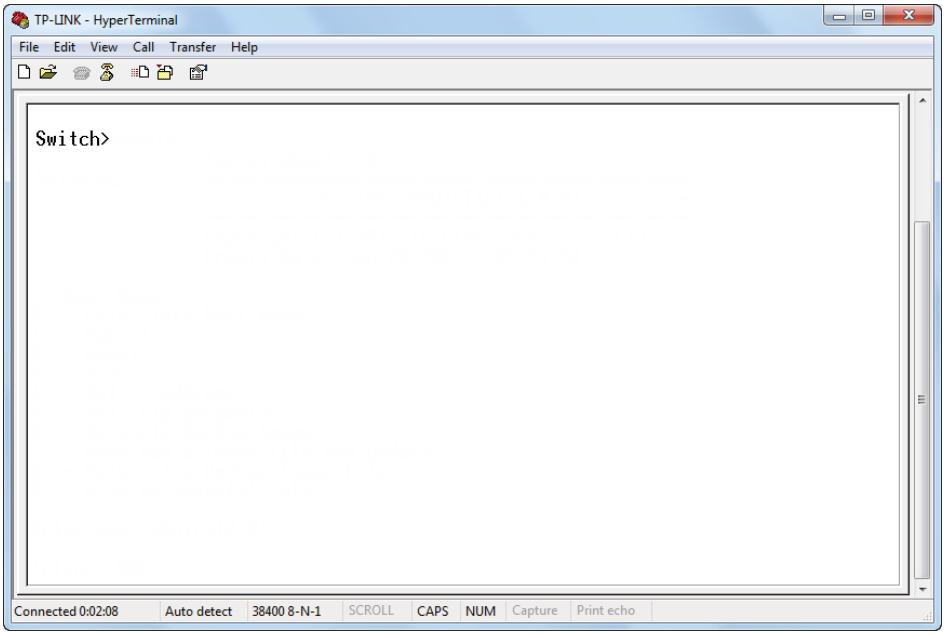
Method	Using Port	Typical Applications
Console	Console port (connected directly)	Hyper Terminal
Telnet	RJ-45 port	CMD
SSH	RJ-45 port	Putty

3.1 Console Login (only for switch with console port)

Follow these steps to log in to the switch via the Console port:

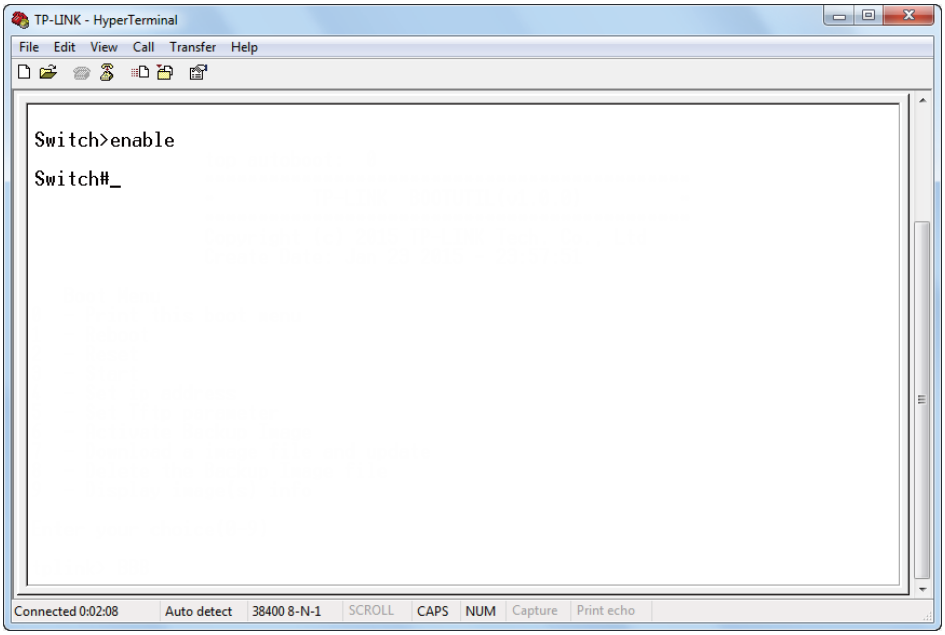
1) Connect the PC or terminal to the Console port on the switch with the serial cable.
2) Start the terminal emulation program (such as the Hyper Terminal) on the PC and configure the terminal emulation program as follows:
   - Baud Rate: 38400bps
   - Data Bits: 8
   - Parity: None
   - Stop Bits: 1
   - Flow Control: None
3) 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 3-1 CLI Main Window



4) Enter **enable** to enter the User EXEC Mode to further configure the switch.

Figure 3-2 User EXEC Mode



Note:

In Windows XP, go to **Start > All Programs > Accessories > Communications > Hyper Terminal** to open the Hyper Terminal and configure the above settings to log in to the switch.

3.2 Telnet Login

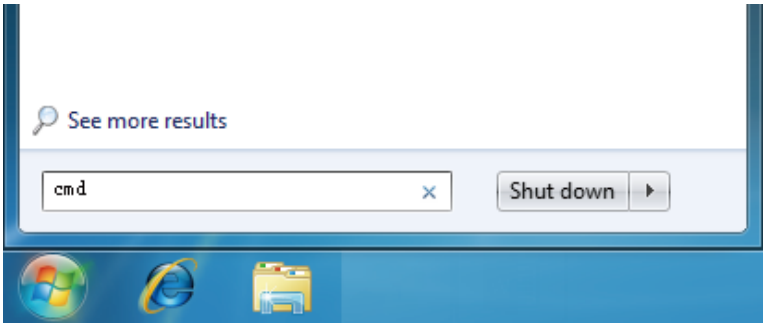
The switch supports Login Local Mode for authentication by default.

Login Local Mode: Username and password are required, which are both admin by default.

The following steps show how to manage the switch via the Login Local Mode:

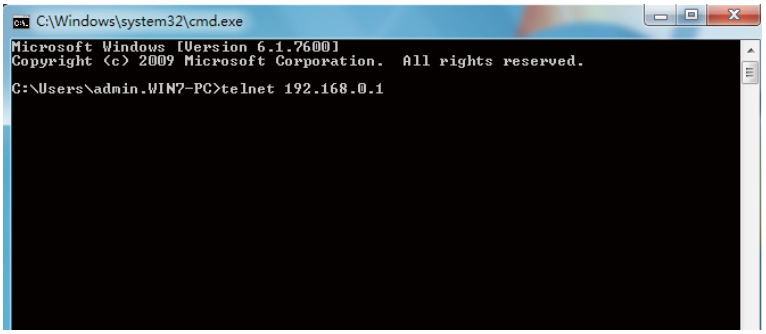
1) Make sure the switch and the PC are in the same LAN (Local Area Network). Click **Start** and type in **cmd** in the Search bar and press **Enter**.

Figure 3-3 Open the cmd Window



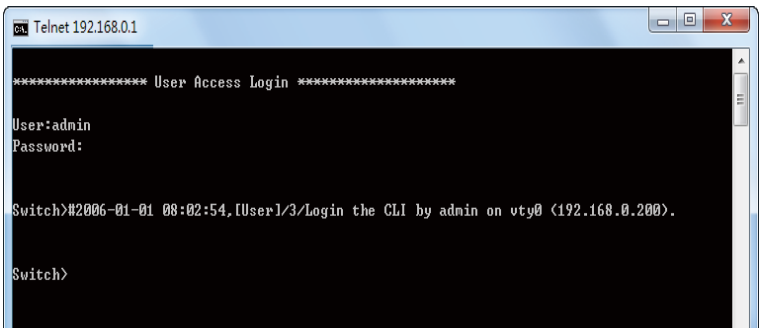
2) Type in **telnet 192.168.0.1** in the cmd window and press **Enter**.

Figure 3-4 Log In to the Switch



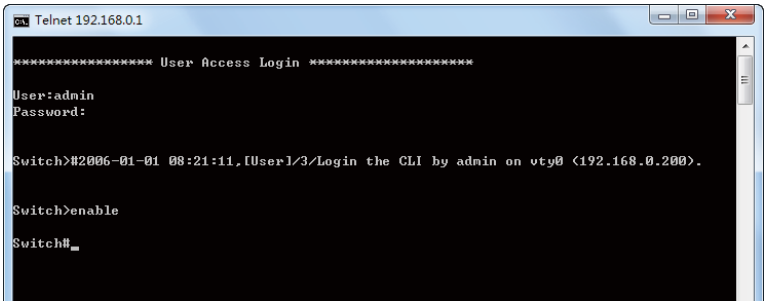
3) Type in the login username and password (both **admin** by default). Press **Enter** and you will enter User EXEC Mode.

Figure 3-5 Enter User EXEC Mode



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 3-6 Enter Privileged EXEC Mode



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

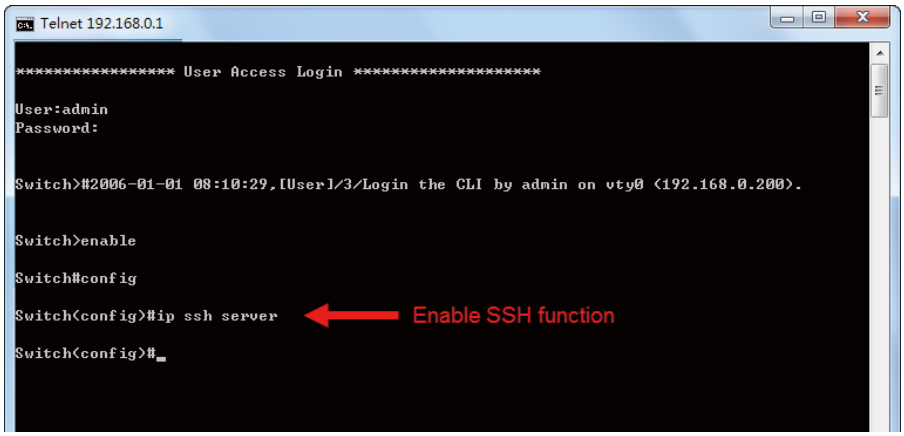
3.3 SSH Login

SSH login supports the following two modes: Password Authentication Mode and Key Authentication Mode. You can choose one according to your needs:

- Password Authentication Mode: Username and password are required, which are both **admin** by default.
- Key Authentication Mode (Recommended): A public key for the switch and a private key for the client software (PuTTY) are required. You can generate the public key and the private key through the PuTTY Key Generator.

Before logging in via SSH, follow the steps below to enable SSH on the terminal emulation program:

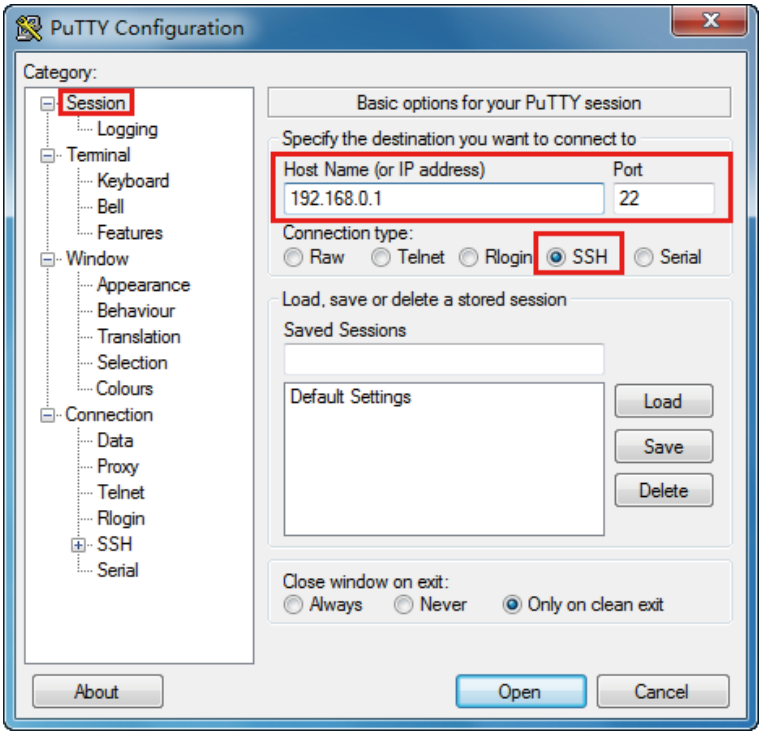
Figure 3-7 Enable SSH



Password Authentication Mode

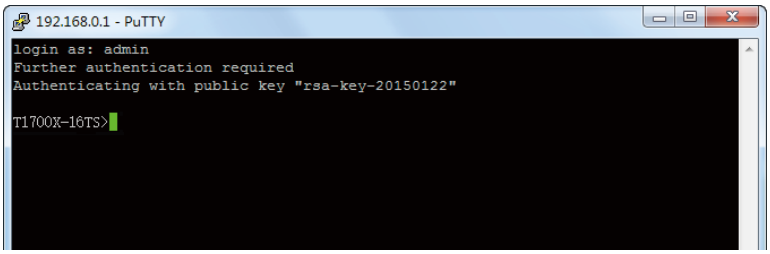
1) Open PuTTY and go to the Session page. Enter the IP address of the switch in the **Host Name** field and keep the default value 22 in the **Port** field; select **SSH** as the Connection type. Click **Open**.

Figure 3-8 Configurations in PuTTY



2) Enter the login username and password to log in to the switch, and you can continue to configure the switch.

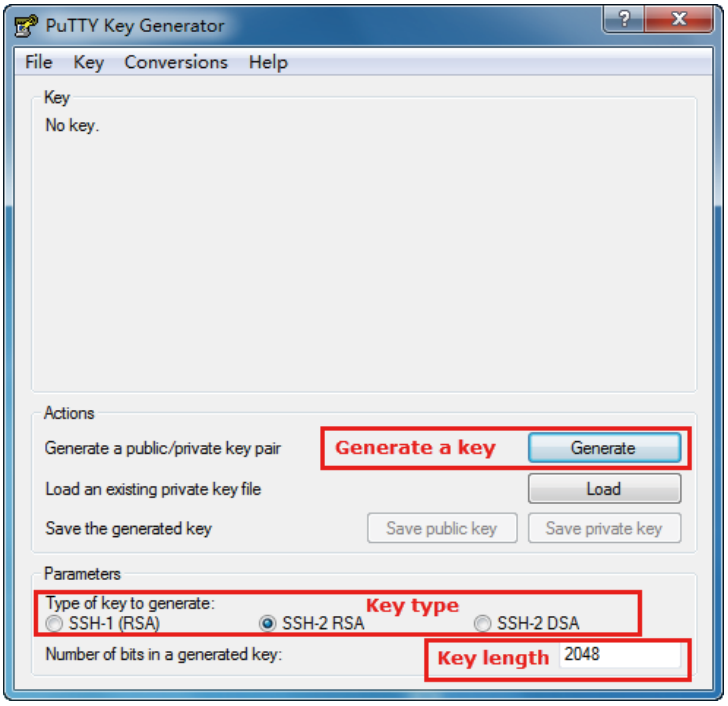
Figure 3-9 Log In to the Switch



Key Authentication Mode

1) Open the PuTTY Key Generator. In the Parameters section, select the key type and enter the key length. In the **Actions** section, click **Generate** to generate a public/private key pair. In the following figure, an SSH-2 RSA key pair is generated, and the length of each key is 1024 bits.

Figure 3-10 Generate a Public/Private Key Pair

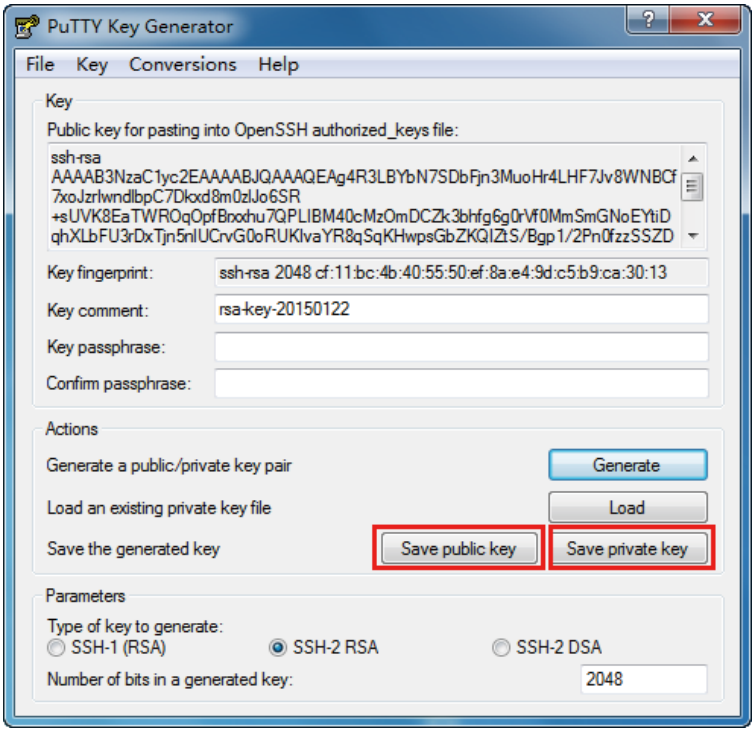


Note:

- The key length should be between 512 and 3072 bits.
- You can accelerate the key generation process by moving the mouse quickly and randomly in the Key section.

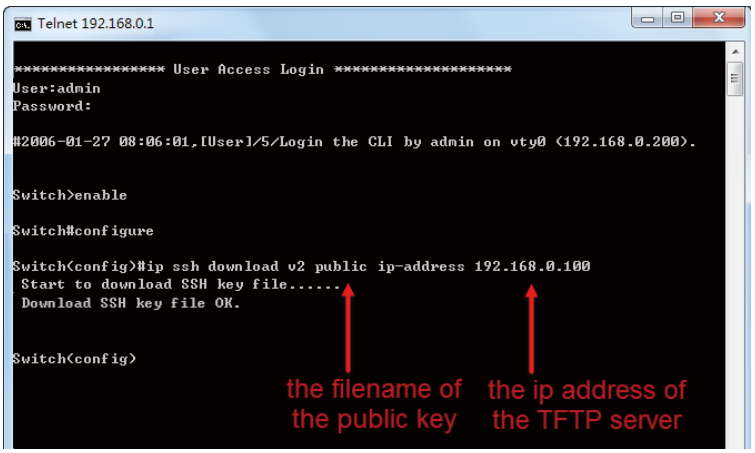
2) After the keys are successfully generated, click **Save public key** to save the public key to a TFTP server; click **Save private key** to save the private key to the host PC.

Figure 3-11 Save the Generated Keys



3) On Hyper Terminal, download the public key file from the TFTP server to the switch as shown in the following figure:

Figure 3-12 Download the Public Key to the Switch

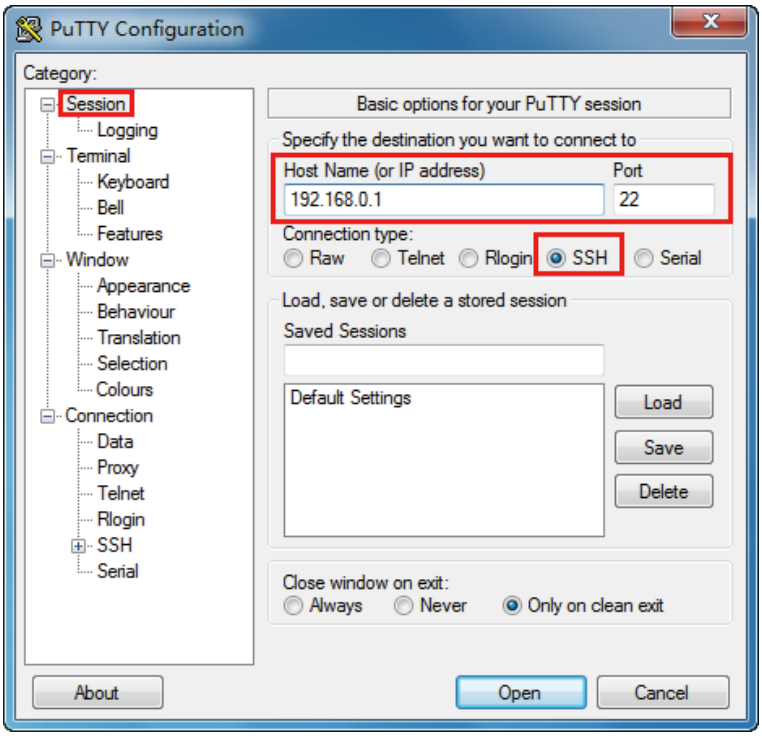


Note:

- The key type should accord with the type of the key file. In the above CLI, v1 corresponds to SSH-1 (RSA), and v2 corresponds to SSH-2 RSA and SSH-2 DSA.
- The key downloading process cannot be interrupted.

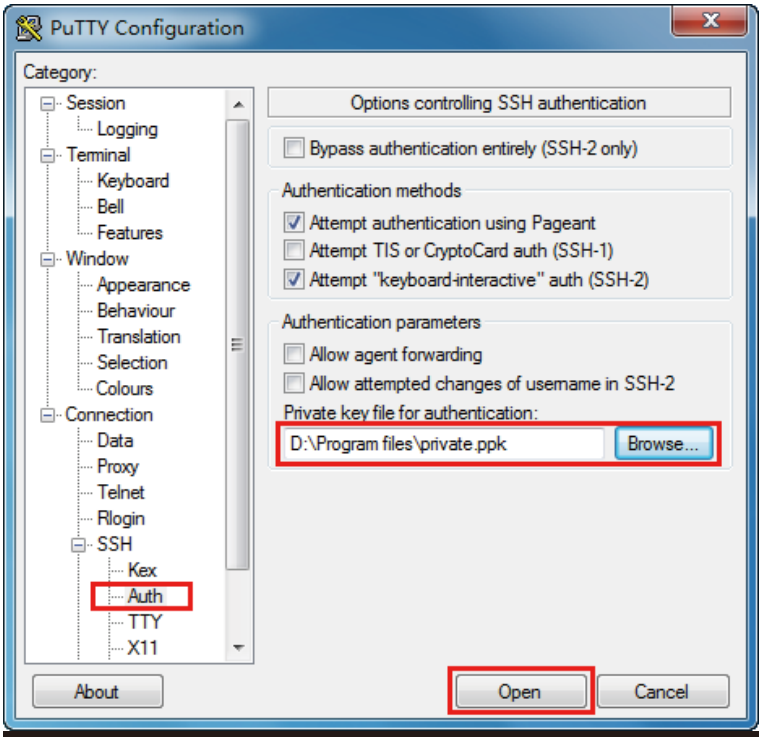
4) After the public key is downloaded, open PuTTY and go to the **Session** page. Enter the IP address of the switch and select **SSH** as the Connection type (keep the default value in the Port field).

Figure 3-13 Configure the Host Name and Connection Type



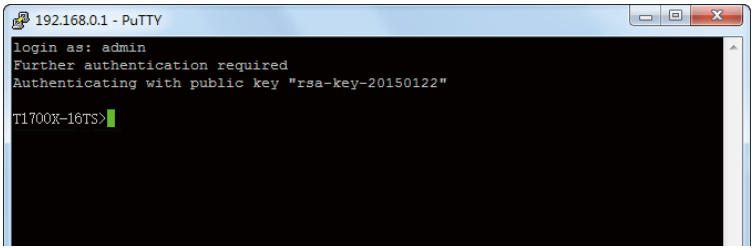
5) Go to **Connection > SSH > Auth**. Click **Browse** to download the private key file to PuTTY. Click **Open** to start the connection and negotiation.

Figure 3-14 Download the Private Key to PuTTY



6) After negotiation is completed, enter the username to log in. If you can log in without entering the password, the key authentication completed successfully.

Figure 3-15 Log In to the Switch



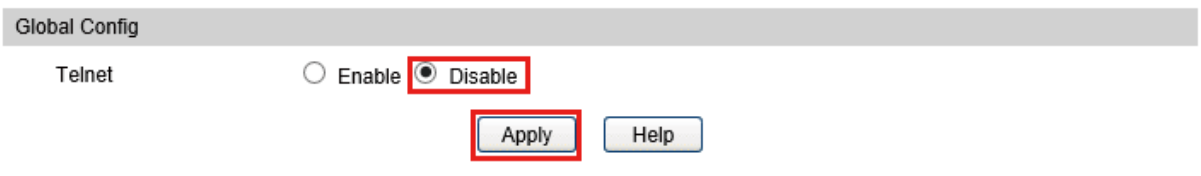
3.4 Disable Telnet login

You can shut down the Telnet function to block any Telnet access to the CLI interface.

- Using the GUI:

Go to **System > Access Security > Telnet Config**, disable the Telnet function and click **Apply**.

Figure 3-16 Disable Telnet login



- Using the CLI:

Switch#configure

Switch(config)#telnet disable

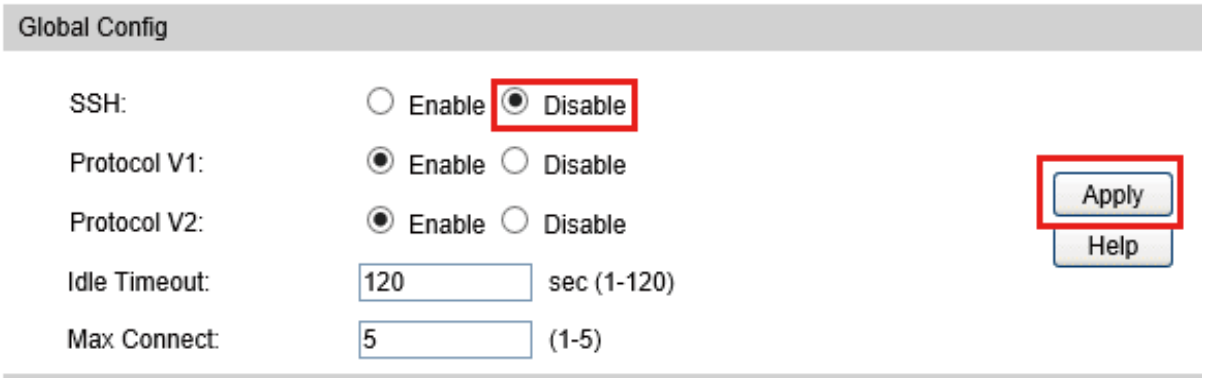
3.5 Disable SSH login

You can shut down the SSH server to block any SSH access to the CLI interface.

- Using the GUI:

Go to **System > Access Security > SSH Config**, disable the SSH server and click **Apply**.

Figure 3-17 Shut down SSH server



- Using the CLI:

Switch#configure

Switch(config)#no ip ssh server

3.6 Copy running-config startup-config

The switch's configuration files fall into two types: the running configuration file and the start-up configuration file.

After you enter each command line, the modifications will be saved in the running configuration file. The configurations will be lost when the switch reboots.

If you need to keep he configurations after the switch reboots, please user the command **copy running-config startup-config** to save the configurations in the start-up configuration file.

Switch(config)#end

Switch#copy running-config startup-config

3.7 Change the Switch's IP Address and Default Gateway

If you want to access the switch via a specified port (hereafter referred to as the access port), you can configure the port as a routed port and specify its IP address, or configure the IP address of the VLAN which the access port belongs to.

- Change the IP Address

By default, all the ports belong to VLAN 1 with the VLAN interface IP 192.168.0.1/24. In the following example, we will show how to replace the switch's default access IP address 192.168.0.1/24 with 192.168.0.10/24.

Switch#configure

Switch(config)#interface vlan 1

Switch(config-if)#ip address 192.168.0.10 255.255.255.0

The connection will be interrupted and you should telnet to the switch's new IP address 192.168.0.10.

C:\Users\Administrator>telnet 192.168.0.10

User:admin

Password:admin

Switch>enable

Switch#copy running-config startup-config

- Configure the Default Gateway

In the following example, we will show how to configure the switch's gateway as 192.168.0.100. By default, the switch has no default gateway.

Switch#configure

Switch(config)#ip route 0.0.0.0 255.255.255.0 192.168.0.100 1

Switch(config)#end

Switch#copy running-config startup-config

Part 2

Managing System

CHAPTERS

1. System
2. System Info Configurations
3. User Management Configurations
4. System Tools Configurations
5. Access Security Configurations
6. SDM Template Configuration
7. Appendix: Default Parameters

1 System

1.1 Overview

The System module is mainly used to configure and view the system information of the switch. It provides controls over the type of the access users and the access security.

1.2 Supported Features

System Info

The System Info is mainly used for the basic properties configuration. You can view the switch's port status and system information, and configure the device description, system time, and daylight saving time.

User management

User Management function is used to configure the user name and password for users to log into the switch with a certain access level so as to protect the settings of the switch from being randomly changed.

System Tools

The System Tools are used to manage the configuration file of the switch. With these tools, you can configure the boot file of the switch, backup and restore the configurations of the switch, update the firmware, reset the switch, and reboot the switch.

Boot Config function is used to configure the boot file of the switch uploaded before, and the switch will boot up according to your configuration file.

Auto Install function is used to download the configuration file and backup image for switch automatically.

Reboot Schedule function is used to set a schedule for the switch to reboot.

Access Security

Access Security provides different security measures for accessing the switch remotely so as to enhance the configuration management security.

Access Control function is used to control the users' access to the switch by filtering IP address, MAC address or port.

HTTP Config function is based on the HTTP protocol. It can allow or deny users to access the switch via a web browser.

HTTPS Config function is based on the SSL or TLS protocol working in transport layer. It supports a security access via a web browser.

SSH Config function is based on the SSH protocol, a security protocol established on application and transport layers. The function with SSH is similar to a telnet connection, but SSH can provide information security and powerful authentication.

SDM Template

The switch SDM (Switch Database Management) templates prioritize system resources to optimize support for certain features. **SDM Template** function provides three templates for users to allocate hardware resources for different usage.

2 System Info Configurations

With system information configurations, you can:

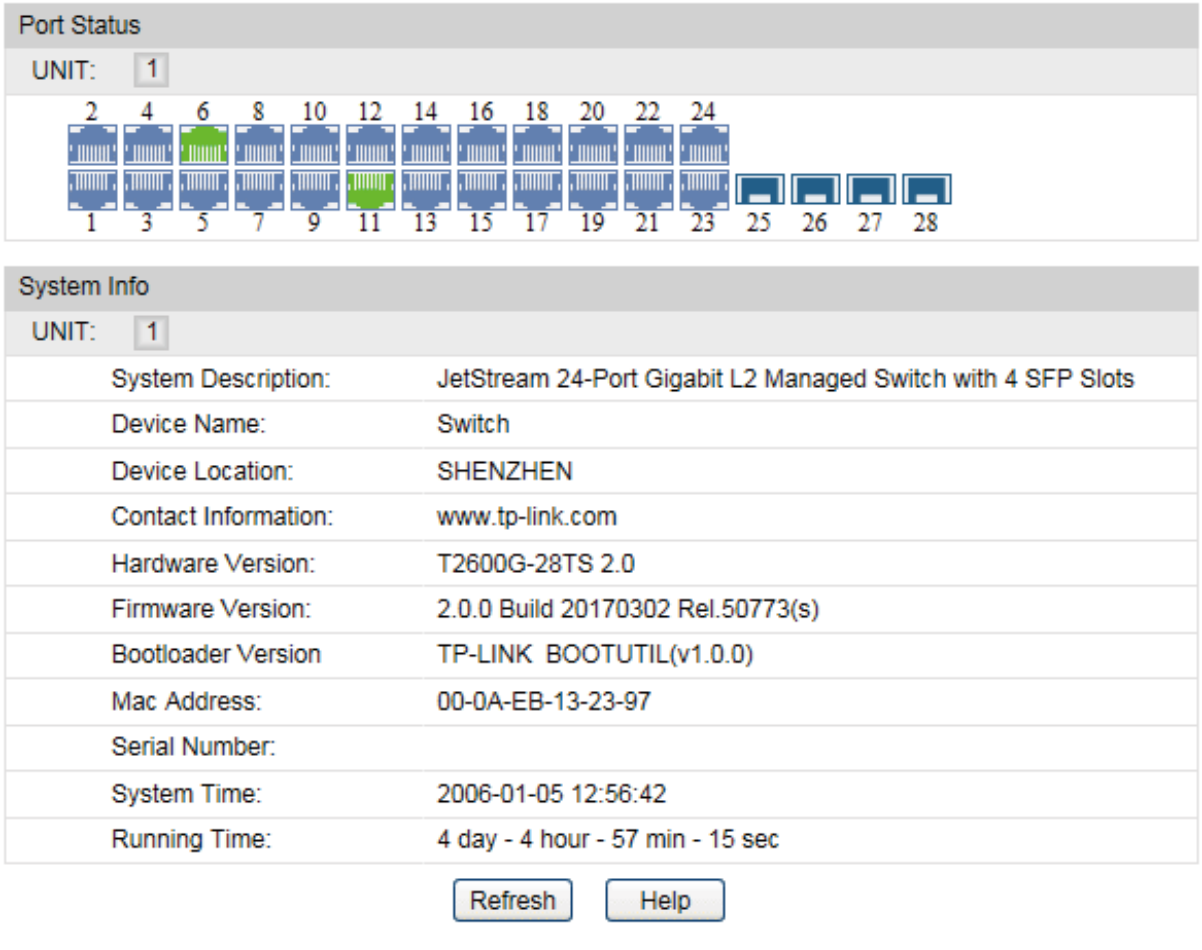
- View the system summary
- Specify the device description
- Set the system time
- Set the daylight saving time
- Specify the Serial Port Parameter

2.1 Using the GUI

2.1.1 Viewing the System Summary

Choose the menu **System** > **System Info** > **System Summary** to load the following page.

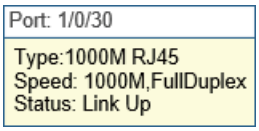
Figure 2-1 Viewing the System Summary



Port Status	Indication
	Indicates that the corresponding 1000Mbps port is not connected to a device.
	Indicates that the corresponding 1000Mbps port is at the speed of 1000Mbps.
	Indicates that the corresponding 1000Mbps port is at the speed of 10Mbps or 100Mbps.
	Indicates that the corresponding SFP port is not connected to a device.
	Indicates the SFP port is at the speed of 1000Mbps.

Move the cursor to the port to view the detailed information of the port.

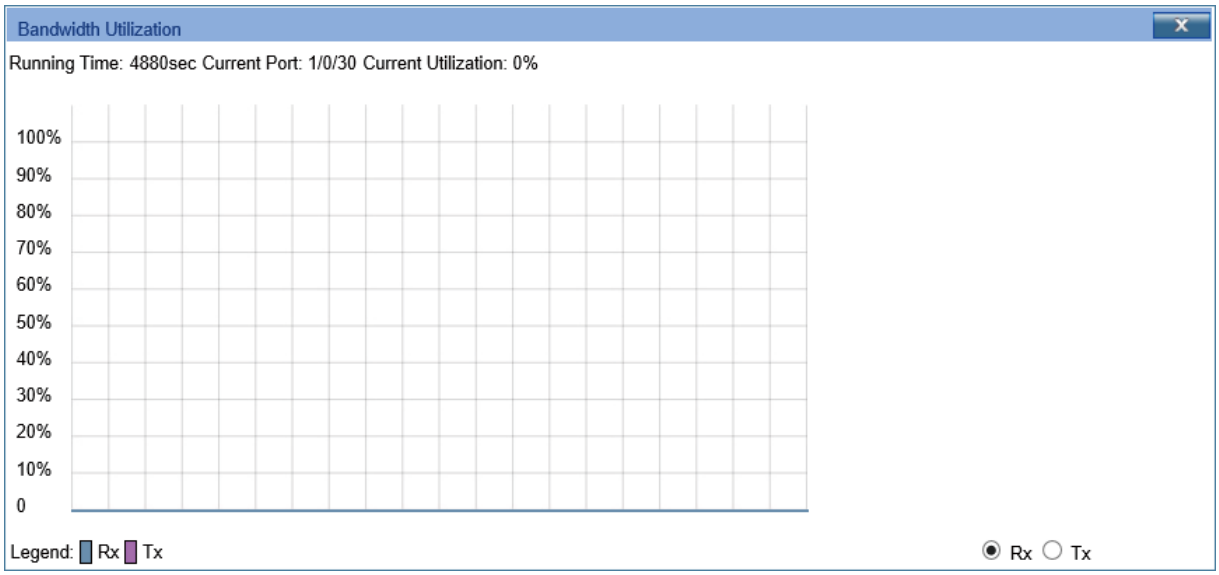
Figure 2-2 Port Information



Port Information	Indication
Port	Displays the port number of the switch.
Type	Displays the type of the port.
Speed	Displays the maximum transmission rate of the port.
Status	Displays the connection status of the port.

Click a port to view the bandwidth utilization on this port.

Figure 2-3 Bnadwidth Utilization

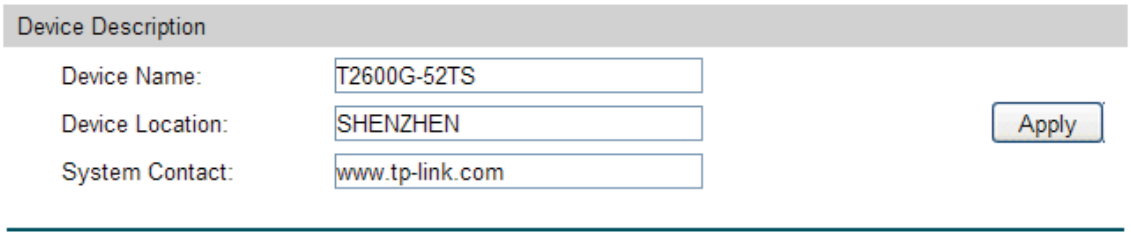


Rx	Select **Rx** to view the bandwidth utilization of receiving packets on this port.
Tx	Select **Tx** to view the bandwidth utilization of sending packets on this port.

2.1.2 Specifying the Device Description

Choose the menu **System** > **System Info** > **Device Description** to load the following page.

Figure 2-4 Specifying the Device Description



1) In the **Device Description** section, specify the following information.

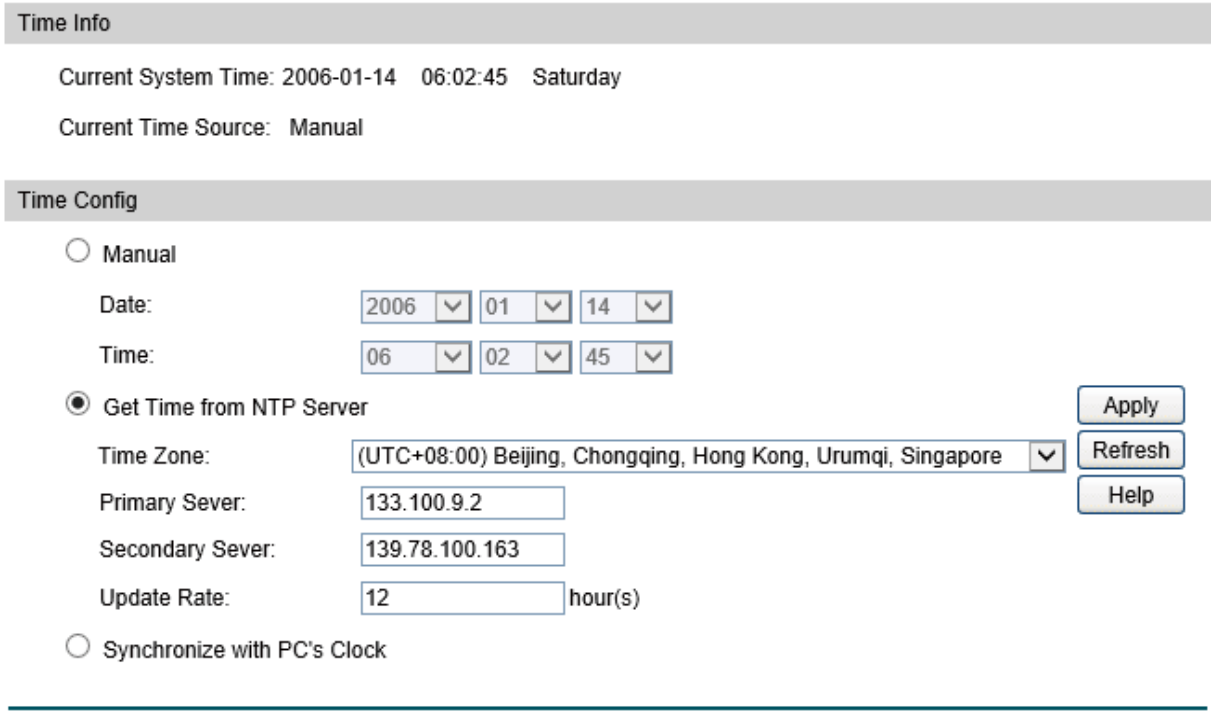
Device Name	Enter the name of the switch.
Device Location	Enter the location of the switch.
System Contact	Enter the contact information.

2) Click **Apply**.

2.1.3 Setting the System Time

Choose the menu **System** > **System Info** > **System Time** to load the following page.

Figure 2-5 Setting the System Time



In the **Time Info** section, view the current time information of the switch.

Current System Time	Displays the current date and time of the switch.
Current Time Source	Displays the current time source of the switch.

In the **Time Config** section, follow these steps to configure the system time:

1) Choose one method to set the system time and specify the information.

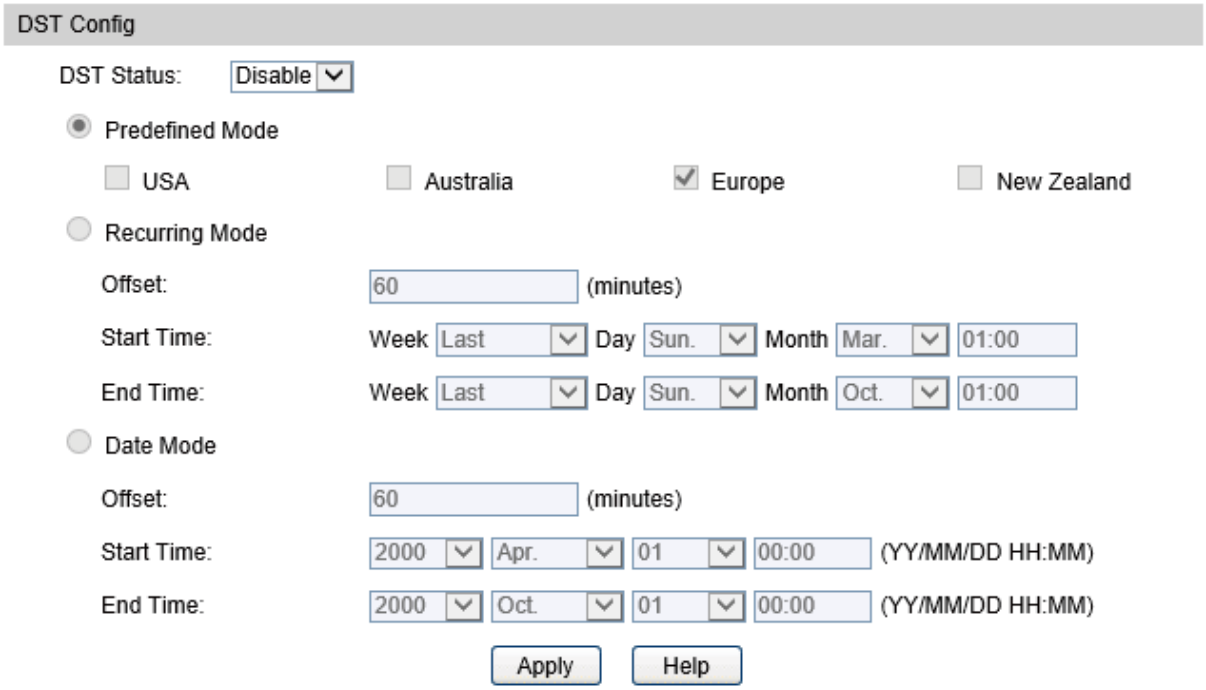
Manual	Set the system time manually. **Date**: Specify the date of the system. **Time**: Specify the time of the system.
Get Time from NTP Server	Set the system time by getting time from NTP server. Make sure the NTP server is accessible on your network. If the NTP server is on the Internet, connect the switch to the Internet first. **Time Zone**: Select your local time zone. **Primary Server**: Enter the IP Address of the primary NTP server. **Secondary Server**: Enter the IP Address of the secondary NTP server. **Update Rate**: Specify the interval the switch fetching time from NTP server, which ranges from 1 to 24 hours. The default value is 12 hours.
Synchronize with PC's Clock	Synchronize the system time of the switch with PC's clock.

2) Click **Apply**.

2.1.4 Setting the Daylight Saving Time

Choose the menu **System** > **System Info** > **Daylight Saving Time** to load the following page.

Figure 2-6 Setting the Daylight Saving Time



Follow these steps to configure Daylight Saving Time:

1) In the **DST Config** section, select **Enable** to enable the Daylight Saving Time function.
2) Choose one method to set the Daylight Saving Time of the switch and specify the information.

Predefined Mode	If you select **Predefined Mode**, choose a predefined DST schedule for the switch. **USA**: Select the Daylight Saving Time of the USA. It is from 2: 00 a.m. on the Second Sunday in March to 2:00 a.m. on the First Sunday in November. **Australia**: Select the Daylight Saving Time of Australia. It is from 2:00 a.m. on the First Sunday in October to 3:00 a.m. on the First Sunday in April. **Europe**: Select the Daylight Saving Time of Europe. It is from 1: 00 a.m. on the Last Sunday in March to 1:00 a.m. on the Last Sunday in October. **New Zealand**: Select the Daylight Saving Time of New Zealand. It is from 2: 00 a.m. on the Last Sunday in September to 3:00 a.m. on the First Sunday in April.

Recurring Mode	If you select **Recurring Mode**, specify a cycle time range for the Daylight Saving Time of the switch. This configuration will be used every year. **Offset**: Specify the time to set the clock forward by. **Start Time**: Specify the start time of Daylight Saving Time. The interval between start time and end time should be more than 1 day and less than 1 year(365 days). **End Time**: Specify the end time of Daylight Saving Time. The interval between start time and end time should be more than 1 day and less than 1 year (365 days).
Date Mode	If you select **Date Mode**, specify an absolute time range for the Daylight Saving Time of the switch. This configuration will be used only one time. **Offset**: Specify the time to set the clock forward by. **Start Time**: Specify the start time of Daylight Saving Time. The interval between start time and end time should be more than 1 day and less than 1 year(365 days). **End Time**: Specify the end time of Daylight Saving Time. The interval between start time and end time should be more than 1 day and less than 1 year (365 days).

3) Click **Apply**.

2.1.5 Specifying the Serial Port Parameter

Choose the menu **System** > **System Info** > **Serial Port Setting** to load the following page.

Figure 2-7 Specifying the Serial Port Parameter



In the **Serial Port Settings** section, specify the **Baud Rate** and click **Apply**.

Baud Rate	Configure the baud rate of the console connection. The default value is 38400 bps.
Date Bits	Displays the data bits.
Parity Bits	Displays the parity bits.
Stop Bits	Displays the stop bits.

2.2 Using the CLI

2.2.1 Viewing the System Summary

On privileged EXEC mode or any other configuration mode, you can use the following command to view the system information of the switch:

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

View status of the interface.

port: Enter the number of the Ethernet port.

show system-info

View the system information including system Description, Device Name, Device Location, System Contact, Hardware Version, Firmware Version, System Time, Run Time and so on.

The following example shows how to view the interface status and the system information of the switch.

Switch#show interface status

Port	Status	Speed	Duplex	FlowCtrl	Jumbo	Active-Medium
Gi1/0/1	LinkDown	N/A	N/A	N/A	Disable	Copper
Gi1/0/2	LinkDown	N/A	N/A	N/A	Disable	Copper
Gi1/0/3	LinkUp	1000M	Full	Disable	Disable	Copper
...						
Gi1/0/50	LinkDown	N/A	N/A	N/A	Disable	Fiber
Gi1/0/51	LinkDown	N/A	N/A	N/A	Disable	Fiber
Gi1/0/52	LinkDown	N/A	N/A	N/A	Disable	Fiber

Switch#show system-info

System Description - JetStream 48-Port Gigabit L2 Managed Switch with 4 SFP Slots

System Name - T2600G-28TS

System Location - SHENZHEN

Contact Information - www.tp-link.com

Hardware Version - T2600G-28TS 2.0

Software Version - 2.0.0 Build 20160923 Rel.39814(s)

System Time - 2006-01-03 12:54:41

Serial Number -

Running Time - 2 day - 4 hour - 55 min - 36 sec

2.2.2 Specifying the Device Description

Follow these steps to specify the device description:

Step 1	**configure** Enter global configuration mode.
Step 2	**hostname [** *hostname* **]** Specify the system name of the switch. *hostname*: Enter the system name. The length of the name ranges from 1 to 32 characters. By default, it is the model name of the switch.
Step 3	**location [** *location* **]** Specify the system location of the switch. *location*: Enter the device location. It should consist of no more than 32 characters. By default, it is "SHENZHEN".
Step 4	**contact-info [** *contact-info* **]** Specify the system contact Information. *contact-info*: Enter the contact information. It should consist of no more than 32 characters. By default, it is "www.tp-link.com".
Step 5	**show system-info** Verify the system information including system Description, Device Name, Device Location, System Contact, Hardware Version, Firmware Version, System Time, Run Time and so on.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set the device name as Switch_A, set the location as BEIJING and set the contact information as https://www.tp-link.com.

Switch#configure

Switch(config)#hostname Switch_A

Switch(config)#location BEIJING

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

Switch(config)#show system-info

System Description - JetStream 48-Port Gigabit Smart Switch with 4 SFP Slots

System Name - Switch_A

System Location - BEIJING

Contact Information - https://www.tp-link.com

...

Switch(config)#end

Switch#copy running-config startup-config

2.2.3 Setting the System Time

Follow these steps and choose one method to set the system time:

Step 1	**configure** Enter global configuration mode.
Step 2	Use the following command to set the system time manually: **system-time manual** *time* Configure the system time manually. *time*: Specify the date and time manually in the format of MM/DD/YYYY-HH:MM:SS. The valid value of the year ranges from 2000 to 2037. Use the following command to set the system time by getting time from the NTP server: **system-time ntp { *timezone* } { *ntp-server* } { *backup-ntp-server* } { *fetching-rate* }** Configure the time zone and the NTP server to get time from the NTP server. Ensure the NTP server is accessible. If the NTP server is on the Internet, connect the switch to the Internet first. *timezone*: Enter your local time-zone, which ranges from UTC-12:00 to UTC+13:00.

The detailed information of each time-zone are displayed as follows:

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: Specify the IP address of the primary NTP server.

backup-ntp-server: Specify the IP address of the backup NTP server.

fetching-rate: Specify the interval fetching time from the NTP server.

Step 3	Use the following command to verify the system time information. **show system-time** Verify the system time information. Use the following command to verify the NTP mode configuration information. **show system-time ntp** Verify the system time information of NTP mode.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set the system time by Get Time from NTP Server and set the time zone as UTC+08:00, set the NTP server as 133.100.9.2, set the backup NTP server as 139.78.100.163 and set the update rate as 11.

Switch#configure

Switch(config)#system-time ntp UTC+08:00 133.100.9.2 139.78.100.163 11

Switch(config)#show system-time ntp

Time zone : UTC+08:00

Prefered NTP server: 133.100.9.2

Backup NTP server: 139.78.100.163

Last successful NTP server: 133.100.9.2

Update Rate: 11 hour(s)

Switch(config)#end

Switch#copy running-config startup-config

2.2.4 Setting the Daylight Saving Time

Follow these steps and choose one method to set the Daylight Saving Time:

Step 1	**configure** Enter global configuration mode.

Step 2 Use the following command to select a predefined Daylight Saving Time configuration:

system-time dst predefined [USA | Australia | Europe | New-Zealand **]**

Specify the Daylight Saving Time using a predefined schedule.

USA | Australia | Europe | New-Zealand: Select one mode of Daylight Saving Time.

USA: 02:00 a.m. on the Second Sunday in March ~ 02:00 a.m. on the First Sunday in November.

Australia: 02:00 a.m. on the First Sunday in October ~ 03:00 a.m. on the First Sunday in April.

Europe: 01:00 a.m. on the Last Sunday in March ~ 01:00 a.m. on the Last Sunday in October.

New Zealand: 02:00 a.m. on the Last Sunday in September ~ 03:00 a.m. on the First Sunday in April.

Use the following command to set the Daylight Saving Time in recurring mode:

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

Specify the Daylight Saving Time in Recuring mode.

sweek: Enter the start week of Daylight Saving Time. There are 5 values showing as follows: first, second, third, fourth, last.

sday: Enter the start day of Daylight Saving Time. There are 7 values showing as follows: Sun, Mon, Tue, Wed, Thu, Fri, Sat.

smonth: Enter the start month of Daylight Saving Time. There are 12 values showing as follows: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.

stime: Enter the start time of Daylight Saving Time,in the format of HH:MM.

eweek: Enter the end week of Daylight Saving Time. There are 5 values showing as follows: first, second, third, fourth, last.

eday: Enter the end day of Daylight Saving Time. There are 7 values showing as follows: Sun, Mon, Tue, Wed, Thu, Fri, Sat.

emonth: Enter the end month of Daylight Saving Time. There are 12 values showing as follows: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.

etime: Enter the end time of Daylight Saving Time,in the format of HH:MM.

offset: Enter the offset of Daylight Saving Time. The default value is 60.

Use the following command to set the Daylight Saving Time in date mode:

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

Specify the Daylight Saving Time in Date mode.

	smonth: Enter the start month of Daylight Saving Time. There are 12 values showing as follows: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. *sday*: Enter the start day of Daylight Saving Time, which ranges from 1 to 31. *stime*: Enter the start time of Daylight Saving Time,in the format of HH:MM. *syear*: Enter the start year of Daylight Saving Time. *emonth*: Enter the end month of Daylight Saving Time. There are 12 values showing as follows: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. *eday*: Enter the end day of Daylight Saving Time, which ranges from 1 to 31. *etime*: Enter the end time of Daylight Saving Time,in the format of HH:MM. *eyear*: Enter the end year of Daylight Saving Time. *offset*: Enter the offset of Daylight Saving Time. The default value is 60.
Step 3	**show system-time dst** Verify the DST information of the switch.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set the Daylight Saving Time by Date Mode. Set the start time as 01:00 August 1st, 2016, set the end time as 01:00 September 1st,2016 and set the offset as 50.

Switch#configure

Switch(config)#system-time dst date Aug 1 01:00 2016 Sep 1 01:00 2016 50

Switch(config)#show system-time dst

DST starts at 01:00:00 on Aug 1 2016

DST ends at 01:00:00 on Sep 1 2016

DST offset is 50 minutes

DST configuration is one-off

Switch(config)#end

Switch#copy running-config startup-config

2.2.5 Specifying the Serial Port Parameter

Follow These steps to specify the serial port parameter.

Step 1	**configure** Enter global configuration mode.

Step 2	**serial_port baud_rate {** 9600 | 19200 | 38400 | 57600 | 115200 **}** Specify the baud rate of the console connection. 9600 | 19200 | 38400 | 57600 | 115200: Specify the communication baud rate on the console port. The default value is 38400 bps.
Step 3	**end** Return to privileged EXEC mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set the baud rate as 9600 and view the serial port parameters.

Switch#config

Switch(config)#serial_port baud_rate 9600

Switch(config)#show serial_port

Serial Port Settings

Baud rate: 9600

Data Bits: 8

Parity Bits: None

Stop Bits: 1

Switch(config)#end

Switch#copy running-config startup-config

3 User Management Configurations

With user management configurations, you can:

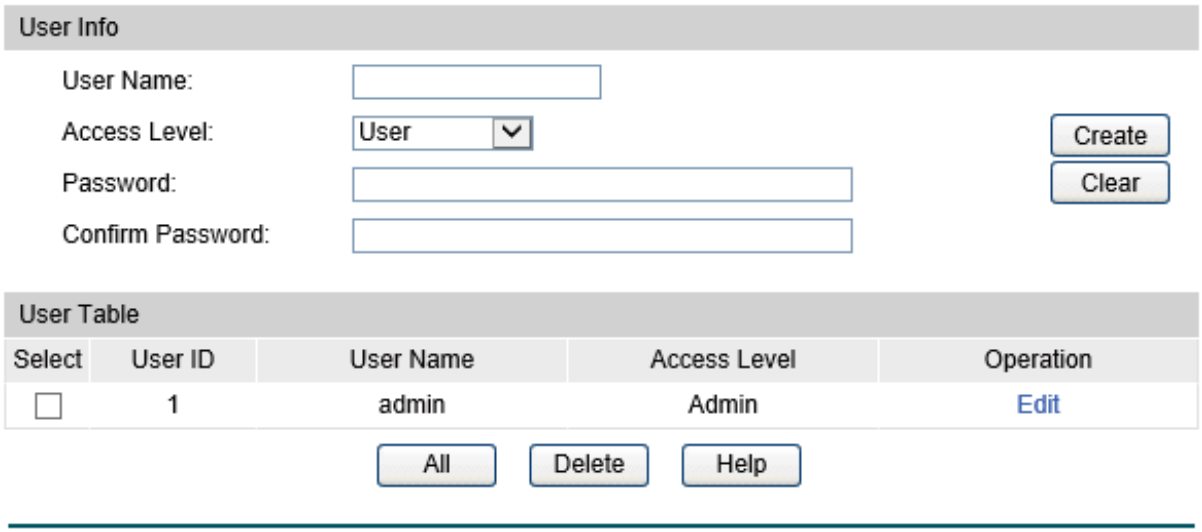
- Create Admin accounts
- Create accounts of other types

3.1 Using the GUI

3.1.1 Creating Admin Accounts

Choose the menu **System** > **User Management** > **User Config** to load the following page.

Figure 3-1 Create Admin Accounts



Follow these steps to create an Admin account:

1) In the **User Info** section, select Admin from the drop-down list and specify the user name and password.

User Name	Create a user name for users' login. It contains 16 characters at most, composed of digits, English letters and underscore only.

Access Level	Select the access level as **Admin**. **Admin**: Admin can edit, modify and view all the settings of different functions. **Operator**: Operator can edit, modify and view most of the settings of different functions. **Power User**: Power User can edit, modify and view some of the settings of different functions. **User**: User can only view the settings without the right to edit or modify.
Password	Type a password for users' login. It is a string from 1 to 31 alphanumeric characters or symbols. You can use digits, English letters (case sensitive), underscore and sixteen special characters.
Confirm Password	Retype the password.

2) Click **Create**.

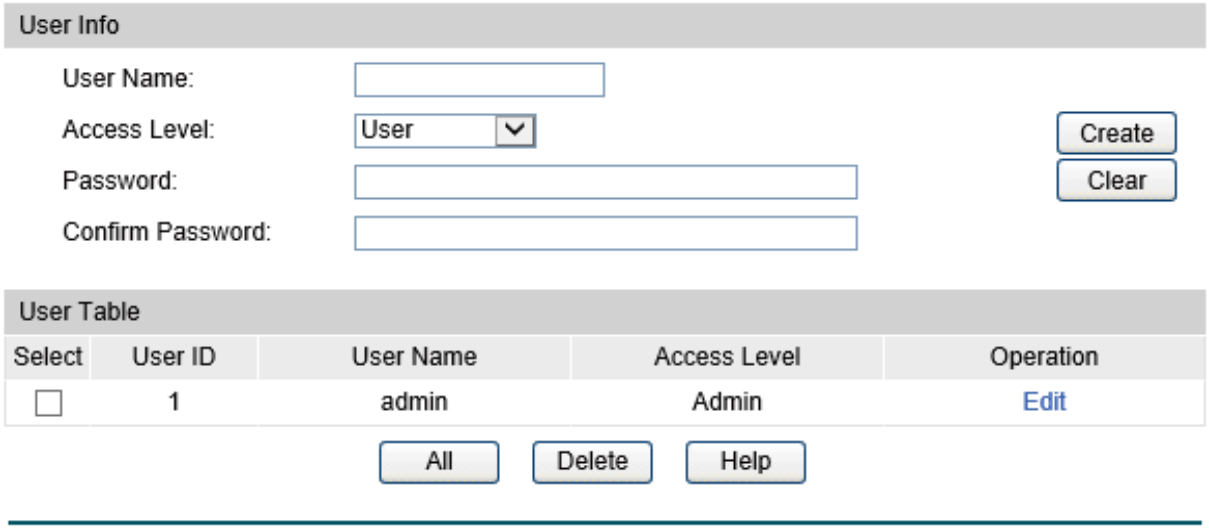
3.1.2 Creating Accounts of Other Types

You can create accounts with the access level of Operator,Power User and User here. You also need to go to the **AAA** section to create an Enable Password for these accounts. The Enable Password is used to change the users' access level to Admin.

- Creating an Account

Choose the menu **System** > **User Management** > **User Config** to load the following page.

Figure 3-2 Create Accounts of Other Types



Follow these steps to create an account of other types:

1) In the **User Info** section, select the access level from the drop-down list and specify the user name and password.

User Name	Create a user name for users' login. It contains 16 characters at most, composed of digits, English letters and under dashes only.
Access Level	Select the access level as **Operator**, **Power User** or **User**. **Admin**: Admin can edit, modify and view all the settings of different functions. **Operater**: Operator can edit, modify and view most of the settings of different functions. **Power User**: Power User can edit, modify and view some of the settings of different functions. **User**: User can only view the settings without the right to edit or modify.
Password	Type a password for users' login. It is a string from 1 to 31 alphanumeric characters or symbols. You can use digits, English letters (case sensitive), underscore and sixteen special characters.
Confirm Password	Retype the password.

2) Click **Create**.

Configuring Enable Password

Choose the menu **Network Security** > **AAA** > **Global Config** to load the following page.

Figure 3-3 Configure the AAA Function



1) Select **Enable** and Click **Apply** to enable the **AAA** function.
2) Specify the Enable Password and Click **Apply**.

Tips:

- The **AAA** function applies another method to manage the access users' name and password. For details, refer to *AAA Configuration* in *Configuring Network Security*.
- The logged-in users can enter the Enable Password on this page to get the administrative privileges.

3.2 Using the CLI

3.2.1 Creating Admin Accounts

Follow these steps to create an Admin account:

Step 1	**configure** Enter global configuration mode.
Step 2	Use the following command to create an account unencrypted or symmetric encrypted. **user name** *name* **{ privilege** admin **} password {** [0] *password* **|** 7 *encrypted-password* **}** Create an account whose access level is Admin. *name*: Enter a user name for users' login. It contains 16 characters at most, composed of digits, English letters and underscore only. admin: Select the access level for the user. Admin can edit, modify and view all the settings of different functions. 0: Specify the encryption type. 0 indicates that the password you entered is unencrypted, and the password is saved to the configuration file unencrypted. By default, the encryption type is 0. *password*: Enter a password for users' login. It is a string from 1 to 31 alphanumeric characters or symbols. The password is case sensitive, allows digits, English letters (case sensitive), underlines and sixteen special characters. 7: Specify the encryption type. 7 indicates that the password you entered is symmetric encrypted, and the password is saved to the configuration file symmetric encrypted. *encrypted-password*: Enter a symmetric encrypted password with fixed length, which you can copy from another switch's configuration file. After the encrypted password is configured, you should use the corresponding unencrypted password to reenter this mode. Use the following command to create an account MD5 encrypted. **user name** *name* **{ privilege** admin **} secret {** [0] *password* **|** 5 *encrypted-password* **}** Create an account whose access level is Admin. *name*: Enter a user name for users' login. It contains 16 characters at most, composed of digits, English letters and underscore only. admin: Select the access level for the user. Admin can edit, modify and view all the settings of different functions. 0: Specify the encryption type. 0 indicates that the password you entered is unencrypted, but the password is saved to the configuration file MD5 encrypted. By default, the encryption type is 0. *password*: Enter a password for users' login. It is a string from 1 to 31 alphanumeric characters or symbols. The password is case sensitive, allows digits, English letters (case sensitive), underlines and sixteen special characters. 5: Specify the encryption type. 5 indicates that the password you entered is MD5 encrypted, and the password is saved to the configuration file MD5 encrypted. *encrypted-password*: Enter a MD5 encrypted password with fixed length, which you can copy from another switch's configuration file.

Step 3	**show user account-list** Verify the information of the current users.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

3.2.2 Creating Accounts of Other Types

You can create accounts with the access level of Operator, Power user and User here. You also need to go to the **AAA** section to create an Enable Password for these accounts. The Enable Password is used to change the users' access level to Admin.

Follow these steps to create an account of other type:

Step 1	**configure** Enter global configuration mode.

Step 2 Use the following command to create an account unencrypted or symmetric encrypted.

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

Create an account whose access level is Operator, Power User or User.

name: Enter a user name for users' login. It contains 16 characters at most, composed of digits, English letters and underscore only.

operator | power_user | user: Select the access level for the user. Operator can edit, modify and view mostly the settings of different functions. Power User can edit, modify and view some the settings of different functions. User only can view the settings without the right to edit and modify.

0: Specify the encryption type. 0 indicates that the password you entered is unencrypted, and the password is saved to the configuration file unencrypted. By default, the encryption type is 0.

password: Enter a password for users' login. It is a string from 1 to 31 alphanumeric characters or symbols. The password is case sensitive, allows digits, English letters (case sensitive), underlines and sixteen special characters.

7: Specify the encryption type. 7 indicates that the password you entered is symmetric encrypted, and the password is saved to the configuration file symmetric encrypted.

encrypted-password: Enter a symmetric encrypted password with fixed length, which you can copy from another switch's configuration file. After the encrypted password is configured, you should use the corresponding unencrypted password to reenter this mode.

Use the following command to create an account MD5 encrypted.

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

Create an account whose access level is Operator, Power User or User.

name: Enter a user name for users' login. It contains 16 characters at most, composed of digits, English letters and underscore only.

operator | power_user | user: Select the access level for the user. Operator can edit, modify and view mostly the settings of different functions. Power User can edit, modify and view some the settings of different functions. User only can view the settings without the right to edit and modify.

0: Specify the encryption type. 0 indicates that the password you entered is unencrypted, but the password is saved to the configuration file MD5 encrypted. By default, the encryption type is 0.

password: Enter a password for users' login. It is a string from 1 to 31 alphanumeric characters or symbols. The password is case sensitive, allows digits, English letters (case sensitive), underlines and sixteen special characters.

5: Specify the encryption type. 5 indicates that the password you entered is MD5 encrypted, and the password is saved to the configuration file MD5 encrypted.

encrypted-password: Enter a MD5 encrypted password with fixed length, which you can copy from another switch's configuration file. After the encrypted password is configured, you should use the corresponding unencrypted password to reenter this mode.

Step 3 **aaa enable**

Globally enable the AAA function.

Step 4	Use the following command to create an enable password unencrypted or symmetric encrypted. **enable admin password { [** 0 **]** *password* | 7 *encrypted-password* **}** Create an Enable Password. It can change the users' access level to Admin. By default, it is empty. 0: Specify the encryption type. 0 indicates that the password you entered is unencrypted, and the password is saved to the configuration file unencrypted. By default, the encryption type is 0. *password*: Enter an enable password. It is a string from 1 to 31 alphanumeric characters or symbols. The password is case sensitive, allows digits, English letters (case sensitive), underlines and sixteen special characters. 7: Specify the encryption type. 7 indicates that the password you entered is symmetric encrypted, and the password is saved to the configuration file symmetric encrypted. *encrypted-password*: Enter a symmetric encrypted password with fixed length, which you can copy from another switch's configuration file. After the encrypted password is configured, you should use the corresponding unencrypted password to reenter this mode. Use the following command to create an enable password unencrypted or MD5 encrypted. **enable admin secret { [** 0 **]** *password* | 5 *encrypted-password* **}** Create an Enable Password. It can change the users' access level to Admin. By default, it is empty. 0: Specify the encryption type. 0 indicates that the password you entered is unencrypted, but the password is saved to the configuration file MD5 encrypted. By default, the encryption type is 0. *password*: Enter an enable password. It is a string from 1 to 31 alphanumeric characters or symbols. The password is case sensitive, allows digits, English letters (case sensitive), underlines and sixteen special characters. 5: Specify the encryption type. 5 indicates that the password you entered is MD5 encrypted, and the password is saved to the configuration file MD5 encrypted. *encrypted-password*: Enter a MD5 encrypted password with fixed length, which you can copy from another switch's configuration file. After the encrypted password is configured, you should use the corresponding unencrypted password to reenter this mode.
Step 5	**show user account-list** Verify the information of the current users.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

Tips:

- The **AAA** function applies another method to manage the access users' name and password. For details, refer to *AAA Configuration* in *Configuring Network Security* .
- The logged-in users can enter the Enable Password on this page to get the administrative privileges.

The following example shows how to create a uesr with the access level of Operator, set the user name as user1 and set the password as 123. Enable AAA function and set the enable password as abc123.

Switch#configure

Switch(config)#user name user1 **privilege** operator **password** 123

Switch(config)#aaa enable

Switch(config)#enable admin password abc123

Switch(config)#show user account-list

Index	User-Name	User-Type
1	user1	Operator
2	admin	Admin

Switch(config)#end

Switch#copy running-config startup-config

4 System Tools Configurations

With system tools configurations, you can:

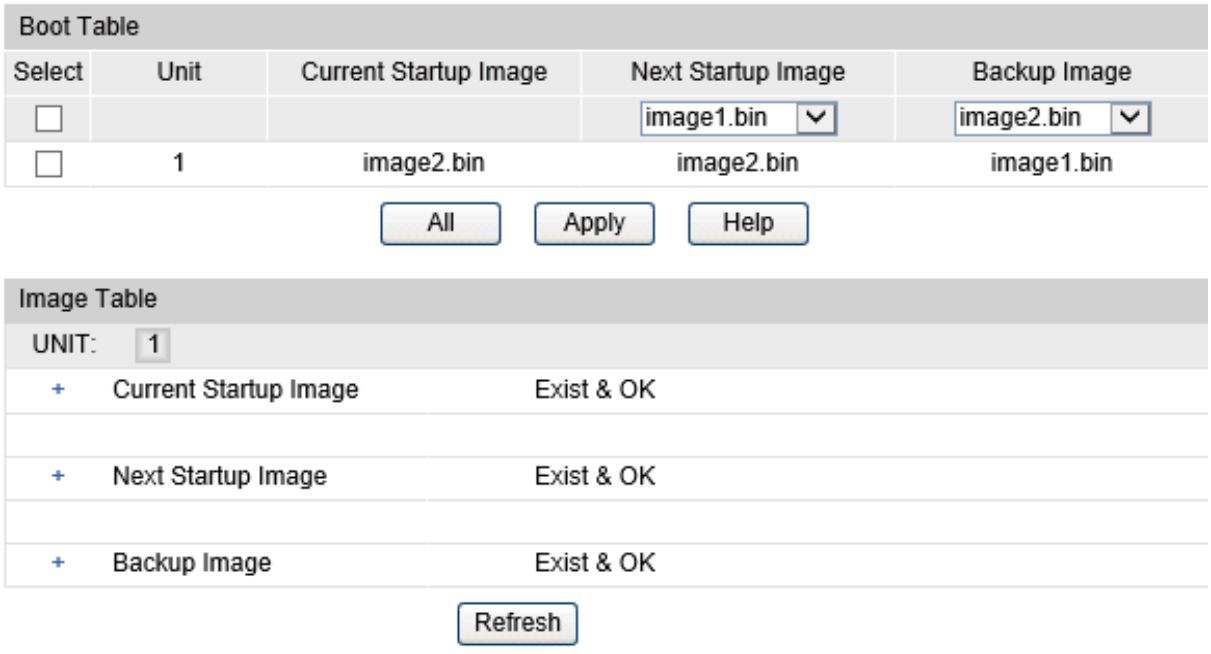
- Configure the boot file
- Restore the configuration of the switch
- Back up the configuration file
- Upgrade the firmware
- Configure the Auto Install Function
- Reboot the switch
- Configure the reboot schedule
- Reset the switch

4.1 Using the GUI

4.1.1 Configuring the Boot File

Choose the menu **System** > **System Tools** > **Boot Config** to load the following page.

Figure 4-1 Configuring the Boot File



Follow these steps to configure the boot file:

1) In the **Boot Table** section, select one or more units and configure the relevant parameters.

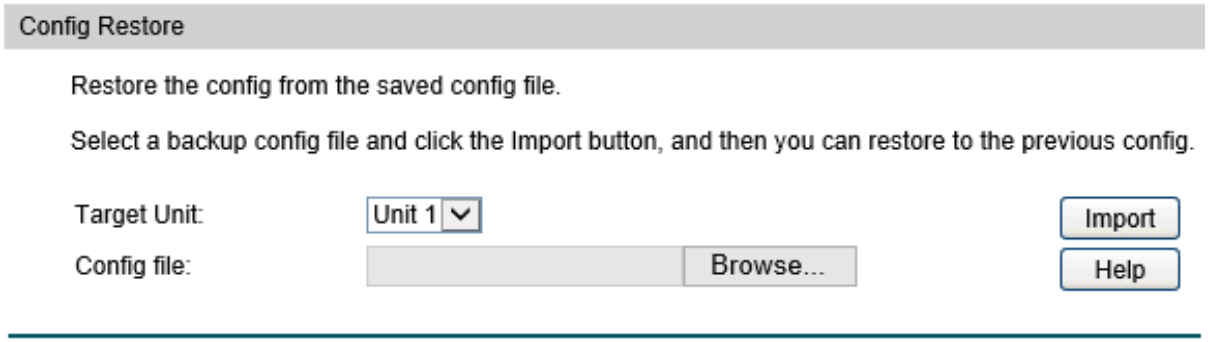
Select	Select one or more units to be configured.
Unit	Displays the number of the unit.
Current Startup Image	Displays the current startup image.
Next Startup Image	Select the next startup image. When the switch is powered on, it will try to start up with the next startup image. The next startup and backup image should not be the same.
Backup Image	Select the backup image. When the switch fails to start up with the next startup image, it will try to start up with the backup image. The next startup and backup image should not be the same.

2) Click **Apply**.

4.1.2 Restoring the Configuration of the Switch

Choose the menu **System** > **System Tools** > **Config Restore** to load the following page.

Figure 4-2 Restoring the Configuration of the Switch



Follow these steps to restore the configuration of the switch:

1) In the **Config Restore** section, select one unit and one configuration file.

Target Unit	Select a member switch to import configuration file. .
Config file	Select the desired configuration file to import.

2) Click **Import** to import the configuration file.

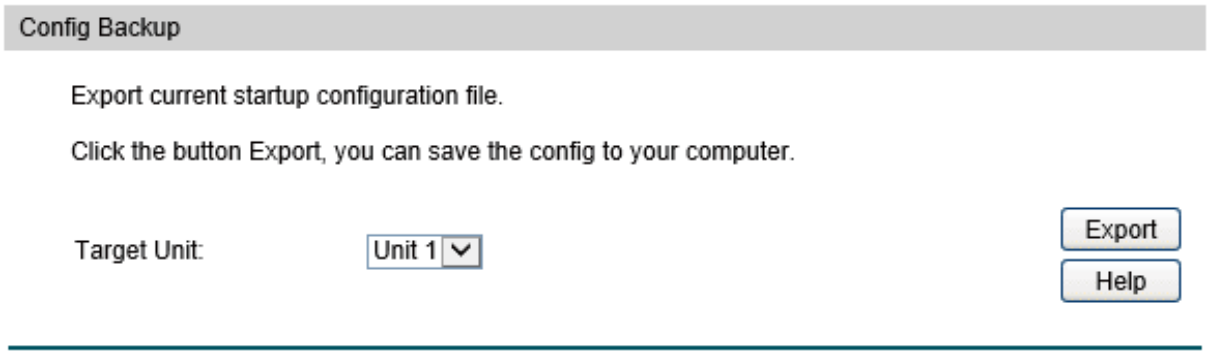
Note:

- It will take a long time to restore the configuration. Please wait without any operation.
- After the configuration is restored successfully, the device will reboot to make the configuration change effective.

4.1.3 Backing up the Configuration File

Choose the menu **System** > **System Tools** > **Config Backup** to load the following page.

Figure 4-3 Backing up the Configuration File

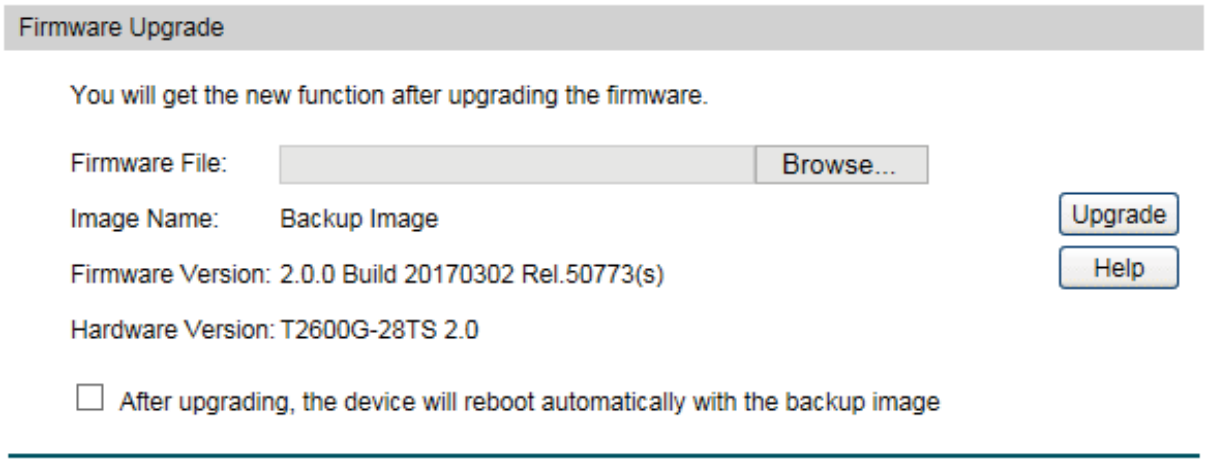


In the **Config Backup** section, select one unit and click **Export** to export the configuration file.

4.1.4 Upgrading the Firmware

Choose the menu **System** > **System Tools** > **Firmware Upgrade** to load the following page.

Figure 4-4 Upgrading the Firmware



In the **Firmware Upgrade** section, select one file and click **Upgrade** to upgrade the system.

Firmware File	Select the desired firmware file to upgrade the system.
Image Name	Displays the image to upgrade. It means that the operation will only effect the backup image.
Firmware Version	Displays the current firmware version of the system.
Hardware Version	Displays the current hardware version of the system.

After upgrading, the device will reboot automatically with the backup image	Select this option to reboot automatically with the backup image after upgrading.

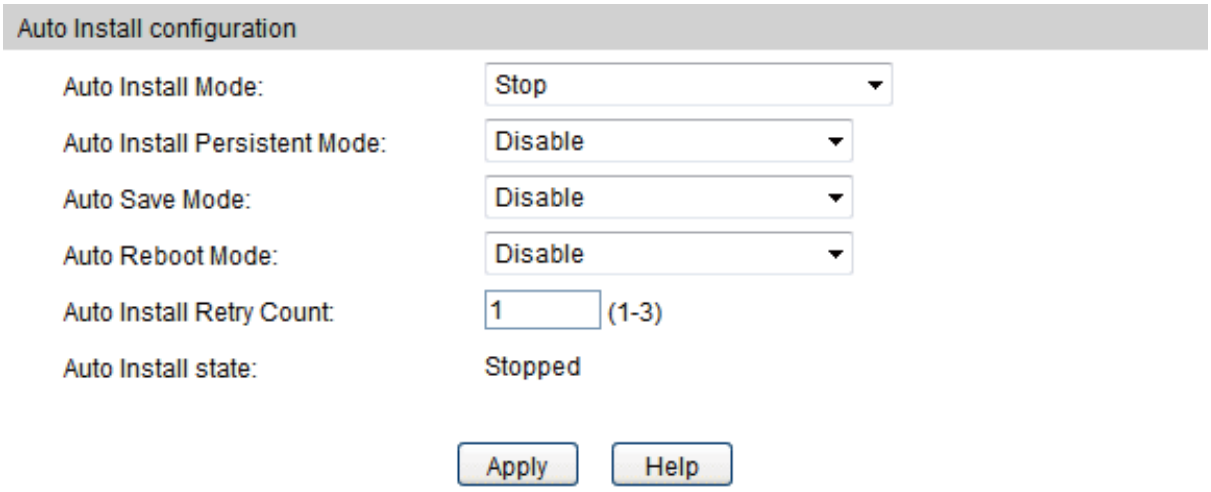
4.1.5 Configuring Auto Install Function

Note:

- You should configure the DHCP server and the TFTP server first before configuring the Auto Install function.

Choose the menu **System > System Tools > Auto Install** to load the following page.

Figure 4-5 Configuring the Auto Install Function



In the **Auto Install Configuration** section, specify the parameters and click **Apply**.

Auto Install Mode	Select **Start** to enable the Auto Install function and the switch will download the configuration file and the backup image automatically.
Auto Install Persistent Mode	Specify the Auto Install Persistent Mode. If you select Enable and save configuration, Auto Install will start during next reboot.
Auto Save Mode	Specify the Auto Save Mode. If you select Enable, the switch will save the configuration file downloaded as startup configuration file automatically.
Auto Reboot Mode	Specify the Auto Reboot Mode. If you select Enable, the switch will reboot automatically after the auto install process is completed successfully.
Auto Install Retry Count	Specify the Auto Install Retry Count. It ranges from 1 to 3.
Auto Install State	Display the state of the auto install function.

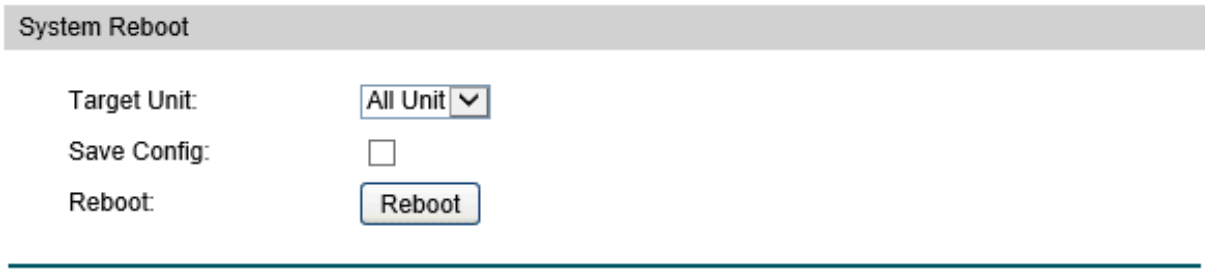
Note:

- The switch will obtain a new IP address from the DHCP server during the process of Auto Install. If you want to access to the switch, you should check the new IP address on the DHCP server.
- IF the Auto Install process is failed, the switch will restart the process every 10 minutes. You can stop the process manually.

4.1.6 Rebooting the switch

Choose the menu **System** > **System Tools** > **System Reboot** to load the following page.

Figure 4-6 Rebooting the switch



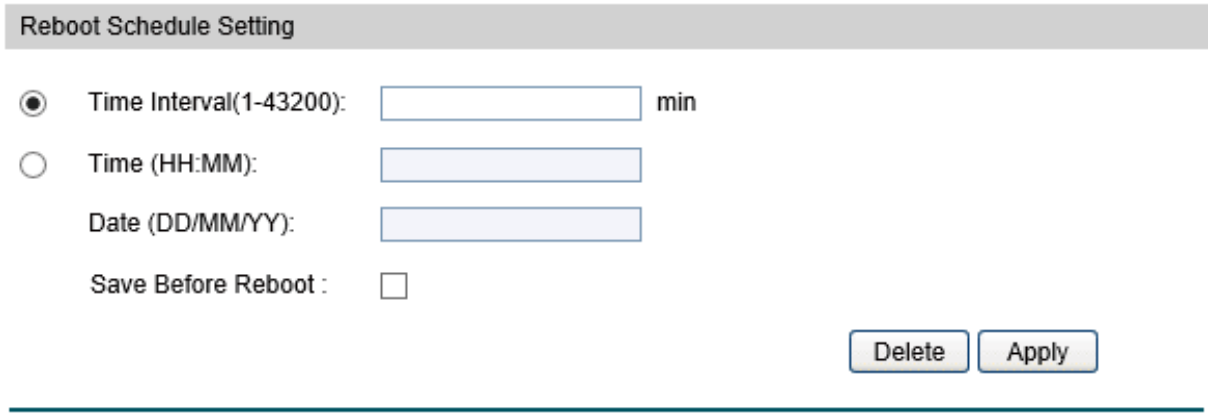
In the S**ystem Reboot** section, select the desired unit and click **Reboot**.

Target Unit	Select the desired unit to reboot. By default, it is ALL Unit.
Save Config	Select this option to save the configuration before the reboot.

4.1.7 Configuring the Reboot Schedule

Choose the menu **System** > **System Tools** > **Reboot Schedule** to load the following page.

Figure 4-7 Configuring the Reboot Schedule



Follow these steps to restore the configuration of the switch:

1) In the **Reboot Schedule Setting** section, select one method and specify the parameters.

Time Interval	Specify a period of time. The switch will reboot after this period. The valid values are from 1 to 43200 minutes. This reboot schedule recurs if users check the **Save Before Reboot**.
Time (HH:MM)/ Date (DD/MM/ YY)	Specify the date and time for the switch to reboot. **Time (HH:MM)**: Specify the time for the switch to reboot, in the format of HH:MM **Date (DD/MM/YY)**: 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	Select to save the switch's configurations before it reboots.

4.1.8 Reseting the Switch

Choose the menu **System** > **System Tools** > **System Reset** to load the following page.

Figure 4-8 Reseting the Switch



In the **System Reset** section, select the desired unit and click **Reset**.

Target Unit	Select the desired unit to reset. By default, it is ALL Unit.

Note:

After the system is reset, configurations of the switch will be reset to the default.

4.2 Using the CLI

4.2.1 Configuring the Boot File

Follow these steps to configure the boot file:

Step 1	**configure** Enter global configuration mode.

Step 2	**boot application filename {** image1 | image2 **} {** startup | backup **}** Specify the configuration of the boot file. By default, the image1.bin is the startup image and the image2.bin is the backup image. image1 | image2: Select the image file to be configured. startup | backup: Select the property of the image file.
Step 3	**show boot** Verify the boot configuration of the system.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set the next startup image as image 1 and set the backup image as image 2.

Switch#configure

Switch(config)#boot application filename image1 startup

Switch(config)#boot application filename image2 backup

Switch(config)#show boot

Boot config:

Current Startup Image - image1.bin

Next Startup Image - image1.bin

Backup Image - image2.bin

Switch(config)#end

Switch#copy running-config startup-config

4.2.2 Restoring the Configuration of the Switch

Follow these steps to restore the configuration of the switch:

Step 1	**enable** Enter privileged mode.
Step 2	**copy tftp startup-config ip-address** *ip-addr* **filename** *name* Download the configuration file to the switch from TFTP server. *ip-addr*: Specify the IP address of the TFTP server. Both IPv4 and IPv6 addresses are supported. *name*: Specify the name of the configuration file to be downloaded.

Note:

- It will take a long time to restore the configuration. Please wait without any operation.
- After the configuration is restored successfully, the device will reboot to make the configuration change effective.

The following example shows how to restore the configuration file named file1 from the TFTP server with IP address 192.168.0.100.

Switch>enable

Switch#copy tftp startup-config ip-address 192.168.0.100 **filename** file1

Start to load user config file...

Operation OK! Now rebooting system...

4.2.3 Backing up the Configuration File

Follow these steps to back up the current configuration of the switch in a file:

Step 1	**enable** Enter privileged mode.
Step 2	**copy startup-config tftp ip-address** *ip-addr* **filename** *name* Back up the configuration file to TFTP server. *ip-addr*: Specify the IP address of the TFTP server. Both IPv4 and IPv6 addresses are supported. *name*: Specify the name of the configuration file to be saved.

The following example shows how to backup the configuration file named file2 from TFTP server with IP address 192.168.0.100.

Switch>enable

Switch#copy startup-config tftp ip-address 192.168.0.100 **filename** file2

Start to backup user config file...

Backup user config file OK.

4.2.4 Upgrading the firmware

Follow these steps to upgrade the firmware:

Step 1	**enable** Enter privileged mode.

Step 2	**firmware upgrade ip-address** *ip-addr* **filename** *name* Upgrade the switch's backup image via TFTP server. To boot up with the new firmware, you need to choose to reboot the switch with the backup image. *ip-addr*: Specify the IP address of the TFTP server. Both IPv4 and IPv6 addresses are supported. *name*: Specify the name of the desired firmware file.
Step 3	Enter Y to continue then enter Y to reboot.

The following example shows how to upgrade the firmware using the configuration file named file3.bin. The TFTP server is 190.168.0.100.

Switch>enable

Switch#firmware upgrade ip-address 192.168.0.100 **filename** file3.bin

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

Operation OK!

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

4.2.5 Configuring Auto Install Function

Note:

- You should configure the DHCP server and the TFTP server first before configuring the Auto Install function.

Follow these steps to configure the Auto Install function.

Step 1	**configure** Enter global configuration mode.
Step 2	**boot autoinstall persistent-mode** Enable the auto install persistent mode. After saving configuration, the switch will start the Auto Install function automatically during next reboot process.
Step 3	**boot autoinstall auto-save** Enable the auto save mode and the switch will save the configuration file downloaded as startup configuration file automatically.
Step 4	**boot autoinstall auto-reboot** Enable the auto reboot mode and the switch will reboot automatically after the auto install process is completed successfully.
Step 5	**boot autoinstall retry-count** *count* Specify the auto install retry count which ranges from 1 to 3. The default value is 1.

Step 6	**boot autoinstall start** Start the Auto Install process and the switch will download the configuration file and the backup image automatically.
Step 7	**end** Return to privileged EXEC mode.
Step 8	**copy running-config startup-config** Save the settings in the configuration file.

Note:

- The switch will obtain a new IP address from the DHCP server during the process of Auto Install. If you want to access to the switch, you should check the new IP address on the DHCP server.
- IF the Auto Install process is failed, the switch will restart the process every 10 minutes. You can stop the process manually.

The following example shows how to configure the Auto Install function.

Switch#configure

Switch(config)#boot autoinstall persistent-mode

Switch(config)#boot autoinstall auto-save

Switch(config)#boot autoinstall auto-reboot

Switch(config)#boot autoinstall retry-count 2

Switch(config)#show boot autoinstall

Auto Insatll Mode.....Stop

Auto Insatll Persistent Mode.....Enabled

Auto Save Mode.....Enabled

Auto Reboot Mode.....Enabled

Auto Insatll Retry Count.....2

Auto Insatll sate.....Stopped

4.2.6 Rebooting the switch

Follow these steps to reboot the switch:

Step 1	**enable** Enter privileged mode.

Step 2	**reboot** Reboot the switch.

4.2.7 Configuring the Reboot Schedule

Follow these steps and choose one type to configure the reboot schedule:

Step 1	**configure** Enter global configuration mode.
Step 2	Use the following command to set the interval to reboot: **reboot-schedule in** *interval* **[save_before_reboot]** (Optional) Specify the reboot schedule. *interval*: Specify a period of time. The switch will reboot after this period. The valid values are from 1 to 43200 minutes. **save_before_reboot**: Save the configuration file before the switch reboots. Use the following command to set the time and date to reboot: **reboot-schedule at** *time* **[** *date* **] [save_before_reboot]** (Optional) Specify the reboot schedule. *time*: Specify the time 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. If no date is specified, the switch reboots according to the time you have set. If the time you set is later than the time that this command is executed, the switch will reboot later the same day; otherwise the switch will reboot the next day.
Step 3	**end** Return to privileged EXEC mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set the switch to reboot at 12:00 on 15/01/2016.

Switch#configure

Switch(config)#reboot-schedule at 12:00 15/01/2016 save_before_reboot

Reboot system at 15/01/2016 12:00. Continue? (Y/N): Y

Reboot Schedule Settings

Reboot schedule at 2016-01-15 12:00 (in 17007 minutes)

Save before reboot: Yes

Switch(config)#end

Switch#copy running-config startup-config

4.2.8 Reseting the Switch

Follow these steps to reset the switch:

Step 1	**enable**	Enter privileged mode.
Step 2	**reset**	Reset the switch.

Note:

After the system is reset, configurations of the switch will be reset to the default.

5 Access Security Configurations

With access security configurations, you can:

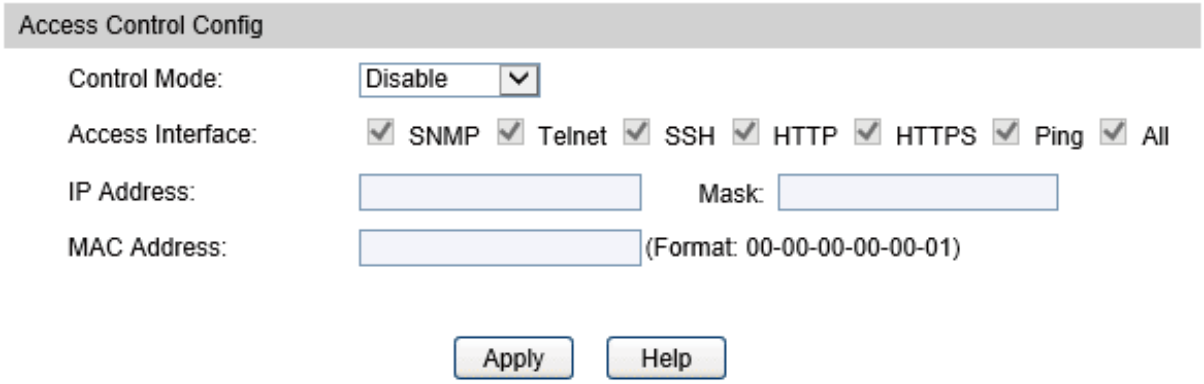
- Configure the Access Control feature
- Configure the HTTP feature
- Configure the HTTPS feature
- Configure the SSH feature
- Enable the telnet function

5.1 Using the GUI

5.1.1 Configuring the Access Control Feature

Choose the menu **System** > **Access Security** > **Access Control** to load the following page.

Figure 5-1 Configuring the Access Control



1) In the **Access Control** section, select one control mode and specify the parameters.

Control Mode	Select the control mode for users to log in to the web management page. **Disable**: The Access Control function is disabled. **IP-based**: Only the users within the IP-range you set here are allowed to access the switch. **MAC-based**: Only the users with the MAC address you set here are allowed to access the switch. **Port-based**: Only the users connecting to the ports you set here are allowed to access the switch.

Access Interface	Select the interface to control the methods for users' accessing. The selected access interfaces will only affect the users you set before. **SNMP**: A function to manage the network devices via NMS. **Telnet**: A connection type for users to remote login. **SSH**: A connection type based on SSH protocol. **HTTP**: A connection type based on HTTP protocol. **HTTPS**: A connection type based on SSL protocol. **Ping**: A communication protocol to test the connection of the network.
IP Address/ Mask	If you select **IP-based** mode, enter the IP address and mask to specify an IP range. Only the users within this IP range can access the switch.
MAC Address	If you select **MAC-based** mode, specify the MAC address. Only the users with the correct MAC address can access the switch.

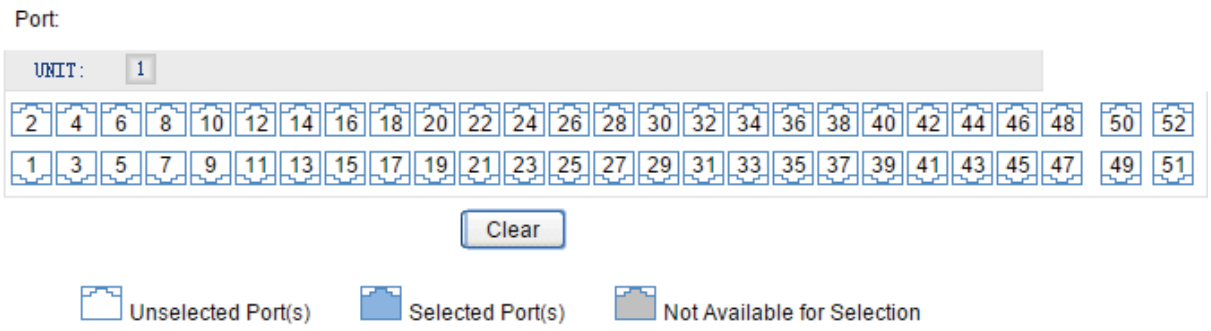
When the **IP-based** mode is selected, the following section will display.

IP Entry Table

Select	Index ID	IP Address	Access Interface	Operation
☐	1	192.168.0.0/16	SNMP Telnet SSH HTTP HTTPS Ping	Edit

IP Address	Displays the IP range of the entry.
Access Interface	Displays the access interface you set of the entry.
Operation	Click **Edit** to modify the parameters of the desired entry.

When the **Port-based** mode is selected, the following section will display.



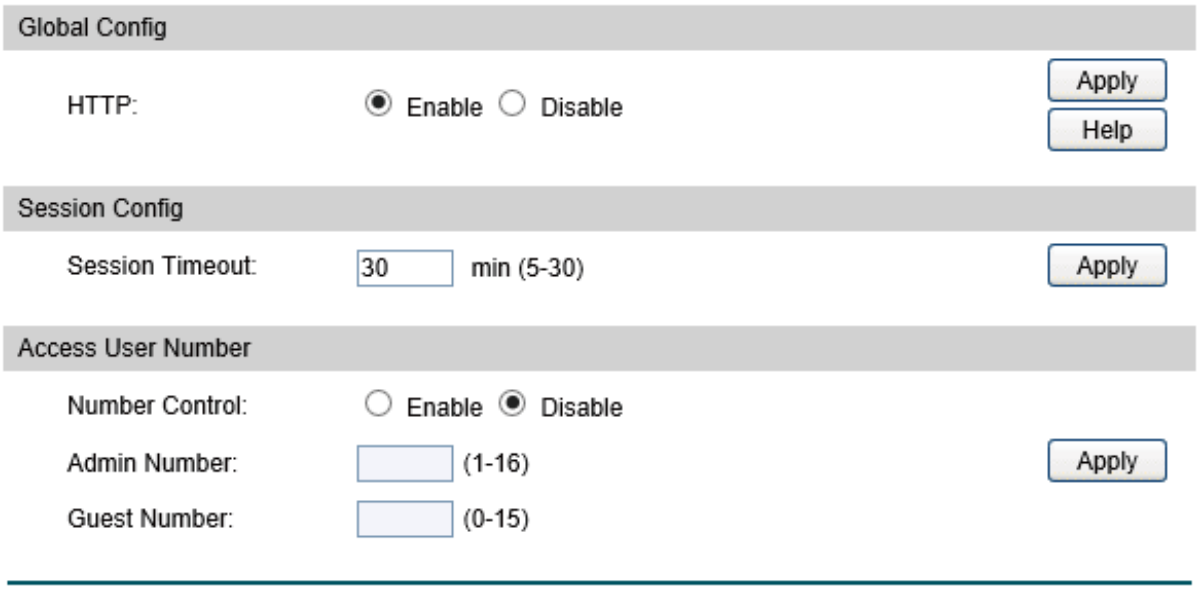
Port	Select one or more ports to configure. Only the users connected to these ports are allowed to access the switch.

2) Click **Apply**.

5.1.2 Configuring the HTTP Function

Choose the menu **System** > **Access Security** > **HTTP Config** to load the following page.

Figure 5-2 Configuring the HTTP Function



1) In the **Global Control** section, Select **Enable** and click **Apply** to enable the HTTP function.

HTTP	HTTP function is based on the HTTP protocol. It allows users to manage the switch through a web browser.

2) In the **Session Config** section, specify the Session Timeout and click **Apply**.

Session Timeout	The system will log out automatically if users do nothing within the Session Timeout time.

3) In the **Access User Number** section, select **Enable** and specify the parameters.

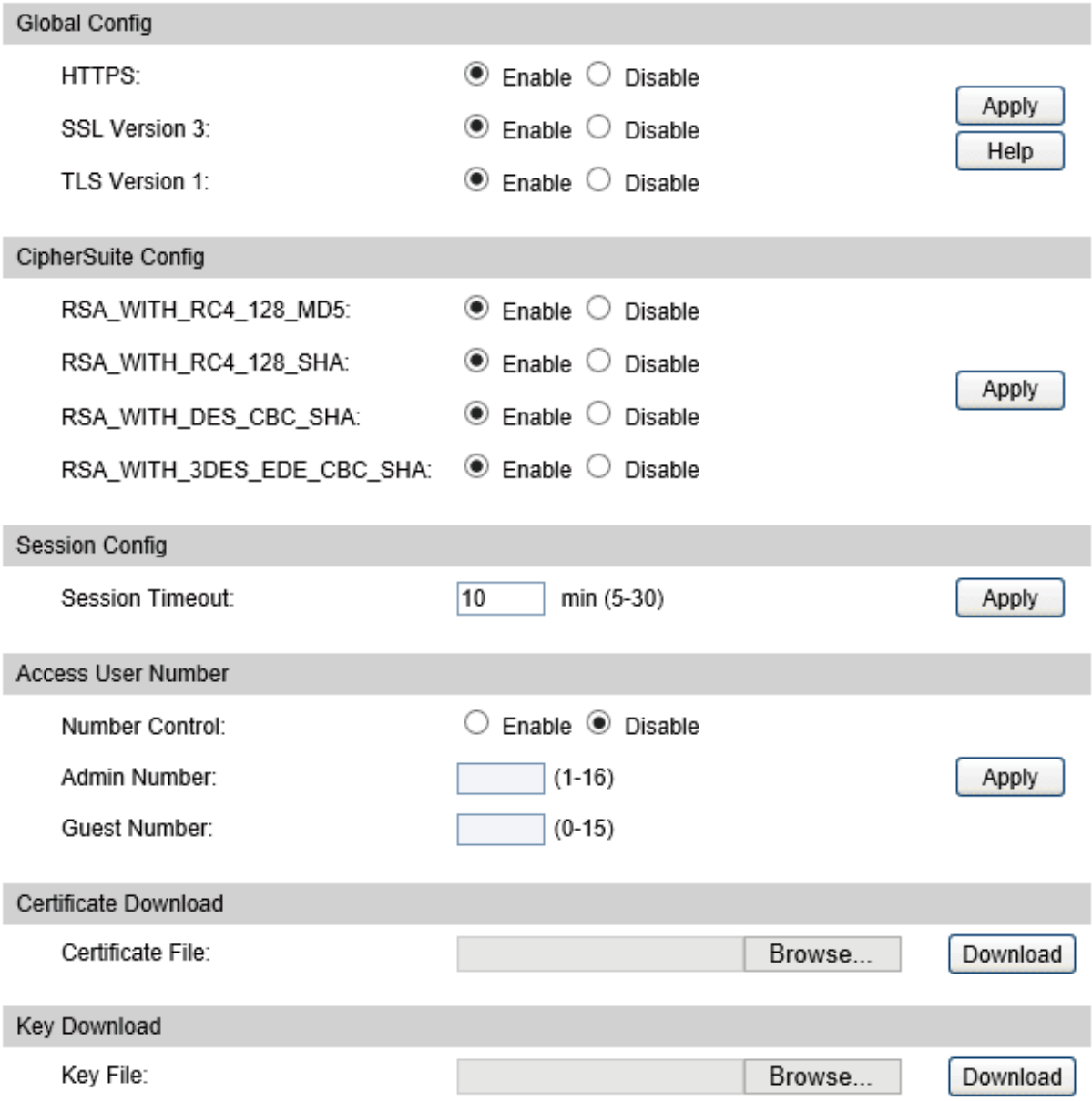
Number Control	Select **Enable** to control the number of the users logging on to the web management page at the same time. The total number of users should be no more than 16.
Admin Number	Specify the maximum number of users whose access level is Admin.
Guest Number	Specify the maximum number of users whose access level is Operator, Power User or User.

4) Click **Apply**.

5.1.3 Configuring the HTTPS Function

Choose the menu **System** > **Access Security** > **HTTPS Config** to load the following page.

Table 5-1 Configuring the HTTPS Function



1) In the **Global Config** section, select **Enable** to enable HTTPS function and select the protocol the switch supports. Click **Apply**.

HTTPS	Select **Enable** to enable the HTTPS function. HTTPS function is based on the SSL or TLS protocol. It provides a secure connection between the client and the switch.

SSL Version 3	Select **Enable** to make the switch support SSL Version 3 protocol. SSL is a transport protocol. It can provide server authentication, encryption and message integrity to allow secure HTTP connection.
TLS Version 1	Select **Enable** to make the switch support TLS Version 1 protocol. TLS is a transport protocol upgraded from SSL. It supports a different encryption algorithm from SSL, so TLS and SSL are not compatible. TLS can support a more secure connection.

2) In the **CipherSuite Config** section, select the algorithm to be enabled and click **Apply**.

RSA_WITH_ RC4_128_MD5	Key exchange with RC4 128-bit encryption and MD5 for message digest.
RSA_WITH_ RC4_128_SHA	Key exchange with RC4 128-bit encryption and SHA for message digest.
RSA_WITH_ DES_CBC_SHA	Key exchange with DES-CBC for message encryption and SHA for message digest.
RSA_ WITH_3DES_ EDE_CBC_SHA	Key exchange with 3DES and DES-EDE3-CBC for message encryption and SHA for message digest.

3) In the **Session Config** section, specify the Session Timeout and click **Apply**.

Session Timeout	The system will log out automatically if users do nothing within the Session Timeout time.

4) In the **Access User Number** section, select **Enable** and specify the parameters. Click **Apply**.

Number Control	Select **Enable** to control the number of the users logging in to the web management page at the same time.
Admin Number	Specify the maximum number of users whose access level is Admin.
Guest Number	Specify the maximum number of users whose access level is Operator, Power User or User.

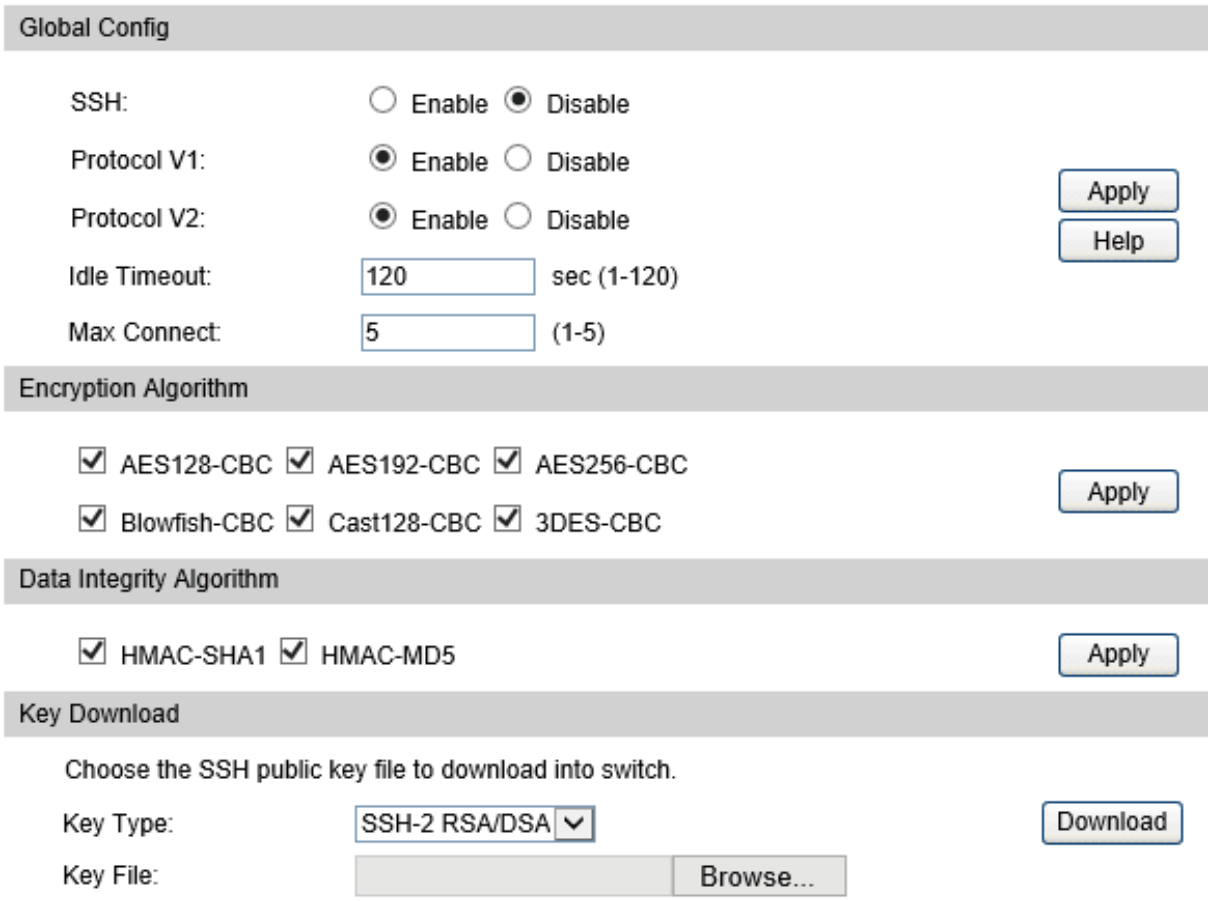
5) In the **Certificate Download** and **Key Download** section, download the certificate and key.

Certificate File	Select the desired certificate to download to the switch. The certificate must be BASE64 encoded. The SSL certificate and key downloaded must match each other, otherwise the HTTPS connection will not work.
Key File	Select the desired Key to download to the switch. The key must be BASE64 encoded. The SSL certificate and key downloaded must match each other, otherwise the HTTPS connection will not work.

5.1.4 Configuring the SSH Feature

Choose the menu **System** > **Access Security** > **SSH Config** to load the following page.

Figure 5-3 Configuring the SSH Feature



1) In the **Global Config** section, select **Enable** to enable SSH function and specify other parameters.

SSH	Select **Enable** to enable the SSH function. SSH is a protocol working in application layer and transport layer. It can provide a secure, remote connection to a device. It is more secure than Telnet protocol as it provides strong encryption.
Protocol V1	Select **Enable** to enable SSH version 1.
Protocol V2	Select **Enable** to enable SSH version 2.
Idle Timeout	Specify the idle timeout time. The system will automatically release the connection when the time is up.
Max Connect	Specify the maximum number of the connections to the SSH server. New connection will not be established when the number of the connections reaches the maximum number you set.

2) In the **Encryption Algorithm** section, select the encryption algorithm you want the switch to support and click **Apply**.

3) In **Data Integrity Algorithm** section, select the integrity algorithm you want the switch to support and click **Apply**.

4) In **Key Download** section, select key type from the drop-down list and select the desired key file to down.

Key Type	Select the key type. The algorithm of the corresponding type is used for both key generation and authentication.
Key File	Select the desired public key to download to the switch. The key length of the downloaded file ranges of 512 to 3072 bits.

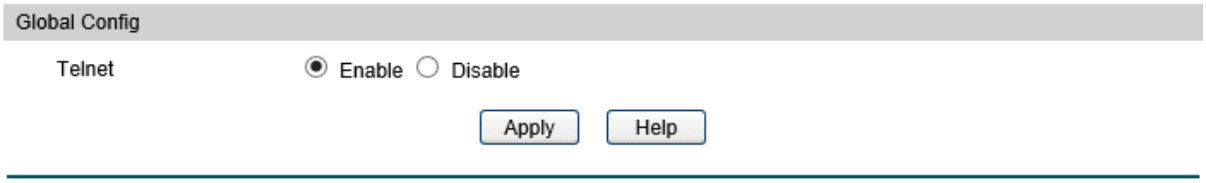
Note:

It will take a long time to download the key file. Please wait without any operation.

5.1.5 Enabling the Telnet Function

Choose the menu **System** > **Access Security** > **Telnet Config** to load the following page.

Figure 5-4 Configuring the Telnet Function



In the **Global Config** section, select **Enable** and click **Apply**.

Telnet	Select **Enable** to make the Telnet function effective. Telnet function is based on the Telnet protocol subjected to TCP/IP protocol. It allows users to log on to the switch remotely.

5.2 Using the CLI

5.2.1 Configuring the Access Control

Follow these steps to configure the access control:

Step 1	**configure** Enter global configuration mode.

Step 2	Use the following command to control the users' access by limiting the IP address: **user access-control ip-based {** *ip-addr ip-mask* **} [** snmp **] [** telnet **] [** ssh **] [** http **] [** https **] [** ping **] [** all **]** Only the users within the IP-range you set here are allowed to access the switch. *ip-addr*: Specify the IP address of the user. *ip-mask*: Specify the subnet mask of the user. **[** snmp **] [** telnet **] [** ssh **] [** http **] [** https **] [** ping **] [** all **]**: Select to control the types for users' accessing. By default, these types are all enabled. Use the following command to control the users' access by limiting the MAC address: **user access-control mac-based {** *mac-addr* **} [** snmp **] [** telnet **] [** ssh **] [** http **] [** https **] [** ping **] [** all **]** Only the users with the MAC address you set here are allowed to access the switch. *mac-addr*: Specify the MAC address of the user. **[** snmp **] [** telnet **] [** ssh **] [** http **] [** https **] [** ping **] [** all **]**: Select to control the types for users' accessing. By default, these types are all enabled. Use the following command to control the users' access by limiting the ports connected to the users: **user access-control port-based interface { fastEthernet** *port-list* **| gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port-list* **} [** snmp **] [** telnet **] [** ssh **] [** http **] [** https **] [** ping **] [** all **]** Only the users connecting to the ports you set here are allowed to access the switch. *port-list*: Specify the list of Ethernet port, in the format of 1/0/1-4. You can appoint 5 ports at most. **[** snmp **] [** telnet **] [** ssh **] [** http **] [** https **] [** ping **] [** all **]**: Select to control the types for users' accessing. By default, these types are all enabled.
Step 3	**show user configuration** Verify the security configuration information of the user authentication information and the access interface.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set the type of access control as IP-based. Set the IP address as 192.168.0.100,set the subnet mask as 255.255.255.0 and make the switch support snmp, telnet, http and https.

Switch#configure

Switch(config)#user access-control ip-based 192.168.0.100 255.255.255.0 snmp telnet http https

Switch(config)#show user configuration

User authentication mode: IP based

Index	IP Address	Access Interface
1	192.168.0.0/24	SNMP Telnet HTTP HTTPS

Switch(config)#end

Switch#copy running-config startup-config

5.2.2 Configuring the HTTP Function

Follow these steps to configure the HTTP function:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip http server** Enable the HTTP function. By default, it is enabled.
Step 3	**ip http session timeout** *minutes* Specify the Session Timeout time. The system will log out automatically if users do nothing within the Session Timeout time. *minutes*: Specify the timeout time, which ranges from 5 to 30 minutes. The default value is 10.
Step 4	**ip http max-users** *admin-num guest-num* Specify the maximum number of users that are allowed to connect to the HTTP server. The total number of users should be no more than 16. *admin-num*: Enter the maximum number of users whose access level is Admin. The valid values are from 1 to 16. *guest-num*: Enter the maximum number of users whose access level is Operator, Power User or User. The valid values are from 0 to 15.
Step 5	**show ip http configuration** Verify the configuration information of the HTTP server, including status, session timeout, access-control, max-user number and the idle-timeout, etc.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set the session timeout as 9, set the maximum admin number as 6, and set the maximum guest number as 5.

Switch#configure

Switch(config)#ip http server

Switch(config)#ip http session timeout 9

Switch(config)#ip http max-user 6 5

Switch(config)#show ip http configuration

HTTP Status:	Enabled
HTTP Session Timeout:	9
HTTP User Limitation:	Enabled
HTTP Max Admin Users:	6
HTTP Max Guest Users:	5

Switch(config)#end

Switch#copy running-config startup-config

5.2.3 Configuring the HTTPS Function

Follow these steps to configure the HTTPS function:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip http secure-server** Enable the HTTPS function. By default, it is enabled.
Step 3	**ip http secure-protocol { [** ssl3 **] [** tls1 **] }** Configure to make the switch support the corresponding protocol. By default, the switch supports SSLv3 and TLSv1. ssl3: Enable the SSL version 3 protocol. SSL is a transport protocol. It can provide server authentication, encryption and message integrity to allow secure HTTP connection. tls1: Enable the TLS version 1 protocol. TLS is s transport protocol upgraded from SSL. It supports different encryption algorithm from SSL, so TLS and SSL are not compatible. TLS can support a more secure connection.
Step 4	**ip http secure-ciphersuite { [3des-ede-cbc-sha] [rc4-128-md5] [rc4-128-sha] [des-cbc-sha] }** Enable the corresponding ciphersuite. By default, these types are all enabled. **[3des-ede-cbc-sha]**: Key exchange with 3DES and DES-EDE3-CBC for message encryption and SHA for message digest. **[rc4-128-md5]**: Key exchange with RC4 128-bit encryption and MD5 for message digest. **[rc4-128-sha]**: Key exchange with RC4 128-bit encryption and SHA for message digest. **[des-cbc-sha]**: Key exchange with DES-CBC for message encryption and SHA for message digest.

Step 5	**ip http secure-session timeout** *minutes* Specify the Session Timeout time. The system will log out automatically if users do nothing within the Session Timeout time. *minutes*: Specify the timeout time, which ranges from 5 to 30 minutes. The default value is 10.
Step 6	**ip http secure-max-users** *admin-num guest-num* Specify the maximum number of users that are allowed to connect to the HTTPS server. The total number of users should be no more than 16. *admin-num*: Enter the maximum number of users whose access level is Admin. The valid value are from 1 to 16. *guest-num*: Enter the maximum number of users whose access level is Operator, Power User or User. The valid value are from 0 to 15.
Step 7	**ip http secure-server download certificate** *ssl-cert* **ip-address** *ip-addr* Download the desired certificate to the switch from TFTP server. *ssl-cert*: Specify the name of the SSL certificate, which ranges from 1 to 25 characters. The certificate must be BASE64 encoded. The SSL certificate and key downloaded must match each other. *ip-addr*: Specify the IP address of the TFTP server. Both IPv4 and IPv6 addresses are supported.
Step 8	**ip http secure-server download key** *ssl-key* **ip-address** *ip-addr* Download the desired key to the switch from TFTP server. *ssl-key*: Specify the name of the key file saved in TFTP server. The key must be BASE64 encoded. *ip-addr*: Specify the IP address of the TFTP server. Both IPv4 and IPv6 addresses are supported.
Step 9	**show ip http secure-server** Verify the global configuration of HTTPS.
Step 10	**end** Return to privileged EXEC mode.
Step 11	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the HTTPS function. Enable SSL3 and TLS1 protocol. Enable the ciphersuite of 3des-ede-cbc-sha. Set the session timeout time as 15, the admin number as 1 and the guest number as 2. Download the certificate named ca.crt and the key named ca.key from the TFTP server with the IP address 192.168.0.100.

Switch#configure

Switch(config)#ip http secure-server

Switch(config)#ip http secure-protocol ssl3 tls1

Switch(config)#ip http secure-ciphersuite 3des-ede-cbc-sha

Switch(config)#ip http secure-session timeout 15

Switch(config)#ip http secure-max-users 1 2

Switch(config)#ip http secure-server download certificate ca.crt **ip-address** 192.168.0.100

Start to download SSL certificate...

Download SSL certificate OK.

Switch(config)#ip http secure-server download key ca.key **ip-address** 192.168.0.100

Start to download SSL key...

Download SSL key OK.

Switch(config)#show ip http secure-server

HTTPS Status:	Enabled
SSL Protocol Level(s):	ssl3 tls1
SSL CipherSuite:	3des-ede-cbc-sha
HTTPS Session Timeout:	15
HTTPS User Limitation:	Enabled
HTTPS Max Admin Users:	1
HTTPS Max Guest Users:	2

Switch(config)#end

Switch#copy running-config startup-config

5.2.4 Configuring the SSH Feature

Follow these steps to configure the SSH function:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip ssh server** Enable the SSH function. By default, it is disabled.
Step 3	**ip ssh version {** v1 | v2 **}** Configure to make the switch support the corresponding protocol. By default, the switch supports SSHv1 and SSHv3. v1 | v2: Select to enable the corresponding protocol.

Step 4	**ip ssh timeout** *value* Specify the idle timeout time. The system will automatically release the connection when the time is up. *value*: Enter the value of the timeout time, which ranges from 1 to 120 seconds. The default value is 120 seconds.
Step 5	**ip ssh max-client** *num* Specify the maximum number of the connections to the SSH server. New connection will not be established when the number of the connections reaches the maximum number you set. *num*: Enter the number of the connections, which ranges from 1 to 5. The default value is 5.
Step 6	**ip ssh algorithm {** AES128-CBC | AES192-CBC | AES256-CBC | Blowfish-CBC | Cast128-CBC | 3DES-CBC | HMAC-SHA1 | HMAC-MD5 **}** Enable the corresponding algorithm. By default, these types are all enabled. AES128-CBC | AES192-CBC | AES256-CBC | Blowfish-CBC | Cast128-CBC | 3DES-CBC: Specify the encryption algorithm you want the switch supports. HMAC-SHA1 | HMAC-MD5: Specify the data integrity algorithm you want the switch supports.
Step 7	**ip ssh download {** v1 | v2 **}** *key-file* **ip-address** *ip-addr* Select the type of the key file and download the desired file to the switch from TFTP server. v1 | v2: Select the key type. The algorithm of the corresponding type is used for both key generation and authentication. *key-file*: Specify the name of the key file saved in TFTP server. Ensure the key length of the downloaded file is in the range of 512 to 3072 bits. *ip-addr*: Specify the IP address of the TFTP server. Both IPv4 and IPv6 addresses are supported.
Step 8	**show ip ssh** Verify the global configuration of SSH.
Step 9	**end** Return to privileged EXEC mode.
Step 10	**copy running-config startup-config** Save the settings in the configuration file.

Note:

It will take a long time to download the key file. Please wait without any operation.

The following example shows how to configure the SSH function. Set the version as SSH V1 and SSH V2. Enable the AES128-CBC and Cast128-CBC encryption algorithm. Enable the HMAC-MD5 data integrity algorithm. Choose the key type as SSH-2 RSA/DSA.

Switch(config)#ip ssh server

Switch(config)#ip ssh version v1

Switch(config)#ip ssh version v2

Switch(config)#ip ssh timeout 100

Switch(config)#ip ssh max-client 4

Switch(config)#ip ssh algorithm AES128-CBC

Switch(config)#ip ssh algorithm Cast128-CBC

Switch(config)#ip ssh algorithm HMAC-MD5

Switch(config)#ip ssh download v2 publickey **ip-address** 192.168.0.100

Start to download SSH key file...

Download SSH key file OK.

Switch(config)#show ip ssh

Global Config:

SSH Server: Enabled

Protocol V1: Enabled

Protocol V2: Enabled

Idle Timeout: 100

MAX Clients: 4

Encryption Algorithm:

AES128-CBC: Enabled

AES192-CBC: Disabled

AES256-CBC: Disabled

Blowfish-CBC: Disabled

Cast128-CBC: Enabled

3DES-CBC: Disabled

Data Integrity Algorithm:

HMAC-SHA1: Disabled

HMAC-MD5: Enabled

Key Type: SSH-2 RSA/DSA

Key File:

---- BEGIN SSH2 PUBLIC KEY ----

Comment: “dsa-key-20160711”

Switch(config)#end

Switch#copy running-config startup-config

5.2.5 Enabling the Telnet Function

Follow these steps enable the Telnet function:

Step 1	**configure** Enter global configuration mode.
Step 2	**telnet enable** Enable the telnet function. By default, it is enabled.
Step 3	**end** Return to privileged EXEC mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

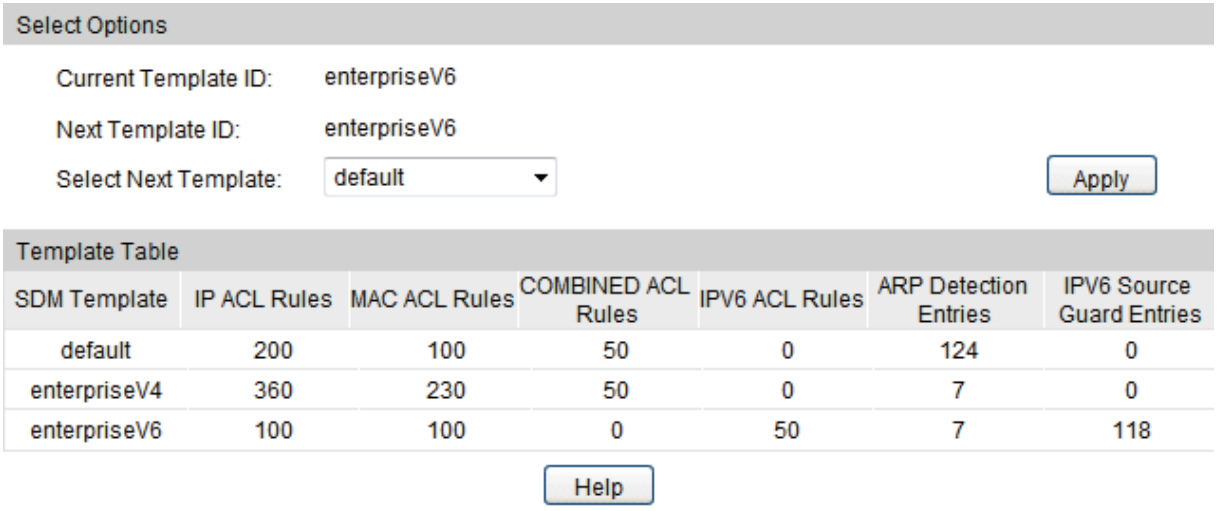
6 SDM Template Configuration

SDM Template function is used to configure system resources in the switch to optimize support for specific features. The switch provides three templates, and the hardware resources allocation is different. Users can choose one according to how the switch is used in the network.

6.1 Using the GUI

Choose the menu **System** > **SDM Template** to load the following page.

Figure 6-1 Configuring the SDM Template Function



In **Select Options** section, select one template and click **Apply**. The setting will be effective after the reboot.

Current Template ID	Displays the template currently in effect.
Next Template ID	Displays the template that will be effective after the reboot.
Select Next Template	Select the template that will be effective after the next reboot. **default**: Select the template of default. It gives balance to the IP ACL rules, MAC ACL rules and ARP detection entries. **enterpriseV4**: Select the template of enterpriseV4. It maximizes system resources for IP ACL rules and MAC ACL rules. **enterpriseV6**: Select the template of enterpriseV6. It allocates resources to IPv6 ACL rules.

The Template Table displays the resources allocation of each template.

SDM Template	Displays the name of the templates.
IP ACL Rules	Displays the number of IP ACL Rules including Lay3 ACL Rules and Lay4 ACL Rules.
MAC ACL Rules	Displays the number of Lay2 ACL Rules.
COMBINED ACL Rules	Displays the number of combined ACL rules.
IPv6 ACL Rules	Displays the number of IPv6 ACL rules.
ARP Detection Entries	Displays the number of TCAM entries for ARP defend.
IPv6 Source Guard Entries	Displays the number of IPv6 source guard entries.

6.2 Using the CLI

Follow these steps to configure the SDM template function:

Step 1	**configure** Enter global configuration mode.
Step 2	**show sdm prefer {** used | default | enterpriseV4 | enterpriseV6 **}** View the template table to select the desired template. used: Displays the resource allocation of the current template. default: Displays the resource allocation of the default template. enterpriseV4: Displays the resource allocation of the enterpriseV4 template. enterpriseV6: Displays the resource allocation of the enterpriseV6 template.
Step 3	**sdm prefer {** default | enterpriseV4 | enterpriseV6 **}** Select the template that will be effective after the next reboot. default: Select the template of default. It gives banlance to the IP ACLrules, MAC ACL rules and ARP detection entries. enterpriseV4: Select the template of enterpriseV4. It maximizes system resources for IP ACL rules and MAC ACL rules. enterpriseV6: Select the template of enterpriseV4. It allocates resources to IPv6 ACL rules.
Step 4	**end** Return to privileged EXEC mode.

Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set the SDM template as enterpriseV4.

Switch#config

Switch(config)#show sdm prefer enterpriseV4

“enterpriseV4” template:

number of IP ACL Rules : 360

number of MAC ACL Rules : 230

number of Combined ACL Rules : 50

number of IPV6 ACL Rules : 0

number of IPV6 Source Guard Entries : 0

number of ARP Detection Entries : 7

Switch(config)#sdm prefer enterpriseV4

Switch to “enterpriseV4” tempale.

Changes to the running SDM preferences have been stored, but cannot take effect until reboot the switch.

Switch(config)#end

Switch#copy running-config startup-config

7 Appendix: Default Parameters

Default settings of System Info are listed in the following tables.

Table 7-1 Default Settings of Device Description Configuration

Parameter	Default Setting
Device Name	The model name of the switch.
Device Location	SHENZHEN
System Contact	www.tp-link.com

Table 7-2 Default Settings of System Time Configuration

Parameter	Default Setting
Time Source	Manual
System Time	2006-01-01 08:01:56 Sunday

Table 7-3 Default Settings of Daylight Saving Time Configuration

Parameter	Default Setting
DST status	Disabled

Default settings of User Management are listed in the following table.

Table 7-4 Default Settings of User Configuration

Parameter	Default Setting
User Name	admin
Password	admin
Access Level	Admin

Default settings of System Tools are listed in the following table.

Table 7-5 Default Settings of Boot Configuration

Parameter	Default Setting
Current Startup Image	image1.bin
Next Startup Image	image1.bin
Backup Image	image2.bin

Default settings of Access Security are listed in the following tables.

Table 7-6 Default Settings of Access Control Configuration

Parameter	Default Setting
Control Mode	Disabled

Table 7-7 Default Settings of HTTP Configuration

Parameter	Default Setting
HTTP	Enabled
Session Timeout	10 minutes
Number Control	Disabled

Table 7-8 Default Settings of HTTPS Configuration

Parameter	Default Setting
HTTPS	Enabled
SSL Version 3	Enabled
TLS Version 1	Enabled
RSA_WITH_RC4_128_MD5	Enabled
RSA_WITH_RC4_128_SHA	Enabled
RSA_WITH_DES_CBC_SHA	Enabled
RSA_WITH_3DES_EDE_CBC_SHA	Enabled
Session Timeout	10 minutes
Number Control	Disabled

Table 7-9 Default Settings of SSH Configuration

Parameter	Default Setting
SSH	Disabled
Protocol V1	Enabled
Protocol V2	Enabled
Idle Timeout	120 seconds
Max Connect	5
AES128-CBC	Enabled
AES192-CBC	Enabled
AES256-CBC	Enabled
Blowfish-CBC	Enabled
Cast128-CBC	Enabled
3DES-CBC	Enabled

Parameter	Default Setting
HMAC-SHA1	Enabled
HMAC-MD5	Enabled
Key Type:	SSH-2 RSA/DSA

Table 7-10 Default Settings of Telnet Configuration

Parameter	Default Setting
Control Mode	Enabled

Default settings of SDM Template are listed in the following table.

Table 7-11 Default Settings of SDM Template Configuration

Parameter	Default Setting
Current Template ID	Default
Next Template ID	Default

Table 7-12 Default Settings of Device Description Configuration

Parameter	Default Setting
Auto Install Mode	Stop
Auto Install Persistent Mode	Disable
Auto Save Mode	Enable
Auto Reboot Mode	Disable
Auto Install Retry Count	1

Part 3

Managing Physical Interfaces

CHAPTERS

1. Physical Interface
2. Basic Parameters Configurations
3. Port Mirror Configuration
4. Port Security Configuration
5. Port Isolation Configurations
6. Loopback Detection Configuration
7. Configuration Examples

1 Physical Interface

1.1 Overview

Interfaces of a device are used to exchange data and interact with other network devices. Interfaces are classified into physical interfaces and logical interfaces.

- Physical interfaces are the ports on the front panel or rear panel of the switch.
- Logical interfaces are manually configured and do not physically exist, such as loopback interfaces and routing interfaces.

This chapter introduces the configurations for physical interfaces.

1.2 Supported Features

The switch supports the following features about physical interfaces:

Basic Parameters

You can configure port status, speed mode, duplex mode, flow control and other basic parameters for ports.

Port Mirror

This function allows the switch to forward packet copies of the monitored ports to a specific monitoring port. Then you can analyze the copied packets to monitor network traffic and troubleshoot network problems.

Port Security

You can use this feature to limit the number of MAC addresses that can be learned on each port, thus preventing the MAC address table from being exhausted by the attack packets.

Port Isolation

You can use this feature to restrict a specific port to send packets to only the ports in the forward-port list that you configure.

Loopback Detection

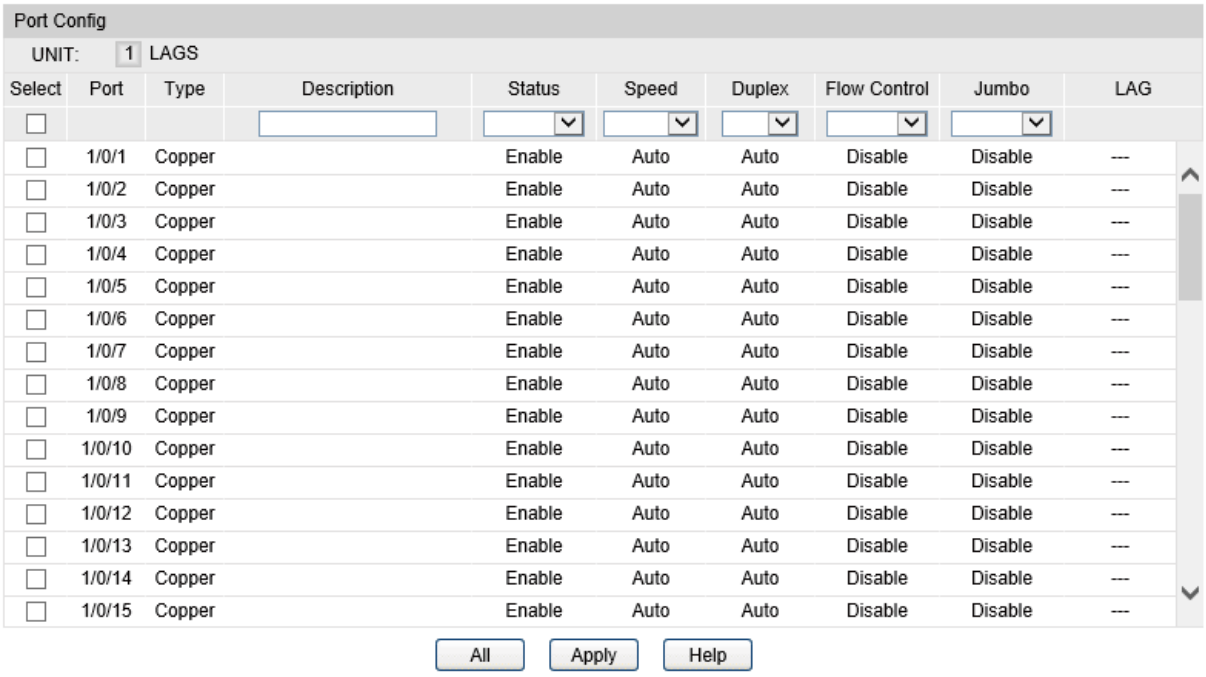
This function allows the switch to detect loops in the network. When a loop is detected on a port, the switch will send a trap message, generate an entry on the log file and further block the corresponding port according to your configurations.

2 Basic Parameters Configurations

2.1 Using the GUI

Choose the menu **Switching > Port > Port Config** to load the following page.

Figure 2-1 Configuring Basic Parameters



Follow these steps to set basic parameters for ports:

Select and configure your desired ports or LAGs. Then click **Apply**.

UNIT:1/LAGS	Click **1** to configure physical ports. Click **LAGS** to configure LAGs.
Type	Displays the port type. **Copper** indicates an Ethernet port, and **SFP** or **SFP+** indicates a fiber port.
Description	Give a port description for identification.
Status	With this option enabled, the port forwards packets normally. Otherwise, the port discards all the received packets. By default, it is enabled.
Speed	Select the appropriate speed mode for the port. When **Auto** is selected, the port autonegotiates speed mode with the connected device. The default setting is **Auto**. This value is recommended if both ends of the line support auto-negotiation.
Duplex	Select the appropriate duplex mode for the port. There are three options: **Half**, **Full** and **Auto**. When **Auto** is selected, the port autonegotiates duplex mode with the connected device. The default setting is **Auto**.

Flow Control	With this option enabled, the switch synchronizes the data transmission speed with the peer device, thus avoiding the packet loss caused by congestion. By default, it is disabled.
Jumbo	With this option enabled, the port can send jumbo frames. The default MTU (Maximum Transmission Unit) size for frames received and sent on all ports is 1518 bytes. For the port with Jumbo enabled, the MTU size is up to 9216 bytes, thus allowing the port to send jumbo frames. By default, it is disabled.

Note:

We recommend that you set the ports on both ends of a link as the same speed and duplex mode.

2.2 Using the CLI

Follow these steps to set basic parameters for the ports.

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** port-list **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-id-list* **}** Enter interface configuration mode.

Step 3	Configure basic parameters for the port: **description** *string* Give a port description for identification. *string*: Content of a port description, ranging from 1 to 16 characters. **shutdown** **no shutdown** Use **shutdown** to disable the port, and use **no shutdown** to enable the port. When the status is enabled, the port can forward packets normally, otherwise it will discard the received packets. By default, all ports are enabled. **speed {** 10 | 100 | 1000 | auto **}** Set the appropriate speed mode for the port. 10 | 100 | 1000 | auto: Speed mode of the port. The options are subject to your actual product. The device connected to the port should be in the same speed and duplex mode with the port. When auto is selected, the speed mode will be determined by auto negotiation. **duplex {** auto | full | half **}** Set the appropriate duplex mode for the port. auto | full | half: Duplex mode of the port. The device connected to the port should be in the same speed and duplex mode with the port. When auto is selected, the duplex mode will be determined by auto negotiation. **flow-control** Enable the switch to synchronize the data transmission speed with the peer device, avoiding the packet loss caused by congestion. By default, this feature is disabled. **jumbo** Enable Jumbo on the port. For the port with Jumbo enabled, the MTU size is up to 9216 bytes, thus allowing the port to send jumbo frames. By default, it is disabled and the MTU size for frames received and sent on the port is 1518 bytes.
Step 4	**show interface configuration [fastEthernet** *port* **| gigabitEthernet** *port* **| port-channel** *port-channel-id* **]** Verify the configuration of the port or LAG.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to implement the basic configurations of port1/0/1, including setting a description for the port, making the port autonegotiate speed and duplex with the neighboring port, and enabling the flow-control and jumbo feature:

Switch#configure

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

Switch(config-if)#no shutdown

Switch(config-if)#description router connection

Switch(config-if)#speed auto

Switch(config-if)#duplex auto

Switch(config-if)#flow-control

Switch(config-if)#jumbo

Switch(config-if)#show interface configuration gigabitEthernet 1/0/1

Port	State	Speed	Duplex	FlowCtrl	Jumbo	Description
Gi1/0/1	Enable	Auto	Auto	Enable	Enable	router connection

Switch(config-if)#end

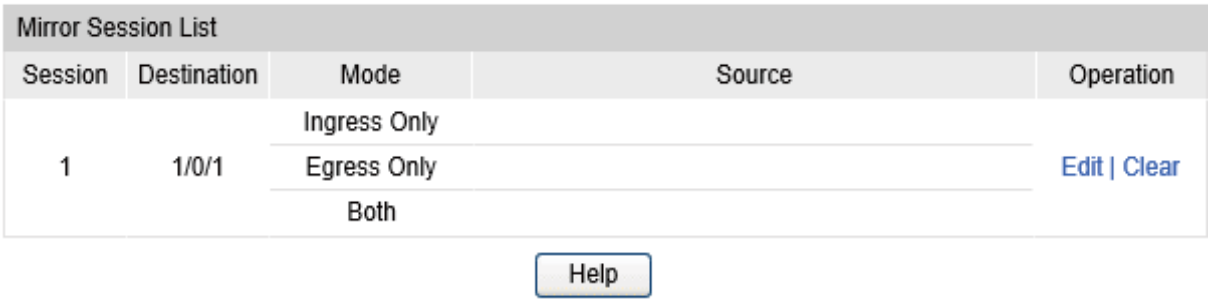
Switch#copy running-config startup-config

3 Port Mirror Configuration

3.1 Using the GUI

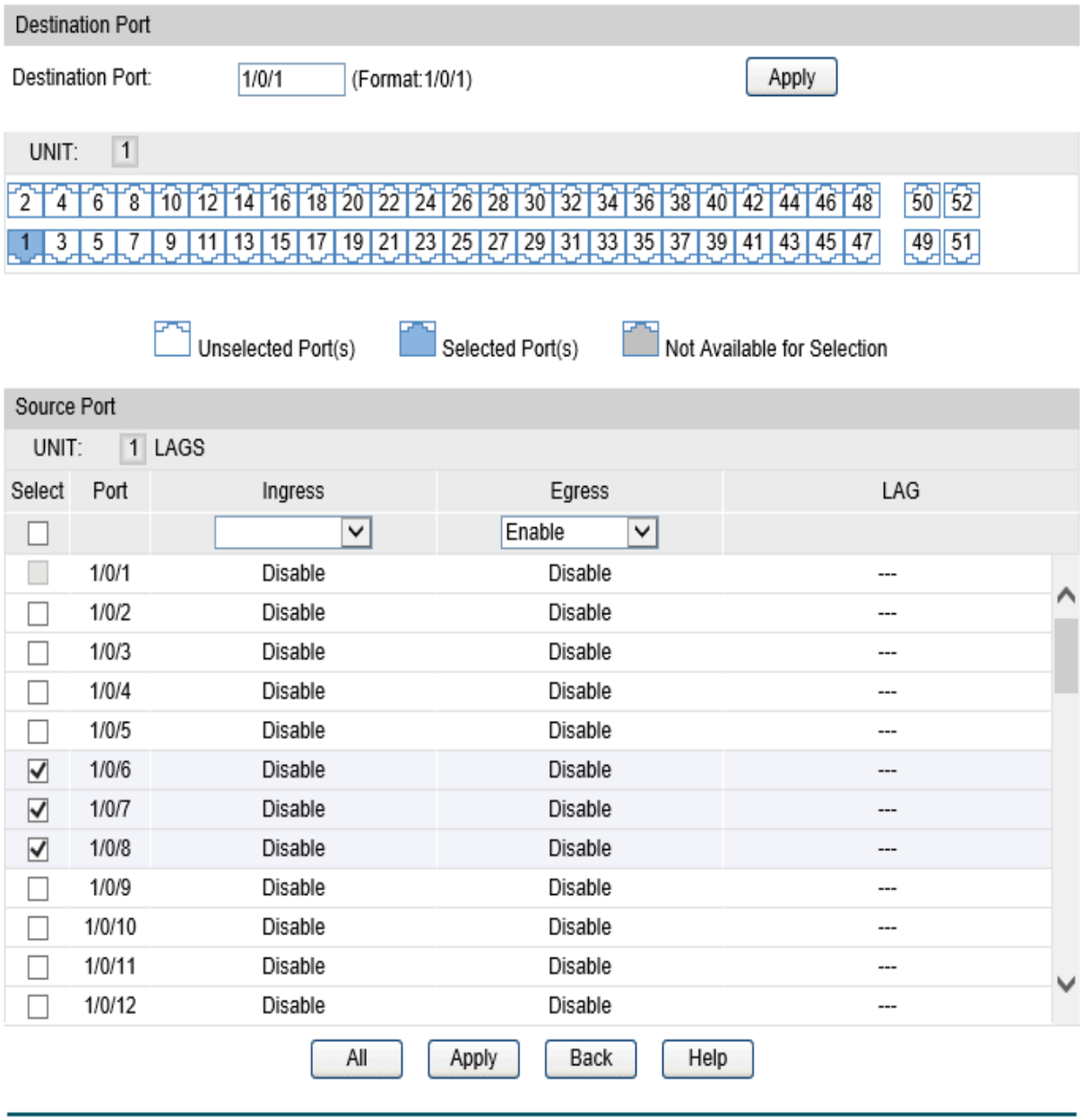
Choose the menu **Switching > Port > Port Mirror** to load the following page.

Figure 3-1 Mirror Session List



The above page displays a mirror session, and no more session can be created. Click **Edit** to configure this mirror session on the following page.

Figure 3-2 Configuring Port Mirror



Follow these steps to configure Port Mirror:

1) In the **Destination Port** section, specify a monitoring port for the mirror session, and click **Apply**.

2) In the **Source Port** section, select one or multiple monitored ports for configuration. Then set the parameters and click **Apply**.

UNIT:1/LAGS	Click **1** to select physical ports. Click **LAGS** to select LAGs.
Ingress	With this option enabled, the packets received by the monitored port will be copied to the monitoring port. By default, it is disabled.
Egress	With this option enabled, the packets sent by the monitored port will be copied to the monitoring port. By default, it is disabled.

Note:

- The member port of an LAG cannot be set as a monitoring port or monitored port.
- A port cannot be set as the monitoring port and monitored port at the same time.

3.2 Using the CLI

Follow these steps to configure Port Mirror.

Step 1	**configure** Enter global configuration mode.
Step 2	**monitor session** *session_num* **destination interface { fastEthernet** *port* **| gigabitEthernet** *port* **}** Enable the port mirror function and set the monitoring port. *session_num*: The monitor session number. It can only be specified as 1. *port*: The monitoring port number. You can specify only one monitoring port for the mirror session.
Step 3	**monitor session** *session_num* **source interface { fastEthernet** *port-list* **| gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **}** *mode* Set the monitored ports. *session_num*: The monitor session number. It can only be specified as 1. *port-list*: List of monitored port. It is multi-optional. *mode*: The monitor mode. There are three options: **rx**, **tx** and **both**: **rx**: The incoming packets of the monitored port will be copied to the monitoring port. **tx**: The outgoing packets of the monitored port will be copied to the monitoring port. **both**: Both of the incoming and outgoing packets on monitored port can be copied to the monitoring port.
Step 4	**show monitor session** Verify the Port Mirror configuration.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to copy the received and transmitted packets on port 1/0/1,2,3 to port 1/0/10.

Switch#configure

Switch(config)#monitor session 1 **destination interface gigabitEthernet** 1/0/10

Switch(config)#monitor session 1 **source interface gigabitEthernet** 1/0/1-3 both

Switch(config)#show monitor session

Monitor Session: 1

Destination Port: Gi1/0/10

Source Ports(Ingress): Gi1/0/1-3

Source Ports(Egress): Gi1/0/1-3

Switch(config-if)#end

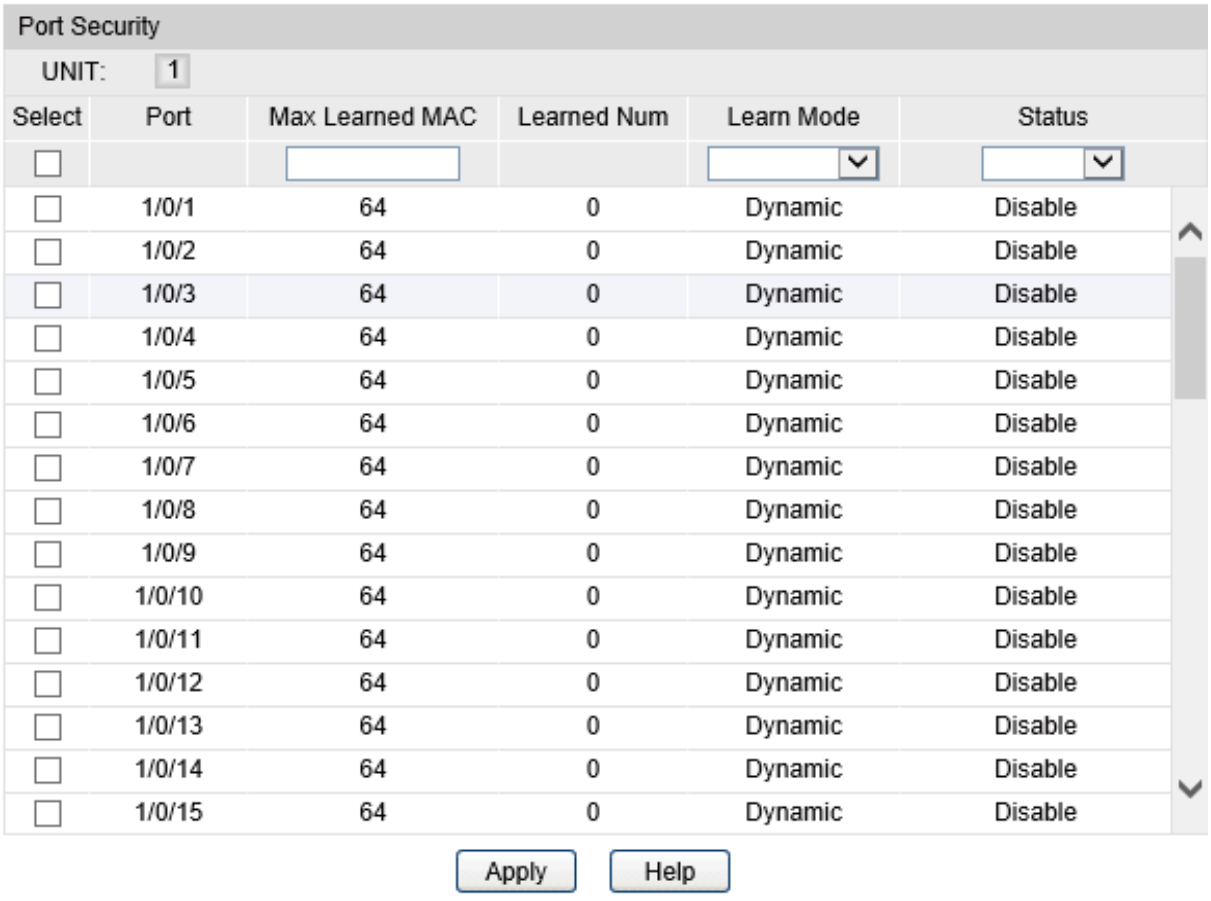
Switch#copy running-config startup-config

4 Port Security Configuration

4.1 Using the GUI

Choose the menu **Switching > Port > Port Security** to load the following page.

Figure 4-1 Port Security



Follow these steps to configure Port Security:

1) Select one or multiple ports for security configuration.
2) Specify the maximum number of the MAC addresses that can be learned on the port, and then select the learn mode of the MAC addresses.

Max Learned MAC	Specify the maximum number of MAC addresses that can be learned on the port. When the learned MAC address number reaches the limit, the port will stop learning. The default value is 64.
Learned Num	Displays the number of MAC addresses that have been learned on the port.

Learn Mode	Select the learn mode of the MAC addresses on the port. Three modes are provided: **Dynamic**: The switch will delete the MAC addresses that are not used or updated within the aging time. It is the default setting. **Static**: The learned MAC addresses are out of the influence of the aging time and can only be deleted manually. The learned entries will be cleared after the switch is rebooted. **Permanent**: The learned MAC addresses are out of the influence of the aging time and can only be deleted manually. The learned entries will be saved even the switch is rebooted.

3) Select the status of the port security feature.

Status	Select the status of Port Security. Three kinds of status can be selected: **Drop**: When the number of learned MAC addresses reaches the limit, the port will stop learning and discard the packets with the MAC addresses that have not been learned. **Forward**: When the number of learned MAC addresses reaches the limit, the port will stop learning but send the packets with the MAC addresses that have not been learned. **Disable**: The number limit on the port is not effective, and the switch follows the original forwarding rules. It is the default setting.

4) Click **Apply**.

Note:

- Port Security cannot be enabled on the member port of a LAG, and the port with Port Security enabled cannot be added to a LAG.
- On one port, Port Security and 802.1X cannot be enabled at the same time.

4.2 Using the CLI

Follow these steps to configure Port Security:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **}** Enter interface configuration mode.

Step 3	**mac address-table max-mac-count { [max-number** *num***] [mode** { dynamic | static | permanent } **] [status** { forward | drop | disable } **] }** Enable the port security feature of the port and configure the related parameters. *num*: The maximum number of MAC addresses that can be learned on the port. The valid values are from 0 to 64. The default value is 64. **mode**: Learn mode of the MAC address. There are three modes: dynamic: The switch will delete the MAC addresses that are not used or updated within the aging time. static: The learned MAC addresses are out of the influence of the aging time and can only be deleted manually. The learned entries will be cleared after the switch is rebooted. permanent: The learned MAC address is out of the influence of the aging time and can only be deleted manually. The learned entries will be saved even the switch is rebooted. **status**: Status of port security feature. By default, it is disabled. drop: When the number of learned MAC addresses reaches the limit, the port will stop learning and discard the packets with the MAC addresses that have not been learned. forward: When the number of learned MAC addresses reaches the limit, the port will stop learning but send the packets with the MAC addresses that have not been learned. disable: The number limit on the port is not effective, and the switch follows the original forwarding rules. It is the default setting.
Step 4	**show mac address-table max-mac-count interface { fastEthernet** *port* **| gigabitEthernet** *port* **}** Verify the Port Security configuration and the current learned MAC addresses of the port.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set the maximum number of MAC addresses that can be learned on port 1/0/1 as 30 and configure the mode as permanent and the status as drop:

Switch#configure

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

Switch(config-if)#mac address-table max-mac-count max-number 30 **mode** permanent **status** drop

Switch(config-if)#show mac address-table max-mac-count interface gigabitEthernet 1/0/1

Port	Max-learn	Current-learn	Mode	Status
----	---------	-----------	------	------
Gi1/0/1	30	0	permanent	drop

Switch(config-if)#end

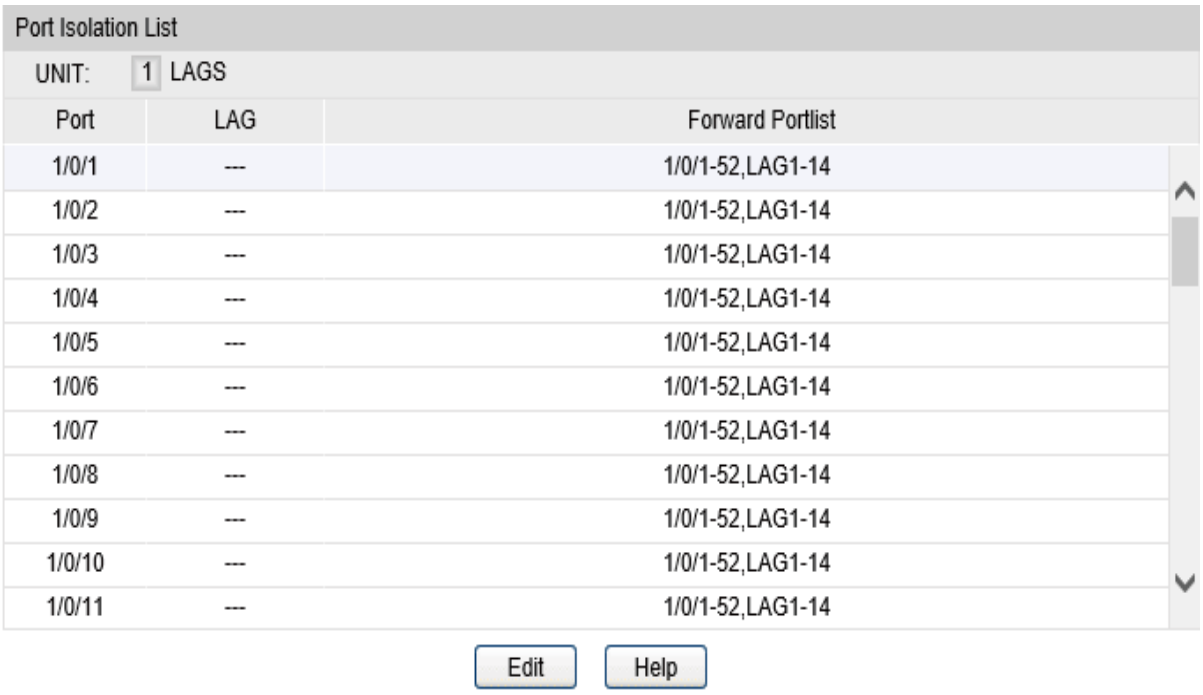
Switch#copy running-config startup-config

5 Port Isolation Configurations

5.1 Using the GUI

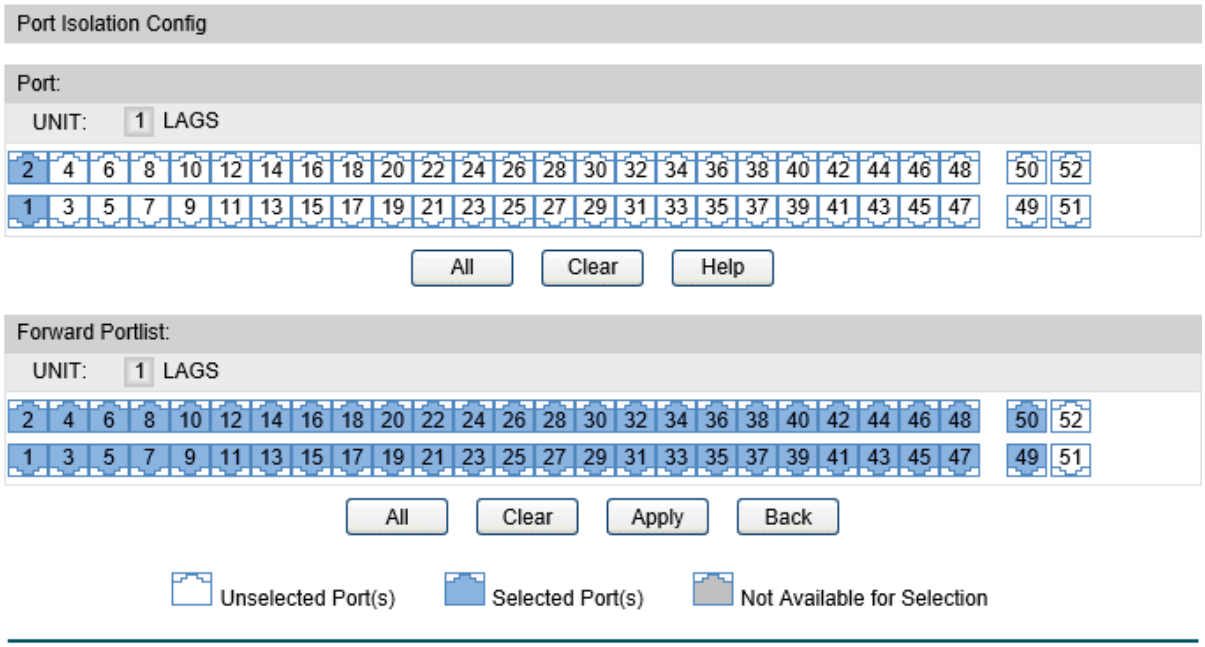
Choose the menu **Switching > Port > Port Isolation** to load the following page.

Figure 5-1 Port Isolation List



The above page displays the port isolation list. Click **Edit** to configure Port Isolation on the following page.

Figure 5-2 Port Isolation



Follow these steps to configure Port Isolation:

1) In the **Port** section, select one or multiple ports to be isolated.
2) In the **Forward Portlist** section, select the forward ports or LAGs which the isolated ports can only communicate with. It is multi-optional.
3) Click **Apply**.

5.2 Using the CLI

Follow these steps to configure Port Isolation:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list***}** Enter interface configuration mode.
Step 3	**port isolation { [gi-forward-list** *gi-forward-list***] [po-forward-list** *po-forward-list* **] }** Specify ports or LAGs to the forward list of the specific port which can only communicate with the forward ports or LAGs. It is multi-optional. *gi-forward-list*: The list of Ethernet ports. *po-forward-list:* The list of LAGs.
Step 4	**show port isolation interface { fastEthernet** *port* **| gigabitEthernet** *port* **}** Verify the Port Isolation configuration of the specified port.
Step 5	**end** Return to privileged EXEC mode.

Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to add ports 1/0/1-3 and LAG 4 to the forward list of port 1/0/5:

Switch#configure

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

Switch(config-if)#port isolation gi-forward-list 1/0/1-3 **po-forward-list** 4

Switch(config-if)#show port isolation interface gigabitEthernet 1/0/5

Port LAG Forward-List

---- --- ----------

Gi1/0/5 N/A Gi1/0/1-3,Po4

Switch(config-if)#end

Switch#copy running-config startup-config

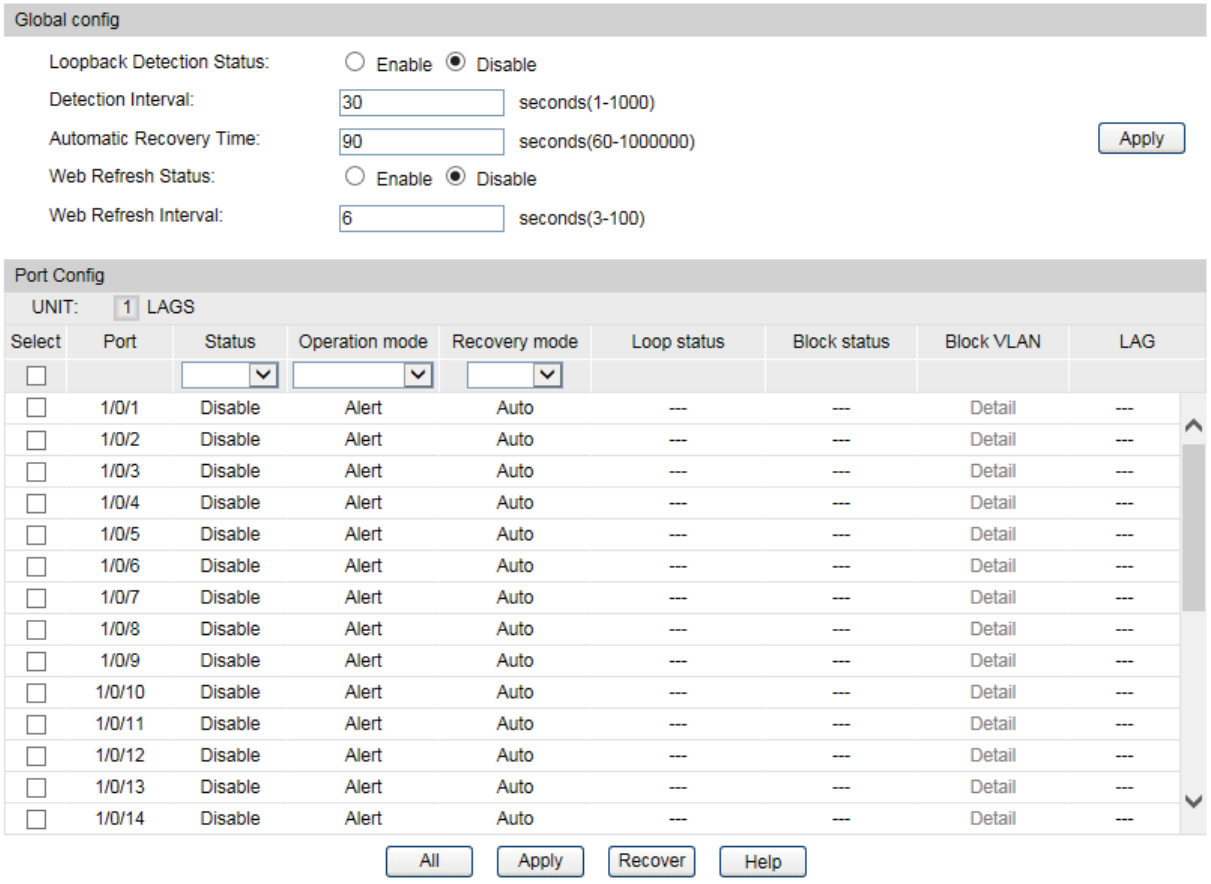
6 Loopback Detection Configuration

6.1 Using the GUI

To avoid broadcast storm, we recommend that you enable storm control before loopback detection is enabled. For detailed introductions about storm control, refer to *Configuring QoS*.

Choose the menu **Switching > Port > Loopback Detection** to load the following page.

Figure 6-1 Loopback Detection



Follow these steps to configure loopback detection:

1) In the **Global Config** section, enable loopback detection and configure the global parameters. Then click **Apply**.

Loopback Detection Status	Enable loopback detection globally.
Detection Interval	Set the interval of sending loopback detection packets. The valid values are from 1 to 1000 seconds and the default value is 30 seconds.

Automatic Recovery Time	Set the recovery time globally, after which the blocked port/VLAN in Auto Recovery mode can automatically recover to normal status. The valid values are from 60 to 1000000 seconds and the default value is 90 seconds.
Web Refresh Status	With this option enabled, the switch refreshes the web timely. By default, it is disabled.
Web Refresh Interval	If you enabled web refresh, set the refresh interval between 3 and 100 seconds. The default value is 6 seconds.

2) In the **Port Config** section, select one or multiple ports for configuration. Then set the parameters and click **Apply**.

Status	Enable loopback detection for the port.
Operation Mode	Select the operation mode when a loop is detected on the port: **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 totally block the port on which the loop is detected and no packets can pass through the port. **VLAN Based**: When a loop is detected, the switch will send a trap message and generate an entry on the log file. In addition, the switch will block the VLAN in which the loop is detected and only the packets of the blocked VLAN cannot pass through the port.
Recovery Mode	If you select **Port Based** or **VLAN Based** as the operation mode, you also need to configure the recovery mode for the blocked port/VLAN: **Auto**: The blocked port/VLAN will automatically recover to normal status after the automatic recovery time. It is the default setting. **Manual**: You need to manually release the blocked port/VLAN. Click the **Recover** button to release the corresponding port/VLAN.

3) View the loopback detection information on this page.

Loop Status	Displays whether a loop is detected on the port.
Block Status	Displays whether the port is blocked.
Block VLAN	Click **Detail** to view the information about the blocked VLAN.

6.2 Using the CLI

Follow these steps to configure Loopback Detection:

Step 1	**configure** Enter global configuration mode.
Step 2	**loopback-detection** Enable the loopback detection feature globally. By default, it is disabled.
Step 3	**loopback-detection interval** *interval-time* Set the interval of sending loopback detection packets which is used to detect the loops in the network. *interval-time:* The interval of sending loopback detection packets. The valid values are from 1 to 1000 seconds. By default, the value is 30 seconds.
Step 4	**loopback-detection recovery-time** *recovery-time* Set the recovery time, after which the blocked port in Auto Recovery mode can automatically recover to normal status. *recovery-time*: It is integral times of detection interval, ranging from 1 to 100. The default value is 3.
Step 5	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **}** Enter interface configuration mode.
Step 6	**loopback-detection** Enable loopback detection of the port. By default, it is disabled.
Step 7	**loopback-detection config process-mode {** alert | port-based | vlan-based **} [recovery-mode {** auto | manual **}]** Set the process mode when a loopback is detected on the port. There are three modes: 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 totally 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. Set the recovery mode for the blocked port. There are two modes: auto: After the recovery time, the blocked port/VLAN will automatically recover to normal status and restart to detect loops in the network. manual: The blocked port/VLAN can only be released manually. You can use the command **loopback-detection recover** under interface configuration mode to recover the blocked port/VLAN to normal status.
Step 9	**show loopback-detection global** Verify the global configuration of Loopback Detection.

Step 10	**show loopback-detection interface { fastEthernet** *port* **| gigabitEthernet** *port* **}** Verify the Loopback Detection configuration of the specified port.
Step 11	**end** Return to privileged EXEC mode.
Step 12	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable loopback detection globally (keeping the default parameters):

Switch#configure

Switch(config)#loopback-detection

Switch(config)#show loopback-detection global

Loopback detection global status : enable

Loopback detection interval : 30 s

Loopback detection recovery time : 90 s

Switch(config-if)#end

Switch#copy running-config startup-config

The following example shows how to enable loopback detection of port 1/0/3 and set the process mode as alert and recovery mode as auto:

Switch#configure

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

Switch(config-if)#loopback-detection

Switch(config-if)#loopback-detection config process-mode alert **recovery-mode** auto

Switch(config-if)#show loopback-detection interface gigabitEthernet 1/0/3

Port	Enable	Process Mode	Recovery Mode	Loopback	Block	LAG
----	------	----------	----------	--------	-----	----
Gi1/0/3	enable	alert	auto	N/A	N/A	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

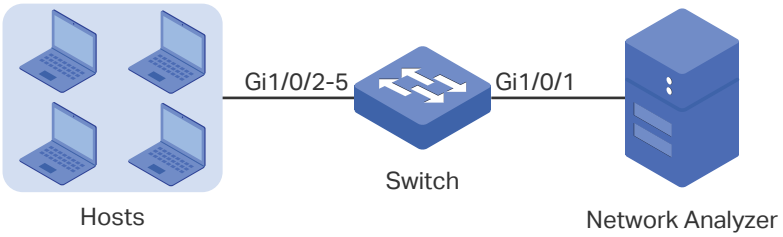
7 Configuration Examples

7.1 Example for Port Mirror

7.1.1 Network Requirements

As shown below, several hosts and a network analyzer are directly connected to the switch. For network security and troubleshooting, the network manager needs to use the network analyzer to monitor the data packets from the end hosts.

Figure 7-1 Network Topology



7.1.2 Configuration Scheme

To implement this requirement, you can configure port mirror to copy the packets from ports 1/0/2-5 to port 1/0/1. The overview of configuration is as follows:

1) Specify ports 1/0/2-5 as the source ports, allowing the switch to copy the packets from the hosts.
2) Specify port 1/0/1 as the destination port so that the network analyzer can receive mirrored packets from the hosts.

Demonstrated with T2600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

7.1.3 Using the GUI

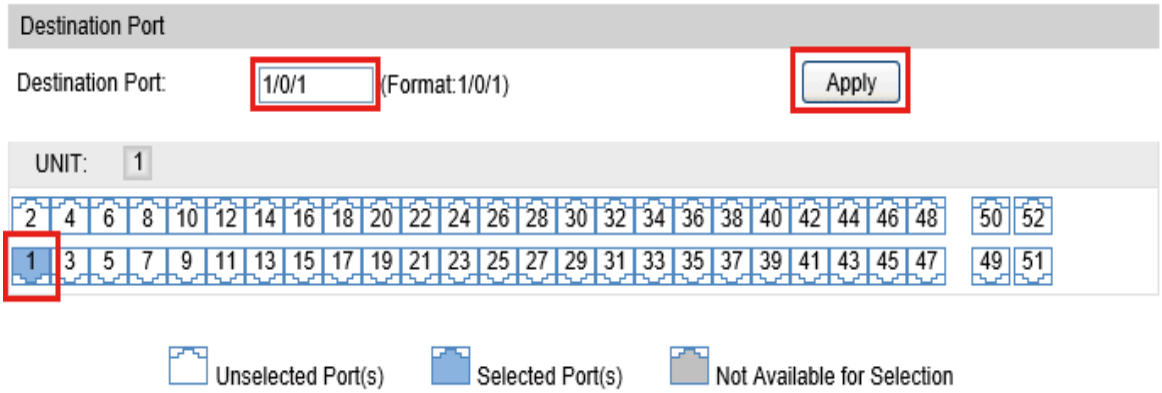
1) Choose the menu **Switching > Port > Port Mirror** to load the following page. It displays the information of the mirror session.

Figure 7-2 Mirror Session List



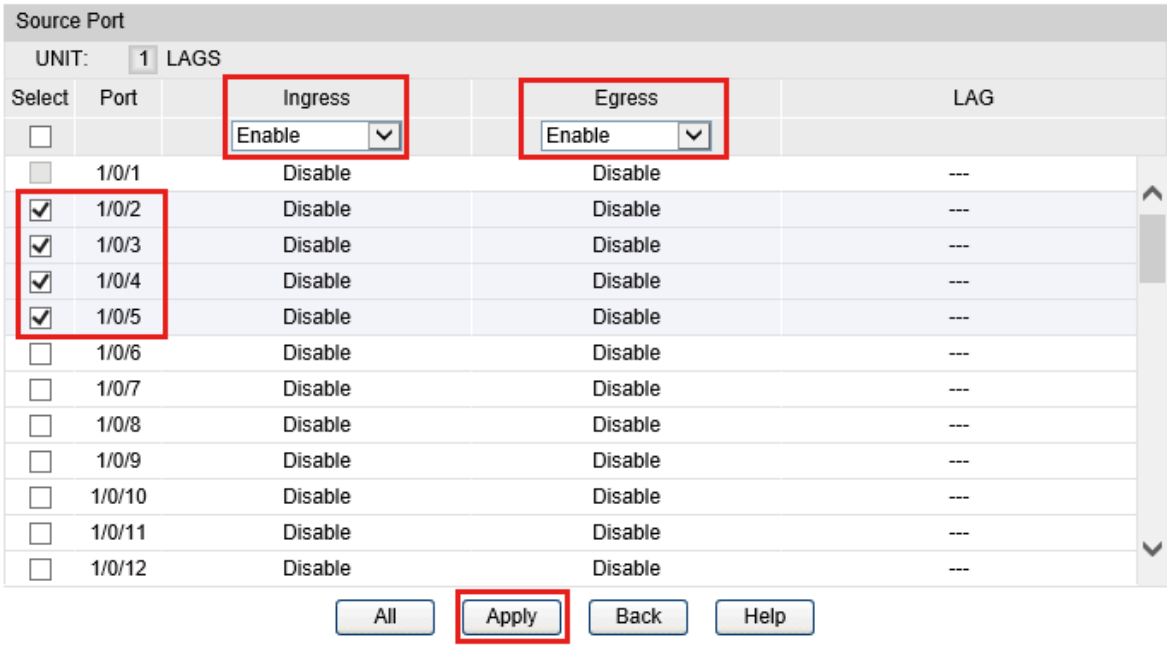
2) Click **Edit** on the above page to load the following page. In the **Destination Port** section, select port 1/0/1 as the monitoring port and click **Apply**.

Figure 7-3 Destination Port Configuration



3) In the **Source Port** section, select ports 1/0/2-5 as the monitored ports, and enable **Ingress** and **Egress** to allow the received and sent packets to be copied to the monitoring port. Then click **Apply.**

Figure 7-4 Source Port Configuration



4) Click **Save Config** to save the settings.

7.1.4 Using the CLI

Switch#configure

Switch(config)#monitor session 1 destination interface gigabitEthernet 1/0/1

Switch(config)#monitor session 1 source interface gigabitEthernet 1/0/2-5 both

Switch(config)#end

Switch#copy running-config startup-config

Verify the Configuration

Switch#show monitor session 1

Monitor Session: 1

Destination Port: Gi1/0/1

Source Ports(Ingress): Gi1/0/2-5

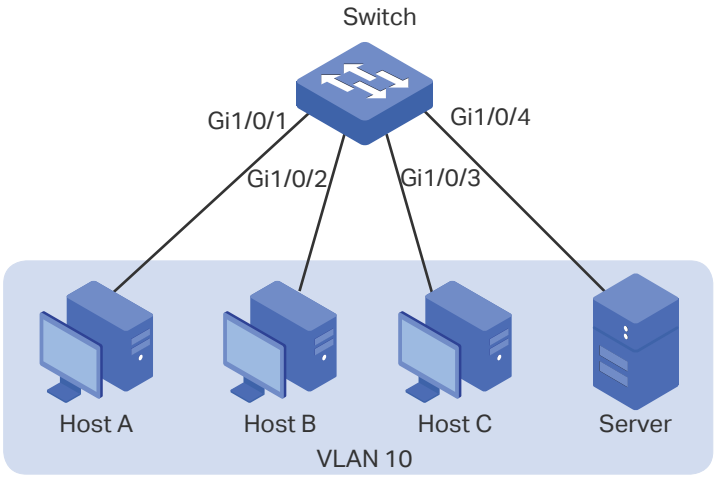
Source Ports(Egress): Gi1/0/2-5

7.2 Example for Port Isolation

7.2.1 Network Requirements

As shown below, three hosts and a server are connected to the switch and all belong to VLAN 10. With the VLAN configuration unchanged, Host A is not allowed to communicate with the other hosts except the server, even if the MAC address or IP address of Host A is changed.

Figure 7-5 Network Topology



7.2.2 Configuration Scheme

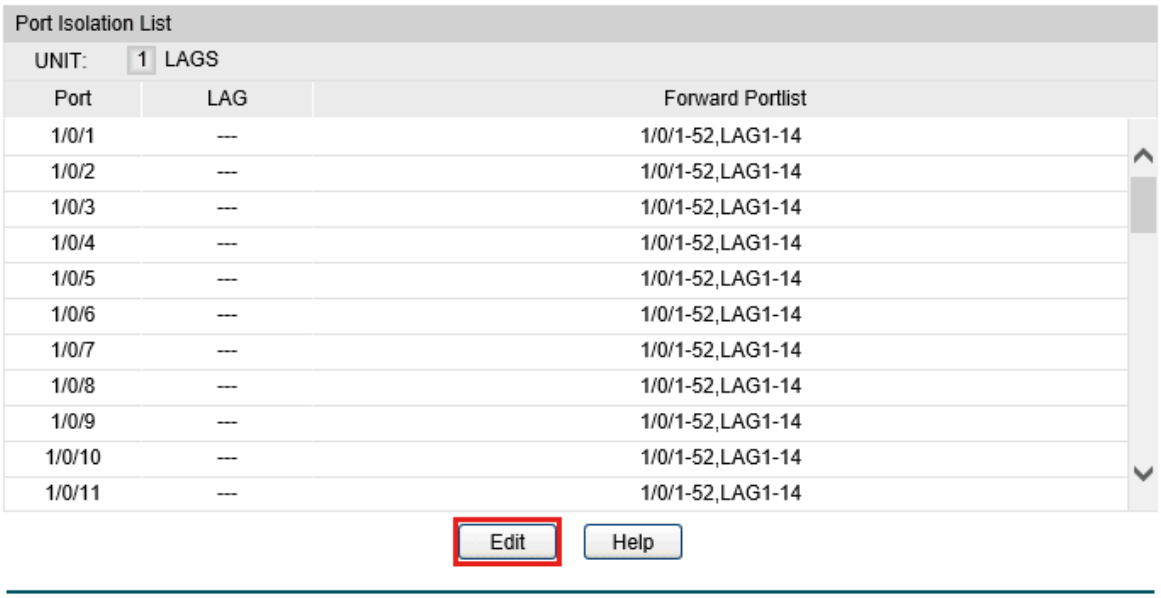
You can configure port isolation to implement the requirement. Set 1/0/4 as the only forwarding port for port 1/0/1, thus forbidding Host A to forward packets to the other hosts.

Demonstrated with T2600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

7.2.3 Using the GUI

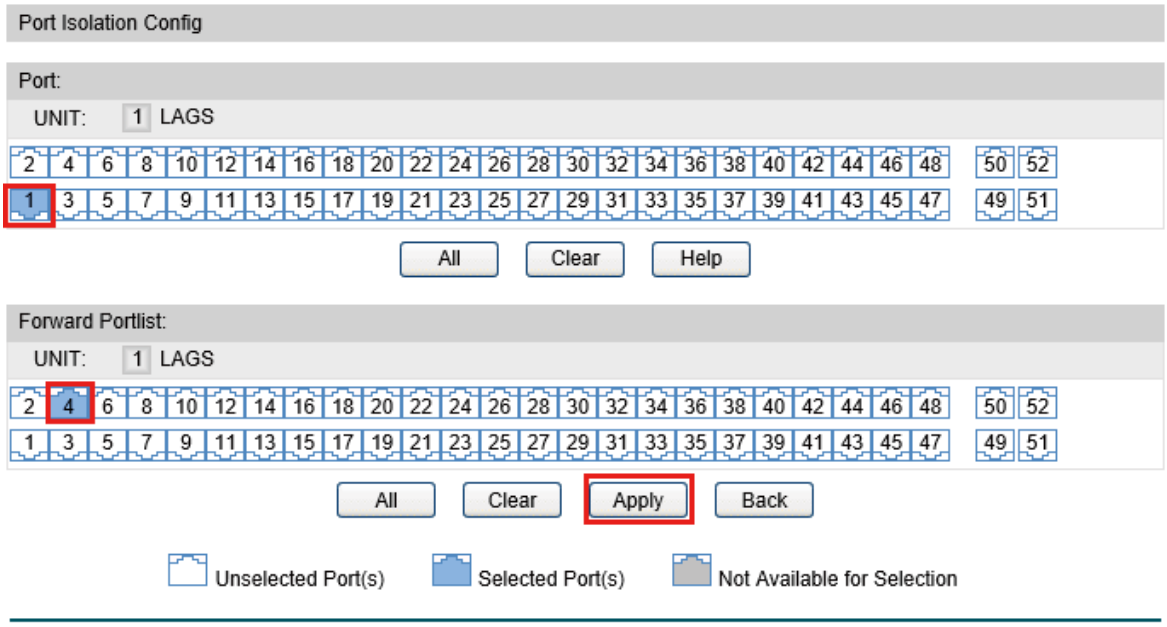
1) Choose the menu **Switching > Port > Port Isolation** to load the following page. It displays the port isolation list.

Figure 7-6 Port Isolation List



2) Click **Edit** on the above page to load the following page. Select port 1/0/1 as the isolated port, and select port 1/0/4 as the forwarding port. Click **Apply**.

Figure 7-7 Port Isolation Configuration



3) Click **Save Config** to save the settings.

7.2.4 Using the CLI

Switch#configure

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

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

Switch(config-if)#end

Switch#copy running-config startup-config

Verify the Configuration

Switch#show port isolation interface

Port	LAG	Forward-List
Gi1/0/1	N/A	Gi1/0/4
Gi1/0/2	N/A	Gi1/0/1-52,Po1-14
Gi1/0/3	N/A	Gi1/0/1-52,Po1-14

...

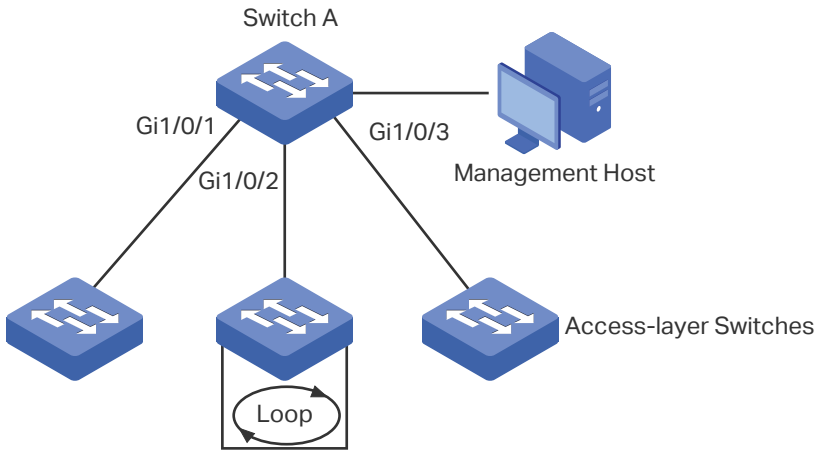
7.3 Example for Loopback Detection

7.3.1 Network Requirements

As shown below, Switch A is a convergence-layer switch connecting several access-layer switches. Loops can be easily caused in case of misoperation on the access-layer switches. If there is a loop on an access-layer switch, broadcast storms will occur on Switch A or even in the entire network, creating excessive traffic and degrading the network performance.

To reduce the impacts of broadcast storms, users need to detect loops in the network via Switch A and timely block the port on which a loop is detected.

Figure 7-8 Network Topology



7.3.2 Configuration Scheme

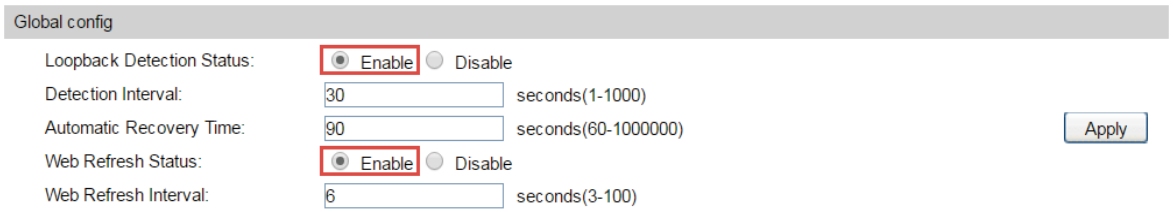
Enable loopback detection on ports 1/0/1-3 and configure SNMP to receive the notifications. For detailed instructions about SNMP, refer to *Configuring SNMP & RMON*. Here we introduce how to configure loopback detection and monitor the detection result on the management interface of the switch.

Demonstrated with T2600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

7.3.3 Using the GUI

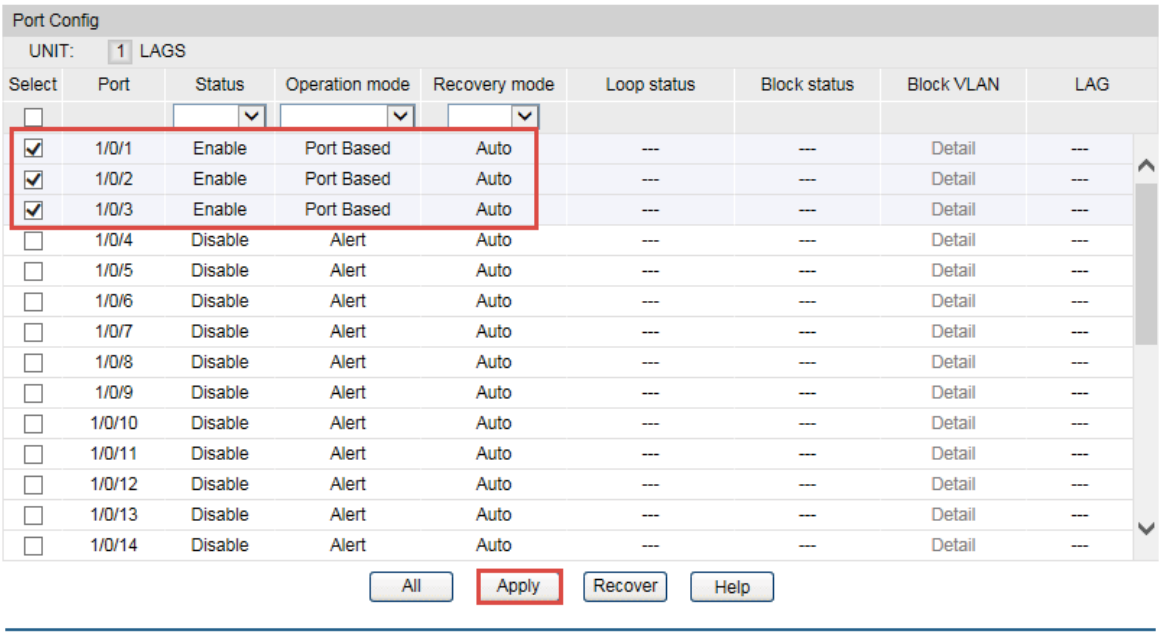
1) Choose the menu **Switching > Port > Loopback Detection** to load the configuration page.
2) In the **Global Config** section, enable loopback detection and web refresh globally. Keep the default parameters and click **Apply**.

Figure 7-9 Global Configuration



3) In the **Port Config** section, enable ports 1/0/1-3, select the operation mode as **Port based** so that the port will be blocked when a loop is detected, and keep the recovery mode as **Auto** so that the port will recover to normal status after the automatic recovery time. Click **Apply**.

Figure 7-10 Port Configuration



4) Monitor the detection result on the above page. The **Loop status** and **Block status** are displayed on the right side of ports.

7.3.4 Using the CLI

1) Enable loopback detection globally and configure the detection interval and recovery time.

Switch#configure

Switch(config)#loopback-detection

Switch(config)#loopback-detection interval 30

Switch(config)#loopback-detection recovery-time 90

2) Enable loopback detection on ports 1/0/1-3 and set the process mode and recovery mode.

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

Switch(config-if)#loopback-detection

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

Switch(config-if)#end

Switch#copy running-config startup-config

Verify the Configuration

Verify the global configuration:

Switch#show loopback-detection global

Loopback detection global status : enable

Loopback detection interval: 30 s

Loopback detection recovery time : 90 s

Verify the loopback detection configuration on ports:

Switch#show loopback-detection interface

Port	Enable	Process Mode	Recovery Mode	Loopback	Block	LAG
----	--------	----------	----------	----------	-- ----	-----
Gi1/0/1	enable	port-based	auto	N/A	N/A	N/A
Gi1/0/2	enable	port-based	auto	N/A	N/A	N/A
Gi1/0/3	enable	port-based	auto	N/A	N/A	N/A

...

8 Appendix: Default Parameters

Default settings of Switching are listed in th following tables.

Table 8-1 Configurations for Ports

Parameter	Default Setting
Port Config	
Type	Copper
Status	Enable
Speed	Auto
Duplex	Auto
Flow Control	Disable
Jumbo	Disable
Port Mirror	
Ingress	Disable
Egress	Disable
Port Security	
Max Learned MAC	64
Learned Num	0
Learned Mode	Dynamic
Status	Disable
Loopback Detection	
Loopback Detection Status	Disable
Detection Interval	30 seconds
Automatic Recovery Time	90 seconds
Web Refresh Status	Disable
Web Refresh Interval	6 seconds

Parameter	Default Setting
Port Status	Disable
Operation mode	Alert
Recovery mode	Auto

Part 4

Configuring LAG

CHAPTERS

1. LAG
2. LAG Configuration
3. Configuration Example
4. Appendix: Default Parameters

1 LAG

1.1 Overview

With LAG (Link Aggregation Group) function, you can aggregate multiple physical ports into a logical interface to increase link bandwidth and configure the backup ports to enhance the connection reliability.

1.2 Supported Features

You can configure LAG in two ways: static LAG and LACP (Link Aggregation Control Protocol).

Static LAG

The member ports are manually added to the LAG.

LACP

The switch uses LACP to implement dynamic link aggregation and disaggregation by exchanging LACP packets with its partner. LACP extends the flexibility of the LAG configuration.

2 LAG Configuration

To complete LAG configuration, follow these steps:

1) Configure the global load-balancing algorithm.
2) Configure Static LAG or LACP.

Configuration Guidelines

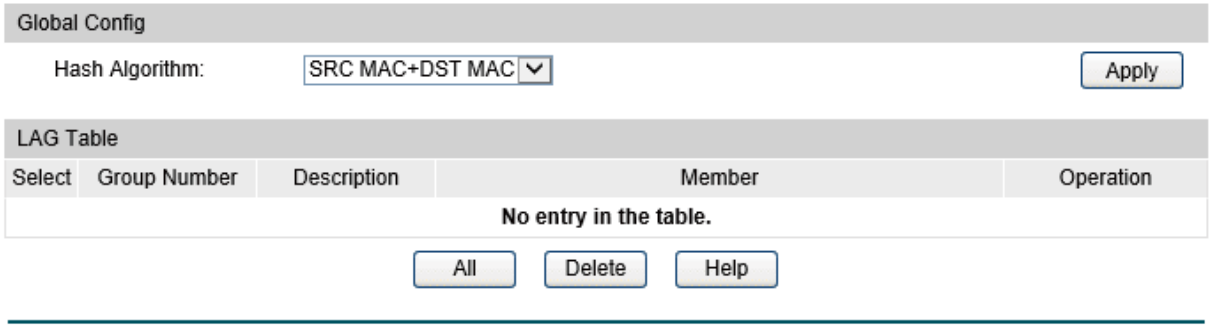
- Ensure that both ends of the aggregation link work in the same LAG mode. For example, if the local end works in LACP mode, the peer end should be set as LACP mode.
- Ensure that devices on both ends of the aggregation link use the same number of physical ports with the same speed, duplex, jumbo and flow control mode.
- A port cannot be added to more than one LAG at the same time.
- LACP does not support half-duplex links.
- One static LAG supports up to eight member ports. All the member ports share the traffic evenly. If an active link fails, the other active links share the traffic evenly.
- One LACP LAG supports more than eight member ports, but at most eight of them can be active. Using LACP protocol, the switches negotiate parameters and determine the active ports. When an active link fails, the link with the highest priority among the inactive links will replace the faulty link and start to forward data.
- For the functions like IGMP Snooping, 802.1Q VLAN, MAC VLAN, Protocol VLAN, VLAN-VPN, GVRP, Voice VLAN, STP, QoS, DHCP Snooping and Flow-Control, the member pot of an LAG follows the configuration of the LAG but not its own. The configurations of the port can take effect only after it leaves the LAG.
- The port which is enabled with Port Security, Port Mirror, MAC Address Filtering or 802.1X cannot be added to LAG, and the member port of an LAG cannot be enabled with these functions.

2.1 Using the GUI

2.1.1 Configuring Load-balancing Algorithm

Choose the menu **Switching > LAG > LAG Table** to load the following page.

Figure 2-1 Global Config



In the **Global Config** section, select the load-balancing algorithm. Click **Apply**.

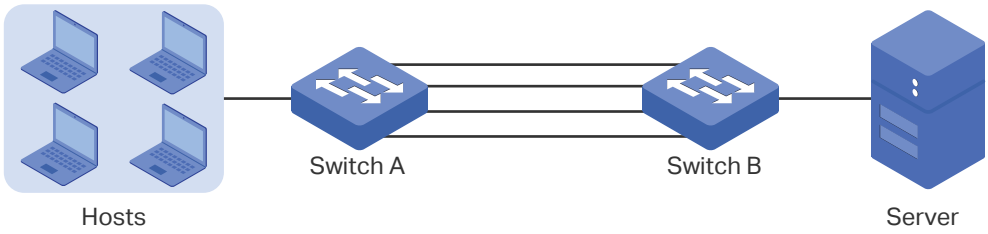
Hash Algorithm	Select the Hash Algorithm, based on which the switch can choose the port to send the received packets. In this way, different data flows are forwarded on different physical links to implement load balancing. There are six options: **SRC MAC**: The computation is based on the source MAC addresses of the packets. **DST MAC**: The computation is based on the destination MAC addresses of the packets. **SRC MAC+DST MAC**: The computation is based on the source and destination MAC addresses of the packets. **SRC IP**: The computation is based on the source IP addresses of the packets. **DST IP**: The computation is based on the destination IP addresses of the packets. **SRC IP+DST IP**: The computation is based on the source and destination IP addresses of the packets.

Tips:

- Load-balancing algorithm is effective only for outgoing traffic. If the data stream is not well shared by each link, you can change the algorithm of the outgoing interface.

- Please properly choose the load-balancing algorithm to avoid data stream transferring only on one physical link. For example, Switch A receives packets from several hosts and forwards them to the Server with the fixed MAC address and IP address, you can set the algorithm as "SRC MAC+SRC IP" to allow Switch A to determine the forwarding port based on the source MAC addresses and source IP addresses of the received packets.

Figure 2-2 Hash Algorithm Configuration



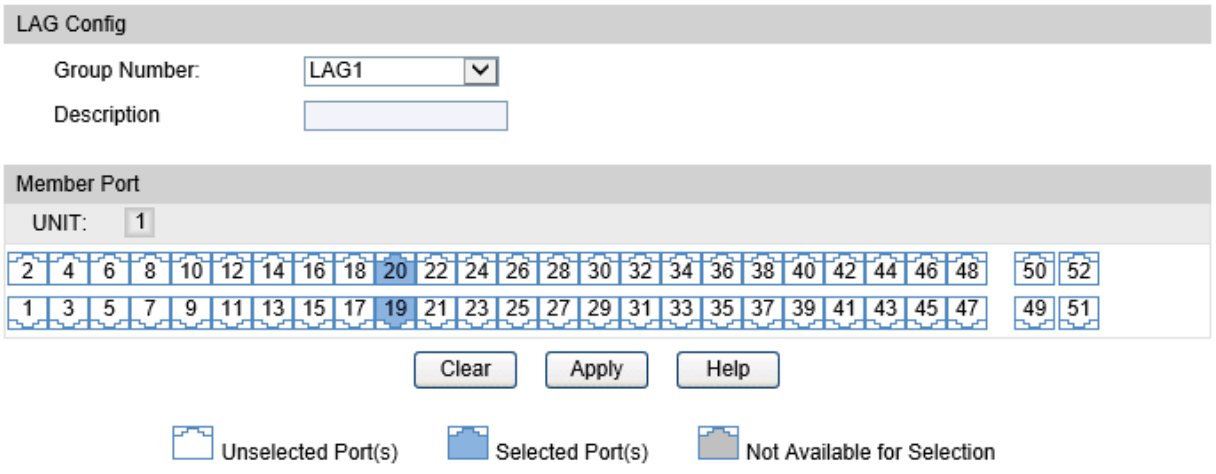
2.1.2 Configuring Static LAG or LACP

For one port, you can choose only one LAG mode: Static LAG or LACP. And make sure both ends of a link use the same LAG mode.

■ Configuring Static LAG

Choose the menu **Switching > LAG > Static LAG** to load the following page.

Figure 2-3 Static LAG



Follow these steps to configure the static LAG:

1) In the **LAG Config** section, select an LAG for configuration.

Group Number	Select an LAG for static LAG configuration.
Description	Displays the LAG mode.

2) In the **Member Port** section, select the member ports for the LAG. It is multi-optional.

3) Click **Apply**.

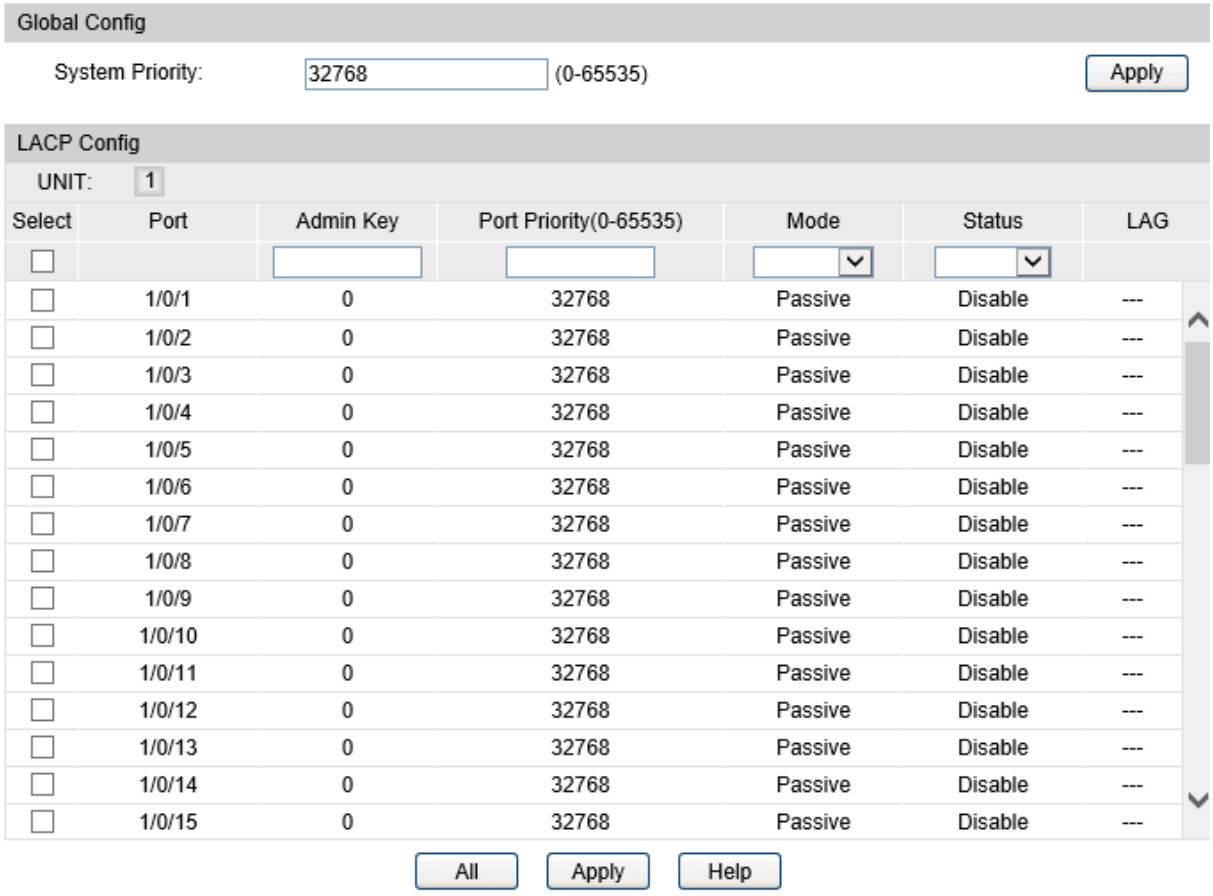
Note:

Clearing all member ports will delete the LAG.

Configuring LACP

Choose the menu **Switching > LAG > LACP** to load the following page.

Figure 2-4 LACP Config



Follow these steps to configure LACP:

1) Specify the system priority for the switch and click **Apply**.

System Priority	Specify the system priority for the switch. A smaller value means a higher priority. To keep active ports consistent at both ends, you can set the priority of one device to be higher than that of the other device. The device with higher priority will determine its active ports, and the other device can select its active ports according to the selection result of the device with higher priority. If the two ends have the same system priority value, the end with a smaller MAC address has the higher priority.

2) Select member ports for the LAG and configure the related parameters. Click **Apply**.

Admin Key	Specify the Admin Key which you can regard as the group number of the LAG. Note that the group number of other static LAGs cannot be set as an Admin Key. The valid value of the Admin Key is determined by the maximum number of LAG supported by your switch. For example, if your switch supports up to 14 LAGs, the valid value is from 1 to 14.

Port Priority (0-65535)	Specify the Port Priority. A smaller value means a higher port priority. The port with higher priority in an LAG will be selected as the active port to forward data. If two ports have the same priority value, the port with a smaller port number has the higher priority.
Mode	Select the LACP mode for the port. In LACP, the switch uses LACPDU (Link Aggregation Control Protocol Data Unit) to negotiate the parameters with the peer end. In this way, the two ends select active ports and form the aggregation link. The LACP mode determines whether the port will take the initiative to send the LACPDU. There are two modes: **Passive**: The port will not send LACPDU before receiving the LACPDU from the peer end. **Active**: The port will take the initiative to send LACPDU.
Status	Enable the LACP function of the port. By default, it is disabled.

2.2 Using the CLI

2.2.1 Configuring Load-balancing Algorithm

Follow these steps to configure the load-balancing algorithm:

Step 1	**configure** Enter global configuration mode.
Step 2	**port-channel load-balance {** src-mac | dst-mac | src-dst-mac | src-ip | dst-ip | src-dst-ip **}** Select the Hash Algorithm. The switch will choose the ports to transfer the packets based on the Hash Algorithm. In this way, different data flows are forwarded on different physical links to implement load balancing. src-mac: The computation is based on the source MAC addresses of the packets. dst-mac: The computation is based on the destination MAC addresses of the packets. src-dst-mac: The computation is based on the source and destination MAC addresses of the packets. src-ip: The computation is based on the source IP addresses of the packets. dst-ip: The computation is based on the destination IP addresses of the packets. src-dst-ip: The computation is based on the source and destination IP addresses of the packets.
Step 3	**show etherchannel load-balance** Verify the configuration of load-balancing algorithm.

Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set the global load-balancing mode as src-dst-mac:

Switch#configure

Switch(config)#port-channel load-balance src-dst-mac

Switch(config)#show etherchannel load-balance

EtherChannel Load-Balancing Configuration: src-dst-mac

EtherChannel Load-Balancing Addresses Used Per-Protocol:

Non-IP: Source XOR Destination MAC address

IPv4: Source XOR Destination MAC address

IPv6: Source XOR Destination MAC address

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Configuring Static LAG or LACP

You can choose only one LAG mode for a port: Static LAG or LACP. And make sure both ends of a link use the same LAG mode.

- Configuring Static LAG

Follow these steps to configure static LAG:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **}** Enter interface configuration mode.
Step 3	**channel-group** *num* **mode {** on | active | passive **}** Add the port to a static LAG. *num*: The group number of the LAG. **mode**:LAG mode. Select on to add the port to a static LAG. Active and passive are two LACP modes.

Step 4	**show ether-channel** *num* **summary** Verify the configuration of the static LAG. *num*: The group number of the LAG.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to add ports1/0/5-8 to LAG 2 and set the mode as static LAG:

Switch#configure

Switch(config)#interface range gigabitEthernet 1/0/5-8

Switch(config-if-range)#channel-group 2 **mode** on

Switch(config-if-range)#show etherchannel 2 **summary**

Flags: D - down P - bundled in port-channel U - in use

I - stand-alone H - hot-standby(LACP only) s - suspended

R - layer3 S - layer2 f - failed to allocate aggregator

u - unsuitable for bundling w - waiting to be aggregated d - default port

Group	Port-channel	Protocol	Ports
2	Po2(S)	-	Gi1/0/5(D) Gi1/0/6(D) Gi1/0/7(D) Gi1/0/8(D)

Switch(config-if-range)#end

Switch#copy running-config startup-config

Configuring LACP

Follow these steps to configure LACP:

Step 1	**configure** Enter global configuration mode.

Step 2	**lacp system-priority** *pri* Specify the system priority for the switch. To keep active ports consistent at both ends, you can set the priority of one device to be higher than that of the other device. The device with higher priority will determine its active ports, and the other device can select its active ports according to the selection result of the device with higher priority. If the two ends have the same system priority value, the end with a smaller MAC address has the higher priority. pri: System priority. The valid values are from 0 to 65535, and the default value is 32768. A smaller value means a higher device priority.
Step 3	**interface {fastEthernet** *port* | *r***ange fastEthernet** *port-list* | **gigabitEthernet** *port* | **range gigabitEthernet** *port-list* **}** Enter interface configuration mode.
Step 4	**channel-group** *num* **mode {** on | active | passive **}** Add the port to an LAG and set the mode as LACP. *num*: The group number of the LAG. **mode**: LAG mode. Here you need to select LACP mode: active or passive. In LACP, the switch uses LACPDU (Link Aggregation Control Protocol Data Unit) to negotiate the parameters with the peer end. In this way, the two ends select active ports and form the aggregation link. The LACP mode determines whether the port will take the initiative to send the LACPDU. on: Enable LACP function on the port. passive: The port will not send LACPDU before receiving the LACPDU from the peer end. active: The port will take the initiative to send LACPDU.
Step 5	**lacp port-priority** *pri* Specify the Port Priority. The port with higher priority in an LAG will be selected as the active port. If two ports have the same priority value, the port with a smaller port number has the higher priority. pri: Port priority. The valid values are from 0 to 65535, and the default value is 32768. A smaller value means a higher port priority.
Step 6	**show lacp sys-id** Verify the global system priority.
Step 7	**show lacp internal** Verify the LACP configuration of the local switch.
Step 8	**end** Return to privileged EXEC mode.
Step 9	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to specify the system priority of the switch as 2:

Switch#configure

Switch(config)#lacp system-priority 2

Switch(config)#show lacp sys-id

2, 000a.eb13.2397

Switch(config)#end

Switch#copy running-config startup-config

The following example shows how to add ports 1/0/1-4 to LAG 6, set the mode as LACP, and select the LACPDU sending mode as active:

Switch#configure

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

Switch(config-if-range)#channel-group 6 **mode** active

Switch(config-if-range)#show lacp internal

Flags: S - Device is requesting Slow LACPDUs

F - Device is requesting Fast LACPDUs

A - Device is in active mode

P - Device is in passive mode

Channel group 6

Port	Flags	State	LACP Port Priority	Admin Key	Oper Key	Port Number	Port State
Gi1/0/1	SA	Up	32768	0x6	0x4b1	0x1	0x7d
Gi1/0/2	SA	Down	32768	0x6	0	0x2	0x45
Gi1/0/3	SA	Down	32768	0x6	0	0x3	0x45
Gi1/0/4	SA	Down	32768	0x6	0	0x4	0x45

Switch(config-if-range)#end

Switch#copy running-config startup-config

3 Configuration Example

3.1 Network Requirements

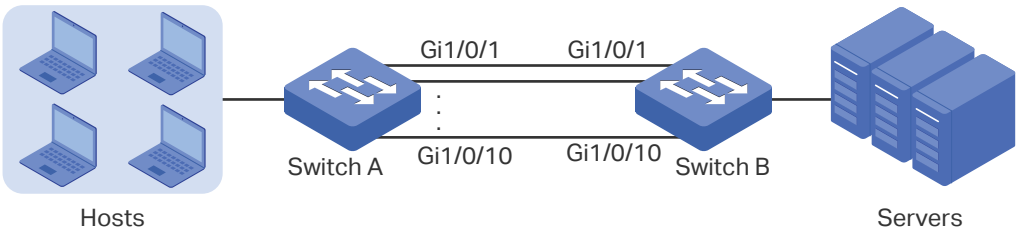
As shown below, users and servers are connected to Switch A and Switch B, and heavy traffic is transmitted between the two switches. To achieve high speed and reliability of data transmission, users need to improve the bandwidth and redundancy of the link between the two switches.

3.2 Configuration Scheme

LAG function can bundle multiple physical ports into one logical interface to increase bandwidth and improve reliability. In this case, we take LACP as an example.

As shown below, you can bundle up to eight physical ports into one logical aggregation group to transmit data on the two switches, and respectively connect the ports of the groups. In addition, another two redundant links can be set as the backup. To avoid traffic bottleneck between the servers and Switch B, you also need to configure LAG on them to increase link bandwidth. Here we mainly introduce the LAG configuration between the two switches.

Figure 3-1 Network Topology



The overview of the configuration is as follows:

1) Considering there are multiple devices on each end, configure the load-balancing algorithm as 'SRC MAC+DST MAC'.
2) Specify the system priority for the switches. Here we choose Switch A as the dominate device and specify a higher system priority for it.
3) Add ports 1/0/1-10 to the LAG and set the mode as LACP.
4) Specify a high port priority for ports 1/0/1-8 to set them as the active ports, and a low port priority for ports 1/0/9-10 to set them as the backup ports. When any of the active ports is down, the backup ports will be enabled to transmit data.

Demonstrated with T2600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

3.3 Using the GUI

The configurations of Switch A and Switch B are similar. The following introductions take Switch A as an example.

1) Choose the menu **Switching > LAG > LAG Table** to load the following page. Select the hash algorithm as 'SRC MAC+DST MAC'.

Figure 3-2 Global Configuration



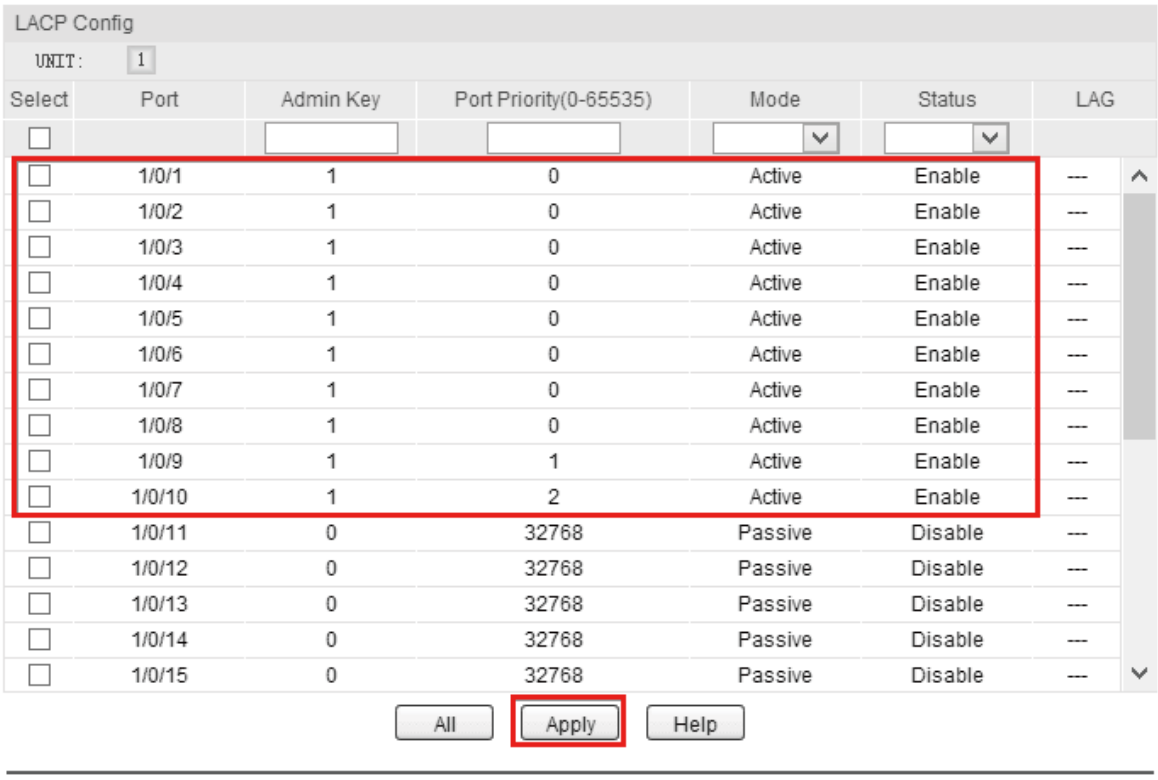
2) Choose the menu **Switching > LAG > LACP Config** to load the following page. In the **Global Config** section, specify the system priority of Switch A as **0** and Click **Apply**. Remember to ensure that the system priority value of Switch B is bigger than 0.

Figure 3-3 System Priority Configuration



3) In the **LACP Config** section, select ports 1/0/1-10, and respectively set the admin key, port priority, mode and status for each port as follows. Click **Apply**.

Figure 3-4 LACP Configuration



4) Click **Save Config** to save the settings.

3.4 Using the CLI

The configurations of Switch A and Switch B are similar. The following introductions take Switch A as an example.

1) Configure the load-balancing algorithm as "src-dst-mac".

   Switch#configure

   Switch(config)#port-channel load-balance src-dst-mac

2) Specify the system priority of Switch A as 0. Remember to ensure that the system priority value of Switch B is bigger than 0.

   Switch(config)#lacp system-priority 0

3) Add ports 1/0/1-8 to LAG 1 and set the mode as LACP. Then specify the port priority as 0 to make them active.

   Switch(config)#interface range gigabitEthernet 1/0/1-8

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

   Switch(config-if-range)#lacp port-priority 0

   Switch(config-if-range)#exit

4) Add port 1/0/9 to LAG 1 and set the mode as LACP. Then specify the port priority as 1 to set it as a backup port. When any of the active ports is down, this port will be preferentially selected to work as an active port.

   Switch(config)#interface gigabitEthernet 1/0/9

   Switch(config-if)#channel-group 1 mode active

   Switch(config-if)#lacp port-priority 1

   Switch(config-if)#exit

5) Add port 1/0/10 to LAG 1 and set the mode as LACP. Then specify the port priority as 2 to set it as a backup port. The priority of this port is lower than port 1/0/9.

   Switch(config)#interface gigabitEthernet 1/0/10

   Switch(config-if)#channel-group 1 mode active

   Switch(config-if)#lacp port-priority 2

   Switch(config-if)#end

   Switch#copy running-config startup-config

Verify the Configuration

Verify the system priority:

   Switch#show lacp sys-id

0, 000a.eb13.2397

Verify the LACP configuration:

Switch#show lacp internal

Flags: S - Device is requesting Slow LACPDUs

F - Device is requesting Fast LACPDUs

A - Device is in active mode

P - Device is in passive mode

Channel group 1

Port	Flags	State	LACP Port Priority	Admin Key	Oper Key	Port Number	Port State
Gi1/0/1	SA	Down	0	0x1	0	0x1	0x45
Gi1/0/2	SA	Down	0	0x1	0	0x2	0x45
Gi1/0/3	SA	Down	0	0x1	0	0x3	0x45
Gi1/0/4	SA	Down	0	0x1	0	0x4	0x45
Gi1/0/5	SA	Down	0	0x1	0	0x5	0x45
Gi1/0/6	SA	Down	0	0x1	0	0x6	0x45
Gi1/0/7	SA	Down	0	0x1	0	0x7	0x45
Gi1/0/8	SA	Down	0	0x1	0	0x8	0x45
Gi1/0/9	SA	Down	1	0x1	0	0x9	0x45
Gi1/0/10	SA	Down	2	0x1	0	0xa	0x45

4 Appendix: Default Parameters

Default settings of Switching are listed in the following tables.

Table 4-1 Default Settings of LAG

Parameter	Default Setting
LAG Table	
Hash Algorithm	SRC MAC+DST MAC
LACP Config	
System Priority	32768
Admin Key	0
Port Priority	32768
Mode	Passive
Status	Disable

Part 5

Monitoring Traffic

CHAPTERS

1. Traffic Monitor
2. Appendix: Default Parameters

1 Traffic Monitor

With Traffic Monitor function, you can monitor the traffic on the switch, including:

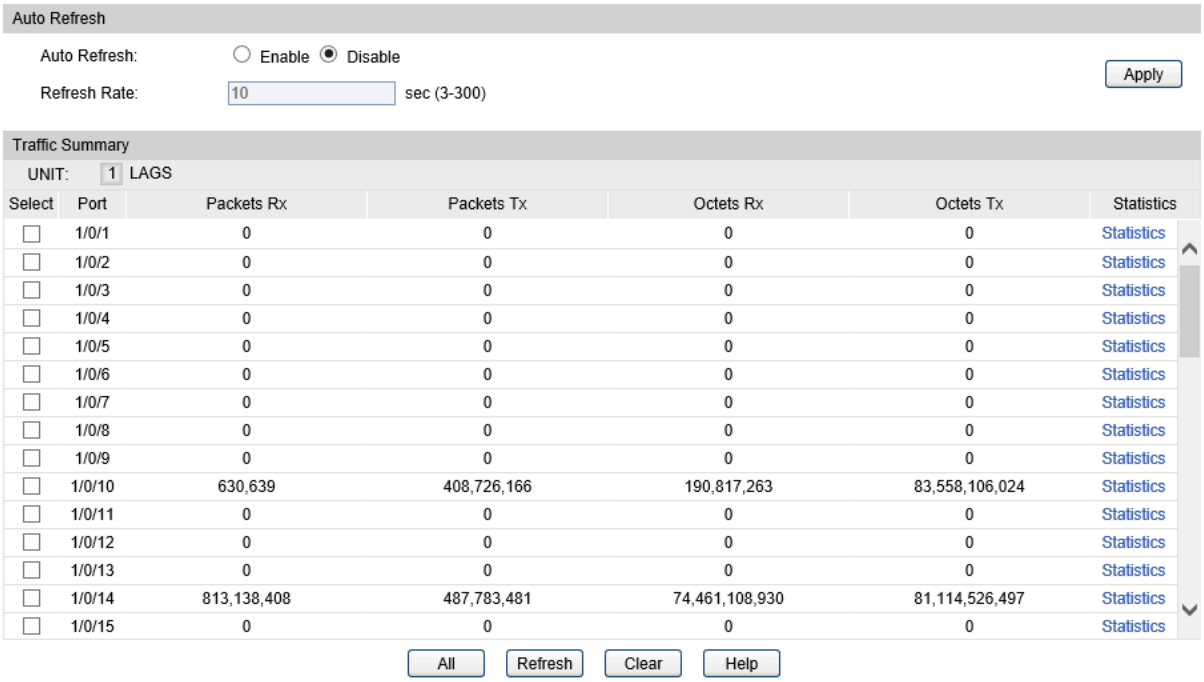
- Traffic Summary
- Traffic Statistics in Detail

1.1 Using the GUI

1.1.1 Viewing the Traffic Summary

Choose the menu **Switching > Traffic Monitor > Traffic Summary** to load the following page.

Figure 1-1 Traffic Summary



Follow these steps to view the traffic summary of each port:

1) To get the real-time traffic summary, enable auto refresh in the **Auto Refresh** section, or click **Refresh** at the bottom of the page.

Auto Refresh:	With this potion enabled, the switch refreshes the web timely.
Refresh Rate:	Specify the refresh interval in seconds.

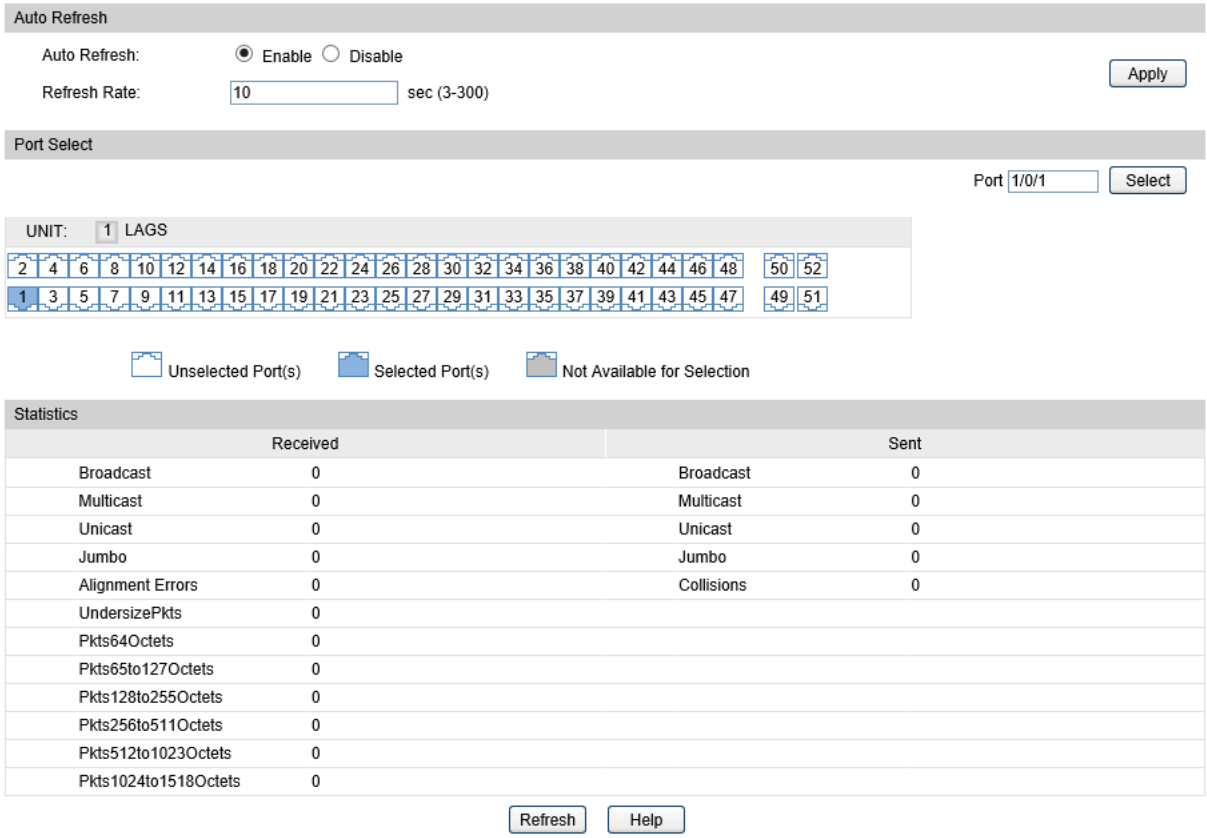
2) In the **Traffic Summary** section, click **1** to show the information of the physical ports, and click **LAGS** to show the information of the LAGs.

Packets Rx:	Displays the number of packets received on the port. Error packets are not counted in.
Packets Tx:	Displays the number of packets transmitted on the port. Error packets are not counted in.
Octets Rx:	Displays the number of octets received on the port. Error octets are counted in.
Octets Tx:	Displays the number of octets transmitted on the port. Error octets are counted in.
Statistics:	Click this button to view the detailed traffic statistics of the port.

1.1.2 Viewing the Traffic Statistics in Detail

Choose the menu **Switching > Traffic Monitor > Traffic Statistics** to load the following page.

Figure 1-2 Traffic Statistics



Follow these steps to view the traffic statistics in detail:

1) To get the real-time traffic statistics, enable auto refresh in the **Auto Refresh** section, or click **Refresh** at the bottom of the page.

Auto Refresh:	With this option enabled, the switch refreshes the web timely.

Refresh Rate:	Specify the refresh interval in seconds.

2) In **Port Select**, select a port or LAG, and click **Select**.

3) In the **Statistics** section, view the detailed information of the selected port or LAG.

Received:	Displays the detailed information of received packets. Broadcast: Displays the number of valid broadcast packets received on the port. Error frames are not counted in. Multicast: Displays the number of valid multicast packets received on the port. Error frames are not counted in. Unicast: Displays the number of valid unicast packets received on the port. Error frames are not counted in. Jumbo: Displays the number of valid jumbo packets received on the port. Error frames are not counted in. Alignment Errors: Displays the number of the received packets that have a Frame Check Sequence (FCS) with a non-integral octet (Alignment Error). The size of the packet is between 64 bytes and 1518 bytes. UndersizePkts: Displays the number of the received packets (excluding error packets) that are less than 64 bytes long. Pkts64Octets: Displays the number of the received packets (including error packets) that are 64 bytes long. Pkts65to127Octets: Displays the number of the received packets (including error packets) that are between 65 and 127 bytes long. Pkts128to255Octets: Displays the number of the received packets (including error packets) that are between 128 and 255 bytes long. Pkts256to511Octets: Displays the number of the received packets (including error packets) that are between 256 and 511 bytes long. Pkts512to1023Octets: Displays the number of the received packets (including error packets) that are between 512 and 1023 bytes long. PktsOver1023Octets: Displays the number of the received packets (including error packets) that are over 1023 bytes.
Sent:	Displays the detailed information of sent packets. Broadcast: Displays the number of valid broadcast packets transmitted on the port. Error frames are not counted in. Multicast: Displays the number of valid multicast packets transmitted on the port. Error frames are not counted in. Unicast: Displays the number of valid unicast packets transmitted on the port. Error frames are not counted in. Jumbo: Displays the number of valid jumbo packets transmitted on the port. Error frames are not counted in. Collisions: Displays the number of collisions experienced by a half-duplex port during packet transmissions.

1.2 Using the CLI

On privileged EXEC mode or any other configuration mode, you can use the following command to view the traffic information of each port or LAG:

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

port: The port number.

port-channel-id : The group number of the LAG.

If you enter no port number or group number, the information of all ports and LAGs will be displayed.

The displaying information includes:

Broadcast: Displays the number of valid broadcast packets received and transmitted on the port. Error frames are not counted in.

Multicast: Displays the number of valid multicast packets received and transmitted on the port. Error frames are not counted in.

Unicast: Displays the number of valid unicast packets received and transmitted on the port. Error frames are not counted in.

Jumbo: Displays the number of valid jumbo packets received and transmitted on the port. Error frames are not counted in.

Alignment Errors: Displays the number of the received packets that have a Frame Check Sequence (FCS) with a non-integral octet (Alignment Error). The size of the packet is between 64 bytes and 1518 bytes.

UndersizePkts: Displays the number of the received packets (excluding error packets) that are less than 64 bytes long.

Pkts64Octets: Displays the number of the received packets (including error packets) that are 64 bytes long.

Pkts65to127Octets: Displays the number of the received packets (including error packets) that are between 65 and 127 bytes long.

Pkts128to255Octets: Displays the number of the received packets (including error packets) that are between 128 and 255 bytes long.

Pkts256to511Octets: Displays the number of the received packets (including error packets) that are between 256 and 511 bytes long.

Pkts512to1023Octets: Displays the number of the received packets (including error packets) that are between 512 and 1023 bytes long.

PktsOver1023Octets: Displays the number of the received packets (including error packets) that are over 1023 bytes.

Collisions: Displays the number of collisions experienced by a port during packet transmissions.

2 Appendix: Default Parameters

Table 2-1 Traffic Statistics Monitoring

Parameter	Default Setting
Traffic Summary	
Auto Refresh	Disable
Refresh Rate	10 seconds
Traffic Statistics	
Auto Refresh	Disable
Refresh Rate	10 seconds

Part 6

Managing MAC Address Table

CHAPTERS

1. MAC Address Table
2. Address Configurations
3. Security Configurations
4. Example for Security Configurations
5. Appendix: Default Parameters

1 MAC Address Table

1.1 Overview

The MAC address table contains address information that the switch uses to forward traffic between ports. As shown below, the table lists map entries of MAC addresses, VLAN IDs and ports. These entries can be manually input or automatically learned by the switch. Based on the MAC-address-to-port mapping in the table, the switch forwards the packet only to the associated port.

Table 1-1 The MAC Address Table

MAC Address	VLAN ID	Port	Type	Aging Status
00:00:00:00:00:01	1	1	Dynamic	Aging
00:00:00:00:00:02	1	2	Config static	no-Aging
...				

1.2 Supported Features

The address table of the switch contains dynamic addresses, static addresses and filtering addresses. You can add or remove these entries to your needs. Furthermore, you can configure notification traps and limit the number of MAC addresses in a VLAN for traffic safety.

Address Configurations

- Dynamic address

Dynamic addresses are source addresses learned by the switch automatically. Then the switch regularly ages out those that are not in use. That is, the switch removes the MAC address entries related to a network device if no packet is received from the device within the aging time. And you can configure the aging time when needed.

- Static address

Static addresses are configured manually and do not age. For some relatively fixed connection, for example, frequently visited server, you can manually set the MAC address of the server as a static entry to enhance the forwarding efficiency of the switch.

- Filtering address

Filtering addresses are manually added to configure the switch to automatically drop the packets with specific source or destination MAC addresses.

Security Configurations

- Configuring MAC Notification Traps

You can configure traps and SNMP (Simple Network Management Protocol) to monitor and receive notifications of the usage of the MAC address table and the MAC address change activity. For example, you can configure the switch to send you notifications when new users access the network.

- Limiting the Number of MAC Addresses in VLANs

You can configure VLAN Security to limit the number of MAC addresses that can be learned in specified VLANs. The switch will not learn addresses when the number of learned addresses has reached the limit, preventing the address table from being used up by broadcast packets of MAC address attacks.

2 Address Configurations

With MAC address table, you can:

- Add static MAC address entries
- Change the address aging time
- Add filtering address entries
- View address table entries

2.1 Using the GUI

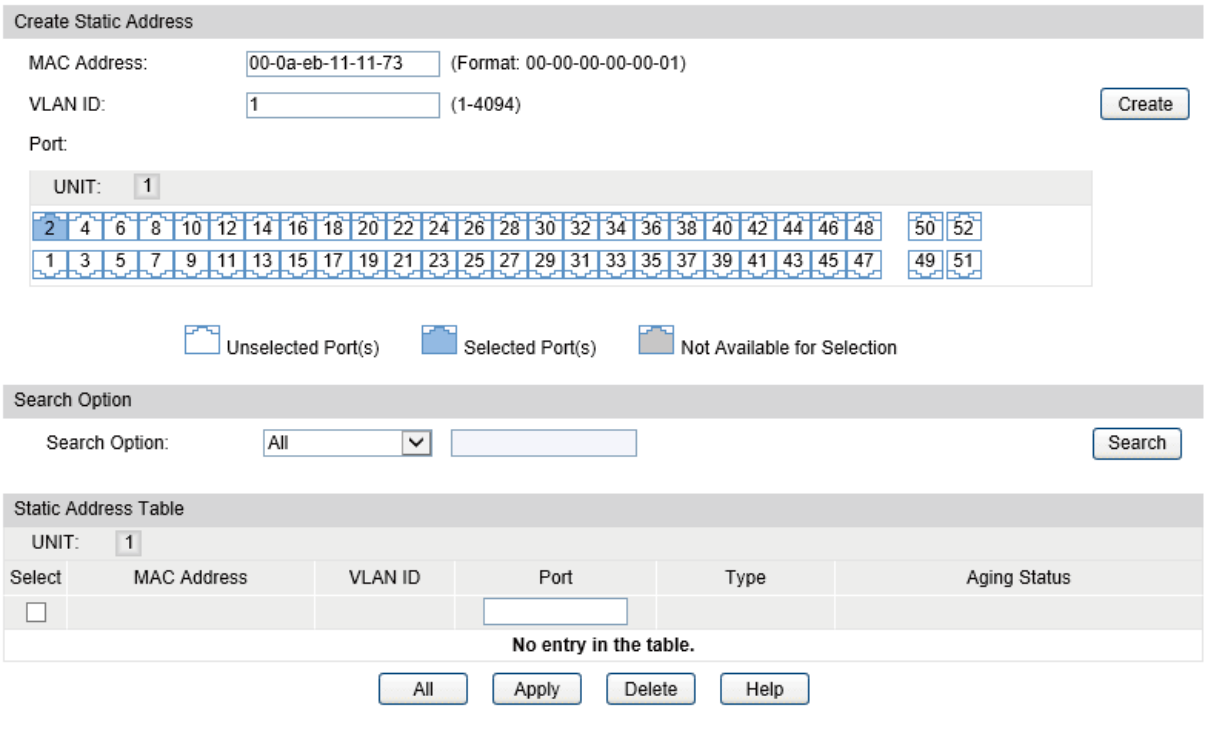
2.1.1 Adding Static MAC Address Entries

You can add static MAC address entries by manually specifying the desired MAC address or binding dynamic MAC address entries.

- Adding MAC Addresses Manually

Choose the menu **Switching > MAC Address > Static Address** to load the following page.

Figure 2-1 Adding MAC Addresses Manually



Follow these steps to add a static MAC address entry:

1) Enter the MAC address, VLAN ID and select a port to bind them together.

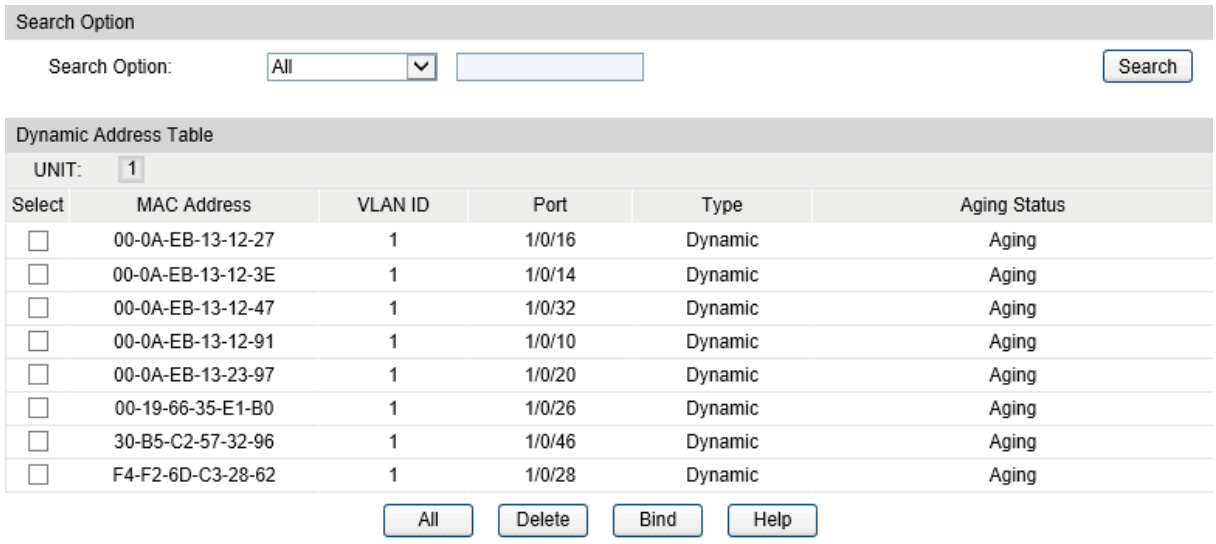
VLAN ID	Specify an existing VLAN in which packets with the specific MAC address are received.
Port	Specify a port to which packets with the specific MAC address are forwarded. The port must belong to the specified VLAN. After you have added the static MAC address, if the corresponding port number of the MAC address is not correct, or the connected port (or the device) has been changed, the switch cannot forward the packets correctly. Please reset the static address entry appropriately.

2) Click **Create**.

Binding Dynamic Address Entries

Choose the menu **Switching > MAC Address > Dynamic Address** to load the following page.

Figure 2-2 Binding Dynamic MAC Address Entries



Follow these steps to bind dynamic MAC address entries:

1) Select your desired MAC address entries. You can select the entries from the **Dynamic Address Table**, or quickly search them out by MAC address/ VLAN ID/ port in the **Search Option** section.

2) Click **Bind**, and then the selected entries will not age.

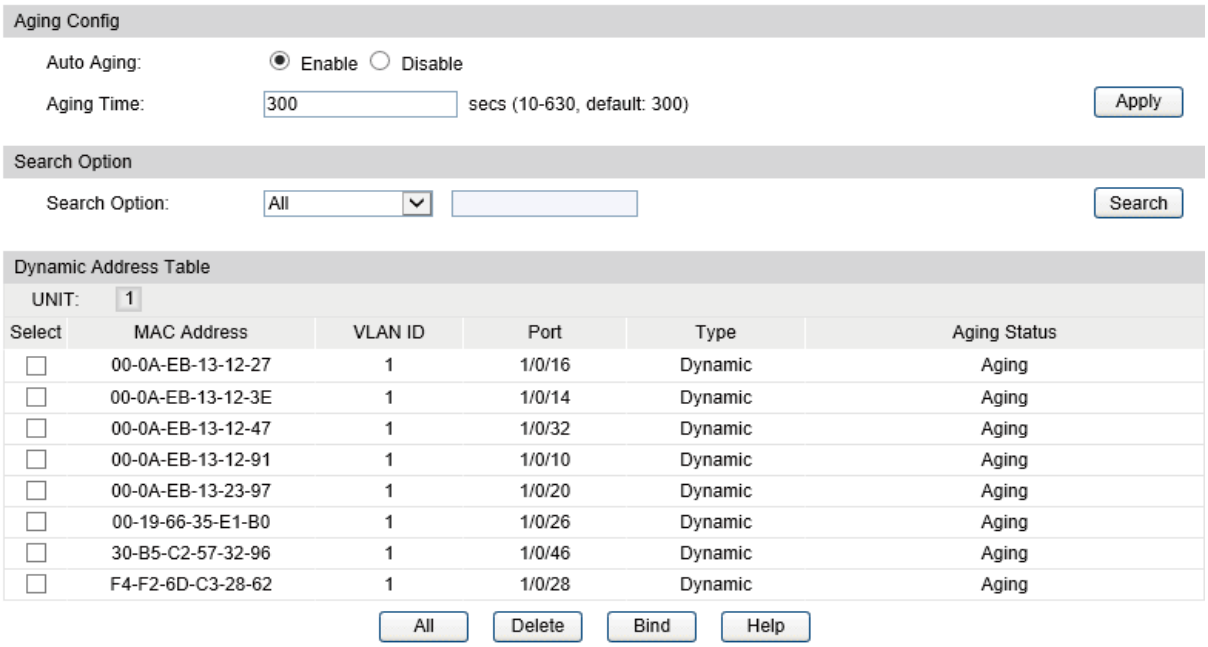
Note:

- In the same VLAN, once an address is configured as a static address, it cannot be set as a filtering address, and vice versa.
- Multicast or broadcast addresses cannot be set as static addresses.
- Ports in LAGs (Link Aggregation Group) are not supported for static address configuration.

2.1.2 Modifying the Aging Time of Dynamic Address Entries

Choose the menu **Switching > MAC Address > Dynamic Address** to load the following page.

Figure 2-3 Modifying the Aging Time of Dynamic Address Entries



Follow these steps to modify the aging time of dynamic address entries:

1) In the **Aging Config** section, enable Auto Aging, and enter your desired length of time.

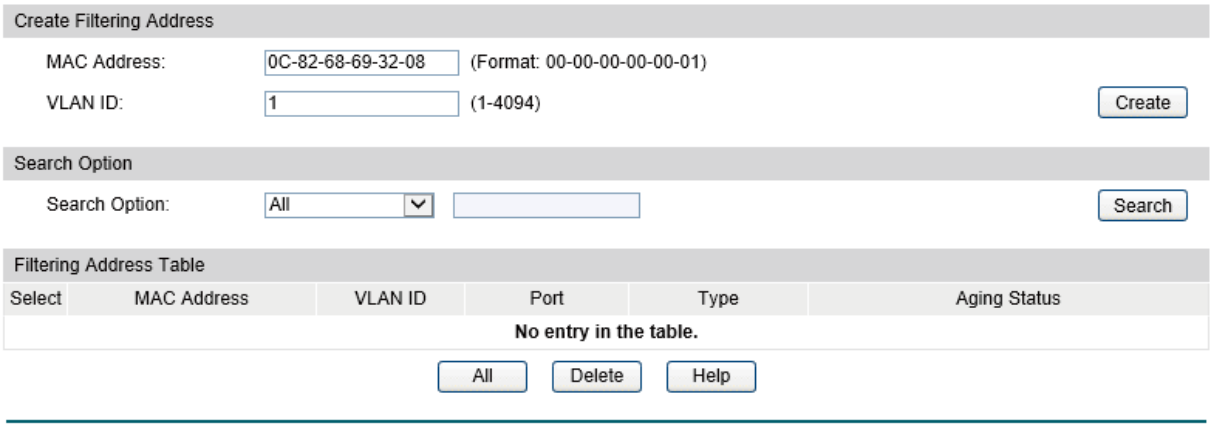
Auto Aging	Enable Auto Aging, then the switch automatically updates the dynamic address table with the aging mechanism. By default, it is enabled.
Aging Time	Set the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated. The valid values are from 10 to 630 seconds, and the default value is 300. A short aging time is applicable to networks where network topology changes frequently, and a long aging time is applicable to stable networks. We recommend that you keep the default value if you are unsure about settings in your case.

2) Click **Apply.**

2.1.3 Adding MAC Filtering Address Entries

Choose the menu **Switching > MAC Address > Filtering Address** to load the following page.

Figure 2-4 Adding MAC Filtering Address Entries



Follow these steps to add MAC filtering address entries:

1) In the **Create Filtering Address** section, enter the MAC Address and VLAN ID.

MAC Address	Specify a MAC address to configure the switch to drop packets which include this MAC address as the source address or destination address.
VLAN ID	Specify an existing VLAN in which packets with the specific MAC address are dropped.

2) Click **Create**.

Note:

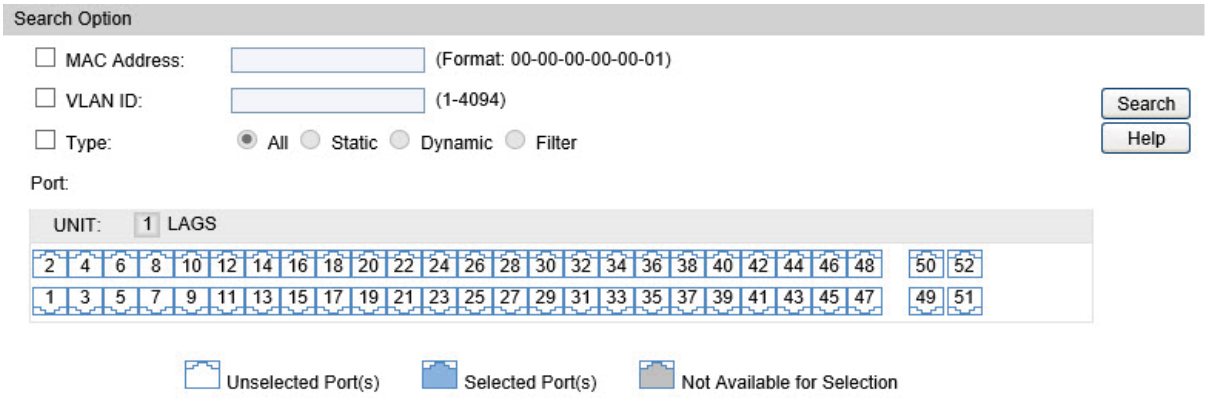
- In the same VLAN, once an address is configured as a filtering address, it cannot be set as a static address, and vice versa.
- Multicast or broadcast addresses cannot be set as filtering addresses .

2.1.4 Viewing Address Table Entries

You can view entries in MAC address table to check your former operations and address information.

Choose the menu **Switching > MAC Address > Address Table** to load the following page.

Figure 2-5 Viewing Address Table Entries



Address Table

UNIT: 1

MAC Address	VLAN ID	Port	Type	Aging Status
00-0A-EB-00-13-01	1	1/0/28	Dynamic	Aging
00-0A-EB-13-12-27	1	1/0/16	Dynamic	Aging
00-0A-EB-13-12-3E	1	1/0/14	Dynamic	Aging
00-0A-EB-13-12-47	1	1/0/32	Dynamic	Aging
00-0A-EB-13-12-91	1	1/0/10	Dynamic	Aging
00-0A-EB-13-12-DB	1	1/0/40	Dynamic	Aging
00-0A-EB-13-23-97	1	1/0/20	Dynamic	Aging
00-11-22-33-44-AC	1	1/0/10	Dynamic	Aging
00-19-66-35-E1-B0	1	1/0/26	Dynamic	Aging
F4-F2-6D-C3-28-62	1	1/0/28	Dynamic	Aging

2.2 Using the CLI

2.2.1 Adding Static MAC Address Entries

Follow these steps to add static MAC address entries:

Step 1 **configure**

Enter global configuration mode.

Step 2 **mac address-table static** *mac-addr* **vid** *vid* **interface gigabitEthernet** *port*

Bind the MAC address, VLAN and port together to add a static address to the VLAN.

mac-addr: Enter the MAC address and packets with this destination address received in the specified VLAN are forwarded to the specified port. The format is xx:xx:xx:xx:xx:xx, for example, 00:00:00:00:00:01.

vid: Specify an existing VLAN in which packets with the specific MAC address are received.

port: Specify a port to which packets with the specific MAC address are forwarded. The port must belong to the specified VLAN.

Step 3	**end** Return to privileged EXEC mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

Note:

- In the same VLAN, once an address is configured as a static address, it cannot be set as a filtering address, and vice versa.
- Multicast or broadcast addresses cannot be set as static addresses.
- Ports in LAGs (Link Aggregation Group) are not supported for static address configuration.

The following example shows how to add a static MAC address entry with MAC address 00:02:58:4f:6c:23, VLAN 10 and port 1. When a packet is received in VLAN 10 with this address as its destination, the packet will be forwarded only to port 1.

Switch#configure

Switch(config)# mac address-table static 00:02:58:4f:6c:23 **vid** 10 **interface gigabitEthernet**

1/0/1

Switch(config)#show mac address-table static

MAC Address Table

MAC	VLAN	Port	Type	Aging
00:02:58:4f:6c:23	10	Gi1/0/1	config static	no-aging

Total MAC Addresses for this criterion: 1

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Modifying the Aging Time of Dynamic Address Entries

Follow these steps to modify the aging time of dynamic address entries:

Step 1	**configure** Enter global configuration mode.

Step 2	**mac address-table aging-time** *aging-time* Set your desired length of address aging time for dynamic address entries. *aging-time:* Set the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated. The valid values are from10 to 630. When 0 is entered, the Auto Aging function is disabled. The default value is 300 and we recommend you keep the default value if you are unsure about settings in your case.
Step 3	**end** Return to privileged EXEC mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to modify the aging time to 500 seconds. A dynamic entry remains in the MAC address table for 500 seconds after the entry is used or updated.

Switch#configure

Switch(config)# mac address-table aging-time 500

Switch(config)#show mac address-table aging-time

Aging time is 500 sec.

Switch(config)#end

Switch#copy running-config startup-config

2.2.3 Adding MAC Filtering Address Entries

Follow these steps to add MAC filtering address entries:

Step 1	**configure** Enter global configuration mode.
Step 2	**mac address-table filtering** *mac-addr* **vid** *vid* Add the filtering address to the VLAN. *mac-addr:* Specify a MAC address to configure the switch to drop packets which include this MAC address as the source address or destination address. The format is xx:xx:xx:xx:xx:xx, for example, 00:00:00:00:00:01. *vid:* Specify an existing VLAN in which packets with the specific MAC address are dropped.
Step 3	**end** Return to privileged EXEC mode.

Step 4	**copy running-config startup-config** Save the settings in the configuration file.

Note:

- In the same VLAN, once an address is configured as a filtering address, it cannot be set as a static address, and vice versa.
- Multicast or broadcast addresses cannot be set as filtering addresses .

The following example shows how to add the MAC filtering address 00:1e:4b:04:01:5d to VLAN 10. Then the switch will drop the packet that is received in VLAN 10 with this address as its source or destination.

Switch#configure

Switch(config)# mac address-table filtering 00:1e:4b:04:01:5d **vid** 10

Switch(config)#show mac address-table filtering

MAC Address Table

MAC	VLAN	Port	Type	Aging
---	------	----	----	-----
00:1e:4b:04:01:5d	10		filter	no-aging

Total MAC Addresses for this criterion: 1

Switch(config)#end

Switch#copy running-config startup-config

3 Security Configurations

With security configurations of the MAC address table, you can:

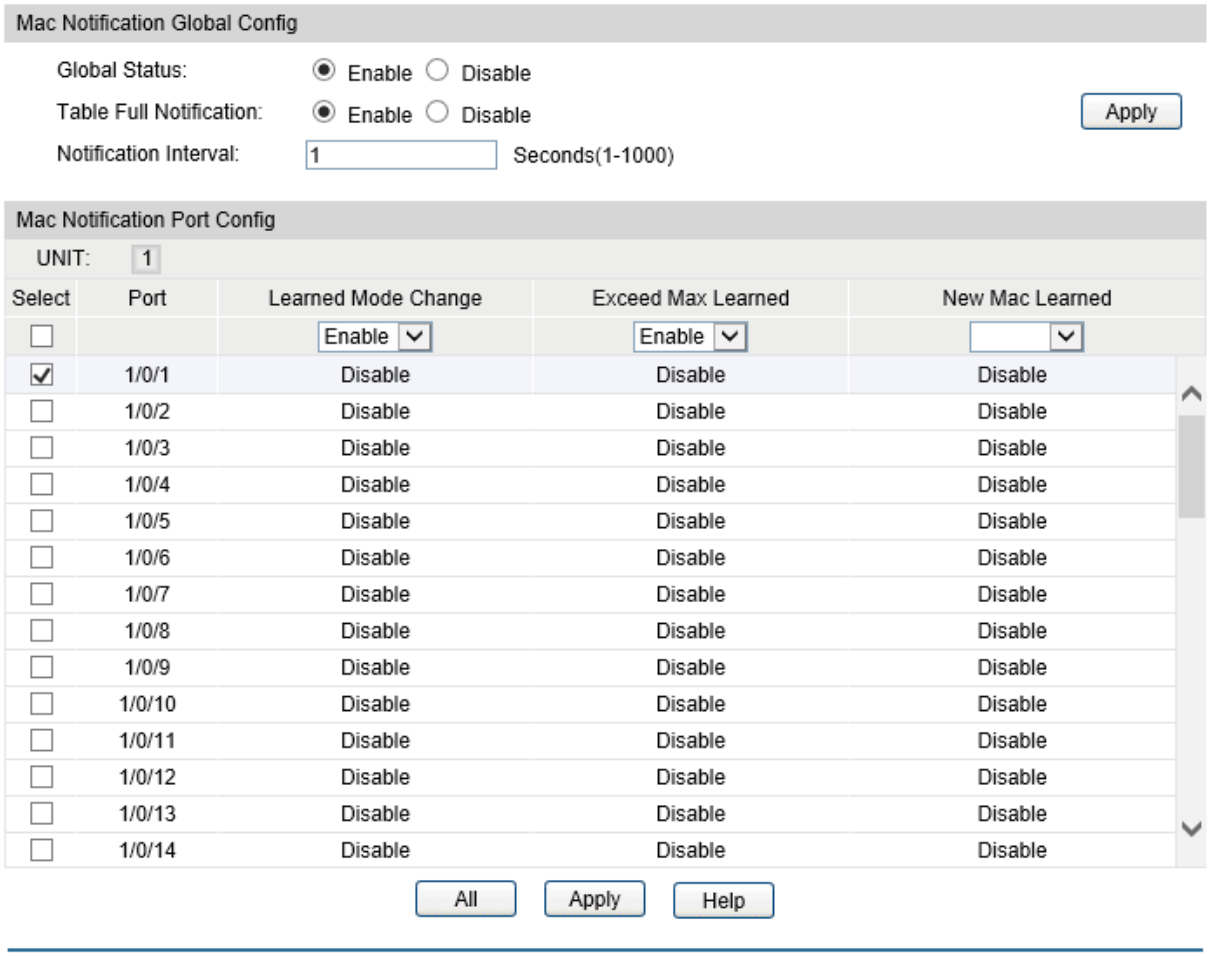
- Configure MAC notification traps
- Limit the number of MAC addresses in VLANs

3.1 Using the GUI

3.1.1 Configuring MAC Notification Traps

Choose the menu **Switching > MAC Address > MAC Notification** to load the following page.

Figure 3-1 Configuring MAC Notification Traps



Follow these steps to configure MAC notification traps:

1) In the **MAC Notification Global Config** section, enable this feature, configure the relevant options, and click **Apply**.

Global Status	Enable MAC notification feature globally.
Table Full Notification	Enable Table Full Notification, and when address table is full, a notification will be generated and sent to the management host .
Notification Interval	Specify a time value in seconds between 1 to 1000 to bundle the notifications and reduce traffic. Notification Interval is the interval time between each set of New MAC Learned notifications that are generated. By default, it is 1 second.

2) In the **MAC Notification Port Config** section, select your desired port and enable its notification traps. You can enable these three types: **Learned Mode Change**, **Exceed Max Learned** and **New MAC Learned**. Click **Apply**.

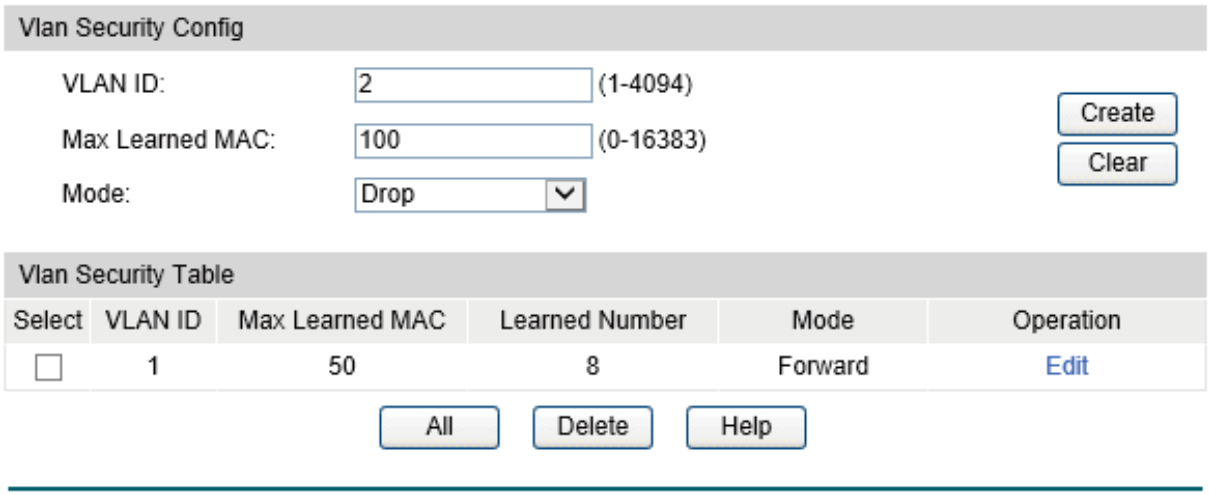
Learned Mode Change	Enable Learned Mode Change, and when the learned mode of the specified port is changed, a notification will be generated and sent to the management host.
Exceed Max Learned	Enable Exceed Max Learned, and when the maximum number of learned MAC addresses on the specified port is exceeded, a notification will be generated and sent to the management host. For Exceed-max-learned notification, you need to enable Port Security and set the maximum number of learned MAC addresses on the specified port. For more information about Port Security, please refer to *Physical Interface*.
New MAC Learned	Enable New MAC Learned, and when the specified port learns a new MAC address, a notification will be generated and sent to the management host.

3) Configure SNMP and set a management host. For detailed SNMP configurations, please refer to *Configuring SNMP & RMON.*

3.1.2 Limiting the Number of MAC Addresses in VLANs

Choose the menu **Switching > MAC Address > MAC VLAN Security** to load the following page.

Figure 3-2 Limiting the Number of MAC Addresses in VLANs



Follow these steps to limit the number of MAC addresses in VLANs:

1) Enter the VLAN ID to limit the number of MAC addresses that can be learned in the specified VLAN.

VLAN ID	Specify an existing VLAN in which you want to limit the number of MAC addresses.

2) Enter your desired value in **Max Learned MAC** to set a threshold.

Max Learned MAC	Set the maximum number of MAC addresses in the specific VLAN. It ranges from 0 to 16383. You can control the available address table space by setting maximum learned MAC number for VLANs. However, an improper maximum number can cause unnecessary floods in the network or a waste of address table space. Therefore, before you set the number limit, please be sure you are familiar with the network topology and the switch system configuration.

3) Choose the mode that the switch adopts when the maximum number of MAC addresses in the specified VLAN is exceeded.

Drop	Packets of new source MAC addresses in the VLAN will be dropped when the maximum number of MAC addresses in the specified VLAN is exceeded.
Forward	Packets of new source MAC addresses will be forwarded but the addresses will not be learned when the maximum number of MAC addresses in the specified VLAN is exceeded.
Disable	The number limit on the VLAN is not valid, and the switch follows the original forwarding rules.

4) Click **Create**.

3.2 Using the CLI

3.2.1 Configuring MAC Notification Traps

Follow these steps to configure MAC notification traps:

Step 1	**configure** Enter global configuration mode.
Step 2	**mac address-table notification global-status {**enable	disable**}** Enable MAC Notification globally. enable	disable: Enable or disable MAC Notification globally.
Step 3	**mac address-table notification table-full-status [**enable	disable**]** (Optional) Enable Table Full Notification. enable	disable: With Table Full Notification enabled, when address table is full, a notification will be generated and sent to the management host.
Step 4	**mac address-table notification interval** *time* Set your desired interval time between each set of New MAC Learned notifications that are generated. *time:* Specify a time value in seconds between 1to 1000 to bundle the notifications and reduce traffic. By default, it is 1 second.
Step 5	**interface {[gigabitEthernet** *port* **]	[range gigabitEthernet** *port-list* **]}** Configure notification traps on the specified port. *port/ port-list:* The number or the list of the Ethernet port that you want to configure notification traps.
Step 6	**mac address-table notification {[learn-mode-change** enable	disable] **[exceed-max-learned** enable	disable] **[new-mac-learned** enable	disable]**}** Enable learn-mode-change, exceed-max-learned, or new-MAC-learned notification traps on the specified port. enable	disable:Enable or disable learn-mode-change, exceed-max-learned, or new-MAC-learned notification traps on the specified port. **learn-mode-change**: With learn-mode-change enabled, when the learned mode of the specified port is changed, a notification will be generated and sent to the management host. **exceed-max-learned**: With exceed-max-learned enabled, when the maximum number of MAC addresses on the specified port is exceeded, a notification will be generated and sent to the management host. For Exceed Max Learned notification, you need to enable Port Security and set the maximum number of MAC addresses on the specified port. For more information about Port Security, please refer to *Physical Interface*. **new-mac-learned**: With new-mac-learned enabled, when the specified port learns a new MAC address, a notification will be generated and sent to the management host.
Step 7	**end** Return to privileged EXEC mode.
Step 8	**copy running-config startup-config** Save the settings in the configuration file.

Now you have configured MAC notification traps. To receive notifications, you need to further enable SNMP and set a management host. For detailed SNMP configurations, please refer to *Configuring SNMP & RMON*.

The following example shows how to enable new-MAC-learned trap on port 1, and set the interval time as 10 seconds. After you have further configured SNMP, the switch will bundle notifications of new addresses in every 10 seconds and send to the management host.

Switch#configure

Switch(config)#mac address-table notification global-status enable

Switch(config)#mac address-table notification interval 10

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

Switch(config-if)#mac address-table notification new-mac-learned enable

Switch(config-if)#show mac address-table notification interface gigabitEthernet 1/0/1

Mac Notification Global Config

Notification Global Status : enable

Table Full Notification Status: disable

Notification Interval : 10

Port	LrnMode Change	Exceed Max Limit	New Mac Learned
----	----------	----------	----------
Gi1/0/1	disable	disable	enable

Switch(config-if)#end

Switch#copy running-config startup-config

3.2.2 Limiting the Number of MAC Addresses in VLANs

Follow these steps to limit the number of MAC addresses in VLANs:

Step 1	**configure** Enter global configuration mode.

Step 2	**mac address-table security vid** *vid* **max-learn** *num* **{**drop | forward | disable**}** Configure the maximum number of MAC addresses in the specified VLAN and select a mode for the switch to adopt when the maximum number is exceeded. *vid*: Specify an existing VLAN in which you want to limit the number of MAC addresses. *num*: Set the maximum number of MAC addresses in the specific VLAN. It ranges from 0 to 16383. drop | forward | disable: The mode that the switch adopts when the maximum number of MAC addresses in the specified VLAN is exceeded. drop: Packets of new source MAC addresses in the VLAN will be dropped when the maximum number of MAC addresses in the specified VLAN is exceeded. forward: Packets of new source MAC addresses will be forwarded but the addresses not learned when the maximum number of MAC addresses in the specified VLAN is exceeded. disable: The number limit on the VLAN is not valid, and the switch follows the original forwarding rules.
Step 3	**end** Return to privileged EXEC mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to limit the number of MAC addresses to 100 in VLAN 10, and configure the switch to drop packets of new source MAC addresses when the limit is exceeded.

Switch#configure

Switch(config)#mac address-table security vid 10 **max-learn** 100 drop

Switch(config)#show mac address-table security vid 10

VlanId	Max-learn	Current-learn	Status
10	100	0	Drop

Switch(config)#end

Switch#copy running-config startup-config

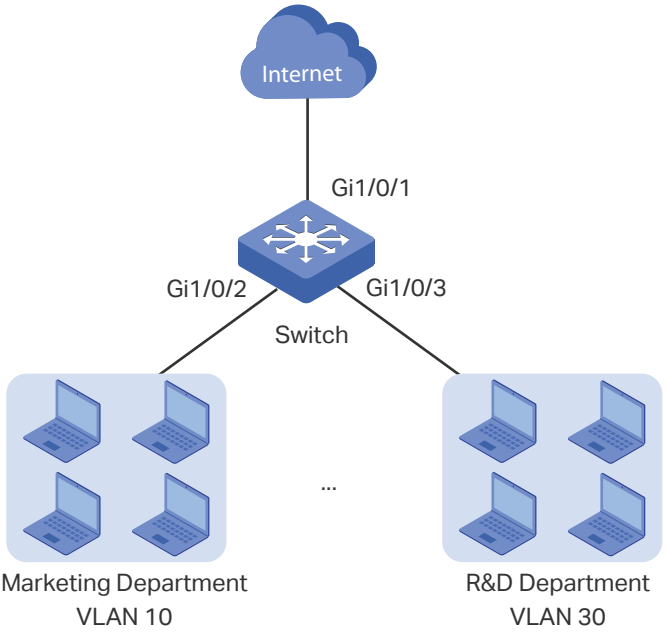
4 Example for Security Configurations

4.1 Network Requirements

Several departments are connected to the company network as shown in Figure 4-1. Now the Marketing Department that is in VLAN 10 has network requirements as follows:

- Free the network system from illegal accesses and MAC address attacks by limiting the number of access users in this department to 100.
- Assist the network manager supervising the network with notifications of any new access users.

Figure 4-1 The Network Topology



4.2 Configuration Scheme

VLAN Security can be configured to limit the number of access users and in this way to prevent illegal accesses and MAC address attacks.

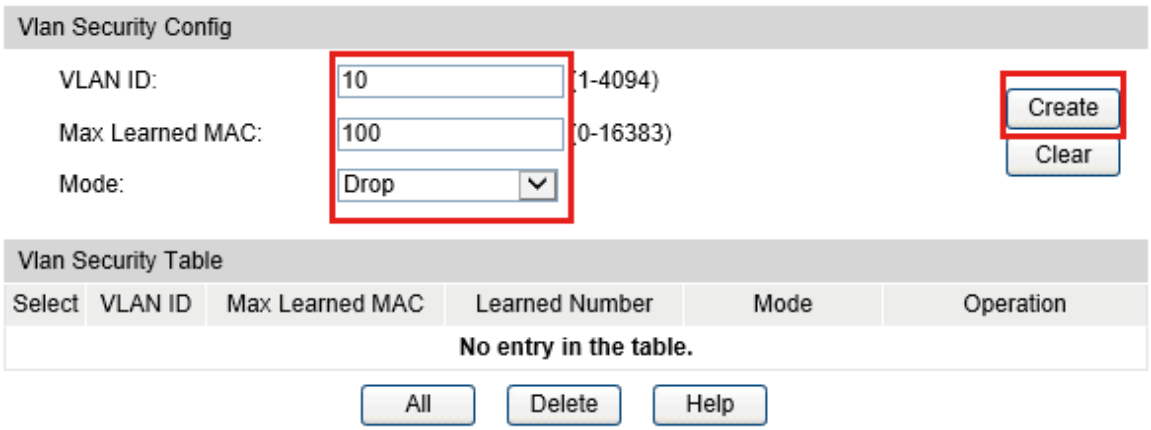
MAC Notification and SNMP can be configured to monitor the interface which is used by the Marketing Department. Enable the new-MAC-learned notification and the SNMP, then the network manager can get notifications when new users access the network.

Demonstrated with T2600G-28TS, this chapter provides configuration procedures in two ways: using the GUI and using the CLI.

4.3 Using the GUI

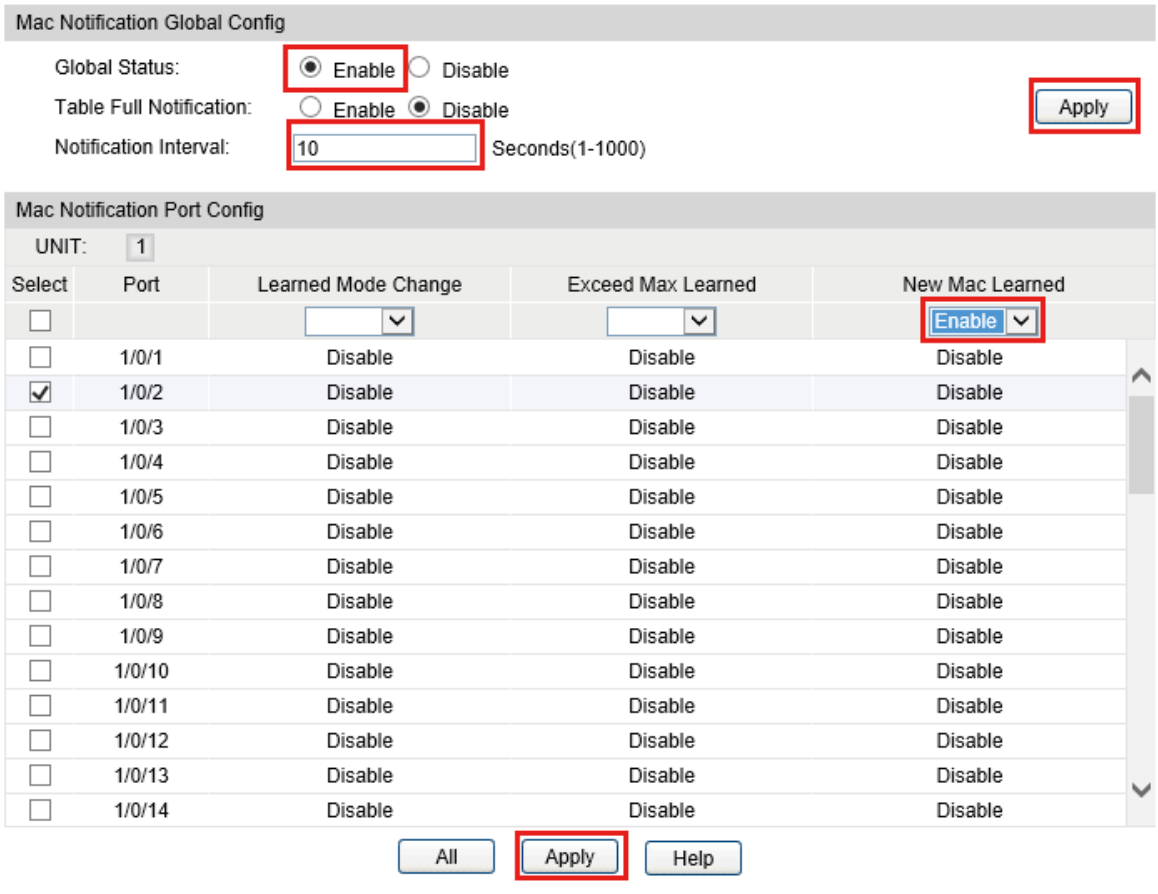
1) Choose the menu **Switching > MAC Address > MAC VLAN Security** to load the following page. Set the maximum number of MAC address in VLAN 10 as 100, choose drop mode and click **Create**.

Figure 4-2 Configuring VLAN Security



2) Choose the menu **Switching > MAC Address > MAC Notification** to load the following page. Enable Global Status, set notification interval as 10 seconds, and click **Apply**. Then, enable new-mac-learned trap on port 1/0/2 and click **Apply**.

Figure 4-3 Configuring New-MAC-learned Traps



3) Click **Save Config** to save the settings.
4) Enable SNMP and set a management host. For detailed SNMP configurations, please refer to *Configuring SNMP & RMON*.

4.4 Using the CLI

1) Set the maximum number of MAC address in VLAN 10 as 100, and choose drop mode.

   Switch#configure

   Switch(config)#mac address-table security vid 10 max-learn 100 drop

2) Configure the new-MAC-learned trap on port 2 and set notification interval as 10 seconds.

   Switch(config)#mac address-table notification global-status enable

   Switch(config)#mac address-table notification interval 10

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

   Switch(config-if)#mac address-table notification new-mac-learned enable

   Switch(config-if)#end

   Switch#copy running-config startup-config

3) Configure SNMP and set a management host. For detailed SNMP configurations, please refer to *Configuring SNMP & RMON*.

Verify the Configurations

Verify the configuration of VLAN Security.

Switch#show mac address-table security vid 10

VlanId	Max-learn	Current-learn	Status
10	100	0	Drop

Verify the configuration of MAC Notification on port 1/0/2.

Switch#show mac address-table notification interface gigabitEthernet 1/0/2

Port	LrnMode Change	Exceed Max Limit	New Mac Learned
Gi1/0/2	disable	disable	enable

5 Appendix: Default Parameters

Default settings of the MAC Address Table are listed in the following tables.

Table 5-1 Entries in the MAC Address Table

Parameter	Default Setting
Static Address Entries	None
Dynamic Address Entries	Auto-learning
Filtering Address Entries	None

Table 5-2 Default Settings of Dynamic Address Table

Parameter	Default Setting
Auto Aging	Enable
Aging Time	300 seconds

Table 5-3 Default Settings of MAC Notification

Parameter	Default Setting
Global Status	Disable
Table Full Notification	Disable
Notification Interval	1 Second
Learned Mode Change Notification	Disable
Exceed Max Learned Notification	Disable
New MAC Learned Notification	Disable

Table 5-4 Default Settings of MAC VLAN Security

Parameter	Default Setting
MAC VLAN Security	Disable

Part 7

Configuring DDM

CHAPTERS

1. Overview
2. DDM Configuration
3. Appendix: Default Parameters

Note:

T2600G-28MPS doesn't support DDM feature.

1 Overview

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 monitored SFP port automatically when the specified parameter exceeds the alarm threshold or warning threshold. The monitoring parameters include: Temperature, Voltage, Bias Current, Tx Power and Rx Power.

2 DDM Configuration

To complete DDM configuration, follow these steps:

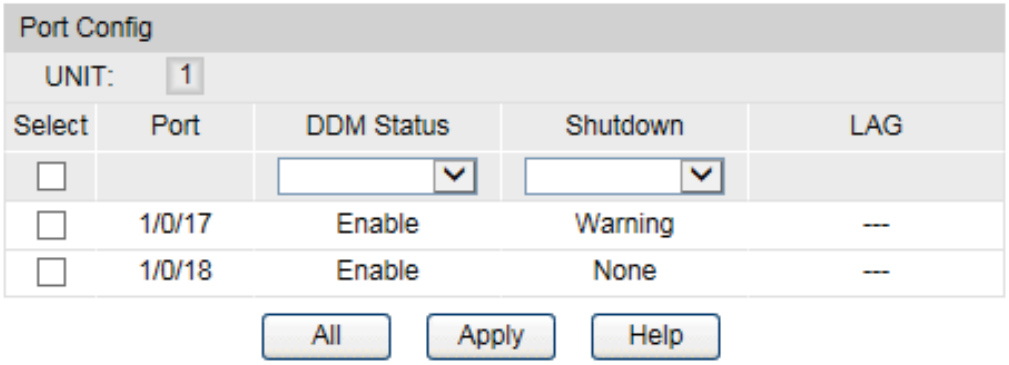
1) Enable DDM on the SFP port.
2) Configure the shutdown condition.
3) Configure the specified threshold for warning or alarm.

2.1 Using the GUI

2.1.1 Configuring DDM Globally

Choose the menu **Switching > DDM > DDM Config** to load the following page.

Figure 2-1 Configure DDM Globally



Follow these steps to configure DDM's global parameters:

1) In the **Port Config** section, configure DDM parameters on the SFP ports.

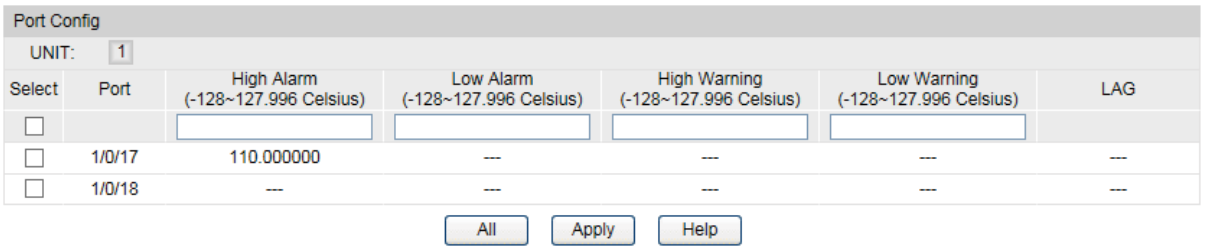
DDM Status	Enable or disable DDM feature on the port.
Shutdown	Specify whether to shut down the port when the alarm threshold or warning threshold is exceeded. **Alarm**: Shut down the port when the alarm threshold is exceeded. **Warning**: Shut down the port when the warning threshold is exceeded. **None**: The port will not be shut down even if the alarm threshold or warning threshold is exceeded. This is the default option.
LAG	Displays the LAG number which the port belongs to.

2) Click **Apply**.

2.1.2 Configuring the Temperature Threshold

Choose the menu **Switching > DDM > Temperature Threshold** to load the following page.

Figure 2-2 Configure Temperature Threshold



Follow these steps to configure DDM's temperature threshold:

1) In the **Port Config** table, configure temperature threshold of the SFP ports.

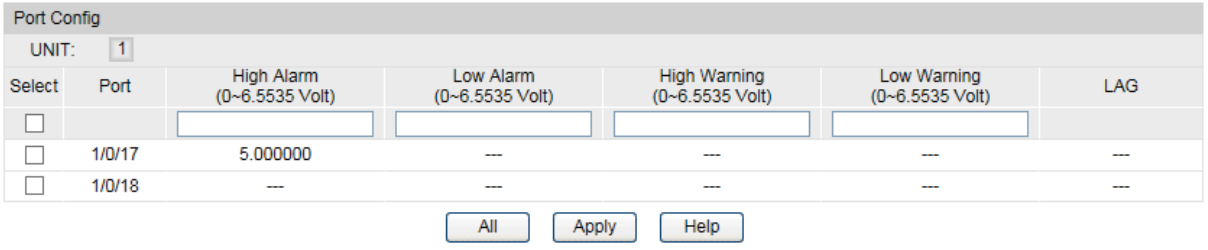
High Alarm	Specify the high threshold for the alarm. When the operating parameter rises above this value, action associated with the alarm will be taken. The valid values are from -128 to 127.996.
Low Alarm	Specify the low threshold for the alarm. When the operating parameter falls below this value, action associated with the alarm will be taken. The valid values are from -128 to 127.996.
High Warning	Specify the high threshold for the warning. When the operating parameter rises above this value, action associated with the warning will be taken. The valid values are from -128 to 127.996.
Low Warning	Specify the low threshold for the warning. When the operating parameter falls below this value, action associated with the warning will be taken. The valid values are from -128 to 127.996.
LAG	Displays the LAG number which the port belongs to.

2) Click **Apply**.

2.1.3 Configuring the Voltage Threshold

Choose the menu **Switching > DDM > Voltage Threshold** to load the following page.

Figure 2-3 Configure Voltage Threshold



Follow these steps to configure DDM's voltage threshold:

1) In the **Port Config** table, configure voltage threshold on the SFP ports.

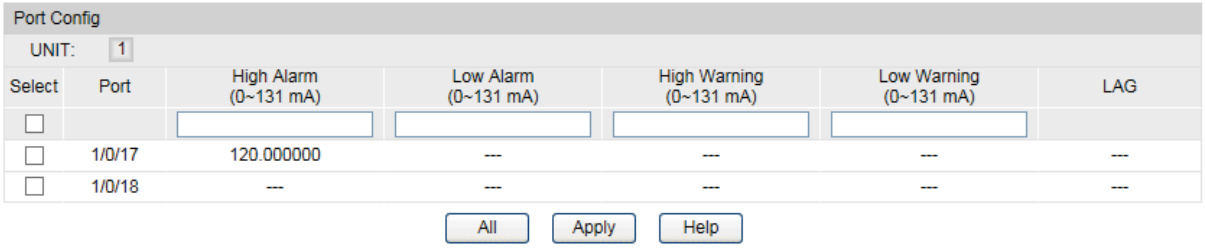
High Alarm	Specify the high threshold for the alarm. When the operating parameter rises above this value, action associated with the alarm will be taken. The valid values are from 0 to 6.5535.
Low Alarm	Specify the low threshold for the alarm. When the operating parameter falls below this value, action associated with the alarm will be taken. The valid values are from 0 to 6.5535.
High Warning	Specify the high threshold for the warning. When the operating parameter rises above this value, action associated with the warning will be taken. The valid values are from 0 to 6.5535.
Low Warning	Specify the low threshold for the warning. When the operating parameter falls below this value, action associated with the warning will be taken. The valid values are from 0 to 6.5535.
LAG	Displays the LAG number which the port belongs to.

2) Click **Apply**.

2.1.4 Configuring the Bias Current Threshold

Choose the menu **Switching > DDM > Bias Current Threshold** to load the following page.

Figure 2-4 Configure Bias Current Threshold



Follow these steps to configure DDM's bias current threshold:

1) In the **Port Config** table, configure bias current threshold on the SFP ports.

High Alarm	Specify the high threshold for the alarm. When the operating parameter rises above this value, action associated with the alarm will be taken. The valid values are from 0 to 131.
Low Alarm	Specify the low threshold for the alarm. When the operating parameter falls below this value, action associated with the alarm will be taken. The valid values are from 0 to 131.
High Warning	Specify the high threshold for the warning. When the operating parameter rises above this value, action associated with the warning will be taken. The valid values are from 0 to 131.

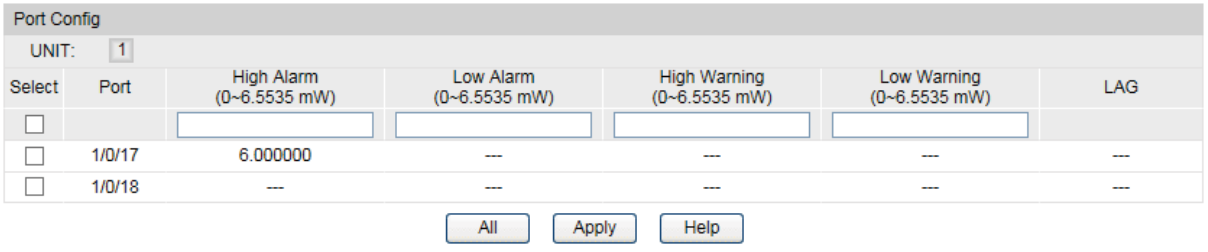
Low Warning	Specify the low threshold for the warning. When the operating parameter falls below this value, action associated with the warning will be taken. The valid values are from 0 to 131.
LAG	Displays the LAG number which the port belongs to.

2) Click **Apply**.

2.1.5 Configuring the Tx Power Threshold

Choose the menu **Switching > DDM > Tx Power Threshold** to load the following page.

Figure 2-5 Configure Tx Power Threshold



Follow these steps to configure DDM's Tx power threshold:

1) In the **Port Config** table, configure Tx power threshold on the SFP ports.

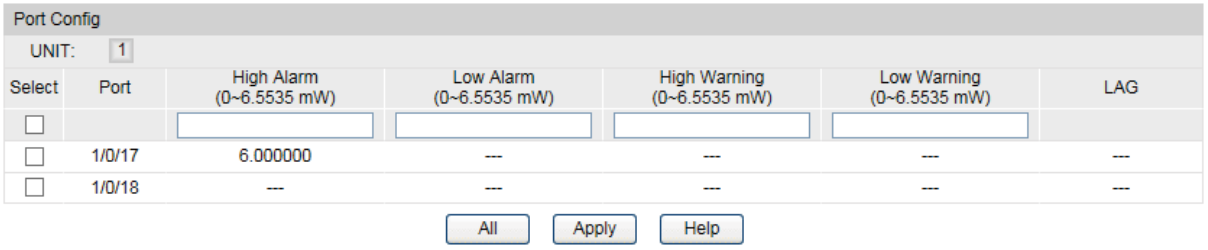
High Alarm	Specify the high threshold for the alarm. When the operating parameter rises above this value, action associated with the alarm will be taken. The valid values are from 0 to 6.5535.
Low Alarm	Specify the low threshold for the alarm. When the operating parameter falls below this value, action associated with the alarm will be taken. The valid values are from 0 to 6.5535.
High Warning	Specify the high threshold for the warning. When the operating parameter rises above this value, action associated with the warning will be taken. The valid values are from 0 to 6.5535.
Low Warning	Specify the low threshold for the warning. When the operating parameter falls below this value, action associated with the warning will be taken. The valid values are from 0 to 6.5535.
LAG	Displays the LAG number which the port belongs to.

2) Click **Apply**.

2.1.6 Configuring the Rx Power Threshold

Choose the menu **Switching > DDM > Rx Power Threshold** to load the following page.

Figure 2-6 Configure Rx Power Threshold



Follow these steps to configure DDM's Rx power threshold:

1) In the **Port Config** table, configure Rx power threshold on the SFP ports.

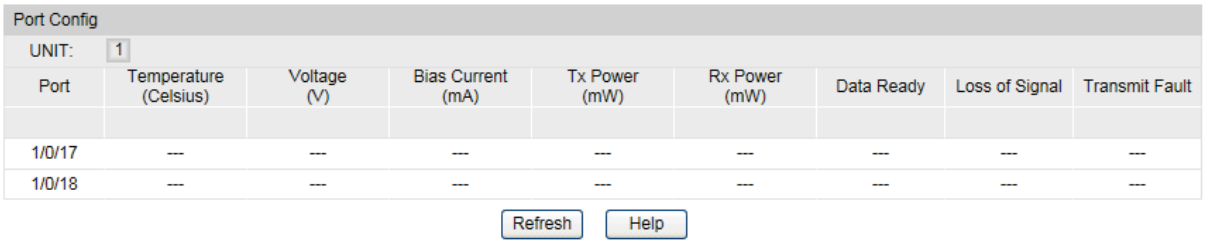
High Alarm	Specify the high threshold for the alarm. When the operating parameter rises above this value, action associated with the alarm will be taken. The valid values are from 0 to 6.5535.
Low Alarm	Specify the low threshold for the alarm. When the operating parameter falls below this value, action associated with the alarm will be taken. The valid values are from 0 to 6.5535.
High Warning	Specify the high threshold for the warning. When the operating parameter rises above this value, action associated with the warning will be taken. The valid values are from 0 to 6.5535.
Low Warning	Specify the low threshold for the warning. When the operating parameter falls below this value, action associated with the warning will be taken. The valid values are from 0 to 6.5535.
LAG	Displays the LAG number which the port belongs to.

2) Click **Apply**.

2.1.7 Viewing DDM Status

Choose the menu **Switching > DDM > DDM Status** to load the following page.

Figure 2-7 View DDM Status



In the **Port Config** table, view the current operating parameters for the SFP modules inserted into the SFP ports.

Temperature	The current temperature of the SFP module inserted into this port.
Voltage	The current voltage of the SFP module inserted into this port.
Bias Current	The current bias current of the SFP module inserted into this port.
Tx Power	The current Tx power of the SFP module inserted into this port.
Rx Power	The current Rx power of the SFP module inserted into this port.
Data Ready	Indicates whether SFP module is operational. The values are True and False.
Loss of Signal	Reports local SFP module signal loss. The values are True and False.
Transmit Fault	Reports remote SFP module signal loss. The values are True, False and No Signal.

2.2 Using the CLI

To complete DDM configuration, follow these steps:

1) Enable DDM on the SFP port.
2) Configure the shutdown condition.
3) Configure the specified threshold for warning or alarm.

2.2.1 Configuring DDM Globally

Follow these steps to enable DDM on specified SFP ports:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Enter interface configuration mode.
Step 3	**ddm state enable** Enable DDM on this SFP port.
Step 4	**show ddm configuration** state Display the DDM state of the SFP ports.
Step 5	**end** Return to Privileged EXEC Mode.

Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable DDM on SFP port 1/0/17:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/17

Switch(config-if)#ddm state enable

Switch(config-if)#show ddm configuration state

	DDM Status	Shutdown
Gi1/0/17	Enable	None
Gi1/0/18	Enable	None

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.2 Configuring DDM Shutdown

Follow these steps to configure settings for shutting down SFP ports when the alarm threshold or warning threshold is exceeded:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Enter interface configuration mode.
Step 3	**ddm shutdown {** none | warning | alarm **}** none: The port will not be shut down if the alarm threshold or warning threshold is exceeded. warning: Shut down the port when the warning threshold is exceeded. alarm: Shut down the port when the alarm threshold is exceeded.
Step 4	**show ddm configuration** state Display the DDM state of the SFP ports.
Step 5	**end** Return to Privileged EXEC Mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set SFP port 1/0/17 to shut down when the warning threshold is exceeded.

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/17

Switch(config-if)#ddm shutdown warning

Switch(config-if)#show ddm configuration state

	DDM Status	Shutdown
Gi1/0/17	Enable	Warning
Gi1/0/18	Enable	None

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.3 Configuring Temperature Threshold

Follow these steps to configure the threshold of the DDM temperature on the specified SFP port.

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Enter interface configuration mode.
Step 3	**ddm temperature_threshold {** high_alarm | high_warning | low_alarm | low-warning **}** *value* high_alarm: Specify the high threshold for the alarm. When the operating parameter rises above this value, action associated with the alarm will be taken. high_warning: Specify the high threshold for the warning. When the operating parameter rises above this value, action associated with the warning will be taken. low_alarm: Specify the low threshold for the alarm. When the operating parameter falls below this value, action associated with the alarm will be taken. low_warning: Specify the low threshold for the warning. When the operating parameter falls below this value, action associated with the warning will be taken. *value*: Enter the threshold value in Celsius. The valid values are from -128 to 127.996.
Step 4	**show ddm configuration** temperature Display the DDM temperature threshold on the SFP ports.
Step 5	**end** Return to Privileged EXEC Mode.

Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set SFP port 1/0/17's high alarm temperature threshold as 110 Celsius.

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/17

Switch(config-if)#ddm temperature_threshold high_alarm 110

Switch(config-if)#show ddm configuration temperature

Temperature Threshold(Celsius) :

	High Alarm	Low Alarm	High Warning	Low Warning
Gi1/0/17	110.000000	--	--	--
Gi1/0/18	--	--	--	--

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.4 Configuring Voltage Threshold

Follow these steps to configure the threshold of the DDM voltage on the specified SFP port.

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Enter interface configuration mode.
Step 3	**ddm voltage_threshold {** high_alarm | high_warning | low_alarm | low-warning **}** *value* high_alarm: Specify the high threshold for the alarm. When the operating parameter rises above this value, action associated with the alarm will be taken. high_warning: Specify the high threshold for the warning. When the operating parameter rises above this value, action associated with the warning will be taken. low_alarm: Specify the low threshold for the alarm. When the operating parameter falls below this value, action associated with the alarm will be taken. low_warning: Specify the low threshold for the warning. When the operating parameter falls below this value, action associated with the warning will be taken. *value*: Enter the threshold value in V. The valid values are from 0 to 6.5535.

Step 4	**show ddm configuration** voltage Display the DDM voltage threshold of the SFP ports.
Step 5	**end** Return to Privileged EXEC Mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set SFP port 1/0/17's high alarm threshold voltage as 5 V.

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/17

Switch(config-if)#ddm vlotage_threshold high_alarm 5

Switch(config-if)#show ddm configuration voltage

Voltage Threshold(V) :

	High Alarm	Low Alarm	High Warning	Low Warning
Gi1/0/17	5.000000	--	--	--
Gi1/0/18	--	--	--	--

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.5 Configuring Bias Current Threshold

Follow these steps to configure the threshold of the DDM bias current on the specified SFP port.

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Enter interface configuration mode.

Step 3	**ddm bias_current_threshold {** high_alarm | high_warning | low_alarm | low-warning **}** *value* high_alarm: Specify the high threshold for the alarm. When the operating parameter rises above this value, action associated with the alarm will be taken. high_warning: Specify the high threshold for the warning. When the operating parameter rises above this value, action associated with the warning will be taken. low_alarm: Specify the low threshold for the alarm. When the operating parameter falls below this value, action associated with the alarm will be taken. low_warning: Specify the low threshold for the warning. When the operating parameter falls below this value, action associated with the warning will be taken. *value*: Enter the threshold value in mA. The valid values are from 0 to 131.
Step 4	**show ddm configuration** bias_current Display the DDM bias current threshold of the SFP ports.
Step 5	**end** Return to Privileged EXEC Mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set SFP port 1/0/17's high alarm threshold bias current as 120 mA.

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/17

Switch(config-if)#ddm vlotage_threshold high_alarm 120

Switch(config-if)#show ddm configuration bias_current

Voltage Threshold(V) :

	High Alarm	Low Alarm	High Warning	Low Warning
Gi1/0/17	120.000000	--	--	--
Gi1/0/18	--	--	--	--

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.6 Configuring Tx Power Threshold

Follow these steps to configure the threshold of the DDM Tx power on the specified SFP port.

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Enter interface configuration mode.
Step 3	**ddm tx_power_threshold {** high_alarm | high_warning | low_alarm | low-warning **}** *value* high_alarm: Specify the high threshold for the alarm. When the operating parameter rises above this value, action associated with the alarm will be taken. high_warning: Specify the high threshold for the warning. When the operating parameter rises above this value, action associated with the warning will be taken. low_alarm: Specify the low threshold for the alarm. When the operating parameter falls below this value, action associated with the alarm will be taken. low_warning: Specify the low threshold for the warning. When the operating parameter falls below this value, action associated with the warning will be taken. *value*: Enter the threshold value in mW. The valid values are from 0 to 6.5535.
Step 4	**show ddm configuration** tx_power Display the DDM tx power threshold on the SFP ports.
Step 5	**end** Return to Privileged EXEC Mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set SFP port 1/0/17's high alarm threshold Tx power as 6 mW.

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/17

Switch(config-if)#ddm tx_power_threshold high_alarm 6

Switch(config-if)#show ddm configuration tx_power

Tx Power Threshold(mW) :

	High Alarm	Low Alarm	High Warning	Low Warning
Gi1/0/17	6.000000	--	--	--
Gi1/0/18	--	--	--	--

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.7 Configuring Rx Power Threshold

Follow these steps to configure the threshold of the DDM Rx power on the specified SFP port.

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Enter interface configuration mode.
Step 3	**ddm rx_power_threshold {** high_alarm | high_warning | low_alarm | low-warning **}** *value* high_alarm: Specify the high threshold for the alarm. When the operating parameter rises above this value, action associated with the alarm will be taken. high_warning: Specify the high threshold for the warning. When the operating parameter rises above this value, action associated with the warning will be taken. low_alarm: Specify the low threshold for the alarm. When the operating parameter falls below this value, action associated with the alarm will be taken. low_warning: Specify the low threshold for the warning. When the operating parameter falls below this value, action associated with the warning will be taken. *value*: Enter the threshold value in mW. The valid values are from 0 to 6.5535.
Step 4	**show ddm configuration** rx_power Display the DDM rx power threshold on the SFP ports.
Step 5	**end** Return to Privileged EXEC Mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set SFP port 1/0/17's high alarm threshold Rx power as 6 mW.

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/17

Switch(config-if)#ddm rx_power_threshold high_alarm 6

Switch(config-if)#show ddm configuration rx_power

Rx Power Threshold(mW) :

	High Alarm	Low Alarm	High Warning	Low Warning
Gi1/0/17	6.000000	--	--	--
Gi1/0/18	--	--	--	--

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.8 Viewing DDM Configuration

Follow these steps to view the DDM configuration.

Step 1	**configure** Enter global configuration mode.
Step 2	**show ddm configuration {** state | temperature | voltage | bias_current | tx_power | rx_power**}** state: Displays 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.
Step 3	**end** Return to Privileged EXEC Mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to view SFP ports' Rx power threshold.

Switch#configure

Switch(config)#show ddm configuration rx_power

Rx Power Threshold(mW) :

	High Alarm	Low Alarm	High Warning	Low Warning
Gi1/0/17	6.000000	--	--	--
Gi1/0/18	--	--	--	--

Switch(config)#end

2.2.9 Viewing DDM Status

Follow these steps to view the DDM status, which is the digital diagnostic monitoring status of SFP modules inserted into the switch's SFP ports.

Step 1	**configure** Enter global configuration mode.
Step 2	**show ddm status** Displays all the monitoring status of SFP modules.
Step 3	**end** Return to Privileged EXEC Mode.

The following example shows how to view SFP ports' DDM status.

Switch#configure

Switch(config)#show ddm status

	Temperature(C)		Voltage(V)	Bias Current(mA)	Tx Power(mW)
Rx Power(mW)	Data Ready		Rx Los	Tx Fault	
Gi1/0/17	--		--	--	--
--		--	--	--	
Gi1/0/18	--		--	--	--
--		--	--	--	

Switch(config)#end

3 Appendix: Default Parameters

Default settings of DDM are listed in the following table.

Table 3-1 Default Settings of DDM

Parameter	Default Setting
DDM Status	Enable. All the SFP ports are being monitored.
Threshold Action	None. The port will not be shut down even if the alarm or warning threshold is exceeded.

Part 8

Configuring L2PT

CHAPTERS

1. Overview
2. L2PT Configuration
3. Configuration Example
4. Appendix: Default Parameters

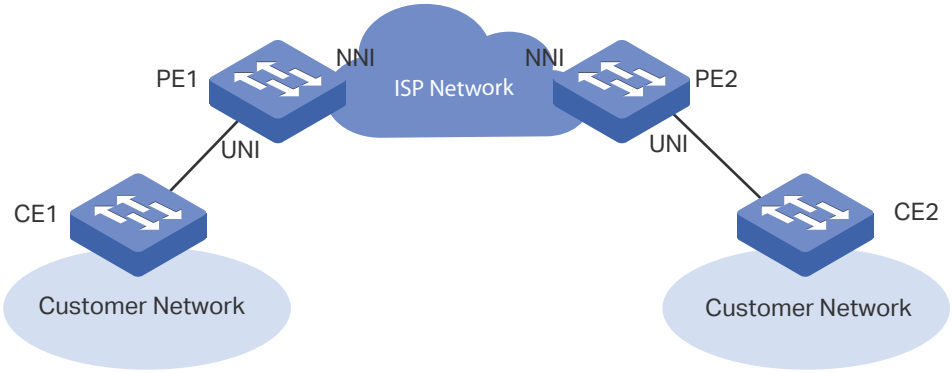
1 Overview

L2PT (Layer 2 Protocol Tunneling) is a feature for service providers to transparently transmit layer 2 protocol data units (PDUs) between customer networks at different locations through a public ISP network. Some terminology that is used in this section is defined as follows:

- Edge Switch: The switch that is connected to the customer network and placed on the boundary of the ISP network.
- UNI: User Network Interface, a port configured on the edge switch which is connected to the customer network.
- NNI: Network Network Interface, a port configured on the edge switch which is connected to the ISP network.

As shown in Figure 1-1, a customer has two local networks which are connected through the ISP network. When the two customer networks run the same layer 2 protocol, the layer 2 PDUs between them must be transmitted through the ISP network to perform layer 2 protocol calculation (for example, calculating a spanning tree). Generally, the PDUs of the same layer 2 protocol use the same destination MAC address. Therefore, when a layer 2 PDU from a customer network reaches a edge switch in the ISP network, the switch cannot identify whether the PDU comes from a customer network or the ISP network and then the PDU will be discarded. As a result, the layer 2 PDUs cannot be transmitted through the ISP network to the other side.

Figure 1-1 L2PT Application



To resolve this problem, the ISP network should transparently transmit the layer 2 PDUs between the two customer networks. In this case, L2PT feature can be configured on the edge switches (PE1 and PE2) to allow the layer 2 PDUs to be tunneled through the network.

The following describes the PDUs transmission procedure through the ISP network from one customer network to the other side:

1) Upon receiving a layer 2 PDU from CE1 via the UNI port, PE1 replaces the destination MAC address of the PDU with a special multicast MAC address (01:00:0c:cd:cd: d0) and then sends the PDU to the ISP network via the NNI port.
2) The ISP network identifies the PDU and directly forwards it to the other end.
3) PE2 receives the PDU via its NNI port and restores the destination MAC address of the PDU to its original destination MAC address.

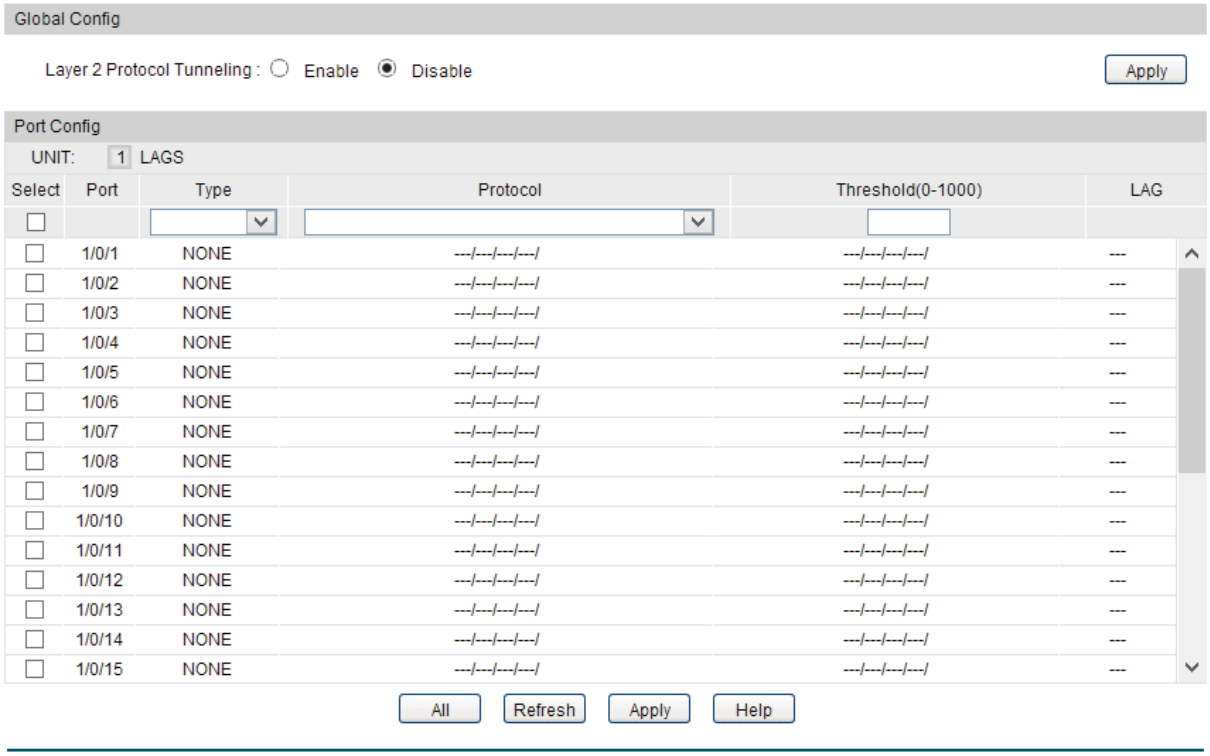
With L2PT feature configured accordingly, the switch can transparently transmit the PDUs of the following layer 2 protocols: STP (Spanning Tree Protocol), GVRP (GARP VLAN Registration Protocol), CDP (Cisco Discovery Protocol), VTP (VLAN Trunking Protocol), PAgP (Port Aggregation Protocol), UDLD (UniDirectional Link Detection) and PVST+(Per VLAN Spanning Tree Plus).

2 L2PT Configuration

2.1 Using the GUI

Choose the menu **Switching > L2PT > L2PT Config** to load the following page.

Figure 2-1 Configuring L2PT



Follow these steps to configure L2PT:

1) In the **Global Config** section, enable L2PT globally and click **Apply**.
2) In the **Port Config** section, configure the port that is connected to the customer network as a UNI port and specify your desired protocols on the port. In addition, you can also set the threshold for packets-per-second to be processed on the UNI port.

UNIT:1/LAGS	Click **1** to configure physical ports. Click **LAGS** to configure LAGs.
Type	Select **UNI** as the port type for the selected port. Usually, the UNI port is connected to the customer network. The default setting is **NONE**, which indicates that L2PT is disabled on this port.

Protocol	Specify the layer 2 protocol types of the packets that can be transparently transmitted on the selected port: **STP**: Enable protocol tunneling for the STP packets. **GVRP**: Enable protocol tunneling for the GVRP packets. **01000CCCCCCC**: Enable protocol tunneling for the CDP/VTP/PAgP/UDLD packets with their destination MAC address as 01-00-0C-CC-CC-CC. **01000CCCCCCD**: Enable protocol tunneling for the PVST+ packets with the destination MAC address as 01-00-0C-CC-CC-CD. **LACP:** Enable protocol tunneling for the LACP packets. **ALL**: All the above layer 2 protocols are supported for tunneling.
Threshold	Specify the maximum number of packets to be processed for the specified protocol on the port in one second. When the threshold is exceeded, the port drops the specified layer 2 protocol packets. This value ranges from 0 to 1000(packets/second). 0 indicates that the threshold feature is disabled.
LAG	Displays the link aggregation group which the port is in.

3) In the **Port Config** section, configure the port that is connected to the ISP network as an NNI port. Note that the protocols and threshold cannot be configured on the NNI port.

UNIT:1/LAGS	Click **1** to configure physical ports. Click **LAGS** to configure LAGs.
Type	Select **NNI** as the port type for the selected port. Usually, NNI port is connected to the ISP network. The default setting is **NONE**, which indicates that L2PT is disabled on this port.
LAG	Displays the link aggregation group which the port is in.

4) Click **Apply**.

2.2 Using the CLI

Follow these steps to configure L2PT feature.

Step 1	**configure** Enter global configuration mode.
Step 2	**l2protocol-tunnel** Enable the L2PT feature globally.

Step 3	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-id-list* **}** Enter interface configuration mode.
Step 4	**l2protocol-tunnel type uni {** 01000cccccc | 01000ccccccd | gvrp | stp | lacp | all **} [threshold** *threshold* **]** Configure the port as a UNI port, specify the layer 2 protocol types of the packets that can be transparently transmitted on the port, and set the threshold for packets-per-second accepted for encapsulation on the UNI port. 01000cccccc: Enable protocol tunneling for the CDP/VTP/PAgP/UDLD packets with their destination MAC address as 01-00-0C-CC-CC-CC. 01000ccccccd: Enable protocol tunneling for the PVST+ packets with the destination MAC address as 01-00-0C-CC-CC-CD. gvrp: Enable protocol tunneling for the GVRP packets. stp: Enable protocol tunneling for the STP packets. lacp: Enable protocol tunneling for the LACP packets. all: All the above layer 2 protocols are supported for tunneling. *threshold:* Set a threshold which determines the maximum number of packets to be processed for the specified protocol on the port in one second. When the threshold is exceeded, the port drops the specified layer 2 protocol packets. The valid values are from 0 to 1000 (packets/second). 0 indicates that the threshold feature is disabled.
Step 5	**exit** Return to global configuration mode.
Step 6	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-id-list* **}** Enter interface configuration mode.
Step 7	**l2protocol-tunnel type nni** Configure the port as an NNI port.
Step 8	**show l2protocol-tunnel global** Verify the global L2PT configuration.
Step 9	**show l2protocol-tunnel interface [fastEthernet** *port* **| gigabitEthernet** *port* **| port-channel** *port-channel-id* **]** Verify the L2PT configuration of the port or LAG.
Step 10	**end** Return to privileged EXEC mode.
Step 11	**copy running-config startup-config** Save the settings in the configuration file.

This example shows how to enable L2PT globally:

Switch#configure

Switch(config)#l2protocol-tunnel

Switch(config)#show l2protocol-tunnel global

l2protocol-tunnel State: Enable

Switch(config)#end

Switch#copy running-config startup-config

This example shows how to configure port 1/0/1 as a UNI port for the layer 2 protocol GVRP and set the threshold as 1000:

Switch#configure

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

Switch(config-if)#l2protocol-tunnel type uni gvrp **threshold** 1000

Switch(config-if)#show l2protocol-tunnel interface gigabitEthernet 1/0/1

Interface	Type	Protocol	Threshold	LAG
---	---	---	---	---
Gi1/0/1	uni	gvrp,--,--,-- --,--	1000,--,--,-- --,--	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

This example shows how to configure port 1/0/5 as an NNI port.

Switch#configure

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

Switch(config-if)#l2protocol-tunnel type nni

Switch(config-if)#show l2protocol-tunnel interface gigabitEthernet 1/0/5

Interface	Type	Protocol	Threshold	LAG
---	---	---	---	---
Gi1/0/5	nni	--,--,--,-- --,--	--,--,--,-- --,--	N/A

Switch(config-if)#end

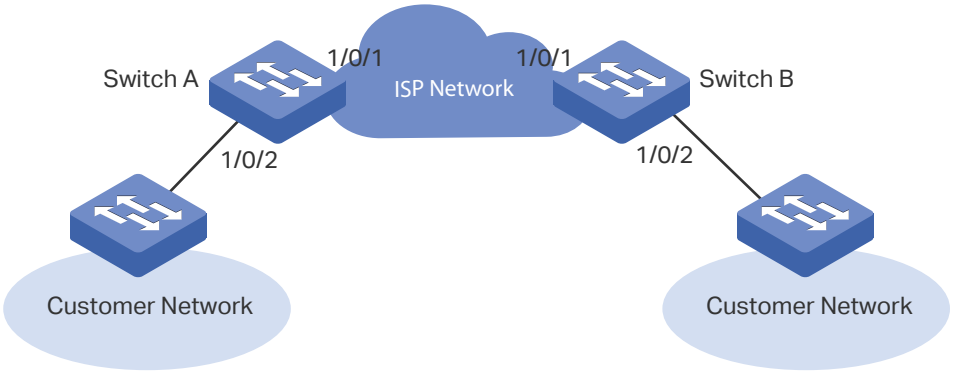
Switch#copy running-config startup-config

3 Configuration Example

3.1 Network Requirements

As shown below, the two branches of a company are connected through the ISP network, and they want to achieve spanning tree calculation by exchanging layer 2 STP packets with each other. To meet this requirement, the ISP network needs to transparently transmit the STP packets between the two customer networks.

Figure 3-1 Network Topology



3.2 Configuration Scheme

The service provider can configure L2PT on the two edge switches (Switch A and Switch B). With the L2PT feature, the STP packets can be encapsulated as normal data packets and sent to the other side without being processed by the devices in the ISP network.

The overview of configuration is as follows:

1) Enable the L2PT feature globally.
2) Specify port 1/0/1 which is connected to the ISP network as an NNI port.
3) Specify port 1/0/2 which is connected to the customer network as a UNI port for the STP. In addition, configure the threshold as 1000 to limit the number of packets to be processed on the port in one second.

Demonstrated with T2600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

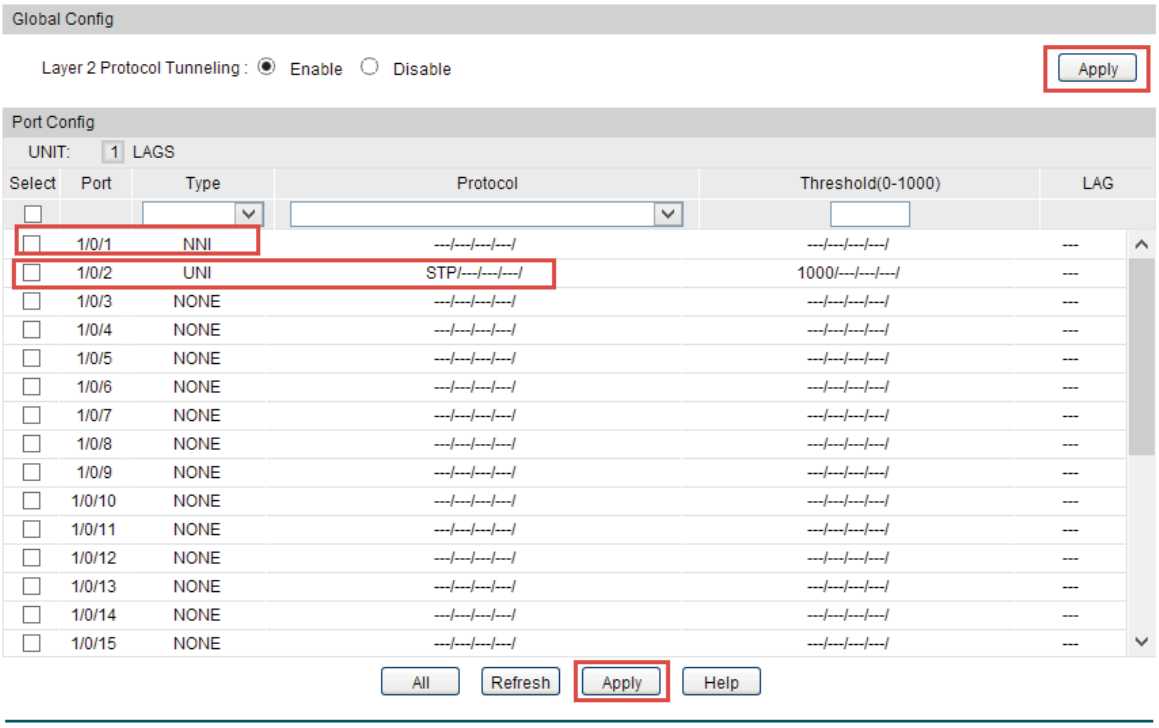
3.3 Using the GUI

The configurations of Switch A and Switch B are similar. The following introductions take Switch A as an example.

1) Choose the menu **Switching > L2PT > L2PT Config** to load the following page. Enable the L2PT feature globally and click **Apply**.

2) Specify port 1/0/1 as an NNI port and click **Apply**. Specify port 1/0/2 as a UNI port for the STP and set the threshold as 1000. Then click **Apply**. The configuration result is as follows:

Figure 3-2 Global Config



3) Click **Save Config** to save the settings.

3.4 Using the CLI

The configurations of Switch A and Switch B are similar. The following introductions take Switch A as an example.

Switch_A#configure

Switch_A(config)#l2protocol-tunnel

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

Switch_A(config-if)#l2protocol-tunnel type nni

Switch_A(config-if)#exit

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

Switch_A(config-if)#l2protocol-tunnel type uni stp threshold 1000

Switch_A(config-if)#end

Switch_A#copy running-config startup-config

Verify the Configuration

Verify the global configuration:

```
Switch_A#show l2protocol-tunnel global
l2protocol-tunnel State:        Enable
```

Verify the configuration on port 1/0/1:

```
Switch_A#show l2protocol-tunnel interface gigabitEthernet 1/0/1
Interface       Type      Protocol        Threshold         LAG
---------       ----      --------        ---------         ----
Gi1/0/1          nni      --,--,--,       --,--,--,         N/A
                                 --,--          --,--
```

Verify the configuration on port 1/0/2:

```
Switch_A#show l2protocol-tunnel interface gigabitEthernet 1/0/2
Interface       Type      Protocol        Threshold         LAG
---------       ----      --------        ---------         ----
Gi1/0/2          uni      stp,--,--,      1000,--,--,       N/A
                                 --,--          --,--
```

4 Appendix: Default Parameters

Default settings of L2PT are listed in the following table.

Table 4-1 Default Settings of L2PT

Parameter	Defualt Setting
Global Config	
Layer 2 Protocol Tunneling	Disable
Port Config	
Type	NONE
Protocol	NONE
Threshold	Disable

Part 9

Configuring 802.1Q VLAN

CHAPTERS

1. Overview
2. 802.1Q VLAN Configuration
3. Configuration Example
4. Appendix: Default Parameters

1 Overview

VLAN (Virtual Local Area Network) is a network technique that solves broadcasting issues in local area networks. It is usually applied in the following occasions:

- To restrict broadcast domain: VLAN technique divides a big local area network into several VLANs, and all VLAN traffic remains within its VLAN. It reduces the influence of broadcast traffic in Layer 2 network to the whole network.

- To enhance network security: Devices from different VLANs cannot achieve Layer 2 communication, and thus users can group and isolate devices to enhance network security.

- For easier management: VLANs group devices logically instead of physically, so devices in the same VLAN need not be located in the same place. It eases the management of devices in the same work group but located in different places.

2 802.1Q VLAN Configuration

To complete 802.1Q VLAN configuration, follow these steps:

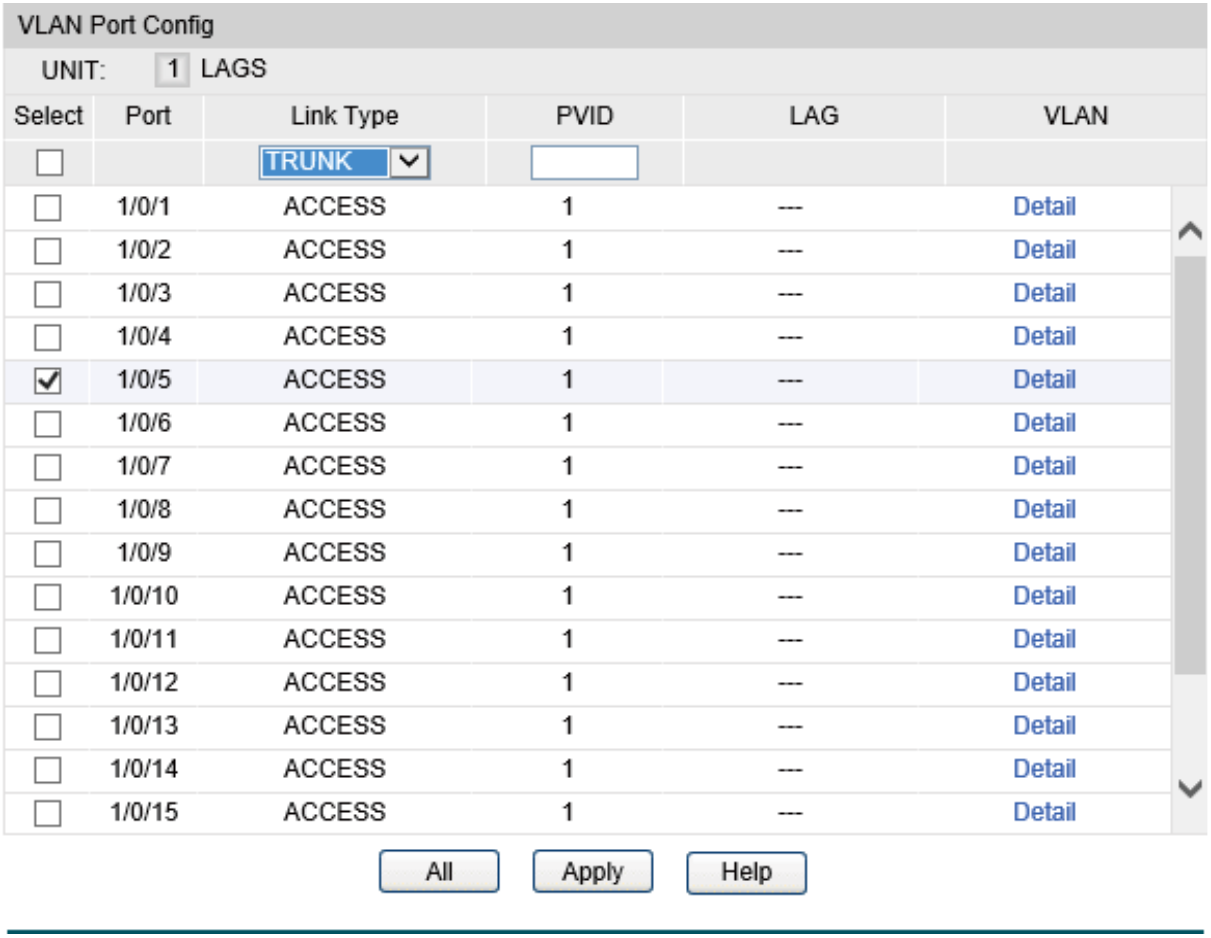
1) Configure PVID (Port VLAN ID) of the port;
2) Configure the VLAN, including creating a VLAN and adding the configured port to the VLAN.

2.1 Using the GUI

2.1.1 Configuring the PVID of the Port

Choose the menu **VLAN > 802.1Q VLAN > Port Config** to load the following page.

Figure 2-1 Configuring the Port



Select a port and configure its PVID. Click **Apply**.

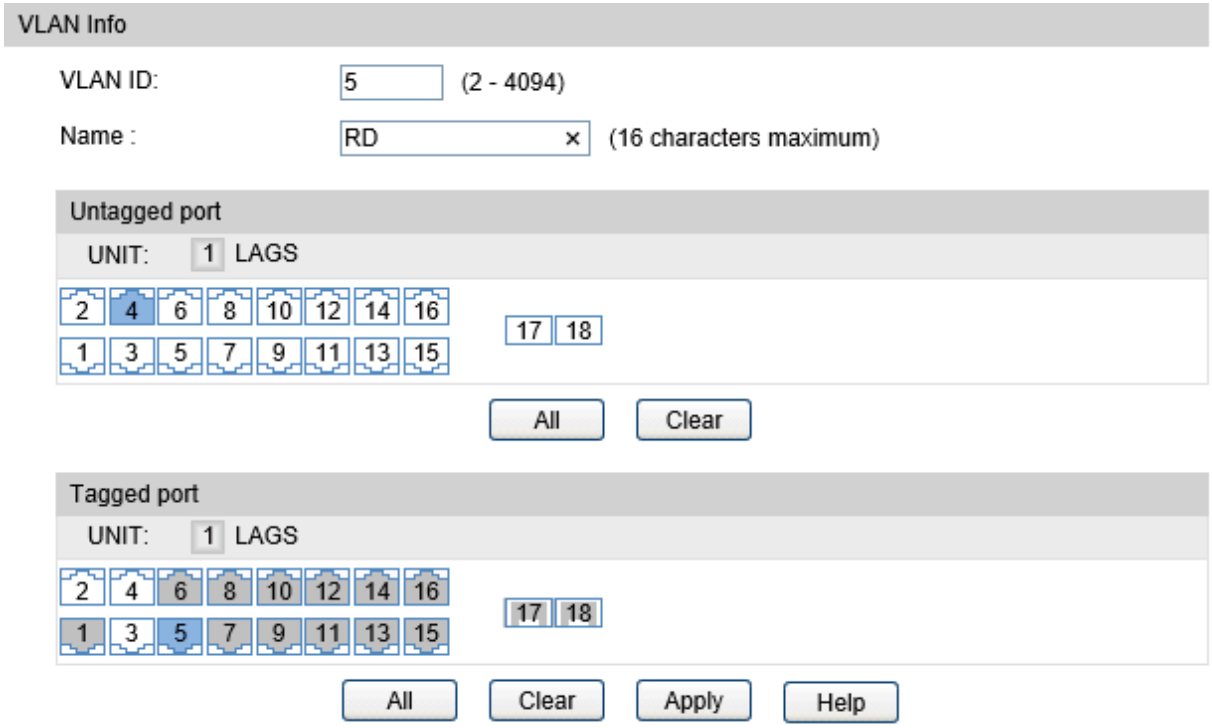
Link Type	Select the link type of the port. It is Access by default. **ACCESS**: The port can only be added to one VLAN and is usually connected to a terminal device that does not support VLAN, a host for example. When receiving frames: • The port accepts untagged frames and adds a VLAN tag with the PVID to the frames. • The port accepts the tagged frames if the frames' VLAN IDs match its PVID. • The port drops the tagged frames if the frames' VLAN IDs differ from its PVID. When forwarding frames: • The port forwards the frames without tag. **TRUNK**: The port can be added to more than one VLAN and is usually connected to an intermediate device, such as a switch or a router, to carry traffic in different VLANs. When receiving frames: • The port adds a VLAN tag with the PVID to the untagged frames, and then decides to accept or drop the frame according to whether the PVID is in the port's allowed VLAN list. • The port accepts the tagged frames if the frames' VLAN ID are in its allowed VLAN list. • The port drops the tagged frames if the frames' VLAN ID are not in its allowed VLAN list. When forwarding frames: • Normally, the port forwards the frames with tags. If the frames' VLAN tags match its PVID, the port will forward the frames without tag. **GENERAL**: The port can be added to more than one VLAN and is usually connected to an intermediate or terminal device. You can configure the egress rule on the **VLAN > 802.1Q VLAN > VLAN Config** page according to the connected device. When receiving frames: • The behavior of a General port is the same with that of a Trunk port. When forwarding frames: • The port decides to forward the frames with or without tag according to the egress rule. You need to specify the egress rule as tagged or untagged when adding the port to each VLAN.
PVID	Set the default VLAN ID of the port. The valid values are from 1 to 4094. It is used mainly in the following two ways: • When the port receives an untagged packet, the switch inserts a VLAN tag to the packet based on the PVID. • When the port receives an untagged UL packet or an untagged broadcast packet, the switch broadcasts the packet within the default VLAN.
LAG	Displays the LAG (Link Aggregation Group) which the port belongs to.

VLAN	Check details of the VLAN which the port is in.

2.1.2 Configuring the VLAN

Choose the menu **VLAN > 802.1Q VLAN > VLAN Config** and click **Create** to load the following page.

Figure 2-2 Configuring VLAN



Follow these steps to configure VLAN:

1) Enter a VLAN ID and a description for identification to create a VLAN.

VLAN ID	Enter a VLAN ID for identification with the values between 2 and 4094.
Name	Give a VLAN description for identification with up to 16 characters.

2) Select the untagged port(s) and the tagged port(s) respectively to add to the created VLAN based on the network topology.

Untagged port	The selected ports will forward untagged packets in the target VLAN.
Tagged port	The selected ports will forward tagged packets in the target VLAN.

3) Click **Apply**.

2.2 Using the CLI

2.2.1 Creating a VLAN

Follow these steps to create a VLAN:

Step 1	**configure** Enter global configuration mode.
Step 2	**vlan** *vlan-list* When you enter a new VLAN ID, the switch creates a new VLAN and enters VLAN configuration mode; when you enter an existing VLAN ID, the switch directly enters VLAN configuration mode. *vlan-list*: Specify the ID or the ID list of the VLAN(s) for configuration. The valid values are from 2 to 4094, for example, 2-3,5.
Step 3	**name** *descript* (Optional) Specify a VLAN description for identification. *descript*: The length of the description should be 1 to 16 characters.
Step 4	**show vlan** [id *vlan-list*] Show the global information of the specified VLAN(s). When no VLAN is specified, this command shows global information of all 802.1Q VLANs. *vlan-list*: Specify the ID or the ID list of the VLAN(s) to show information. The valid values are from 1 to 4094.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create VLAN 2 and name it as RD :

Switch#configure

Switch(config)#vlan 2

Switch(config-vlan)#name RD

Switch(config-vlan)#show vlan id 2

VLAN	Name	Status	Ports
2	RD	active	

Switch(config-vlan)#end

Switch#copy running-config startup-config

2.2.2 Configuring the Port

Follow these steps to configure the port:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *lag-id* **| range port-channel** *lag-list* **}** Enter interface configuration mode. *port* |*port-list*: The number or the list of the Ethernet port that you want to configure. *lag-id* |*lag-list:* The ID or the list of the LAG that you want to configure.
Step 3	**switchport mode {** access | trunk | general **}** Specify the link type of the port. access | trunk | general: The link type. By default, it is Access.
Step 4	**switchport pvid** *vlan-id* Configure the PVID of the port(s). By default, it is 1. *vlan-id*: The default VLAN ID of the port with the values between 1 and 4094.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the link type of port 1/0/5 as Trunk, the PVID of port 1/0/5 as VLAN 2:

Switch#configure

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

Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport pvid 2

Switch(config-if)#show interface switchport gigabitEthernet 1/0/5

Port Gi1/0/5:

PVID: 2

Member in LAG: N/A

Link Type: Trunk

Member in VLAN:

```
Vlan    Name            Egress-rule
----    ----------      ---------------
1       System-VLAN     Tagged
```

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.3 Adding the Port to the Specified VLAN

Follow these steps to add the port to the specified VLAN:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *lag-id* **| range port-channel** *lag-list* **}** Enter interface configuration mode. *port* |*port-list*: The number or the list of the Ethernet port that you want to configure. *lag-id* |*lag-list:* The ID or the list of the LAG that you want to configure.
Step 3	**switchport access vlan** *vlan-id* **switchport trunk allowed vlan** *vlan-list* **switchport trunk allowed vlan all** **switchport general allowed vlan** *vlan-list* **{** tagged **|** untagged **}** Add Access/Trunk/General port to the specified VLAN. *vlan-id	vlan-list:* Specify the ID or ID list of the VLAN(s) that the port will be added to. The ID ranges from 1 to 4094. tagged **|** untagged: Egress rule for the port.
Step 4	**show interface switchport [fastEthernet** *port* **| gigabitEthernet** *port* **| port-channel** *lag-id***]** Verify the information of the port. *port*: Specify the ID of the port to show information. *lag-id*: Specify the ID of the LAG to show information.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to add the General port 1/0/5 to VLAN 2, and specify its egress rule as tagged:

Switch#configure

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

Switch(config-if)#switchport general allowed vlan 2 tagged

Switch(config-if)#show interface switchport gigabitEthernet 1/0/5

Port Gi1/0/5:

PVID: 2

Member in LAG: N/A

Link Type: General

Member in VLAN:

Vlan	Name	Egress-rule
1	System-VLAN	Untagged
2	rd	Tagged

Switch(config-if)#end

Switch#copy running-config startup-config

3 Configuration Example

3.1 Network Requirements

- Offices of both Department A and Department B in the company are located in different places, and computers in different offices are connected to different switches.
- It is required that computers can communicate with each other in the same department but not with computers in the other department.

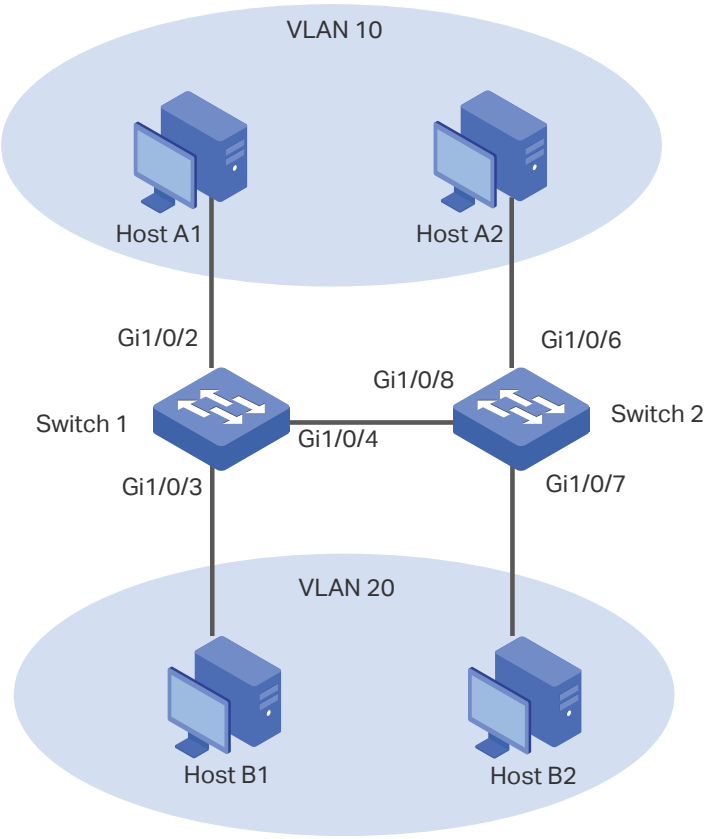
3.2 Configuration Scheme

- Divide computers in Department A and Department B into two VLANs respectively so that computers can communicate with each other in the same department but not with computers in the other department.
- Terminal devices like computers usually do not support VLAN tags. Configure the switch ports connected to the computers as Access. Then add the ports to the corresponding VLANs.
- The intermediate link between two switches carries traffic from two VLANs simultaneously. Configure the ports on both ends of the intermediate link as Trunk, and add the ports to both VLANs.

3.3 Network Topology

The figure below shows the network topology. Host A1 and Host A2 are used in Department A, while Host B1 and Host B2 are used in Department B. Switch 1 and Switch 2 are located in two different places. Host A1 and Host B1 are connected to port 1/0/2 and port 1/0/3 on Switch 1 respectively, while Host A2 and Host B2 are connected to port 1/0/6 and port 1/0/7 on Switch 2 respectively. Port 1/0/4 on Switch 1 is connected to port 1/0/8 on Switch 2.

Figure 3-1 Network Topology



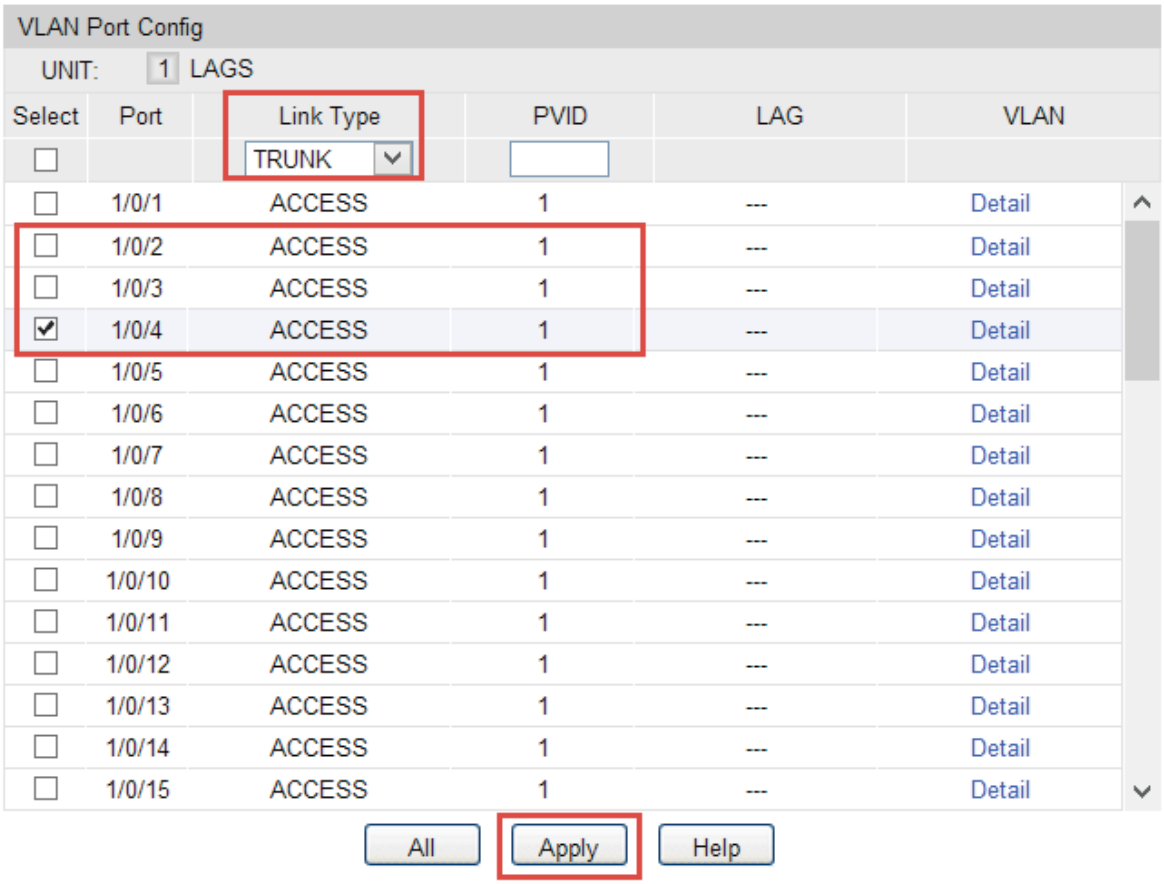
Demonstrated with T2600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

3.4 Using the GUI

The configurations of Switch 1 and Switch 2 are similar. The following introductions take Switch 1 as an example.

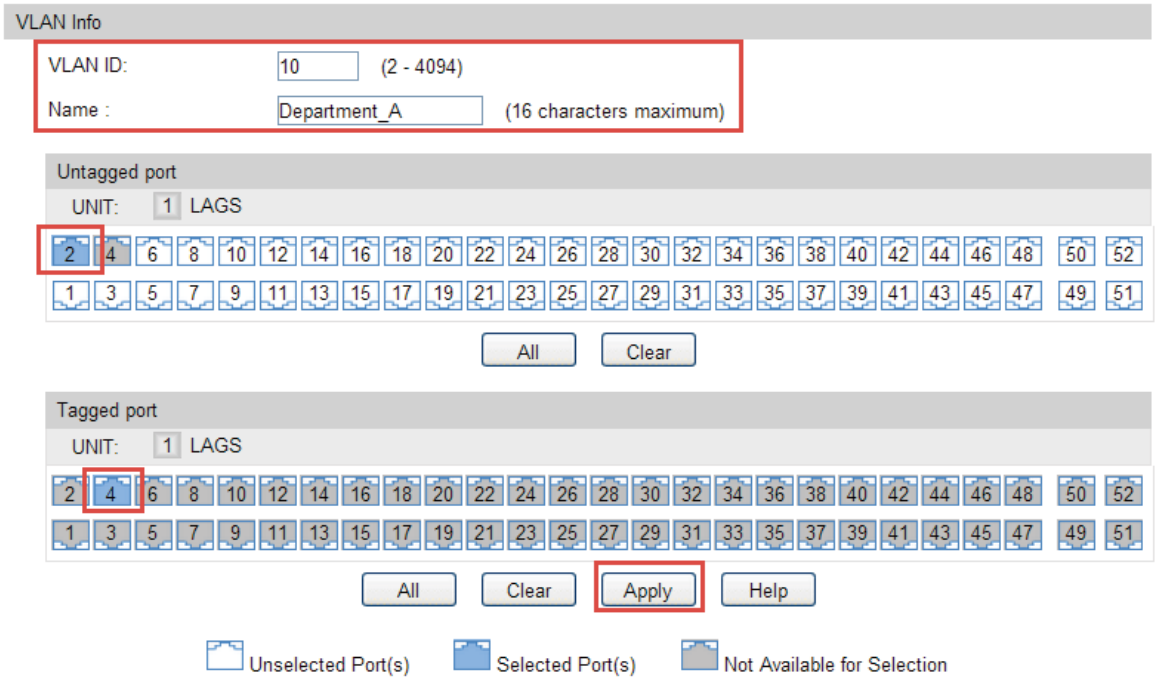
1) Choose the menu **VLAN > 802.1Q VLAN > Port Config** to load the following page. For port 1/0/2 and port 1/0/3, set the link type as **Access**; for port 1/0/4, set the link type as **Trunk**. Then click **Apply**.

Figure 3-2 Create VLAN 10 for Department A



2) Choose the menu **VLAN > 802.1Q VLAN > VLAN Config** and click **Create** to load the following page. Create VLAN 10 with the description of Department_A. Add port 1/0/2 as an untagged port and port 1/0/4 as a tagged port to VLAN 10. Then click **Apply**.

Figure 3-3 Create VLAN 10 for Department A



3) Click **Create** again to load the following page. Create VLAN 20 with the description of Department_B. Add port 1/0/2 as an untagged port and port 1/0/4 as a tagged port to VLAN 20. Then click **Apply**.

Figure 3-4 Create VLAN 20 for Department B



4) Click **Save Config** to save the settings.

3.5 Using the CLI

The configurations of Switch 1 and Switch 2 are similar. The following introductions take Switch 1 as an example.

1) Create VLAN 10 for Department A, and configure the description as Department-A. Similarly, create VLAN 20 for Department B, and configure the description as Department-B.

   Switch_1#configure

   Switch_1(config)#vlan 10

   Switch_1(config-vlan)#name Department-A

   Switch_1(config-vlan)#exit

   Switch_1(config)#vlan 20

   Switch_1(config-vlan)#name Department-B

   Switch_1(config-vlan)#exit

2) Set the link type of port 1/0/2 and port 1/0/3 as Access, and then add port 1/0/2 to VLAN 10 and add port 1/0/3 to VLAN 20.

   Switch_1(config)#interface gigabitEthernet 1/0/2

   Switch_1(config-if)#switchport mode access

   Switch_1(config-if)#switchport access vlan 10

   Switch_1(config-if)#exit

   Switch_1(config)#interface gigabitEthernet 1/0/3

   Switch_1(config-if)#switchport mode access

   Switch_1(config-if)#switchport access vlan 20

   Switch_1(config-if)#exit

3) Set the link type of port 1/0/4 as Trunk, and then add it to both VLAN 10 and VLAN 20.

   Switch_1(config)#interface gigabitEthernet 1/0/4

   Switch_1(config-if)#switchport mode trunk

   Switch_1(config-if)#switchport trunk allowed vlan 10,20

   Switch_1(config-if)#end

   Switch_1#copy running-config startup-config

Verify the Configurations

Switch_1#show vlan

```
VLAN     Name            Status     Ports
---------  ----------------  ----------  ------------------------
1          Default VLAN      active     Gi1/0/1, Gi1/0/4,
                                        Gi1/0/5, Gi1/0/6, Gi1/0/7, Gi1/0/8,
                                        ...
                                        Gi1/0/15, Gi1/0/16, Gi1/0/17, Gi1/0/18
10         Department-A      active     Gi1/0/2, Gi1/0/4
20         Department-B      active     Gi1/0/3, Gi1/0/4
```

4 Appendix: Default Parameters

Default settings of 802.1Q VLAN are listed in the following table.

Table 4-1 Default Settings of 802.1Q VLAN

Parameter	Default Setting
VLAN ID	1
PVID	1
Link Type	ACCESS

Part 10

Configuring MAC VLAN

CHAPTERS

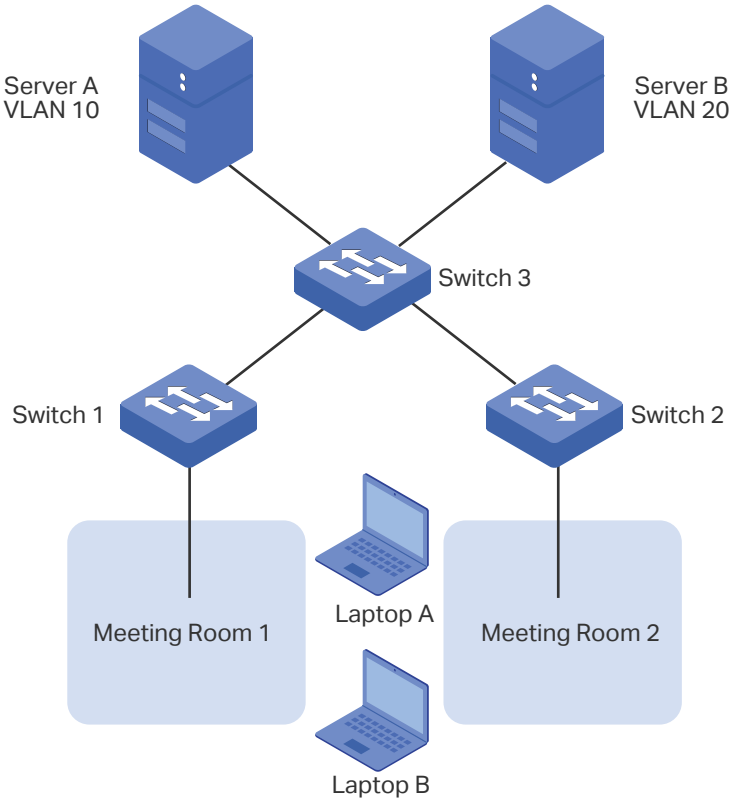
1. Overview
2. MAC VLAN Configuration
3. Configuration Example
4. Appendix: Default Parameters

1 Overview

VLAN is generally divided by ports. This way of division is simple but isn't suitable for those networks that require frequent topology changes. With the popularity of mobile office, a terminal device may access the switch via different ports. For example, a terminal device that accessed the switch via port 1 last time may change to port 2 this time. If port 1 and port 2 belong to different VLANs, the user has to re-configure the switch to access the original VLAN. Using MAC VLAN can free the user from such a problem. It divides VLANs based on the MAC addresses of terminal devices. In this way, terminal devices always belong to their original VLANs even when their access ports change.

The figure below shows a common application scenario of MAC VLAN.

Figure 1-1 Common Application Scenario of MAC VLAN



Two departments share all the meeting rooms in the company, but use different servers and laptops. Department A uses Server A and Laptop A, while Department B uses Server B and Laptop B. Server A is in VLAN 10 while Server B is in VLAN 20. It is required that Laptop A can only access Server A and Laptop B can only access Server B, no matter which meeting room the laptops are being used in. To meet this requirement, simply bind the MAC addresses of the laptops to the corresponding VLANs respectively. In this way, the MAC address rather than the access port determines the VLAN each laptop joins. Each laptop can access only the server in the VLAN it joins.

2 MAC VLAN Configuration

To complete MAC VLAN configuration, follow these steps:

1) Configure 802.1Q VLAN.
2) Bind the MAC address to the VLAN.
3) Enable MAC VLAN for the port.

Configuration Guidelines

When a port in a MAC VLAN receives an untagged data packet, the switch will first check whether the source MAC address of the data packet has been bound to the MAC VLAN. If yes, the switch will insert the corresponding tag to the data packet and forward it within the VLAN. If no, the switch will continue to match the data packet with the matching rules of other VLANs (such as the protocol VLAN). If there is a match, the switch will forward the data packet. Otherwise, the switch will process the data packet according to the processing rule of the 802.1 Q VLAN. When the port receives a tagged data packet, the switch will directly process the data packet according to the processing rule of the 802.1 Q VLAN.

2.1 Using the GUI

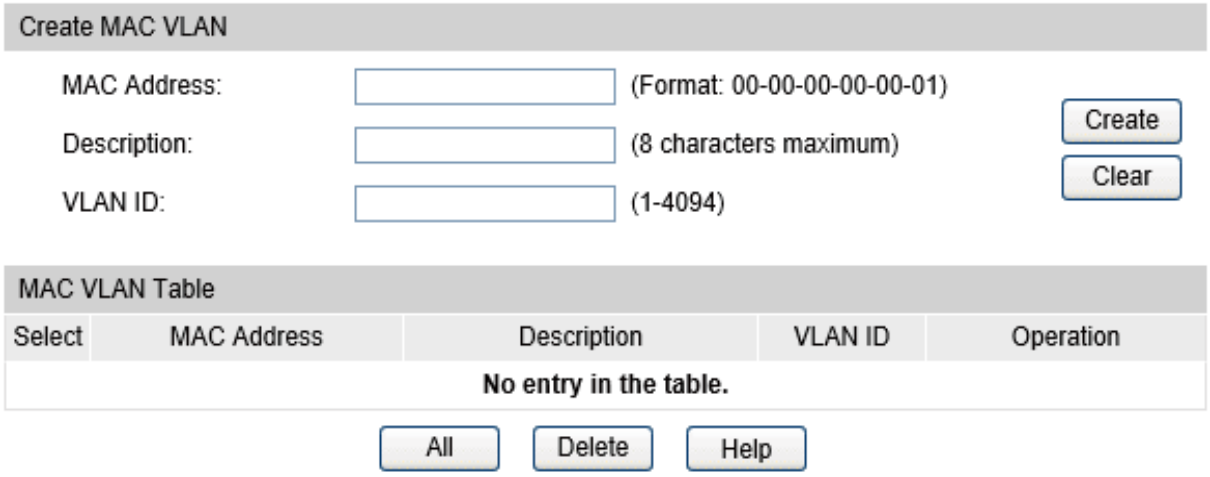
2.1.1 Configuring 802.1Q VLAN

Before configuring MAC VLAN, create an 802.1Q VLAN and set the port type according to network requirements. For details, refer to *Configuring 802.1Q VLAN*.

2.1.2 Binding the MAC Address to the VLAN

Choose the menu **VLAN > MAC VLAN > MAC VLAN** to load the following page.

Figure 2-1 MAC VLAN Configuration



Follow these steps to bind the MAC address to the VLAN:

1) Enter the MAC address of the device, give it a description, and enter the VLAN ID to bind it to the VLAN.

MAC Address	Enter the MAC address of the device. The address should be in 00-00-00-00-00-01 format.
Description	Give a MAC address description for identification with up to 8 characters.
VLAN ID	Enter the ID of the 802.1Q VLAN where the port with MAC VLAN enabled is.

2) Click **Create** to create the MAC VLAN.

Note:

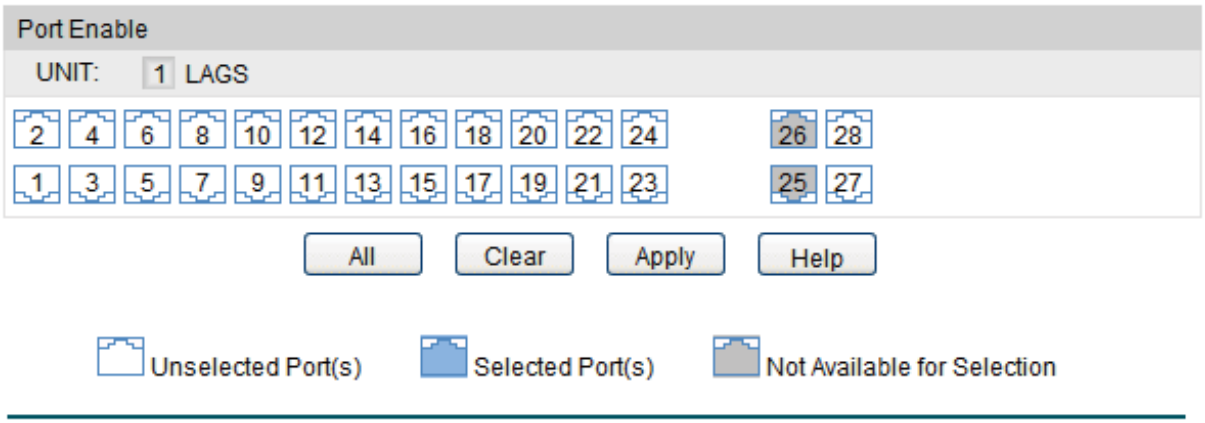
One MAC address can be bound to only one VLAN.

2.1.3 Enabling MAC VLAN for the Port

By default, MAC VLAN is disabled on all ports. You need to enable MAC VLAN for your desired ports manually.

Choose the menu **VLAN > MAC VLAN > Port Enable** to load the following page.

Figure 2-2 Enable MAC VLAN for the Port



Follow these steps to enable MAC VLAN for the port:

Select your desired ports to enable MAC VLAN, and click **Apply**.

Note:

The member port of an LAG (Link Aggregation Group) follows the configuration of the LAG but not its own. The configurations of the port can take effect only after it leaves the LAG.

2.2 Using the CLI

2.2.1 Configuring 802.1Q VLAN

Before configuring MAC VLAN, create an 802.1Q VLAN and set the port type according to network requirements. For details, refer to *Configuring 802.1Q VLAN*.

2.2.2 Binding the MAC Address to the VLAN

Follow these steps to bind the MAC address to the VLAN:

Step 1	**configure** Enter global configuration mode.
Step 2	**mac-vlan mac-address** *mac-addr* **vlan** *vlan-id* **[description** *descript***]** Bind the MAC address to the VLAN. *mac-addr*: MAC address of the device. The address should be in xx:xx:xx:xx:xx:xx format. *vlan-id*: ID of the 802.1Q VLAN where the port with MAC VLAN enabled is. *descript*: MAC address description for identification, with up to 8 characters.

Step 3	**show mac-vlan VLAN** *vid* Verify the configuration of MAC VLAN. *vid*: Specify the MAC VLAN to be displayed.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to bind the MAC address 00:19:56:8A:4C:71 to VLAN 10, with the address description as Dept.A.

Switch#configure

Switch(config)#mac-vlan mac-address 00:19:56:8a:4c:71 **vlan** 10 **description** Dept.A

Switch(config)#show mac-vlan vlan 10

MAC-Addr	Name	VLAN-ID
00:19:56:8A:4C:71	Dept.A	10

Switch(config)#end

Switch#copy running-config startup-config

2.2.3 Enabling MAC VLAN for the Port

Follow these steps to enable MAC VLAN for the port:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *lag-id* **| range port-channel** *lag-list* **}** Enter interface configuration mode. *port* |*port-list*: The number or the list of the Ethernet port that you want to configure. *lag-id* |*lag-list:* The ID or the list of the LAG that you want to configure.
Step 3	**mac-vlan** Enable MAC VLAN for the port.
Step 4	**show mac-vlan interface** Verify the configuration of MAC VLAN on each interface.

Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable MAC VLAN for port 1/0/1.

Switch#configure

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

Switch(config-if)#mac-vlan

Switch(config-if)#show mac-vlan interface

Port STATUS

------- -----------

Gi1/0/1 Enable

Gi1/0/2 Disable

...

Switch(config-if)#end

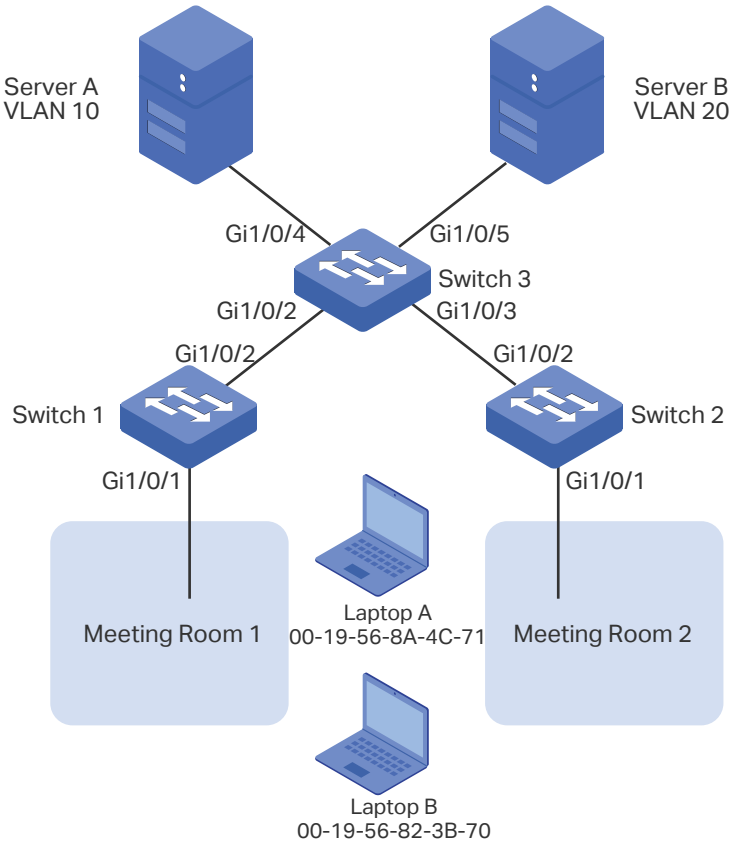
Switch#copy running-config startup-config

3 Configuration Example

3.1 Network Requirements

Two departments share all the meeting rooms in the company, but use different servers and laptops. Department A uses Server A and Laptop A, while Department B uses Server B and Laptop B. Server A is in VLAN 10 while Server B is in VLAN 20. It is required that Laptop A can only access Server A and Laptop B can only access Server B, no matter which meeting room the laptops are being used in. The figure below shows the network topology.

Figure 3-1 Network Topology



3.2 Configuration Scheme

You can configure MAC VLAN to meet this requirement. On Switch 1 and Switch 2, bind the MAC addresses of the laptops to the corresponding VLANs respectively. In this way, each laptop can access only the server in the VLAN it joins, no matter which meeting room the laptops are being used in. The overview of the configuration is as follows:

1) Create VLAN 10 and VLAN 20 on each of the three switches, set different port types, and add the ports to the VLANs based on the network topology. Note: For the ports connecting the laptops, set the link type as General, and set the egress rule as

Untagged; for the ports connecting to other switch, set the link type as General, and set the egress rule as Tagged.

2) On Switch 1 and Switch 2, bind the MAC addresses of the laptops to their corresponding VLANs, and enable MAC VLAN for the ports.

Demonstrated with T2600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

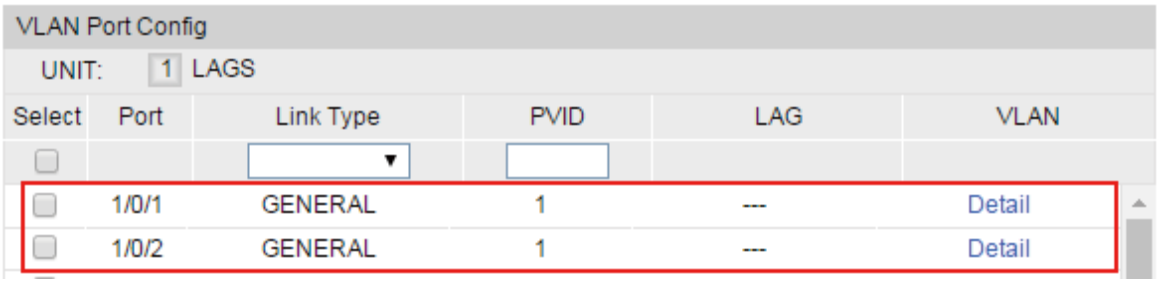
3.3 Using the GUI

- Configurations for Switch 1 and Switch 2

The configurations of Switch 1 and Switch 2 are similar. The following introductions take Switch 1 as an example.

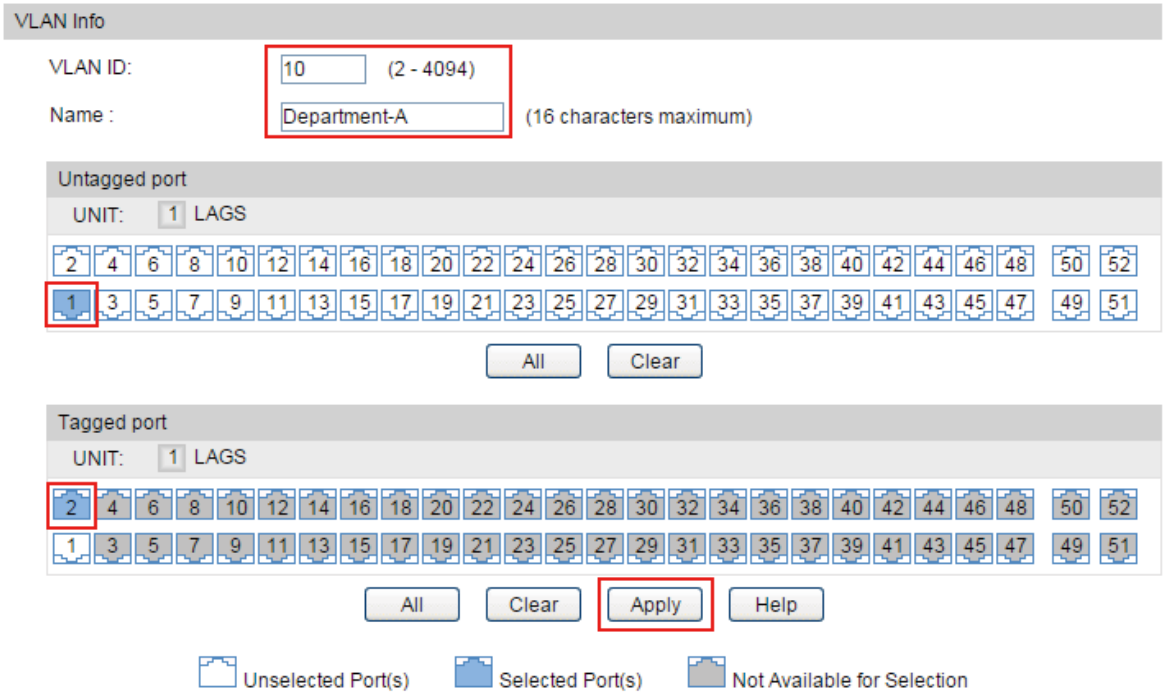
1) Choose the menu **VLAN > 802.1Q VLAN > Port Config** to load the following page. Set the link type of port1/0/1 and port1/0/2 as **General,** and click **Apply**.

Figure 3-2 Port Configuration



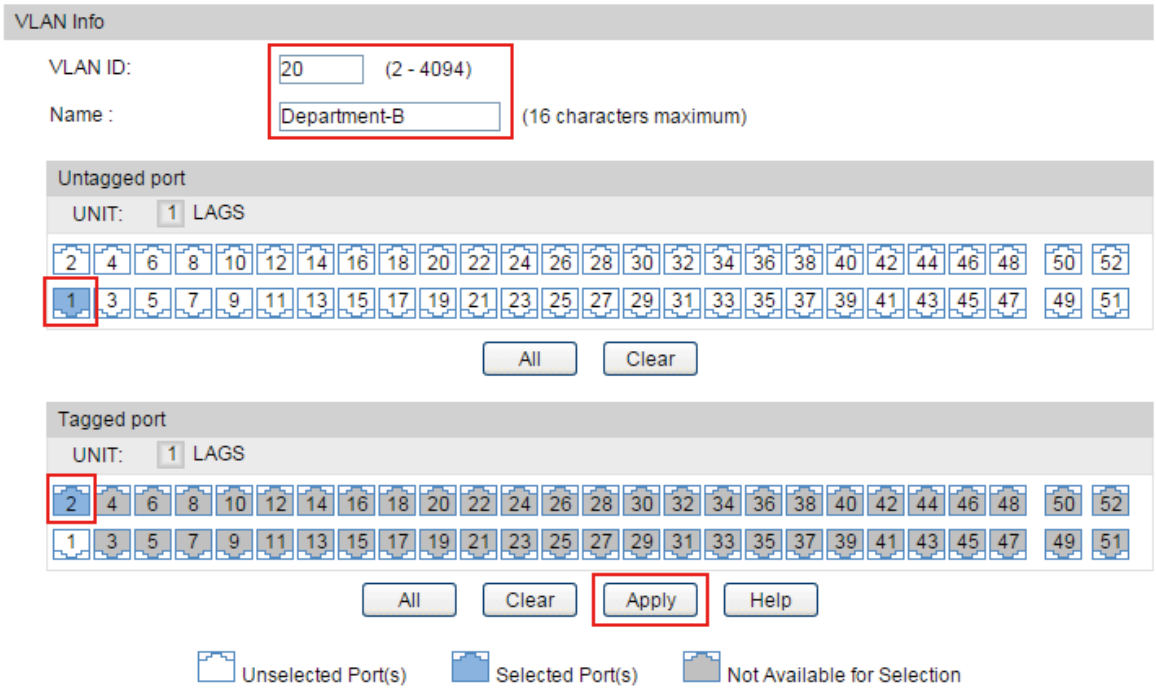
2) Choose the menu **VLAN > 802.1Q VLAN > VLAN Config** and click **Create** to load the following page. Create VLAN 10, and add port 1/0/1 as untagged port and port 1/0/2 as tagged ports to VLAN 10. Click **Apply**.

Figure 3-3 VLAN 10 Configuration



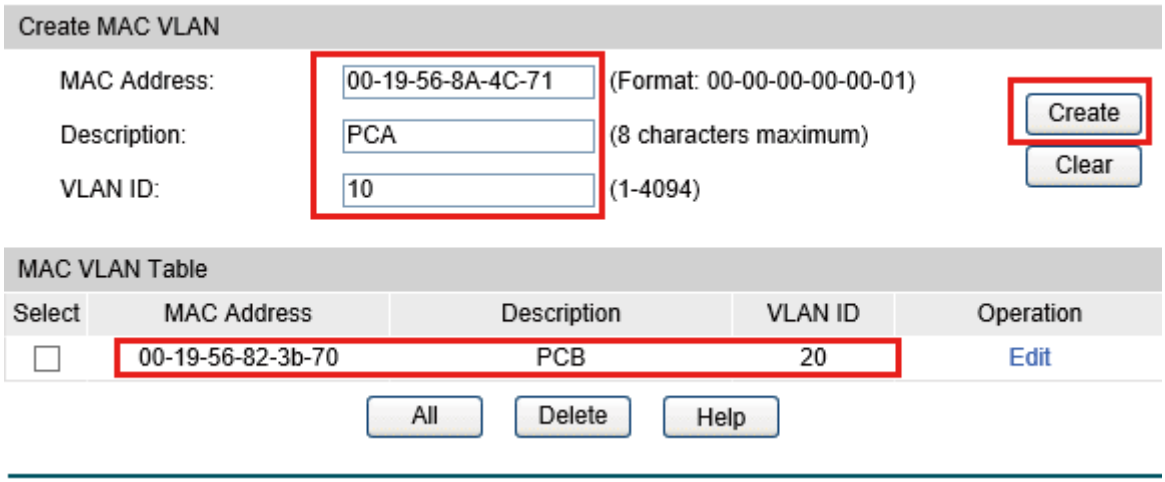
3) Choose the menu **VLAN > 802.1Q VLAN > VLAN Config** and click **Create** to load the following page. Create VLAN 20, and add port 1/0/1 as untagged port and port 1/0/2 as tagged ports to VLAN 20. Click **Apply**.

Figure 3-4 VLAN 20 Configuration



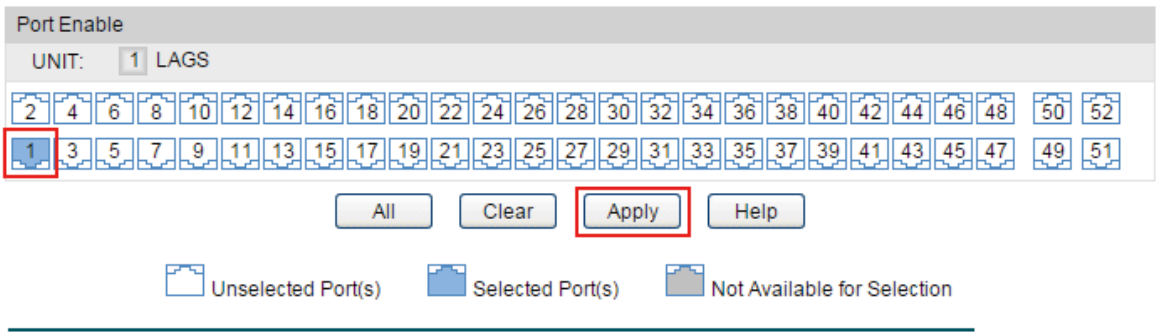
4) Choose the menu **VLAN > MAC VLAN > MAC VLAN** to load the following page. Enter **MAC Address**, **Description**, **VLAN ID** and click **Create** to bind the MAC address of Laptop A to VLAN 10 and bind the MAC address of Laptop B to VLAN 20.

Figure 3-5 MAC VLAN Configuration



5) Choose the menu **VLAN > MAC VLAN > Port Enable** to load the following page. Select port 1/0/1 and click **Apply** to enable MAC VLAN for it.

Figure 3-6 Enable MAC VLAN for the Port

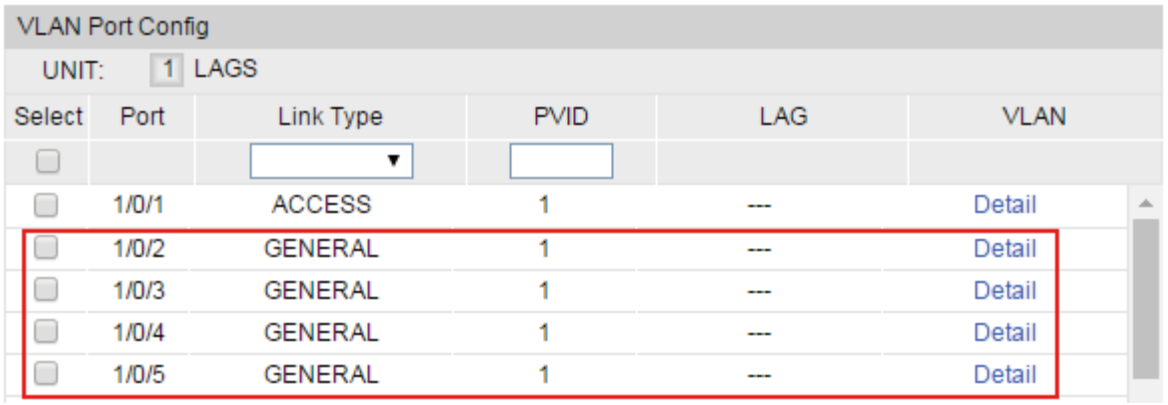


6) Click **Save Config** to save the settings.

Configurations for Switch 3

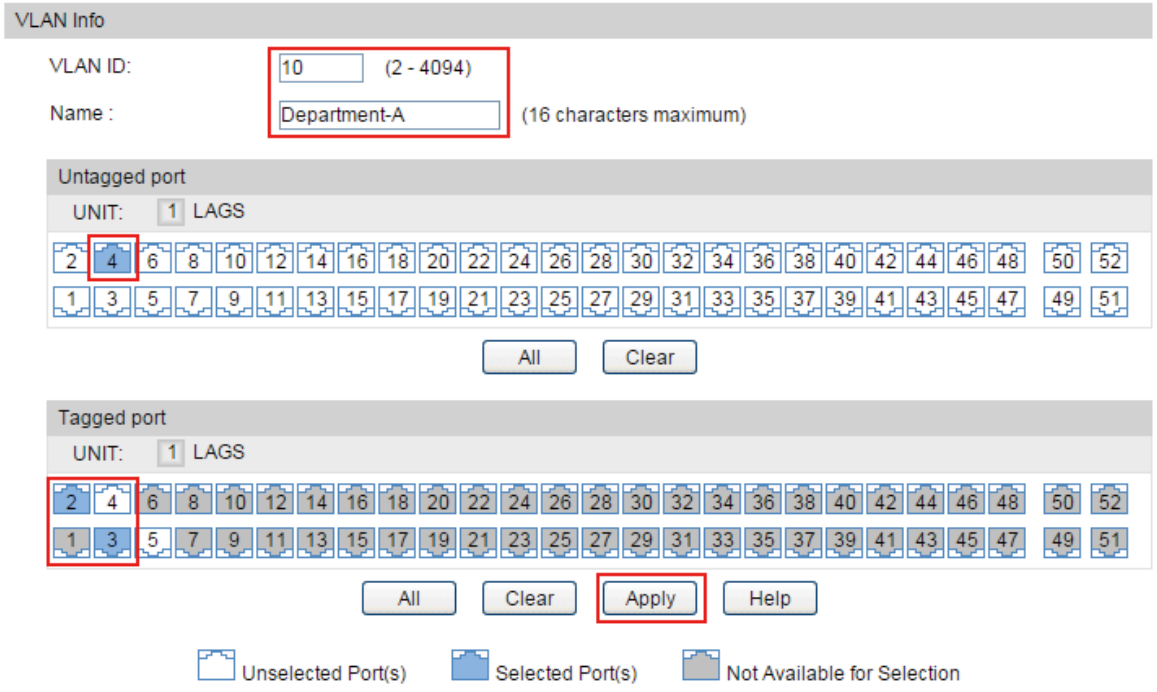
1) Choose the menu **VLAN > 802.1Q VLAN > Port Config** to load the following page. Set the link type of port1/0/2-5 as **General,** and click **Apply**.

Figure 3-7 Port Configuration



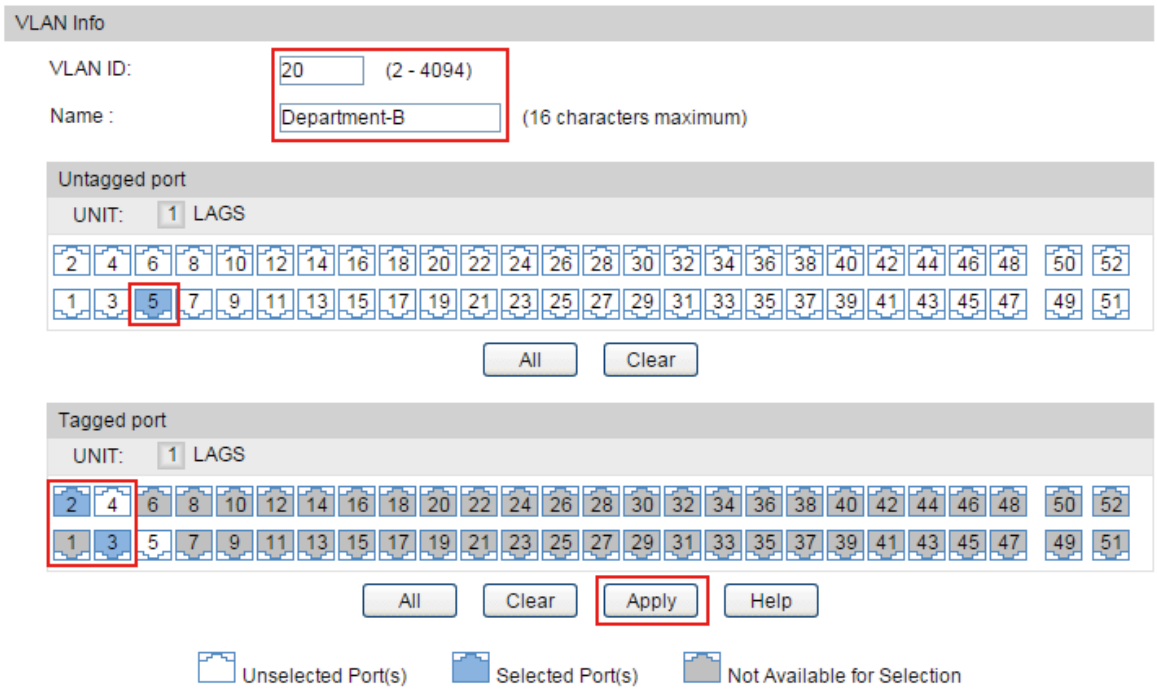
2) Choose the menu **VLAN > 802.1Q VLAN > VLAN Config** and click **Create** to load the following page. Create VLAN 10, and add port 1/0/4 as untagged port and ports 1/0/2-3 as tagged ports to VLAN 10. Click **Apply**.

Figure 3-8 VLAN 10 Configuration



3) Click **Create** to load the following page. Create VLAN 20, and add port 1/0/5 as untagged port and ports 1/0/2-3 as tagged ports to VLAN 20. Click **Apply**.

Figure 3-9 VLAN 20 Configuration



4) Click **Save Config** to save the settings.

3.4 Using the CLI

- Configurations for Switch 1 and Switch 2

The configurations of Switch 1 and Switch 2 are the same. The following introductions take Switch 1 as an example.

1) Create VLAN 10 for Department A and create VLAN 20 for Department B.

```
Switch_1#configure
Switch_1(config)#vlan 10
Switch_1(config-vlan)#name deptA
Switch_1(config-vlan)#exit
Switch_1(config)#vlan 20
Switch_1(config-vlan)#name deptB
Switch_1(config-vlan)#exit
```

2) For port 1/0/2, set the type as General, set the egress rule as Tagged, and add it to both VLAN 10 and VLAN 20.

```
Switch_1(config)#interface gigabitEthernet 1/0/2
Switch_1(config-if)#switchport mode general
Switch_1(config-if)#switchport general allowed vlan 10,20 tagged
Switch_1(config-if)#exit
```

3) Set port 1/0/1 set the type as General, set the egress rule as Untagged, and add it to both VLAN 10 and VLAN 20. Then enable MAC VLAN for port 1/0/1.

```
Switch_1(config)#interface gigabitEthernet 1/0/1
Switch_1(config-if)#switchport mode general
Switch_1(config-if)#switchport general allowed vlan 10,20 untagged
Switch_1(config-if)#mac-vlan
Switch_1(config-if)#exit
```

4) Bind the MAC address of Laptop A to VLAN 10 and bind the MAC address of Laptop B to VLAN 20.

```
Switch_1(config)#mac-vlan mac-address 00:19:56:8A:4C:71 vlan 10 description PCA
Switch_1(config)#mac-vlan mac-address 00:19:56:82:3B:70 vlan 20 description PCB
Switch_1(config)#end
```

Switch_1#copy running-config startup-config

- Configurations for Switch 3

1) Create VLAN 10 for Department A and create VLAN 20 for Department B.

Switch_3#configure

Switch_3(config)#vlan 10

Switch_3(config-vlan)#name deptA

Switch_3(config-vlan)#exit

Switch_3(config)#vlan 20

Switch_3(config-vlan)#name deptB

Switch_3(config-vlan)#exit

2) For port 1/0/2 and port 1/0/3, set the type as General, set the egress rule as Tagged, and add them to both VLAN 10 and VLAN 20.

Switch_3(config)#interface gigabitEthernet 1/0/2

Switch_3(config-if)#switchport mode general

Switch_3(config-if)#switchport general allowed vlan 10,20 tagged

Switch_3(config-if)#exit

Switch_3(config)#interface gigabitEthernet 1/0/3

Switch_3(config-if)#switchport general allowed vlan 10,20 tagged

Switch_3(config-if)#exit

3) For port 1/0/4 and port 1/0/5, set the type as General, set the egress rule as Untagged, and respectively add them to VLAN 10 and VLAN 20.

Switch_3(config)#interface gigabitEthernet 1/0/4

Switch_3(config-if)#switchport mode general

Switch_3(config-if)#switchport general allowed vlan 10 untagged

Switch_3(config-if)#exit

Switch_3(config)#interface gigabitEthernet 1/0/5

Switch_3(config-if)#switchport mode general

Switch_3(config-if)#switchport general allowed vlan 20 untagged

Switch_3(config-if)#end

Switch_3#copy running-config startup-config

Verify the Configurations

- Switch 1

```
Switch_1#show mac-vlan all
MAC Address          Description          VLAN
----------------------  -----------------  ----------
00:19:56:8A:4C:71     PCA                 10
00:19:56:82:3B:70     PCB                 20
-----------------------------------------------------------------
```

- Switch 2

```
Switch_2#show mac-vlan all
MAC Address          Description          VLAN
----------------------  ---------------------  -----------
00:19:56:8A:4C:71     PCA                  10
00:19:56:82:3B:70     PCB                  20
-----------------------------------------------------------------------
```

- Switch 3

```
Switch_3#show vlan
VLAN      Name            Status        Ports
--------  ---------------  -------------  -------------------------------------
1         Default VLAN    active        Gi1/0/1, Gi1/0/2, Gi1/0/3, Gi1/0/4,
                                        Gi1/0/5, Gi1/0/6, Gi1/0/7, Gi1/0/8
                                        ...
10        DeptA           active        Gi1/0/2, Gi1/0/3, Gi1/0/4
20        DeptB           active        Gi1/0/2, Gi1/0/3, Gi1/0/5
```

4 Appendix: Default Parameters

Default settings of MAC VLAN are listed in the following table.

Table 4-1 Default Settings of MAC VLAN

Parameter	Default Setting
MAC Address	None
Description	None
VLAN ID	None
Port Enable	Disable

Part 11

Configuring Protocol VLAN

CHAPTERS

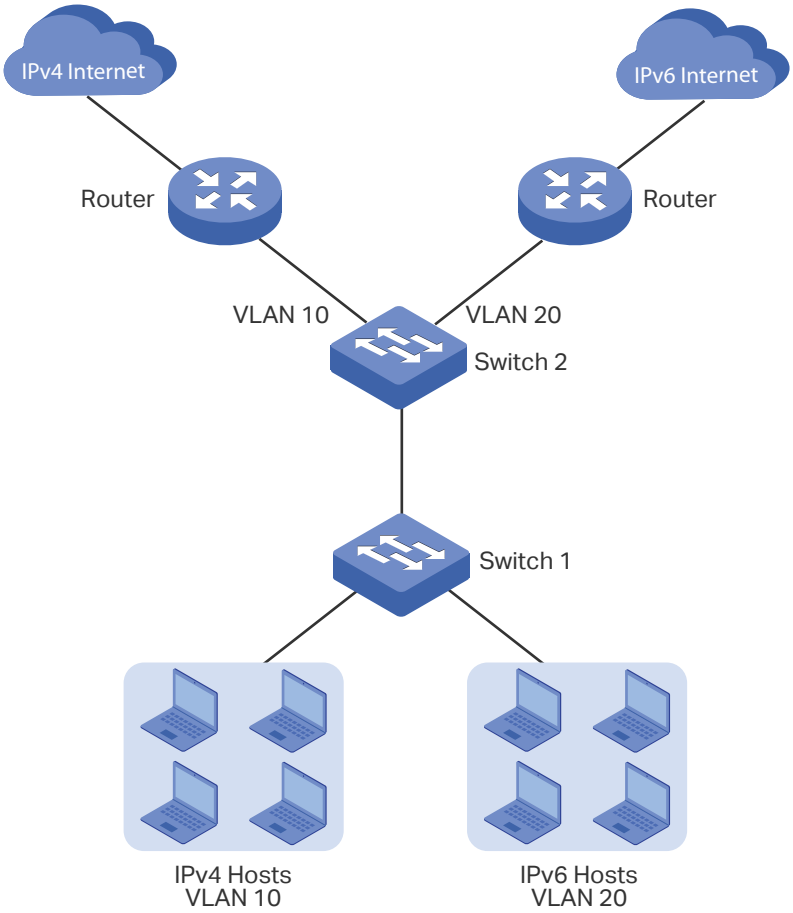
1. Overview
2. Protocol VLAN Configuration
3. Configuration Example
4. Appendix: Default Parameters

1 Overview

Protocol VLAN is a technology that divides VLANs based on the network layer protocol. With the protocol VLAN rule configured on the basis of the existing 802.1Q VLAN, the switch can analyze special fields of received packets, encapsulate the packets in specific formats, and forward the packets of different protocols to the corresponding VLANs. Since different applications and services use different protocols, network administrators can use protocol VLAN to manage the network based on specific applications and services of network users.

The figure below shows a common application scenario of protocol VLAN. With protocol VLAN configured, Switch 2 can forward IPv4 and IPv6 packets from different VLANs to the IPv4 and IPv6 networks respectively.

Figure 1-1 Common Application Scenario of Protocol VLAN



2 Protocol VLAN Configuration

To complete protocol VLAN configuration, follow these steps:

1) Configure 802.1Q VLAN, including creating a VLAN and setting the port type.
2) Create protocol template.
3) Configure Protocol VLAN.

Configuration Guidelines

- You can use the IP, ARP, RARP, and other protocol templates provided by TP-Link switches, or create new protocol templates.

- In a protocol VLAN, when a port receives an untagged data packet, the switch will first search for the protocol VLAN matching the protocol type value of the packet. (If MAC VLAN is also configured, the switch will first process MAC VLAN.) If there is a match, the switch will insert the corresponding VLAN tag to the data packet and forward it within the VLAN. Otherwise, the switch will forward the data packet to the default VLAN based on the PVID (Port VLAN ID) of the receiving port. When the port receives a tagged data packet, the switch will directly process the data packet according to the processing rule of the 802.1 Q VLAN.

2.1 Using the GUI

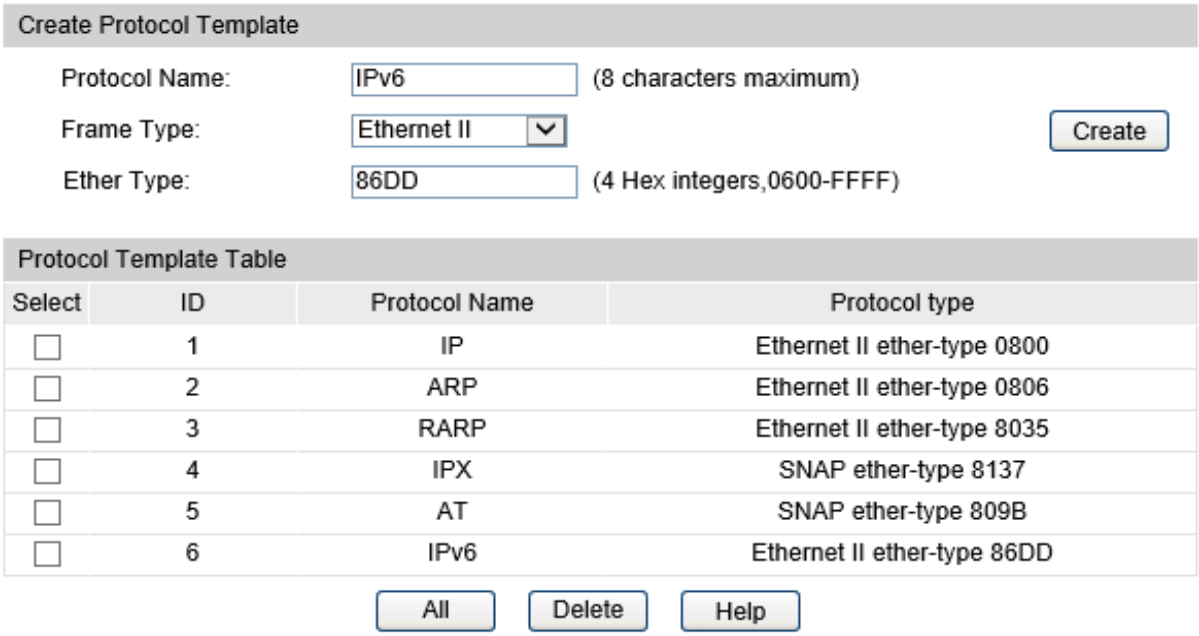
2.1.1 Configuring 802.1Q VLAN

Before configuring protocol VLAN, create an 802.1Q VLAN and set the port type according to network requirements. For details, refer to *Configuring 802.1Q VLAN*.

2.1.2 Creating Protocol Template

Choose the menu **VLAN > Protocol VLAN > Protocol Template** to load the following page.

Figure 2-1 Create a Protocol Template



Follow these steps to create a protocol template:

1) Check whether your desired template already exists in the **Protocol Template Table** section. If not, create it in the **Create Protocol Template** section.

Protocol Name	Enter the name of the new protocol template.
Frame Type	Select the frame type of the new protocol template.
Ether Type	Enter the Ethernet protocol type value for the protocol template. This value is the EtherType field in the Ethernet frame and is used to specify the data type of the frame.

2) Click **Create** to create the protocol template.

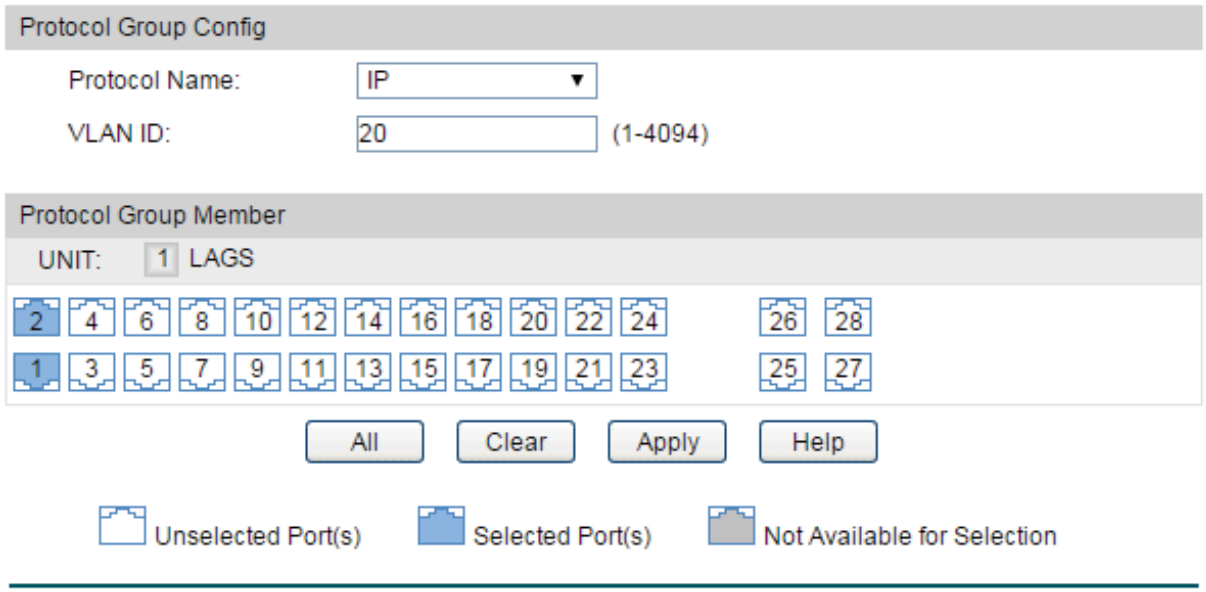
Note:

A protocol template that is bound to a VLAN cannot be deleted.

2.1.3 Configuring Protocol VLAN

Choose the menu **VLAN > Protocol VLAN > Protocol Group** to load the following page.

Figure 2-2 Configure the Protocol Group



Follow these steps to configure the protocol group:

1) In the **Protocol Group Config** section, select the protocol name and enter the VLAN ID to bind the protocol type to the VLAN.

Protocol Name	Select the protocol type.
VLAN ID	Enter the ID of the 802.1Q VLAN to be bound to the protocol type.

2) In the **Protocol Group Member** section, select the port or LAG to add to the protocol group.

3) Click **Apply**.

Note:

The member port of an LAG (Link Aggregation Group) follows the configuration of the LAG but not its own. The configurations of the port can take effect only after it leaves the LAG.

2.2 Using the CLI

2.2.1 Configuring 802.1Q VLAN

Before configuring protocol VLAN, create an 802.1Q VLAN and set the port type according to network requirements. For details, refer to *Configuring 802.1Q VLAN*.

2.2.2 Creating a Protocol Template

Follow these steps to create a protocol template:

Step 1	**configure** Enter global configuration mode.
Step 2	**protocol-vlan template name** *protocol-name* **frame { ether_2 ether-type** *type* **| snap ether-type** *type* **| llc dsap** *dsap_type* **ssap** *ssap_type* **}** Create a protocol template. *protocol-name:* Specify the protocol name with 1 to 8 characters. *type*: Specify the Ethernet protocol type with 4 hexadecimal numbers. *dsap_type*: Specify the destination service access point with 2 hexadecimal numbers. *ssap_type*: Specify the source service access point with 2 hexadecimal numbers.
Step 3	**show protocol-vlan template** Verify the protocol templates.
Step 4	**end** Return to Privileged EXEC Mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create an IPv6 protocol template:

Switch#configure

Switch(config)#protocol-vlan template name IPv6 **frame ether_2 ether-type** 86dd

Switch(config)#show protocol-vlan template

Index	Protocol Name	Protocol Type
1	IP	EthernetII ether-type 0800
2	ARP	EthernetII ether-type 0806
3	RARP	EthernetII ether-type 8035
4	IPX	SNAP ether-type 8137
5	AT	SNAP ether-type 809B
6	IPv6	EthernetII ether-type 86DD

Switch(config)#end

Switch#copy running-config startup-config

2.2.3 Configuring Protocol VLAN

Follow these steps to configure protocol VLAN:

Step 1	**configure** Enter global configuration mode.
Step 2	**show protocol-vlan template** Check the index of each protocol template.
Step 3	**protocol-vlan vlan** *vid* **template** *index* Bind the protocol template to the VLAN. *vid* : ID of the 802.1Q VLAN where the port with protocol VLAN enabled is. *index* : Protocol template index.
Step 4	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *lag-id* **| range port-channel** *lag-list* **}** Enter interface configuration mode. *port |port-list*: The number or the list of the Ethernet port that you want to configure. *lag-id |lag-list:* The ID or the list of the LAG that you want to configure.
Step 5	**show protocol-vlan vlan** Check the protocol VLAN index (entry-id) of each protocol group.
Step 6	**protocol-vlan group** *entry-id* Add the specified port to the protocol group. *entry-id:* Protocol VLAN index.
Step 7	**end** Return to Privileged EXEC Mode.
Step 8	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to bind the IPv6 protocol template to VLAN 10:

Switch#configure

Switch(config)#show protocol-vlan template

```
Index    Protocol Name    Protocol Type
--------  ------------------  --------------------------------
 1       IP                  EthernetII ether-type 0800
```

```
2          ARP              EthernetII ether-type 0806
3          RARP             EthernetII ether-type 8035
4          IPX              SNAP       ether-type 8137
5          AT               SNAP       ether-type 809B
6          IPv6             EthernetII ether-type 86DD
```

Switch(config)#protocol-vlan vlan 10 **template** 6

Switch(config)#end

Switch#copy running-config startup-config

The following example shows how to add port 1/0/2 to the IPv6 protocol group:

Switch#configure

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

Switch(config-if)#show protocol-vlan vlan

```
Index          Protocol-Name          VID     Member
--------       --------------------   ------  ------------
1              IPv6                   10
```

Switch(config-if)#protocol-vlan group 1

Switch(config-if)#show protocol-vlan vlan

```
Index    Protocol-Name    VID     Member
------   ---------------  ------  ------------
1        IPv6             10      Gi1/0/2
```

Switch(config-if)#end

Switch#copy running-config startup-config

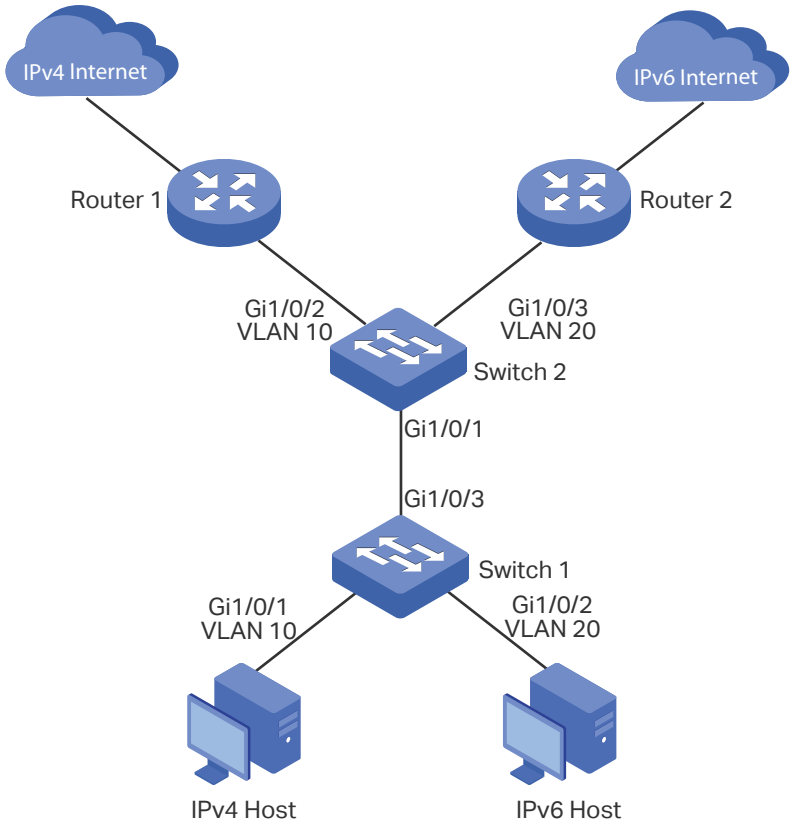
3 Configuration Example

3.1 Network Requirements

A company uses both IPv4 and IPv6 hosts, and these hosts access the IPv4 network and IPv6 network respectively via different routers. It is required that IPv4 packets are forwarded to the IPv4 network, IPv6 packets are forwarded to the IPv6 network, and other packets are dropped.

The figure below shows the network topology. The IPv4 host belongs to VLAN 10, the IPv6 host belongs to VLAN 20, and these hosts access the network via Switch 1. Switch 2 is connected to two routers to access the IPv4 network and IPv6 network respectively. The routers belong to VLAN 10 and VLAN 20 respectively.

Figure 3-1 Network Topology



3.2 Configuration Scheme

You can configure protocol VLAN on port 1/0/1 of Switch 2 to meet this requirement. When this port receives packets, Switch 2 will forward them to the corresponding VLANs according to their protocol types. The overview of the configuration on Switch 2 is as follows:

1) Create VLAN 10 and VLAN 20, set the port type, and add each port to the corresponding VLAN.
2) Use the IPv4 protocol template provided by the switch, and create the IPv6 protocol template.
3) Bind the protocol templates to the corresponding VLANs to form protocol groups, and add port 1/0/1 to the groups.

For Switch 1, configure 802.1Q VLAN according to the network topology.

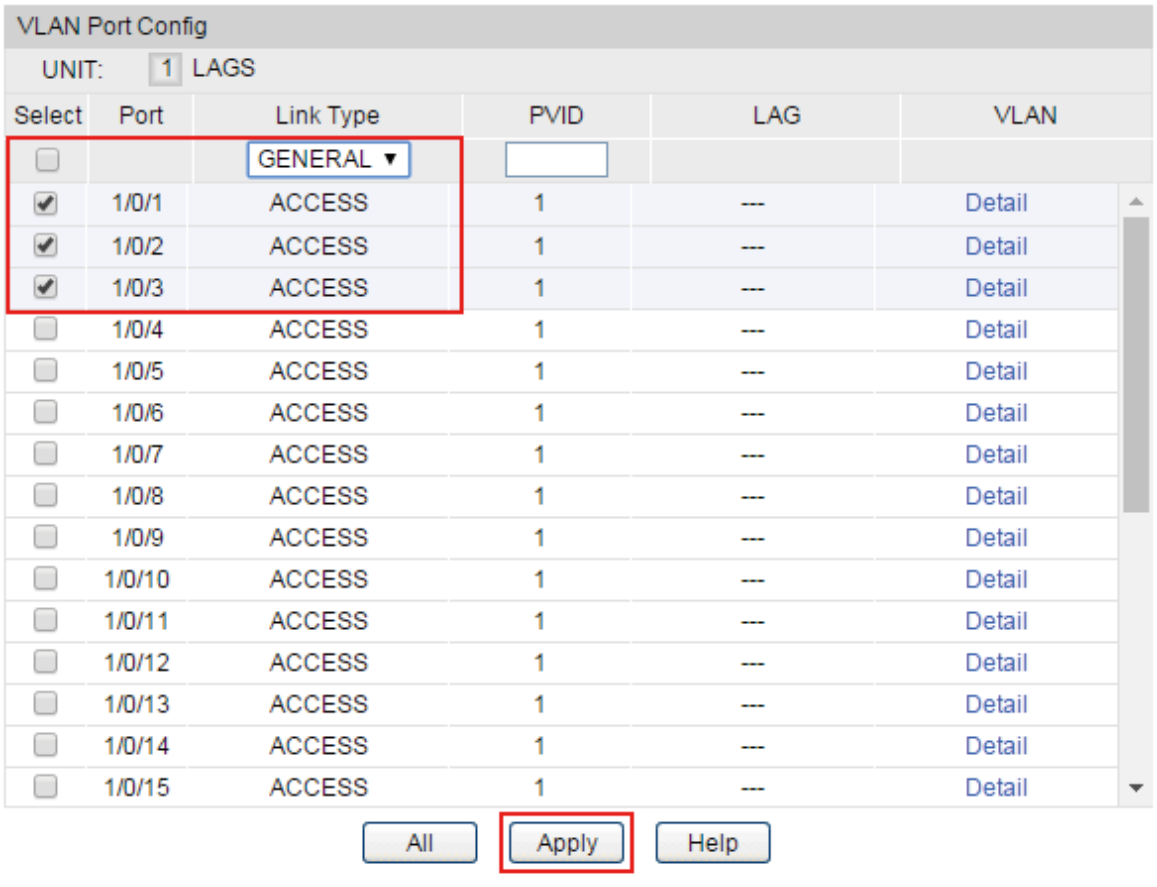
Demonstrated with T2600G-28TS, this chapter provides configuration procedures in two ways: using the GUI and using the CLI.

3.3 Using the GUI

- Configurations for Switch 1

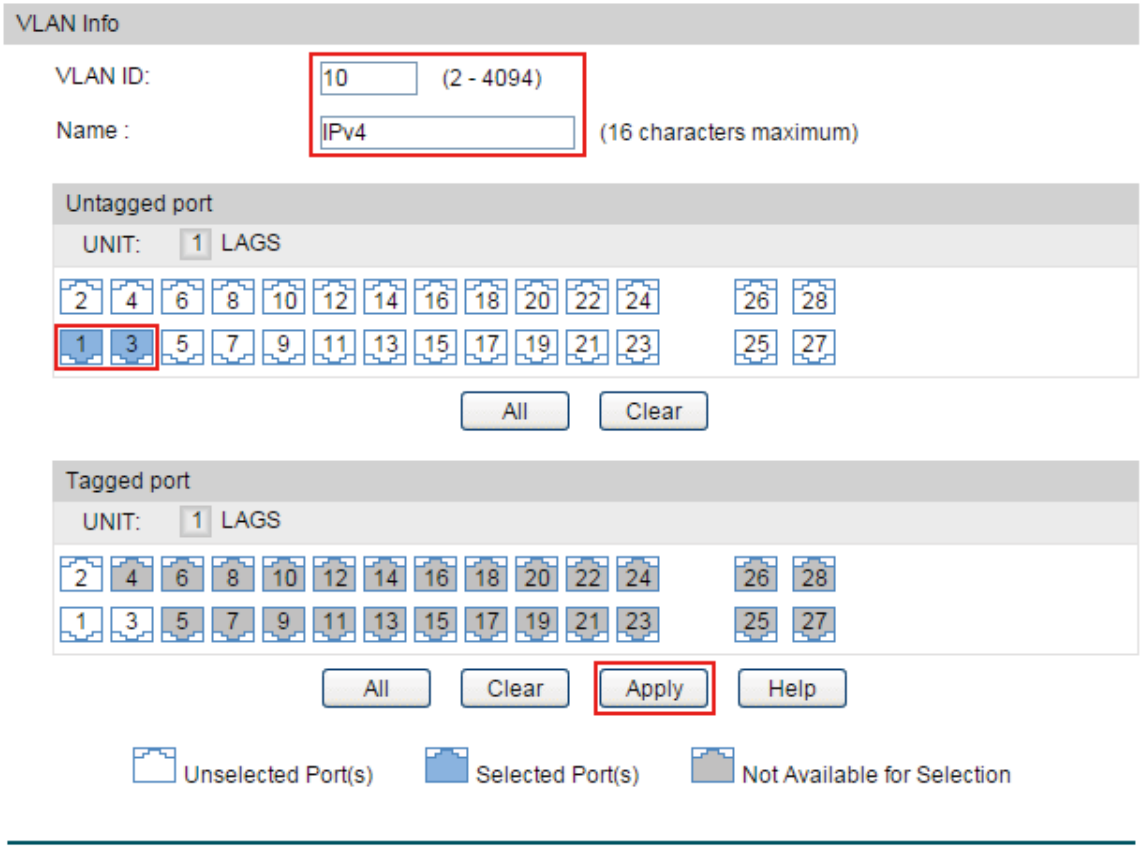
1) Choose the menu **VLAN > 802.1Q VLAN > Port Config** to load the following page. Set the link type of port1/0/1-3 as **General,** and click **Apply**.

Figure 3-2 Port Configuration



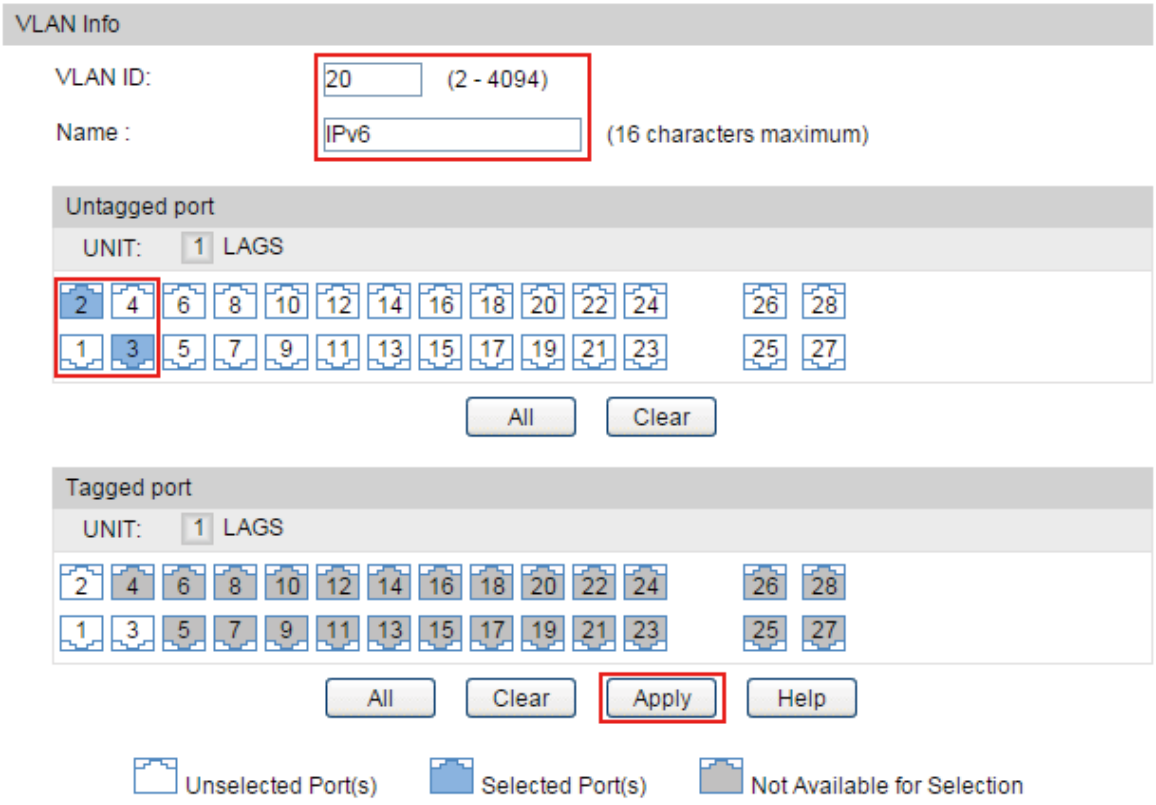
2) Choose the menu **VLAN > 802.1Q VLAN > VLAN Config** and click **Create** to load the following page. Create VLAN 10, and add port 1/0/1 and port 1/0/3 as untagged ports to VLAN 10. Click **Apply**.

Figure 3-3 Create VLAN 10



3) Click **Create** to load the following page. Create VLAN 20, and add ports 1/0/2-3 as untagged ports to VLAN 20. Click **Apply**.

Figure 3-4 Create VLAN 20

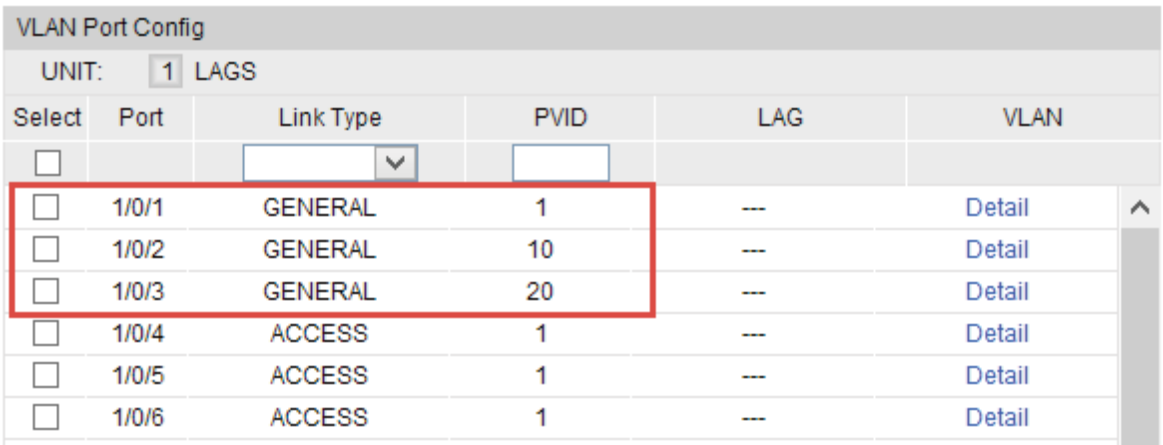


4) Click **Save Config** to save the settings.

Configurations for Switch 2

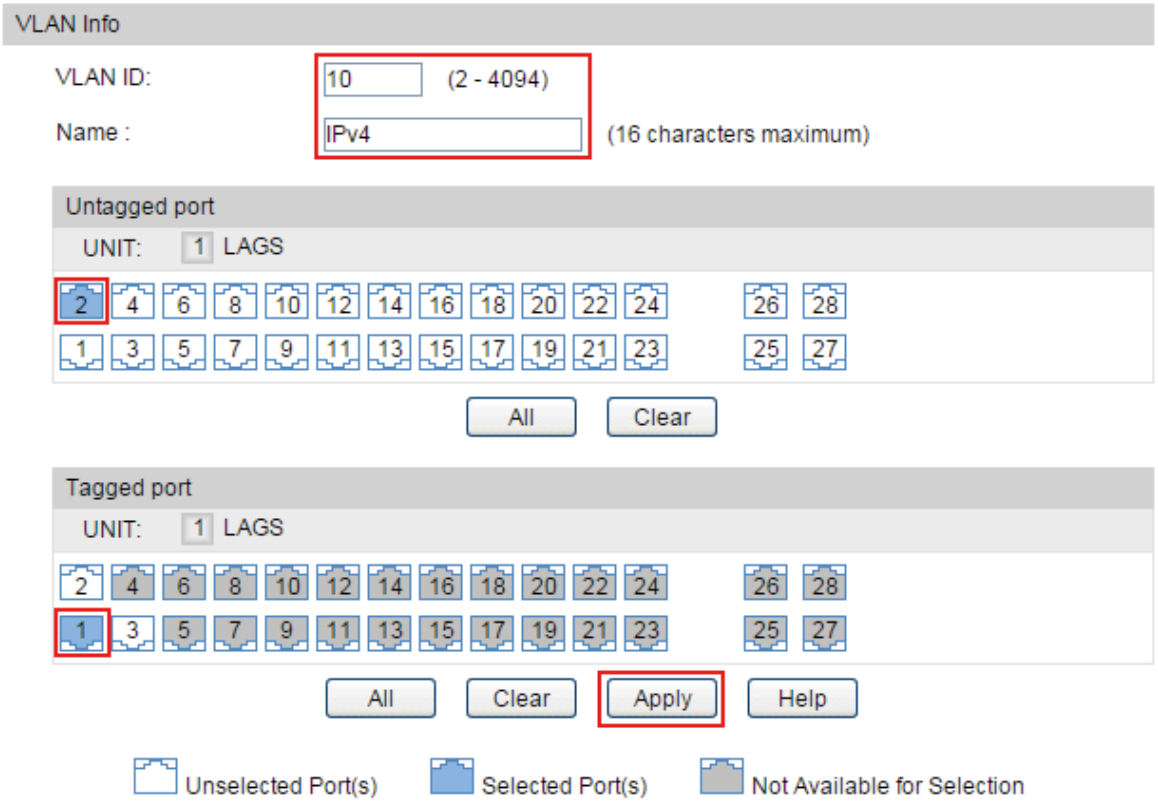
1) Choose the menu **VLAN > 802.1Q VLAN > Port Config** to load the following page. Set the link type of ports 1/0/1-3 as **General,** and respectively set the PVID of port 1/0/2 and port 1/0/3 as 10 and 20. Click **Apply**.

Figure 3-5 Port Configuration



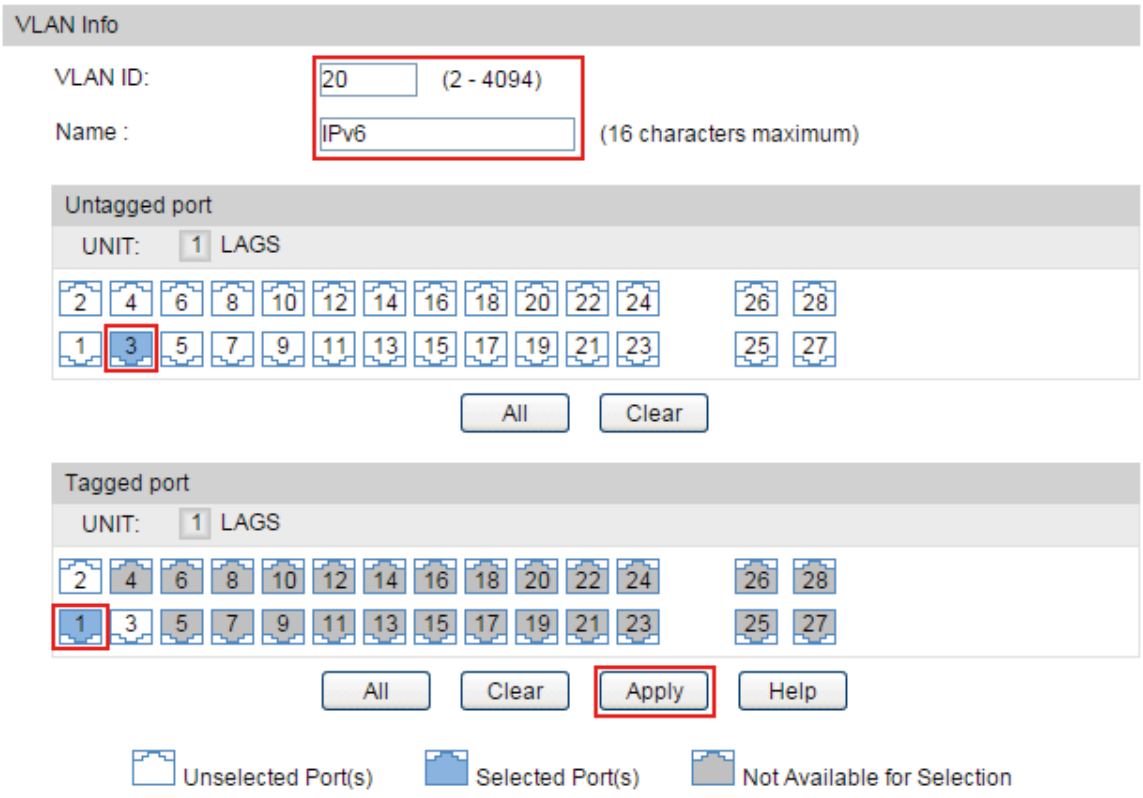
2) Choose the menu **VLAN > 802.1Q VLAN > VLAN Config** and click **Create** to load the following page. Create VLAN 10, and add port 1/0/1 as tagged port and port 1/0/2 as untagged port to VLAN 10. Click **Apply**.

Figure 3-6 Create VLAN 10



3) Click **Create** to load the following page. Create VLAN 20, and add port 1/0/1 as tagged port and port 1/0/3 as untagged port to VLAN 20. Click **Apply**.

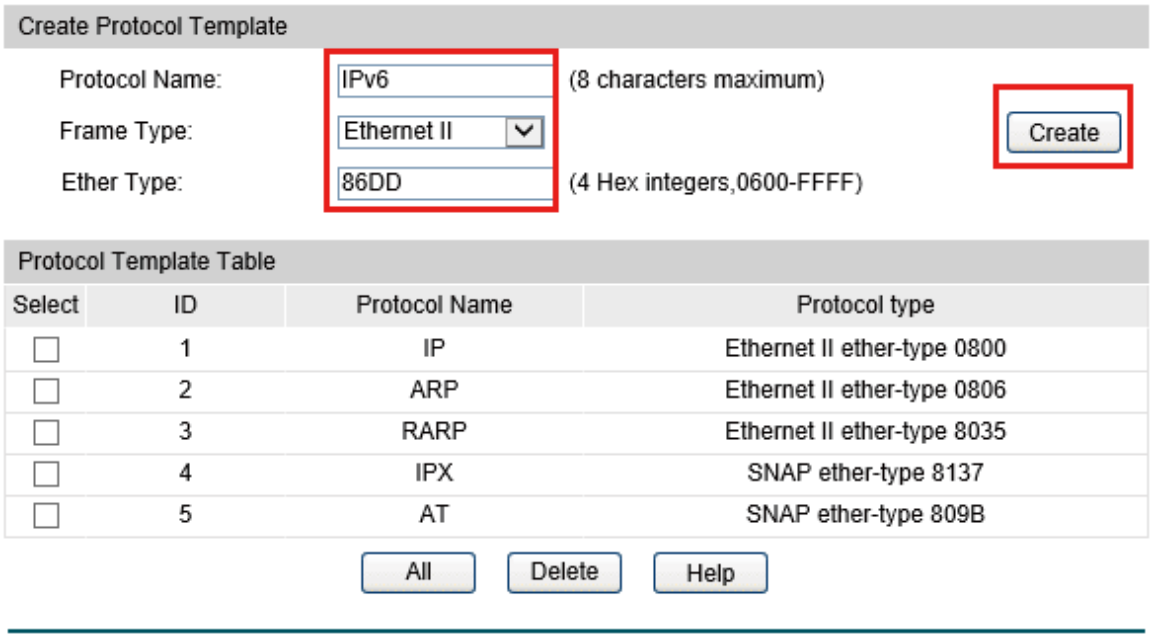
Figure 3-7 Create VLAN 20



4) Choose the menu **VLAN > Protocol VLAN > Protocol Template** to load the following page. Enter **IPv6** in the protocol name, select the **Ethernet II** frame type, enter **86DD** in the Ether Type field, and click **Create** to create the IPv6 protocol template.

Tips: The IPv4 protocol template is already provided by the switch. You only need to create the IPv6 protocol template.

Figure 3-8 Create the IPv6 Protocol Template



5) Choose the menu **VLAN > Protocol VLAN > Protocol Group** to load the following page. Select the IP protocol name (that is the IPv4 protocol template), enter VLAN ID 10, select port 1, and click **Apply**. Select the IPv6 protocol name, enter VLAN ID 20, select port 1, and click **Apply**.

Figure 3-9 Configure the IPv4 Protocol Group

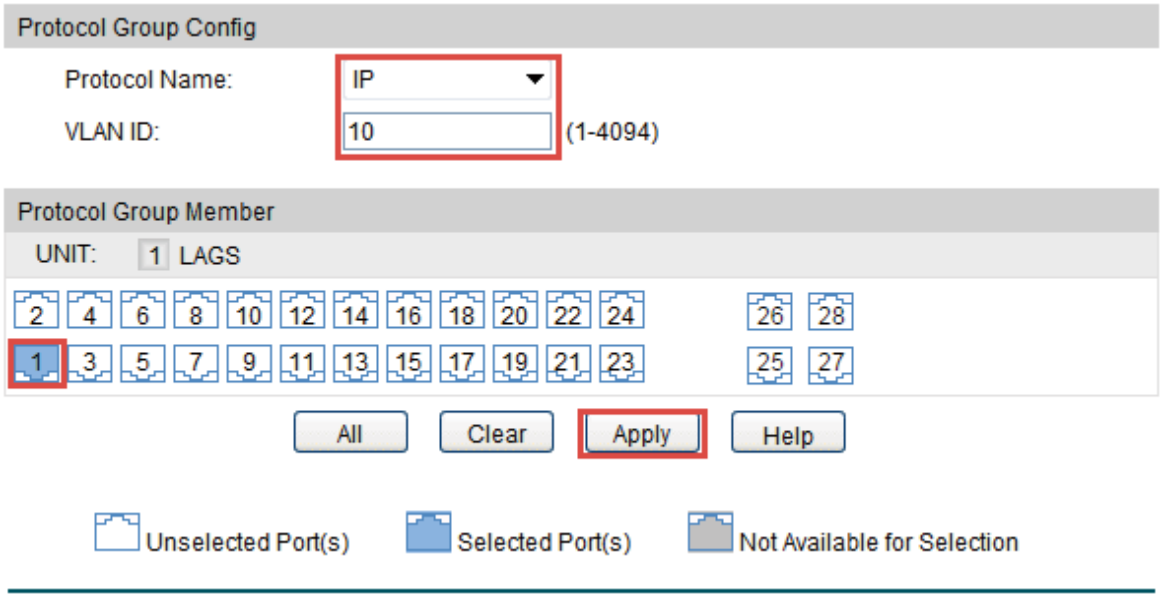
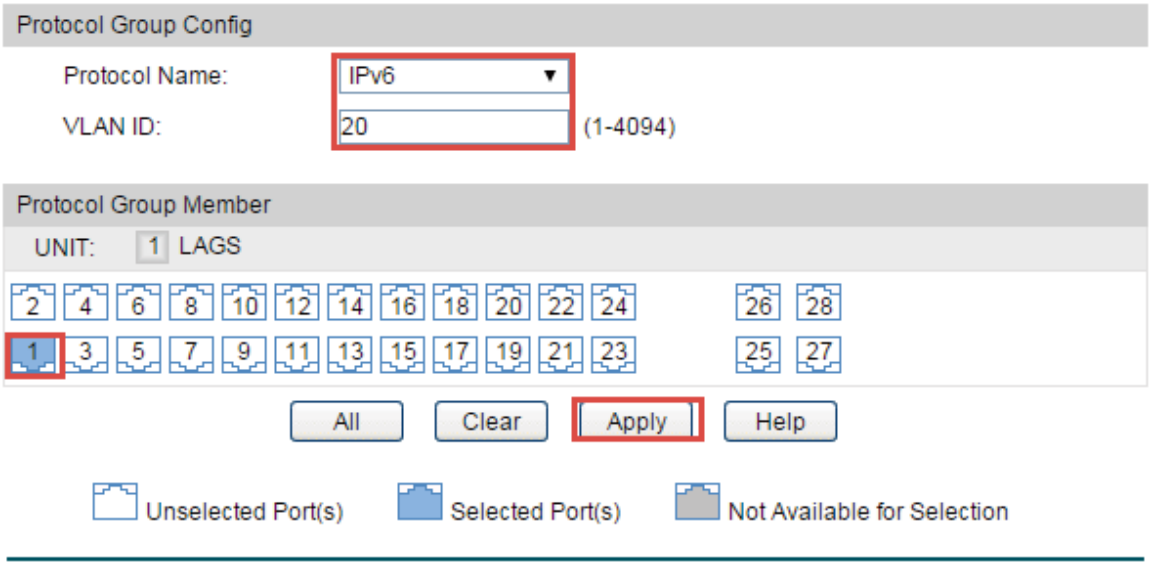
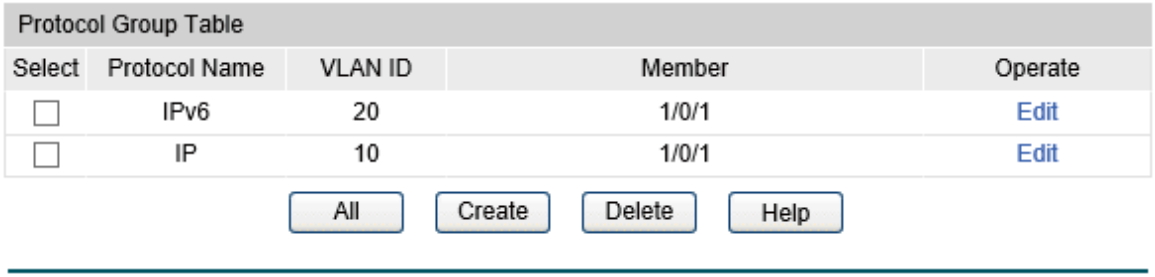


Figure 3-10 Configure the IPv6 Protocol Group



6) Choose the menu **VLAN > Protocol VLAN > Protocol Group Table** to load the following page. Here you can view the protocol VLAN configuration.

Figure 3-11 Protocol VLAN configuration



7) Click **Save Config** to save the settings.

3.4 Using the CLI

- Configurations for Switch 1

1) Create VLAN 10 and VLAN 20.

```
Switch_1#configure
Switch_1(config)#vlan 10
Switch_1(config-vlan)#name IPv4
Switch_1(config-vlan)#exit
Switch_1(config)#vlan 20
Switch_1(config-vlan)#name IPv6
Switch_1(config-vlan)#exit
```

2) For port 1/0/1 and port 1/0/2, set the type as General, set the egress rule as Untagged, and respectively add them to VLAN 10 and VLAN 20.

Switch_1(config)#interface gigabitEthernet 1/0/1

Switch_1(config-if)#switchport mode general

Switch_1(config-if)#switchport general allowed vlan 10 untagged

Switch_1(config-if)#exit

Switch_1(config)#interface gigabitEthernet 1/0/2

Switch_1(config-if)#switchport mode general

Switch_1(config-if)#switchport general allowed vlan 20 untagged

Switch_1(config-if)#exit

3) For port 1/0/3, set the type as General, set the egress rule as Untagged, and add it to both VLAN 10 and VLAN 20.

Switch_1(config)#interface gigabitEthernet 1/0/3

Switch_1(config-if)#switchport mode general

Switch_1(config-if)#switchport general allowed vlan 10,20 untagged

Switch_1(config-if)#end

Switch_1#copy running-config startup-config

- Configurations for Switch 2

1) Create VLAN 10 and VLAN 20.

Switch_2#configure

Switch_2(config)#vlan 10

Switch_2(config-vlan)#name IPv4

Switch_2(config-vlan)#exit

Switch_2(config)#vlan 20

Switch_2(config-vlan)#name IPv6

Switch_2(config-vlan)#exit

2) For port 1/0/1, set the type as General, set the egress rule as Tagged, and add it to both VLAN 10 and VLAN 20.

Switch_2(config)#interface gigabitEthernet 1/0/1

Switch_2(config-if)#switchport mode general

Switch_2(config-if)#switchport general allowed vlan 10,20 tagged

Switch_2(config-if)#exit

3) For port 1/0/2 and port 1/0/3, set the type as General, set the egress rule as Untagged, and add them to VLAN 10 and VLAN 20 respectively.

Switch_2(config)#interface gigabitEthernet 1/0/2

Switch_2(config-if)#switchport mode general

Switch_2(config-if)#switchport pvid 10

Switch_2(config-if)#switchport general allowed vlan 10 untagged

Switch_2(config-if)#exit

Switch_2(config)#interface gigabitEthernet 1/0/3

Switch_2(config-if)#switchport mode general

Switch_2(config-if)#switchport pvid 20

Switch_2(config-if)#switchport general allowed vlan 20 untagged

Switch_2(config-if)#exit

4) Create the IPv6 protocol template.

Switch_2(config)#protocol-vlan template name IPv6 frame ether_2 ether-type 86dd

Switch_2(config)#show protocol-vlan template

Index	Protocol Name	Protocol Type
1	IP	EthernetII ether-type 0800
2	ARP	EthernetII ether-type 0806
3	RARP	EthernetII ether-type 8035
4	IPX	SNAP ether-type 8137
5	AT	SNAP ether-type 809b
6	IPv6	Ethernet II ether-type 86dd

5) Configure the protocol groups.

Switch_2(config)#protocol-vlan vlan 10 template 1

Switch_2(config)#protocol-vlan vlan 20 template 6

6) Add port 1/0/1 to the protocol groups.

Switch_2(config)#show protocol-vlan vlan

```
Index      Protocol-Name     VID          Member
----       --------------    ----------   -------------
 1         IP                10
 2         IPv6              20
Switch_2(config)#interface gigabitEthernet 1/0/1
Switch_2(config-if)#protocol-vlan group 1
Switch_2(config-if)#protocol-vlan group 2
Switch_2(config-if)#exit
Switch_2(config)#end
Switch_2#copy running-config startup-config
```

Verify the Configurations

- Switch 1

  Verify 802.1Q VLAN configuration:

  ```
  Switch_1#show vlan
  VLAN        Name             Status       Ports
  --------    -------------    ---------    ----------------------------------------------
  1           System-VLAN      active       Gi1/0/1, Gi1/0/2, Gi1/0/3, Gi1/0/4
                                            ...
                                            Gi1/0/25, Gi1/0/26, Gi1/0/27, Gi1/0/28
  10          IPv4             active       Gi1/0/1, Gi1/0/3
  20          IPv6             active       Gi1/0/2, Gi1/0/3
  ```

- Switch 2

  Verify 802.1Q VLAN configuration:

  ```
  Switch_2#show vlan
  VLAN        Name             Status       Ports
  -------     -------------    ----------   -----------------------------------------
  1           System-VLAN      active       Gi1/0/1, Gi1/0/2, Gi1/0/3, Gi1/0/4
                                            ...
                                            Gi1/0/25, Gi1/0/26, Gi1/0/27, Gi1/0/28
  ```

10	IPv4	active	Gi1/0/1, Gi1/0/2
20	IPv6	active	Gi1/0/1, Gi1/0/3

Verify protocol group configuration:

Switch_2#show protocol-vlan vlan

Index	Protocol-Name	VID	Member
1	IP	10	Gi1/0/1
2	IPv6	20	Gi1/0/1

4 Appendix: Default Parameters

Default settings of Protocol VLAN are listed in the following table.

Table 4-1 Default Settings of Protocol VLAN

Parameter	Default Setting		
Protocol Template Table	1	IP	Ethernet II ether-type 0800
	2	ARP	Ethernet II ether-type 0806
	3	RARP	Ethernet II ether-type 8035
	4	IPX	SNAP ether-type 8137
	5	AT	SNAP ether-type 809B

Part 12

Configuring VLAN-VPN

CHAPTERS

1. VLAN-VPN
2. Basic VLAN-VPN Configuration
3. Flexible VLAN-VPN Configuration
4. Configuration Example
5. Appendix: Default Parameters

1 VLAN-VPN

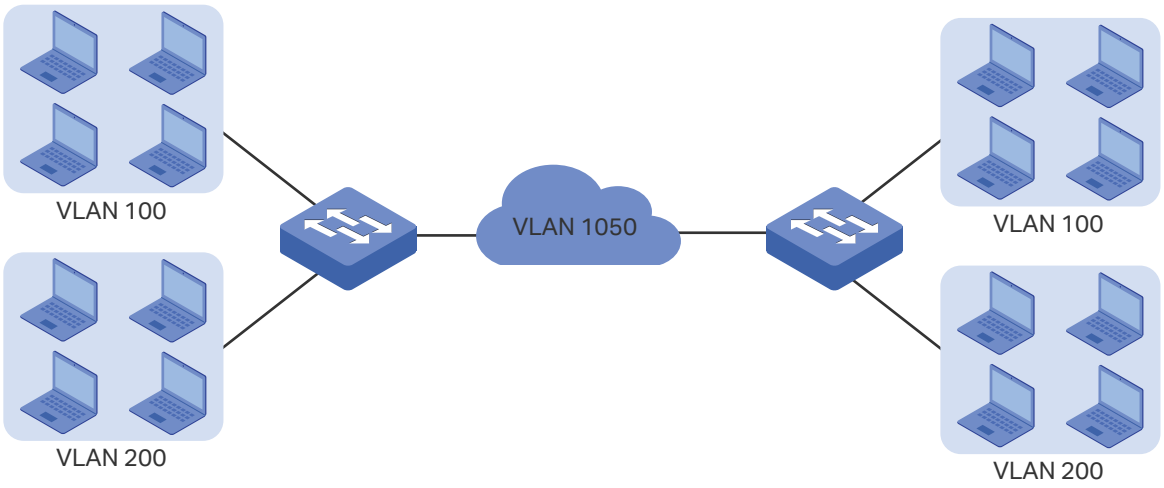
1.1 Overview

VLAN-VPN (Virtual Private Network) is an easy-to-implement layer 2 VLAN technology, and it is usually deployed at the edge of the ISP (Internet Service Provider) network.

With VLAN-VPN, when forwarding packets from the customer network to the ISP network, the switch tags the packets with outer VLAN tags. Thus, packets can be transmitted through ISP networks with double VLAN tags. In the ISP network, packets are forwarded according to the outer VLAN tag (VLAN tag of the ISP network), while the inner VLAN tag is treated as part of the payload. When forwarding packets from the ISP network to the customer network, the switch remove the outer VLAN tag of the packets. Thus, packets are forwarded according to the inner VLAN tag (VLAN tag of the customer network) in the customer network.

The following figure shows the typical application scenario of VLAN-VPN. To realize the communication between two customer VLANs across the ISP network, you can configure VLAN-VPN at the ISP edge switches to allow packets from customer VLAN 100 and VLAN 200 to be forwarded through the ISP network with the outer tag of VLAN 1050.

Figure 1-1 Application Scenario of VLAN-VPN



1.2 Supported Features

The VLAN-VPN function includes: basic VLAN-VPN and flexible VLAN-VPN (VLAN mapping).

Basic VLAN-VPN

All packets from customer VLANs are encapsulated with the same VLAN tag of the ISP network, and sent to the ISP network. Additionally, you can set the TPID (Tag Protocol Identifier) of to-be-sent packets for compatibility with devices in the ISP network.

Flexible VLAN-VPN

You can configure different VLANs in the customer network to map to different VLANs in the ISP network.

When the switch receives a packet with the customer network tag, the switch will check the VLAN Mapping List. If a match is found, the switch encapsulates the packet with the corresponding VLAN tag of the ISP network, and forwards it to the corresponding port. If no match is found, the switch process the packet in rules of MAC VLAN, Protocol VLAN and 802.1Q VLAN. For untagged packets, the switch directly processes them in rules of MAC VLAN, Protocol VLAN and 802.1Q VLAN.

2 Basic VLAN-VPN Configuration

To complete the basic VLAN-VPN configuration, follow these steps:

1) Configure 802.1Q VLAN.
2) Configure VPN up-link ports and VPN ports.
3) Enable VLAN-VPN globally.

Configuration Guidelines

The TPID preset by the switch is 0x8100. If devices in the ISP network do not support the value, you should change it to ensure VLAN-VPN packets sent to the ISP network can be recognized and forwarded by devices of other manufacturers.

2.1 Using the GUI

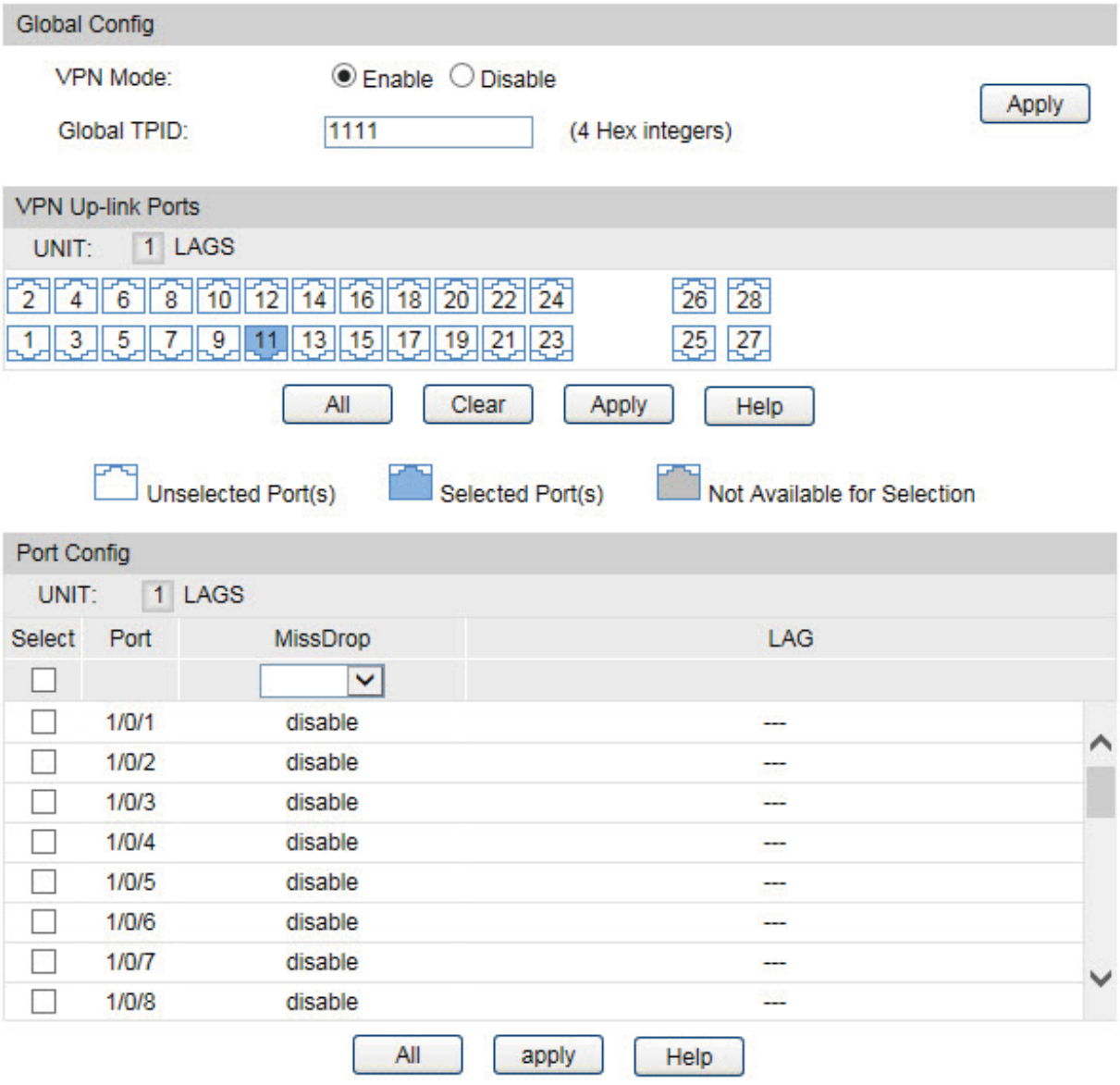
2.1.1 Configuring 802.1Q VLAN

Before configuring VLAN-VPN, set the link type of ports according to network requirements, and create an 802.1Q VLAN as ISP network VLAN and an 802.1Q VLAN as customer network VLAN. Add ports connecting the customer network to the customer network VLAN; add ports connecting the customer network and ports connecting the ISP network to the ISP network VLAN. For details, refer to *Configuring 802.1Q VLAN*.

2.1.2 Configuring Global VLAN-VPN and Up-link Ports

Choose the menu **VLAN > VLAN-VPN > VPN Config** to load the following page.

Figure 2-1 Global VPN Configuration



Follow these steps to configure the global VLAN-VPN parameters and up-link ports:

1) In the **Global Config** section, enable VPN mode in the Global Config section, modify the TPID value for compatibility with devices in the ISP network, and click **Apply**.

VPN Mode	VLAN-VPN works only when the VPN mode is enabled.
Global TPID	Set the global TPID which is used to identify the protocol of the tag. The default value is 0x8100 in hexadecimal format. You can modify it if needed. Before a VPN up-link port forwards a packet, the port will replace its TPID value in the outer VLAN tag with the user-defined value.

2) In the **VPN Up-link Ports** section, set ports that are connected to the ISP network as VPN up-link ports. Click **Apply**.

VPN Up-link Port	VPN up-link ports are usually connected to the ISP network , and packets sent out from these ports will be tagged with the outer VLAN tag of the ISP network.

3) In the **Port Config** section, enable the VLAN-VPN missdrop function for the port. Click **Apply**.

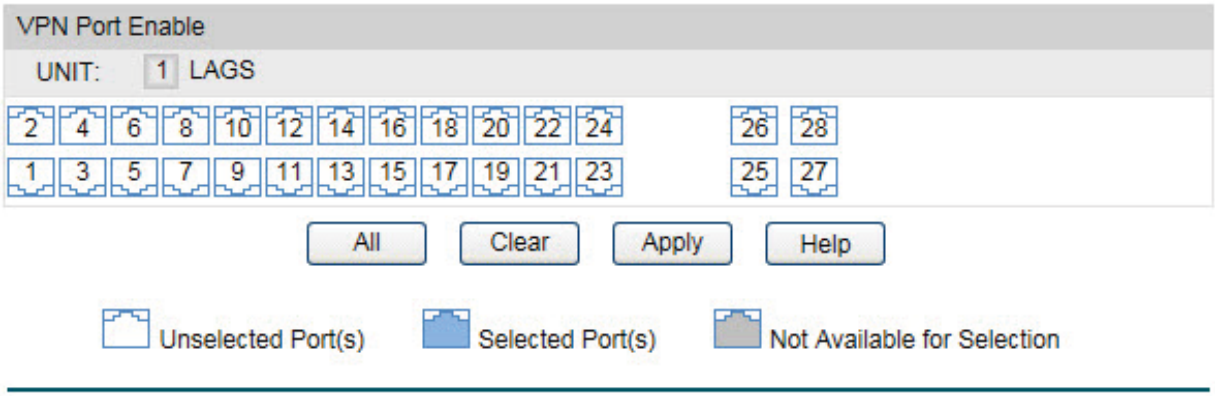
Note:

The member pot of an LAG (Link Aggregation Group) follows the configuration of the LAG but not its own. The configurations of the port can take effect only after it leaves the LAG.

2.1.3 Configuring VPN Ports

Choose the menu **VLAN > VLAN-VPN > Port Enable** to load the following page.

Figure 2-2 Enabling VPN Ports



Follow these steps to configure VPN ports:

1) Select ports that are connected to the customer network.

2) Click **Apply** to enable the VLAN-VPN feature on the selected ports.

Note:

The member pot of an LAG (Link Aggregation Group) follows the configuration of the LAG but not its own. The configurations of the port can take effect only after it leaves the LAG.

2.2 Using the CLI

2.2.1 Configuring 802.1Q VLAN

Before configuring VLAN-VPN, set the link type of ports according to network requirements, and create an 802.1Q VLAN as ISP network VLAN and an 802.1Q VLAN as customer network VLAN. Add ports connecting the customer network to the customer network VLAN; add ports connecting the customer network and ports connecting the ISP network to the ISP network VLAN. For details, refer to *Configuring 802.1Q VLAN*.

2.2.1 Configuring Basic VLAN-VPN

Follow these steps to configure basic VLAN-VPN:

Step 1	**configure** Enter global configuration mode.
Step 2	**dot1q-tunnel** Enable the VLAN-VPN feature globally.
Step 3	**dot1q-tunnel tpid** *num* Set the TPID value globally. *num*: Set the global TPID which is used to identify the protocol of the tag. The default value is 0x8100 in hexadecimal format. You can modify it if needed. Before a VPN up-link port forwards a packet, the port will replace its TPID value in the outer VLAN tag with the user-defined value.
Step 4	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *lagid* **| range port-channel** *lag-list* **}** Enter interface configuration mode. **switchport dot1q-tunnel missdrop** Optional. Enable the VLAN-VPN missdrop function for a specific port.
Step 5	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *lagid* **| range port-channel** *lag-list* **}** Enter interface configuration mode for VPN up-link ports and VPN ports respectively. **switchport dot1q-tunnel mode** { nni | uni } Set ports that are connected to the ISP network as VPN up-link ports, and ports that connected to the customer network as VPN ports. *nni* : Set ports that are connected to the ISP network as VPN up-link ports. *uni* : Set ports that are connected to the customer network as VPN ports. *Note:* The direct shift between ports modes uni and nni is not supported. To switch from the current mode to another mode, you can use **no switchport dot1q-tunnel mode** to disable the current mode.
Step 6	**show dot1q-tunnel** Verify the global configuration of VLAN-VPN.
Step 7	**show dot1q-tunnel interface** Verify the interface configuration of VLAN-VPN.
Step 8	**end** Return to privileged EXEC mode.

Step 9	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable the VLAN-VPN feature globally and set the TPID as 0x9100:

Switch#configure

Switch(config)#dot1q-tunnel

Switch(config)#dot1q-tunnel tpid 9100

Switch(config)#show dot1q-tunnel

VLAN-VPN Mode: Enabled

Global TPID: 0X9100

Mapping Mode: Disabled

Switch(config)#end

Switch#copy running-config startup-config

The following example shows how to set port 1/0/1 of switch as the VPN port and 1/0/2 as the VPN up-link port:

Switch#configure

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

Switch(config-if)#switchport dot1q-tunnel mode uni

Switch(config-if)#exit

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

Switch(config-if)#switchport dot1q-tunnel mode nni

Switch(config-if)#show dot1q-tunnel interface

Port Type Member

--- ---

NNI Gi1/0/2

UNI Gi1/0/1

Switch(config-if)#end

Switch#copy running-config startup-config

3 Flexible VLAN-VPN Configuration

To complete the flexible VLAN-VPN configuration, follow these steps:

1) Configure 802.1Q VLAN and basic VLAN-VPN.
2) Configure VLAN mapping.

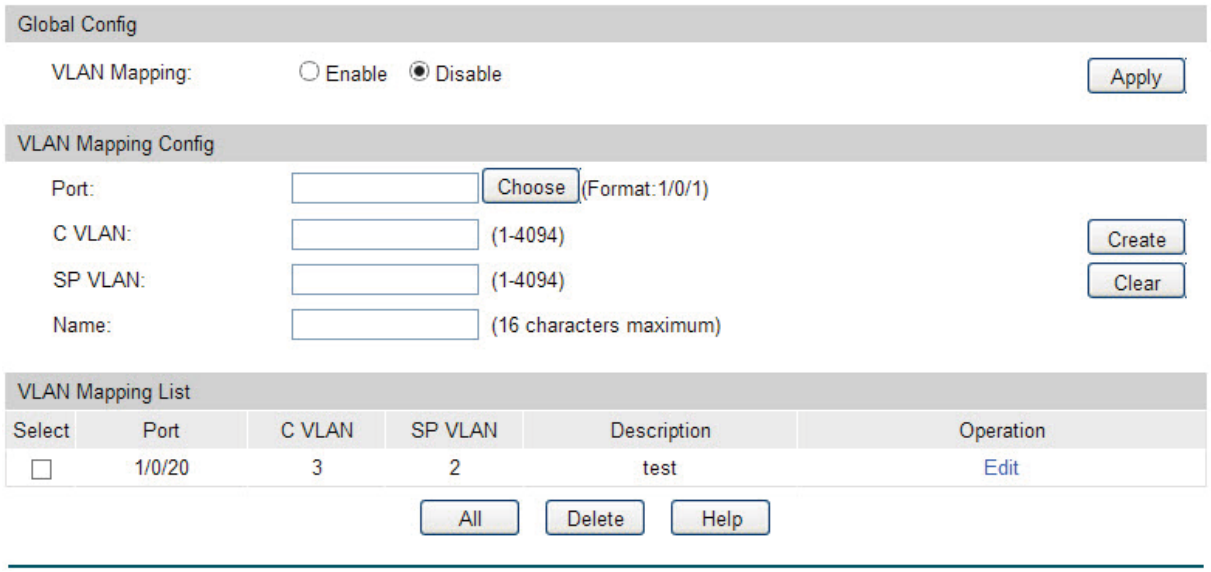
Configuration Guidelines

- Before you start, configure 802.1Q VLAN and the basic VLAN-VPN. VLAN mapping entries work only after you have set VPN up-link ports and VPN ports in the basic VLAN-VPN configuration and enabled the VPN feature globally.
- With the flexible VLAN-VPN feature, the switch processes tagged packets and untagged packets differently. When a VPN port receives a packet with the customer network tag, the switch will check the VLAN Mapping List. If a match is found, the switch encapsulates the packet with the corresponding VLAN tag of the ISP network, and forwards it to the corresponding port. If no match is found, the switch process the packet in rules of MAC VLAN, Protocol VLAN and 802.1Q VLAN. For untagged packets, the switch directly processes them in rules of MAC VLAN, Protocol VLAN and 802.1Q VLAN.

3.1 Using the GUI

Choose the menu **VLAN > VLAN-VPN > VLAN Mapping** to load the following page.

Figure 3-1 Configuring Flexible VLAN-VPN



Follow these steps to configure flexible VLAN-VPN:

1) In the **Global Config** section, enable VLAN mapping globally and click **Apply**.

2) In the **VLAN Mapping Config** section, choose a VPN port to enable VLAN mapping. Enter customer network VLAN ID in the **C VLAN** field, enter ISP network VLAN ID in the **SP VLAN** field, and enter a name to identify the entry. Then click **Create** to add a mapping entry.

Port	Choose a VPN port to enable VLAN mapping. Usually, ports that are connected to the customer network are set as VPN ports. You can also enter the port number in 1/0/1 format.
C_VLAN	Enter the VLAN ID of the customer network. When the specified port receives a packet from the VLAN, the switch will encapsulate the packet with the VLAN tag of the ISP VLAN based on the mapping entry.
SP_VLAN	Enter the VLAN ID of the ISP network.
Name	Enter a name of the mapping entry for identification.

3.2 Using the CLI

Follow these steps to configure flexible VLAN-VPN:

Step 1	**configure** Enter global configuration mode.
Step 2	**dot1q-tunnel mapping** Enable VLAN mapping.
Step 3	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *lag-id* **| range port-channel** *lag-list* **}** Enter interface configuration mode. *port |port-list*: The number or the list of the Ethernet port that you want to configure. *lag-id |lag-list:* The ID or the list of the LAG that you want to configure.
Step 4	**switchport dot1q-tunnel mapping** *c-vlan sp-vlan [descript]* Set VLAN mapping entries for the specified port. *c vlan:* Enter VLAN ID of the customer network. *sp vlan:* Enter VLAN ID of the ISP network. *descript:* Give a description of the mapping entry for identification.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable VLAN mapping and set a VLAN mapping entry named mapping1 on port 1/0/3 to map customer network VLAN 15 to ISP network VLAN 1040:

Switch#configure

Switch(config)#dot1q-tunnel mapping

Switch(config)#show dot1q-tunnel

VLAN-VPN Mode: Enabled

Global TPID: 0X8100

Mapping Mode: Enabled

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

Switch(config-if)#switchport dot1q-tunnel mapping 15 1040 mapping1

Switch(config-if)#show dot1q-tunnel mapping

Port	C-VLAN	SP-VLAN	Name
Gi1/0/3	15	1040	mapping1

Switch(config-if)#end

Switch#copy running-config startup-config

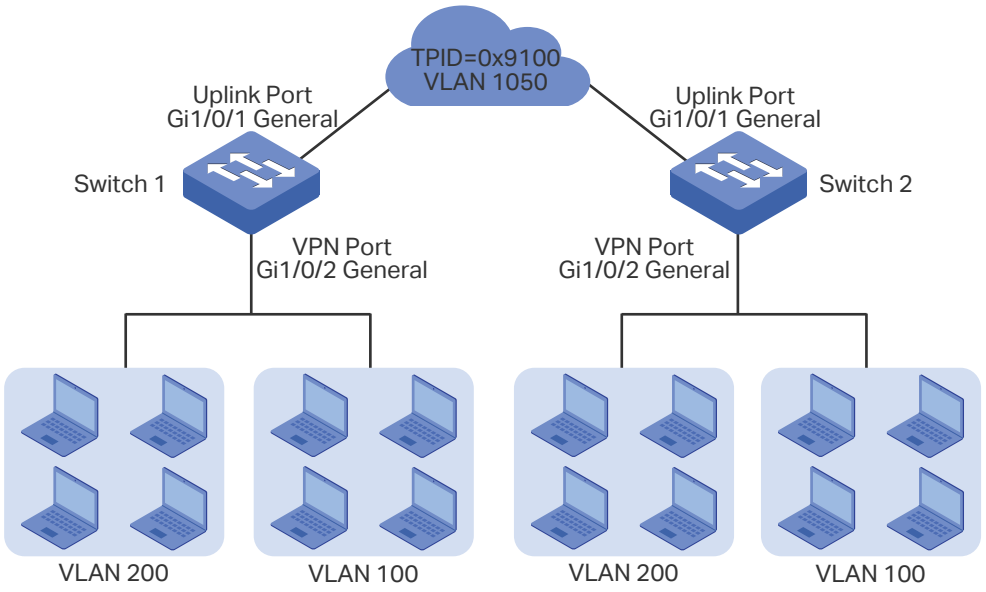
4 Configuration Example

4.1 Network Requirements

Two divisions of the company are located in different areas and have to communicate across an ISP network. A normal communication is required.

Figure 4-1 shows the network topology. Switches of the two divisions are connected to customer networks VLAN 100 and VLAN 200 respectively. And they communicate across ISP network VLAN 1050. Devices in the ISP network adopt TPID value 0x9100.

Figure 4-1 Network Topology



4.2 Configuration Scheme

Users can configure VLAN-VPN on Switch 1 and Switch 2 to allow packets sent with double VLAN tags, and thus ensure the communication between them. The general configuration procedure is as follows:

1) Configure 802.1Q VLAN before VLAN-VPN configuration. Create ISP network VLAN 1050 on the switch, and add port1/0/1 tagged and port 1/0/2 untagged to the VLAN. Create client network VLAN 100 and VLAN 200, and add port 1/0/2 tagged to both the VLANs. Set the PVID of port 1/0/1 and port 1/0/2 as 1050.
2) Set port 1/0/1 as the VPN up-link port and port 1/0/2 as the VPN port.
3) Enable the VPN feature globally, and set global TPID as 0x9100.

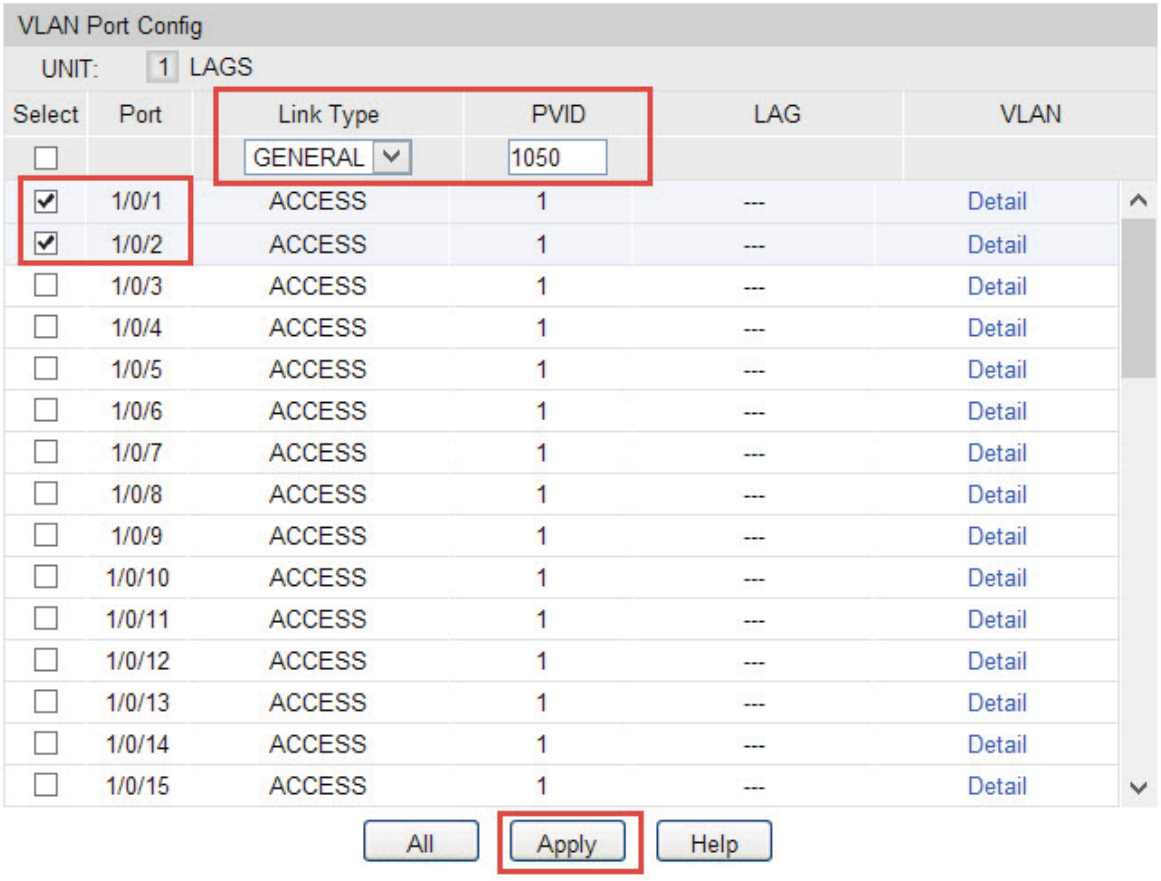
Demonstrated with T2600G-28TS, this chapter provides configuration procedures in two ways: using the GUI and using the CLI.

4.3 Using the GUI

The configurations of Switch 1 and Switch 2 are similar. The following introductions take Switch 1 as an example.

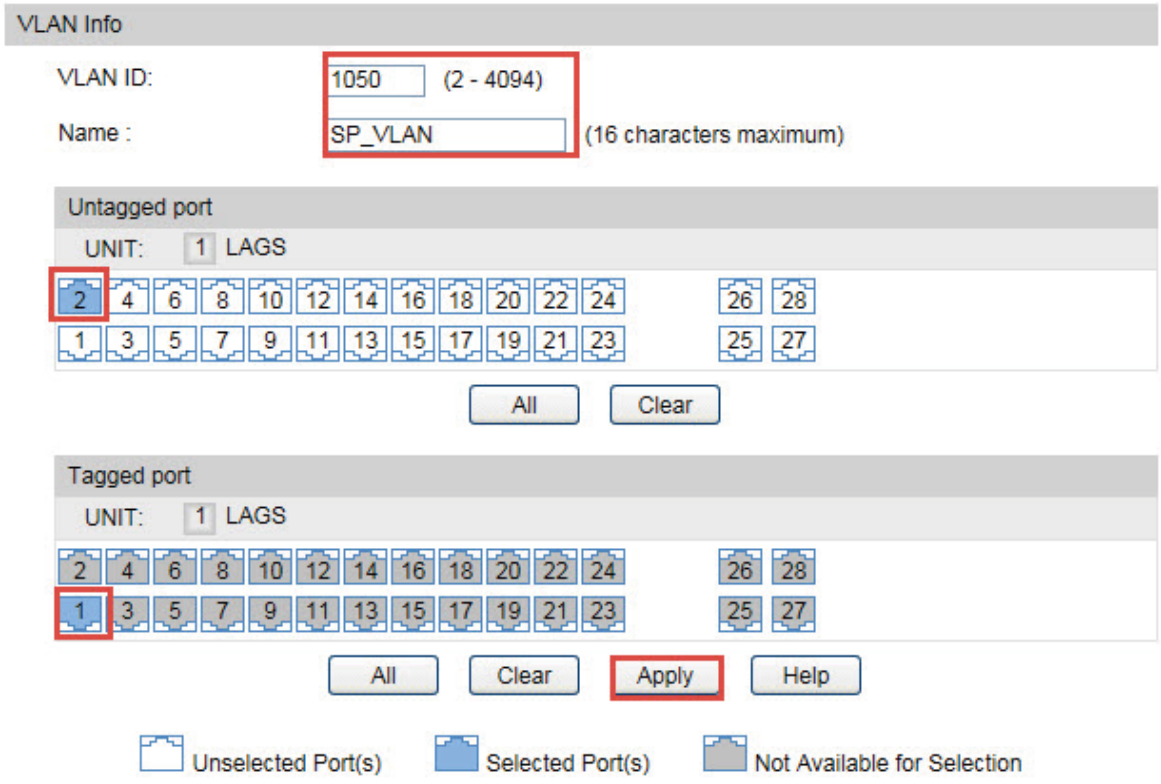
1) Choose the menu **VLAN > 802.1Q VLAN > Port Config** to load the following page. Set the link type of ports 1/0/1-2 as General, and modify PVID of the two ports as 1050. Then click **Apply**.

Figure 4-2 Setting Link Type of Ports



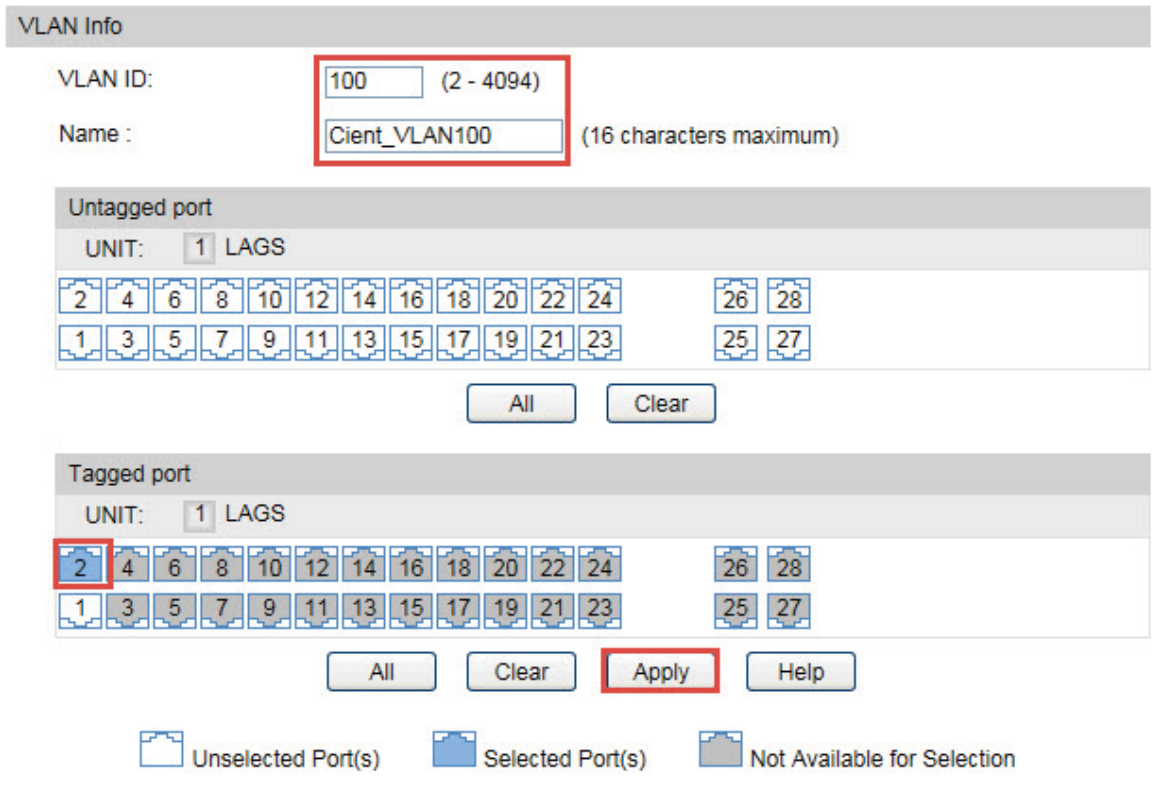
2) Choose the menu **VLAN > 802.1Q VLAN > VLAN Config** and click **Create** to load the following page. Create VLAN 1050, and add port 1/0/1 tagged and port 1/0/2 untagged to the VLAN. Then click **Apply**.

Figure 4-3 Creating VLAN 1050



3) Choose the menu **VLAN > 802.1Q VLAN > VLAN Config** and click **Create** to load the following page. Create VLAN 100, and add port 1/0/2 tagged to the VLAN. Click **Apply**.

Figure 4-4 Creating VLAN 100



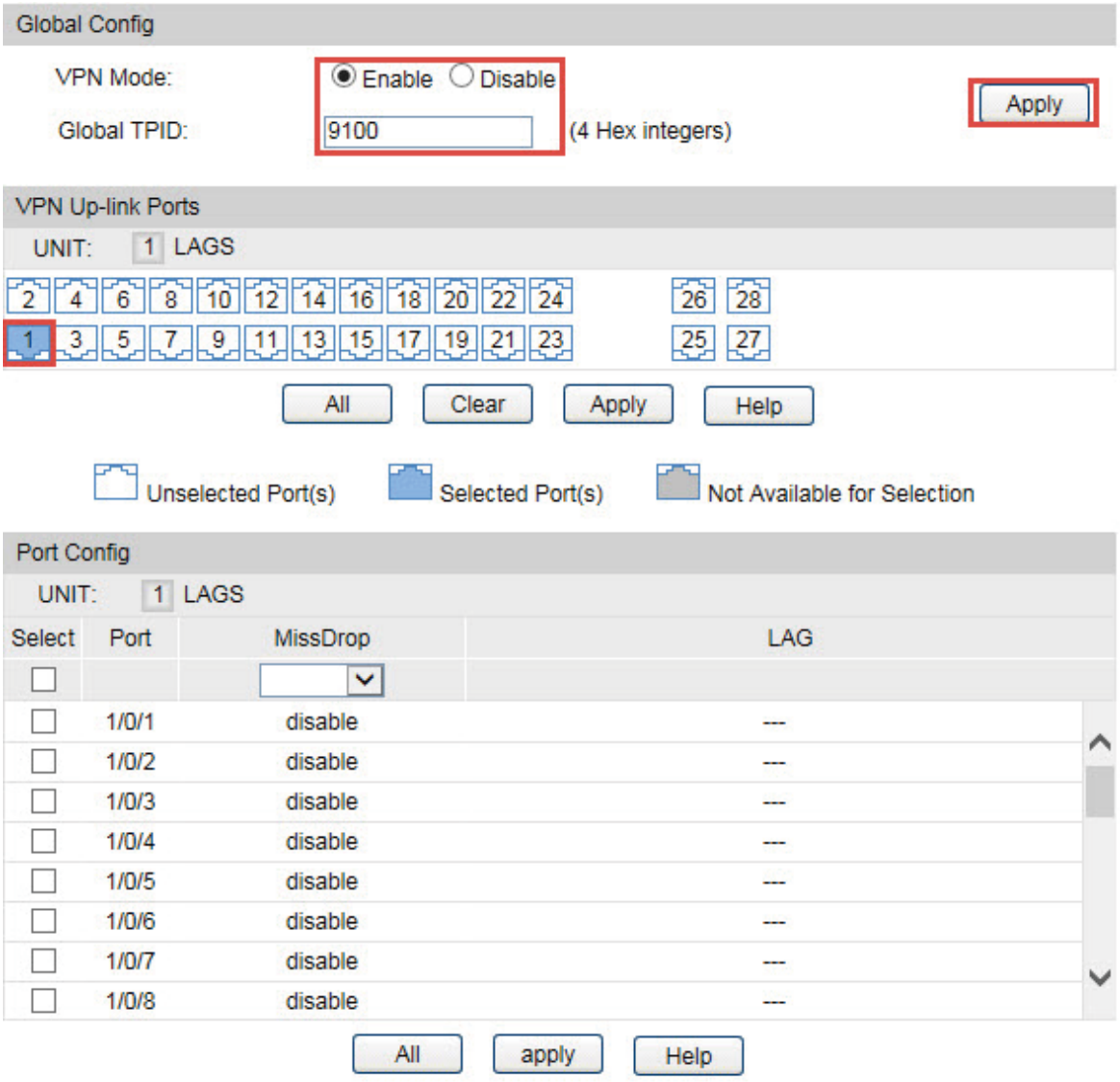
4) Choose the menu **VLAN > 802.1Q VLAN > VLAN Config** and click **Create** to load the following page. Create VLAN 200, and add port 1/0/2 tagged to the VLAN. Click **Apply**.

Figure 4-5 Creating VLAN 200



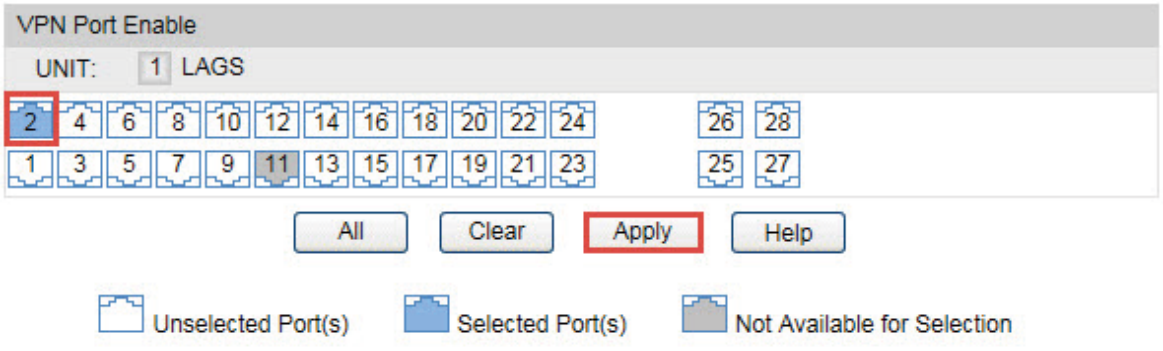
5) Choose the menu **VLAN > VLAN-VPN > VPN Config** to load the following page. Enable VPN globally, set TPID as 9100, and select port 1/0/1 as the up-link port. Click **Apply**.

Figure 4-6 Configuring Global VLAN-VPN



6) Choose the menu **VLAN > VLAN-VPN > Port Enable** to load the following page. Select port 1/0/2 and click **Apply**.

Figure 4-7 Enabling the VPN Port



7) Click **Save Config** to save the settings.

4.4 Using the CLI

The configurations of Switch 1 and Switch 2 are similar. The following introductions take Switch 1 as an example.

1) Create VLAN 1050, VLAN 100 and VLAN 200.

```
Switch_1#configure
Switch_1(config)#vlan 1050
Switch_1(config-vlan)#name SP_VLAN
Switch_1(config-vlan)#exit
Switch_1(config)#vlan 100
Switch_1(config-vlan)#name Client_VLAN100
Switch_1(config-vlan)#exit
Switch_1(config)#vlan 200
Switch_1(config-vlan)#name Client_VLAN200
Switch_1(config-vlan)#exit
```

2) Set the link type of port 1/0/1 as General, add it to VLAN 1050 as tagged port, modify PVID as 1050, and set the port as VPN up-link port.

```
Switch_1(config)#interface gigabitEthernet 1/0/1
Switch_1(config-if)#switchport mode general
Switch_1(config-if)#switchport general allowed vlan 1050 tagged
Switch_1(config-if)#switchport pvid1050
Switch_1(config-if)#switchport dot1q-tunnel mode nni
Switch_1(config-if)#exit
```

3) Set the link type of port 1/0/2 as general, add it to VLAN 1050 as untagged port, and add it to VLAN 100 and VLAN 200 as tagged port. Modify PVID of the port as 1050. Set the port as the VPN port.

```
Switch_1(config)#interface gigabitEthernet 1/0/2
Switch_1(config-if)#switchport mode general
Switch_1(config-if)#switchport general allowed vlan 1050 untagged
Switch_1(config-if)#switchport general allowed vlan 100,200 tagged
Switch_1(config-if)#switchport pvid 1050
Switch_1(config-if)#switchport dot1q-tunnel mode uni
Switch_1(config-if)#exit
```

4) Enable VLAN-VPN globally, and modify TPID as 9100.

```
Switch_1(config)#dot1q-tunnel
Switch_1(config)#dot1q-tunnel tpid 9100
Switch_1(config)#end
Switch_1#copy running-config startup-config
```

Verify the Configurations

Verify the configurations of global VLAN-VPN:

```
Switch_1#show dot1q-tunnel
VLAN-VPN Mode: Enabled
Global TPID: 0X9100
Mapping Mode: Disabled
```

Verify the configurations of VPN up-link port and VPN port:

```
Switch_1#show dot1q-tunnel interface
Port Type          Member
-------------      -----------------
NNI                Gi1/0/1
UNI                Gi1/0/2
```

Verify the port configuration:

```
Switch_1#show interface switchport gigabitEthernet 1/0/1
Port Gi1/0/1:
PVID: 1050
Member in LAG: N/A
Link Type: General
Member in VLAN:
Vlan      Name              Egress-rule
----      -----------       -----------
1         System-VLAN       Untagged
1050      SP_VLAN           Tagged
```

```
Switch_1#show interface switchport gigabitEthernet 1/0/2
Port Gi1/0/2:
PVID: 1050
Member in LAG: N/A
Link Type: General
Member in VLAN:
Vlan     Name              Egress-rule
----     ----------        ----------
1        System-VLAN       Untagged
100      Client_VLAN100    Tagged
200      Client_VLAN200    Tagged
1050     SP_VLAN           Untagged
```

5 Appendix: Default Parameters

Default settings of VLAN-VPN are listed in the following table.

Table 5-1 Default Settings of VLAN-VPN

Parameter	Default Setting
Global VLAN-VPN	Disable
MissDrop	Disable
VLAN Mapping	Disable
Global TPID	0x8100

Part 13

Configuring GVRP

CHAPTERS

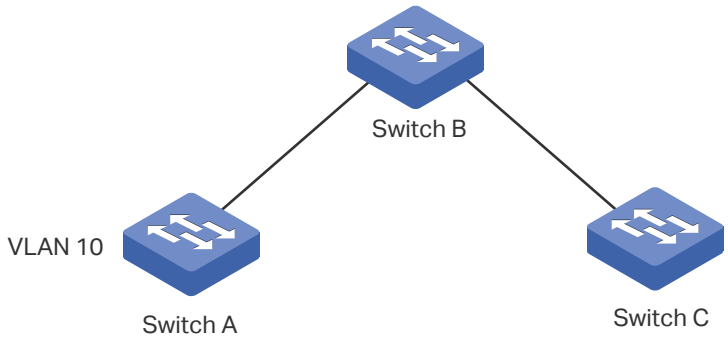
1. Overview
2. GVRP Configuration
3. Configuration Example
4. Appendix: Default Parameters

1 Overview

GVRP (GARP VLAN Registration Protocol) is a GARP (Generic Attribute Registration Protocol) application that allows registration and deregistration of VLAN attribute values and dynamic VLAN creation.

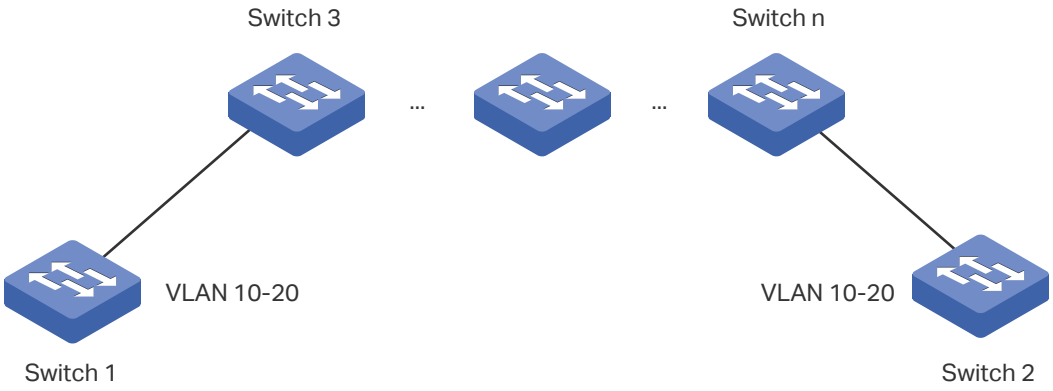
Without GVRP operating, configuring the same VLAN on a network would require manual configuration on each device. As shown in Figure 1-1, Switch A, B and C are connected through trunk ports. VLAN 10 is configured on Switch A, and VLAN 1 is configured on Switch B and Switch C. Switch C can receive messages sent from Switch A in VLAN 10 only when the network administrator has manually created VLAN 10 on Switch B and Switch C.

Figure 1-1 VLAN Topology



The configuration may seem easy in this situation. However, for a larger or more complex network, such manual configuration would be time-costing and fallible. GVRP can be applied to implement dynamic VLAN configuration. With GVRP, the switch can exchange VLAN configuration information with the adjacent GVRP switches and dynamically create and manage the VLANs. This reduces VLAN configuration workload and ensures correct VLAN configuration.

Figure 1-2 GVRP Topology



2 GVRP Configuration

To complete GVRP configuration, follow these steps:

1) Create a VLAN, and set link type as Trunk for ports that need to enable GVRP.
2) Enable GVRP globally.
3) Enable GVRP on each trunk port and configure the corresponding parameters.

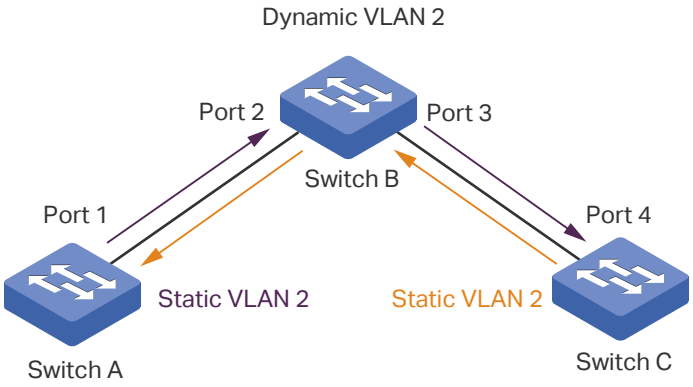
Configuration Guidelines

To dynamically create a VLAN on all ports in a network link, you must configure the same static VLAN on both ends of the link.

We call manually configured 802.1Q VLAN as static VLAN and VLAN created through GVRP as dynamic VLAN. Ports in a static VLAN can initiate the sending of GVRP registration message to other ports. And a port registers VLANs only when it receives GVRP messages. As the messages can only be sent from one GVRP participant to another, two-way registration is required to configure a VLAN on all ports in a link. To implement two-way registration, you need to manually configure the same static VLAN on both ends of the link.

As shown in the figure below, VLAN registration from Switch A to Switch C adds Port 2 to VLAN 2. And VLAN registration from Switch C to Switch A adds Port 3 to VLAN 2.

Figure 2-1



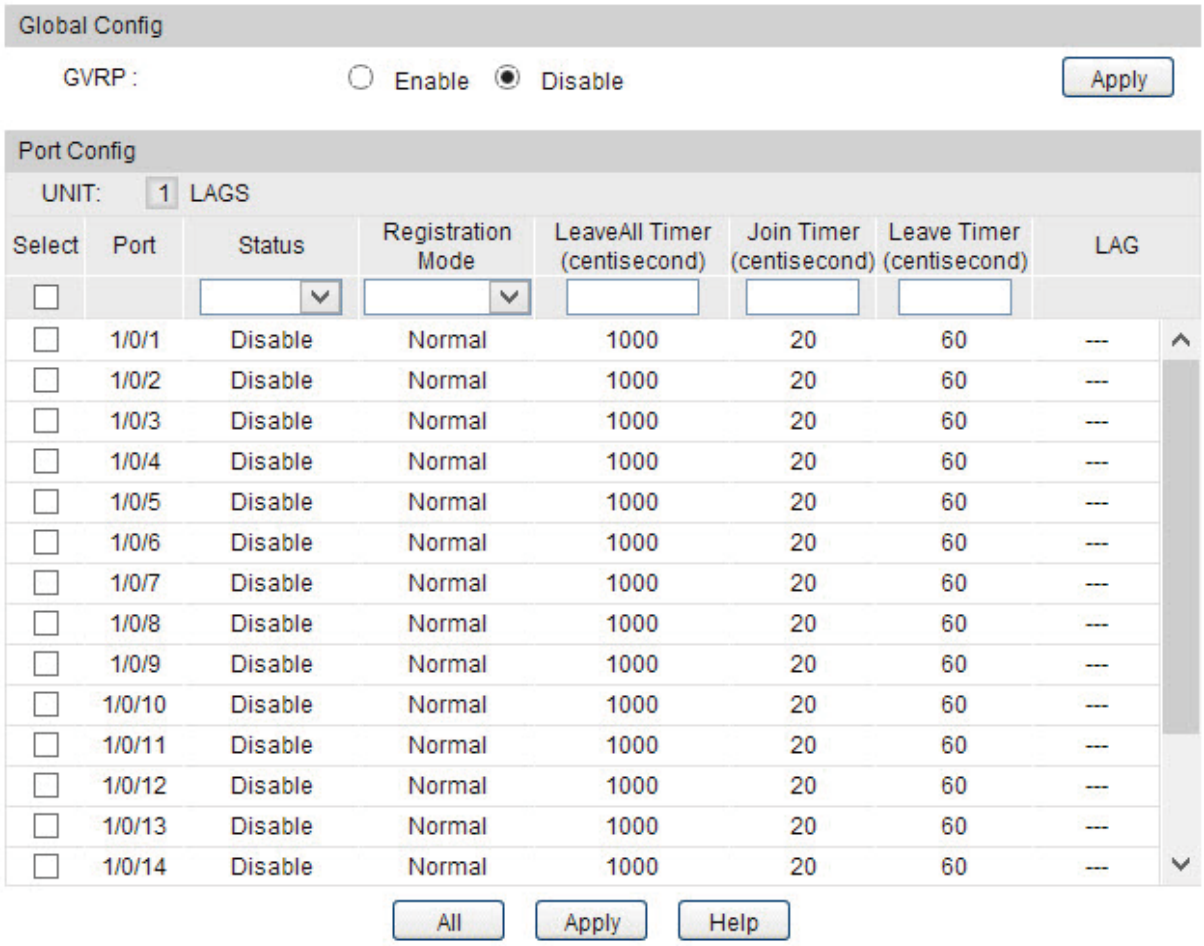
Similarly, if you want to delete a VLAN from all ports, two-way deregistration is required. And you need to manually delete the static VALN on both ends of the link.

2.1 Using the GUI

GVRP requires VLAN creation first. And you need to set the link type of the ports as Trunk, for GVRP can be enabled only on trunk interfaces. For details, refer to *Configuring 802.1Q VLAN*.

Choose the menu **VLAN > GVRP > GVRP Config** to load the following page.

Figure 2-1 GVRP Config



Follow these steps to configure GVRP:

1) In the **Global Config** section, enable GVRP globally, then click **Apply**.
2) In the **Port Config** section, select one or more ports, set the status as Enable and configure the related parameters according to your needs.

Port	Select the desired port for GVRP configuration. It is multi-optional. For selected ports, the link type must be set as Trunk, or the system will prompt error when applying the configuration.
Status	Enable or disable GVRP on the port. By default, it is disabled.

Registration Mode	Select the GVRP registration mode for the port. **Normal**: In this mode, the port can dynamically register and deregister VLANs, and transmit both dynamic and static VLAN registration information. **Fixed**: In this mode, the port is unable to dynamically register and deregister VLANs, and can transmit only the static VLAN registration information. **Forbidden**: In this mode, the port is unable to dynamically register and deregister VLANs, and can transmit only information of VLAN 1.
LeaveAll Timer (centisecond)	When a GARP participant is enabled, the LeaveAll timer is started. When the LeaveAll timer expires, the GARP participant sends LeaveAll messages to request other GARP participants to re-register all its attributes. After that, the participant restarts the LeaveAll timer. The timer ranges from 1000 to 30000 centiseconds. The default is 1000 centiseconds.
Join Timer (centisecond)	Join timer controls the sending of Join messages. A participant starts the Join timer after sending the first Join message. If the participant does not receive any respond, it sends the second Join message when the Join timer expires. This ensures that the Join message can be sent to other participants. The timer ranges from 20 to 1000 centiseconds. The default is 20 centiseconds.
Leave Timer (centisecond)	The Leave timer controls attribute deregistration. A participant sends a Leave message if one of its attributes is deleted. The participant receiving the message starts the Leave timer. If the participant does not receive any Join message of the corresponding attribute before the Leave timer expires, the participant deregisters the attribute. The range is 60 to 3000 centiseconds. The default is 60 centiseconds.
LAG	Displays the LAG the port is in.

3) Click **Apply**.

Note:

- The member port of an LAG follows the configuration of the LAG but not its own. The configurations of the port can take effect only after it leaves the LAG.
- When setting the timer values, make sure the values are within the required range. The configuration value for LeaveAll should be greater than or equal to ten times the Leave value. The value for Leave should be greater than or equal to two times the Join value.

2.2 Using the CLI

GVRP requires VLAN creation first. And you need to set the link type of the ports as Trunk, for GVRP can be enabled only on trunk interfaces. For details, refer to *Configuring 802.1Q VLAN*.

Step 1	**configure** Enter global configuration mode.
Step 2	**gvrp** Enable GVRP globally.
Step 3	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channelid-list* **}** Enter interface configuration mode.
Step 4	**gvrp** Enable GVRP on the port.
Step 5	**gvrp registration** { normal | fixed | forbidden } Configure the GVRP registration mode for the port. normal: In this mode, the port can dynamically register and deregister VLANs , and transmit both dynamic and static VLAN registration information. It is the default mode. fixed: In this mode, the port is unable to dynamically register and deregister VLANs, and can transmit only the static VLAN registration information. In Fixed mode, only the static VLAN the port belongs to is allowed to pass. forbidden: In this mode, the port is unable to dynamically register and deregister VLANs, and can transmit only information of VLAN 1. In Forbidden mode, only the default VLAN 1 is allowed to pass.
Step 6	**gvrp timer** { leaveall | join | leave } *value* Set the GARP timers according to your needs. leaveall: When a GARP participant is enabled, the LeaveAll timer is started. When the LeaveAll timer expires, the GARP participant sends LeaveAll messages to request other GARP participants to re-register all its attributes. join: Join timer controls the sending of Join messages. After sending the first Join message, a participant starts the Join timer. If the participant does not receive any JoinIn message, it sends the second Join message when the Join timer expires. This ensures that the Join message can be sent to other participants. leave: A participant sends a Leave message if one of its attributes is deleted. The participant receiving the message starts the Leave timer. If the participant does not receive any Join message of the corresponding attribute before the Leave timer expires, the participant deregisters the attribute. *value*: Set a value for the timer. For LeaveAll timer, the range is 1000 to 30000 centiseconds and the default is 1000 centiseconds. For Join timer, the range is is 20 to 1000 centiseconds and the default is 20 centiseconds. For Leave timer, the range is is 60 to 3000 centiseconds and the default is 60 centiseconds.
Step 7	**show gvrp global** Verify the global configurations of GVRP.

Step 8	**show gvrp interface [fastEthernet** *port* **| gigabitEthernet** *port* **| port-channel** *port-channel-id* **]** Verify the GVRP configuration of the specified port or LAG.
Step 9	**end** Return to privileged EXEC mode.
Step 10	**copy running-config startup-config** Save the settings in the configuration file.

Note:

- The member port of an LAG follows the configuration of the LAG but not its own. The configurations of the port can take effect only after it leaves the LAG.
- When setting the timer values, make sure the values are within the required range. The value for LeaveAll should be greater than or equal to ten times the Leave value. The value for Leave should be greater than or equal to two times the Join value.

The following example shows how to enable GVRP globally and on trunk port 1/0/1, configure the GVRP registration mode as fixed and keep the values of timers as default:

Switch#configure

Switch(config)#gvrp

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

Switch(config-if)#gvrp

Switch(config-if)#gvrp registration fixed

Switch(config-if)#show gvrp global

GVRP Global Status

Enabled

Switch(config-if)# show gvrp interface gigabitEthernet 1/0/1

Port	Status	Reg-Mode	LeaveAll	JoinIn	Leave	LAG
----	------	--------	--------	------	-----	---
Gi1/0/1	Enabled	Fixed	1000	20	60	N/A

Switch(config-if)#end

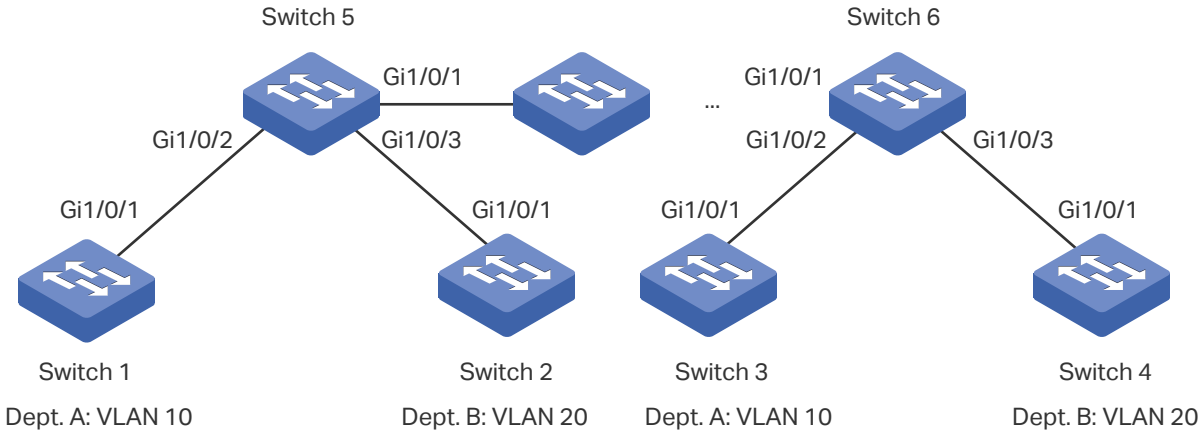
Switch#copy running-config startup-config

3 Configuration Example

3.1 Network Requirements

Department A and Department B of a company are connected using switches. Offices of one department are distributed on different floors. As shown in Figure 3-1, the network topology is complicated. Configuration of the same VLAN on different switches is required so that computers in the same department can communicate with each other.

Figure 3-1 Network Topology



3.2 Configuration Scheme

To reduce manual configuration and maintenance workload, GVRP can be enabled to implement dynamic VLAN registration and update on the switches.

When configuring GVRP, please note the following:

- Before enabling GVRP, set the link type for all ports in the link as Trunk.
- The two departments are in separate VLANs. To make sure the switches only dynamically create VLAN of their own department, you need to set the registration mode for ports on Switch 1 to Switch 4 as Fixed to prevents dynamic registration and deregistration of VLANs and allow the port to transmit only the static VLAN registration information.
- To configure dynamic VLAN creation on other switches, set the registration mode of the corresponding ports as Normal to allow dynamic registration and de-registration of VLANs.

Demonstrated with T2600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

3.3 Using the GUI

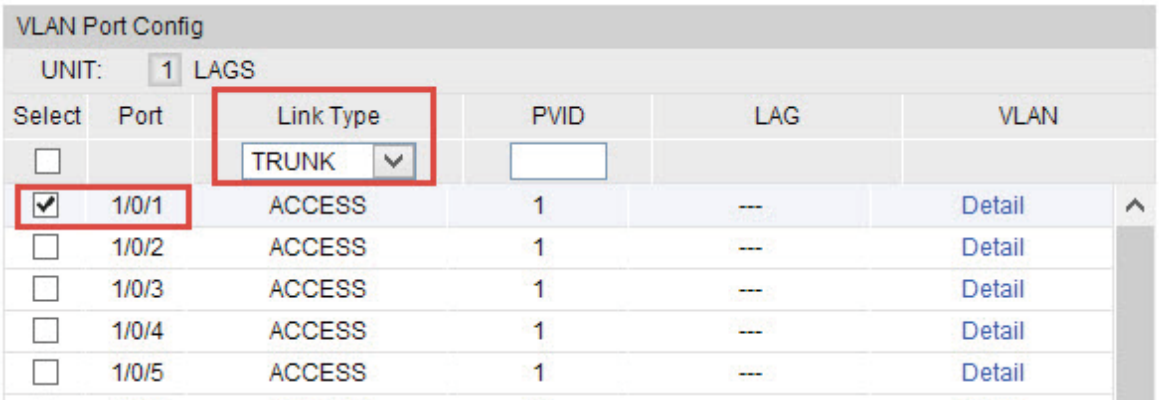
GVRP configuration for Switch 3 is the same as Switch 1, and Switch 4 the same as Switch 2. Other switches share similar configurations.

The following configuration procedures take Switch 1, Switch 2 and Switch 5 as example.

- Configurations for Switch 1

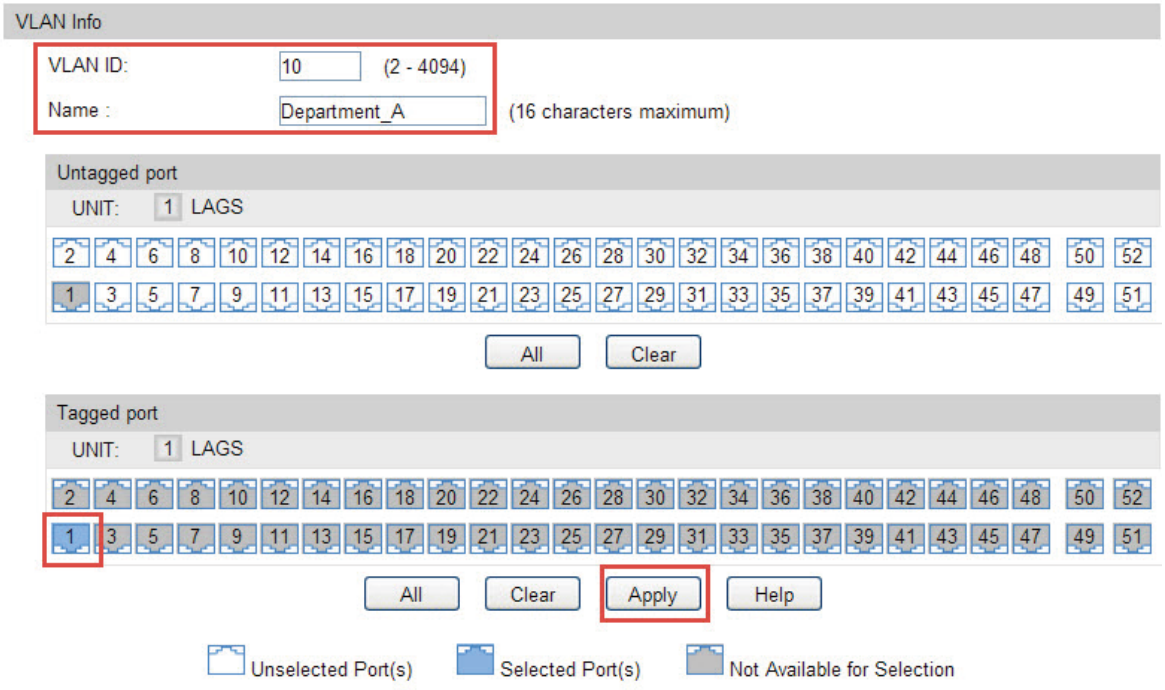
1) Choose the menu **VLAN > 802.1Q VLAN > Port Config** to load the following page. Set the link type of port 1/0/1 as Trunk, and click **Apply**.

Figure 3-2 Set Link Type for the Port



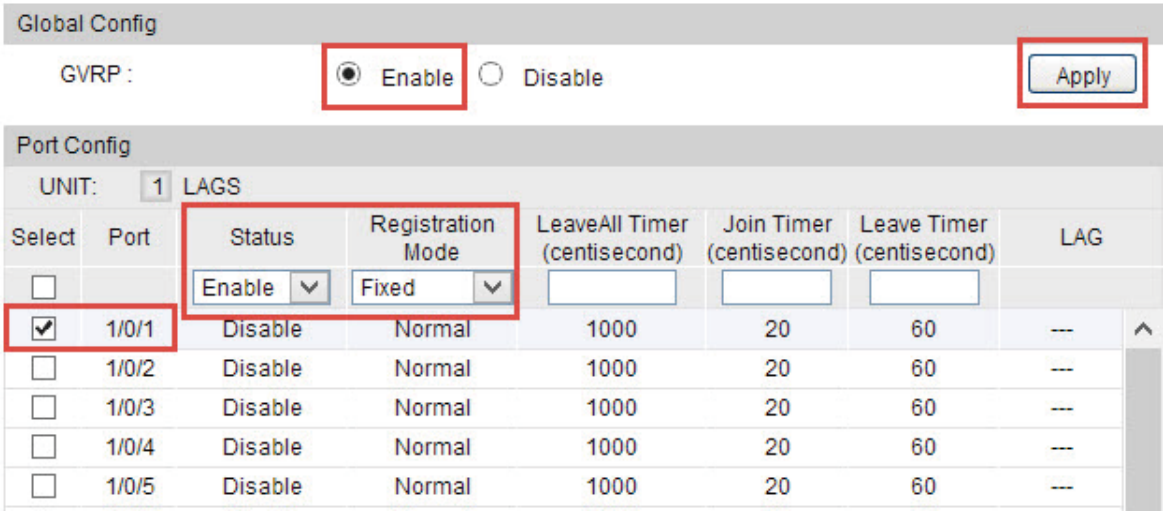
2) Choose the menu **VLAN > 802.1Q VLAN > VLAN Config** to load the following page. Create VLAN 10, and add port 1/0/1 to it. Click **Apply.**

Figure 3-3 VLAN Configuration



3) Choose the menu **VLAN > GVRP > GVRP Config** to load the following page. Enable GVRP globally, then click **Apply**. Select port 1/0/1, set Status as Enable, and set Registration Mode as Fixed. Keep the values of the timers as default. Click **Apply**.

Figure 3-4 GVRP Configuration

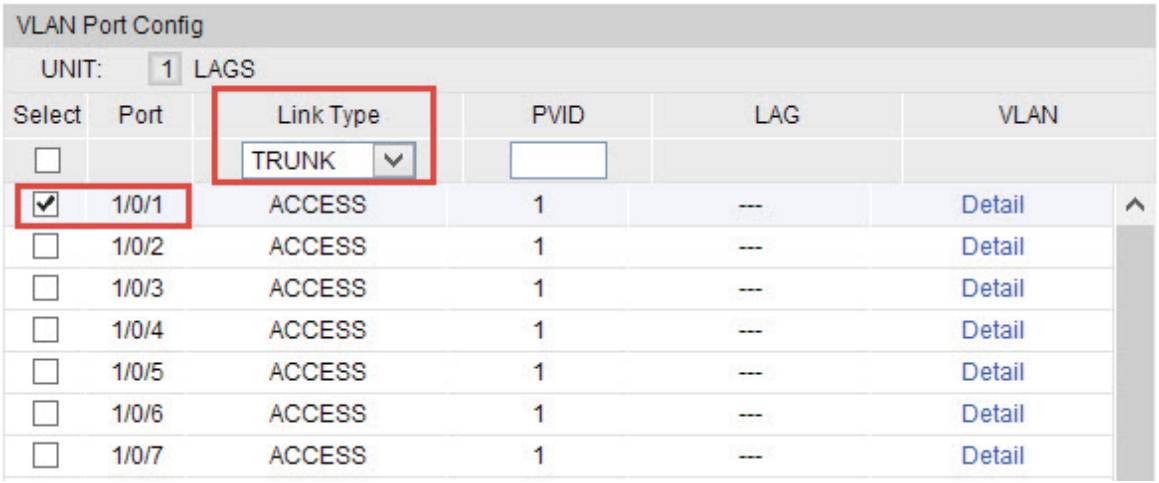


4) Click **Save Config** to save the settings.

Configurations for Switch 2

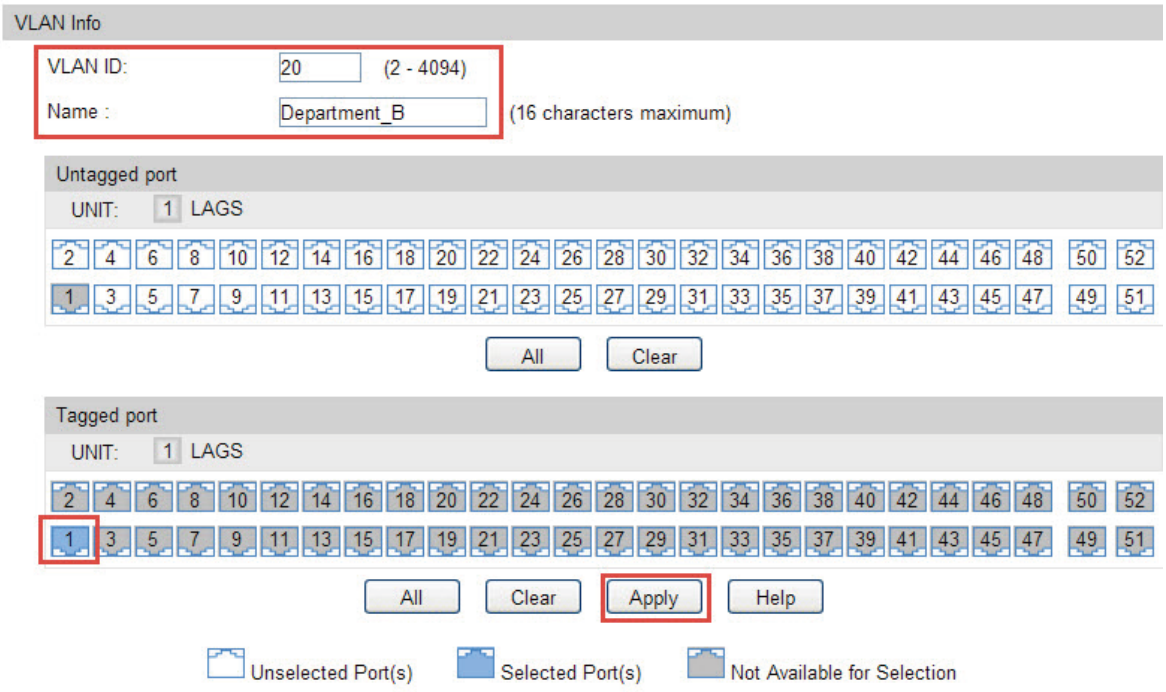
1) Choose the menu **VLAN > 802.1Q VLAN > Port Config** to load the following page. Set the link type of port 1/0/1 as Trunk.

Figure 3-5 Set Link Type for the Port



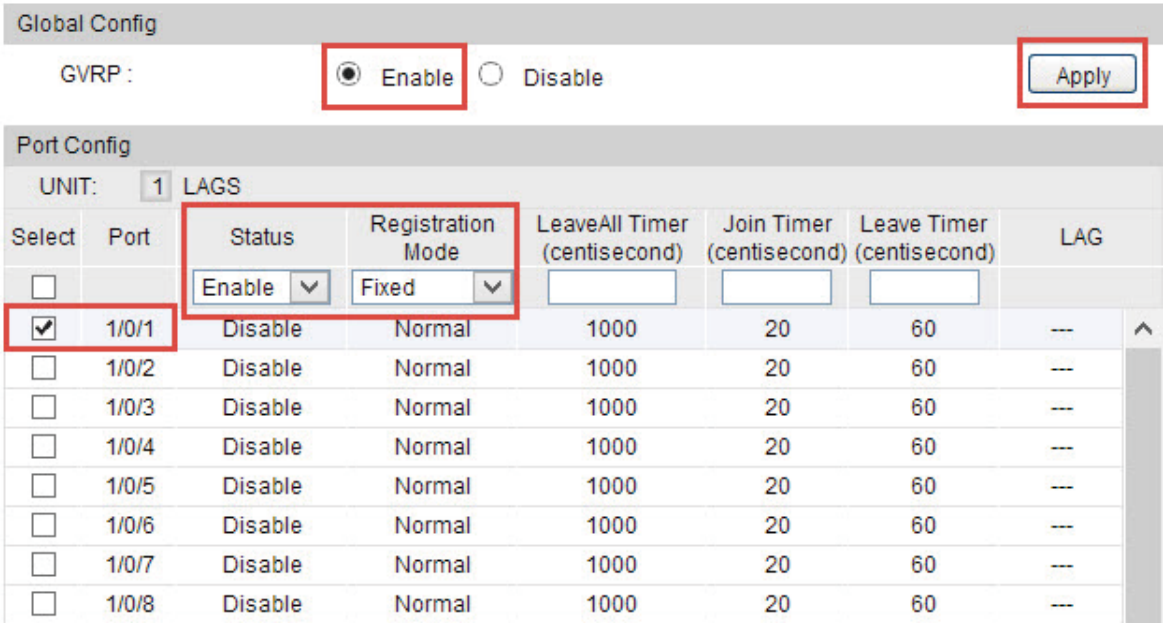
2) Choose the menu **VLAN > 802.1Q VLAN > VLAN Config** to load the following page. Create VLAN 10, and add port 1/0/1 to it. Click **Apply**.

Figure 3-6 VLAN Configuration



3) Choose the menu **VLAN > GVRP > GVRP Config** to load the following page. Enable GVRP globally, then click **Apply**. Select port 1/0/1, set Status as Enable, and set Registration Mode as Fixed. Keep the values of the timers as default. Click **Apply**.

Figure 3-7 GVRP Configuration

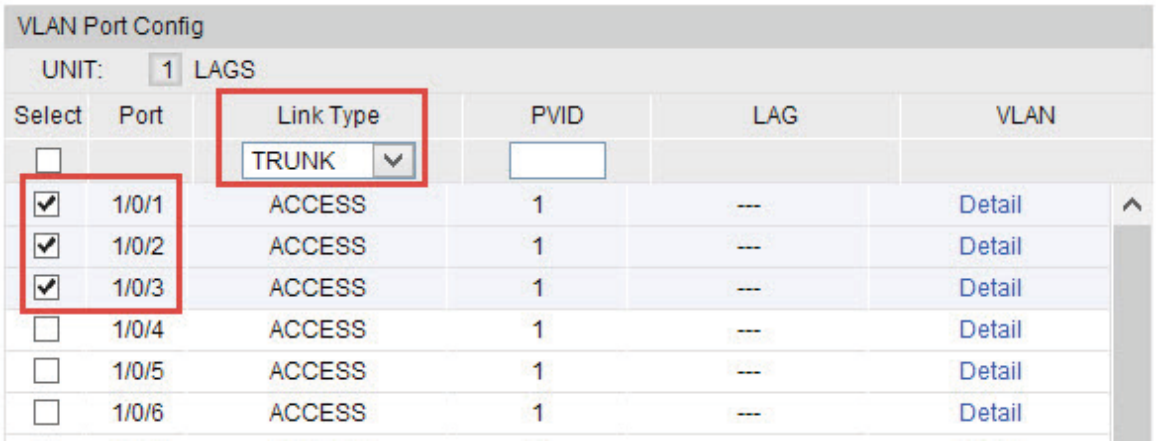


4) Click **Save Config** to save the settings.

Configurations for Switch 5

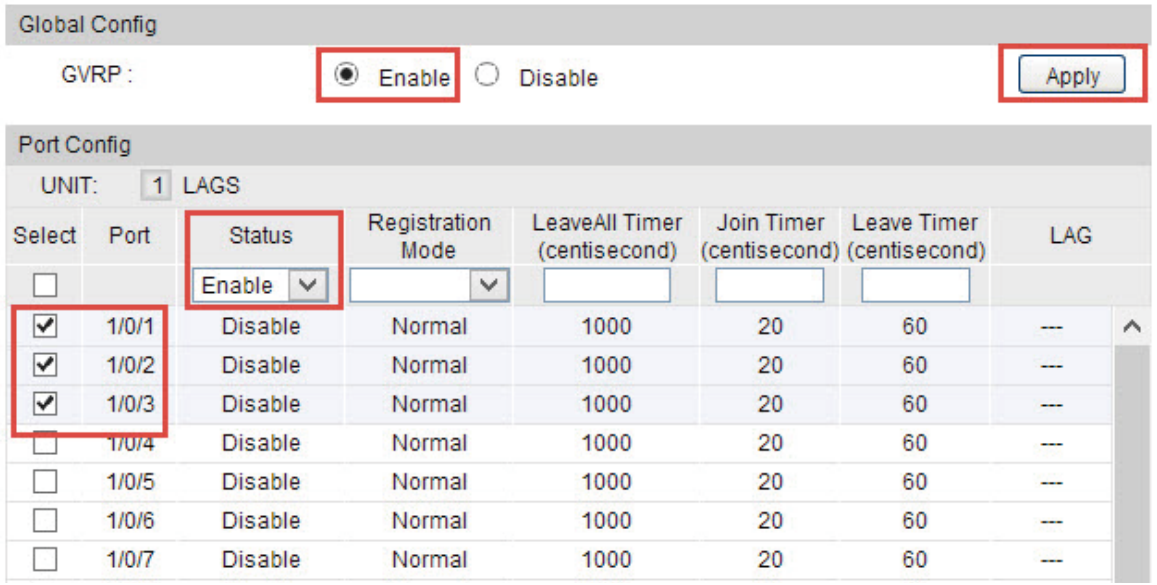
1) Choose the menu **VLAN > 802.1Q VLAN > Port Config** to load the following page. Set the link type of ports 1/0/1-3 as Trunk.

Figure 3-8 Set Link Type for the Port



2) Choose the menu **VLAN > GVRP > GVRP Config** to load the following page. Enable GVRP globally, then click **Apply**. Select ports 1/0/1-3, set Status as Enable, and keep the Registration Mode and the values of the timers as default. Click **Apply**.

Figure 3-9 GVRP Configuration



3) Click **Save Config** to save the settings.

3.4 Using the CLI

GVRP configuration for Switch 3 is the same as Switch 1, and Switch 4 the same as Switch 2. Other switches share similar configurations.

The following configuration procedures take Switch 1, Switch 2 and Switch 5 as example.

- Configurations for Switch 1

1) Enable GVRP globally.

```
Switch_1#configure
Switch_1(config)#gvrp
```

2) Create VLAN 10.

```
Switch_1(config)#vlan 10
Switch_1(config-vlan)#name Department A
Switch_1(config-vlan)#exit
```

3) For port 1/0/1, set the link type as Trunk, and add it to VLAN 10. Enable GVRP and set the registration mode as Fixed.

```
Switch_1(config)#interface gigabitEthernet 1/0/1
Switch_1(config-if)#switchport mode trunk
Switch_1(config-if)#switchport trunk allowed vlan 10
Switch_1(config-if)#gvrp
Switch_1(config-if)#gvrp registration fixed
Switch_1(config-if)#end
Switch_1#copy running-config startup-config
```

- Configurations for Switch 2

1) Enable GVRP globally.

```
Switch_2#configure
Switch_2(config)#gvrp
```

2) Create VLAN 20.

```
Switch_2(config)#vlan 20
Switch_2(config-vlan)#name Department B
Switch_2(config-vlan)#exit
```

3) For port 1/0/1, set the link type as Trunk, and add it to VLAN 20. Enable GVRP and set the registration mode as Fixed.

```
Switch_2(config)#interface gigabitEthernet 1/0/1
Switch_2(config-if)#switchport mode trunk
Switch_2(config-if)#switchport trunk allowed vlan 20
Switch_2(config-if)#gvrp
Switch_2(config-if)#gvrp registration fixed
Switch_2(config-if)#end
Switch_2#copy running-config startup-config
```

- Configurations for Switch 5

1) Enable GVRP globally.

   Switch_5#configure

   Switch_5(config)#gvrp

2) For ports 1/0/1-3, set the link type as Trunk and enable GVRP.

   Switch_5(config)#interface range gigabitEthernet 1/0/1-3

   Switch_5(config-if-range)#switchport mode trunk

   Switch_5(config-if-range)#gvrp

   Switch_5(config-if-range)#end

   Switch_5#copy running-config startup-config

Verify the Configuration

- Switch 1

  Verify the global GVRP configuration:

  Switch_1#show gvrp global

  GVRP Global Status

  Enabled

  Verify GVRP configuration for port 1/0/1:

  Switch_1#show gvrp interface

Port	Status	Reg-Mode	LeaveAll	JoinIn	Leave	LAG
Gi1/0/1	Enabled	Fixed	1000	20	60	N/A
Gi1/0/2	Disabled	Normal	1000	20	60	N/A

  ...

- Switch 2

  Verify the global GVRP configuration:

  Switch_2#show gvrp global

  GVRP Global Status

Enabled

Verify GVRP configuration for port 1/0/1:

Switch_2#show gvrp interface

Port	Status	Reg-Mode	LeaveAll	JoinIn	Leave	LAG
Gi1/0/1	Enabled	Fixed	1000	20	60	N/A
Gi1/0/2	Disabled	Normal	1000	20	60	N/A

...

- Switch 5

Verify global GVRP configuration:

GVRP Global Status

Enabled

Verify GVRP configuration for ports 1/0/1-3:

Switch_5#show gvrp interface

Port	Status	Reg-Mode	LeaveAll	JoinIn	Leave	LAG
Gi1/0/1	Enabled	Normal	1000	20	60	N/A
Gi1/0/2	Enabled	Normal	1000	20	60	N/A
Gi1/0/3	Enabled	Normal	1000	20	60	N/A
Gi1/0/4	Disabled	Normal	1000	20	60	N/A

...

4 Appendix: Default Parameters

Default settings of GVRP are listed in the following tables.

Table 4-1 Default Settings of GVRP

Parameter	Default Setting
Global Config	
GVRP	Disable
Port Config	
Status	Disable
Registration Mode	Normal
LeaveAll Timer	1000 centisecond
Join Timer	20 centisecond
Leave Timer	60 centisecond

Part 14

Configuring Private VLAN

CHAPTERS

1. Overview
2. Private VLAN Configurations
3. Configuration Example
4. Appendix: Default Parameters

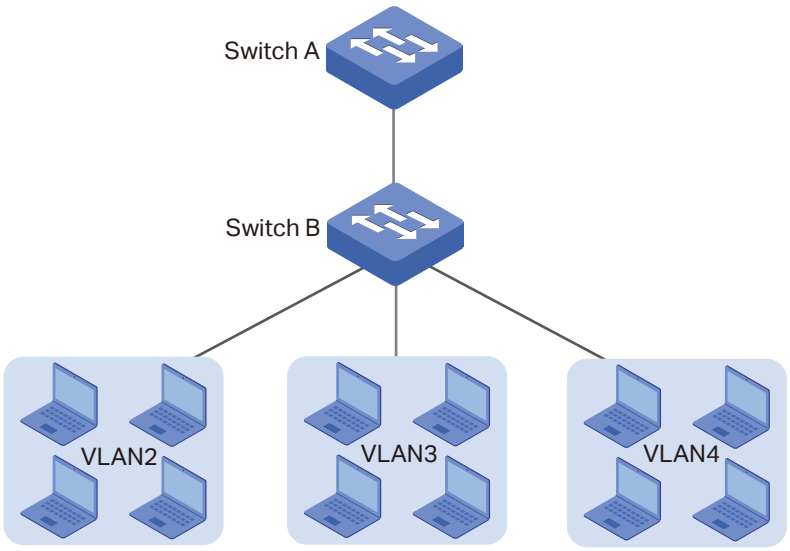
1 Overview

Common large networks such as ISP networks generally isolate users by VLAN. However, with the increasing number of users, upper-layer devices have to create large amount of VLANs to manage all the users. According to IEEE 802.1Q protocol, each upper-layer device can create no more than 4094 VLANs, which means upper-layer devices in backbone networks will face shortage of VLANs. By creating primary VLAN and secondary VLAN, private VLAN is an effective solution to this problem.

Based on 802.1Q VLAN, private VLAN pairs a secondary VLAN with a primary VLAN. A primary VLAN can pair with more than one secondary VLAN to compose several private VLANs. In a private VLAN, Layer 2 isolation can be achieved between end users with secondary VLANs, while upper-layer devices only need to recognize primary VLANs, which solves the problem of VLAN shortage. Meanwhile, private VLAN resolves the conflicts triggered when users' need of VLANs is different from what the ISP can provide.

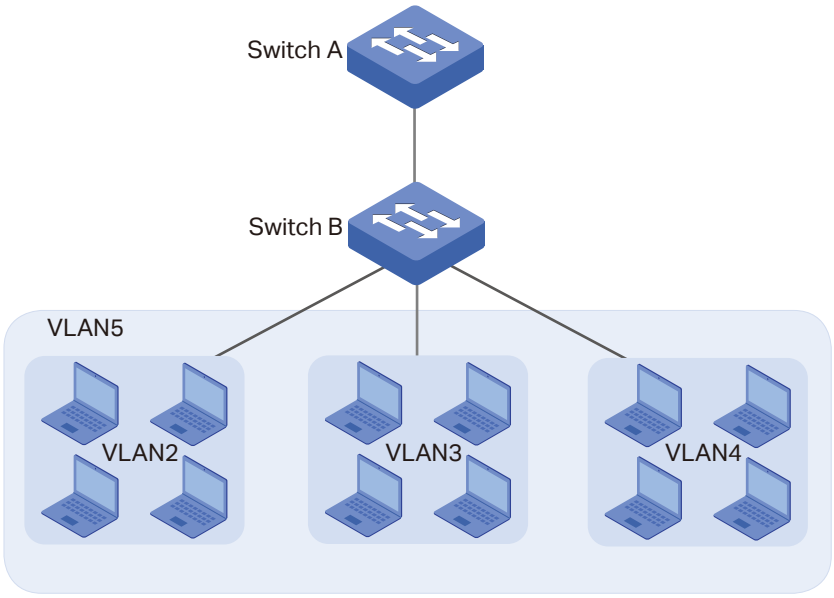
The network models of traditional VLAN and private VLAN are shown in Figure 1-1 and Figure 1-2 respectively. In the network model of traditional VLAN, isolation between users is achieved by creating VLAN2, VLAN3 and VLAN4. In this case, the upper-layer device, Switch A, needs to recognize 3 VLANs including VLAN2, VLAN3 and VLAN4.

Figure 1-1 Topology of Traditional VLAN



If private VLAN is configured on Switch B, Switch A only needs to recognize primary VLAN, VLAN5; and end users can be isolated by secondary VLANs, VLAN2, VLAN3 and VLAN4, saving VLAN resources for Switch A.

Figure 1-2 Topology of Private VLAN



2 Private VLAN Configurations

With private VLAN configuration, you can:

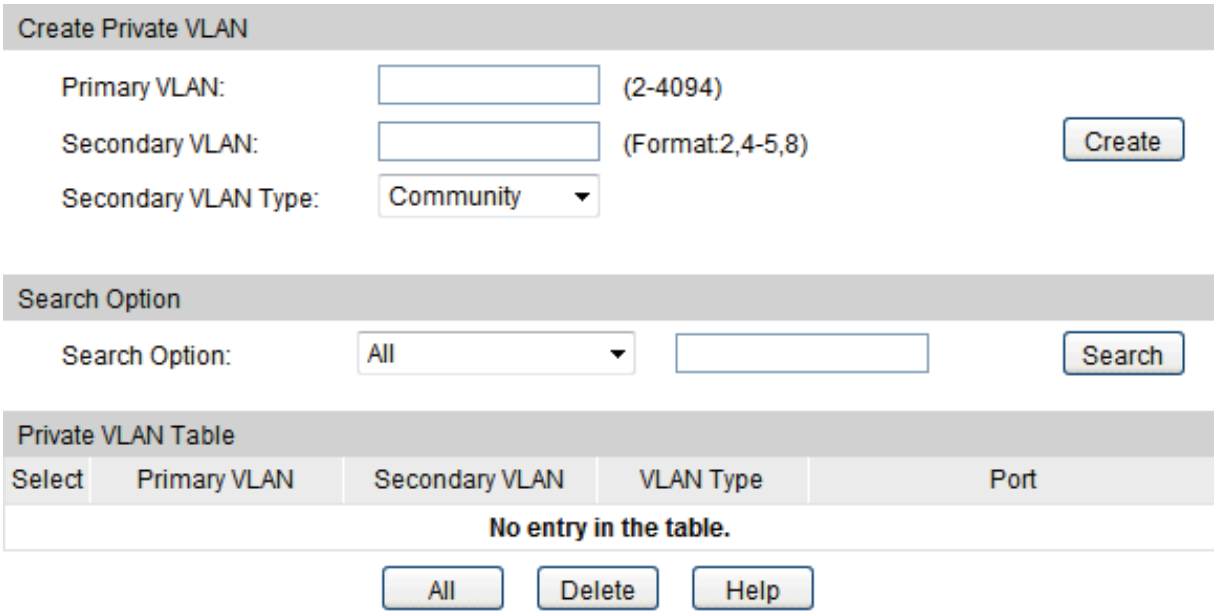
1) Create Private VLAN
2) Configure Private VLAN on Ports

2.1 Using the GUI

2.1.1 Creating Private VLAN

Choose the menu **VLAN** > **Private VLAN** > **PVLAN Config** to load the following page.

Figure 2-1 PVLAN Config



1) In **Create Private VLAN** section, enter the IDs of Primary VLAN and Secondary VLAN, and select Secondary VLAN Type as you need.

Primary VLAN	Enter an ID for Primary VLAN. A primary VLAN can pair with more than one secondary VLAN to compose several private VLANs.
Secondary VLAN	Enter an ID or an ID list for Secondary VLAN. A secondary VLAN can pair with only one primary VLAN to compose one private VLAN. To avoid long response time of the switch, you are recommended to create less than 10 secondary VLANs at a time.

Secondary VLAN Type	Select the Secondary VLAN Type. **Isolated VLAN**: Select this option and users in the same isolated VLAN cannot communicate with each other. **Community VLAN**: Select this option and users in the same community VLAN can communicate with each other.

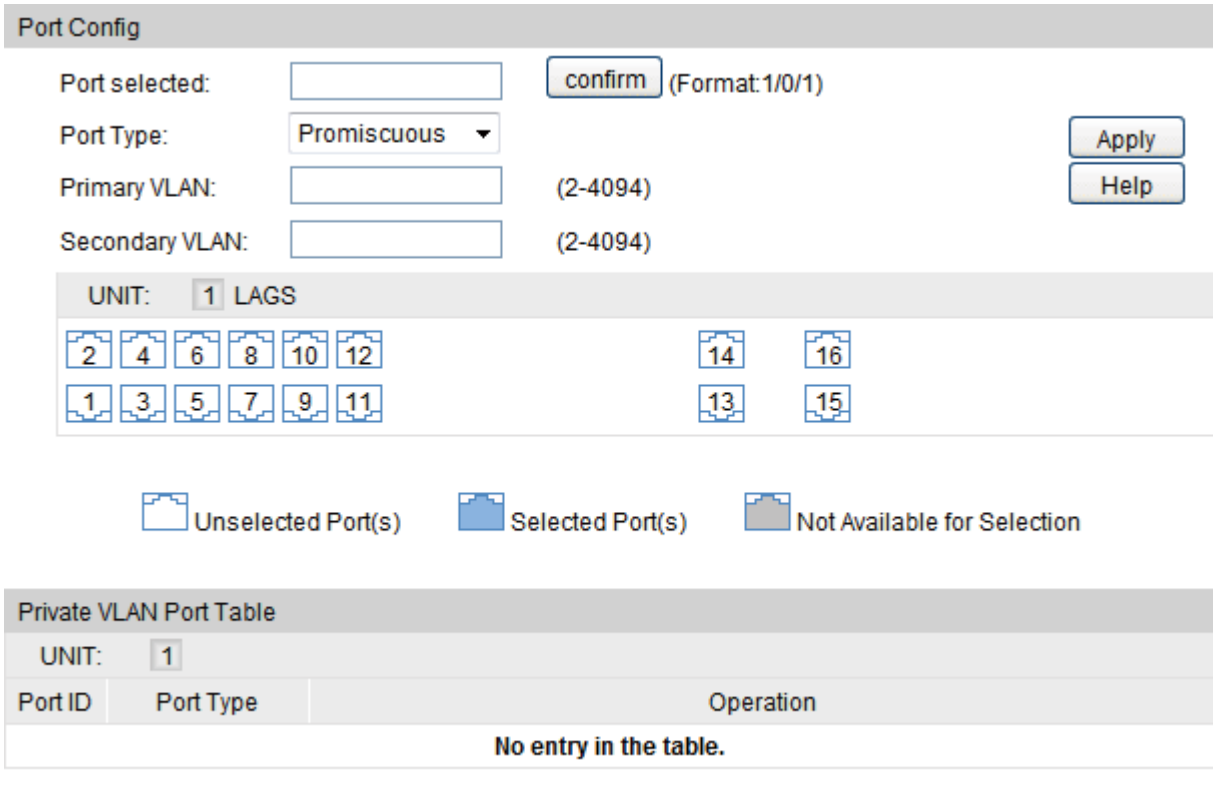
2) Click **Create**.

2.1.2 Configuring the Up-link Port

The switch requires that only access port can be added to a private VLAN.

Choose the menu **VLAN** > **Private VLAN** > **Port Config** to load the following page.

Figure 2-2 Port Config (Configuring the Up-link Port)



1) In the **Port Config** section, select the port to be configured, set the Port Type as Promiscuous, and enter the IDs of Primary VLAN and Secondary VLAN.

Port selected	Specify the port to be configured.
Port Type	Configure the Port Type to be Promiscuous. The port type of up-link port in a primary VLAN must be Promiscuous. This type of port is used to connect upper-layer devices or connect the switch with other switches. The PVID of this port is its primary VLAN ID.
Primary VLAN	Specify the ID of the primary VLAN to add the port to the primary VLAN.

Secondary VLAN	Specify the ID of the secondary VLAN to add the port to the secondary VLAN.

2) Click **Apply**.

Note:

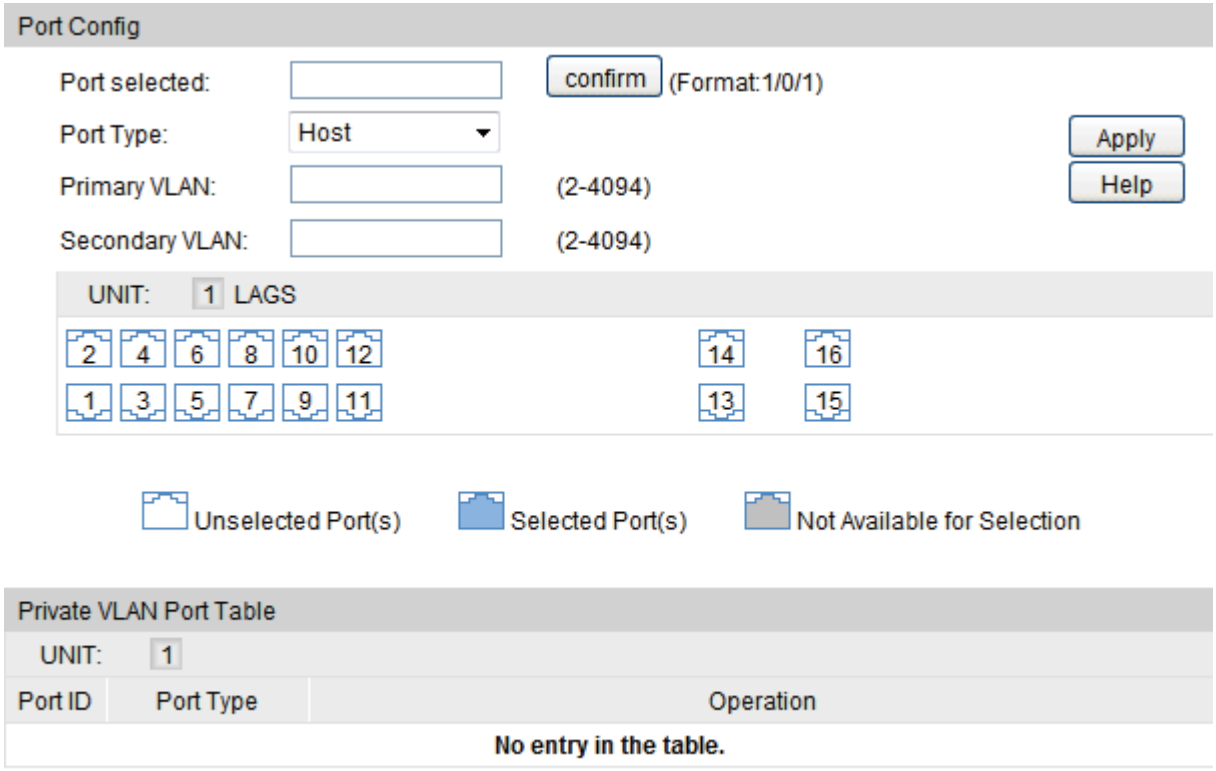
When configuring the up-link port, you only need to add the port to one private VLAN and set the port type as Promiscuous. The switch will automatically add the port to private VLANs with the same primary VLAN.

2.1.3 Configuring the Down-link Port

The switch requires that only access port can be added to a private VLAN.

Choose the menu **VLAN** > **Private VLAN** > **Port Config** to load the following page.

Figure 2-3 Port Config (Configuring the Down-link Port)



1) In the **Port Config** section, select the port to be configured, set the Port Type as Host, and enter the IDs of Primary VLAN and Secondary VLAN.

Port selected	Specify the port to be configured.
Port Type	Configure the Port Type to be Host. The port type of down-link port in a secondary VLAN must be Host. This type of port is used to connect to end users and shield information from upper-layer devices. The PVID of this port is its secondary VLAN ID.

Primary VLAN	Specify the ID of the primary VLAN to add the port to the primary VLAN.
Secondary VLAN	Specify the ID of the secondary VLAN to add the port to the secondary VLAN.

2) Click **Apply**.

2.2 Using the CLI

2.2.1 Creating Private VLAN

Note:

If you need to create a private VLAN with existing VLANs, delete all member ports of the existing VLANs before creating the private VLAN.

Step 1	**configure** Enter global configuration mode.
Step 2	**vlan** *vlan-list* Specify Primary VLAN ID, and enter VLAN configuration mode. *vlan-list*: Specify the ID or the ID list of the VLAN(s) for configuration. The ID ranges from 2 to 4094, for example, 2-3,5.
Step 3	**private-vlan primary** Specify the VLAN to be the primary VLAN.
Step 4	**exit** Exit VLAN configuration mode.
Step 5	**vlan** *vlan-list* Specify Primary VLAN ID, and enter VLAN configuration mode. *vlan-list*: Specify the ID or the ID list of the VLAN(s) for configuration. The ID ranges from 2 to 4094, for example, 2-3,5.
Step 6	**private-vlan {** community **|** isolated **}** Specify the VLAN to be the secondary VLAN, and configure the secondary VLAN type. community: Set the secondary VLAN type as Community. Users in the same isolated VLAN cannot communicate with each other. isolated: Set the secondary VLAN type as Isolated. Users in the same community VLAN can communicate with each other.
Step 7	**exit** Exit VLAN configuration mode.

Step 8	**vlan** *vlan-id* Specify the primary VLAN ID, and enter VLAN configuration mode.
Step 9	**private-vlan association** *vlan-list* Specify the ID or the ID list of the secondary VLAN(s) to pair with this primary VLAN. To avoid long response time of the switch, you are recommended to pair less than 10 secondary VLANs with the primary VLAN at a time. *vlan-list*: Specify the ID or the ID list of the secondary VLAN(s).
Step 10	**show vlan private-vlan** Verify configurations of private VLAN.
Step 11	**end** Return to Privileged EXEC Mode.
Step 12	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create primary VLAN 6 and secondary VLAN 5, set the secondary VLAN type as community, and pair primary VLAN 6 with secondary VLAN 5 as a private VLAN.

Switch#configure

Switch(config)#vlan 6

Switch(config-vlan)#private-vlan primary

Switch(config-vlan)#exit

Switch(config)#vlan 5

Switch(config-vlan)#private-vlan community

Switch(config-vlan)#exit

Switch(config)#vlan 6

Switch(config-vlan)#private-vlan association 5

Switch(config-vlan)#exit

Switch(config)#show vlan private-vlan

Primary	Secondary	Type	Ports
---	---	---	---
6	5	Community	

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Configuring the Up-link Port

The switch requires that only access port can be added to a private VLAN.

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *lag-id* **| range port-channel** *lag-list* **}** Enter interface configuration mode. *port* |*port-list*: The number or the list of the Ethernet port that you want to configure. *lag-id* |*lag-list:* The ID or the list of the LAG that you want to configure.
Step 3	**switchport private-vlan** promiscuous Configure the port type as Promiscuous.
Step 4	**switchport private-vlan mapping** *primary-vlan-id secondary-vlan-id* Add the specified port(s) to the private VLAN. *primary-vlan-id*: Specify the ID of the primary VLAN. The ID ranges from 2 to 4094. *secondary-vlan-id*: Specify the ID of the secondary VLAN. The ID ranges from 2 to 4094.
Step 5	**show vlan private-vlan** Verify configurations of private VLAN.
Step 6	**show vlan private-vlan interface [fastEthernet** *port* **| gigabitEthernet** *port* **| port-channel** *lag-id***]** Verify private VLAN configurations of ports. *port*: Specify the ID of the port to show information. *lag-id*: Specify the ID of the LAG to show information.
Step 7	**end** Return to Privileged EXEC Mode.
Step 8	**copy running-config startup-config** Save the settings in the configuration file.

Note:

When configuring the up-link port, you only need to add the port to one private VLAN and set the port type as Promiscuous. The switch will automatically add the port to private VLANs with the same primary VLAN.

The following example shows how to configure the port type of port 1/0/2 as Promiscuous, and add it to the private VLAN composed of primary VLAN 6 and secondary VLAN 5.

Switch#configure

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

Switch(config-if)#switchport private-vlan promiscuous

Swtich(config-if)#switchport private-vlan mapping 6 5

Switch(config-if)#exit

Switch(config)#show vlan private-vlan

Primary	Secondary	Type	Ports
6	5	Community	Gi1/0/2

Switch(config)#show vlan private-vlan interface gigabitEthernet 1/0/2

Port	type
Gi1/0/2	Promiscuous

Switch(config)#end

Switch#copy running-config startup-config

2.2.3 Configuring the Down-link Port

The switch requires that only access port can be added to a private VLAN.

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *lag-id* **| range port-channel** *lag-list* **}** Enter interface configuration mode. *port* |*port-list*: The number or the list of the Ethernet port that you want to configure. *lag-id* |*lag-list:* The ID or the list of the LAG that you want to configure.
Step 3	**switchport private-vlan** host Configure the port type as host.
Step 4	**switchport private-vlan host-association** *primary-vlan-id secondary-vlan-id vlantype* Add the specified port(s) to the private VLAN. *primary-vlan-id*: Specify the ID of the primary VLAN. The ID ranges from 2 to 4094. *secondary-vlan-id*: Specify the ID of the secondary VLAN. The ID ranges from 2 to 4094. *vlantype*: Specify the secondary VLAN type, either community or isolated.
Step 5	**show vlan private-vlan** Verify configurations of private VLAN.

Step 6	**show vlan private-vlan interface [fastEthernet** *port* **| gigabitEthernet** *port* **| port-channel** *lag-id***]** Verify private VLAN configurations of ports. *port*: Specify the ID of the port to show information. *lag-id*: Specify the ID of the LAG to show information.
Step 7	**end** Return to Privileged EXEC Mode.
Step 8	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the port type of port 1/0/3 as Host, and add it to the private VLAN composed of primary VLAN 6 and secondary VLAN 5.

Switch#configure

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

Switch(config-if)#switchport private-vlan host

Swtich(config-if)#switchport private-vlan host-association 6 5 community

Switch(config-if)#exit

Switch(config)#show vlan private-vlan

Primary	Secondary	Type	Ports
---	---	---	---
6	5	Community	Gi1/0/3

Switch(config)#show vlan private-vlan interface gigabitEthernet 1/0/3

Port	type
---	---
Gi1/0/3	Host

Switch(config)#end

Switch#copy running-config startup-config

3 Configuration Example

3.1 Network Requirements

Usually, an ISP divides its network into subnets to differentiate different areas by using VLAN. Company A belongs to Area VI which is marked as VLAN 6 by the ISP. It is required that departments in Company A can achieve Layer 2 isolation by using VLAN and users in the same department can communicate with each other.

3.2 Configuration Scheme

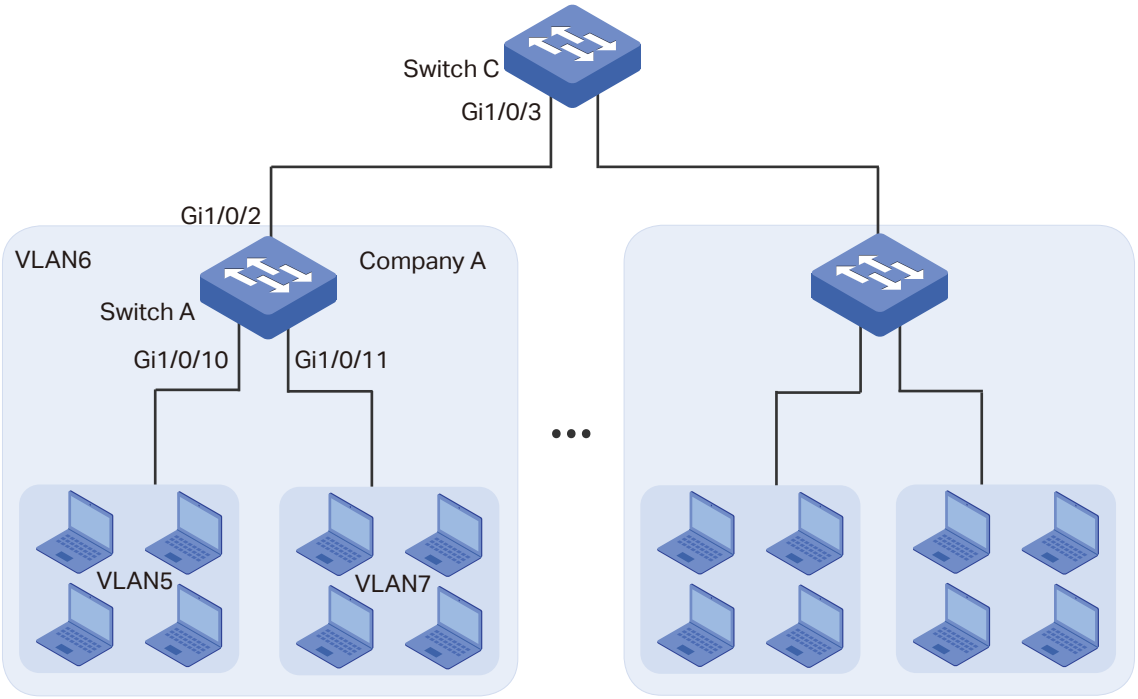
You can create primary VLAN and secondary VLAN and pair them into private VLAN. This allows upper-layer switch to recognize only the primary VLAN instead of all the secondary VLANs. Also, Company A can achieve Layer 2 isolation by using secondary VLAN.

Since it is required that users in the same department can communicate with each other, secondary VLAN type should be configured as Community.

3.3 Network Topology

As shown in the following figure, Switch C is the ISP's central switch, and Switch A is in Company A. To meet the requirement, configure private VLAN on Switch A. This chapter provides configuration procedures in two ways: using the GUI and using the CLI.

Figure 3-1 Network Topology



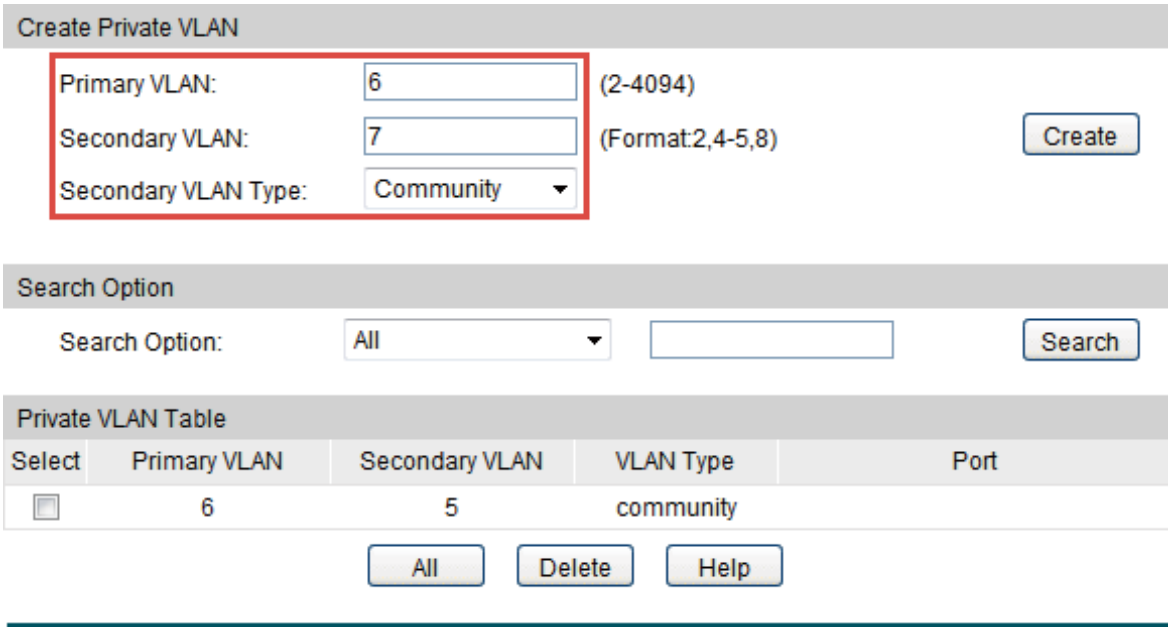
3.4 Using the GUI

- Configurations for Switch A

1) Creating private VLAN

Choose the menu **VLAN** > **Private VLAN** > **PVLAN Config** to load the following page. Create primary VLAN 6 and secondary VLAN 5, select Community as the Secondary VLAN Type, click Create and primary VLAN 6 is paired with secondary VLAN 5. Similarly, create primary VLAN 6 and secondary VLAN 7, select Community as the Secondary VLAN Type, click Create and primary VLAN 6 is paired with secondary VLAN 7.

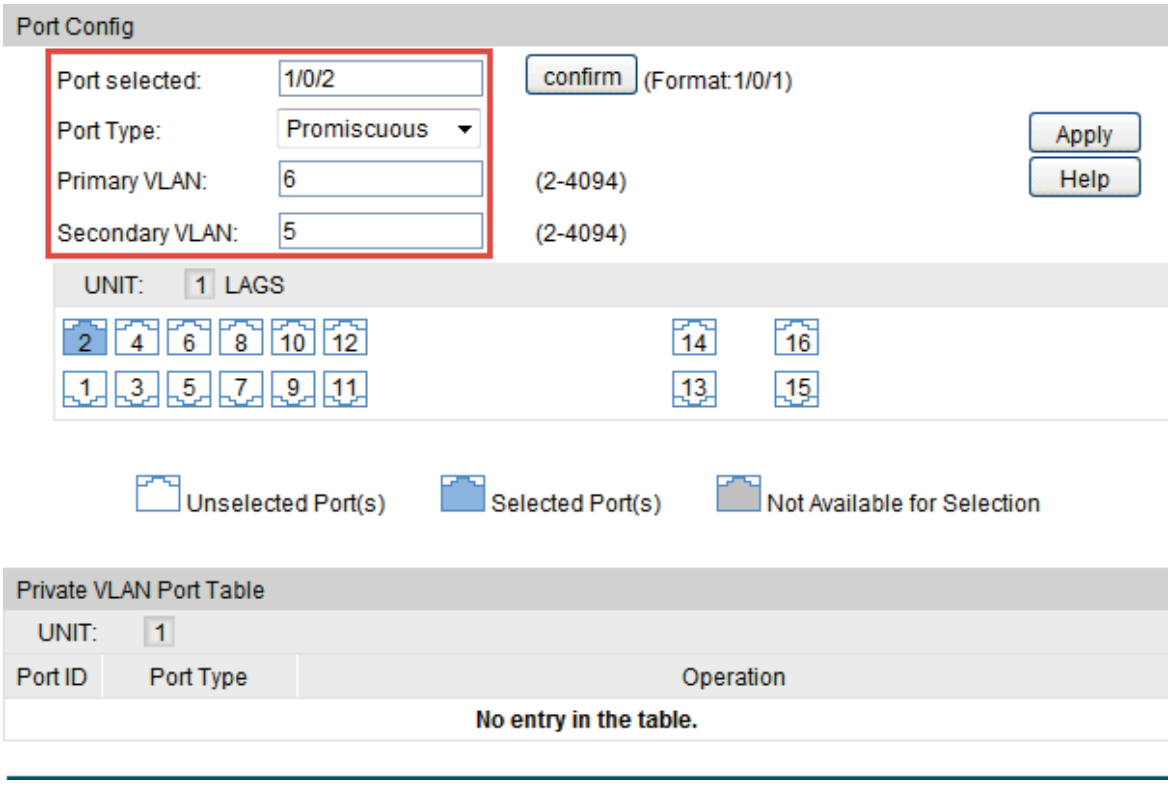
Figure 3-2 Creating Private VLAN



2) Add up-link port to the private VLAN and configure the port type

Choose the menu **VLAN** > **Private VLAN** > **Port Config** to load the following page. Add port 1/0/2 to primary VLAN 6 and secondary VLAN 5, and select Promiscuous as its port type.

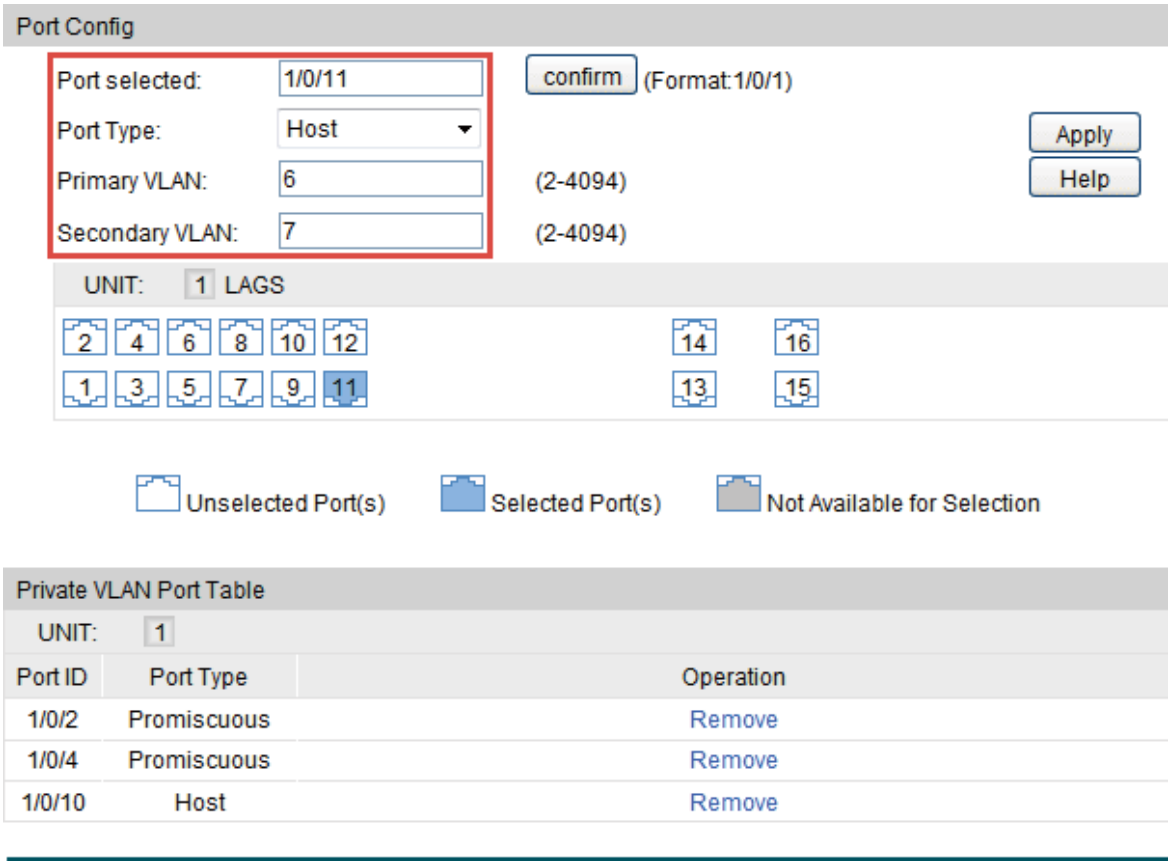
Figure 3-3 Configuring the Up-link Port



3) Add down-link port to the private VLAN and configure the port type

Choose the menu **VLAN** > **Private VLAN** > **Port Config** to load the following page. Add port 1/0/10 to primary VLAN 6 and secondary VLAN 5, add port 1/0/11 to primary VLAN 6 and secondary VLAN 7, and select Host as their port type.

Figure 3-4 Configuring the Down-link Port



3.5 Using the CLI

- Configurations for Switch A

1) Enter global configuration mode

Switch_A>enable

Switch_A#configure

2) Create primary VLAN 6 and secondary VLAN 5, and pair them into a private VLAN

Switch_A(config)#vlan 6

Switch_A(config-vlan)#private-vlan primary

Switch_A(config-vlan)#exit

Switch_A(config)#vlan 5

Switch_A(config-vlan)#private-vlan community

Switch_A(config-vlan)#exit

Switch_A(config)#vlan 6

Switch_A(config-vlan)#private-vlan association 5

Switch_A(config-vlan)#exit

3) Create secondary VLAN 7, and pair it with primary VLAN 6 into a private VLAN

Switch_A(config)#vlan 7

Switch_A(config-vlan)#private-vlan community

Switch_A(config-vlan)#exit

Switch_A(config)#vlan 6

Switch_A(config-vlan)#private-vlan association 7

Switch_A(config-vlan)#exit

4) Add up-link port to the corresponding private VLAN and configure the port type as Promiscuous

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

Switch_A(config-if)#switchport private-vlan promiscuous

Switch_A(config-if)#switchport private-vlan mapping 6 5

Switch_A(config-if)#exit

5) Add down-link port to the corresponding private VLAN and configure the port type as Host

Switch_A(config)#interface gigabitEthernet 1/0/10

Switch_A(config-if)#switchport private-vlan host

Switch_A(config-if)#switchport private-vlan host-association 6 5 community

Switch_A(config-if)#exit

Switch_A(config)#interface gigabitEthernet 1/0/11

Switch_A(config-if)#switchport private-vlan host

Switch_A(config-if)#switchport private-vlan host-association 6 7 community

Switch_A(config-if)#end

Switch_A#copy running-config startup-config

Verify the Configurations

- Switch A

  Verify the configuration of private VLAN:

  Switch_A(config)#show vlan private-vlan

Primary	Secondary	Type	Ports
6	5	Community	Gi1/0/2,1/0/10
6	7	Community	Gi1/0/2,1/0/11

  Verify the configuration of ports:

  Swtich_A(config)#show vlan private-vlan interface

Port	type
Gi1/0/1	Normal
Gi1/0/2	Promiscuous
Gi1/0/3	Normal
Gi1/0/4	Normal
Gi1/0/5	Normal
Gi1/0/6	Normal
Gi1/0/7	Normal
Gi1/0/8	Normal
Gi1/0/9	Normal
Gi1/0/10	Host
Gi1/0/11	Host
Gi1/0/12	Normal

  ...

4 Appendix: Default Parameters

Default settings of Private VLAN are listed in the following tables.

Table 4-1 Default Settings of Private VLAN

Parameter	Default Setting
Primary VLAN	None
Secondary VLAN	None
Secondary VLAN Type	Community

Table 4-2 Default Settings of Port Configuration

Parameter	Default Setting
Port selected	None
Port Type	Promiscuous
Primary VLAN	None
Secondary VLAN	None

Part 15

Configuring Spanning Tree

CHAPTERS

1. Spanning Tree
2. STP/RSTP Configurations
3. MSTP Configurations
4. STP Security Configurations
5. Configuration Example for MSTP
6. Appendix: Default Parameters

1 Spanning Tree

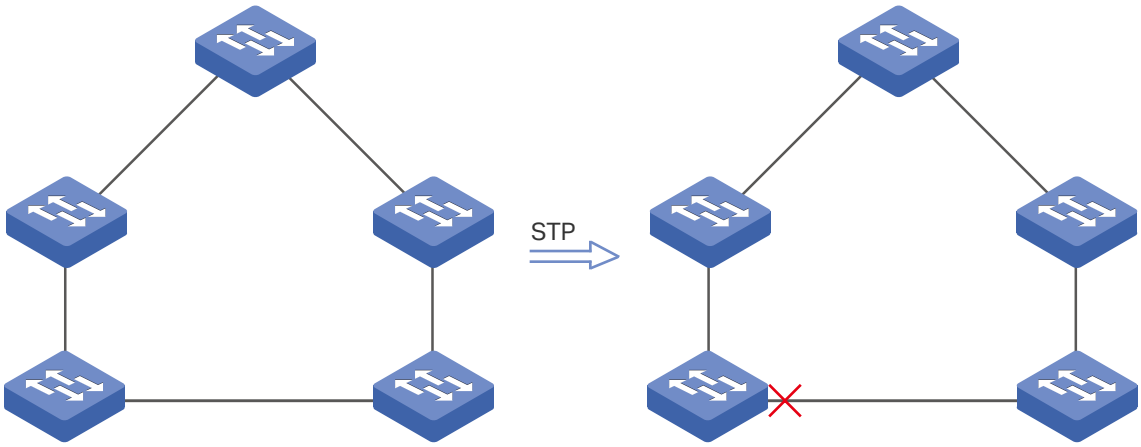
1.1 Overview

STP

STP (Spanning Tree Protocol) is a layer 2 Protocol that prevents loops in the network. As is shown in Figure 1-1, STP helps to:

- Block specified ports of the switches to build a loop-free topology.
- Detect topology changes and automatically generate a loop-free topology.

Figure 1-1 STP Function



RSTP

RSTP (Rapid Spanning Tree Protocol) provides the same features as STP. But RSTP also provides much faster spanning tree convergence.

MSTP

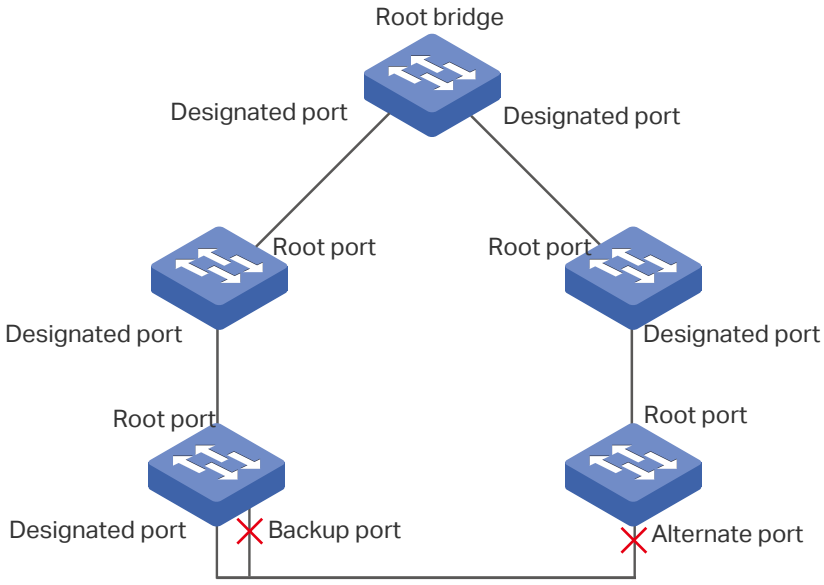
MSTP (Multiple Spanning Tree Protocol) also provides the fast spanning tree convergence as RSTP. In addition, MSTP enables VLANs to be mapped to different spanning trees (MST instances), and traffic in different VLANs will be transmitted along their respective paths, implementing load balancing among VLANs.

1.2 Basic Concepts

1.2.1 STP/RSTP Concepts

Based on the networking topology, this section will introduce some basic concepts in STP/RSTP.

Figure 1-2 STP/RSTP Topology



Root Bridge

The root bridge is the root of a spanning tree. There is only one root bridge in each spanning tree, and the root bridge has the lowest bridge ID.

Bridge ID

The value of the priority and MAC address of the switch. It is used to select the root bridge. The bridge ID is composed of a 2-byte priority and a 6-byte MAC address. The priority is allowed to be configured manually on the switch, and the switch with the lowest priority value will be elected as the root bridge. If the priority of all the switches are the same, the switch with the lowest MAC address is selected as the root bridge.

Port Role

- Root Port

The port selected on non-root bridges to provide the lowest root path cost. There is only one root port in each non-root bridge.

- Designated Port

The port selected for each LAN segment to provide the lowest root path cost from that LAN segment to the root bridge.

- Alternate Port

If a port is not selected as the designated port for it receives better BPDUs from another switch, it will become an alternate port.

In RSTP/MSTP, the alternate port is the backup for the root port. It is blocked when the root port works normally. Once the root port fails, the alternate port will become the new root port.

In STP, the alternate port is always blocked.

- Backup Port

If a port is not selected as the designated port for it receives better BPDUs from the switch it belongs to, it will become an backup port.

In RSTP/MSTP, the backup port is the backup for the designated port. It is blocked when the designated port works normally. Once the root port fails, the backup port will become the new designated port.

In STP, the backup port is always blocked.

- Disable Port

The disconnected port with spanning tree function enabled .

Port Status

Generally, in STP, the port status includes: Blocking, Listening, Learning, Forwarding and Disabled.

- Blocking

In this status, the port receives and sends BPDUs. The other packets are dropped.

- Listening

In this status, the port receives and sends BPDUs. The other packets are dropped.

- Learning

In this status, the port receives and sends BPDUs. It also receives the other user packets to update its MAC address table, but doesn't forward them.

- Forwarding

In this status, the port receives and sends BPDUs. It also receives the other user packets to update its MAC address table, and forwards them.

- Disabled

In this status, the port is not participating in the spanning tree, and drops all the packets it receives.

In RSTP/MSTP, the port status includes: Discarding, Learning and Forwarding. The Discarding status is the grouping of STP's Blocking, Listening and Disabled, and the

Learning and Forwarding status correspond exactly to the Learning and Forwarding status specified in STP.

In TP-Link switches, the port status includes: Blocking, Learning, Forwarding and Disconnected.

- Blocking

In this status, the port receives and sends BPDUs. The other packets are dropped.

- Learning

In this status, the port receives and sends BPDUs. It also receives the other user packets to update its MAC address table, but doesn't forward them.

- Forwarding

In this status, the port receives and sends BPDUs. It also receives the other user packets to update its MAC address table, and forwards them.

- Disconnected

In this status, the port is enabled with spanning tree function but not connected to any device.

Path Cost

The path cost reflects the link speed of the port. The smaller the value, the higher link speed the port has.

The path cost can be manually configured on each port. If not, the path cost values are automatically calculated according to the link speed as shown below:

Table 1-1 The Default Path Cost Value

Link Speed	Path Cost Value
10Mb/s	2,000,000
100Mb/s	200,000
1Gb/s	20,000
10Gb/s	2,000

Root Path Cost

The root path cost is the accumulated path costs from the root bridge to the other switches. When root bridge sends its BPDU, the root path cost value is 0. When a connected switch receives this BPDU, it increments the path cost of its local incoming port. Then it forwards this BPDU to the downstream switch, with the updated root path cost. The value of the accumulated root path cost increases as the BPDU propagates further.

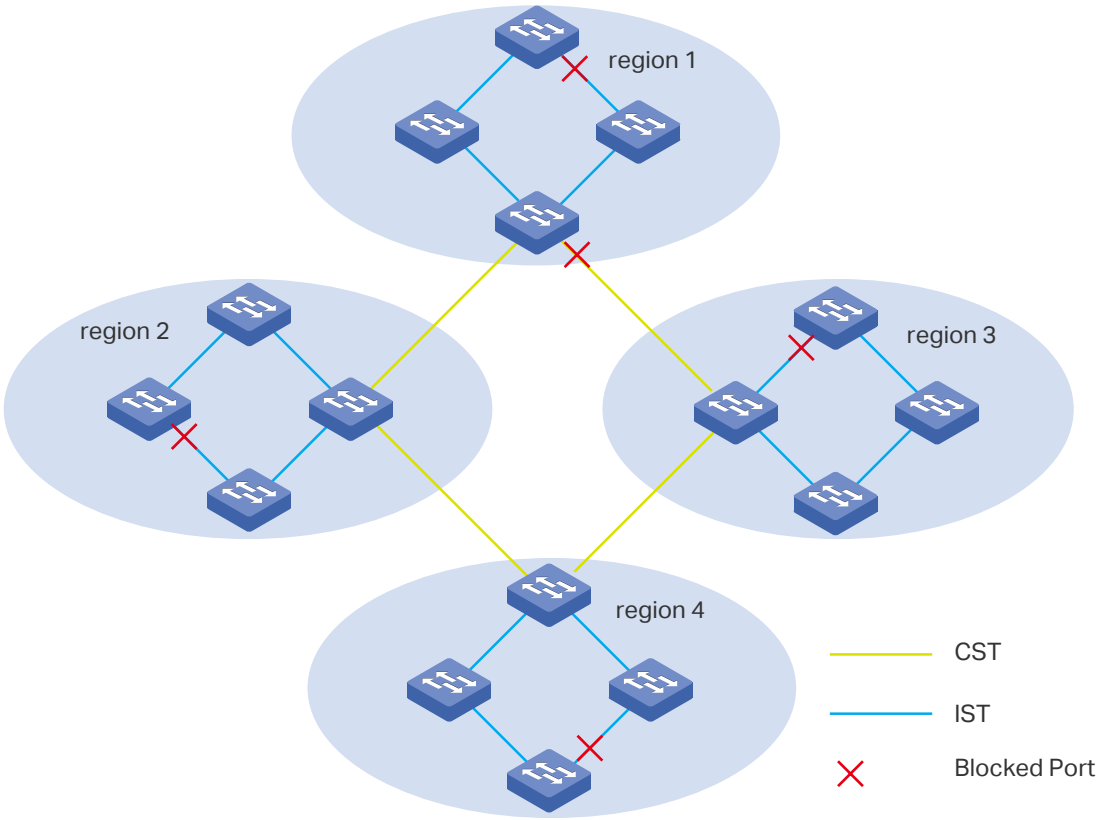
BPDU

The packets used to generate the spanning tree. The BPDUs (Bridge Protocol Data Unit) contain a lot of information, like bridge ID, root path cost, port priority and so on. Switches share these information to help determine the tree topology.

1.2.2 MSTP Concepts

MSTP, compatible with STP and RSTP, has the same basic elements used in STP and RSTP. Based on the networking topology, this section will introduce some concepts only exist in MSTP.

Figure 1-3 MSTP Topology



MST Region

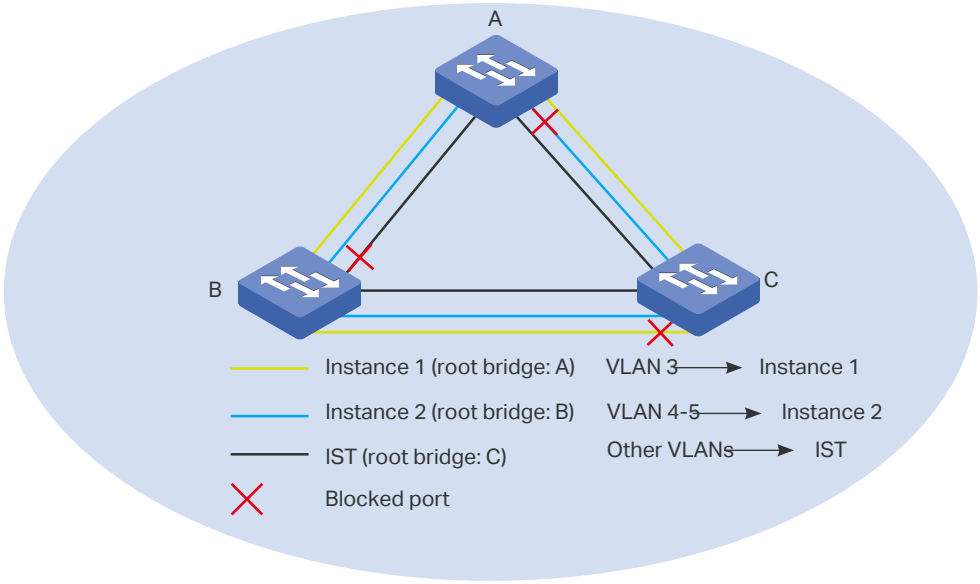
An MST region consists of multiple interconnected switches. The switches that have the following characteristics are considered as in the same region:

- Same region name
- Same revision level
- Same VLAN-Instance mapping

MST Instance

The MST instance is a spanning tree running in the MST region. Multiple MST instances can be established in one MST region and they are independent of each other. As is shown in Figure 1-4, there are three instances in a region, and each instance has its own root bridge.

Figure 1-4 MST Region



VLAN-Instance Mapping

VLAN-Instance Mapping describes the mapping relationship between VLANs and instances. Multiple VLANs can be mapped to a same instance, but one VLAN can be mapped to only one instance. As Figure 1-4 shows, VLAN 3 is mapped to instance 1, VLAN 4 and VLAN 5 are mapped to instance 2, the other VLANs are mapped to the IST.

IST

The Internal Spanning Tree, which is a special MST instance with an instance ID of 0. By default, all the VLANs are mapped to IST.

CST

The Common Spanning Tree, which is the spanning tree connects all MST regions. As is shown in Figure 1-3, region1-region 4 are connected by the CST.

CIST

The Common and Internal Spanning Tree, comprising IST and CST, is the spanning tree that connects all the switches in the network.

1.3 STP Security

STP Security prevents the loops caused by wrong configurations or BPDU attacks. It contains Loop Protect, Root Protect, BPDU Protect, BPDU Filter and TC Protect functions.

» Loop Protect

Loop Protect function is used to prevent loops caused by link congestions or link failures. It is recommended to enable this function on root ports and alternate ports.

If the switch cannot receive BPDUs because of link congestions or link failures, the root port will become a designated port and the alternate port will transit to forwarding status, so loops will occur.

With Loop Protect function enabled, the port will temporarily transit to blocking state when the port does not receive BPDUs. After the link restores to normal, the port will transit to its normal state, so loops can be prevented.

» Root Protect

Root Protect function is used to ensure that the desired root bridge will not lose its position. It is recommended to enable this function on the designated ports of the root bridge.

Generally, the root bridge will lose its position once receiving higher-priority BPDUs caused by wrong configurations or malicious attacks. In this case, the spanning tree will be regenerated, and traffic needed to be forwarded along high-speed links may be lead to low-speed links.

With root protect function enabled, when the port receives higher-priority BDPUs, it will temporarily transit to blocking state. After two times of forward delay, if the port does not receive any higher-priority BDPUs, it will transit to its normal state.

» BPDU Protect

BPDU Protect function is used to prevent the port from receiving BPUDs. It is recommended to enable this function on edge ports.

Normally edge ports do not receive BPDUs, but if a user maliciously attacks the switch by sending BPDUs, the system automatically configures these ports as non-edge ports and regenerates the spanning tree.

With BPDU protect function enabled, the edge port will be shutdown when it receives BPDUs, and reports these cases to the administrator. Only the administrator can restore it.

» BPDU Filter

BPDU filter function is to prevent BPDU flooding in the network. It is recommended to enable this function on edge ports.

If a switch receives malicious BPDUs, it forwards these BPDUs to the other switches in the network, and the spanning tree will be continuously regenerated. In this case, the switch occupies too much CPU or the protocol status of BPDUs is wrong.

With BPDU filter function enabled, the port does not receive or forward BPDUs, but it sends out its own BPDUs, preventing the switch from being attacked by BPDUs.

» TC Protect

TC Protect function is used to prevent the switch from frequently removing MAC address entries. It is recommended to enable this function on the ports of non-root switches.

A switch removes MAC address entries upon receiving TC-BPDUs (the packets used to announce changes in the network topology). If a user maliciously sends a large number of TC-BPDUs to a switch in a short period, the switch will be busy with removing MAC address entries, which may decrease the performance and stability of the network.

With TC protect function enabled, if the number of the received TC-BPDUs exceeds the maximum number you set in the TC threshold, the switch will not remove MAC address entries in the TC protect cycle.

2 STP/RSTP Configurations

To complete the STP/RSTP configuration, follow these steps:

1) Configure STP/RSTP parameters on ports.
2) Configure STP/RSTP globally.
3) Verify the STP/RSTP configurations.

Configuration Guidelines

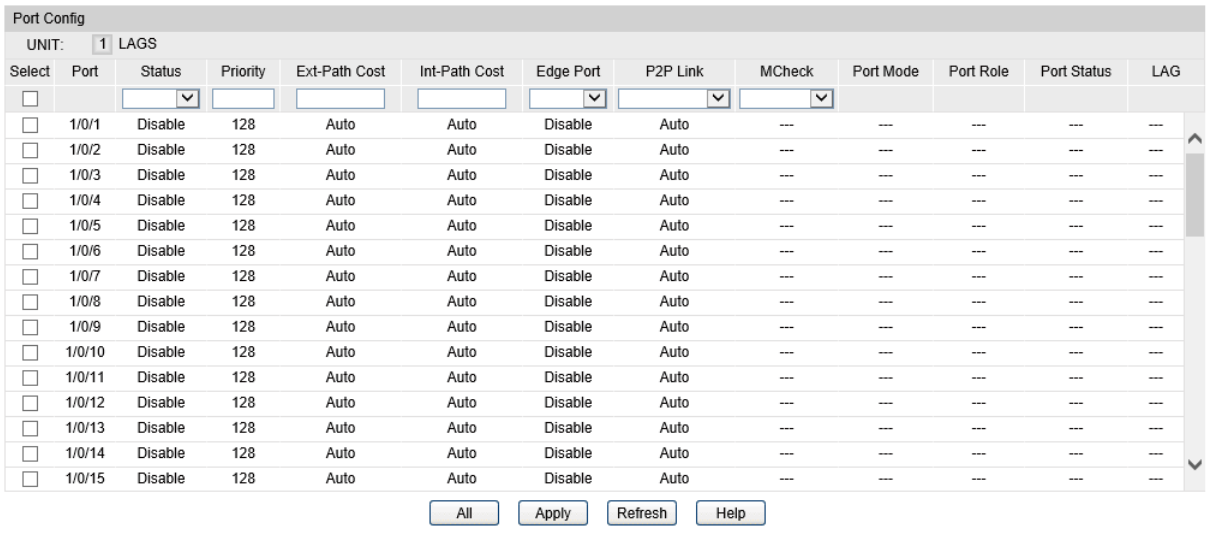
- Before configuring the spanning tree, it's necessary to make clear the role that each switch plays in a spanning tree.
- To avoid any possible network flapping caused by STP/RSTP parameter changes, you are suggested to enable STP/RSTP function globally after configuring the relevant parameters.

2.1 Using the GUI

2.1.1 Configuring STP/RSTP Parameters on Ports

Choose the menu **Spanning Tree > Port Config > Port Config** to load the following page.

Figure 2-1 Configuring STP/RSTP Parameters on Ports



Follow these steps to configure STP/RSTP parameters on ports:

1) In the **Port Config** section, configure STP/RSTP parameters on ports.

UNIT	Select the desired unit or LAGs.

Status	Enable or disable spanning tree function on the desired port.
Priority	Enter the value of the port priority from 0 to 240, which is divisible by 16, and the default value is 128. The port with the lower value has the higher priority. In the same condition, the port with the highest priority will be elected as the root port.
Ext-Path Cost	Enter the value of the external path cost. The default setting is Auto, which means the port calculates the external path cost automatically according to the port's link speed. External path cost is usually a parameter configured in MSTP, which indicates the path cost of the port in CST. In STP/RSTP, external path cost indicates the path cost of the port in the spanning tree. The port with the lowest external root path cost will be elected as the root port.
Int-Path Cost	Enter the value of the internal path cost. Note: Internal path cost is a parameter configured in MSTP. You need not configure it if the spanning tree mode is STP/RSTP.
Edge Port	Enable or disable Edge Port. By default, it is disabled. The edge port can transit its state from blocking to forwarding directly. If the port is connected to an end device, like a PC, it is recommended to set the port as an edge port.
P2P Link	Select the P2P (Point-to-Point) link status. If the two ports in the P2P link are a root port and a designated port, they can transit their states to forwarding directly. Three options are supported: Auto, Open(Force) and Close(Force). By default, it is Auto. **Auto**: The switch automatically checks if the port is connected to a P2P link, then determines the status is Open or Close. **Open(Force)**: The port is manually identified as connected to a P2P link. **Close(Force)**: The port is manually identified as not connected to a P2P link.
MCheck	Select whether to do MCheck operation on the port. Unchange means no MCheck operation. Note: MCheck is configured in MSTP. You need not configure it if the spanning tree mode is STP/RSTP.
Port Mode	Displays the spanning tree mode of the port. **STP**: The spanning tree mode of the port is STP. **RSTP**: The spanning tree mode of the port is RSTP. **MSTP**: The spanning tree mode of the port is MSTP.

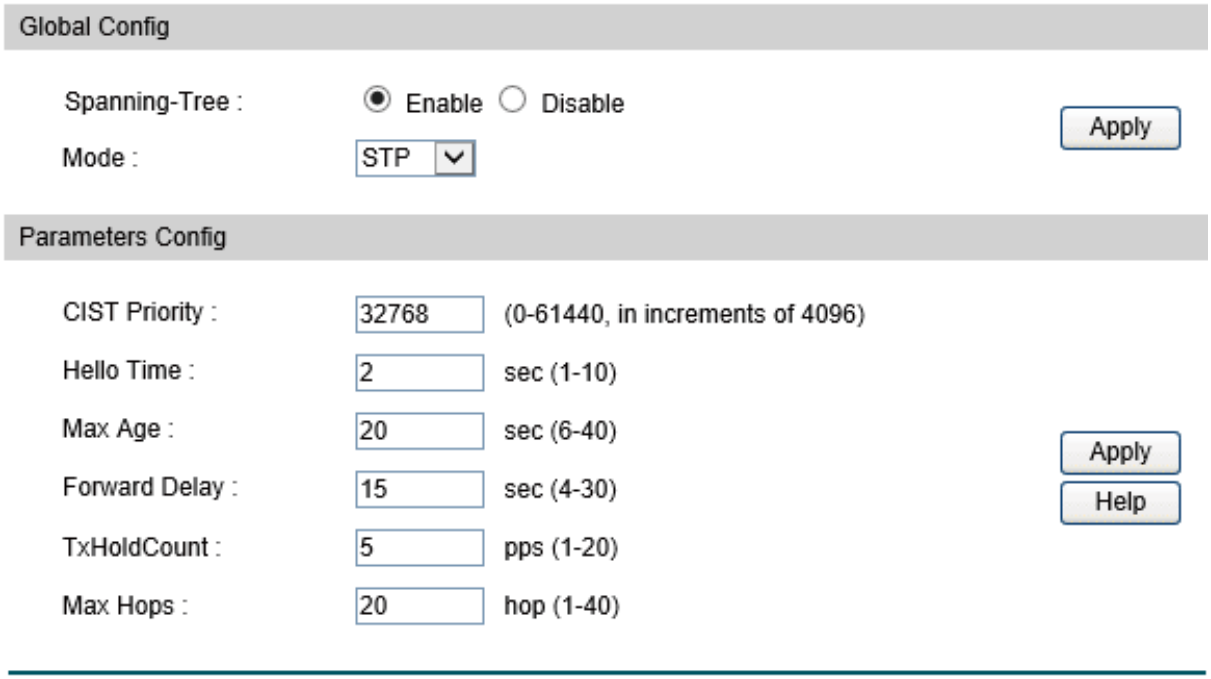
Port Role	Displays the role that the port plays in the spanning tree. **Root Port**: Indicates the port is a root port. **Designated Port**: Indicates the port is a designated port . **Alternate Port**: Indicates the port is a backup of a root port. **Backup Port**: Indicates the port is a backup of a designated port. **Disabled**: Indicates the port is not participating in the spanning tree.
Port Status	Displays the port status. **Forwarding**: The port receives and sends BPDUs, and forwards user data. **Learning**: The port receives and sends BPDUs, and drops the other packets. **Blocking**: The port only receives BPDUs and drops the other packets. **Disconnected**: The port is enabled with spanning tree function but not connected to any device.
LAG	Displays the LAG the port belongs to.

2) Click **Apply**.

2.1.2 Configuring STP/RSTP Globally

Choose the menu **Spanning Tree > STP Config > STP Config** to load the following page.

Figure 2-2 Configuring STP/RSTP Globally



Follow these steps to configure STP/RSTP globally:

1) In the **Parameters Config** section, configure the global parameters of STP/RSTP and click **Apply**.

CIST Priority	Specify the CIST priority of the switch. The valid values are from 0 to 61440, which are divisible by 4096.By default, it is 32768. The switch with the lower value has the higher priority. CIST priority is usually a parameter configured in MSTP, which means the priority of a switch in CIST. The switch with the highest priority will be elected as the root bridge in CIST. In STP/RSTP, CIST priority means the priority of a switch in the spanning tree. The switch with the highest priority is elected as the root bridge.
Hello Time	Specify the interval to send BPDUs. The valid values are from 1 to 10 in seconds, and the default value is 2.
Max Age	Specify the maximum time the switch can wait without receiving a BPDU before attempting to regenerate a spanning tree. The valid values are from 6 to 40 in seconds, and the default value is 20.
Forward Delay	Specify the time for the port to transit its state after the network topology is changed. The valid values are from 4 to 30 in seconds, and the default value is 15.
TxHoldCount	Specify the maximum BPDU transmission rate of a port. The valid values are from 1 to 20, and the default value is 5.
Max Hops	Specify the scale of an MST region. Note: Max Hops is a parameter configured in MSTP. You need not configure it if the spanning tree mode is STP/RSTP.

Note:

To prevent frequent network flapping, make sure that Hello Time, Forward Delay, and Max Age conform to the following formulas:

- 2*(Hello Time + 1) <= Max Age
- 2*(Forward Delay - 1) >= Max Age

2) In the **Global Config** section, enable spanning tree function, choose the STP mode as STP/RSTP, and click **Apply**.

Spanning-Tree	Enable or disable spanning tree function globally on the switch.

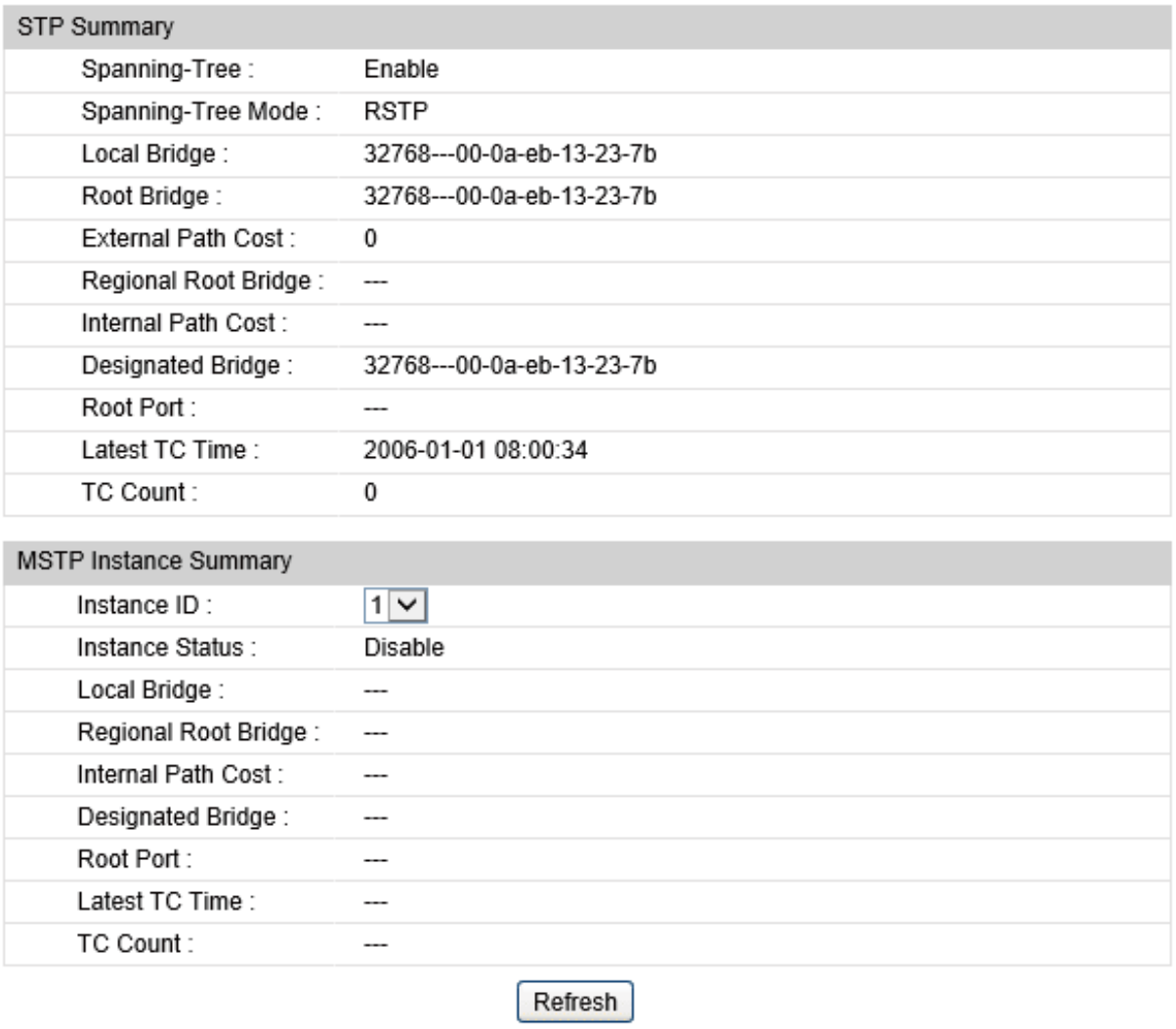
Mode	Select the desired spanning tree mode as STP/RSTP on the switch. By default, it's STP. **STP**: Specify the spanning tree mode as STP. **RSTP**: Specify the spanning tree mode as RSTP. **MSTP**: Specify the spanning tree mode as MSTP.

2.1.3 Verifying the STP/RSTP Configurations

Verify the STP/RSTP information of your switch after all the configurations are finished.

Choose the menu **Spanning Tree > STP Config > STP Summary** to load the following page.

Figure 2-3 Verifying the STP/RSTP Configurations



The **STP Summary** section shows the summary information of spanning tree :

Spanning Tree	Displays the status of the spanning tree function.

Spanning-Tree Mode	Displays the spanning tree mode.
Local Bridge	Displays the bridge ID of the local bridge. The local bridge is the current switch.
Root Bridge	Displays the bridge ID of the root bridge.
External Path Cost	Displays the root path cost from the switch to the root bridge.
Regional Root Bridge	It is the root bridge of IST. It is not displayed when you choose the spanning tree mode as STP/RSTP.
Internal Path Cost	The internal path cost is the root path cost from the switch to the root bridge of IST. It is not displayed when you choose the spanning tree mode as STP/RSTP.
Designated Bridge	Displays the bridge ID of the designated bridge. The designated bridge is the switch that has designated ports.
Root Port	Displays the root port of the current switch.
Latest TC Time	Displays the latest time when the topology is changed.
TC Count	Displays how many times the topology has changed.

2.2 Using the CLI

2.2.1 Configuring STP/RSTP Parameters on Ports

Follow these steps to configure STP/RSTP parameters on ports:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {gigabitEthernet** *port* **| range gigabitEthernet** *port-list***} [port-channel** *port-channel* **| range port-channel** *port-channel-list***}** Enter interface configuration mode.
Step 3	**spanning-tree** Enable spanning tree function for desired ports.

Step 4	**spanning-tree common-config** [**port-priority** *pri*] [**ext-cost** *ext-cost*] [**portfast** { enable | disable }] [**point-to-point** { auto | open | close }] Configure STP/RSTP parameters on the desired port . *pri:* Specify the value of port priority. The valid values are from 0 to 240, which are divisible by 16, and the default value is 128. The port with the lower value has the higher priority. In the same condition, the port with the highest priority will be elected as the root port. *ext-cost:* Specify the value of external path cost. The valid values are from 0 to 2000000. It is 0 by default, which means the path cost is automatically calculated according to the port's link speed. External path cost is usually a parameter configured in MSTP, which indicates the path cost of the port in CST. In STP/RSTP, it indicates the path cost of the port in the spanning tree. The port with the lowest external root path cost will be elected as the root port. **portfast** { enable | disable }*:* Enable or disable the edge Port. By default, it is disabled. The edge port can transit its state from blocking to forwarding directly. If the port is connected to an end device, like a PC, it is recommended to set the port as an edge port. **point-to-point** { auto | open | close }*:* Specify the P2P link status, with auto, open and close options. By default, it is auto. If the two ports in the P2P link are a root port and a designated port, they can transit their states to forwarding directly.
Step 5	**show spanning-tree interface** [**fastEthernet** *port* **| gigabitEthernet** *port* | **port-channel** *lagid*] [**edge** | ext-cost | int-cost | mode | p2p | priority | role | state | status] (Optional) View the information of all ports or a specified port. *port*: Specify the port number. *lagid:* Specify the ID of the LAG. ext-cost | int-cost | mode | p2p | priority | role | state | status: Display the specified information.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable spanning tree function on port 1/0/3 and configure the port priority as 32 :

Switch#configure

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

Switch(config-if)#spanning-tree

Switch(config-if)#spanning-tree common-config port-priority 32

Switch(config-if)#show spanning-tree interface gigabitEthernet 1/0/3

Interface	State	Prio	Ext-Cost	Int-Cost	Edge	P2p	Mode	Role	Status
Gi1/0/3	Enable	32	Auto	Auto	No	No(auto)	N/A	N/A	LnkDwn

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.2 Configuring Global STP/RSTP Parameters

Follow these steps to configure global STP/RSTP parameters of the switch:

Step 1	**configure** Enter global configuration mode.
Step 2	**spanning-tree priority** *pri* Configure the priority of the switch. *pri:* Specify the value of the switch priority from 0 to 61440, which are divisible by 4096. By default, it is 32768. The switch with the lower value has the higher priority, and the switch with the highest priority will be elected as the root bridge.
Step 3	**spanning-tree timer** {[**forward-time** *forward-time*] [**hello-time** *hello-time*] [**max-age** *max-age*]} (Optional) Configure the Forward Delay, Hello Time and Max Age. *forward-time:* Specify the value of Forward Delay. The valid values are from 4 to 30 in seconds, and the default value is 15. Forward Delay is the time for the port to transit its state after the network topology is changed. *hello-time:* Specify the value of Hello Time. The valid values are from 1 to 10 in seconds, and the default value is 2. The root bridge sends configuration BPDUs at an interval of Hello Time to check whether the links are failed. *max-age:* Specify the value of Max Age. The valid values are from 6 to 40 in seconds, and the default value is 20. Max Age is the maximum time the switch can wait without receiving a BPDU before attempting to regenerate a spanning tree.
Step 4	**spanning-tree hold-count** *value* Configure the maximum number of BPDU packets transmitted per Hello Time interval. *value:* Specify the maximum number of BPDU packets transmitted per Hello Time interval. The valid values are from 1 to 20 pps, and the default value is 5.
Step 5	**show spanning-tree bridge** (Optional) View the global STP/RSTP parameters of the switch.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

Note:

To prevent frequent network flapping, make sure that Hello Time, Forward Delay, and Max Age conform to the following formulas:

- 2*(Hello Time + 1) <= Max Age
- 2*(Forward Delay - 1) >= Max Age

This example shows how to configure the priority of the switch as 36864, the Forward Delay as 12 seconds:

Switch#configure

Switch(config)#spanning-tree priority 36864

Switch(config)#spanning-tree timer forward-time 12

Switch(config)#show spanning-tree bridge

State	Mode	Priority	Hello-Time	Fwd-Time	Max-Age	Hold-Count	Max-Hops
Enable	Rstp	36864	2	12	20	5	20

Switch(config)#end

Switch#copy running-config startup-config

2.2.3 Enabling STP/RSTP Globally

Follow these steps to configure the spanning tree mode as STP/RSTP, and enable spanning tree function globally:

Step 1	**configure** Enter global configuration mode.
Step 2	**spanning-tree mode** { stp | rstp } Configure the spanning tree mode as STP/RSTP. *stp*: Specify the spanning tree mode as STP . *rstp:* Specify the spanning tree mode as RSTP .
Step 3	**spanning-tree** Enable spanning tree function globally.
Step 4	**show spanning-tree active** (Optional) View the active information of STP/RSTP.
Step 5	**end** Return to privileged EXEC mode.

Step 6	**copy running-config startup-config** Save the settings in the configuration file.

This example shows how to enable spanning tree function, configure the spanning tree mode as RSTP and verify the configurations:

Switch#configure

Switch(config)#spanning tree mode rstp

Switch(config)#spanning-tree

Switch(config)#show spanning-tree active

Spanning tree is enabled

Spanning-tree's mode: RSTP (802.1w Rapid Spanning Tree Protocol)

Latest topology change time: 2006-01-02 10:04:02

Root Bridge

Priority : 32768

Address : 00-0a-eb-13-12-ba

Local bridge is the root bridge

Designated Bridge

Priority : 32768

Address : 00-0a-eb-13-12-ba

Local Bridge

Priority : 32768

Address : 00-0a-eb-13-12-ba

Interface	State	Prio	Ext-Cost	Int-Cost	Edge	P2p	Mode	Role	Status
---	---	---	---	---	---	---	---	---	---
Gi1/0/16	Enable	128	200000	200000	No	Yes(auto)	Rstp	Desg	Fwd
Gi1/0/18	Enable	128	200000	200000	No	Yes(auto)	Rstp	Desg	Fwd
Gi1/0/20	Enable	128	200000	200000	No	Yes(auto)	Rstp	Desg	Fwd

Switch(config)#end

Switch#copy running-config startup-config

3 MSTP Configurations

To complete the MSTP configuration, follow these steps:

1) Configure parameters on ports in CIST.
2) Configure the MSTP region.
3) Configure the MSTP globally.
4) Verify the MSTP configurations.

Configuration Guidelines

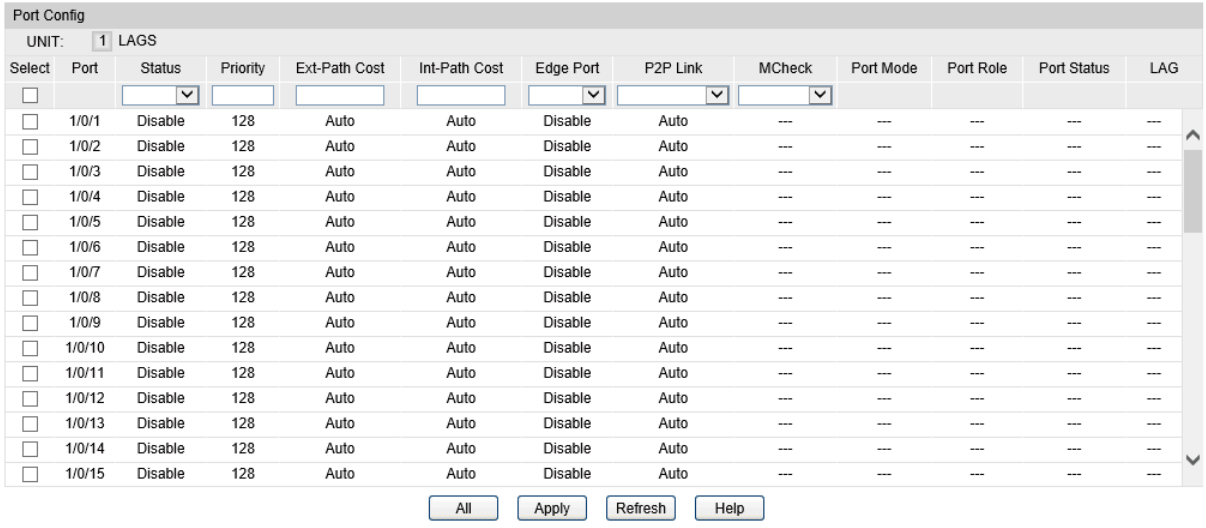
- Before configuring the spanning tree, it's necessary to make clear the role that each switch plays in a spanning tree.
- To avoid any possible network flapping caused by MSTP parameter changes, you are suggested to enable MSTP function globally after configuring the relevant parameter.

3.1 Using the GUI

3.1.1 Configuring Parameters on Ports in CIST

Choose the menu **Spanning Tree > Port Config > Port Config** to load the following page.

Figure 3-1 Configuring the Parameters of the Ports



Follow these steps to configure parameters on ports in CIST:

1) In the **Port Config** section, configure the parameters on ports.

UNIT	Select the desired unit or LAGs.

Status	Enable or disable spanning tree function on the desired port.
Priority	Enter the value of port priority from 0 to 240 divisible by 16, and the default value is 128. The port with the lower value has the higher priority. In the same condition, the port with the highest priority will be elected as the root port in CIST.
Ext-Path Cost	Enter the value of the external path cost. The default setting is Auto, which means the port calculates the path cost automatically according to the port's link speed. External path cost is the path cost of the port in CST. The port with the lowest external root path cost will be elected as the root port in CIST
Int-Path Cost	Enter the value of the internal path cost. The default setting is Auto, which means the port calculates the path cost automatically according to the port's link speed. Internal path cost is the path cost of the port in IST. The port with the lowest internal root path cost will be elected as the root port in IST.
Edge Port	Enable or disable Edge Port. By default, it is disabled. The edge port can transit its state from blocking to forwarding directly. If the port is connected to an end device, like a PC, it is recommended to set the port as an edge port.
P2P Link	Select the P2P link status. If the two ports in the P2P link are a root port and a designated port, they can transit their states to forwarding directly. Three options are supported: Auto, Open(Force) and Close(Force). By default, it is Auto. **Auto**: The switch automatically detects if the port is connected to a P2P link, then determines the status is Open or Close. **Open(Force)**: The port is manually identified as connected to a P2P link. **Close(Force)**: The port is manually identified as not connected to a P2P link.
MCheck	Select whether to do MCheck operation on the port. Unchange means no MCheck operation. If a port on an MSTP-enabled device is connected to a STP/RSTP-enabled device, the port switches to the STP/RSTP compatible mode. If the STP/RSTP-enabled device is powered off or disconnected from the MSTP-enabled device, the port cannot switch back to MSTP mode. In this case, you can switch the port to MSTP mode by enabling MCheck operation.
Port Mode	Displays the spanning tree mode of the port.

Port Role	Displays the role that the port plays in CIST. **Root Port**: Indicates the port is the root port in CIST. **Designated Port**: Indicates the port is the designated port in CIST. **Master Port**: Indicates the port provides the lowest root path cost from the region to the root bridge in CIST. In CIST, each region is regarded as a 'switch', and the master port is the root port of that 'switch'. **Alternate Port**: Indicates the port is a backup of a root or master port in CIST. **Backup Port**: Indicates the port is a backup of a designated port in CIST. **Disabled**: Indicates the port is not participating in the spanning tree in CIST.
Port Status	Displays the port status. **Forwarding**: The port receives and sends BPDUs, and forwards user data. **Learning**: The port receives and sends BPDUs, and drops the other packets. **Blocking**: The port only receives BPDUs and drops the other packets. **Disconnected**: The port is enabled with spanning tree function but not connected to any device.
LAG	Displays the LAG the port belongs to.

2) Click **Apply**.

3.1.2 Configuring the MSTP Region

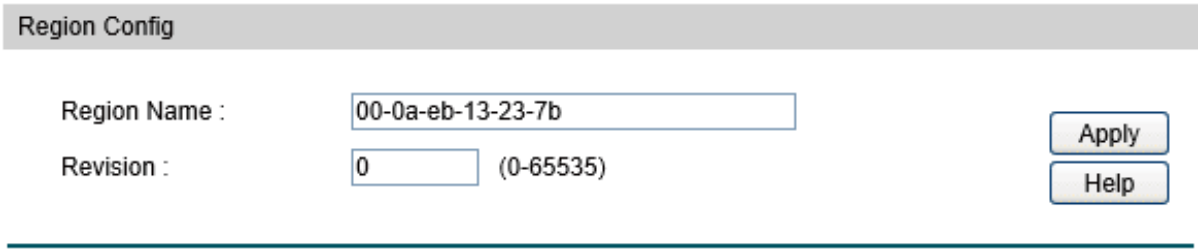
Configure the region name, revision level, VLAN-Instance mapping of the switch. The switches with the same region name, the same revision level and the same VLAN-Instance mapping are considered as in the same region.

Besides, configure the priority of the switch, the priority and path cost of ports in the desired instance.

- Configuring the Region Name and Revision Level

Choose the menu **Spanning Tree > MSTP Instance > Region Config** to load the following page.

Figure 3-2 Configuring the Region



Follow these steps to create an MST region:

1) In the **Region Config** section, set the name and revision level to specify an MSTP region.

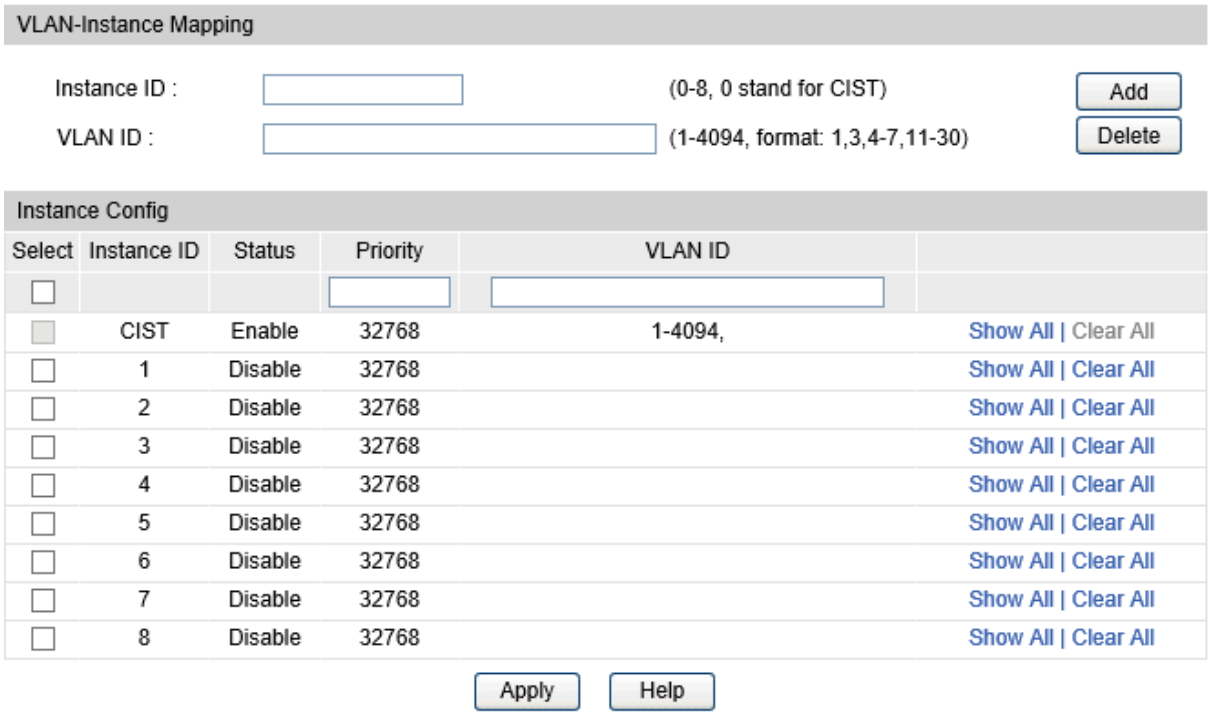
Region Name	Configure the name for an MST region using up to 32 characters. By default, it is the MAC address of the switch.
Revision	Enter the revision number from 0 to 65535. By default, it is 0.

2) Click **Apply**.

Configuring the VLAN-Instance Mapping and Switch Priority

Choose the menu **Spanning Tree > MSTP Instance > Instance Config** to load the following page.

Figure 3-3 Configuring the VLAN-Instance Mapping



Follow these steps to map VLANs to the corresponding instance, and configure the priority of the switch in the desired instance:

1) In the **VLAN-Instance Mapping** section, enter the instance ID and the corresponding VLAN ID, and click **Add.**

Instance ID	Enter the corresponding instance ID.
VLAN ID	Enter the desired VLAN ID. Click **Add**, the VLAN(s) will be added to the corresponding instance and the previous VLAN won't be replaced. Click **Delete**, and the VLAN will be deleted from the corresponding instance.

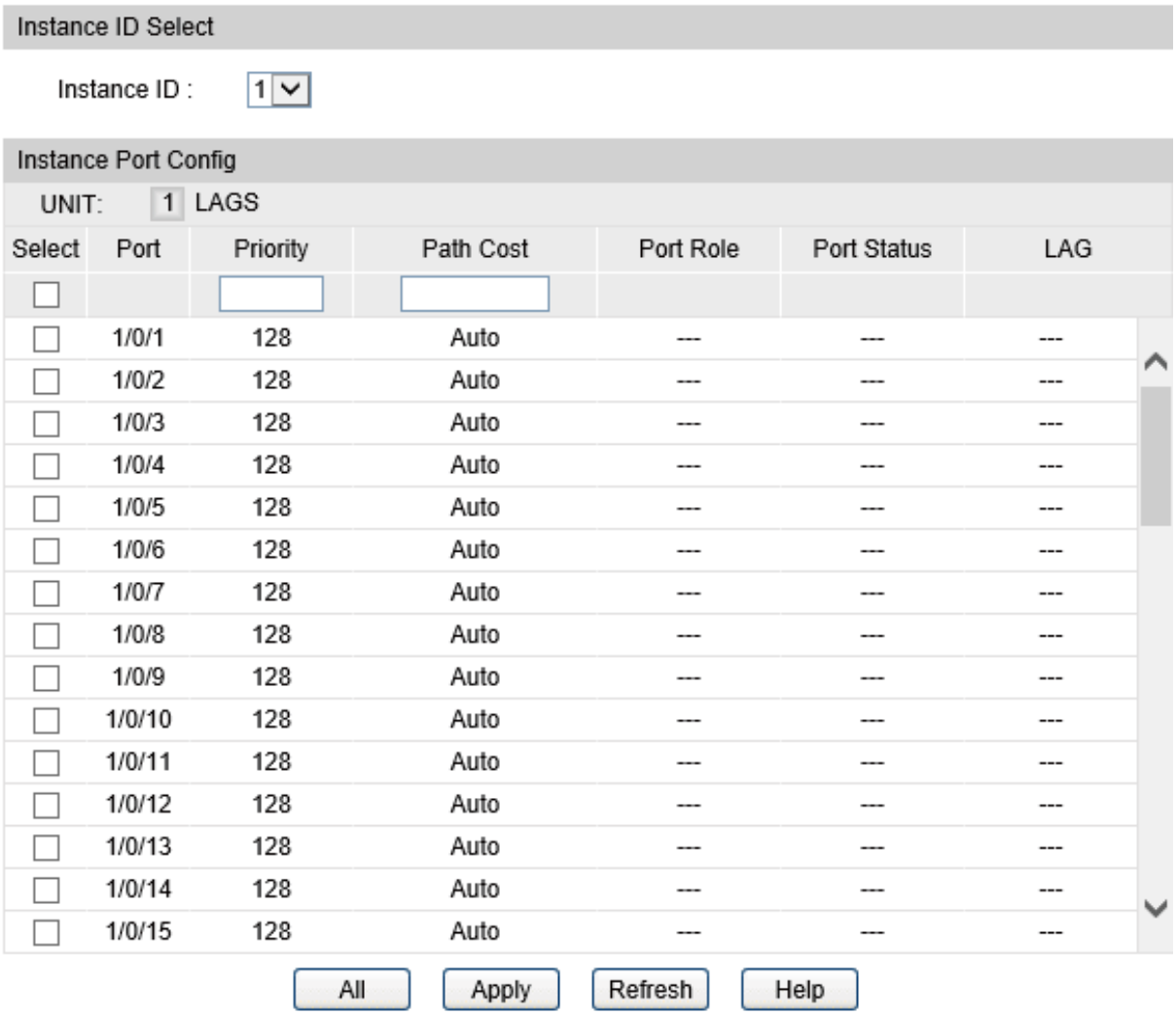
2) In the **Instance Config** section, configure the priority of the switch in the desired instance, and click **Apply.**

Instance ID	Displays the instance ID.
Status	Displays the status of the instance.
Priority	Enter a value from 0 to 61440 to specify the priority of the switch, which is divisible by 4096, and the default value is 32768. The switch with the lower value has the higher priority, and the switch with the highest priority will be elected as the root bridge in the desired instance.
VLAN ID	Enter the VLAN ID mapped to the corresponding instance ID. After the modification, the previous VLAN will be cleared and mapped to the CIST.
Show All	Click the **Show All** to show all VLANs mapped to the instance.
Clear All	Click the **Clear All** to clear up all VLANs from the instance. The cleared VLAN will be automatically mapped to the CIST.

Configuring Parameters on Ports in the Instance

Choose the menu **Spanning Tree > MSTP Instance > Instance Port Config** to load the following page.

Figure 3-4 Configuring Port Parameters in the Instance



Follow these steps to configure port parameters in the instance:

1) In the **Instance ID Select** section, select the desired instance ID for its port configuration.

Instance ID	Select the desired instance.

2) In the **Instance Port Config** section, configure port parameters in the desired instance.

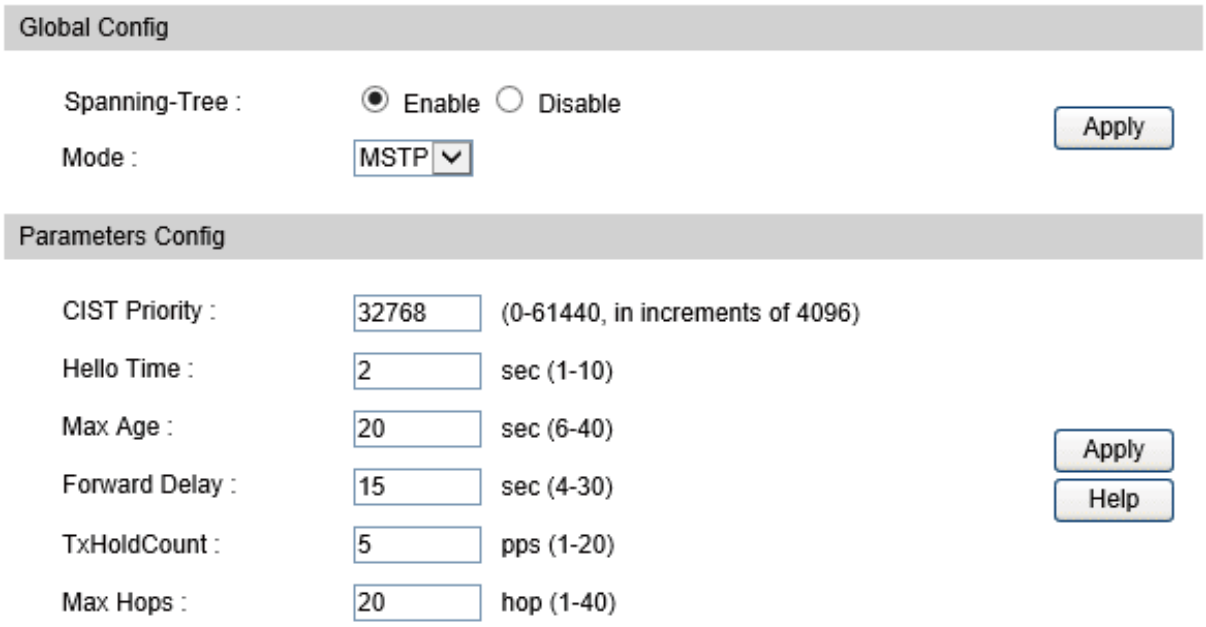
UNIT	Select the desired unit or LAGs for configuration.

Priority	Enter the value of port priority from 0 to 240, which is divisible by 16, and the default value is 128. The port with the lower value has the higher priority. In the same condition, the port with the highest priority will be elected as the root port in the desired instance.
Path Cost	Enter the value of the path cost. The default setting is Auto, which means the port calculates the path cost automatically according to the port's link speed. It is the path cost of the port in the desired instance. The port with the lowest path cost will be elected as the root of the desired instance.
Port Role	Displays the role that the port plays in the desired instance. **Root Port**: Indicates the port is the root port. **Designated Port**: Indicates the port is the designated port . **Alternate Port**: Indicates the port is a backup of a root port. **Backup Port**: Indicates the port is a backup of a designated port. **Disabled**: Indicates the port is not participating in the spanning tree.
Port Status	Displays the port status. **Forwarding**: The port receives and sends BPDUs, and forwards user data. **Learning**: The port receives and sends BPDUs, and drops the other packets. **Blocking**: The port only receives BPDUs and drops the other packets. **Disconnected**: The port is enabled with spanning tree function but not connected to any device.
LAG	Displays the LAG which the port belongs to.

3.1.3 Configuring MSTP Globally

Choose the menu **Spanning Tree > STP Config > STP Config** to load the following page.

Figure 3-5 Configure MSTP Function Globally



Follow these steps to configure MSTP globally:

1) In the **Parameters Config** section, Configure the global parameters of MSTP and click **Apply**.

CIST Priority	Enter a value from 0 to 61440 to specify the CIST priority of the switch, which is divisible by 4096, and the default value is 32768. The switch with the lower value has the higher priority. CIST priority is the priority of a switch in CIST. The switch with the highest priority will be elected as the root bridge.
Hello Time	Specify the interval to send BPDUs. The valid values are from 1 to 10 in seconds, and the default value is 2.
Max Age	Specify the maximum time the switch can wait without receiving a BPDU before attempting to regenerate a spanning tree. The valid values are from 6 to 40 in seconds, and the default value is 20.
Forward Delay	Specify the time for the port to transit its state after the network topology is changed. The valid values are from 4 to 30 in seconds, and the default value is 15.
TxHoldCount	Specify the maximum BPDU transmission rate of a port. The valid values are from 1 to 20, and the default value is 5.
Max Hops	Specify the maximum number of hops that occur in a specific region before the BPDU is discarded. The valid values are from 1 to 40, and the default value is 20.

Note:

To prevent frequent network flapping, make sure that Hello Time, Forward Delay, and Max Age conform to the following formulas:

- 2*(Hello Time + 1) <= Max Age
- 2*(Forward Delay - 1) >= Max Age

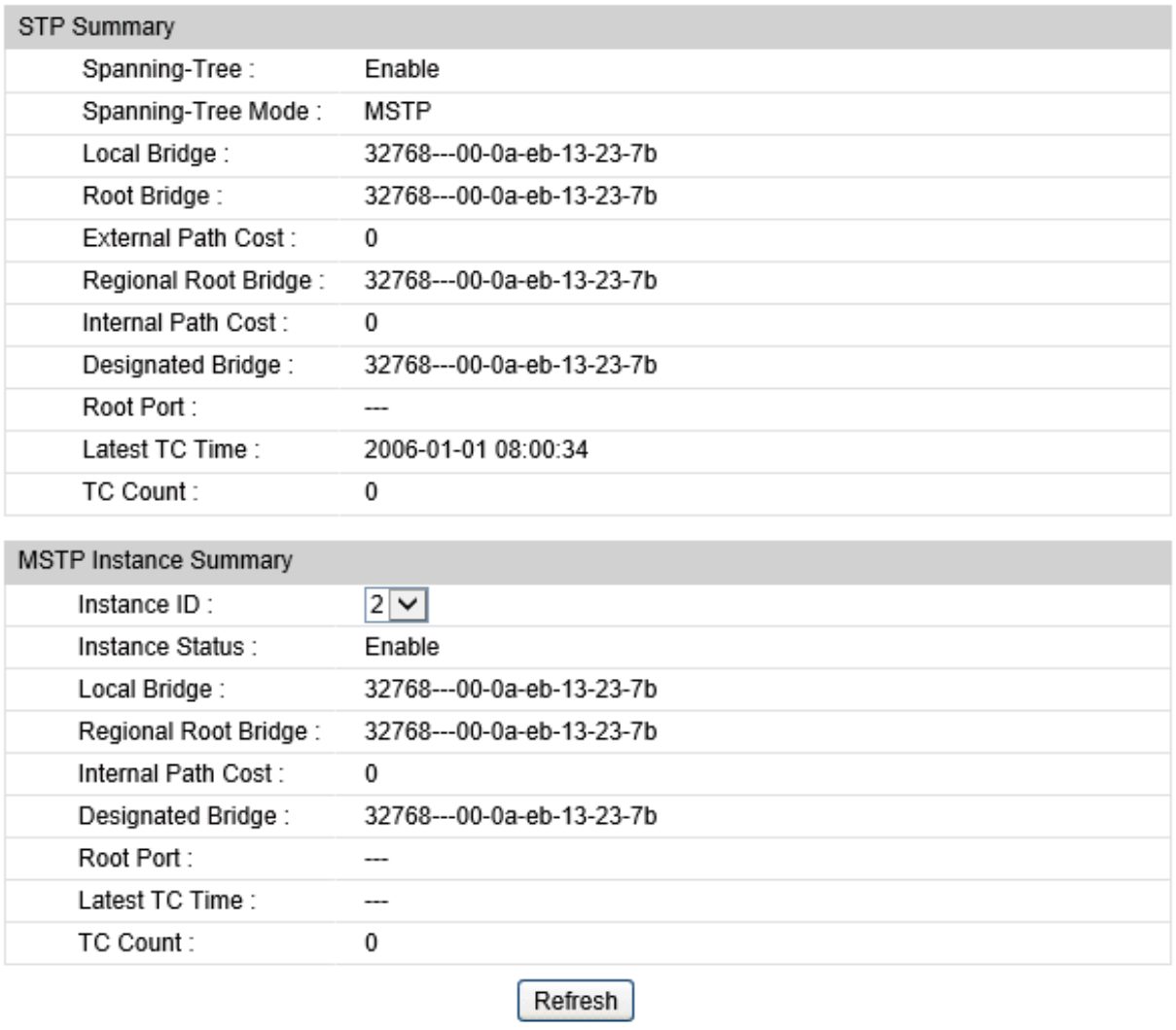
2) In the **Global Config** section, enable Spanning-Tree function and choose the STP mode as MSTP and click **Apply**.

Spanning-Tree	Enable or disable spanning tree function globally on the switch.
Mode	Select the desired STP mode as MSTP on the switch. By default, it is STP. **STP**: Specify the spanning tree mode as STP. **RSTP**: Specify the spanning tree mode as RSTP. **MSTP**: Specify the spanning tree mode as MSTP.

3.1.4 Verifying the MSTP Configurations

Choose the menu **Spanning Tree > STP Config > STP Summary** to load the following page.

Figure 3-6 Verifying the MSTP Configurations



The **STP Summary** section shows the summary information of CIST:

Spanning Tree	Displays the status of the spanning tree function.
Spanning-Tree Mode	Displays the spanning tree mode.
Local Bridge	Displays the bridge ID of the local switch. The local bridge is the current switch.
Root Bridge	Displays the bridge ID of the root bridge in CIST.
External Path Cost	Displays the external path cost. It is the root path cost from the switch to the root bridge in CIST.
Regional Root Bridge	Displays the bridge ID of the root bridge in IST.

Internal Path Cost	Displays the internal path cost. It is the root path cost from the current switch to the root bridge in IST.
Designated Bridge	Displays the bridge ID of the designated bridge in CIST.
Root Port	Displays the root port of in CIST.
Latest TC Time	Displays the latest time when the topology is changed.
TC Count	Displays how many times the topology has changed.

The **MSTP Summary** section shows the information in MST instances:

Instance ID	Select the desired instance.
Instance Status	Displays the status of the desired instance.
Local Bridge	Displays the bridge ID of the local switch. The local bridge is the current switch.
Regional Root Bridge	Displays the bridge ID of the root bridge in the desired instance.
Internal Path Cost	Displays the internal path cost. It is the root path cost from the current switch to the regional root bridge.
Designated Bridge	Displays the bridge ID of the designated bridge in the desired instance.
Root Port	Displays the root port of the desired instance.
Latest TC Time	Displays the latest time when the topology is changed.
TC Count	Displays how many times the topology has changed.

3.2 Using the CLI

3.2.1 Configuring Parameters on Ports in CIST

Follow these steps to configure the parameters of the port in CIST:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { gigabitEthernet** *port* **| range gigabitEthernet** *port-list*] **[port-channel** *port-channel* **| range port-channel** *port-channel-list* **}** Enter interface configuration mode.
Step 3	**spanning-tree** Enable spanning tree function for the desired port.

Step 4	**spanning-tree common-config** [**port-priority** *pri*] [**ext-cost** *ext-cost*] [**int-cost** *int-cost*][**portfast** { enable | disable }] [**point-to-point** { auto | open | close }] Configure the parameters on ports in CIST. *pri:* Specify the value of port priority. The valid values are from 0 to 240, which are divisible by 16, and the default value is 128. The port with the lower value has the higher priority. In the same condition, the port with the highest priority will be elected as the root port in CIST. *ext-cost:* Specify the value of external path cost. The valid values are from 0 to 2000000. It is 0 by default, which means the path cost is automatically calculated according to the port's link speed. External path cost is the path cost of the port in CST. The port with the lowest external root path cost will be elected as the root port in CIST. *int-cost:* Specify the value of internal path cost. The valid values are from 0 to 2000000. It is 0 by default, which means the path cost is automatically calculated according to the port's link speed. Internal path cost is the path cost of the port in IST. The port with the lowest internal root path cost will be elected as the root port in IST. **portfast** { enable | disable }*:* Enable or disable edge Port. By default, it is disabled. The edge port can transit its state from blocking to forwarding directly. If the port is connected to an end device, like a PC, it is recommended to set the port as an edge port. **point-to-point** { auto | open | close }*:* Specify the P2P link status, with auto, open and close options. By default, the option is auto. If the two ports in the P2P link are a root port and a designated port, they can transit their states to forwarding directly.
Step 5	**spanning-tree mcheck** (Optional) Select whether to do MCheck operation on the port. If a port on an MSTP-enabled device is connected to an STP-enabled device, the port switches to the STP compatible mode. If the STP-enabled device is powered off or disconnected from the MSTP-enabled device, the port cannot switch back to MSTP mode. In this case, you can switch the port to MSTP mode by MCheck operation.
Step 6	**show spanning-tree interface** [**fastEthernet** *port* | **gigabitEthernet** *port* | **port-channel** *lagid*] [**edge** | ext-cost | int-cost | mode | p2p | priority | role | state | status] (Optional) View the information of all ports or a specified port. *port*: Specify the port number. *lagid*: Specify the ID of the LAG. ext-cost | int-cost | mode | p2p | priority | role | state | status: Display the specified information.
Step 7	**end** Return to privileged EXEC mode.
Step 8	**copy running-config startup-config** Save the settings in the configuration file.

This example shows how to enable spanning tree function for port 1/0/3 and configure the port priority as 32 :

Switch#configure

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

Switch(config-if)#spanning-tree

Switch(config-if)#spanning-tree common-config port-priority 32

Switch(config-if)#show spanning-tree interface gigabitEthernet 1/0/3

MST-Instance 0 (CIST)

Interface	State	Prio	Ext-Cost	Int-Cost	Edge	P2p	Mode	Role	Status
Gi1/0/3	Enable	32	Auto	Auto	No	No(auto)	N/A	N/A	LnkDwn

MST-Instance 5

Interface	Prio	Cost	Role	Status
Gi1/0/3	144	200	N/A	LnkDwn

Switch(config-if)#end

Switch#copy running-config startup-config

3.2.2 Configuring the MSTP Region

- Configuring the MST Region

Follow these steps to configure the MST region and the priority of the switch in the instance:

Step 1	**configure** Enter global configuration mode.
Step 2	**spanning-tree mst instance** *instance-id* **priority** *pri* Configure the priority of the switch in the instance. *instance-id*: Specify the instance ID, the valid values ranges from 1 to 8. *pri*: Specify the priority of the switch. The valid values are from 0 to 61440, which are divisible by 4096, and the default value is 32768. The switch with the lower value has the higher priority, and the switch with the highest priority will be elected as the root bridge in the desired instance.
Step 3	**spanning-tree mst configuration** Enter MST configuration mode, as to configure the VLAN-Instance mapping, region name and revision level.

Step 4	**name** *name* Configure the region name of the region. *name*: Specify the region name, used to identify an MST region. The valid values are from 1 to 32 characters.
Step 5	**revision** *revision* Configure the revision level of the region. *revision:* Specify the revision level of the region. The valid values are from 0 to 65535.
Step 6	**instance** *instance-id* **vlan** *vlan-id* Configure the VLAN-Instance mapping. *instance-id*: Specify the Instance ID. The valid values are from 1 to 8. *vlan-id*: Specify the VLAN mapped to the corresponding instance.
Step 7	**show spanning-tree mst** { **configuration** [digest] | **instance** *instance-id* [**interface** [**fastEthernet** *port* | **gigabitEthernet** *port* | **port-channel** *lagid*]] } (Optional) View the related information of MSTP Instance. *digest*: Display digest calculated by instance-vlan map. *instance-id*: Specify the Instance ID desired to view, ranging from 1 to 8. *port*: Specify the port number. *lagid*: Specify the ID of the LAG.
Step 8	**end** Return to privileged EXEC mode.
Step 9	**copy running-config startup-config** Save the settings in the configuration file.

This example shows how to create an MST region, of which the region name is R1, the revision level is 100 and VLAN 2-VLAN 6 are mapped to instance 5:

Switch#configure

Switch(config)#spanning-tree mst configuration

Switch(config-mst)#name R1

Switch(config-mst)#revision 100

Switch(config-mst)#instance 5 **vlan** 2-6

Switch(config-mst)#show spanning-tree mst configuration

Region-Name : R1

Revision : 100

```
MST-Instance        Vlans-Mapped
---------------     ------------------------------------------------------
0                   1,7-4094
5                   2-6,
---------------------------------------------------------------------------
```

Switch(config-mst)#end

Switch#copy running-config startup-config

■ Configuring the Parameters on Ports in Instance

Follow these steps to configure the priority and path cost of ports in the specified instance:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {gigabitEthernet** *port* **| range gigabitEthernet** *port-list***} {port-channel** *port-channel* **| range port-channel** *port-channel-list***}** Enter interface configuration mode.
Step 3	**spanning-tree mst instance** *instance-id* **{[port-priority** *pri* **] | [cost** *cost* **]}** Configure the priority and path cost of ports in the specified instance. *instance-id:* Specify the instance ID, the valid values ranges from 1 to 8. *pri:* Specify the priority of the port. The valid values are from 0 to 240, which are divisible by 16, and the default value is 128. The port with the lower value has the higher priority. In the same condition, the port with the highest priority will be elected as the root port in the desired instance. *cost:* Specify the path cost of the port. The valid values are from 0 to 2000000. By default, it is 0, which means the port calculates the path cost automatically according to the port's link speed. It is the root path cost from the port to the root bridge in the specified instance. The port with the lowest path cost will be elected as the root port in the desired instance.
Step 4	**show spanning-tree mst** { **configuration** [digest] | **instance** *instance-id* [**interface** [**fastEthernet** *port* | **gigabitEthernet** *port* | **port-channel** *lagid*]] } (Optional) View the related information of MSTP Instance. *digest:* Display digest calculated by instance-vlan map. *instance-id:* Specify the Instance ID desired to view, ranging from 1 to 8. *port:* Specify the port number. *lagid:* Specify the ID of the LAG.
Step 5	**end** Return to privileged EXEC mode.

Step 6	**copy running-config startup-config** Save the settings in the configuration file.

This example shows how to configure the priority as 144, the path cost as 200 of port 1/0/3 in instance 5:

Switch#configure

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

Switch(config-if)#spanning-tree mst instance 5 **port-priority** 144 **cost** 200

Switch(config-if)#show spanning-tree interface gigabitEthernet 1/0/3

MST-Instance 0 (CIST)

Interface	State	Prio	Ext-Cost	Int-Cost	Edge	P2p	Mode	Role	Status
Gi1/0/3	Enable	32	Auto	Auto	No	No(auto)	N/A	N/A	LnkDwn

MST-Instance 5

Interface	Prio	Cost	Role	Status
Gi1/0/3	144	200	N/A	LnkDwn

Switch(config-if)#end

Switch#copy running-config startup-config

3.2.3 Configuring Global MSTP Parameters

Follow these steps to configure the global MSTP parameters of the switch:

Step 1	**configure** Enter global configuration mode.
Step 2	**spanning-tree priority** *pri* Configure the priority of the switch for comparison in CIST. *pri:* Specify the CIST priority of the switch. The valid values are from 0 to 61440, which are divisible by 4096, and the default value is 32768. The switch with the lower value has the higher priority. CIST priority the priority of a switch in CIST. The switch with the highest priority will be elected as the root bridge in CIST.

Step 3	**spanning-tree timer** {[**forward-time** *forward-time*] [**hello-time** *hello-time*] [**max-age** *max-age*]} (Optional) Configure the Forward Delay, Hello Time and Max Age. *forward-time:* Specify the value of Forward Delay. The valid values are from 4 to 30 in seconds, and the default value is 15. Forward Delay is the time for the port to transit its state after the network topology is changed. *hello-time:* Specify the value of Hello Time. The valid values are from 1 to 10 in seconds, and the default value is 2. The root bridge sends configuration BPDUs at an interval of Hello Time to check whether the links are failed. *max-age:* Specify the value of Max Age. The valid values are from 6 to 40 in seconds, and the default value is 20. Max Age is the maximum time the switch can wait without receiving a BPDU before attempting to regenerate a spanning tree.
Step 4	**spanning-tree hold-count** *value* (Optional) Configure the maximum number of BPDU packets transmitted per Hello Time interval. *value:* Specify the maximum number of BPDU packets transmitted per Hello Time interval. The valid values are from 1 to 20 pps, and the default value is 5.
Step 5	**spanning-tree max-hops** *value* (Optional) Configure the maximum number of hops that occur in a specific region before the BPDU is discarded. *value:* Specify the maximum number of hops that occur in a specific region before the BPDU is discarded. The valid values are from 1 to 40 in hop, and the default value is 20.
Step 6	**show spanning-tree bridge** (Optional) View the global parameters of the switch.
Step 7	**end** Return to privileged EXEC mode.
Step 8	**copy running-config startup-config** Save the settings in the configuration file.

Note:

To prevent frequent network flapping, make sure that Hello Time, Forward Delay, and Max Age conform to the following formulas:

- 2*(Hello Time + 1) <= Max Age
- 2*(Forward Delay - 1) >= Max Age

This example shows how to configure the CIST priority as 36864, the Forward Delay as 12 seconds, the Hold Count as 8 and the Max Hop as 25:

Switch#configure

Switch(config)#spanning-tree priority 36864

Switch(config-if)#spanning-tree timer forward-time 12

Switch(config-if)#spanning-tree hold-count 8

Switch(config-if)#spanning-tree max-hops 25

Switch(config-if)#show spanning-tree bridge

State	Mode	Priority	Hello-Time	Fwd-Time	Max-Age	Hold-Count	Max-Hops
Enable	Mstp	36864	2	12	20	8	25

Switch(config-if)#end

Switch#copy running-config startup-config

3.2.4 Enabling Spanning Tree Globally

Follow these steps to configure the spanning tree mode as MSTP and enable spanning tree function globally:

Step 1	**configure** Enter global configuration mode.
Step 2	**spanning-tree mode** mstp Configure the spanning tree mode as MSTP. *mstp:* Specify the spanning tree mode as MSTP.
Step 3	**spanning-tree** Enable spanning tree function globally.
Step 4	**show spanning-tree active** (Optional) View the active information of MSTP.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

This example shows how to configure the spanning tree mode as MSTP and enable spanning tree function globally :

Switch#configure

Switch(config)#spanning-tree mode mstp

Switch(config)#spanning-tree

Switch(config)#show spanning-tree active

Spanning tree is enabled

Spanning-tree's mode: MSTP (802.1s Multiple Spanning Tree Protocol)

Latest topology change time: 2006-01-04 10:47:42

MST-Instance 0 (CIST)

Root Bridge

Priority : 32768

Address : 00-0a-eb-13-23-97

External Cost : 200000

Root Port : Gi/0/20

Designated Bridge

Priority : 32768

Address : 00-0a-eb-13-23-97

Regional Root Bridge

Priority : 36864

Address : 00-0a-eb-13-12-ba

Local bridge is the regional root bridge

Local Bridge

Priority : 36864

Address : 00-0a-eb-13-12-ba

Interface	State	Prio	Ext-Cost	Int-Cost	Edge	P2p	Mode	Role	Status
Gi/0/16	Enable	128	200000	200000	No	Yes(auto)	Mstp	Altn	Blk
Gi/0/20	Enable	128	200000	200000	No	Yes(auto)	Mstp	Root	Fwd

MST-Instance 1

Root Bridge

Priority : 32768

Address : 00-0a-eb-13-12-ba

Local bridge is the root bridge

Designated Bridge

Priority : 32768

Address : 00-0a-eb-13-12-ba

Local Bridge

Priority : 32768

Address : 00-0a-eb-13-12-ba

Interface	Prio	Cost	Role	Status
Gi/0/16	128	200000	Altn	Blk
Gi/0/20	128	200000	Mstr	Fwd

Switch(config)#end

Switch#copy running-config startup-config

4 STP Security Configurations

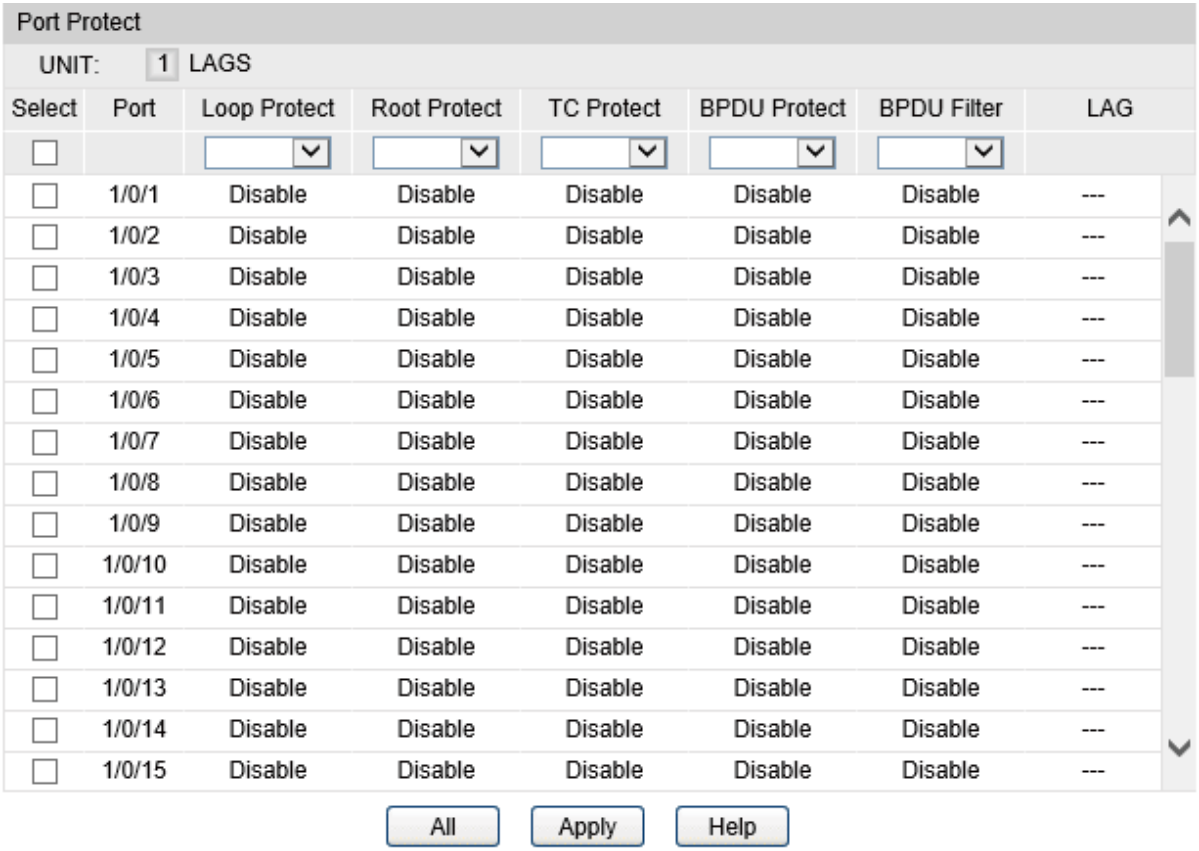
With STP security, you can:

- Configure the Loop Protect function.
- Configure the Root Protect function.
- Configure the TC Protect function.
- Configure the BPDU Protect function.
- Configure the BPDU Filter function.

4.1 Using the GUI

Choose the menu **Spanning Tree > STP Security > Port Protect** to load the following page.

Figure 4-1 Configuring the Port Protect



Configure the Port Protect features for the selected ports, and click **Apply**.

UNIT	Select the desired unit or LAGs for configuration.

Loop Protect	Enable or disable the Loop Protect function. It is recommended to enable this function on root ports and alternate ports. Loop Protect function is used to prevent loops caused by link congestions or link failures. With Loop Protect function enabled, the port will temporarily transit to blocking state when it does not receive BPDUs. After the link restores to normal, the port will transit to its normal state, so loops can be prevented.
Root Protect	Enable or disable the Root Protect function. It is recommended to enable this function on the designated ports of the root bridge. Root Protect function is used to ensure that the desired root bridge will not lose its position. With root protect function enabled, the port will temporarily transit to blocking state when it receives higher-priority BDPUs. After two times of forward delay, if the port does not receive any higher-priority BDPUs, it will transit to its normal state.
TC Protect	Enable or disable the TC Protect function. It is It is recommended to enable this function on the ports of non-root switches. TC Protect function is used to prevent the switch from frequently removing MAC address entries. With TC protect function enabled, if the number of the received TC-BPDUs exceeds the maximum number you set in the TC threshold, the switch will not remove MAC address entries in the TC protect cycle.
BPDU Protect	Enable or disable the BPDU Protect function. It is It is recommended to enable this function on edge ports. BPDU Protect function is used to prevent the edge port from receiving BPUDs. With BPDU protect function enabled, the edge port will be shutdown when it receives BPDUs, and reports these cases to the administrator. Only the administrator can restore it.
BPDU Filter	Enable or disable the BPDU Filter function. It is It is recommended to enable this function on edge ports. BPDU filter function is to prevent BPDU flooding in the network. With BPDU filter function enabled, the port does not receive or forward BPDUs, but it sends out its own BPDUs, preventing the switch from being attacked by BPDUs.

4.2 Using the CLI

Follow these steps to configure the Root protect feature, BPDU protect feature and BPDU filter feature for ports:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {gigabitEthernet** *port* **| range gigabitEthernet** *port-list***} [port-channel** *port-channel* **| range port-channel** *port-channel-list***}** Enter interface configuration mode.

Step 3	**spanning-tree guard loop** (Optional) Enable the Loop Protect feature on the port. t is recommended to enable this function on root ports and alternate ports. Loop Protect function is used to prevent loops caused by link congestions or link failures. With Loop Protect function enabled, the port will temporarily transit to blocking state when it does not receive BPDUs. After the link restores to normal, the port will transit to its normal state, so loops can be prevented.
Step 4	**spanning-tree guard root** (Optional) Enable the Root Protect function on the port. It is recommended to enable this function on the designated ports of the root bridge. Root Protect function is used to ensure that the desired root bridge will not lose its position. With root protect function enabled, the port will temporarily transit to blocking state when it receives higher-priority BDPUs. After two times of forward delay, if the port does not receive any higher-priority BDPUs, it will transit to its normal state.
Step 5	**spanning-tree bpdufilter** (Optional) Enable the BPDU Filter function on the port. It is It is recommended to enable this function on edge ports. BPDU filter function is to prevent BPDU flooding in the network. With BPDU filter function enabled, the port does not receive or forward BPDUs, but it sends out its own BPDUs, preventing the switch from being attacked by BPDUs.
Step 6	**spanning-tree bpduguard** (Optional) Enable the BPDU Protect function on the port. It is It is recommended to enable this function on edge ports. BPDU Protect function is used to prevent the edge port from receiving BPUDs. With BPDU protect function enabled, the edge port will be shutdown when it receives BPDUs, and reports these cases to the administrator. Only the administrator can restore it..
Step 7	**show spanning-tree interface-security [gigabitEthernet** *port* | port-channel l*agid*] [bpdufilter | bpduguard | loop | root | tc | tc-defend] (Optional) View the protect inforamtion of ports. *port*: Specify the port number. *lagid*: Specify the ID of the LAG.
Step 8	**end** Return to privileged EXEC mode.
Step 9	**copy running-config startup-config** Save the settings in the configuration file.

This example shows how to enable Loop Protect, Root Protect, BPDU Filter and BPDU Protect functions on port 1/0/3:

Switch#configure

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

Switch(config-if)#spanning-tree guard loop

Switch(config-if)#spanning-tree guard root

Switch(config-if)#spanning-tree bpdufilter

Switch(config-if)#spanning-tree bpduguard

Switch(config-if)#show spanning-tree interface-security gigabitEthernet 1/0/3

Interface	BPDU-Filter	BPDU-Guard	Loop-Protect	Root-Protect	TC-Protect
Gi1/0/3	Enable	Enable	Enable	Enable	Disable

Switch(config-if)#end

Switch#copy running-config startup-config

5 Configuration Example for MSTP

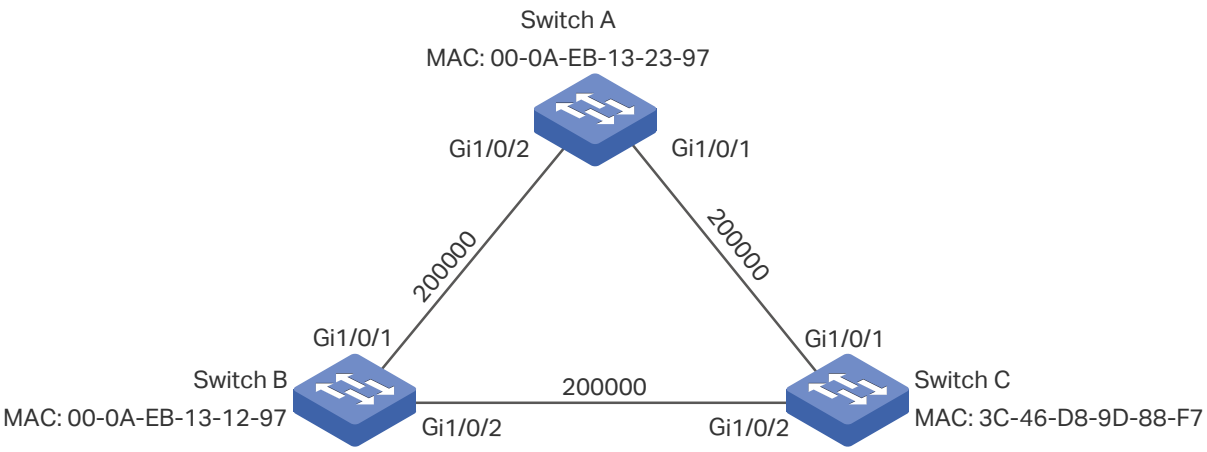
MSTP, backwards-compatible with STP and RSTP, can map VLANs to instances to enable load-balancing, thus providing a more flexible method in network management. Here we take the MSTP configuration as an example.

5.1 Network Requirements

As shown in figure 5-1, the network consists of three switches. Traffic in VLAN 101-VLAN 106 is transmitted in this network. The link speed between the switches is 100Mb/s (the default path cost of the port is 200000).

It is required that traffic in VLAN 101 - VLAN 103 and traffic in VLAN 104 - VLAN 106 should be transmitted along different paths.

Figure 5-1 Network Topology

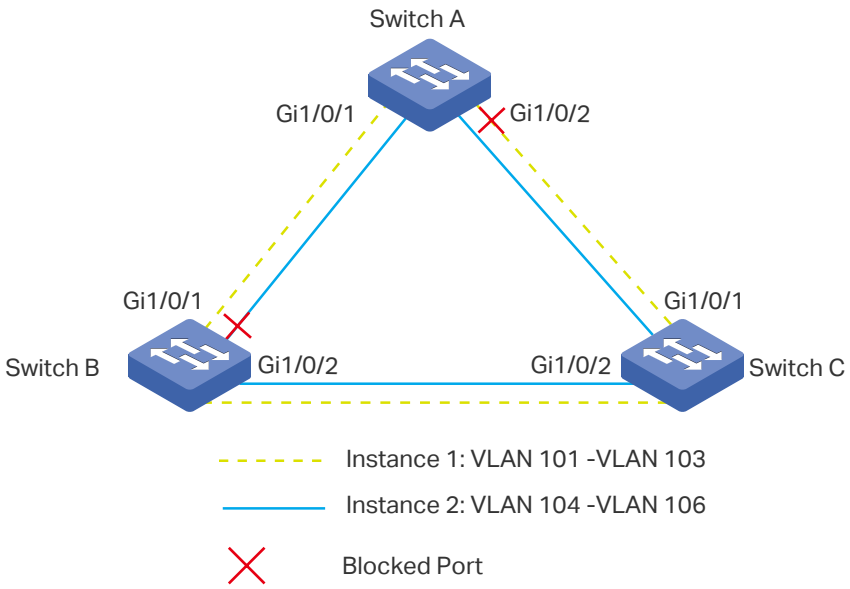


5.2 Configuration Scheme

To meet this requirement, you are suggested to configure MSTP function on the switches. Map the VLANs to different instances to ensure traffic can be transmitted along the respective instance.

Here we configure two instances to meet the requirement, as is shown below:

Figure 5-2 VLAN-Instance Mapping



The overview of configuration is as follows:

1) Enable the Spanning Tree function on the ports in each switch.
2) Configure Switch A, Switch B and Switch C in the same region. Configure the region name as 1, and the revision level as 100. Map VLAN 101 - VLAN 103 to instance 1 and VLAN 104 - VLAN 106 to instance 2.
3) Configure the priority of Switch B as 0 to set is as the root bridge in instance 1; configure the priority of Switch C as 0 to set is as the root bridge in instance 2.
4) Configure the path cost to block the specified ports. For instance 1, set the path cost of port 1/0/1 of Switch A to be greater than the default path cost (200000). For instance 2, set the path cost of port 1/0/2 of Switch B to be greater than the default path cost (200000).
5) Enable MSTP function in all the switches.

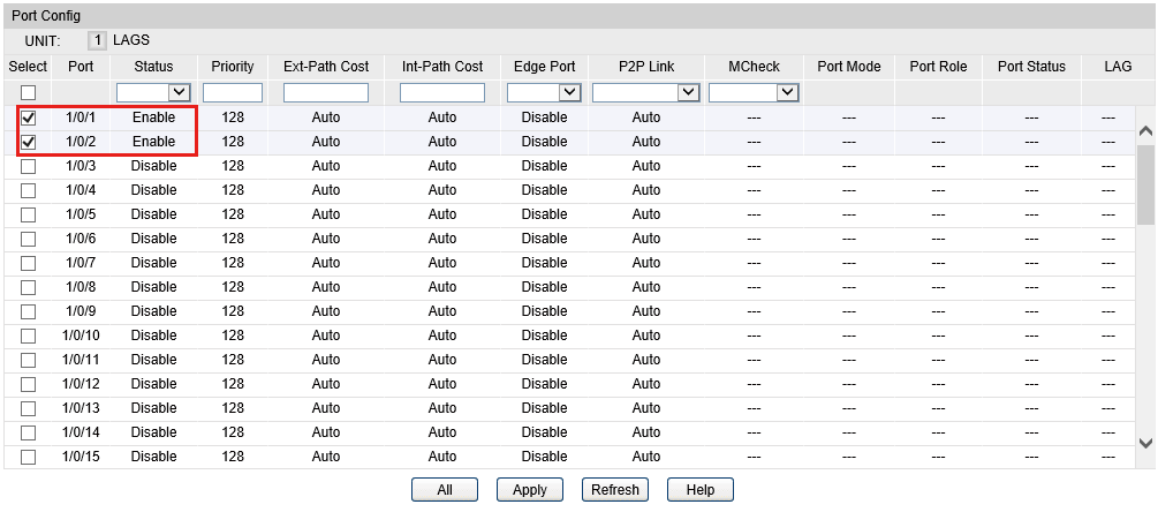
Demonstrated with T2600G-28TS, this chapter provides configuration procedures in two ways: using the GUI and using the CLI.

5.3 Using the GUI

- Configurations for Switch A

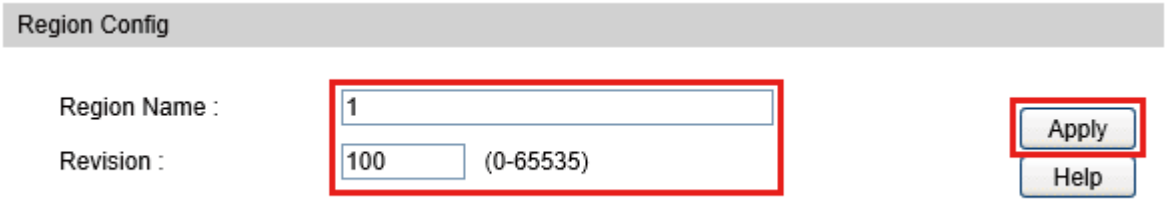
1) Choose the menu **Spanning Tree > STP Config > Port Config** to load the following page. Enable spanning tree function on port 1/0/1 and port 1/0/2. Here we leave the values of the other parameters as default settings.

Figure 5-3 Enable Spanning Tree Function on Ports



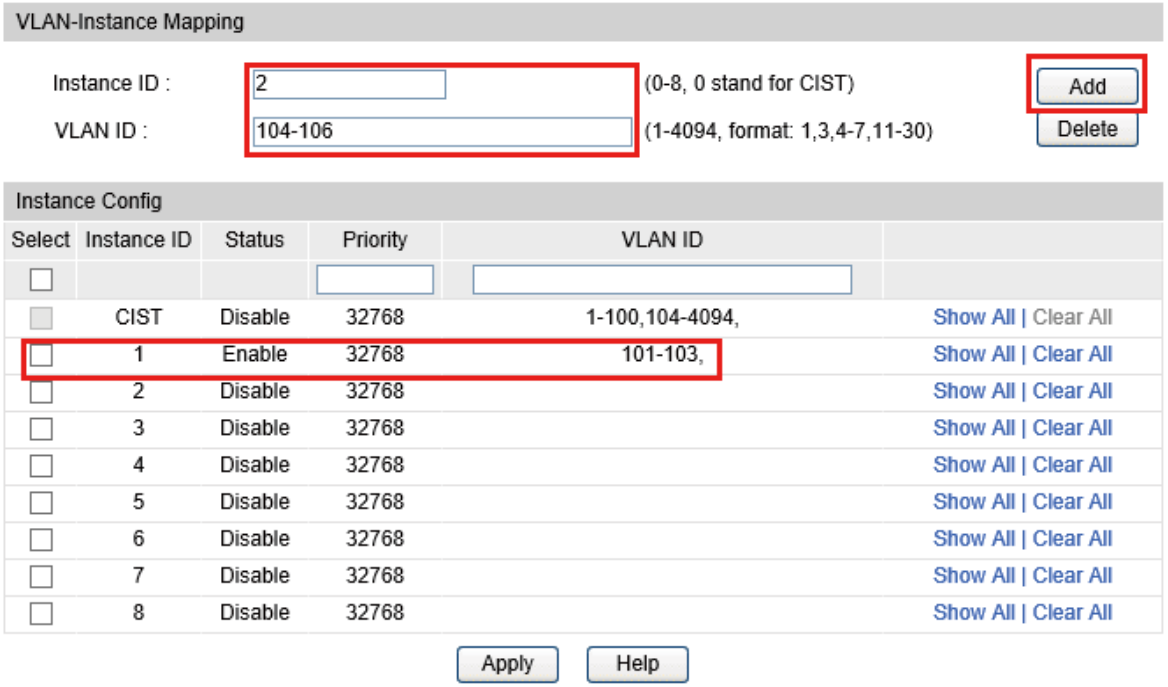
2) Choose the menu **Spanning Tree > MSTP Instance > Region Config** to load the following page. Set the region name as 1 and the revision level as 100.

Figure 5-4 Configuring the MST Region



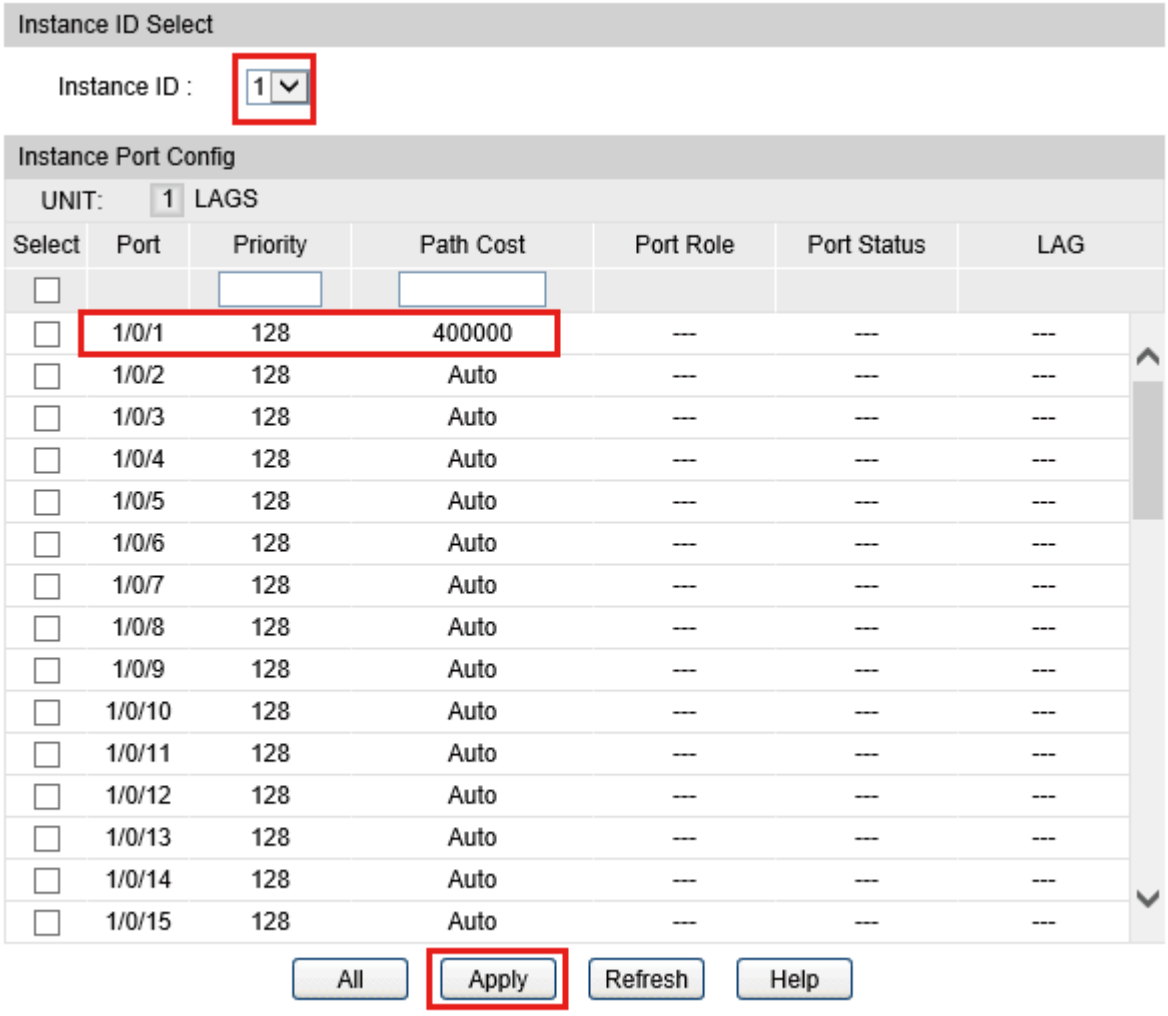
3) Choose the menu **Spanning Tree > MSTP Instance > Instance Config** to load the following page. Map VLAN101-VLAN103 to instance 1; map VLAN104-VLAN106 to instance 2.

Figure 5-5 Configuring the VLAN-Instance Mapping



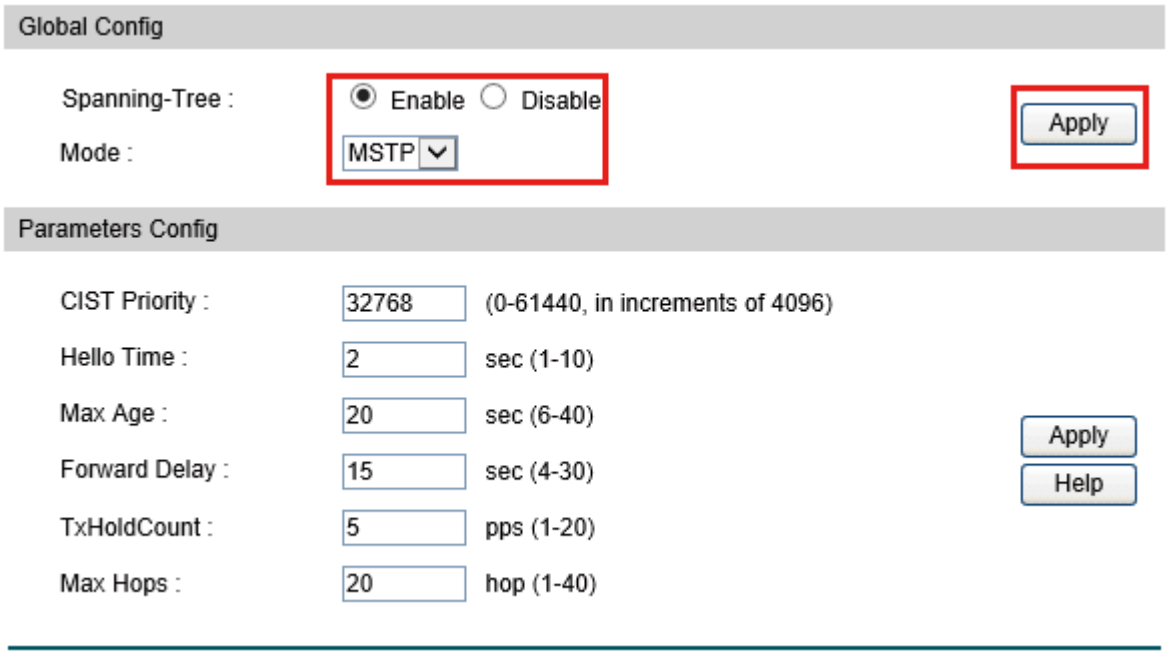
4) Choose the menu **Spanning Tree > MSTP Instance > Instance Port Config** to load the following page. Set the path cost of port 1/0/1 in instance 1 as 400000.

Figure 5-6 Configure the Path Cost of Port 1/0/1 In Instance 1



5) Choose the menu **Spanning Tree > STP Config > STP Config** to load the following page. Enable MSTP function globally, here we leave the values of the other global parameters as default settings.

Figure 5-7 Configure the Global MSTP Parameters of the Switch

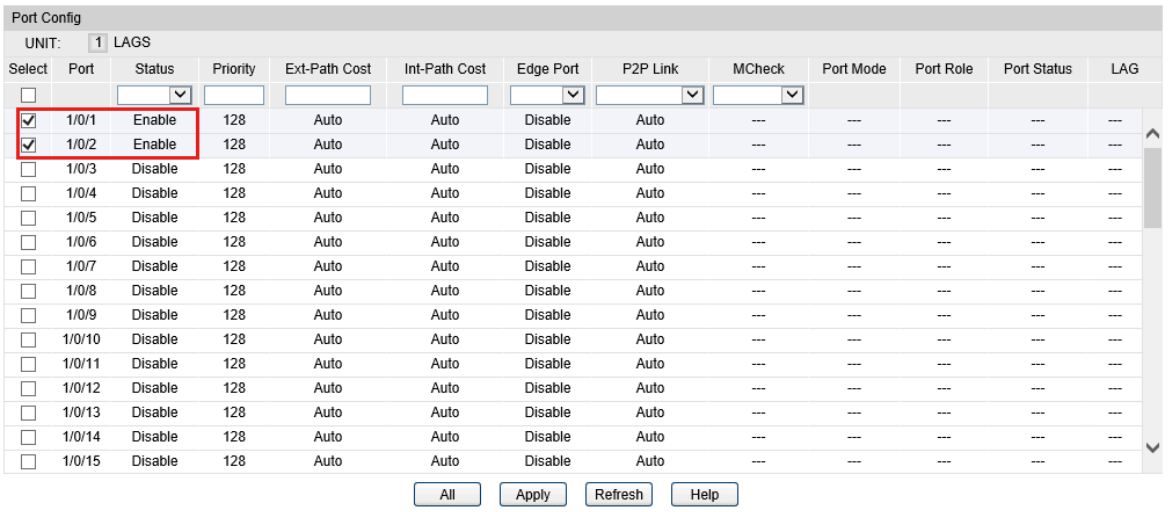


6) Click **Save Config** to save the settings.

Configurations for Switch B

1) Choose the menu **Spanning Tree > STP Config > Port Config** to load the following page. Enable the spanning tree function on port 1/0/1 and port 1/0/2. Here we leave the values of the other parameters as default settings.

Figure 5-8 Enable Spanning Tree Function on Ports



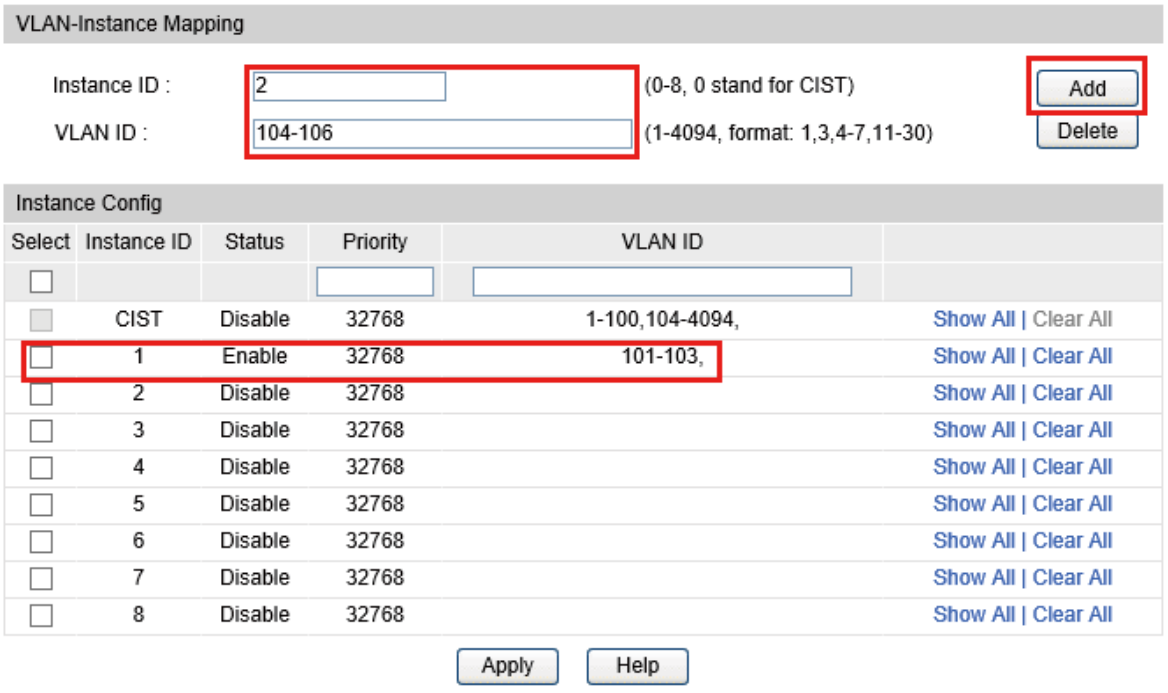
2) Choose the menu **Spanning Tree > MSTP Instance > Region Config** to load the following page. Set the region name as 1 and the revision level as 100.

Figure 5-9 Configuring the Region



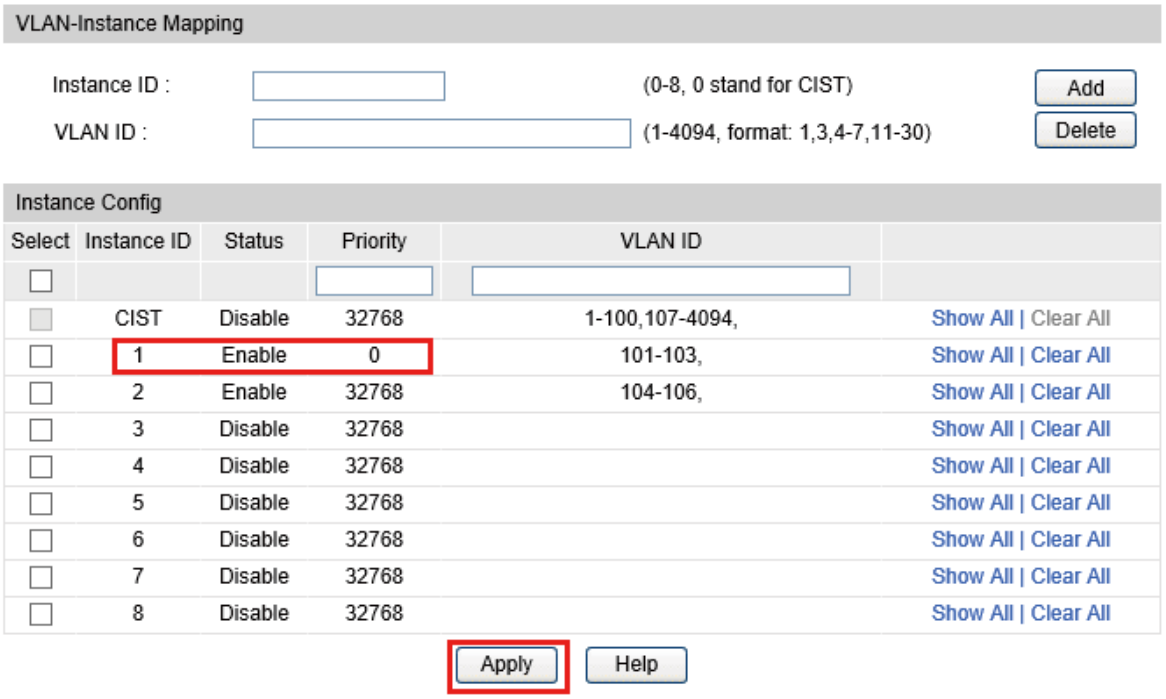
3) Choose the menu **Spanning Tree > MSTP Instance > Instance Config** to load the following page. Map VLAN101-VLAN103 to instance 1; map VLAN104-VLAN106 to instance 2.

Figure 5-10 Configuring the VLAN-Instance Mapping



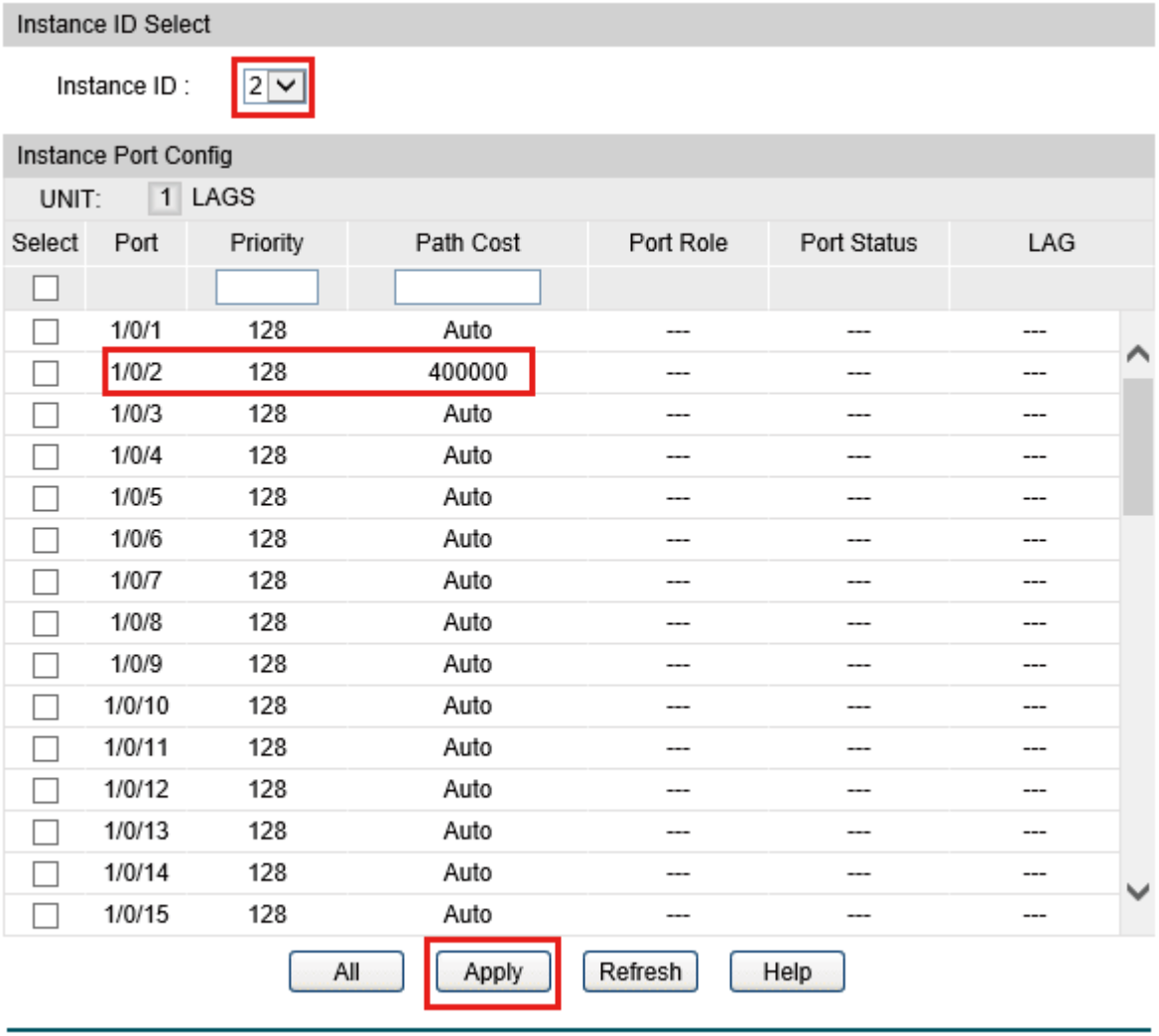
4) Choose the menu **Spanning Tree > MSTP Instance > Instance Config** to load the following page. Configure the priority of Switch B as 0 to set it as the root bridge in instance 1.

Figure 5-11 Configuring the Priority of Switch B in Instance 1



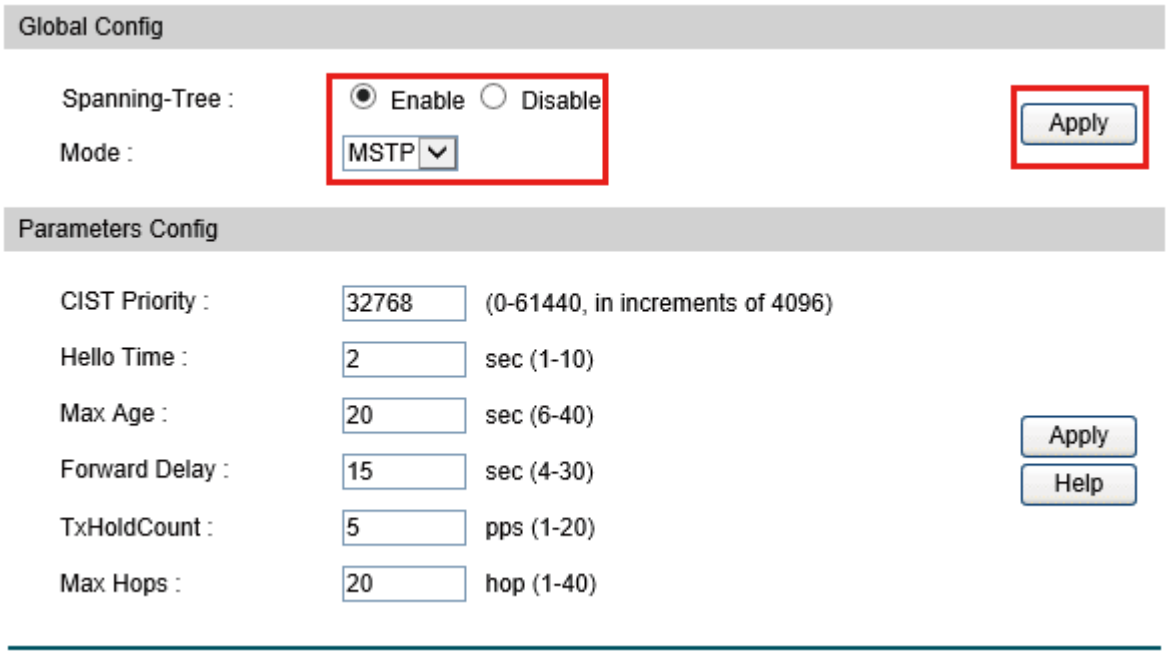
5) Choose the menu **Spanning Tree > MSTP Instance > Instance Port Config** to load the following page. Set the path cost of port 1/0/2 in instance 2 as 400000.

Figure 5-12 Configure the Path Cost of Port 1/0/2 in Instance 2



6) Choose the menu **Spanning Tree > STP Config > STP Config** to load the following page. Enable MSTP function globally. Here we leave the values of the other global parameters as default settings.

Figure 5-13 Configuring the MSTP Globally

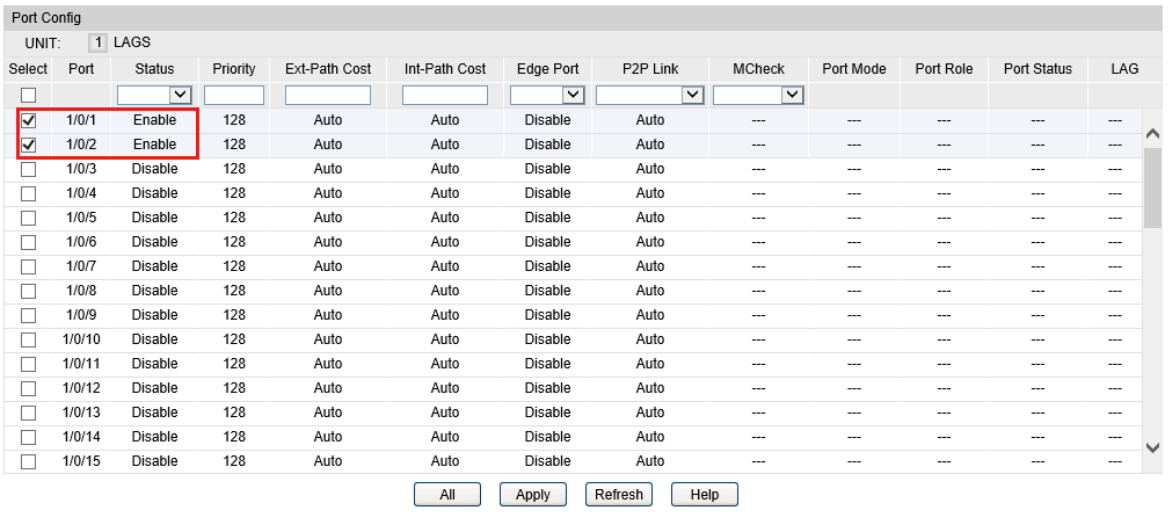


7) Click **Save Config** to save the settings.

Configurations for Switch C

1) Choose the menu **Spanning Tree > STP Config > Port Config** to load the following page. Enable the spanning tree function on port 1/0/1 and port 1/0/2. Here we leave the values of the other parameters as default settings.

Figure 5-14 Enable Spanning Tree Function on Ports



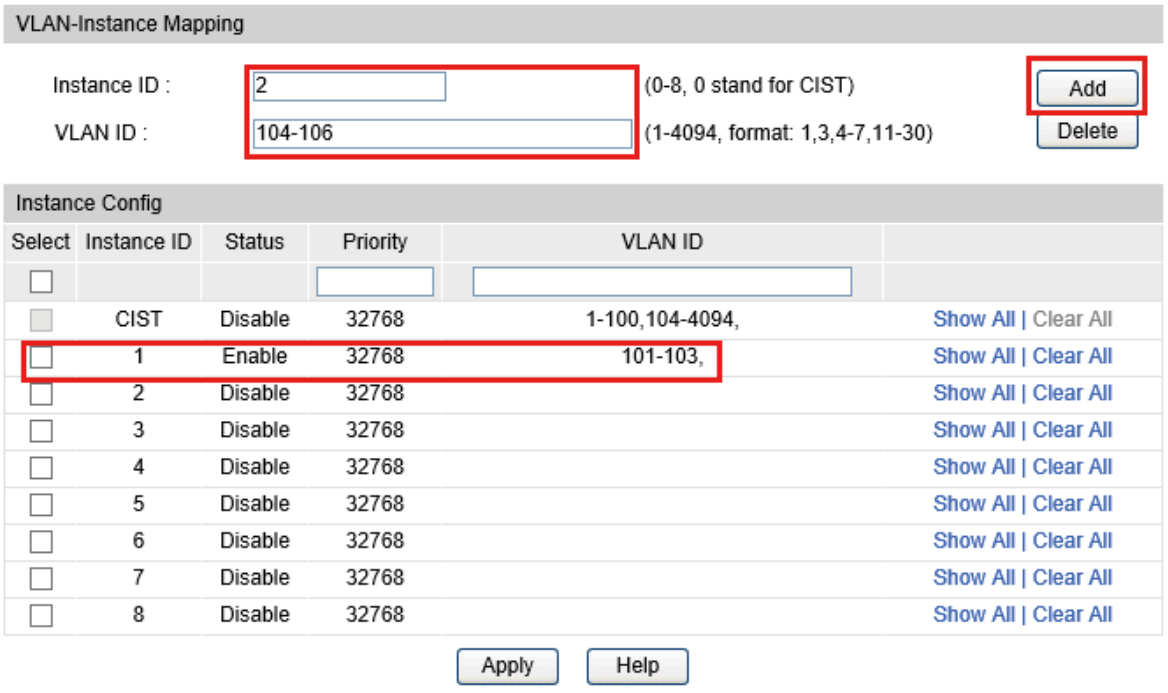
2) Choose the menu **Spanning Tree > MSTP Instance > Region Config** to load the following page. Set the region name as 1 and the revision level as 100.

Figure 5-15 Configuring the Region



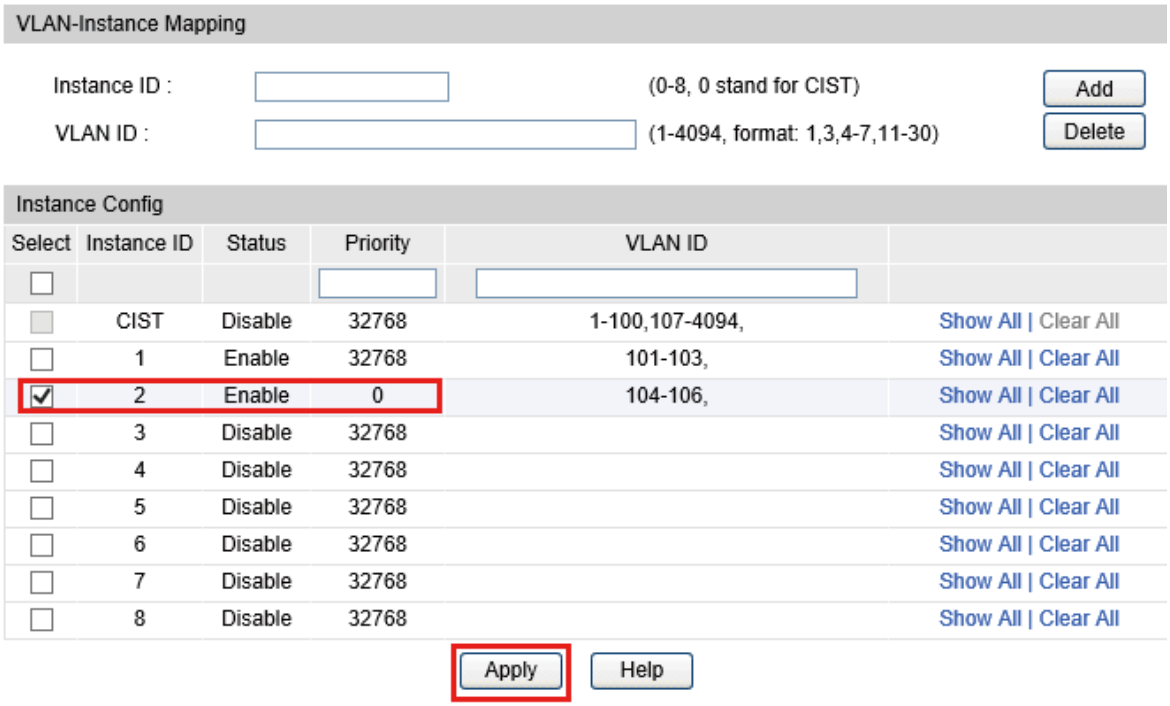
3) Choose the menu **Spanning Tree > MSTP Instance > Instance Config** to load the following page. Map VLAN101-VLAN103 to instance 1; map VLAN104-VLAN106 to instance 2.

Figure 5-16 Configuring the VLAN-Instance Mapping



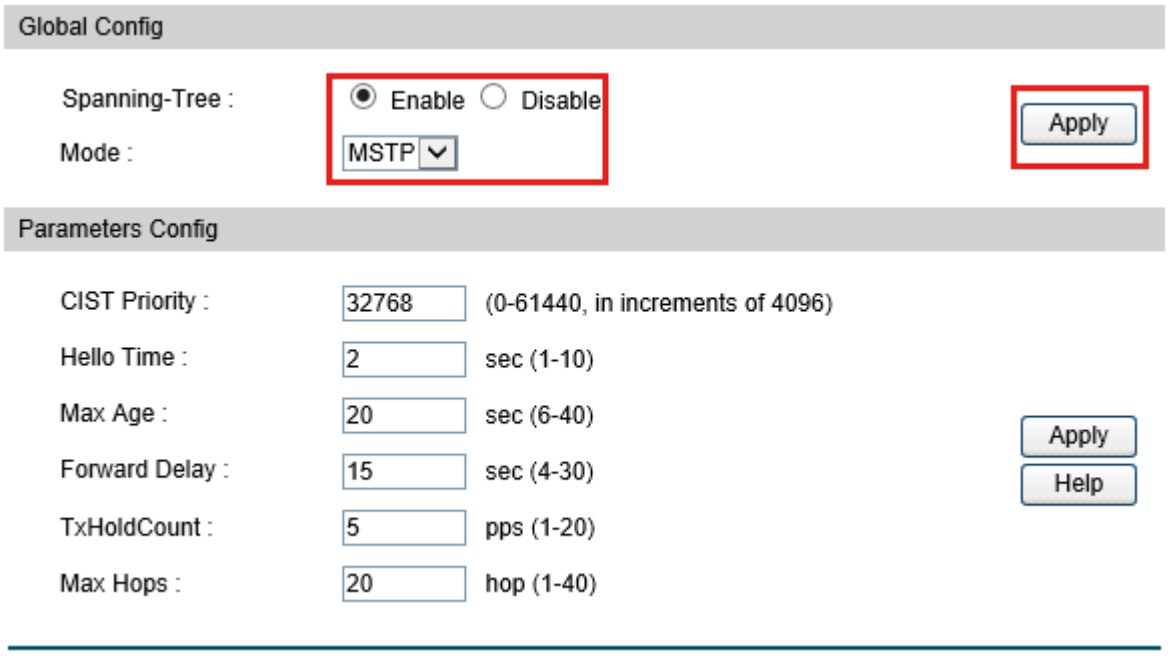
4) Choose the menu **Spanning Tree > MSTP Instance > Instance Config** to load the following page. Configure the priority of Switch C as 0 to set it as the root bridge in instance 2.

Figure 5-17 Configuring the Priority of Switch C in Instance 2



5) Choose the menu **Spanning Tree > STP Instance > STP Config** to load the following page. Enable MSTP function globally, here we leave the values of the other global parameters as default settings.

Figure 5-18 Configuring the MSTP Globally



6) Click **Save Config** to save the settings.

5.4 Using the CLI

- Configurations for Switch A

1) Enable the spanning tree function on port 1/0/1 and port 1/0/2, and specify the path cost of port 1/0/1 in instance 1 as 400000.

```
Switch#configure
Switch(config)#interface gigabitEthernet 1/0/1
Switch(config-if)#spanning-tree
Switch(config-if)#spanning-tree mst instance 1 cost 400000
Switch(config-if)#exit
Switch(config)#interface gigabitEthernet 1/0/2
Switch(config-if)#spanning-tree
Switch(config-if)#exit
```

2) Configure the region name as 1, the revision number as 100; map VLAN101-VLAN103 to instance 1; map VLAN104-VLAN106 to instance 2:

```
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#name 1
Switch(config-mst)#revision 100
Switch(config-mst)#instance 1 vlan 101-103
Switch(config-mst)#instance 2  vlan 104-106
Switch(config-mst)#exit
```

3) Configure the spanning tree mode as MSTP, then enable spanning tree function globally.

```
Switch(config)#spanning-tree mode mstp
Switch(config)#spanning-tree
Switch(config)#end
Switch#copy running-config startup-config
```

- Configurations for Switch B

1) Enable the spanning tree function on port 1/0/1 and port 1/0/2, and specify the path cost of port 1/0/2 in instance 2 as 400000.

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

Switch(config-if)#spanning-tree

Switch(config-if)#spanning-tree mst instance 2 cost 400000

Switch(config-if)#exit

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

Switch(config-if)#spanning-tree

Switch(config-if)#exit

2) Configure the region name as 1, the revision number as 100; map VLAN101-VLAN103 to instance 1; map VLAN104-VLAN106 to instance 2; configure the priority of Switch B in instance 1 as 0 to set it as the root bridge in instance 1:

Switch(config)#spanning-tree mst configuration

Switch(config-mst)#name 1

Switch(config-mst)#revision 100

Switch(config-mst)#instance 1 vlan 101-103

Switch(config-mst)#instance 2 vlan 104-106

Switch(config-mst)#exit

Switch(config)#spanning-tree mst instance 1 priority 0

3) Configure the spanning tree mode as MSTP, then enable spanning tree function globally.

Switch(config)#spanning-tree mode mstp

Switch(config)#spanning-tree

Switch(config)#end

Switch#copy running-config startup-config

- Configurations for Switch C

1) Enable the spanning tree function on port 1/0/1 and port 1/0/2.

Switch#configure

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

Switch(config-if-range)#spanning-tree

Switch(config-if-range)#exit

2) Configure the region name as 1, the revision number as 100; map VLAN101-VLAN103 to instance 1; map VLAN104-VLAN106 to instance 2; configure the priority of Switch C in instance 2 as 0 to set it as the root bridge in instance 2:

Switch(config)#spanning-tree mst configuration

Switch(config-mst)#name 1

Switch(config-mst)#revision 100

Switch(config-mst)#instance 1 vlan 101-103

Switch(config-mst)#instance 2 vlan 104-106

Switch(config-mst)#exit

Switch(config)#spanning-tree mst instance 2 priority 0

3) Configure the spanning tree mode as MSTP, then enable spanning tree function globally.

Switch(config)#spanning-tree mode mstp

Switch(config)#spanning-tree

Switch(config)#end

Switch#copy running-config startup-config

Verify the Configurations

- Switch A

Verify the configurations of Switch A in instance 1:

Switch(config)#show spanning-tree mst instance 1

MST-Instance 1

Root Bridge

Priority : 0

Address : 00-0a-eb-13-12-ba

Internal Cost : 400000

Root Port : 1

Designated Bridge

Priority : 0

Address : 00-0a-eb-13-12-ba

Local Bridge

Priority : 32768

Address : 00-0a-eb-13-23-97

```
Interface   Prio    Cost        Role    Status    LAG
---------   ----    --------    ------  -----     ----
Gi1/0/1     128     400000      Root    Fwd       N/A
Gi1/0/2     128     200000      Altn    Blk       N/A
```

Verify the configurations of Switch A in instance 2:

```
Switch(config)#show spanning-tree mst instance 2
MST-Instance 2
Root Bridge
Priority    : 0
Address     : 3c-46-d8-9d-88-f7
Internal Cost : 200000
Root Port   : 2
Designated Bridge
Priority    : 0
Address     : 3c-46-d8-9d-88-f7
Local Bridge
Priority    : 32768
Address     : 00-0a-eb-13-23-97
Interface   Prio    Cost        Role     Status    LAG
---------   ----    --------    -------  -------   ----
Gi1/0/1     128     200000      Desg     Fwd       N/A
Gi1/0/2     128     200000      Root     Fwd       N/A
```

- Switch B

  Verify the configurations of Switch B in instance 1:

```
Switch(config)#show spanning-tree mst instance 1
MST-Instance 1
Root Bridge
Priority    : 0
Address     : 00-0a-eb-13-12-ba
```

Local bridge is the root bridge

Designated Bridge

Priority : 0

Address : 00-0a-eb-13-12-ba

Local Bridge

Priority : 0

Address : 00-0a-eb-13-12-ba

Interface	Prio	Cost	Role	Status
Gi1/0/1	128	200000	Desg	Fwd
Gi1/0/2	128	200000	Desg	Fwd

Verify the configurations of Switch B in instance 2:

Switch(config)#show spanning-tree mst instance 2

MST-Instance 2

Root Bridge

Priority : 0

Address : 3c-46-d8-9d-88-f7

Internal Cost : 400000

Root Port : 2

Designated Bridge

Priority : 0

Address : 3c-46-d8-9d-88-f7

Local Bridge

Priority : 32768

Address : 00-0a-eb-13-12-ba

Interface	Prio	Cost	Role	Status
Gi1/0/1	128	200000	Altn	Blk
Gi1/0/2	128	200000	Root	Fwd

- Switch C

  Verify the configurations of Switch C in instance 1:

  Switch(config)#show spanning-tree mst instance 1

  MST-Instance 1

  Root Bridge

  Priority : 0

  Address : 00-0a-eb-13-12-ba

  Internal Cost : 200000

  Root Port : 2

  Designated Bridge

  Priority : 0

  Address : 00-0a-eb-13-12-ba

  Local Bridge

  Priority : 32768

  Address : 3c-46-d8-9d-88-f7

Interface	Prio	Cost	Role	Status
Gi1/0/1	128	200000	Desg	Fwd
Gi1/0/2	128	200000	Root	Fwd

  Verify the configurations of Switch C in instance 2:

  Switch(config)#show spanning-tree mst instance 2

  MST-Instance 2

  Root Bridge

  Priority : 0

  Address : 3c-46-d8-9d-88-f7

  Local bridge is the root bridge

  Designated Bridge

  Priority : 0

  Address : 3c-46-d8-9d-88-f7

```
Local Bridge
Priority    : 0
Address     : 3c-46-d8-9d-88-f7
Interface     Prio      Cost        Role      Status
-----------   ------    ---------   -------   ----------
Gi1/0/1       128       200000      Desg      Fwd
Gi1/0/2       128       200000      Desg      Fwd
```

6 Appendix: Default Parameters

Default settings of the Spanning Tree feature are listed in the following table.

Table 6-1 Default Settings of the Global Parameters

Parameter	Default Setting
Spanning-tree	Disable
Mode	STP
CIST Priority	32768
Hello Time	2 seconds
Max Age	20 seconds
Forward Delay	15 seconds
TxHoldCount	5 pps
Max Hops	20 hops

Table 6-2 Default Settings of the Port Parameters

Parameter	Default Setting
Status	Disable
Priority	128
Ext-Path Cost	Auto
In-Path Cost	Auto
Edge Port	Disable
P2P Link	Auto
MCheck	------

Table 6-3 Default Settings of the MSTP Instance

Parameter	Default Setting
Status	Disable
Priority	32768

Parameter	Default Setting
Port Priority	128
Path Cost	Auto

Part 16

Configuring OAM

CHAPTERS

1 . Ethernet OAM
2 . Ethernet OAM Configurations
3 . Viewing OAM Statistics
4 . Configuration Example
5 . Appendix: Default Parameters

1 Ethernet OAM

1.1 Overview

Ethernet OAM (Operation, Administration, and Maintenance) is a Layer 2 protocol for monitoring and troubleshooting Ethernet networks. It can monitor link performance, monitor faults and generate alarms so that a network administrator can manage the network effectively. TP-Link switches support EFM OAM which is defined in IEEE 802.3ah.

The following basic concepts of OAM will be introduced: OAM entity, OAMPDUs (OAM Protocol Data Units), and OAM connection.

OAM Entity

A port that is enabled with OAM on the switch is called an OAM entity.

OAMPDUs

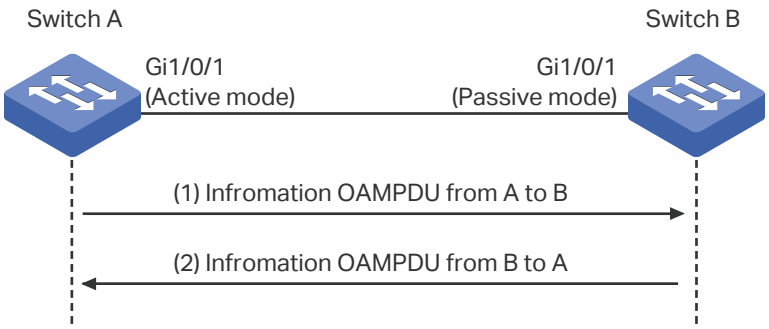
Through OAMPDUs exchanged between OAM entities, failure conditions on the network are reported to network administrators. The OAMPDUs are defined as follows:

- **Information OAMPDU**: The Information OAMPDU is used to send state information, such as local information, remote information, and user-defined information, to the remote OAM entity for maintaining OAM connection.
- **Event Notification OAMPDU**: The Event Notification OAMPDU is used for the Link Monitoring feature. The local OAM entity can use the Event Notification OAMPDU to notify the remote OAM entity that a fault has occurred to the link.
- **Loopback Control OAMPDU**: Loopback Control OAMPDU is used for the Remote Loopback feature. The local OAM entity can control OAM remote loopback state of the remote OAM entity through the Loopback Control OAMPDU.

OAM Connection

OAM connection is established between OAM entities before OAM works. An OAM entity can operate in two modes: active and passive. Only the active OAM entity can initiate an OAM connection; the passive OAM entity waits and responds to OAM connection establishment requests. So at least one of the two entities should be in active mode.

Figure 1-1 OAM Connection Establishment



As the above figure shows, the OAM entity on Switch A is in active mode, and that on Switch B is in passive mode. Switch A initiates an OAM connection by sending an Information OAMPDU. Switch B compares the OAM information in the received OAMPDU with its own and sends back an Information OAMPDU to Switch A. If the OAM information of the two entities matches, an OAM connection will be established. After that, the two OAM entities will exchange Information OAMPDUs periodically to keep the OAM connection valid.

1.2 Supported Features

The switch supports the following OAM features: Link Monitoring, Remote Failure Indication (RFI), and Remote Loopback.

Link Monitoring

Link Monitoring is for monitoring link performance under various circumstances. When problems are detected on the link, the OAM entity will send its remote peer the Event Notification OAMPDUs to report link events.

The link events are described as follows:

Table 1-1 OAM Link Events

OAM Link Events	Definition
Symbol Period Error	A Symbol Period Error event occurs if the number of symbol errors exceeds the defined threshold within a specific period of time.
Frame Error	A Frame Error event occurs if the number of frame errors exceeds the defined threshold within a specific period of time.
Frame Period Error	A Frame Period Error event occurs if the number of frame errors in specific number of received frames exceeds the defined threshold. The period means a specific number of received frames, which can be configured by users.

OAM Link Events	Definition
Frame Seconds Error	A Frame Seconds Error event occurs if the number of error frame seconds exceeds the threshold within a specific period of time. A second is called an error frame second if error frames occur in the second.

Remote Failure Indication

With Remote Failure Indication, an OAM entity can send the failure conditions of the link, such as disruption in traffic because of the device failure, to its peer through Information OAMPDUs. So the network administrator can get informed of the link faults and take action in time. The switch supports two kinds of failure conditions:

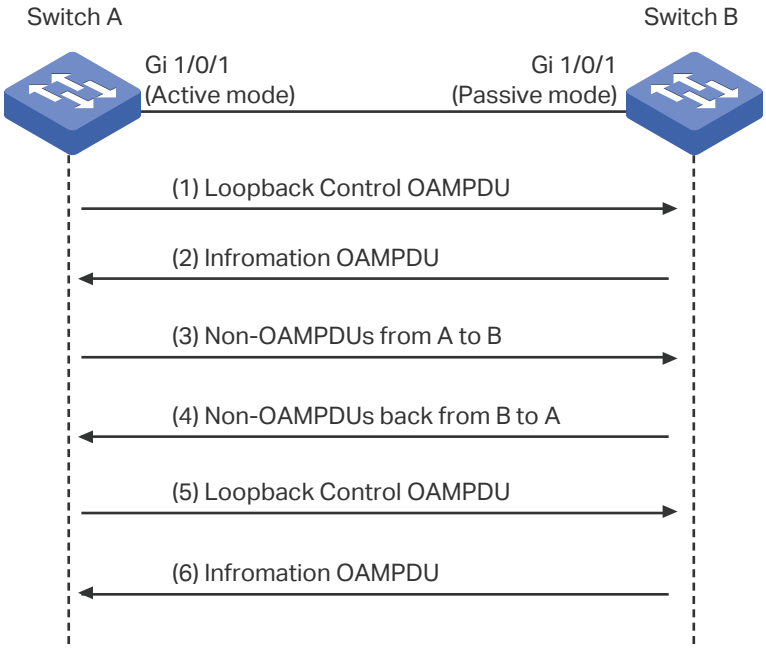
Dying Gasp: An unrecoverable fault, such as power failure, occurs.

Critical Event: Unspecified critical event occurs.

Remote Loopback

With Remote Loopback, administrators can test the link performance like delay, jitter, and frame loss rate during installation or for troubleshooting.

Figure 1-2 Remote Loopback



As the above figure shows, the OAM connection has been established between the two entities. The OAM entity on Switch A is in active mode, and that on Switch B is in passive mode.

The working mechanism of Remote Loopback is as follows:

1) Switch A sends a Loopback Control OAMPDU to put the peer into remote loopback mode. Note that at least one of the two entities should be configured in active mode because only the entity in active mode can generate Loopback Control OAMPDU.
2) After receiving the Loopback Control OAMPDU, Switch B turns into remote loopback mode and sends an Information OAMPDU to inform its state updating.
3) Switch A sends Non-OAMPDU packets to Switch B for link testing.
4) Switch B receives the testing packets and sends back these packets along the original path. Through these returned packets, administrators can test the link performance.
5) When Remote Loopback is finished, Switch A sends a Loopback Control OAMPDU to disable the remote loopback mode on Switch B.
6) Switch B receives the Loopback Control OAMPDU and exits remote loopback mode. Besides, Switch B sends an Information OAMPDU to inform its state updating.

TP-Link switches can act as Switch A and initiate Remote Loopback request.

2 Ethernet OAM Configurations

To complete OAM configurations, follow these steps:

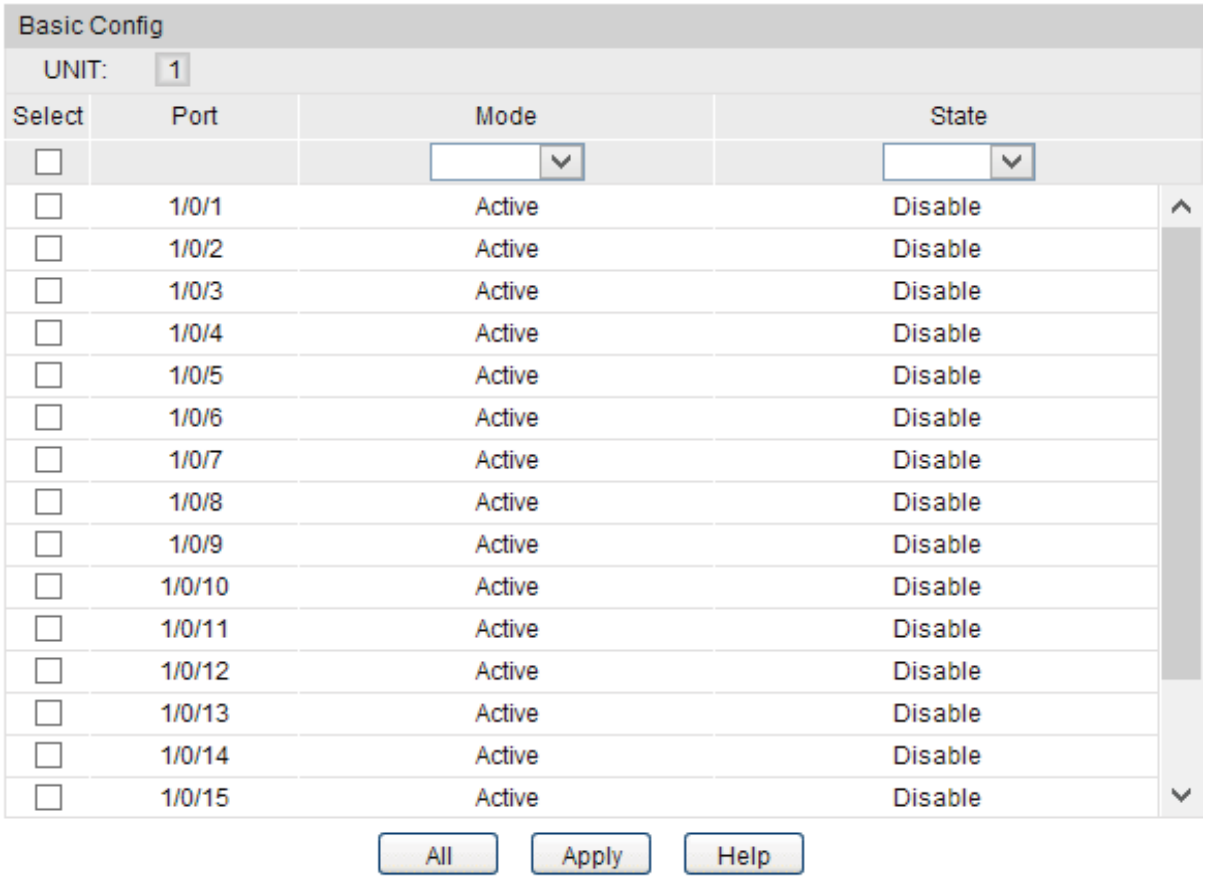
1) Enable OAM and configure OAM mode on the port.
2) Configure the following OAM features according to your needs:
   - Link Monitoring
   - Remote Failure Indication (RFI)
   - Remote Loopback
3) View the OAM status on the port.

2.1 Using the GUI

2.1.1 Enabling OAM and Configuring OAM Mode

Choose the menu **Ethernet OAM > Basic Config > Basic Config** to load the following page.

Figure 2-1 Basic Configuration



Follow these steps to complete the basic OAM configuration:

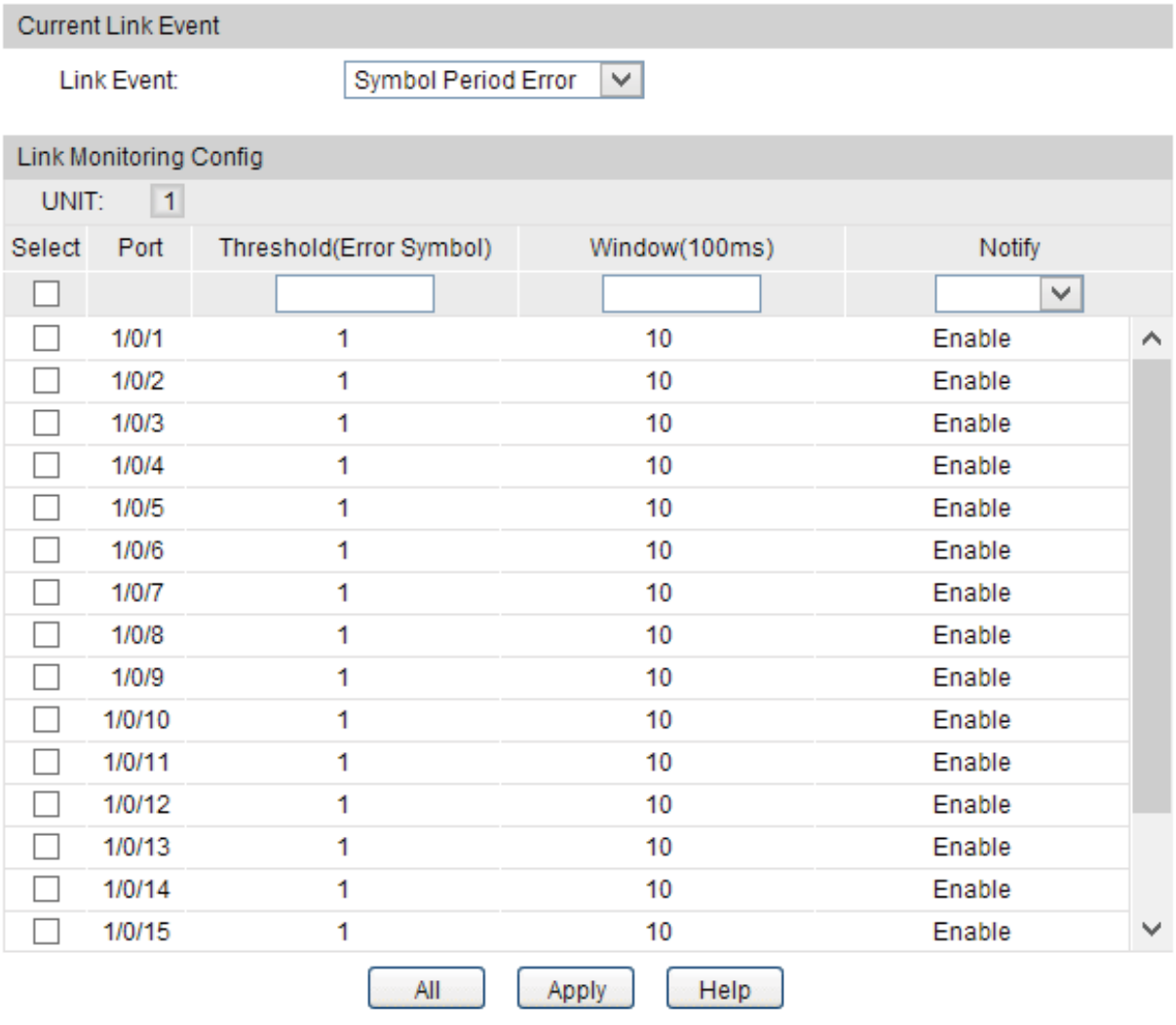
1) Select one or more ports, configure the OAM mode and enable OAM.

Mode	Select OAM mode for the port. **Active:** The port in this mode can initiate OAM connection. It is the default setting. **Passive:** The port in this mode cannot initiate OAM connection or send loopback control OAMPDUs. Note: OAM connection cannot be established between two ports in passive mode. Make sure that at least one side is in active mode.
State	Enable or disable OAM on the port. By default, it is disabled.

2) Click **Apply**.

2.1.2 Configuring Link Monitoring

Choose the menu **Ethernet OAM > Link Monitoring > Link Monitoring** to load the following page.



Follow these steps to configure Link Monitoring:

1) In the **Current Link Event** section, select a Link Event type to be configured.

Current Link Event	Select Link Event type. The following options are provided: **Symbol Period Error**: A Symbol Period Error event occurs if the number of symbol errors exceeds the defined threshold within a specific period of time. **Frame Error**: A Frame Error event occurs if the number of frame errors exceeds the defined threshold within a specific period of time. **Frame Period Error**: A Frame Period Error event occurs if the number of frame errors in specific number of received frames exceeds the defined threshold. **Frame Seconds Error**: A Frame Seconds Error event occurs if the number of error frame seconds exceeds the threshold within a specific period of time. A second is called an error frame second if error frames occur in the second.

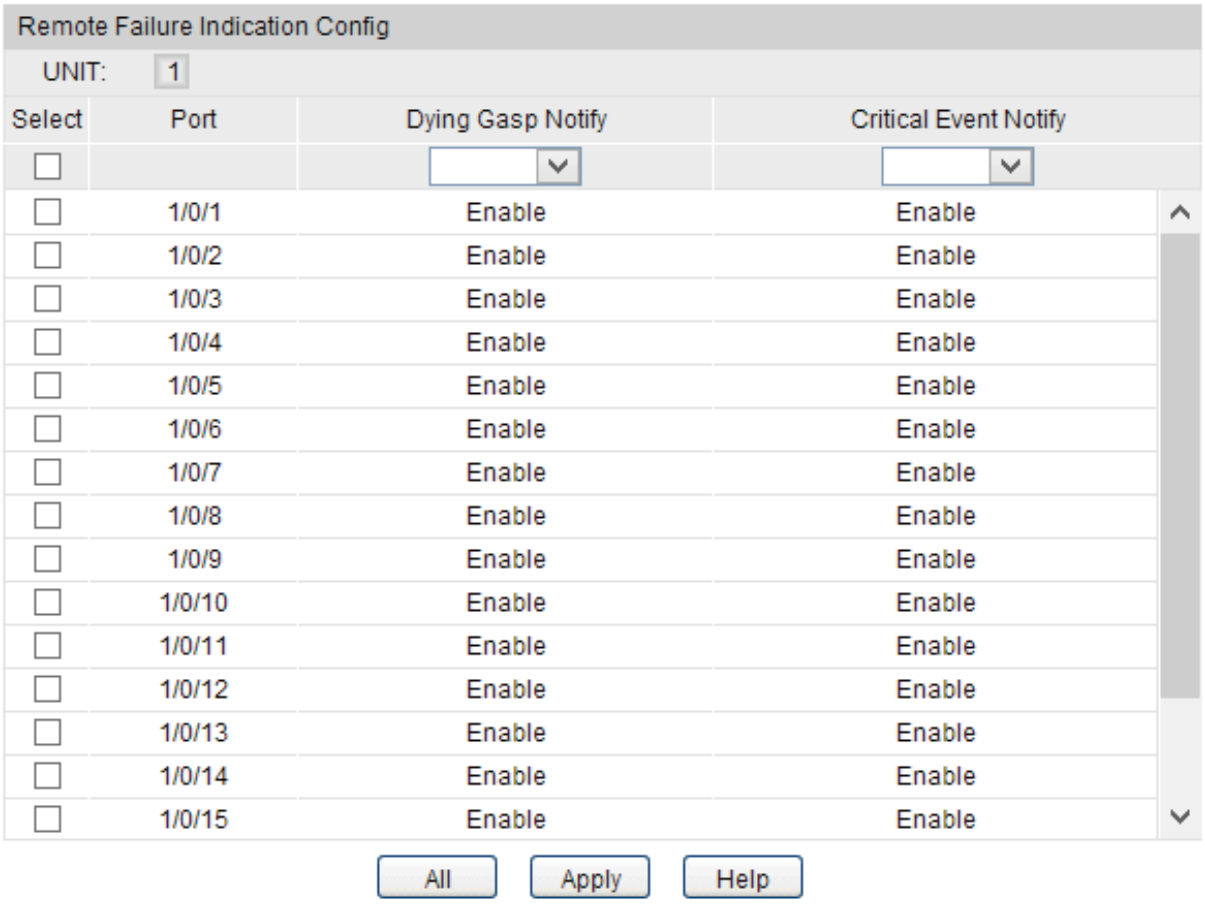
3) In the **Link Monitoring Config** section, select one or more ports, and configure the threshold and period for the selected link event.

Threshold	Specify the threshold for the selected link event. **Threshold (Error Symbol)**: If you select **Symbol Period Error** as the link event type, specify the threshold of received symbol errors within a specific period of time. The valid values are from 1 to 4294967295 error frames, and the default value is 1 error frame. **Threshold (Error Frame)**: If you select **Frame Error** or **Frame Period Error** as the link event type, specify the threshold of frame errors within a specific period of time or in specific number of received frames. The valid values are from 1 to 4294967295 error frames, and the default value is 1 error frame. **Threshold (Error Seconds)**: If you select **Frame Seconds Error** as the link event type, specify the threshold of error frame seconds. The valid values are from 1 to 900 error frame seconds, and the default value is 1 error frame second.
Window	Specify the period for the selected link event. **Window (100ms)**: If you select **Symbol Period Error**, **Frame Error** or **Frame Seconds Error** as the link event type, specify the period time in 100ms, in which if the received errors exceed the threshold, a link event will be generated. For **Symbol Period Error** and **Frame Error**, the valid values are from 10*100 to 600*100 ms, and the default value is 10*100 ms. For **Frame Seconds Error**, the valid values are from 100*100 to 9000*100 ms, and the default value is 600*100 ms. **Window (Frames)**: If you select **Frame Period Error** as the link event type, specify the number of frames, in which if the frame errors exceed the threshold, a link event will be generated. The valid values are from 148810 to 89286000 frames, and the default value is 1488100 frames.
Notify	Enable or disable the port to report the Link Event. By default, all types of the Link Events can be reported.

4) Click **Apply**.

2.1.3 Configuring RFI

Choose the menu **Ethernet OAM > RFI > Remote Failure Indication Config** to load the following page.



Follow these steps to configure Remote Failure Indication:

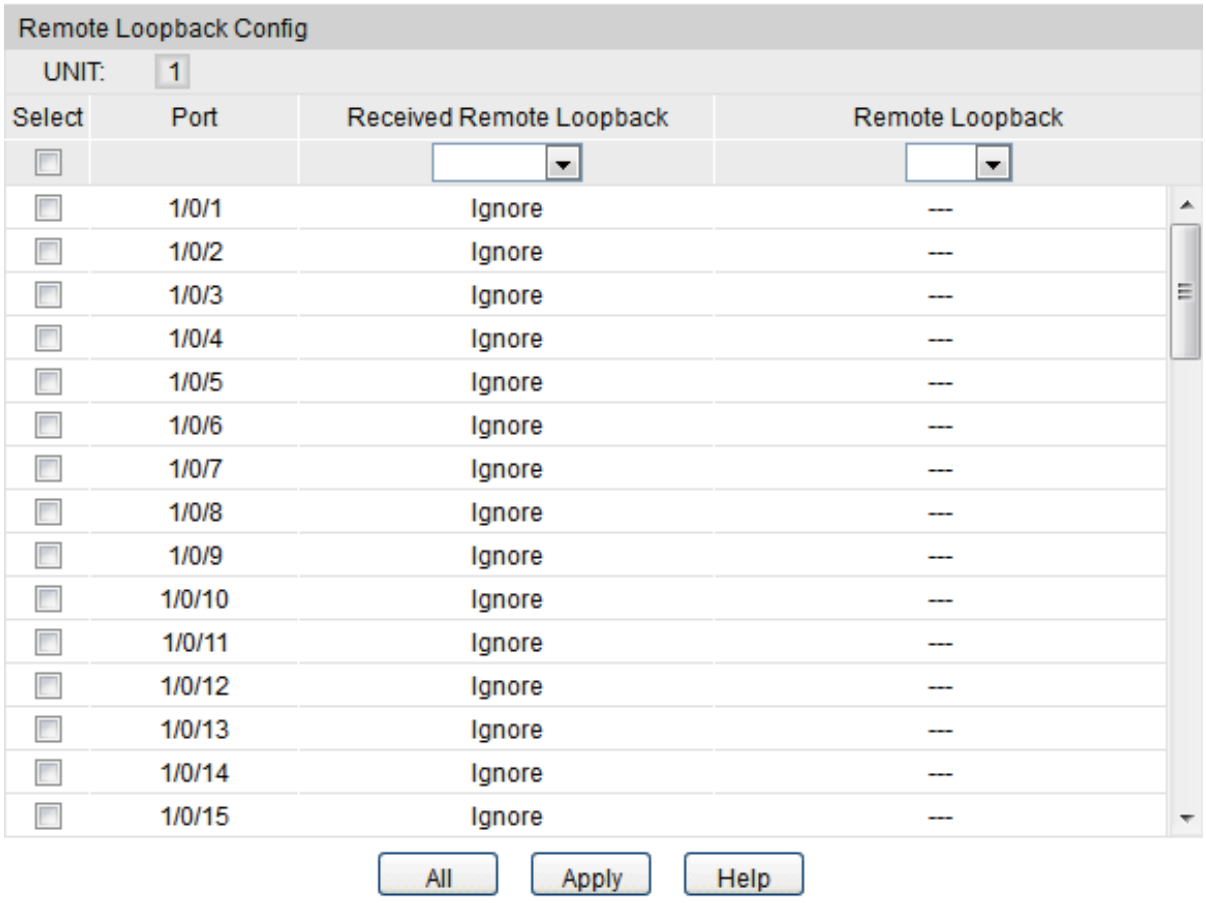
1) Select one or more ports and configure the Dying Gasp Notify and Critical Event Notify features.

Dying Gasp Notify	Enable Dying Gasp Notify. If the switch detects an unrecoverable fault on the network, it will report this condition locally and send Information OAMPDU to notify the peer.
Critical Event Notify	Enable Critical Event Notify. If the switch detects an unspecified critical event occurs, it will report this condition locally and send Information OAMPDU to notify the peer.

2) Click **Apply**.

2.1.4 Configuring Remote Loopback

Choose the menu **Ethernet OAM > Remote Loopbak > Remote Loopback** to load the following page.



Follow these steps to configure Remote Loopback:

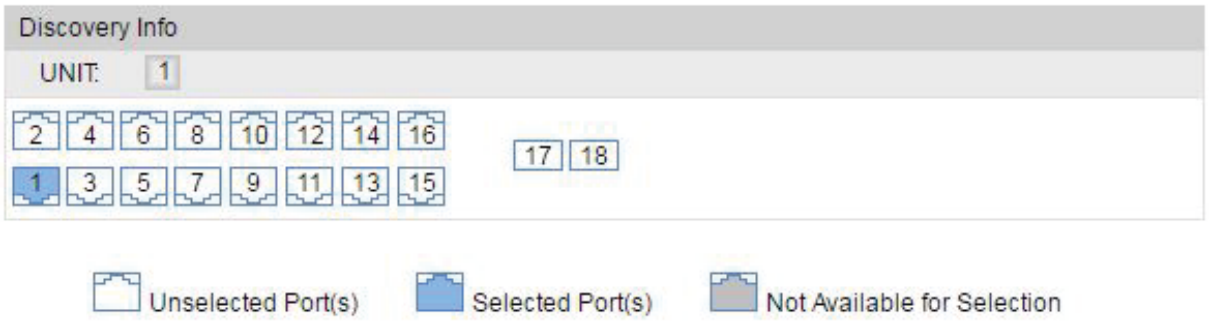
1) Select one or more ports and configure the relevant options.

Received Remote Loopback	Choose to ignore or to process the received remote loopback request.
Remote Loopback	Start or stop the remote loopback process. **Start**: Request the remote peer to start the OAM remote loopback mode. **Stop**: Request the remote peer to stop the OAM remote loopback mode. Note: The port to be configured here should be in active mode and has established OAM connection with the peer.

2) Click **Apply**.

2.1.5 Viewing OAM Status

Choose the menu **Ethernet OAM > Basic Config > Discovery Info** to load the following page.



Local Client	
OAM:	Enable
Mode:	Passive
Max OAMPDU:	1518 Bytes
Remote Loopback:	Not Supported
Unidirection:	Not Supported
Link Monitoring:	Supported
Variable Request:	Not Supported
PDU Revision:	1
Operation Status:	Operational
Loopback Status:	No Loopback

Remote Client	
Mode:	Active
Mac Address:	18-A6-F7-DB-63-81
Vendor(OUI):	000aeb
Max OAMPDU:	1518 Bytes
Remote Loopback:	Supported
Unidirection:	Not Supported
Link Monitoring:	Supported
Variable Request:	Not Supported
PDU Revision:	0
Vendor Information:	00000000

Select a port to view whether the OAM connection is established with the peer. Additionally, you can view the OAM information of the local and the remote entities.

The OAM information of the local entity is as follows:

OAM	Displays whether OAM is enabled.
Mode	Displays OAM mode of the local entity.

Max OAMPDU	Displays the maximum size of OAMPDU.
Remote Loopback	Displays whether the local entity supports Remote Loopback.
Unidirection	Displays whether the local entity supports Unidirection.
Link Monitoring	Displays whether the local entity supports Link Monitoring.
Variable Request	Displays whether the local entity supports Variable Request.
PDU Revision	Displays the PDU Revision of the local entity.
Operation Status	Displays the status of OAM connection: **Disable**: OAM is disabled on the port. **LinkFault**: The link between the local entity and the remote entity is down. **PassiveWait**: The port is in passive mode and is waiting to see if the peer device is OAM capable. **ActiveSendLocal**: The port is in active mode and is sending local information. **SendLocalAndRemote**: The local port has discovered the peer but has not yet accepted or rejected the configuration of the peer. **SendLocalAndRemoteOK**: The local device agrees the OAM peer entity. **PeeringLocallyRejected**: The local OAM entity rejects the remote peer OAM entity. **PeeringRemotelyRejected**: The remote OAM entity rejects the local device. **NonOperHalfDuplex**: Ethernet OAM is enabled but the port is in half-duplex operation. You should configure the port as a full-duplex port. **Operational**: OAM connection is established with the peer and OAM works normally.
Loopback Status	Displays the loopback status. **No Loopback**: Neither the local entity nor the remote entity is in the loopback mode. **Local Loopback**: The local entity is in the loopback mode. **Remote Loopback**: The remote entity is in the loopback mode.

The OAM information of the remote entity is as follows:

Mode	Displays OAM mode of the remote entity.
MAC Address	Displays the MAC address of the remote entity.
Vendor (OUI)	Displays the Vendor's OUI of the remote entity.
Max OAMPDU	Displays the maximum size of OAMPDU.

Remote Loopback	Displays whether the remote entity supports Remote Loopback.
Unidirection	Displays whether the remote entity supports Unidirection.
Link Monitoring	Displays whether the remote entity supports Link Monitoring.
Variable Request	Displays whether the remote entity supports Variable Request.
PDU Revision	Displays the PDU Revision of the remote entity.
Vendor Information	Displays the vendor information of the remote entity.

2.2 Using the CLI

2.2.1 Enabling OAM and Configuring OAM Mode

Follow these steps to enable OAM and configure OAM mode on the port:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list***}** Enter interface configuration mode.
Step 3	**ethernet-oam** Enable OAM on the port.
Step 4	**ethernet-oam mode** { passive | active } Configure the OAM mode of the port. passive: Specify the OAM mode as passive. The port in this mode cannot initiate OAM connection or send Loopback Control OAMPDU. active: Specify the OAM mode as active. The port in this mode can initiate OAM connection. It is the default setting. Note: OAM connection cannot be established between two ports in passive mode. Make sure that at least one side is in active mode.
Step 5	**show ethernet-oam configuration [interface fastEthernet** { *port* **|** *port-list* } **| interface gigabitEthernet** { *port* **|** *port-list* } **]** Verify the OAM configuration.
Step 6	**end** Return to privileged EXEC mode.

Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable OAM and configure the OAM mode as passive on port 1/0/1.

Switch#configure

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

Switch(config-if)#ethernet-oam

Switch(config-if)#ethernet-oam mode passive

Switch(config-if)#show ethernet-oam configuration interface gigabitEthernet 1/0/1

Gi1/0/1

OAM: Enabled

Mode: Passive

...

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.2 Configuring Link Monitoring

With Link Monitoring, the following failure conditions can be reported: Symbol Period Error, Frame Error, Frame Period Error, Frame Seconds Error.

- Configuring Symbol Period Error

With Symbol Period Error enabled, a Symbol Period Error event occurs if the number of symbol errors exceeds the defined threshold within a specific period of time.

Follow these steps to configure Symbol Period Error:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list***}** Enter interface configuration mode.

Step 3	**ethernet-oam link-monitor symbol-period** [**threshold** *threshold*] [**window** *window*] [**notify** {disable | enable}] Configure the relevant parameters of Symbol Period Error. *threshold*: Specify the threshold of received symbol errors within a specific period of time. The valid values are from 1 to 4294967295, and the default value is 1. *window*: Specify specify the period time in 100ms, in which if the received errors exceed the threshold, a link event will be generated. The valid values are from 10*100 to 600*100 ms, and the default value is 10*100 ms. disable | enable: Enable or disable the port to report the failure condition.
Step 4	**show ethernet-oam configuration [interface fastEthernet** { *port* **|** *port-list* } **| interface gigabitEthernet** { *port* **|** *port-list* } **]** Verify the OAM configuration.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable Frame Error notifying and configure the threshold as 1 and the window as 1000 ms (10*100 ms) on port 1/0/1:

Switch#configure

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

Switch(config-if)#ethernet-oam link-monitor symbol-period threshold 1 **window** 10 **notify** enable

Switch(config-if)#show ethernet-oam configuration interface gigabitEthernet 1/0/1

Gi1/0/1

...

Symbol Period Error

Notify State : Enabled

Window : 1000 milliseconds

Threshold : 1 Error Symbol

...

Switch(config-if)#end

Switch#copy running-config startup-config

Configuring Frame Error

With Frame Error enabled, a Frame Error event occurs if the number of frame errors exceeds the defined threshold within a specific period of time.

Follow these steps to configure Frame Error:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list***}** Enter interface configuration mode.
Step 3	**ethernet-oam link-monitor frame [threshold** *threshold* **] [window** *window* **] [notify** {disable | enable}] Configure the relevant parameters of Frame Error. *threshold*: Specify the threshold of received frame errors within a specific period of time. The valid values are from 1 to 4294967295, and the default value is 1. *window*: Specify the period time in 100ms, in which if the number of received errors exceeds the threshold, a link event will be generated. The valid values are from 10*100 to 600*100 ms, and the default value is 10*100 ms. disable | enable: Enable or disable the port to report the failure condition.
Step 4	**show ethernet-oam configuration [interface fastEthernet** { *port* **|** *port-list* } **| interface gigabitEthernet** { *port* **|** *port-list* } **]** Verify the OAM configuration.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable Frame Error notifying and configure the threshold as 1 and the window as 2000 ms (20*100 ms) on port 1/0/1:

Switch#configure

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

Switch(config-if)#ethernet-oam link-monitor frame threshold 1 **window** 20 **notify** enable

Switch(config-if)#show ethernet-oam configuration interface gigabitEthernet 1/0/1

Gi1/0/1

...

Frame Error

Notify State : Enabled

Window : 2000 milliseconds

Threshold : 1 Error Frame

...

Switch(config-if)#end

Switch#copy running-config startup-config

■ Configuring Frame Period Error

With Frame Period Error enabled, a Frame Period Error event occurs if the number of frame errors in specific number of received frames exceeds the defined threshold.

Follow these steps to configure Frame Period Error:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list***}** Enter interface configuration mode.
Step 3	**ethernet-oam link-monitor frame-period** [**threshold** *threshold*] [**window** *window*] [**notify** {disable | enable}] Configure the relevant parameters of Frame Period Error. *threshold*: Specify the threshold of received symbol errors in specific number of received frames. The valid values are from 1 to 4294967295, and the default value is 1. *window*: Specify the number of frames, in which if the frame errors exceed the threshold, a link event will be generated. The valid values are from 148810 to 89286000, and the default value is 1488100. disable | enable: Enable or disable the port to report the failure condition.
Step 4	**show ethernet-oam configuration [interface fastEthernet** { *port* **|** *port-list* } **| interface gigabitEthernet** { *port* **|** *port-list* } **]** Verify the OAM configuration.
Step 5	**end** Return to privileged EXEC mode.

Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable Frame Period Error notifying and configure the threshold as 1 and the window as 1488100 on port 1/0/1:

Switch#configure

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

Switch(config-if)#ethernet-oam link-monitor frame-period threshold 1 **window** 1488100 **notify** enable

Switch(config-if)#show ethernet-oam configuration interface gigabitEthernet 1/0/1

Gi1/0/1

...

Frame Period Error

Notify State : Enabled

Window : 1488100 Frames

Threshold : 1 Error Frame

...

Switch(config-if)#end

Switch#copy running-config startup-config

■ Configuring Frame Seconds Error

With Frame Seconds Error enabled, a Frame Seconds Error event occurs if the number of error frame seconds exceeds the threshold within a specific period of time. A second is called an error frame second if error frames occur in the second.

Follow these steps to configure Frame Seconds Error:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list***}** Enter interface configuration mode.

Step 3	**ethernet-oam link-monitor frame-seconds** [**threshold** *threshold*] [**window** *window*] [**notify** {disable | enable}] Configure the relevant parameters of Frame Period Error. *threshold*: Specify the threshold of received error frame seconds within a specific period of time. The valid values are from 1 to 900, and the default value is 1. *window*: Specify the period time in 100ms, in which if the received errors exceed the threshold, a link event will be generated. The valid values are from 100*100 to 9000*100 ms, and the default value is 600*100 ms. disable | enable : Enable or disable the port to report the failure condition.
Step 4	**show ethernet-oam configuration [interface fastEthernet** { *port* **|** *port-list* } **| interface gigabitEthernet** { *port* **|** *port-list* } **]** Verify the OAM configuration.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable Frame Seconds Error notifying and configure the threshold as 1 and the window as 80000 ms (800*100 ms)on port 1/0/1:

Switch#configure

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

Switch(config-if)#ethernet-oam link-monitor frame-seconds threshold 1 **window** 800 **notify** enable

Switch(config-if)#show ethernet-oam configuration interface gigabitEthernet 1/0/1

Gi1/0/1

...

Frame Seconds Error

Notify State : Enabled

Window : 80000 milliseconds

Threshold : 1 Error Seconds

...

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.3 Configuring Remote Failure Indication

Follow these steps to configure Remote Failure Indication:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list***}** Enter interface configuration mode.
Step 3	**ethernet-oam remote-failure {** dying-gasp | critical-event **} notify {** disable | enable **}** Configure the Dying Gasp Notify and Critical Event Notify features on the port. dying-gasp: Enable Dying Gasp Notify, and if the switch detects an unrecoverable fault on the network, such as power failure, occurs, it will send Information OAMPDU to notify the peer. critical-event: Enable Critical Event Notify, and if the switch detects an unspecified critical event occurs, it will send Information OAMPDU to notify the peer. disable | enable: Enable or disable the port to report the link events.
Step 4	**show ethernet-oam configuration [interface fastEthernet** { *port* **|** *port-list* } **| interface gigabitEthernet** { *port* **|** *port-list* } **]** Verify the OAM configuration.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable Dying Gasp and Critical Event on port 1/0/1:

Switch#configure

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

Switch(config-if)#ethernet-oam dying-gasp **notify** enable

Switch(config-if)#ethernet-oam remote-failure **notify** enable

Switch(config-if)#show ethernet-oam configuration interface gigabitEthernet 1/0/1

Gi1/0/1

...

Dying Gasp : Enabled

Critical Event : Enabled

...

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.4 Configuring Remote Loopback

Follow these steps to configure Remote Loopback:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list***}** Enter interface configuration mode.
Step 3	**ethernet-oam remote-loopback received-remote-loopback {** process | ignore **}** Configure the port to ignore or to process the received remote loopback request.
Step 4	**ethernet-oam remote-loopback {** start | stop **}** Request the remote peer to start or stop the OAM remote loopback mode. The port to be configured here should be in active mode that has established OAM connection with the peer.
Step 5	**show ethernet-oam configuration [interface fastEthernet** { *port* **|** *port-list* } **| interface gigabitEthernet** { *port* **|** *port-list* } **]** Verify the OAM configuration.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to start the OAM remote loopback mode of the peer on port 1/0/1:

Switch#configure

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

Switch(config-if)# ethernet-oam remote-loopback start

2.2.5 Verifying OAM Connection

On privileged EXEC mode or any other configuration mode, you can use the following command to view whether the OAM connection is established with the peer. Additionally, you can view the OAM information of the local entity and the remote entity.

show ethernet-oam status [interface fastEthernet { *port* **|** *port-list* } **| interface gigabitEthernet** { *port* **|** *port-list* } **]**

View the OAM status and the relevant information of the specified port, including the local entity and the remote entity.

The displayed OAM information of the local entity is as follows:

OAM: Displays whether OAM is enabled.

Mode: Displays OAM mode of the local entity.

Max OAMPDU: Displays the maximum size of OAMPDU.

Remote Loopback: Displays whether the local entity supports Remote Loopback.

Unidirection: Displays whether the local entity supports Unidireciton.

Link Monitoring: Displays whether the local entity supports Link Monitoring.

Variable Request: Displays whether the local entity supports Variable Request.

PDU Revision: Displays the PDU Revision of the local entity.

Operation Status: Displays the status of OAM connection, including:

Disable: OAM is disabled on the port.

LinkFault: The link between the local entity and the remote entity is down.

PassiveWait: The port is in passive mode and is waiting to see if the peer device is OAM capable.

ActiveSendLocal: The port is in active mode and is sending local information.

SendLocalAndRemote: The local port has discovered the peer but has not yet accepted or rejected the configuration of the peer.

SendLocalAndRemoteOK: The local device agrees the OAM peer entity.

PeeringLocallyRejected: The local OAM entity rejects the remote peer OAM entity.

PeeringRemotelyRejected: The remote OAM entity rejects the local device.

NonOperHalfDuplex: Ethernet OAM is enabled but the port is in half-duplex operation. You should configure the port as a full-duplex port.

Operational: OAM connection is established with the peer and OAM works normally.

Loopback Status: Displays the loopback status, including:

No Loopback: Neither the local client nor the remote client is in the loopback mode.

Local Loopback: The local client is in the loopback mode.

Remote Loopback: The remote client is in the loopback mode.

The displayed OAM information of the remote entity is as follows:

Mode: Displays OAM mode of the local entity.

MAC Address: Displays the MAC address of the remote entity.

Vendor (OUI): Displays the Vendor's OUI of the remote entity.

Max OAMPDU: Displays the maximum size of OAMPDU.

Remote Loopback: Displays whether the remote entity supports Remote Loopback.

Unidirection: Displays whether the remote entity supports Unidireciton.

Link Monitoring: Displays whether the remote entity supports Link Monitoring.

Variable Request: Displays whether the remote entity supports Variable Request.

PDU Revision: Displays the PDU Revision of the remote entity.

Vendor Information: Displays the vendor information of the remote entity.

The following example shows how to view the OAM status of port 1/0/1:

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

Gi1/0/1

Local Client

OAM : Enabled

Mode : Active

Max OAMPDU : 1518 Bytes

Remote Loopback : Supported

Unidirection : Not Supported

Link Monitoring : Supported

Variable Request : Not Supported

PDU Revision : 1

Operation Status : Operational

Loopback Status : No Loopback

Remote Client

Mode : Passive

MAC Address : 18-A6-F7-DB-63-81

Vendor(OUI) : 000aeb

Max OAMPDU : 1518 Bytes

Remote Loopback : Supported

Unidirection : Not Supported

Link Monitoring : Supported

Variable Request : Not Supported

PDU Revision : 1

Loopback Status : No Loopback

Vendor Information : 00000000

3 Viewing OAM Statistics

You can view the following OAM statistics:

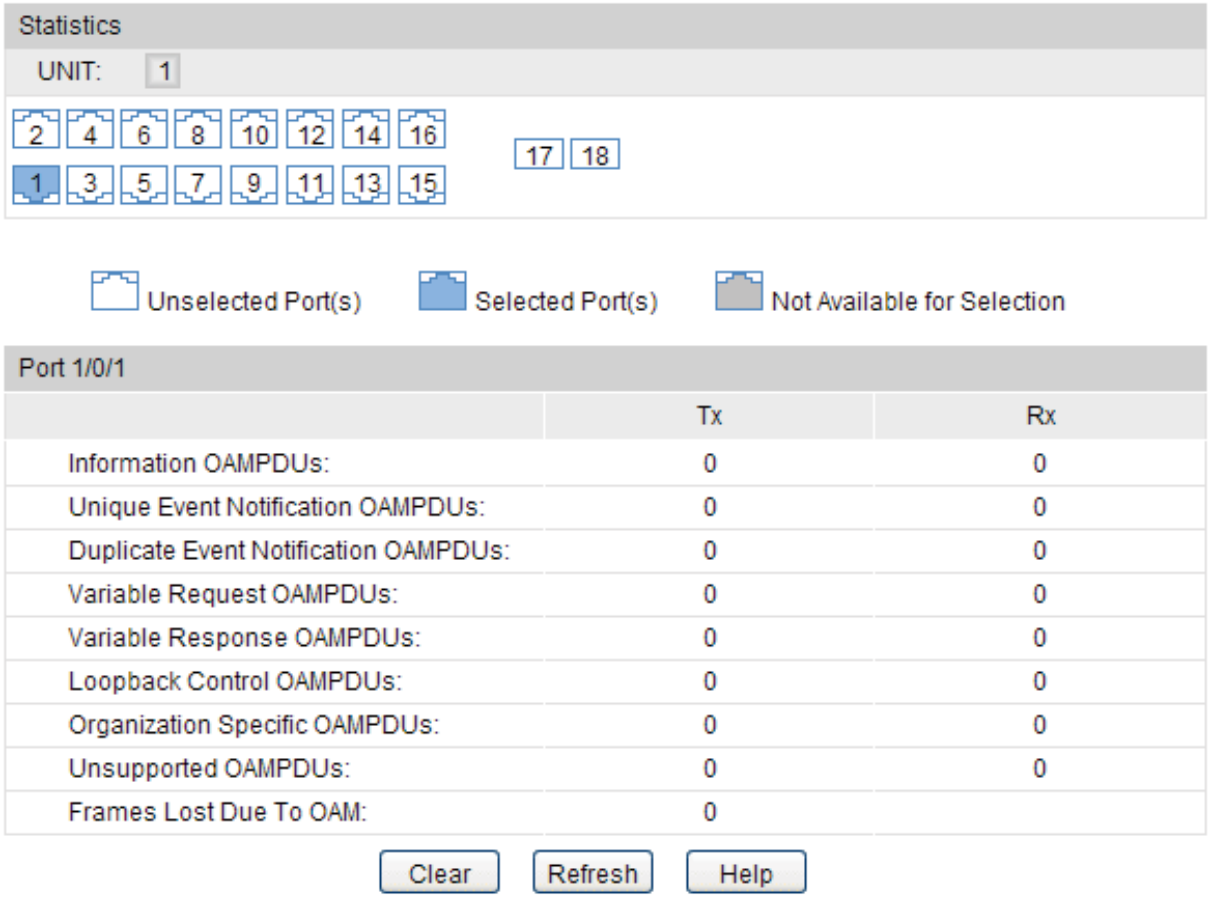
- OAMPDUs
- Event Logs

3.1 Using the GUI

3.1.1 Viewing OAMPDUs

Choose the menu **Ethernet OAM > Statistics > Statistics** to load the following page.

Figure 3-1 OAM Statistics



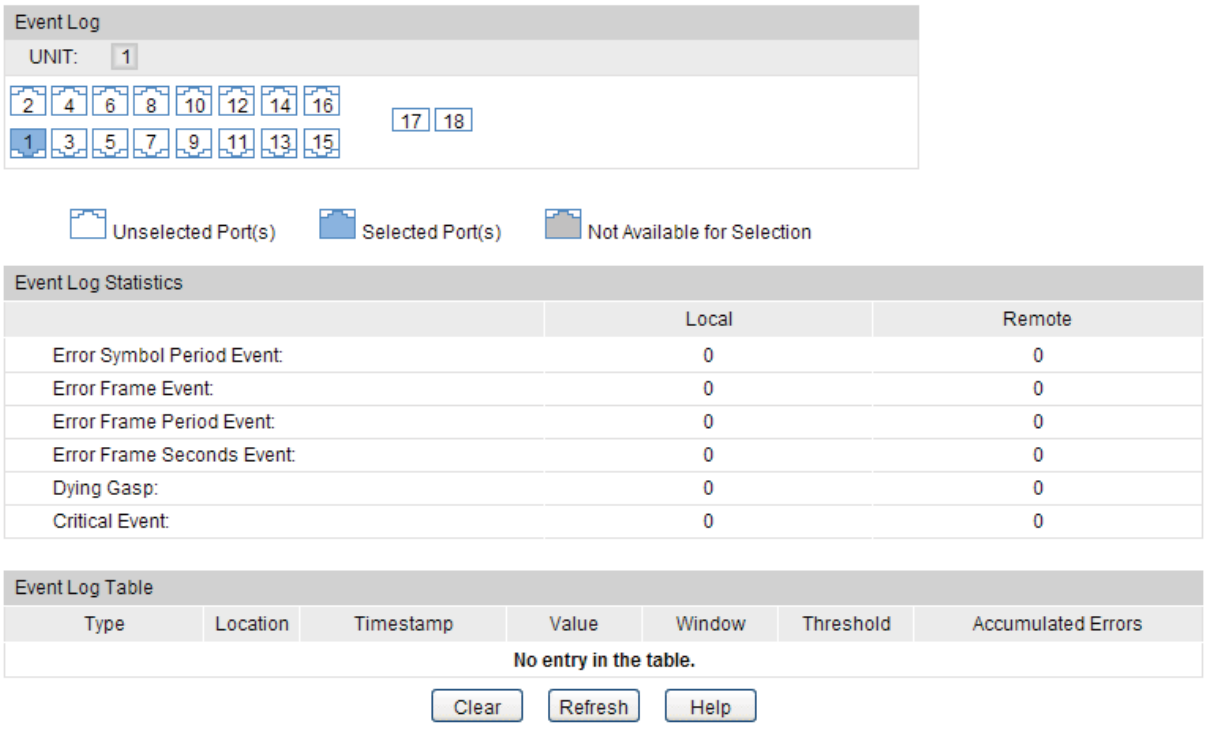
Select a port and view the number of different OAMPDUs transmitted and received on this port:

Tx	Displays the number of OAMPDUs that have been transmitted on the port.
Rx	Displays the number of OAMPDUs that have been received on the port.
Information OAMPDUs	Displays the number of Information OAMPDUs that have been transmitted or received on the port.
Unique Event Notification OAMPDUs	Displays the number of Unique Event Notification OAMPDUs that have been transmitted or received on the port.
Duplicate Event Notification OAMPDUs	Displays the number of Duplicate Event Notification OAMPDUs that have been transmitted or received on the port.
Variable Request OAMPDUs	Displays the number of Variable Request OAMPDUs that have been transmitted or received on the port.
Variable Response OAMPDUs	Displays the number of Variable Response OAMPDUs that have been transmitted or received on the port.
Loopback Control OAMPDUs	Displays the number of Loopback Control OAMPDUs that have been transmitted or received on the port.
Organization Specific OAMPDUs	Displays the number of Organization Specific OAMPDUs that have been transmitted or received on the port.
Unsupported OAMPDUs	Displays the number of Unsupported OAMPDUs that have been transmitted or received on the port.
Frames Lost Due To OAM	Displays the number of frames that are not transmitted successfully on the OAM sublayer but not due to an internal OAM error.

3.1.2 Viewing Event Logs

Choose the menu **Ethernet OAM > Statistics > Event Log** to load the following page.

Figure 3-2 OAM Event Log



Select a port and view the local and remote event logs on this port in the **Event Log Statistics** section:

Local	Displays the number of link events that have occurred on the local link.
Remote	Displays the number of link events that have occurred on the remote link.
Error Symbol Period Event	Displays the number of error symbol period link events that have occurred on the local link or remote link.
Error Frame Event	Displays the number of error frame link events that have occurred on the local link or remote link.
Error Frame Period Event	Displays the number of error frame period link events that have occurred on the local link or remote link.
Error Frame Seconds Event	Displays the number of error frame seconds link events that have occurred on the local link or remote link.
Dying Gasp	Displays the number of Dying Gasp link events that have occurred on the local link or remote link.
Critical Event	Displays the number of Critical Event link events that have occurred on the local link or remote link.

Additionally, you can view the detailed information of the event logs in the **Event Log Table** section.

Type	Displays the type of the link event.
Location	Displays the location where the link event occurred.
Timestamp	Displays the time reference when the link event occurred.
Value	Displays the number of symbol errors or frame errors in the period.
Window	Displays the period of the link event.
Threshold	Displays the threshold of the errors.
Accumulated Errors	Displays the number of errors that have been detected since the OAM feature is reset.

3.2 Using the CLI

3.2.1 Viewing OAMPDUs

On privileged EXEC mode or any other configuration mode, you can use the following command to view the number of OAMPDUs received and sent on the specified port.

show ethernet-oam statistics [interface fastEthernet { *port* | *port-list* } **| interface gigabitEthernet** { *port* | *port-list* } **]**

View the number of different OAMPDUs transmitted and received on the specified port, including Information OAMPDU, Unique Event Notification OAMPDU, Duplicate Event Notification OAMPDU, Loopback Control OAMPDU, Variable Request OAMPDU, Variable Response OAMPDU, Organization Specific OAMPDUs, Unsupported OAMPDU, and Frames Lost Due To OAM (frames that are not transmitted successfully on the OAM sublayer but not due to an internal OAM error).

The following example shows how to view the transmitted and received OAMDPUs on port 1/0/1.

Switch#show ethernet-oam statistics interface gigabitEthernet 1/0/1

Gi1/0/1

Information OAMPDU TX : 28

Information OAMPDU RX : 28

Unique Event Notification OAMPDU TX : 0

Unique Event Notification OAMPDU RX : 0

Duplicate Event Notification OAMPDU TX : 0

Duplicate Event Notification OAMPDU RX : 0

Loopback Control OAMPDU TX : 1

Loopback Control OAMPDU RX : 0

Variable Request OAMPDU TX : 0

Variable Request OAMPDU RX : 0

Variable Response OAMPDU TX : 0

Variable Response OAMPDU RX : 0

Organization Specific OAMPDUs TX : 0

Organization Specific OAMPDUs RX : 0

Unsupported OAMPDU TX : 0

Unsupported OAMPDU RX : 0

Frames Lost Due To OAM : 0

3.2.2 Viewing Event Logs

On privileged EXEC mode or any other configuration mode, you can use the following command to view the local and remote event logs on the specified port.

show ethernet-oam event-log [interface fastEthernet { *port* **|** *port-list* } **| interface gigabitEthernet** { *port* **|** *port-list* } **]**

View the local and remote event logs on the specified port.

An event list will be displayed, including the following information:

Type: Displays the type of the link event.

Location: Displays the location where the link event occurred (local or remote).

Timestamp: Displays the time reference when the link event occurred.

And the number of local and remote event logs will be displayed, including the following events:

Error Symbol Event: Displays the number of error symbol period link events that have occurred on the local link or remote link.

Error Frame Event: Displays the number of error frame link events that have occurred on the local link or remote link.

Error Frame Period Event: Displays the number of error frame period link events that have occurred on the local link or remote link.

Error Frame Seconds Event: Displays the number of error frame seconds link events that have occurred on the local link or remote link.

Dying Gasp: Displays the number of Dying Gasp link events that have occurred on the local link or remote link.

Critical Event: Displays the number of Critical Event link events that have occurred on the local link or remote link.

The following example shows how to view the event logs on port 1/0/1.

Switch#show ethernet-oam event-log interface gigabitEthernet 1/0/1

Gi1/0/1

Event Listing

Type	Location	Time Stamp
Critical Event	Remote	2016-01-01 08:08:00

Local Event Statistics

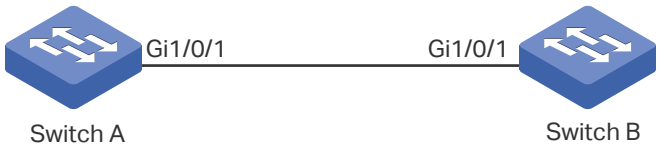
```
        Error Symbol Event          : 0
        Error Frame Event           : 0
        Error Frame Period Event    : 0
        Error Frame Seconds Event   : 0
        Dying Gasp                  : 0
        Critical Event              : 0
    Remote Event Statistics
        Error Symbol Event          : 0
        Error Frame Event           : 0
        Error Frame Period Event    : 0
        Error Frame Seconds Event   : 0
        Dying Gasp                  : 0
        Critical Event              : 1
```

4 Configuration Example

4.1 Network Requirements

A network administrator wants to manage and troubleshoot the network more effectively, requiring that the link failure and frame errors on the link between Switch A and Switch B can be monitored and reported via the Ethernet OAM feature.

Figure 4-1 Network Topology



4.1.1 Configuration Scheme

To meet the requirement, configure OAM on port 1/0/1 of each switch. Two features can be configured: Link Monitoring and Remote Failure Indication. With Link Monitoring, the frame errors on the link can be monitored and reported; with Remote Failure Indication, the link failure can be monitored and reported.

The overview of configuration is as follows:

1) Enable OAM and configure the OAM mode for port 1/0/1 on each switch. Here we configure OAM mode of the port on Switch A as active, and that on switch B as passive.
2) Configure Link Monitoring for port 1/0/1 on each switch.
3) Configure Remote Failure Indication for port 1/0/1 on each switch.

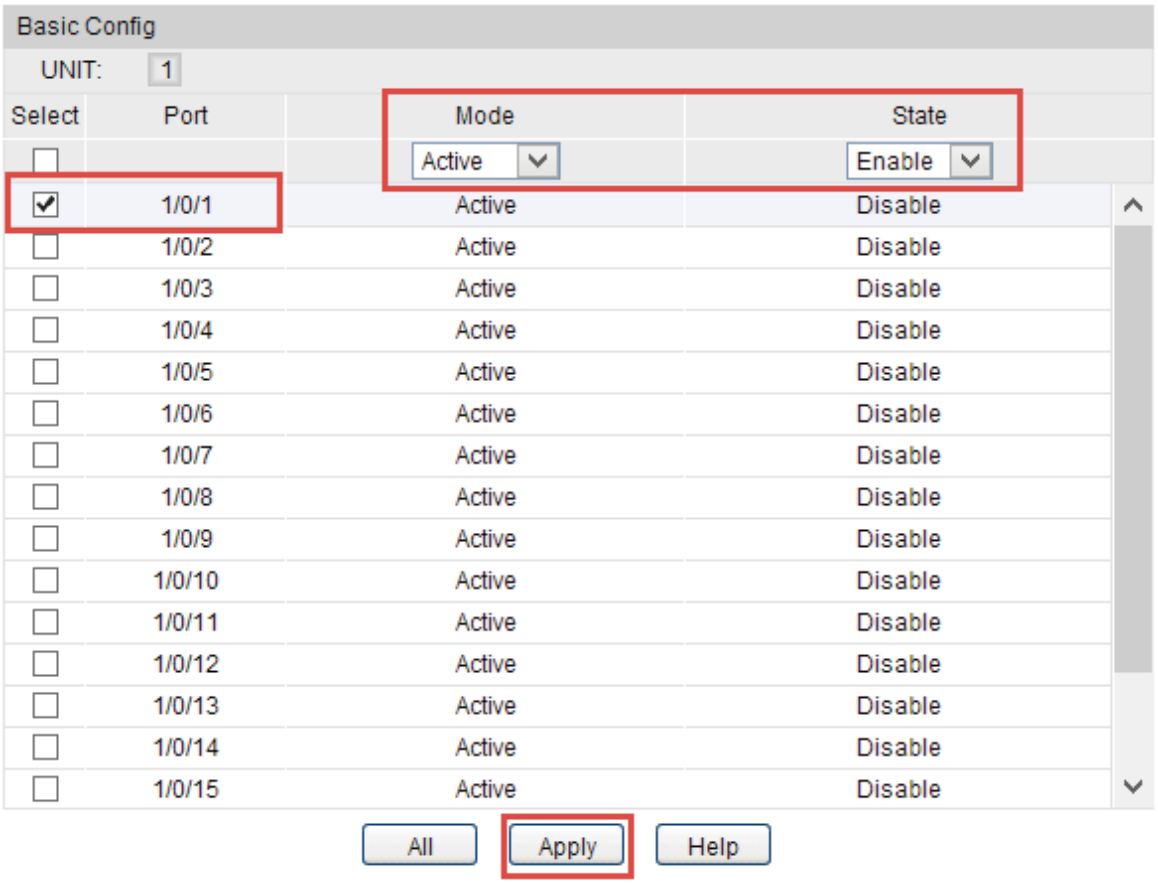
Demonstrated with T2600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

4.1.2 Using the GUI

The configurations for Switch A and Switch B are similar. We take Switch A as an example.

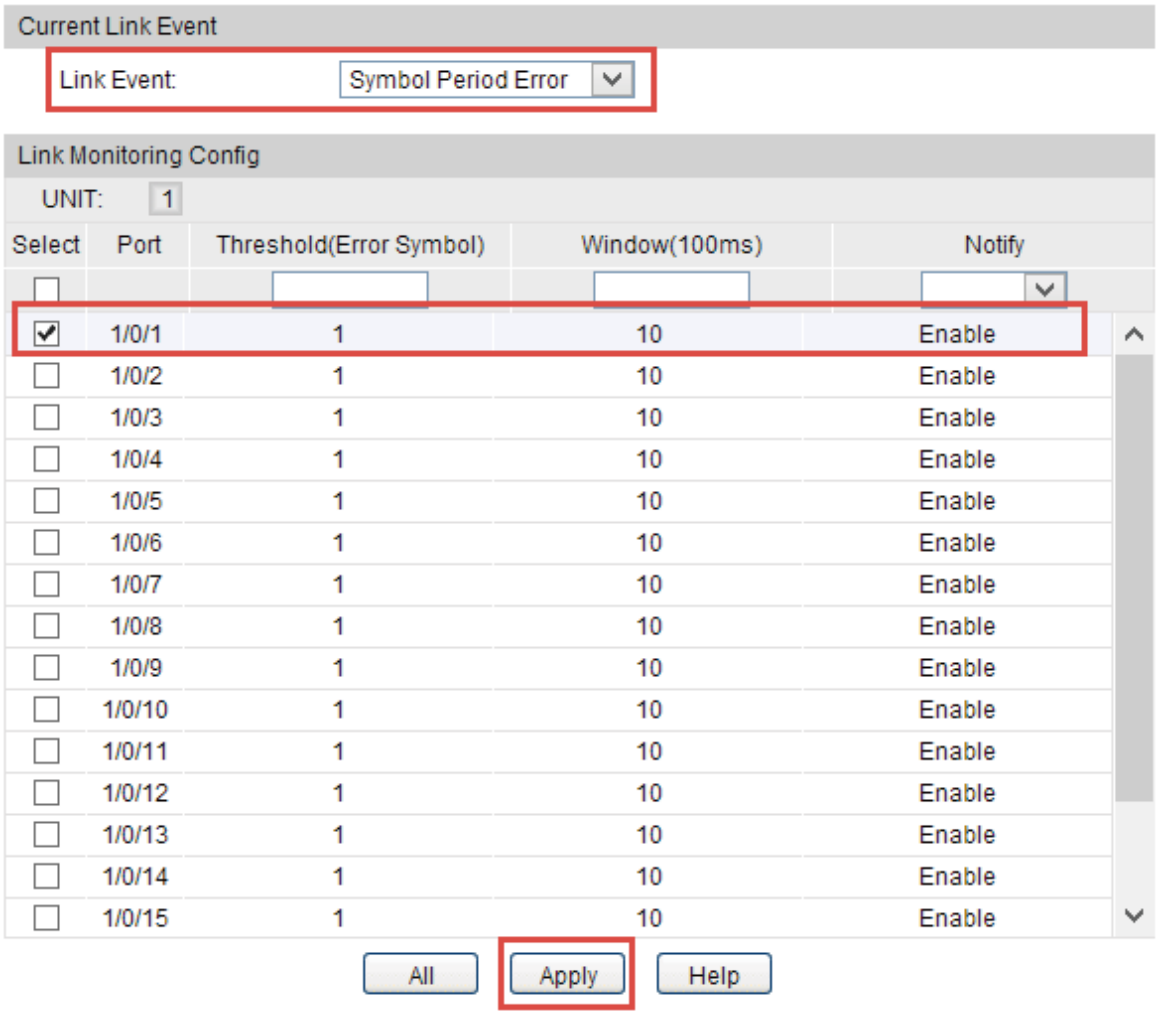
1) Choose the menu **Ethernet OAM > Basic Config > Basic Config** to load the following page. Select port 1/0/1, and configure the mode as Active and the state as Enable. Click **Apply**.

Figure 4-2 Basic Configuration



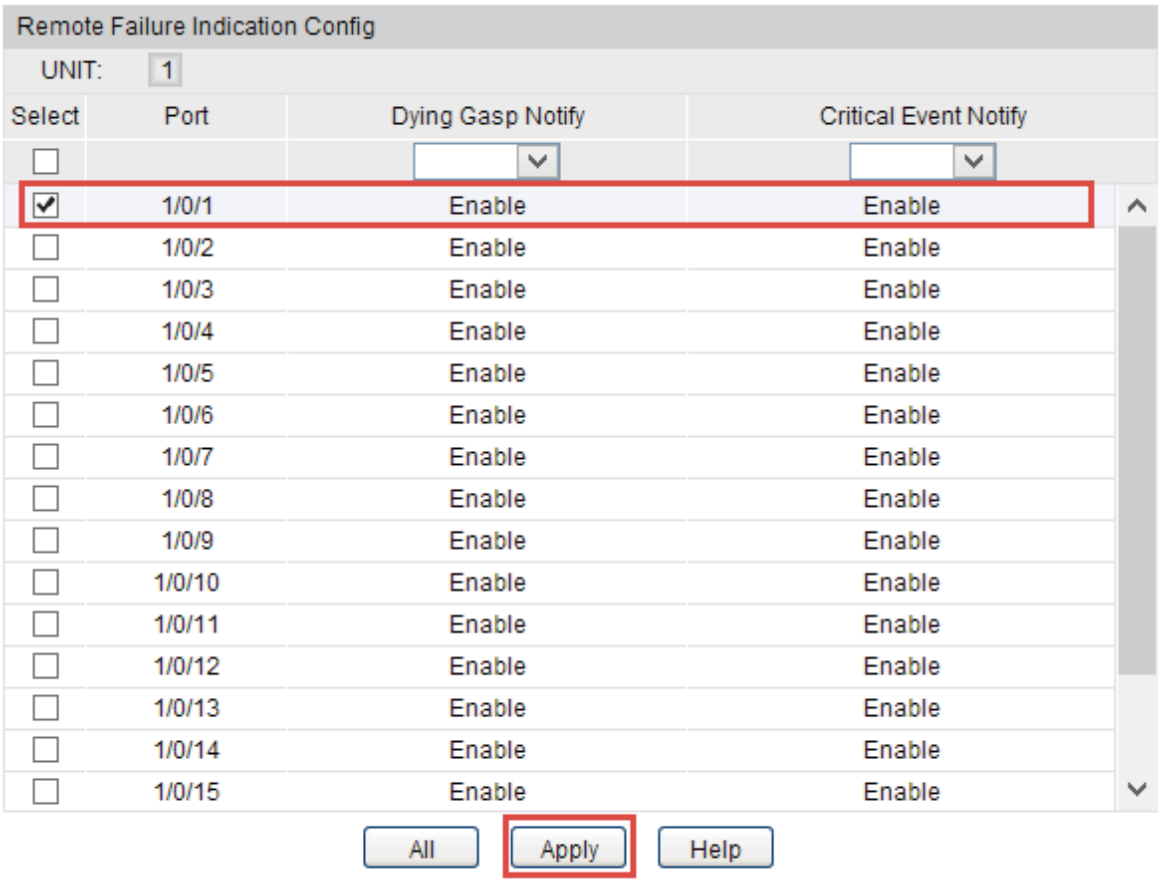
2) Choose the menu **Ethernet OAM > Link Monitoring > Link Monitoring** to load the following page. Select each Link Event type and configure the relevant parameters on port 1/0/1. Make sure that Notify is enabled and specify the threshold and window according to your needs. Here we keep the default parameters. Click **Apply**.

Figure 4-3 Link Monitoring Configuration



3) Choose the menu **Ethernet OAM > RFI > Remote Failure Indication** to load the following page. Select port 1/0/1 and enable Dying Gasp Notify and Critical Event Notify. Click **Apply**.

Figure 4-4 Remote Failure Indication Configuration



4) Choose the menu **Ethernet OAM > Basic Config > Discovery Info** to load the following page. Select port 1/0/1 to check the OAM status. When the connection status becomes **Operational**, it indicates that OAM connection has been established and OAM works normally.

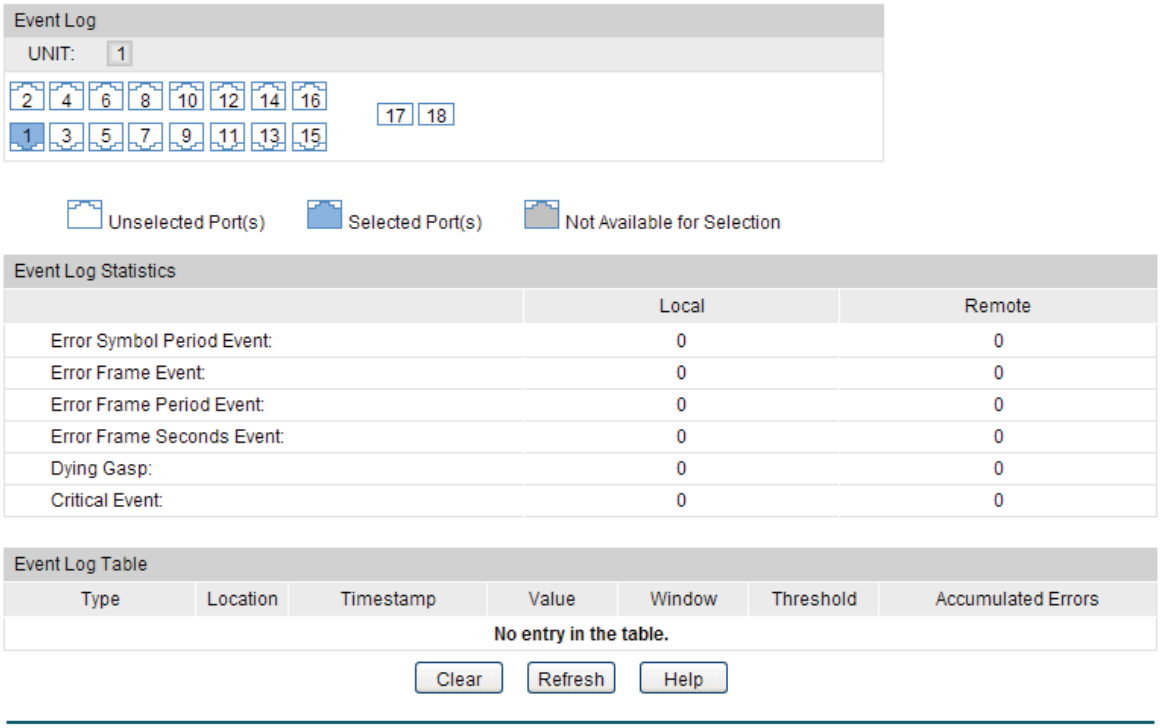
Figure 4-5 Discovery Infomation



5) Click **Save Config** to save the settings.

6) Choose the menu **Ethernet OAM > Statistics > Event Log** to load the following page. Select port 1/0/1 to view the event logs on the port.

Figure 4-6 OAM Event Logs



4.1.3 Using the CLI

1) Enable OAM and configure OAM mode as active on port 1/0/1.

   Switch_A#configure

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

   Switch_A(config-if)# ethernet-oam

   Switch_A(config-if)# ethernet-oam mode active

2) Configure Link Monitoring on the port. Enable event Notify and keep the threshold and window as the default.

   Switch_A(config-if)#ethernet-oam link-monitor symbol-period notify enable

   Switch_A(config-if)#ethernet-oam link-monitor frame-period notify enable

   Switch_A(config-if)#ethernet-oam link-monitor frame notify enable

   Switch_A(config-if)#ethernet-oam link-monitor frame-seconds notify enable

3) Configure Remote Failure Indication on the port. Enable dying gasp and critical event Notify.

   Switch_A(config-if)#ethernet-oam remote-failure critical-event notify enable

   Switch_A(config-if)#ethernet-oam dying-gasp critical-event notify enable

   Switch_A(config-if)#ethernet-oam link-monitor frame-period notify enable

```
Switch_A(config-if)#ethernet-oam link-monitor frame notify enable
Switch_A(config-if)#end
Switch_A#copy running-config startup-config
```

Verify the Configuration

Verify the configuration of OAM:

```
Switch_A#show ethernet-oam configuration interface gigabitEthernet 1/0/1
Gi1/0/1
------------------------------------------------------------
OAM                    : Enabled
Mode                   : Active
Dying Gasp             : Enabled
Critical Event         : Enabled
Remote Loopback OAMPDU  : Not Processed

Symbol Period Error
 Notify State          : Enabled
 Window                : 1000 milliseconds
 Threshold             : 1 Error Symbol

Frame Error
 Notify State          : Enabled
 Window                : 1000 milliseconds
 Threshold             : 1 Error Frame

Frame Period Error
 Notify State          : Enabled
 Window                : 148810 Frames
 Threshold             : 1 Error Frame
```

Frame Seconds Error

Notify State : Enabled

Window : 60000 milliseconds

Threshold : 1 Error Seconds

Verify the OAM connection:

Switch_A#show ethernet-oam status interface gigabitEthernet 1/0/1

Gi1/0/1

Local Client

OAM : Enabled

Mode : Active

Max OAMPDU : 1518 Bytes

Remote Loopback : Supported

Unidirection : Not Supported

Link Monitoring : Supported

Variable Request : Not Supported

PDU Revision : 1

Operation Status : Operational

Loopback Status : No Loopback

Remote Client

Mode : Passive

MAC Address : 18-A6-F7-DB-63-81

Vendor(OUI) : 000aeb

Max OAMPDU : 1518 Bytes

Remote Loopback : Supported

```
Unidirection              : Not Supported
Link Monitoring           : Supported
Variable Request          : Not Supported
PDU Revision              : 1
Loopback Status           : No Loopback
Vendor Information        : 00000000
```

View the OAM event logs:

```
Switch_A#show ethernet-oam event-log interface gigabitEthernet 1/0/1
Gi1/0/1
Event Listing
-------------------------------------------------------------
Type                      Location       Time Stamp
------------------------  -------------  --------------------
Critical Event            Remote         2016-01-01 08:08:00

Local Event Statistics
    Error Symbol Event              : 0
    Error Frame Event               : 0
    Error Frame Period Event        : 0
    Error Frame Seconds Event       : 0
    Dying Gasp                      : 0
    Critical Event                  : 0
Remote Event Statistics
    Error Symbol Event              : 0
    Error Frame Event               : 0
    Error Frame Period Event        : 0
    Error Frame Seconds Event       : 0
    Dying Gasp                      : 0
```

Critical Event : 1

5 Appendix: Default Parameters

Default settings of Ethernet OAM are listed in the following tables.

Table 5-1 Ethernet OAM

Parameter	Default Setting
Basic Config	
Mode	Active
State	Disable
Link Monitoring	
Symbol Period Error	Threshold : 1 Window: 10*100 ms Notify: Enable
Frame Error	Threshold : 1 Window: 10*100 ms Notify: Enable
Frame Period Error	Threshold : 1 Window: 1488100 frames Notify: Enable
Frame Seconds Error	Threshold : 1 Window: 600*100 ms Notify: Enable
Remote Failure Indication	
Dying Gasp Notify	Enable
Critical Event Notify	Enable
Remote Loopback	
Receive Remote Loopback	Ignore
Remote Loopback	None

Part 17

Configuring Layer 2 Multicast

CHAPTERS

1. Layer 2 Multicast
2. IGMP Snooping Configurations
3. Configuring MLD Snooping
4. Viewing Multicast Snooping Configurations
5. Configuration Examples
6. Appendix: Default Parameters

1 Layer 2 Multicast

1.1 Overview

In a point-to-multipoint network, packets can be sent in three ways: unicast, broadcast and multicast. With unicast, many copies of the same information will be sent to all the receivers, occupying a large bandwidth.

With broadcast, information will be sent to all users in the network no matter they need it or not, wasting network resources and impacting information security.

Multicast, however, solves all the problems caused by unicast and broadcast. With multicast, the source only need to send one piece of information, and all and only the users who need the information will receive copies of the information. In a point-to-multipoint network, multicast technology not only transmits data with high efficiency, but also saves a large bandwidth and reduces network load.

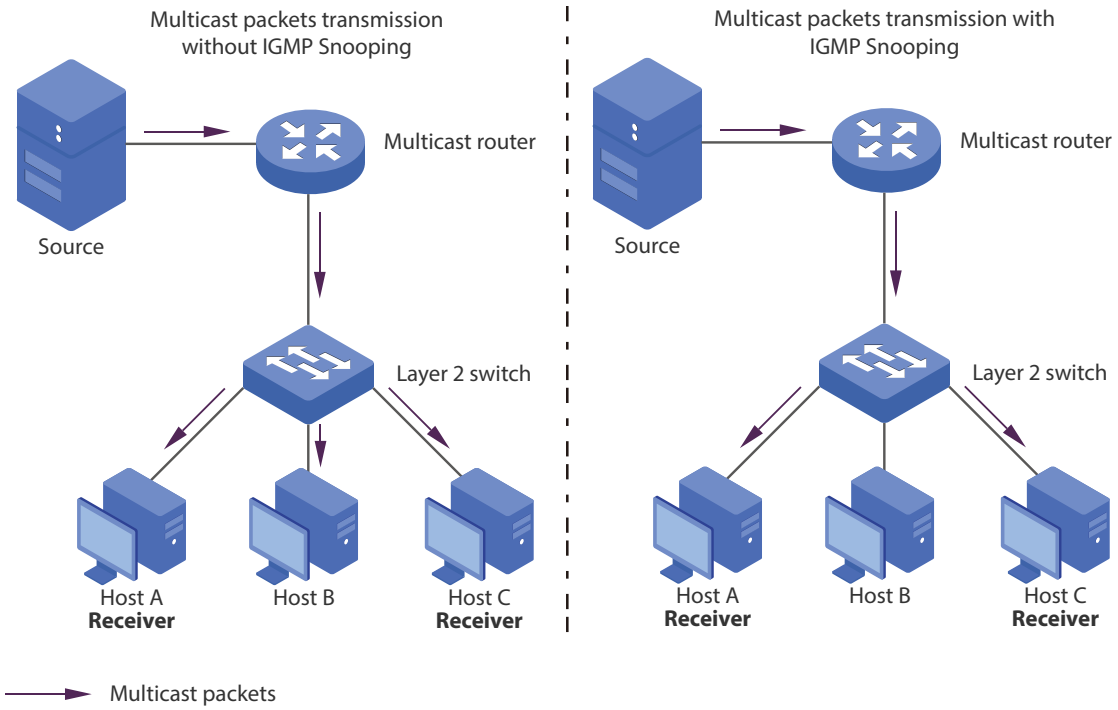
In practical applications, Internet information provider can provide value-added services such as Online Live, IPTV, Distance Education, Telemedicine, Internet Radio and Real-time Video Conferences more conveniently using multicast.

Layer 2 Multicast allows Layer 2 switches to listen for IGMP packets between Layer 3 devices and user hosts to establish multicast forwarding table and to manage and control transmission of packets.

Take IGMP Snooping as an example. When IGMP Snooping is disabled on the Layer 2 device, multicast packets will be broadcast in the Layer 2 network; when IGMP Snooping is enabled on the Layer 2 device, multicast data from a known multicast group will be transmitted to the designated receivers instead of being broadcast in the Layer2 network.

Demonstrated as below:

Figure 1-1 IGMP Snooping



1.2 Supported Layer 2 Multicast Protocols

- Layer 2 Multicast protocol for IPv4: IGMP Snooping

On the Layer 2 device, IGMP Snooping transmits data on demand on data link layer by analyzing IGMP packets between Layer 3 devices and users, to build and maintain Layer 2 multicast forwarding table.

- Layer 2 Multicast protocol for IPv6: MLD Snooping

On the Layer 2 device, MLD Snooping (Multicast Listener Discovery Snooping) transmits data on demand on data link layer by analyzing IGMP packets between Layer 3 devices and users, to build and maintain Layer 2 multicast forwarding table.

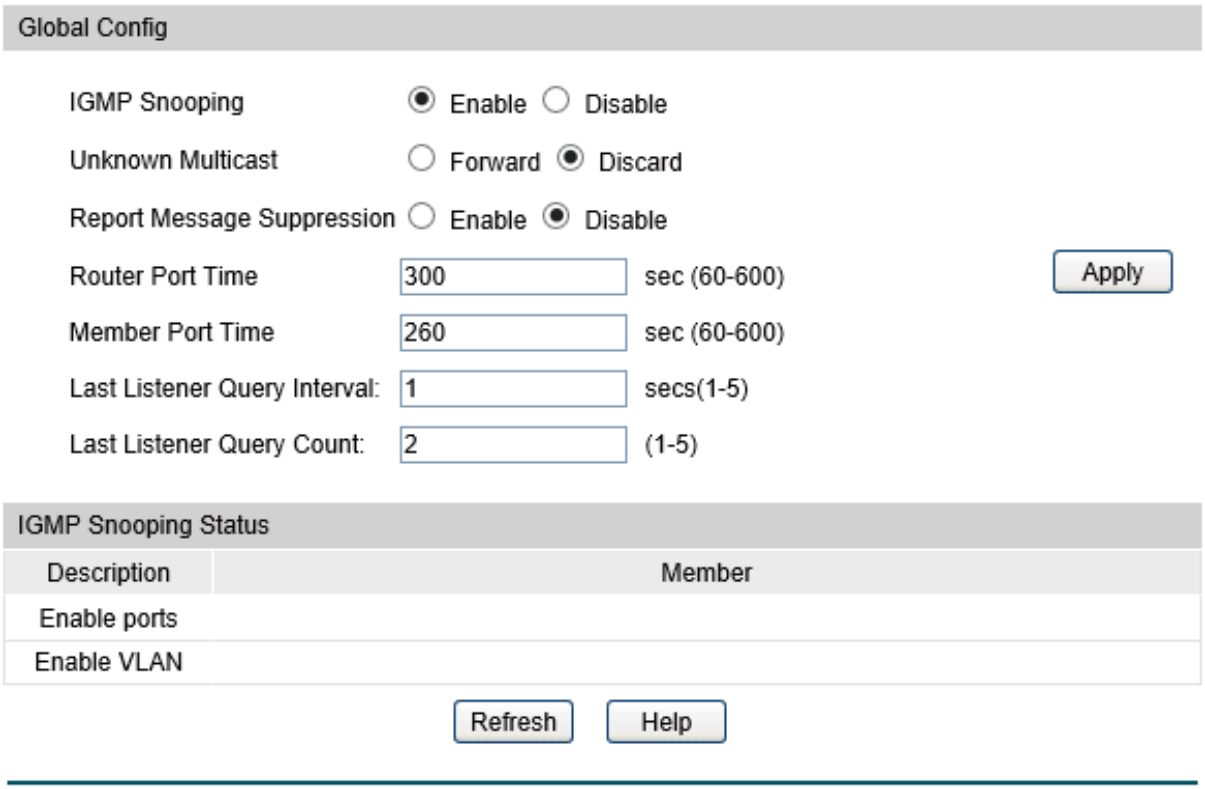
2 IGMP Snooping Configurations

2.1 Using the GUI

2.1.1 Configuring IGMP Snooping Globally

Choose the menu **Multicast > IGMP Snooping > Snooping Config** to load the following page.

Figure 2-1 IGMP Snooping Global Config



Enabling IGMP Snooping Globally

Before configuring functions related to IGMP Snooping, enable IGMP Snooping globally first.

1) Select **Enable** to enable IGMP Snooping globally.
2) Click **Apply**.

(Optional) Configuring Unknown Multicast

Unknown Multicast decides how to process the multicast data when its destination multicast address is not in the multicast forwarding table of the switch.

For switches that support MLD Snooping, IGMP Snooping and MLD Snooping share the setting of Unknown Multicast, so you have to enable MLD Snooping globally on the **Multicast > MLD Snooping > Snooping Config** page at the same time.

Follow these steps to configure unknown multicast.

1) Configure Unknown Multicast as Forward or Discard.

Unknown Multicast	Configure the way how the switch processes the multicast data sent to unknown multicast groups as Forward or Discard. Unknown multicast groups are multicast groups whose destination multicast address is not in the multicast forwarding table of the switch.

2) Click **Apply**.

(Optional) Configuring Report Message Suppression

Enabling Report Message Suppression can reduce the number of packets in the network.

Follow these steps to configure report message suppression.

1) Enable or disable Report Message Suppression globally.

Report Message Suppression	If this function is enabled, the switch will only forward the first IGMP report message to Layer 3 devices and suppress subsequent IGMP report messages from the same multicast group during one query interval, which reduces the number of IGMP packets.

2) Click **Apply**.

Configuring Router Port Time and Member Port Time

Follow these steps to configure the aging time of the router ports and the member ports:

1) Specify the aging time of the router ports.

Router Port Time	Router ports are ports connected to Layer 3 devices on the switch. The router port ages if the switch does not receive IGMP query message from the router port within the router port time. The switch will no longer consider this port as a router port and delete it from the router port table. The valid values are from 60 to 600 seconds.

2) Specify the aging time of the member ports.

Member Port Time	Member ports are ports connected to multicast group members on the switch. A port is considered to be a member port when it is added to a multicast group. The member port ages if the switch does not receive IGMP membership report message from the member port within the member port time. The switch will no longer consider this port as a member port and delete it from the multicast forwarding table. The valid values are from 60 to 600 seconds.

3) Click **Apply**.

Configuring IGMP Snooping Last Listener Query

Configure the Last Listener Query Interval and Last Listener Query Count when the switch receives an IGMP leave message. If specified count of Multicast-Address-Specific Queries (MASQs) are sent and no report message is received, the switch will delete the multicast address from the multicast forwarding table.

Follow these steps to configure Last Listener Query Interval and Last Listener Query Count in the **Global Config** section:

1) Specify the interval between MASQs.

Last Listener Query Interval	When the switch receives an IGMP leave message, the switch obtains the address of the multicast group that the host wants to leave from the message. Then the switch sends out MASQs to this multicast group through the port receiving the leave message. This parameter determines the interval between MASQs. The valid values are from 1 to 5 seconds.

2) Specify the number of MASQs to be sent.

Last Listener Query Count	When the switch receives an IGMP leave message, the switch obtains the address of the multicast group that the host wants to leave from the message. Then the switch sends out MASQs to this multicast group through the port receiving the leave message. This parameter determines the number of MASQs to be sent. The valid values are from 1 to 5.

3) Click **Apply**.

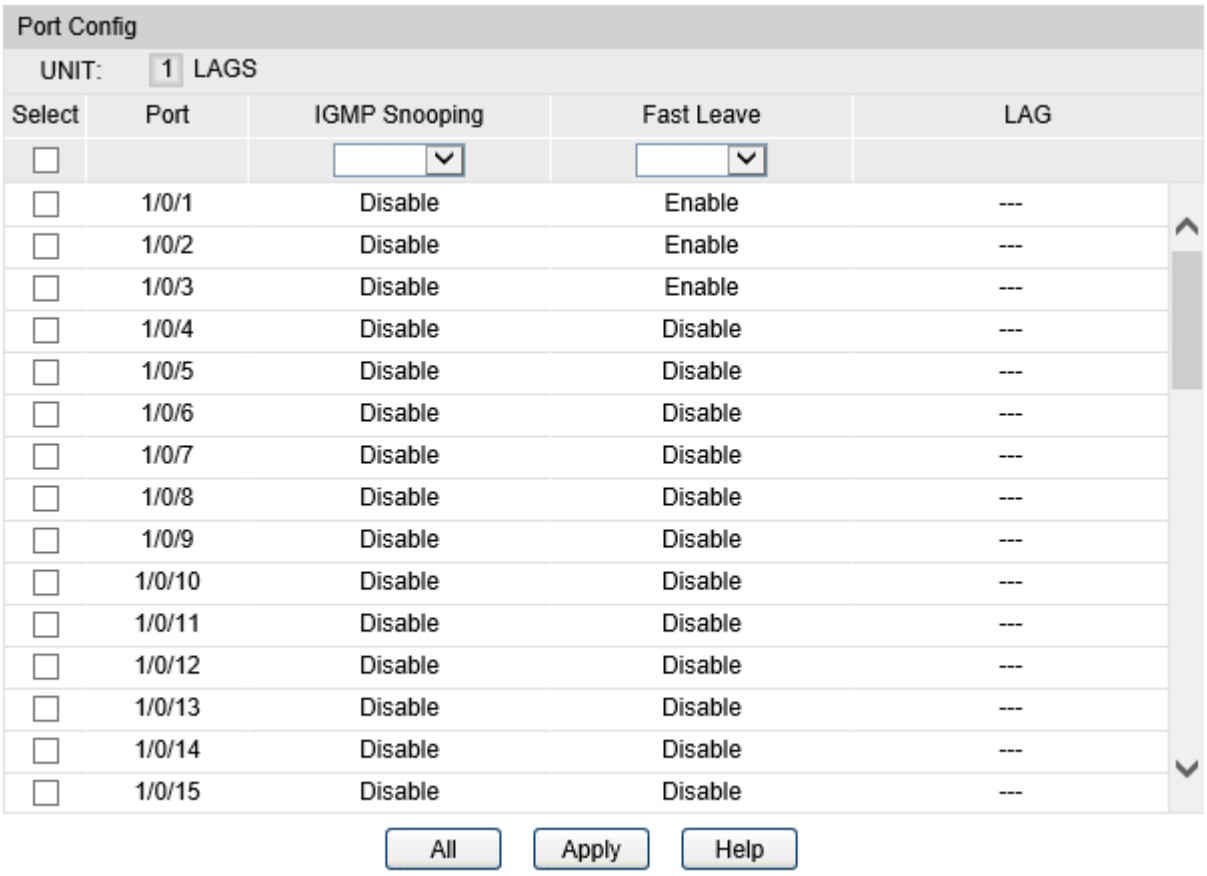
Verifying IGMP Snooping Status

IGMP Snooping Status Table displays VLANs and ports with IGMP Snooping enabled.

2.1.2 Configuring the Port's Basic IGMP Snooping Features

Choose the menu **Multicast > IGMP Snooping > Port Config** to load the following page.

Figure 2-2 Enable IGMP Snooping on Port



Enabling IGMP Snooping on the Port

Follow these steps to enable or disable IGMP Snooping on the port.

1) Select the port to be configured and select **Enable** under the IGMP Snooping column.
2) Click **Apply**.

(Optional) Configuring Fast Leave

With Fast Leave enabled on a port, the switch will remove this port from the forwarding list of the corresponding multicast group once the port receives a leave message. Once deleted, the switch will no longer forward MASQs to this port to verify if there are other members of this multicast group.

Follow these steps to configure fast leave.

1) Select the port to be configured and select **Enable** under the Fast Leave column.

Fast Leave	With Fast Leave enabled on a port, the switch will remove this port from the forwarding list of the corresponding multicast group once the port receives a leave message. You should only use this function when there is a single receiver present on the port.

2) Click **Apply**.

2.1.3 Configuring IGMP Snooping in the VLAN

Choose the menu **Multicast > IGMP Snooping > VLAN Config** to load the following page.

Figure 2-3 IGMP Snooping in VLAN



Configuring IGMP Snooping Globally in the VLAN

In the VLAN Config section, follow these steps to configure relevant parameters for the designate VLAN.

1) Set up the VLAN that the router ports and the member ports are in. For details, please refer to *Configuring 802.1Q VLAN*.

2) Enable IGMP Snooping in the designate VLAN, and configure the aging time of the router ports and the member ports.

VLAN ID	Specify the VLAN to enable IGMP Snooping.

Router Port Time	Specify the aging time of the router ports in the VLAN. If the router port does not receive any IGMP general query message within the router port time, the switch will no longer consider this port as a router port and delete it from the router port list. The valid values are from 60 to 600 seconds. When the router port time is 0, the VLAN uses the global time.
Member Port Time	Specify the aging time of the member ports in the VLAN. If the member port does not receive any IGMP membership report message from the multicast group within the member port time, the switch will no longer consider this port as a member port and delete it from the multicast forwarding table. The valid values are from 60 to 600 seconds. When the member port time is 0, the VLAN uses the global time.

3) Click **Create**.

(Optional) Configuring the Static Router Ports in the VLAN

Follow these steps to configure static router ports in the designate VLAN:

1) Configure the router ports in the designate VLAN.

VLAN ID	Specify the VLAN to be configured.
Static Router Ports	Select one or more ports to be the static router ports in the VLAN. All multicast data in this VLAN will be forwarded through the static router ports.

2) Click **Create**.

(Optional) Configuring the Forbidden Router Ports in the VLAN

Follow these steps to forbid the selected ports to be the router ports in the designate VLAN:

1) Configure the forbidden router ports in the designate VLAN.

VLAN ID	Specify the VLAN to be configured.
Forbidden Router Ports	Select the ports to forbid them from being router ports in the VLAN.

2) Click **Create**.

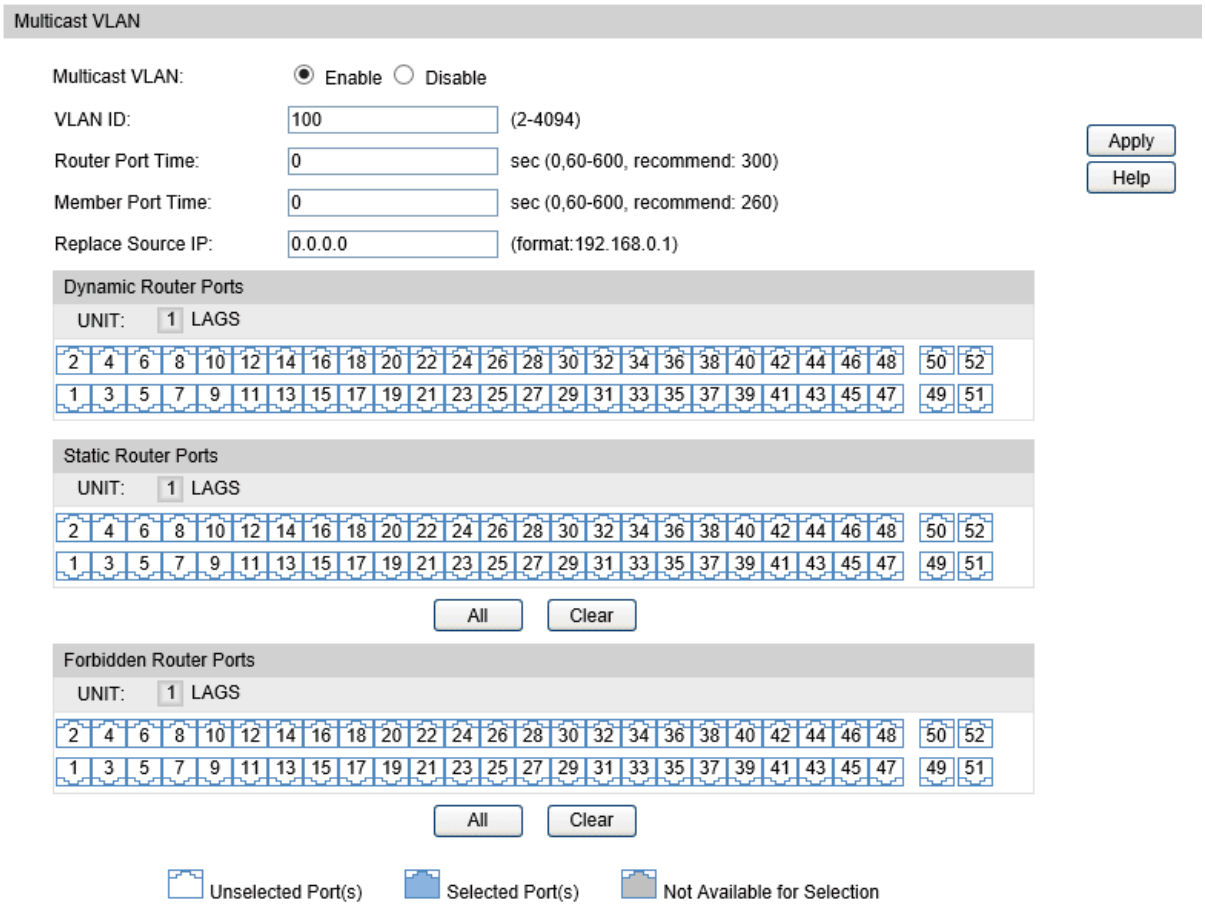
2.1.4 Configuring the Multicast VLAN

In old multicast transmission mode, when users in different VLANs apply for data from the same multicast group, the Layer 3 device will duplicate this multicast data and deliver copies to the Layer 2 devices.

With Multicast VLAN configured, all multicast group members will be added to a VLAN. Layer 3 device only need to send one piece of multicast data to a Layer 2 device, and the Layer 2 device will send the data to all member ports of the VLAN. In this way, Multicast VLAN saves bandwidth and reduces network load of Layer 3 devices.

Choose the menu **Multicast > IGMP Snooping > Multicast VLAN** to load the following page.

Figure 2-4 Multicast VLAN Config



Creating Multicast VLAN and Configuring Basic Settings

In the Multicast VLAN section, follow these steps to enable Multicast VLAN and to finish the basic settings:

1) Set up the VLAN that the router ports and the member ports are in. For details, please refer to *Configuring 802.1Q VLAN*.
2) Enable Multicast VLAN, configure the specific VLAN to be the multicast VLAN, and configure the Router Port Time and Member Port Time.

Multicast VLAN	Select **Enable** to enable multicast VLAN function.
VLAN ID	Specify the 802.1Q VLAN to be the multicast VLAN.
Router Port Time	Specify the aging time of the router ports in the multicast VLAN. If the router port does not receive any IGMP general query message within the router port time, the switch will no longer consider this port as a router port and delete it from the router port table. The valid values are from 60 to 600 seconds. When the router port time is 0, the VLAN uses the global time.

Member Port Time	Specify the aging time of the member ports in the multicast VLAN. If the member port does not receive any IGMP membership report message from the multicast group within the member port time, the switch will no longer consider this port as a member port and delete it from the multicast forwarding table. The valid values are from 60 to 600 seconds. When the member port time is 0, the VLAN uses the global time.

3) Click **Apply**.

(Optional) Creating Replace Source IP

This function allows you to use a new IP instead of the source IP to send data to multicast group members. In the Multicast VLAN section, follow these steps to configure Replace Source IP.

1) Configure the new multicast source IP.

Replace Source IP	Enter the new source IP address. The switch will replace the source IP in the IGMP multicast data sent by the multicast VLAN with the IP address you enter.

2) Click **Apply**.

Viewing Dynamic Router Ports in the Multicast VLAN

This table displays all the dynamic router ports in the multicast VLAN.

(Optional) Configuring the Static Router Ports

Follow these steps to configure static router ports in the multicast VLAN:

1) Configure the router ports in the multicast VLAN.

VLAN ID	Specify the VLAN to be configured.
Static Router Ports	Select one or more ports to be the static router ports in the VLAN. All multicast data in this VLAN will be forwarded through the static router ports.

2) Click **Apply**.

(Optional) Configuring the Forbidden Router Ports

Follow these steps to forbid the selected ports to be the router ports in the multicast VLAN.

1) Configure the router ports in the designate VLAN.

VLAN ID	Specify the VLAN to be configured.
Forbidden Router Ports	Select the ports to forbid them from being router ports in the VLAN.

2) Click **Apply**.

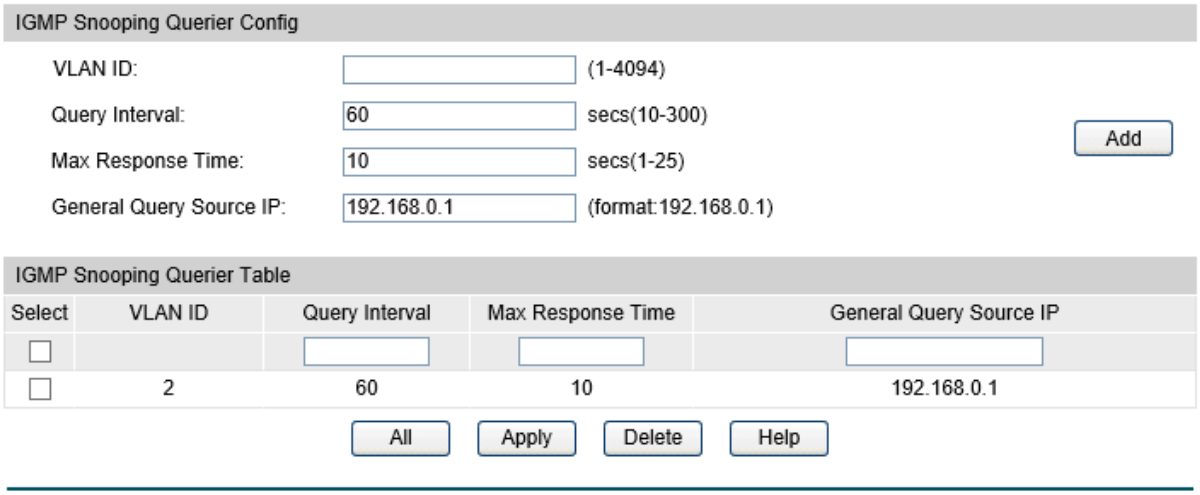
Note:

When configuration is finished, all multicast data through the ports in the VLAN will be processed in this multicast VLAN.

2.1.5 (Optional) Configuring the Querier

IGMP Snooping Querier sends general query packets regularly to maintain the multicast forwarding table. Choose the menu **Multicast > IGMP Snooping > Querier Config** to load the following page.

Figure 2-5 Querier Config



Configuring the Querier

Follow these steps to configure the querier.

1) Specify a VLAN and configure the querier on this VLAN.

VLAN ID	Specify the VLAN to be configured.
Query Interval	Enter the interval between general query messages sent by the querier. The valid values are from 10 to 300 seconds.
Max Response Time	Enter the host's maximum response time to general query messages in a range of 1 to 25 seconds.
General Query Source IP	Specify the source IP address of the general query messages sent by the querier. It cannot be a multicast address or a broadcast address.

2) Click **Add**.

3) You can edit the settings in the IGMP Snooping Querier Table.

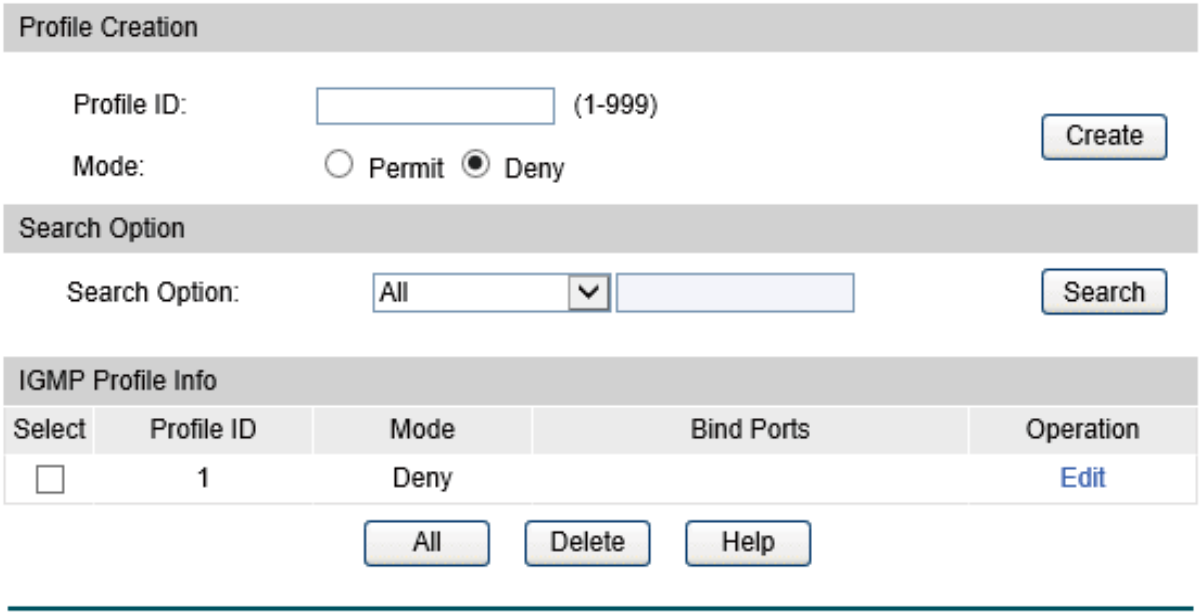
Viewing Settings of IGMP Querier

The IGMP Snooping Querier Table displays all the related settings of the IGMP querier.

2.1.6 Configuring IGMP Profile

With IGMP Profile, the switch can define a blacklist or whitelist of multicast addresses so as to filter multicast sources, Choose the menu **Multicast > IGMP Snooping > Profile Config** to load the following page.

Figure 2-6 Profile Create



Creating Profile

Follow these steps to create a profile and configure its filtering mode.

1) Create a profile and configure its filtering mode.

Profile ID	Enter a profile ID between 1 and 999.
Mode	Select **Permit** or **Deny** as the filtering mode. **Permit**: similar to a whitelist, means that the switch only allows specified member ports to join specific multicast groups. **Deny**: similar to a blacklist, means that the switch disallows specific member ports to join specific multicast groups.

2) Click **Create**.

Searching Profile

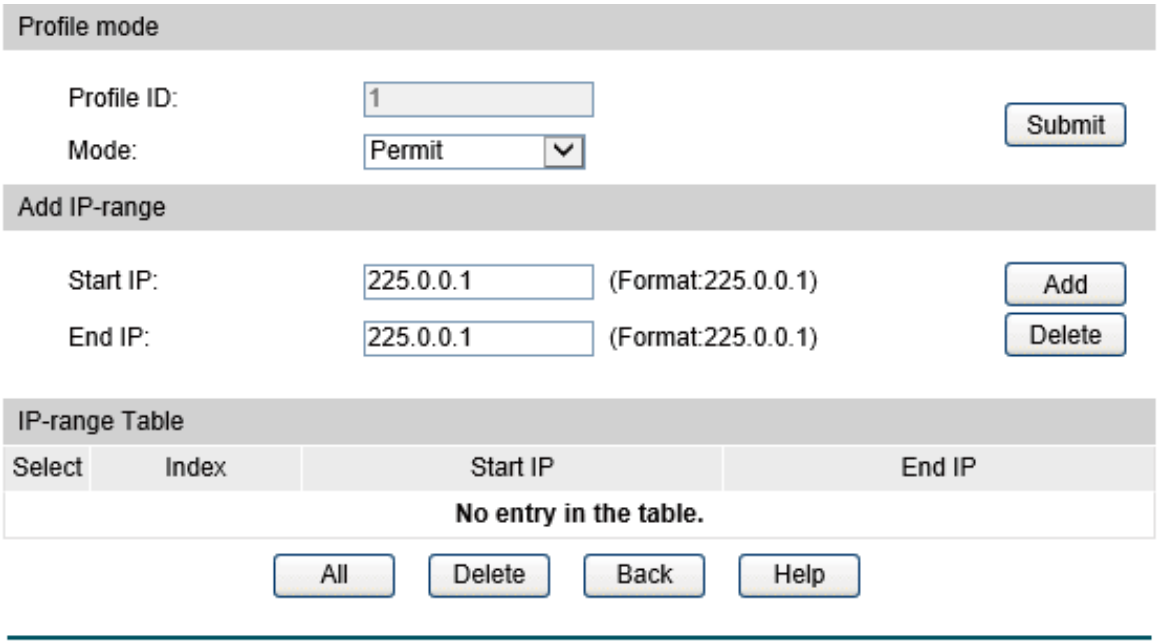
Enter the search condition in the **Search Option** field to search the profile in the IGMP Profile Info table.

Editing IP Range of the Profile

Follow these steps to edit profile mode and its IP range:

1) Click **Edit** in the IGMP Profile Info table. Edit its IP range and click **Add** to save the settings.

Figure 2-7 Add IP-range



Profile ID	Displays the ID of the profile to be edited.
Mode	Select **Permit** or **Deny** as the filtering mode. **Permit**: similar to a whitelist, means that the switch only allows specified member ports to join specific multicast groups. **Deny**: similar to a blacklist, means that the switch disallows specific member ports to join specific multicast groups.
Start IP	Specify the Start IP of the multicast IP range.
End IP	Specify the End IP of the multicast IP range.

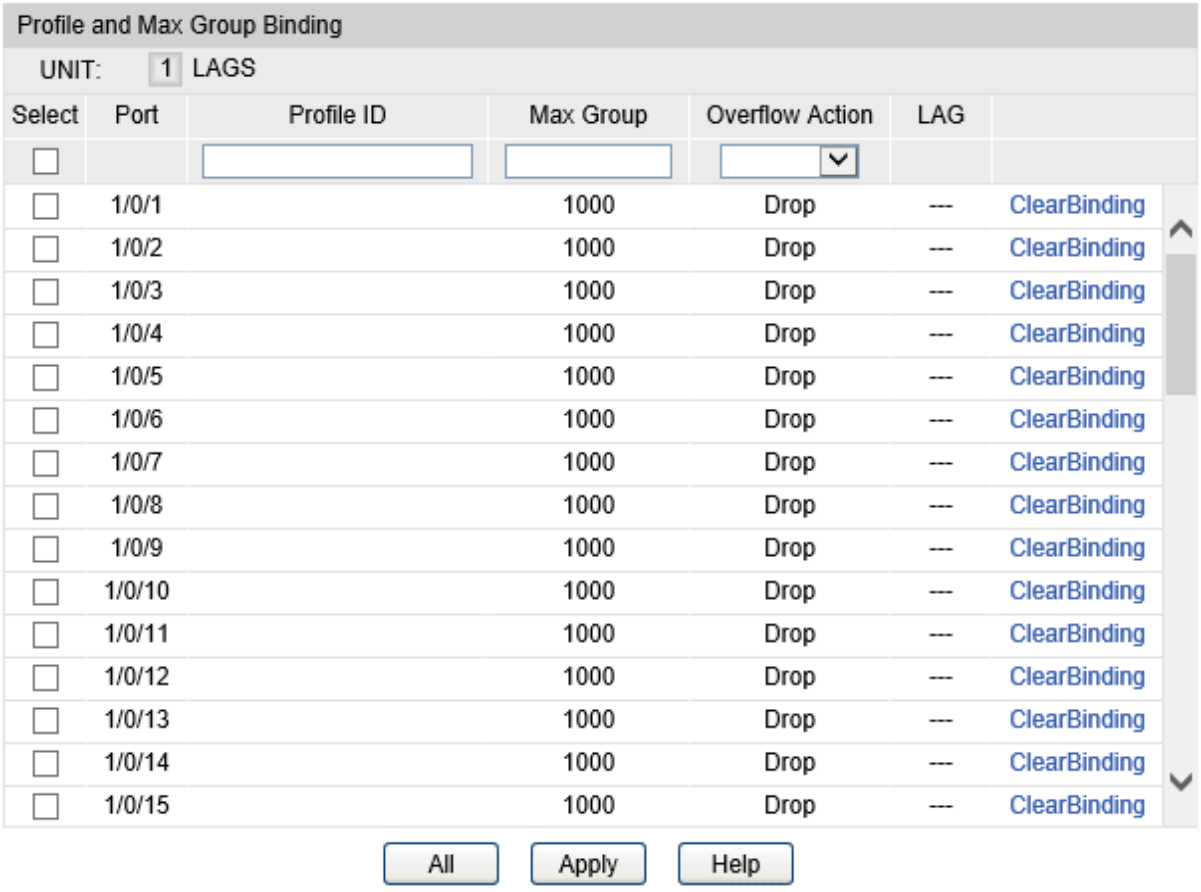
2) In the IP-range Table, you can select an IP range and click **Delete** to delete an IP range.

3) Click **Submit** to save the settings; click **Back** to go back to the previous page.

2.1.7 Binding Profile and Member Ports

With this function, you can configure each port's filtering profile and the number of multicast groups a port can join. Choose the menu **Multicast > IGMP Snooping > Profile Binding** to load the following page.

Figure 2-8 Profile Binding



Binding Profile and Member Ports

Follow these steps to bind the profile to the port.

1) Select the port to be bound, and enter the Profile ID in the **Profile ID** column.

Select	Select the port to be bound.
Port	Displays the port number.
Profile ID	Enter the profile ID you create to bind the profile to the port. One port can only be bound to one profile.
ClearBinding	Click to clear the binding between the profile and the port.

2) Click **Apply**.

Configuring Max Groups a Port Can Join

Follow these steps to configure the maximum groups a port can join and overflow action.

1) Select a port to configure its Max Group and Overflow Action.

Select	Select the port to be configured.

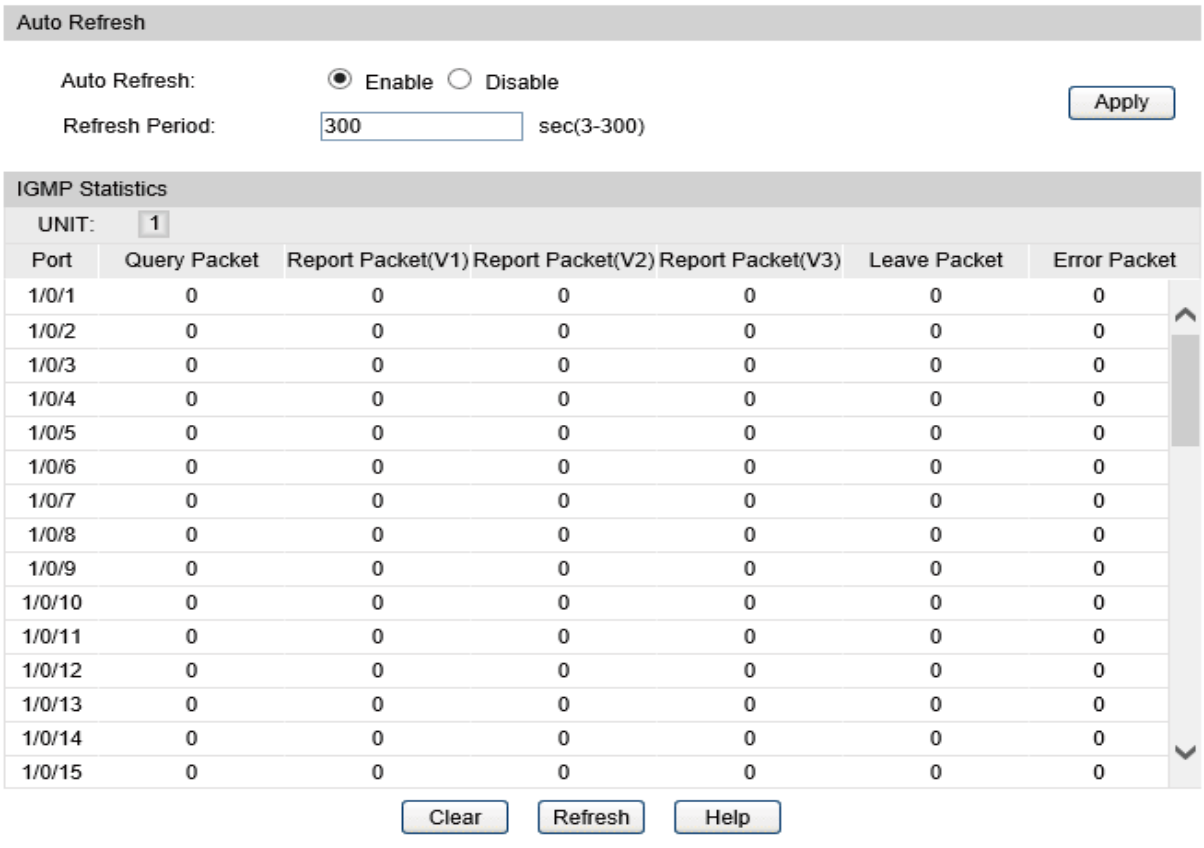
Max Group	Enter the number of multicast groups the port can join. The valid values are from 0 to 1000.
Overflow Action	Select the action towards the new multicast group when the number of multicast groups the port joined exceeds max group. **Drop**: Drop all subsequent membership report messages, and the port will not join any new multicast groups. **Replace**: Replace the existing multicast group owning the lowest multicast MAC address with the new multicast group.

2) Click **Apply**.

2.1.8 Viewing IGMP Statistics on Each Port

Choose the menu **Multicast > IGMP Snooping > Packet Statistic** to load the following page.

Figure 2-9 View IGMP Statistics on the Port



Configuring Auto Refresh

Follow these steps to configure auto refresh.

1) Enable or disable Auto Refresh.

Auto Refresh	If Auto Refresh is enabled, statistics of IGMP packets on this page will refresh automatically.
Refresh Period	After Auto Refresh is enabled, enter the interval between each refresh. The valid values are from 3 to 300 seconds.

2) Click **Apply**.

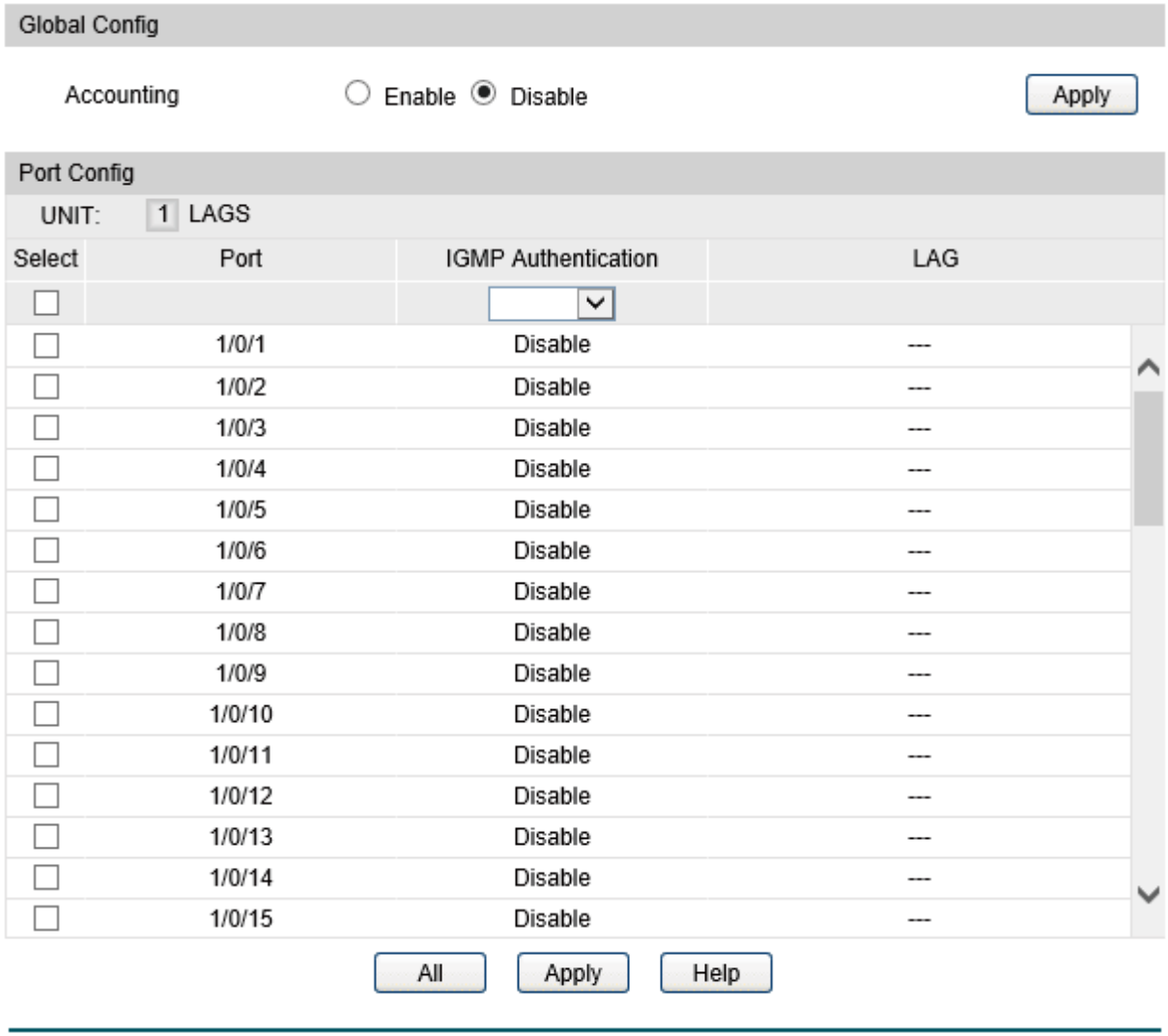
Viewing IGMP Statistics

The IGMP Statistics table displays all kinds of IGMP statistics of all the ports.

2.1.9 Enabling IGMP Accounting and Authentication

Choose the menu **Multicast > IGMP Snooping > IGMP Authentication** to load the following page.

Figure 2-10 IGMP Accounting and Authentication



Configuring IGMP Accounting Globally

To use this function, you should also enable Authentication, Authorization and Accounting (AAA) globally and configure RADIUS server on the switch.

Follow these steps to enable IGMP Accounting globally.

1) Enable IGMP Accounting globally.

Accounting	Select Enable to enable IGMP Snooping accounting.

2) Click **Apply**.

Configuring IGMP Authentication on the Port

To use this function, you should also enable AAA globally and configure RADIUS server on the switch.

Follow these steps to enable IGMP Authentication on the port.

1) Specify the ports and enable IGMP Authentication.

IGMP Authentication	Select one or more ports and select **Enable** in the IGMP Authentication column.

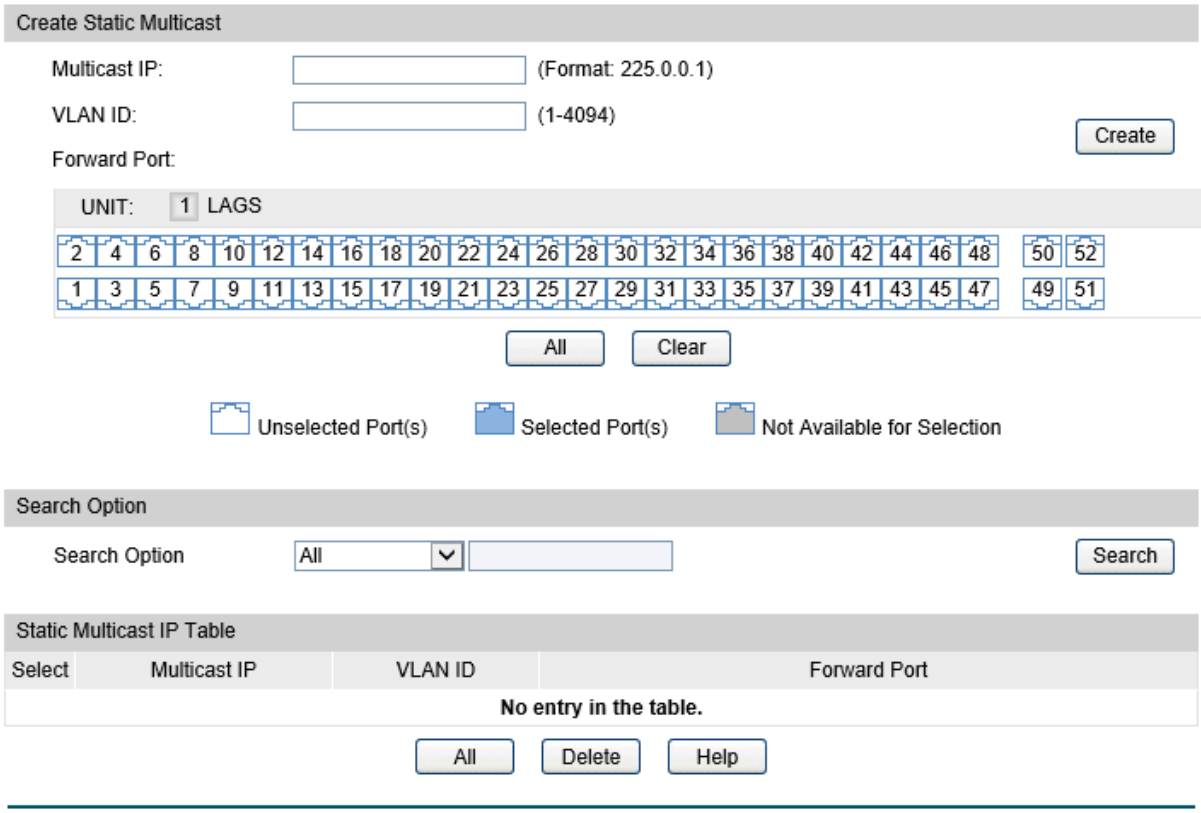
2) Click **Apply**.

2.1.10 Configuring Static Member Port

This function allows you to specify a port as a static member port in the multicast group.

Choose the menu **Multicast > Multicast Table > Static IPv4 Multicast Table** to load the following page.

Figure 2-11 Static Member Port



Configuring Static Member Port

Follow these steps to configure static member port.

1) Enter the Multicast IP and VLAN ID. Specify the Static Member Port.

Multicast IP	Specify the multicast group that the static member is in.
VLAN ID	Specify the VLAN that the static member is in.
Forward Port	Specify one or more ports to be the static member port in the multicast group. Without aging, the static member port receives all multicast data sent to this multicast group.

2) Click **Create**.

Viewing IGMP Static Multicast Groups

You can search IGMP static multicast entries by using Multicast IP, VLAN ID or Forward Port as the Search Option.

Static Multicast IP Table displays details of all IGMP static multicast groups.

2.2 Using the CLI

2.2.1 Enabling IGMP Snooping Globally

Step 1	**configure** Enter global configuration mode.
Step 2	**ip igmp snooping** Enable IGMP Snooping Globally.
Step 3	**end** Return to privileged EXEC mode.
Step 4	**show ip igmp snooping** Show the basic IGMP snooping configuration.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

2.2.2 Enabling IGMP Snooping on the Port

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channe** *port-channel-list***}** Enter interface configuration mode.
Step 3	**ip igmp snooping** Enable IGMP Snooping on the specified port.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**show ip igmp snooping** Show the basic IGMP snooping configuration.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable IGMP Snooping globally and enable IGMP Snooping on port 1/0/3:

Switch#configure

Switch(config)#ip igmp snooping

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

Switch(config-if)#ip igmp snooping

Switch(config-if)#show ip igmp snooping

IGMP Snooping :Enable

Unknown Multicast :Pass

Last Query Times :2

Last Query Interval :1

Global Member Age Time :260

Global Router Age Time :300

Global Report Suppression :Disable

Global Authentication Accounting:Disable

Enable Port:Gi1/0/3

Enable VLAN:

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.3 Configuring IGMP Snooping Parameters Globally

Configuring Report Message Suppression

Step 1	**configure** Enter global configuration mode.
Step 2	**ip igmp snooping report-suppression** Enable Report Message Suppression globally. If this function is enabled, the switch will only forward the first IGMP report message to Layer 3 devices and suppress subsequent IGMP report messages from the same multicast group during one query interval, which reduces the number of IGMP packets.
Step 3	**end** Return to privileged EXEC mode.
Step 4	**show ip igmp snooping** Show the basic IGMP snooping configuration.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable Report Message Suppression:

Switch#configure

Switch(config)#ip igmp snooping

Switch(config)#ip igmp snooping report-suppression

Switch(config)#show ip igmp snooping

IGMP Snooping :Enable

Unknown Multicast :Pass

Last Query Times :2

Last Query Interval :1

Global Member Age Time :260

Global Router Age Time :300

Global Report Suppression :Enable

Global Authentication Accounting:Disable

Enable Port:

Enable VLAN:

Switch(config-if)#end

Switch#copy running-config startup-config

Configuring Unknown Multicast

Step 1	**configure** Enter global configuration mode.
Step 2	**ip igmp snooping drop-unknown** Configure the way how the switch processes the multicast data from unknown multicast groups as Discard. Unknown multicast groups are multicast groups whose destination multicast address is not in the multicast forwarding table of the switch.
Step 3	**end** Return to privileged EXEC mode.
Step 4	**show ip igmp snooping** Show the basic IGMP snooping configuration.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

For switches that support MLD Snooping, IGMP Snooping and MLD Snooping share the setting of Unknown Multicast, so you have to enable MLD Snooping globally at the same time.

The following example shows how to configure the switch to discard unknown multicast data:

Switch#configure

Switch(config)#ip igmp snooping

Switch(config)#ipv6 mld snooping

Switch(config)#ip igmp snooping drop-unknown

Switch(config)#show ip igmp snooping

IGMP Snooping :Enable

Unknown Multicast :Discard

Last Query Times :2

Last Query Interval :1

Global Member Age Time :260

Global Router Age Time :300

Global Report Suppression :Disable

Global Authentication Accounting:Disable

Enable Port:

Enable VLAN:

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.4 Configuring IGMP Snooping Parameters on the Port

Configuring Router Port Time and Member Port Time

Step 1	**configure** Enter global configuration mode.
Step 2	**ip igmp snooping rtime** *rtime* **ip igmp snooping mtime** *mtime* *rtime* is the aging time of router ports, ranging from 60 to 600 seconds. *mtime* is the aging time of member ports, ranging from 60 to 600 seconds.

Step 3	**end** Return to privileged EXEC mode.
Step 4	**show ip igmp snooping** Show the basic IGMP snooping configuration.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the global router port time and member port time as 200 seconds:

Switch#configure

Switch(config)#ip igmp snooping

Switch(config)#ip igmp snooping rtime 200

Switch(config)#ip igmp snooping mtime 200

Switch(config)#show ip igmp snooping

IGMP Snooping :Enable

Unknown Multicast :Pass

Last Query Times :2

Last Query Interval :1

Global Member Age Time :200

Global Router Age Time :200

Global Report Suppression :Disable

Global Authentication Accounting:Disable

Enable Port:

Enable VLAN:

Switch(config-if)#end

Switch#copy running-config startup-config

Configuring Fast Leave

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channe** *port-channel-list***}** Enter interface configuration mode

Step 3	**ip igmp snooping immediate-leave** Enable Fast Leave on the specified port. With Fast Leave enabled on a port, the switch will delete the port-multicast group entry from the multicast forwarding table once the port receives a leave message. You should only use this function when there is a single receiver present on the port.
Step 4	**show ip igmp snooping interface [fastEthernet** [*port* | *port-list*] | **gigabitEthernet** [*port* | *port-list*]] **basic-config** Show the basic IGMP snooping configuration on the specified port(s) or of all the ports.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable Fast Leave on port 1/0/3:

Switch#configure

Switch(config)#ip igmp snooping

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

Switch(config-if)#ip igmp snooping

Switch(config-if)#ip igmp snooping immediate-leave

Switch(config-if)#show ip igmp snooping interface gigabitEthernet 1/0/3 **basic-config**

Port IGMP-Snooping Fast-Leave

---- ------------ ----------

Gi1/0/3 enable enable

Switch(config-if)#end

Switch#copy running-config startup-config

Configuring Max Group and Overflow Action on the Port

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channe** *port-channel-list***}** Enter interface configuration mode
Step 3	**ip igmp snooping max-groups** *maxgroup* Enter the number of multicast groups the port can join. The range is 0 to 1000.

Step 4	**ip igmp snooping max-groups action {**drop	replace**}** Specify the action towards the new multicast group when the number of multicast groups the port joined exceeds max group. drop: Drop all subsequent membership report messages, and the port join no more new multicast groups. replace: Replace the existing multicast group with the lowest multicast MAC address with the new multicast group.
Step 5	**show ip igmp snooping interface [fastEthernet [** *port*	*port-list* **]	gigabitEthernet [** *port*	*port-list* **]] max-groups** Show the IGMP group limitation on the specified port(s) or of all the ports.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the Max Group as 500 and the Overflow Action as Drop on port 1/0/3:

Switch#configure

Switch(config)#ip igmp snooping

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

Switch(config-if)#ip igmp snooping

Switch(config-if)#ip igmp snooping max-groups 500

Switch(config-if)#ip igmp snooping max-groups action drop

Switch(config-if)#show ip igmp snooping interface gigabitEthernet 1/0/3 **max-groups**

Port Max-Groups Overflow-Action

---- ------------ ----------

Gi1/0/3 500 Drop

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.5 Configuring IGMP Snooping Last Listener Query

Step 1	**configure** Enter global configuration mode.

Step 2	**ip igmp snooping last-listener query-inteval** *interval* *interval* determines the interval between MASQs sent by the switch. The valid values are from 1 to 5 seconds.
Step 3	**ip igmp snooping last-listener query-count** *num* *num* determines the number of MASQs sent by the switch. The valid values are from 1 to 5.
Step 4	**show ip igmp snooping** Show the basic IGMP snooping configuration.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the last listener query count as 5 and the last listener query interval as 5 seconds:

Switch#configure

Switch(config)#ip igmp snooping

Switch(config)#ip igmp snooping last-listener query-count 5

Switch(config)#ip igmp snooping last-listener query-interval 5

Switch(config)#show ip igmp snooping

IGMP Snooping :Enable

Unknown Multicast :Pass

Last Query Times :5

Last Query Interval :5

Global Member Age Time :260

Global Router Age Time :300

Global Report Suppression :Disable

Global Authentication Accounting:Disable

Enable Port:

Enable VLAN:

Switch(config)#end

Switch#copy running-config startup-config

2.2.6 Configuring IGMP Snooping Parameters in the VLAN

Configuring Router Port Time and Member Port Time

Step 1	**configure** Enter global configuration mode.
Step 2	**ip igmp snooping vlan-config** *vlan-id-list* **[rtime** *router-time* **| mtime** *member-time***]** *router-time* is the aging time of the router ports in the specified VLAN, ranging from 60 to 600 seconds. *member-time* is the aging time of the member ports in the specified VLAN, ranging from 60 to 600 seconds.
Step 3	**show ip igmp snooping vlan** *vlan-id* Show the basic IGMP snooping configuration in the specified VLAN.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable IGMP Snooping in VLAN 2 and VLAN 3, configure the router port time as 500 seconds and the member port time as 400 seconds:

Switch#configure

Switch(config)#ip igmp snooping

Switch(config)#ip igmp snooping vlan-config 2-3 **rtime** 500

Switch(config)#ip igmp snooping vlan-config 2-3 **mtime** 400

Switch(config)#show ip igmp snooping vlan 2

Vlan Id: 2

Router Time:500

Member Time:400

Static Router Port:None

Dynamic Router Port:None

Forbidden Router Port:None

Switch(config)#show ip igmp snooping vlan 3

Vlan Id: 3

Router Time:500

Member Time:400

Static Router Port:None

Dynamic Router Port:None

Forbidden Router Port:None

Switch(config)#end

Switch#copy running-config startup-config

Configuring Static Router Port

Step 1	**configure** Enter global configuration mode.
Step 2	**ip igmp snooping vlan-config** *vlan-id-list* **[rport interface {gigabitEthernet** *port-list* **| port-channel** *port-channel-id***}]** *port-list* and *port-channel-id* are the static router ports in the specified VLAN.
Step 3	**show ip igmp snooping vlan** *vlan-id* Show the basic IGMP snooping configuration in the specified VLAN.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable IGMP Snooping in VLAN 2 and configure port 1/0/2 as the static router port:

Switch#configure

Switch(config)#ip igmp snooping

Switch(config)#ip igmp snooping vlan-config 2 **rport interface gigabitEthernet** 1/0/2

Switch(config)#show ip igmp snooping vlan 2

Vlan Id: 2

Router Time:0

Member Time:0

Static Router Port:Gi1/0/2

Dynamic Router Port:None

Forbidden Router Port:None

Switch(config)#end

Switch#copy running-config startup-config

Configuring Forbidden Router Port

Step 1	**configure** Enter global configuration mode.
Step 2	**ip igmp snooping vlan-config** *vlan-id-list* **router-ports-forbidden interface {gigabitEthernet** *port-list* **| port-channel** *port-channel-id***}** *port-list* and *port-channel-id* are the ports that cannot become router ports in the specified VLAN.
Step 3	**show ip igmp snooping vlan** *vlan-id* Show the basic IGMP snooping configuration in the specified VLAN.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable IGMP Snooping in VLAN 2 and forbid port 1/0/4-6 from becoming router ports (port 1/0/4-6 will drop all multicast data from Layer 3 devices):

Switch#configure

Switch(config)#ip igmp snooping

Switch(config)#ip igmp snooping vlan-config 2 **router-ports-forbidden interface gigabitEthernet** 1/0/4-6

Switch(config)#show ip igmp snooping vlan 2

Vlan Id: 2

Router Time:0

Member Time:0

Static Router Port:None

Dynamic Router Port:None

Forbidden Router Port:Gi1/0/4-6

Switch(config)#end

Switch#copy running-config startup-config

Configuring Static Multicast (Multicast IP and Forward Port)

Step 1	**configure** Enter global configuration mode.
Step 2	**ip igmp snooping vlan-config** *vlan-id-list* **static** *ip* **interface {gigabitEthernet** *port-list* **| port-channel** *port-channel-id***}** *vlan-id-list* specifies the VLAN to be configured. *ip* specifies the static multicast IP address. *port-list* and *port-channel-id* specify the forward ports (member ports) bound to the static multicast IP address in the specified VLAN.
Step 3	**show ip igmp snooping groups static** Show the static IGMP snooping configuration.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure 226.0.0.2 as the static multicast IP and specify port 1/0/9-10 as the forward ports:

Switch#configure

Switch(config)#ip igmp snooping

Switch(config)#ip igmp snooping vlan-config 2 **static** 226.0.0.2 **interface gigabitEthernet** 1/0/9-10

Switch(config)#show ip igmp snooping groups static

Multicast-ip	VLAN-id	Addr-type	Switch-port
---	---	---	---
226.0.0.2	2	static	Gi1/0/9-10

Switch(config)#end

Switch#copy running-config startup-config

2.2.7 Configuring IGMP Snooping Parameters in the Multicast VLAN

Configuring Router Port Time and Member Port Time

Step 1	**configure** Enter global configuration mode.

Step 2	**ip igmp snooping multi-vlan-config** [*vlan-id*] **[rtime** *router-time* **| mtime** *member-time***]** *vlan-id* specifies the VLAN to be created or to be configured. *router-time* is the aging time of the router ports in the multicast VLAN, ranging from 60 to 600 seconds. *member-time* is the aging time of the member ports in the multicast VLAN, ranging from 60 to 600 seconds.
Step 3	**show ip igmp snooping multi-vlan** Show the IGMP snooping configuration in the multicast VLAN.
Step 4	**end** Return to privileged EXEC mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure VLAN 5 as the multicast VLAN, set the router port time as 500 seconds and the member port time as 400 seconds:

Switch#configure

Switch(config)#ip igmp snooping

Switch(config)#ip igmp snooping multi-vlan-config 5 **rtime** 500

Switch(config)#ip igmp snooping multi-vlan-config 5 **mtime** 400

Switch(config)#show ip igmp snooping multi-vlan

Multicast Vlan:Enable

Vlan Id: 5

Router Time:500

Member Time:400

Replace Source IP:0.0.0.0

Static Router Port:None

Dynamic Router Port:None

Forbidden Router Port:None

Switch(config)#end

Switch#copy running-config startup-config

Configuring Static Router Port

Step 1	**configure** Enter global configuration mode.

Step 2	**ip igmp snooping multi-vlan-config [*vlan-id*] [rport interface {gigabitEthernet *port-list* | port-channel *port-channel-id*}]** *vlan-id* specifies the VLAN to be created or to be configured. *port-list* and *port-channel-id* are the static router ports in the multicast VLAN.
Step 3	**show ip igmp snooping multi-vlan** Show the IGMP snooping configuration in the multicast VLAN.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure VLAN 5 as the multicast VLAN, and set port 1/0/5 as the static router port:

Switch#configure

Switch(config)#ip igmp snooping

Switch(config)#ip igmp snooping multi-vlan-config 5 **rport interface gigabitEthernet** 1/0/5

Switch(config)#show ip igmp snooping multi-vlan

Multicast Vlan:Enable

Vlan Id: 5

Router Time:300

Member Time:260

Replace Source IP:0.0.0.0

Static Router Port:Gi1/0/5

Dynamic Router Port:None

Forbidden Router Port:None

Switch(config)#end

Switch#copy running-config startup-config

Configuring Forbidden Router Port

Step 1	**configure** Enter global configuration mode.

Step 2	**ip igmp snooping multi-vlan-config [***vlan-id***] router-ports-forbidden interface {gigabitEthernet** *port-list* **| port-channel** *port-channel-id***}** *vlan-id* specifies the multicast VLAN to be configured. *port-list* and *port-channel-id* are the ports that cannot become router ports in the multicast VLAN.
Step 3	**show ip igmp snooping multi-vlan** Show the IGMP snooping configuration in the multicast VLAN.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure VLAN 5 as the multicast VLAN, and set port 1/0/6 as the forbidden router port:

Switch#configure

Switch(config)#ip igmp snooping

Switch(config)#ip igmp snooping multi-vlan-config 5 **router-ports-forbidden interface gigabitEthernet** 1/0/6

Switch(config)#show ip igmp snooping multi-vlan

Multicast Vlan:Enable

Vlan Id: 5

Router Time:300

Member Time:260

Replace Source IP:0.0.0.0

Static Router Port:None

Dynamic Router Port:None

Forbidden Router Port:Gi1/0/6

Switch(config)#end

Switch#copy running-config startup-config

Configuring Replace Source IP

Step 1	**configure** Enter global configuration mode.

Step 2	**ip igmp snooping multi-vlan-config [*vlan-id*] replace-sourceip *ip*** *vlan-id* specifies the multicast VLAN to be configured. *ip* specifies the new source IP. The switch will replace the source IP in the IGMP multicast data sent by the multicast VLAN with the IP address you enter.
Step 3	**show ip igmp snooping multi-vlan** Show the IGMP snooping configuration in the multicast VLAN.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure VLAN 5 as the multicast VLAN and replace the source IP in the IGMP packets sent by the switch with 192.168.0.1:

Switch#configure

Switch(config)#ip igmp snooping

Switch(config)#ip igmp snooping multi-vlan-config 5 **replace-sourceip** 192.168.0.1

Switch(config)#show ip igmp snooping multi-vlan

Multicast Vlan:Enable

Vlan Id: 5

Router Time:300

Member Time:260

Replace Source IP:192.168.0.1

Static Router Port:None

Dynamic Router Port:None

Forbidden Router Port:None

Switch(config)#end

Switch#copy running-config startup-config

2.2.8 Configuring the Querier

Enabling IGMP Querier

Step 1	**configure** Enter global configuration mode.

Step 2	**ip igmp snooping querier vlan** *vlan-id* *vlan-id* specifies the VLAN to enable IGMP Querier.
Step 3	**show ip igmp snooping querier** [**vlan** *vlan-id*] Show the IGMP querier configuration.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable IGMP Snooping and IGMP Querier in VLAN 4:

Switch#configure

Switch(config)#ip igmp snooping

Switch(config)#ip igmp snooping querier vlan 4

Switch(config)#show ip igmp snooping querier

VLAN 4:

Maximum Response Time: 10

Query Interval: 60

General Query Source IP: 192.168.0.1

Switch(config)#end

Switch#copy running-config startup-config

Configuring Query Interval, Max Response Time and General Query Source IP

Step 1	**configure** Enter global configuration mode.
Step 2	**ip igmp snooping querier vlan** vlan-id **{query-interval** *interval* **| max-response-time** *response-time* **| general-query source-ip** *ip-addr***}** *vlan-id* specifies the VLAN where the querier is. *interval* is the interval between general query messages sent by the querier. *response-time* is the host's maximum response time to general query messages in a range of 1 to 25 seconds. *ip-addr* is the source IP address of the general query messages sent by the querier. It cannot be a multicast address or a broadcast address.

Step 3	**show ip igmp snooping querier** [**vlan** *vlan-id*] Show the detailed IGMP querier configuration.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable IGMP Snooping and IGMP Querier in VLAN 4, set the query interval as 100 seconds, the max response time as 20 seconds, and the general query source IP as 192.168.0.1:

Switch#configure

Switch(config)#ip igmp snooping

Switch(config)#ip igmp snooping querier vlan 4 **query-interval** 100

Switch(config)#ip igmp snooping querier vlan 4 **max-response-time** 20

Switch(config)#ip igmp snooping querier vlan 4 **general-query source-ip** 192.168.0.1

Switch(config)#show ip igmp snooping querier

VLAN 4:

Maximum Response Time: 20

Query Interval: 100

General Query Source IP: 192.168.0.1

Switch(config)#end

Switch#copy running-config startup-config

2.2.9 Configuring Multicast Filtering

Creating Profile

Step 1	**configure** Enter global configuration mode.
Step 2	**ip igmp profile** *id* Create a new profile and enter profile configuration mode.

Step 3	**permit** **deny** Configure the profile's filtering mode. **permit** is similar to a whitelist, indicating that the switch only allow specific member ports to join specific multicast groups. **deny** is similar to a blacklist, indicating that the switch disallow specific member ports to join specific multicast groups.
Step 4	**range** *start-ip end-ip* Configure the range of multicast IP to be filtered. *start-ip*, *end-ip* are the start IP and end IP of the IP range respectively.
Step 5	**show ip igmp profile** [*id*] Show the detailed IGMP profile configuration.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure Profile 1 so that the switch filters multicast data sent to 226.0.0.5-226.0.0.10:

Switch#configure

Switch(config)#ip igmp snooping

Switch(config)#ip igmp profile 1

Switch(config-igmp-profile)#deny

Switch(config-igmp-profile)#range 226.0.0.5 226.0.0.10

Switch(config-igmp-profile)#show ip igmp profile

IGMP Profile 1

deny

range 226.0.0.5 226.0.0.10

Switch(config)#end

Switch#copy running-config startup-config

Binding Profile to the Port

Step 1	**configure** Enter global configuration mode.

Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channe** *port-channel-list***}** Enter interface configuration mode
Step 3	**ip igmp filter** *profile-id* Bind profile-id to the specified port.
Step 4	**show ip igmp profile** [*id*] Show the detailed IGMP profile configuration.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to bind Profile 1 to port 1/0/2 so that port 1/0/2 filters multicast data sent to 226.0.0.5-226.0.0.10:

Switch#configure

Switch(config)#ip igmp snooping

Switch(config)#ip igmp profile 1

Switch(config-igmp-profile)#deny

Switch(config-igmp-profile)#range 226.0.0.5 226.0.0.10

Switch(config-igmp-profile)#exit

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

Switch(config-if)#ip igmp snooping

Switch(config-if)#ip igmp filter 1

Switch(config-if)#show ip igmp profile

IGMP Profile 1

deny

range 226.0.0.5 226.0.0.10

Binding Port(s)

Gi1/0/2

Switch(config)#end

Switch#copy running-config startup-config

2.2.10 Enabling IGMP Accounting and Authentication

Enabling IGMP Authentication on the Port

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channe** *port-channel-list***}** Enter interface configuration mode
Step 3	**ip igmp snooping authentication** Enable IGMP Authentication on the specified port.
Step 4	**show ip igmp snooping interface [gigabitEthernet** *port***] authentication** Show the IGMP authentication status of the specified port or of all the ports.
Step 6	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable IGMP Authentication on port 1/0/2:

Switch#configure

Switch(config)#ip igmp snooping

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

Switch(config-if)#ip igmp snooping

Switch(config-if)#ip igmp snooping authentication

Switch(config-if)#show ip igmp snooping interface gigabitEthernet 1/0/2 **authentication**

Port IGMP-Authentication

---- -------------

Gi1/0/2 enable

Switch(config)#end

Switch#copy running-config startup-config

Note:

IGMP Authentication takes effect only after AAA is enabled and RADIUS server is configured.

Enabling IGMP Accounting Globally

Step 1	**configure** Enter global configuration mode.
Step 2	**ip igmp snooping accounting** Enable IGMP Accounting globally.
Step 3	**show ip igmp snooping** Show the global IGMP snooping configuration.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

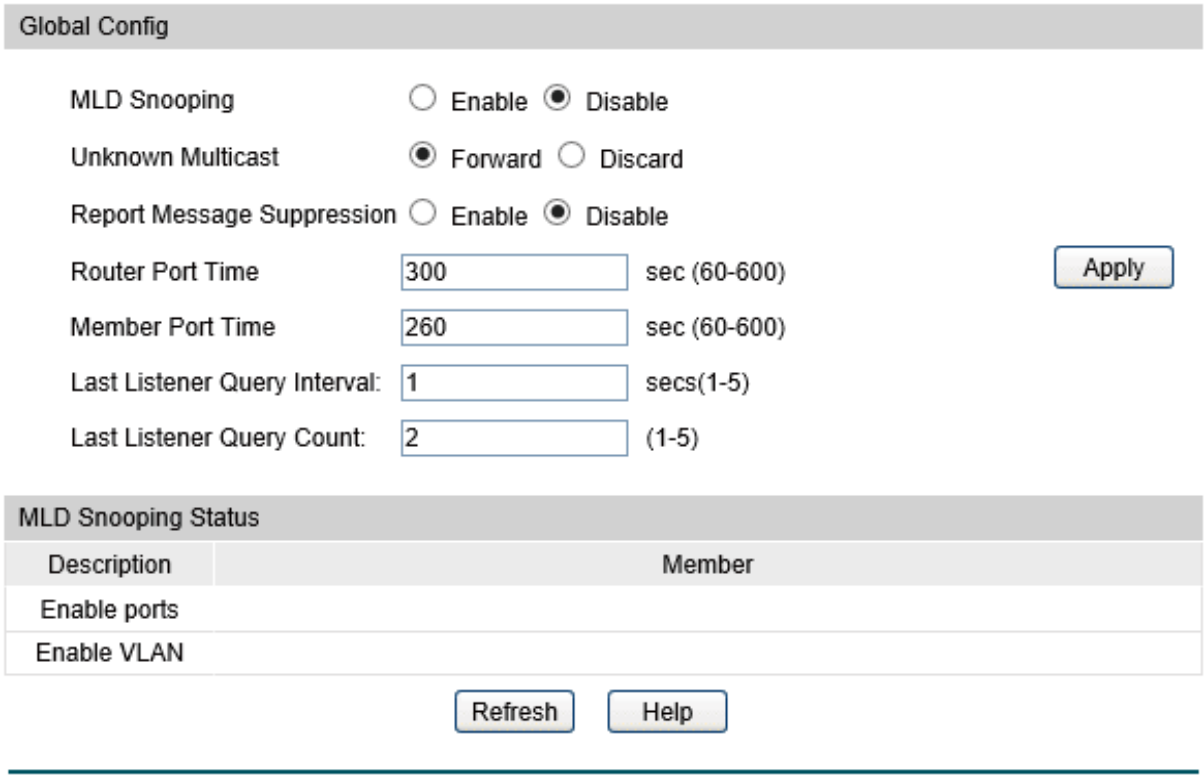
3 Configuring MLD Snooping

3.1 Using the GUI

3.1.1 Configuring MLD Snooping Globally

Choose the menu **Multicast > MLD Snooping > Snooping Config**

Figure 3-1 MLD Snooping Global Config



Enabling MLD Snooping Globally

Before configuring functions related to MLD Snooping, enable MLD Snooping globally first.

1) Select **Enable** to enable MLD Snooping globally.
2) Click **Apply**.

(Optional) Configuring Unknown Multicast

Unknown Multicast decides how to process the multicast data when its destination multicast address is not in the multicast forwarding table of the switch.

IGMP Snooping and MLD Snooping share the setting of Unknown Multicast, so you have to enable IGMP Snooping globally on the **Multicast > IGMP Snooping > Snooping Config** page at the same time.

Follow these steps to configure unknown multicast.

1) Configure Unknown Multicast as Forward or Discard.

Unknown Multicast	Configure the way how the switch processes the multicast data sent to unknown multicast groups as Forward or Discard. Unknown multicast groups are multicast groups whose destination multicast address is not in the multicast forwarding table of the switch.

2) Click **Apply**.

(Optional) Configuring Report Message Suppression

Enabling Report Message Suppression can reduce the number of packets in the network.

Follow these steps to configure report message suppression.

1) Enable or disable Report Message Suppression globally.

Report Message Suppression	If this function is enabled, the switch will only forward the first MLD report message to Layer 3 devices and suppress subsequent MLD report messages from the same multicast group during one query interval, which reduces the number of MLD packets.

2) Click **Apply**.

Configuring Router Port Time and Member Port Time

Follow these steps to configure the aging time of the router ports and the member ports:

1) Specify the aging time of the router ports.

Router Port Time	Router ports are ports connected to Layer 3 devices on the switch. The router port ages if the switch does not receive MLD query message from the router port within the router port time. The switch will no longer consider this port as a router port and delete it from the router port table. The valid values are from 60 to 600 seconds.

2) Specify the aging time of the member ports.

Member Port Time	Member ports are ports connected to multicast group members on the switch. A port is considered to be a member port when it is added to a multicast group. The member port ages if the switch does not receive MLD membership report message from the member port within the member port time. The switch will no longer consider this port as a member port and delete it from the multicast forwarding table. The valid values are from 60 to 600 seconds.

3) Click **Apply**.

Configuring MLD Snooping Last Listener Query

Configure the Last Listener Query Interval and Last Listener Query Count when the switch receives an MLD leave message. If specified count of Multicast-Address-Specific Queries (MASQs) are sent and no report message is received, the switch will delete the multicast address from the multicast forwarding table.

Follow these steps to configure Last Listener Query Interval and Last Listener Query Count in the **Global Config** section:

1) Specify the interval between MASQs.

Last Listener Query Interval	When the switch receives an MLD leave message, the switch obtains the address of the multicast group that the host wants to leave from the message. Then the switch sends out MASQs to this multicast group through the port receiving the leave message. This parameter determines the interval between MASQs. The valid values are from 1 to 5 seconds.

2) Specify the number of MASQs to be sent.

Last Listener Query Count	When the switch receives an MLD leave message, the switch obtains the address of the multicast group that the host wants to leave from the message. Then the switch sends out MASQs to this multicast group through the port receiving the leave message. This parameter determines the number of MASQs to be sent. The valid values are from 1 to 5.

3) Click **Apply**.

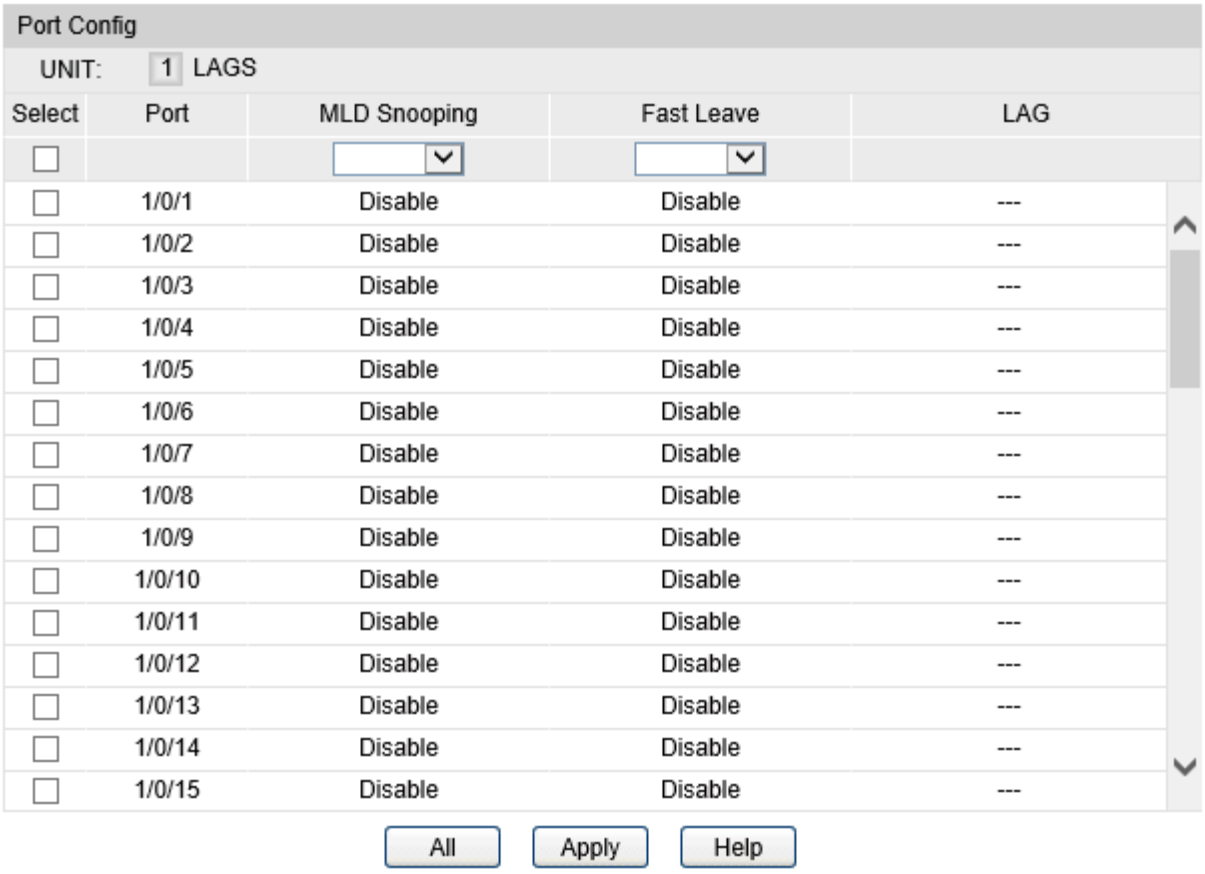
Verifying MLD Snooping Status

MLD Snooping Status Table displays VLANs and ports with MLD Snooping enabled.

3.1.2 Configuring the Port's Basic MLD Snooping Features

Choose the menu **Multicast > MLD Snooping > Port Config** to load the following page.

Figure 3-2 Enable MLD Snooping on Port



Enabling MLD Snooping on the Port

Follow these steps to enable or disable MLD Snooping on the port.

1) Select the port to be configured and select **Enable** under the MLD Snooping column.
2) Click **Apply**.

(Optional) Configuring Fast Leave

With Fast Leave enabled on a port, the switch will remove this port from the forwarding list of the corresponding multicast group once the port receives a leave message. Once deleted, the switch will no longer send MASQs to this port to verify if there are other members of this multicast group.

Follow these steps to configure fast leave.

1) Select the port to be configured and select **Enable** under the Fast Leave column.

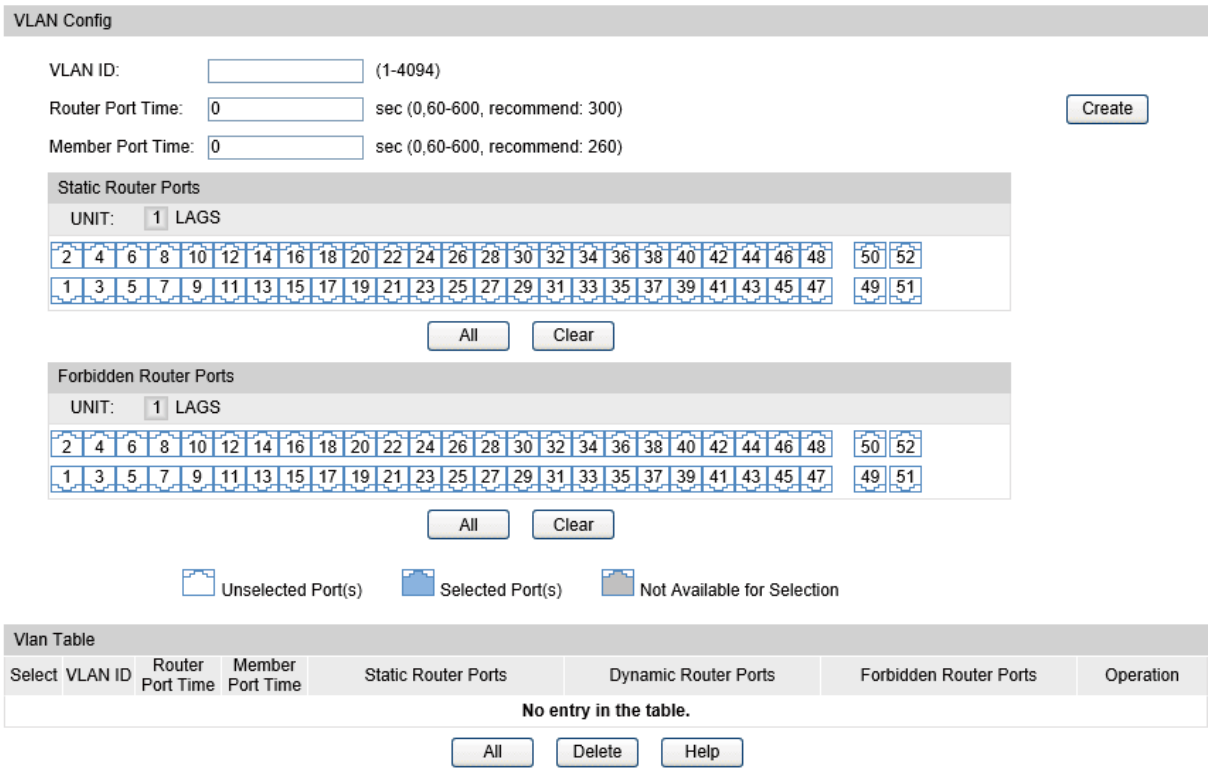
Fast Leave	With Fast Leave enabled on a port, the switch will remove this port from the forwarding list of the corresponding multicast group once the port receives a leave message. You should only use this function when there is a single receiver present on the port.

2) Click **Apply**.

3.1.3 Configuring MLD Snooping in the VLAN

Choose the menu **Multicast > MLD Snooping > VLAN Config** to load the following page.

Figure 3-3 MLD Snooping in VLAN



Configuring MLD Snooping Globally in the VLAN

In the VLAN Config section, follow these steps to configure relevant parameters for the designate VLAN.

1) Set up the VLAN that the router ports and the member ports are in. For details, please refer to *Configuring 802.1Q VLAN*.

2) Enable MLD Snooping in the designate VLAN, and configure the aging time of the router ports and the member ports.

VLAN ID	Specify the VLAN to enable MLD Snooping.

Router Port Time	Specify the aging time of the router ports in the VLAN. If the router port does not receive any MLD general query message within the router port time, the switch will no longer consider this port as a router port and delete it from the router port list. The valid values are from 60 to 600 seconds. When the router port time is 0, the VLAN uses the global time.
Member Port Time	Specify the aging time of the member ports in the VLAN. If the member port does not receive any MLD membership report message from the multicast group within the member port time, the switch will no longer consider this port as a member port and delete it from the multicast forwarding table. The valid values are from 60 to 600 seconds. When the member port time is 0, the VLAN uses the global time.

3) Click **Create**.

(Optional) Configuring the Static Router Ports in the VLAN

Follow these steps to configure static router ports in the designate VLAN:

1) Configure the router ports in the designate VLAN.

VLAN ID	Specify the VLAN to be configured.
Static Router Ports	Select one or more ports to be the static router ports in the VLAN. All multicast data in this VLAN will be forwarded through the static router ports.

2) Click **Create**.

(Optional) Configuring the Forbidden Router Ports in the VLAN

Follow these steps to forbid the selected ports to be the router ports in the designate VLAN:

1) Configure the forbidden router ports in the designate VLAN.

VLAN ID	Specify the VLAN to be configured.
Forbidden Router Ports	Select the ports to forbid them from being router ports in the VLAN.

2) Click **Create**.

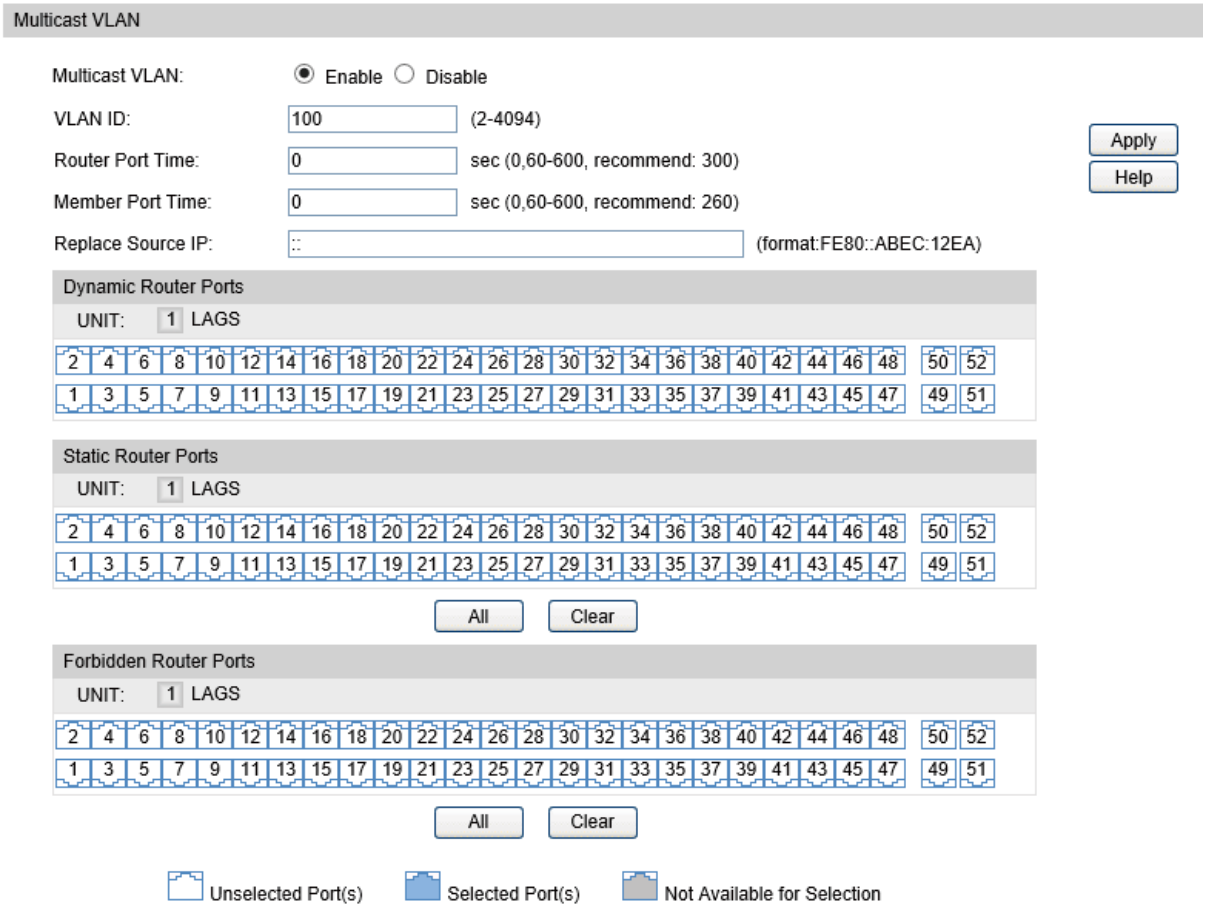
3.1.4 Configuring the Multicast VLAN

In old multicast transmission mode, when users in different VLANs apply for data from the same multicast group, the Layer 3 device will duplicate this multicast data and deliver copies to the Layer 2 devices.

With Multicast VLAN configured, all multicast group members will be added to a VLAN. Layer 3 device only need to send one piece of multicast data to a Layer 2 device, and the Layer 2 device will send the data to all member ports of the VLAN. In this way, Multicast VLAN saves bandwidth and reduces network load of Layer 3 devices.

Choose the menu **Multicast > MLD Snooping > Multicast VLAN** to load the following page.

Figure 3-4 Multicast VLAN Config



Creating Multicast VLAN and Configuring Basic Settings

In the Multicast VLAN section, follow these steps to enable Multicast VLAN and to finish the basic settings:

1) Set up the VLAN that the router ports and the member ports are in. For details, please refer to *Configuring 802.1Q VLAN*.
2) Enable Multicast VLAN, configure the specific VLAN to be the multicast VLAN, and configure the Router Port Time and Member Port Time.

Multicast VLAN	Select **Enable** to enable multicast VLAN function.
VLAN ID	Specify the 802.1Q VLAN to be the multicast VLAN.
Router Port Time	Specify the aging time of the router ports in the multicast VLAN. If the router port does not receive any MLD general query message within the router port time, the switch will no longer consider this port as a router port and delete it from the router port table. The valid values are from 60 to 600 seconds. When the router port time is 0, the VLAN uses the global time.

Member Port Time	Specify the aging time of the member ports in the multicast VLAN. If the member port does not receive any MLD membership report message from the multicast group within the member port time, the switch will no longer consider this port as a member port and delete it from the multicast forwarding table. The valid values are from 60 to 600 seconds. When the member port time is 0, the VLAN uses the global time.

3) Click **Apply**.

(Optional) Creating Replace Source IP

This function allows you to use a new IP instead of the source IP to send data to multicast group members. In the Multicast VLAN section, follow these steps to configure Replace Source IP.

1) Configure the new multicast source IP.

Replace Source IP	Enter the new source IP address. The switch will replace the source IP in the MLD multicast data sent by the multicast VLAN with the IP address you enter.

2) Click **Apply**.

Viewing Dynamic Router Ports in the Multicast VLAN

This table displays all the dynamic router ports in the multicast VLAN.

(Optional) Configuring the Static Router Ports

Follow these steps to configure static router ports in the multicast VLAN:

1) Configure the router ports in the multicast VLAN.

VLAN ID	Specify the VLAN to be configured.
Static Router Ports	Select one or more ports to be the static router ports in the VLAN. All multicast data in this VLAN will be forwarded through the static router ports.

2) Click **Apply**.

(Optional) Configuring the Forbidden Router Ports

Follow these steps to forbid the selected ports to be the router ports in the multicast VLAN.

1) Configure the router ports in the designate VLAN.

VLAN ID	Specify the VLAN to be configured.
Forbidden Router Ports	Select the ports to forbid them from being router ports in the VLAN.

2) Click **Apply**.

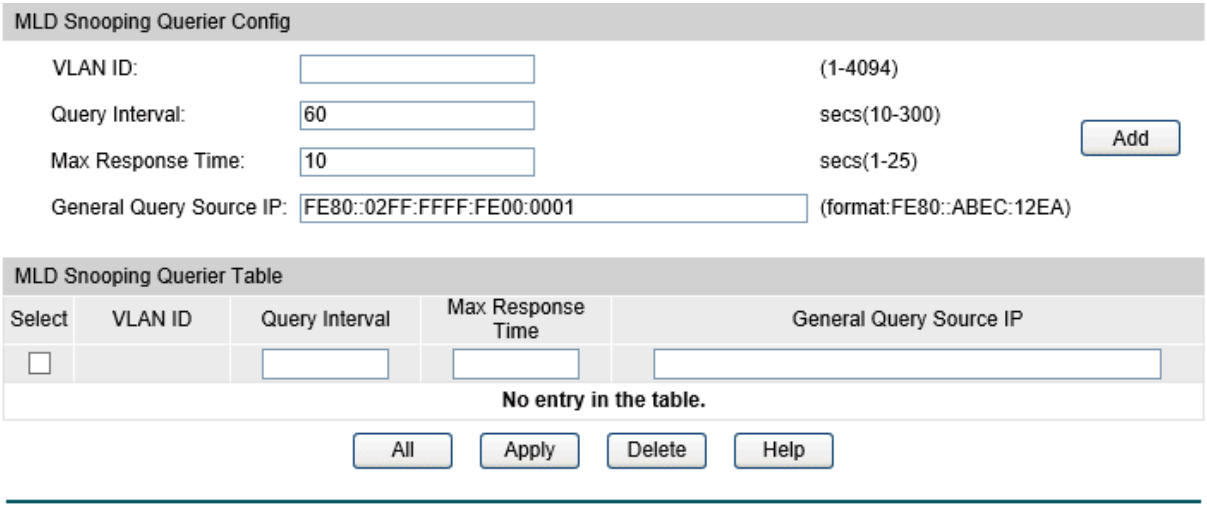
Note:

When configuration is finished, all multicast data through the ports in the VLAN will be processed in this multicast VLAN.

3.1.5 (Optional) Configuring the Querier

MLD Snooping Querier sends general query packets regularly to maintain the multicast forwarding table. Choose the menu **Multicast > MLD Snooping > Querier Config** to load the following page.

Figure 3-5 Querier Config



Configuring the Querier

Follow these steps to configure the querier.

1) Specify a VLAN and configure the querier on this VLAN.

VLAN ID	Specify the VLAN to be configured.
Query Interval	Enter the interval between general query messages sent by the querier. The valid values are from 10 to 300 seconds.
Max Response Time	Enter the host's maximum response time to general query messages in a range of 1 to 25 seconds.
General Query Source IP	Specify the source IP address of the general query messages sent by the querier. It cannot be a multicast address or a broadcast address.

2) Click **Add**.

3) You can edit the settings in the MLD Snooping Querier Table.

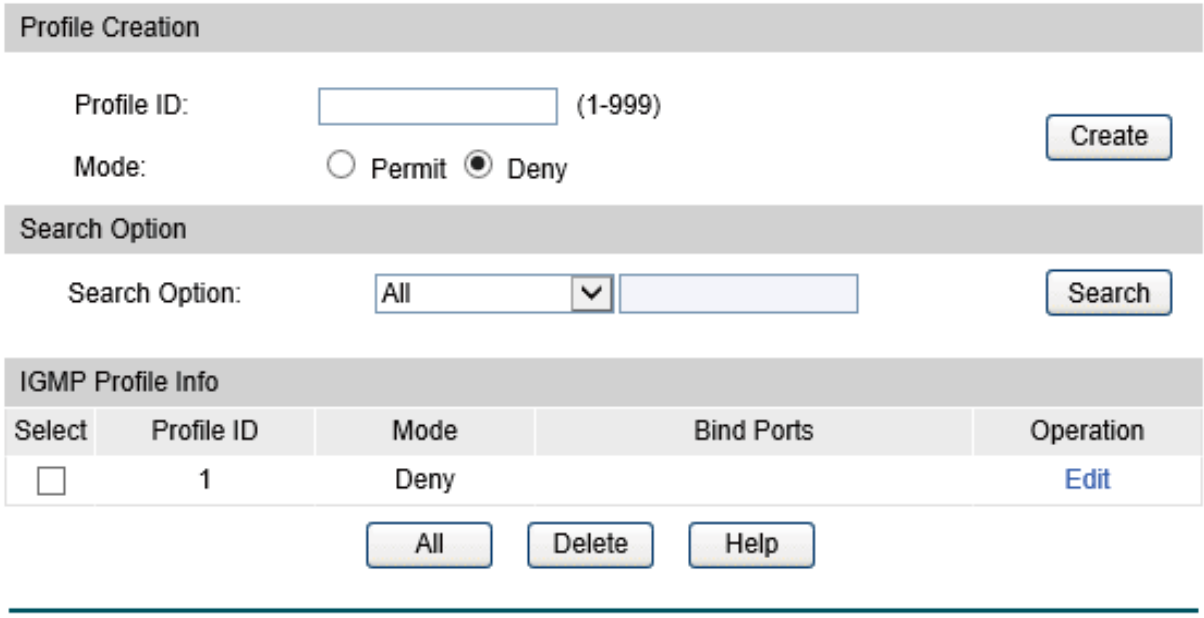
Viewing Settings of MLD Querier

The MLD Snooping Querier Table displays all the related settings of the MLD querier.

3.1.6 Configuring MLD Profile

With MLD Profile, the switch can define a blacklist or whitelist of multicast addresses so as to filter multicast sources, Choose the menu **Multicast > MLD Snooping > Profile Config** to load the following page.

Figure 3-6 Profile Create



Creating Profile

Follow these steps to create a profile and configure its filtering mode.

1) Create a profile and configure its filtering mode.

Profile ID	Enter a profile ID between 1 and 999.
Mode	Select **Permit** or **Deny** as the filtering mode. **Permit**: similar to a whitelist, means that the switch only allows specified member ports to join specific multicast groups. **Deny**: similar to a blacklist, means that the switch disallows specific member ports to join specific multicast groups.

2) Click **Create**.

Searching Profile

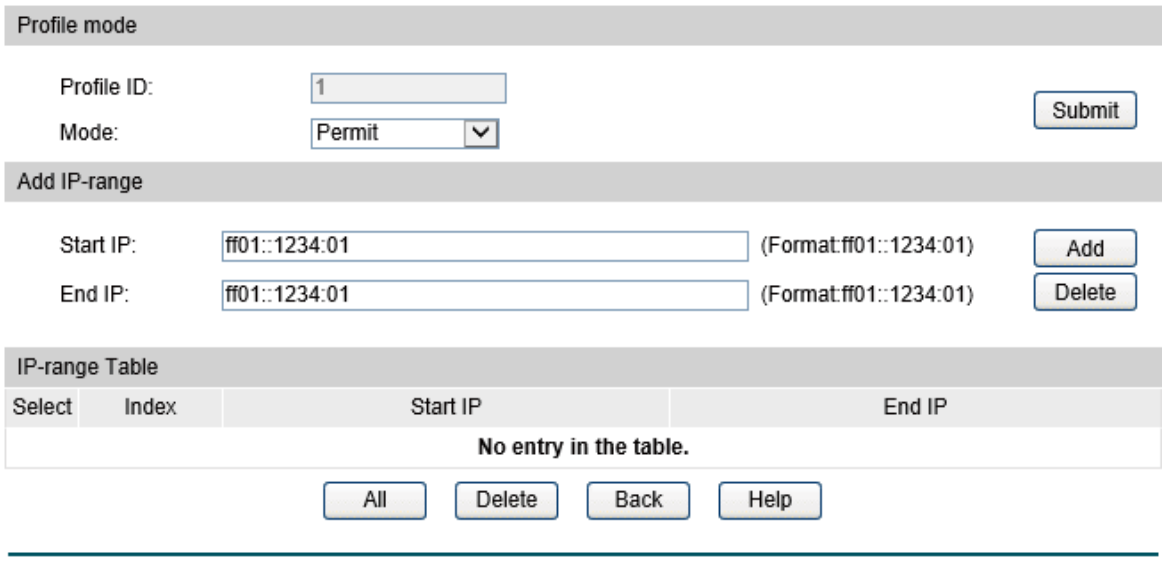
Enter the search condition in the **Search Option** field to search the profile in the MLD Profile Info table.

Editing IP Range of the Profile

Follow these steps to edit profile mode and its IP range:

1) Click **Edit** in the MLD Profile Info table. Edit its IP range and click **Add** to save the settings.

Figure 3-7 Add IP-range



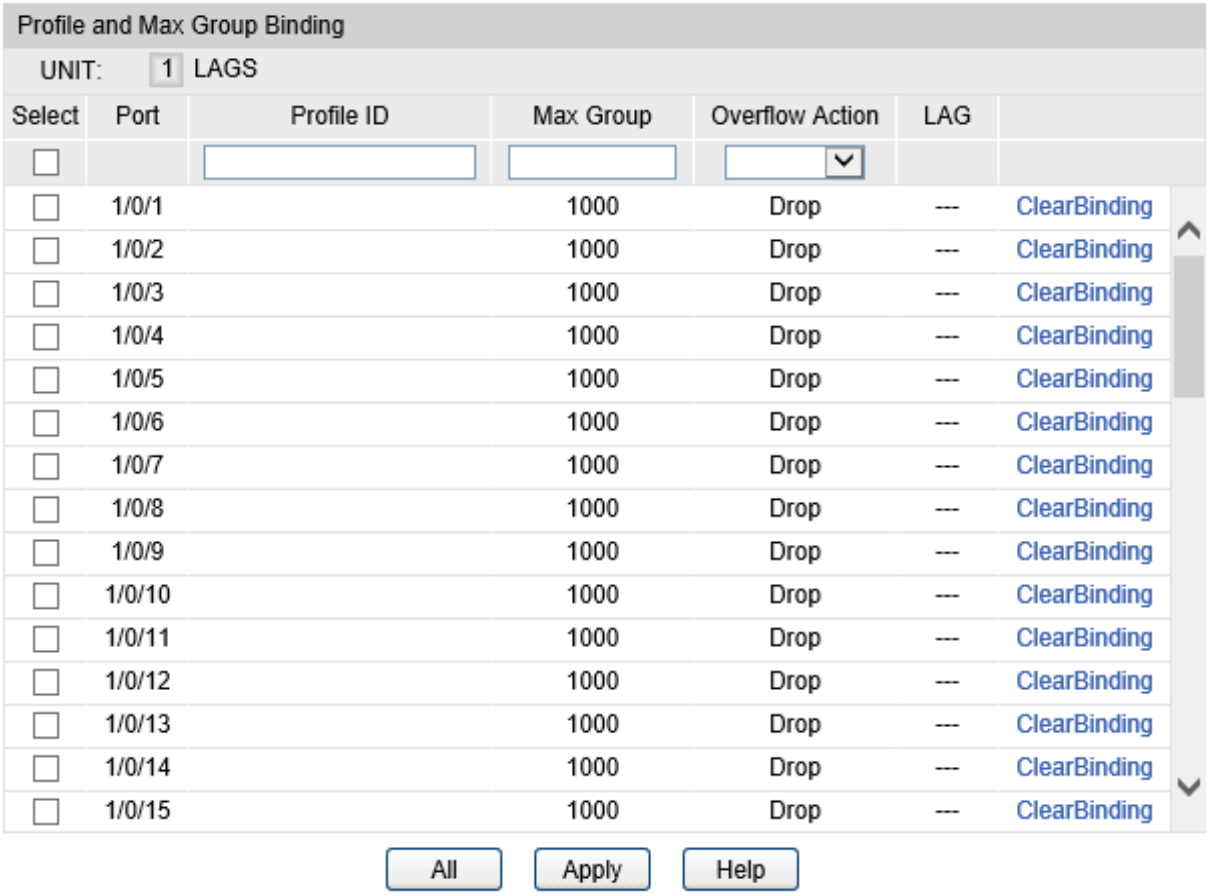
2) In the IP-range Table, you can select an IP range and click **Delete** to delete an IP range.

3) Click **Submit** to save the settings; click **Back** to go back to the previous page.

3.1.7 Binding Profile and Member Ports

With this function, you can configure each port's filtering profile and the number of multicast groups a port can join. Choose the menu **Multicast > MLD Snooping > Profile Binding** to load the following page.

Figure 3-8 Profile Binding



Binding Profile and Member Ports

Follow these steps to bind the profile to the port.

1) Select the port to be bound, and enter the Profile ID in the **Profile ID** column.

Select	Select the port to be bound.
Port	Displays the port number.
Profile ID	Enter the profile ID you create to bind the profile to the port. One port can only be bound to one profile.
ClearBinding	Click to clear the binding between the profile and the port.

2) Click **Apply**.

Configuring Max Groups a Port Can Join

Follow these steps to configure the maximum groups a port can join and overflow action.

1) Select a port to configure its Max Group and Overflow Action.

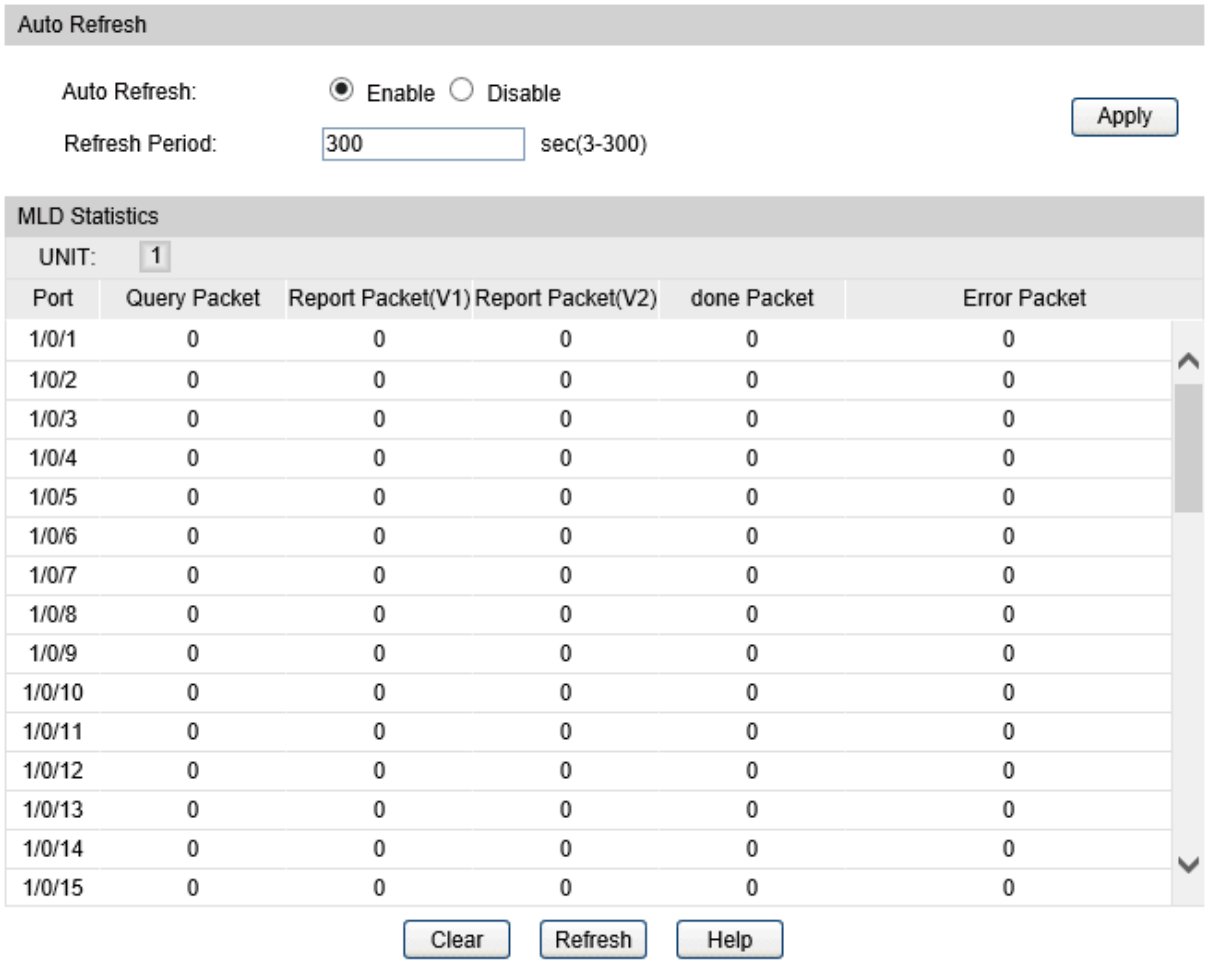
Select	Select the port to be configured.
Max Group	Enter the number of multicast groups the port can join. The valid values are from 0 to 1000.
Overflow Action	Select the action towards the new multicast group when the number of multicast groups the port joined exceeds max group. **Drop**: Drop all subsequent membership report messages, and the port will not join any new multicast groups. **Replace**: Replace the existing multicast group owning the lowest multicast MAC address with the new multicast group.

2) Click **Apply**.

3.1.8 Viewing MLD Statistics on Each Port

Choose the menu **Multicast > MLD Snooping > Packet Statistic** to load the following page.

Figure 3-9 View MLD Statistics on the Port



Configuring Auto Refresh

Follow these steps to configure auto refresh.

1) Enable or disable Auto Refresh.

Auto Refresh	If Auto Refresh is enabled, statistics of MLD packets on this page will refresh automatically.
Refresh Period	After Auto Refresh is enabled, enter the interval between each refresh. The valid values are from 3 to 300 seconds.

2) Click **Apply**.

Viewing MLD Statistics

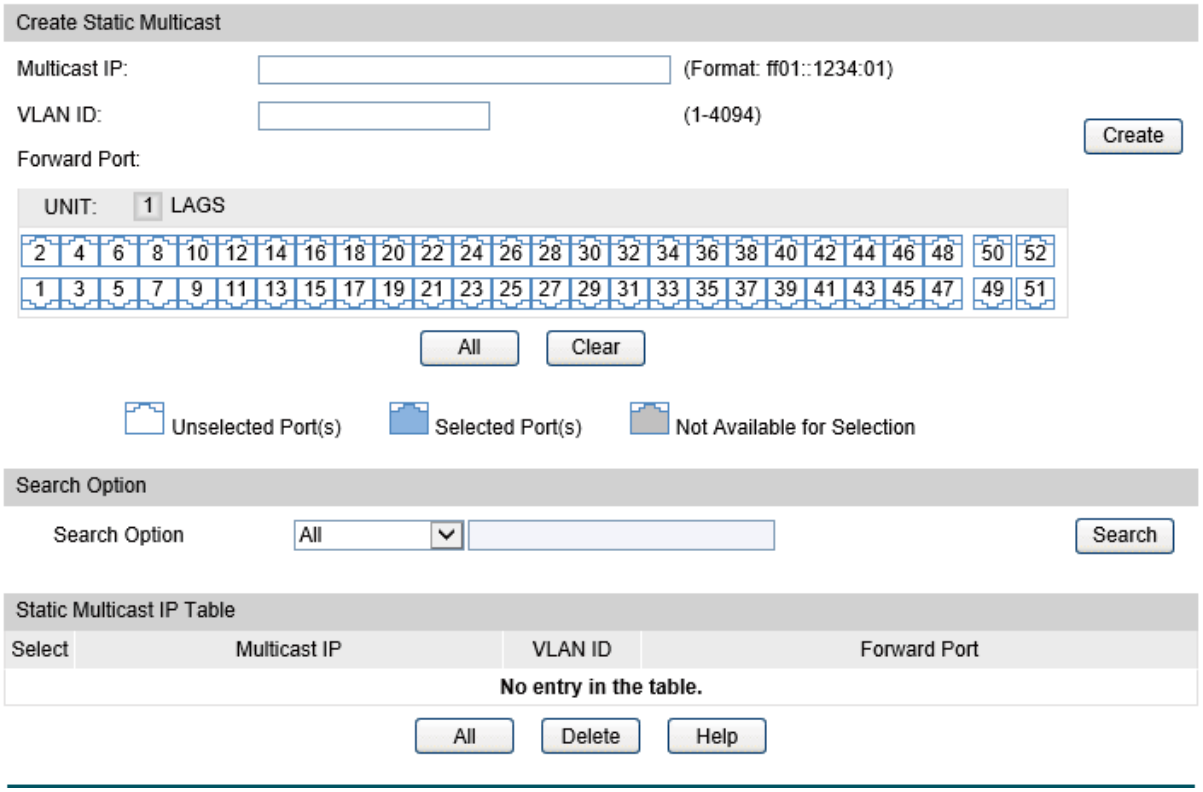
The MLD Statistics table displays all kinds of MLD statistics of all the ports.

3.1.9 Configuring Static Member Port

This function allows you to specify a port as a static member port in the multicast group.

Choose the menu **Multicast > Multicast Table > Static IPv4 Multicast Table** to load the following page.

Figure 3-10 Static Member Port



Configuring Static Member Port

Follow these steps to configure static member port.

1) Enter the Multicast IP and VLAN ID. Specify the Static Member Port.

Multicast IP	Specify the multicast group that the static member is in.
VLAN ID	Specify the VLAN that the static member is in.
Forward Port	Specify one or more ports to be the static member port in the multicast group. Without aging, the static member port receives all multicast data sent to this multicast group.

2) Click **Create**.

Viewing MLD Static Multicast Groups

You can search MLD static multicast entries by using Multicast IP, VLAN ID or Forward Port as the Search Option.

Static Multicast IP Table displays details of all MLD static multicast groups.

3.2 Using the CLI

3.2.1 Enabling MLD Snooping Globally

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 mld snooping** Enable MLD Snooping Globally.
Step 3	**show ipv6 mld snooping** Show the basic MLD snooping configuration.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

3.2.2 Enabling MLD Snooping on the Port

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channe** *port-channel-list***}** Enter interface configuration mode.
Step 3	**ipv6 mld snooping** Enable MLD Snooping on the specified port.
Step 4	**show ipv6 mld snooping** Show the basic MLD snooping configuration.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable MLD Snooping globally and enable MLD Snooping **Switch#configure**

Switch(config)#ipv6 mld snooping

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

Switch(config-if)#ipv6 mld snooping

Switch(config-if)#show ipv6 mld snooping

MLD Snooping :Enable

Unknown Multicast :Pass

Last Query Times :2

Last Query Interval :1

Global Member Age Time :260

Global Router Age Time :300

Global Report Suppression :Disable

Enable Port:Gi1/0/3

Enable VLAN:

Switch(config-if)#end

Switch#copy running-config startup-config

3.2.3 Configuring MLD Snooping Parameters Globally

Configuring Report Message Suppression

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 mld snooping report-suppression** Enable Report Message Suppression globally. If this function is enabled, the switch will only forward the first MLD report message to Layer 3 devices and suppress subsequent MLD report messages from the same multicast group during one query interval, which reduces the number of MLD packets.
Step 3	**show ipv6 mld snooping** Show the basic MLD snooping configuration.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable Report Message Suppression:

Switch#configure

Switch(config)#ipv6 mld snooping

Switch(config)#ipv6 mld snooping report-suppression

Switch(config)#show ipv6 mld snooping

MLD Snooping :Enable

Unknown Multicast :Pass

Last Query Times :2

Last Query Interval :1

Global Member Age Time :260

Global Router Age Time :300

Global Report Suppression :Enable

Enable Port:

Enable VLAN:

Switch(config)#end

Switch#copy running-config startup-config

Configuring Unknown Multicast

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 mld snooping drop-unknown** Configure the way how the switch processes the multicast data from unknown multicast groups as Discard. Unknown multicast groups are multicast groups whose destination multicast address is not in the multicast forwarding table of the switch.
Step 3	**show ipv6 mld snooping** Show the basic MLD snooping configuration.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

IGMP Snooping and MLD Snooping share the setting of Unknown Multicast, so you have to enable IGMP Snooping globally at the same time.

The following example shows how to configure the switch to discard unknown multicast data:

Switch#configure

Switch(config)#ipv6 mld snooping

Switch(config)#ip igmp snooping

Switch(config)#ipv6 mld snooping drop-unknown

Switch(config)#show ipv6 mld snooping

MLD Snooping :Enable

Unknown Multicast :Discard

Last Query Times :2

Last Query Interval :1

Global Member Age Time :260

Global Router Age Time :300

Global Report Suppression :Disable

Enable Port:

Enable VLAN:

Switch(config)#end

Switch#copy running-config startup-config

3.2.4 Configuring MLD Snooping Parameters on the Port

Configuring Router Port Time and Member Port Time

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 mld snooping rtime** *rtime* **ipv6 mld snooping mtime** *mtime* *rtime* is the aging time of router ports, ranging from 60 to 600 seconds. *mtime* is the aging time of member ports, ranging from 60 to 600 seconds.
Step 3	**show ipv6 mld snooping** Show the basic MLD snooping configuration.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the global router port time and member port time as 200 seconds:

Switch#configure

Switch(config)#ipv6 mld snooping

Switch(config)#ipv6 mld snooping rtime 200

Switch(config)#ipv6 mld snooping mtime 200

Switch(config)#show ipv6 mld snooping

MLD Snooping :Enable

Unknown Multicast :Pass

Last Query Times :2

Last Query Interval :1

Global Member Age Time :200

Global Router Age Time :200

Global Report Suppression :Disable

Enable Port:

Enable VLAN:

Switch(config)#end

Switch#copy running-config startup-config

Configuring Fast Leave

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channe** *port-channel-list***}** Enter interface configuration mode
Step 3	**ipv6 mld snooping immediate-leave** Enable Fast Leave on the specified port. With Fast Leave enabled on a port, the switch will delete the port-multicast group entry from the multicast forwarding table once the port receives a leave message. You should only use this function when there is a single receiver present on the port.
Step 4	**show ipv6 mld snooping interface [fastEthernet [** *port* | *port-list* **] | gigabitEthernet [** *port* | *port-list* **]] basic-config** Show the basic MLD snooping configuration on the specified port(s) or of all the ports.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable Fast Leave on port 1/0/3:

Switch#configure

Switch(config)#ipv6 mld snooping

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

Switch(config-if)#ipv6 mld snooping

Switch(config-if)#ipv6 mld snooping immediate-leave

Switch(config-if)#show ipv6 mld snooping interface gigabitEthernet 1/0/3 **basic-config**

Port MLD-Snooping Fast-Leave

---- ------------ ----------

Gi1/0/3 enable enable

Switch(config-if)#end

Switch#copy running-config startup-config

Configuring Max Group and Overflow Action on the Port

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channe** *port-channel-list***}** Enter interface configuration mode
Step 3	**ipv6 mld snooping max-groups** *maxgroup* Enter the number of multicast groups the port can join. The range is 0 to 1000.
Step 4	**ipv6 mld snooping max-groups action {**drop | replace**}** Specify the action towards the new multicast group when the number of multicast groups the port joined exceeds max group. drop: Drop all subsequent membership report messages, and the port join no more new multicast groups. replace: Replace the existing multicast group with the lowest multicast MAC address with the new multicast group.
Step 5	**show ipv6 mld snooping interface [fastEthernet** [*port* | *port-list*] **| gigabitEthernet** [*port* | *port-list*]**] max-groups** Show the IGMP group limitation on the specified port(s) or of all the ports.
Step 6	**end** Return to privileged EXEC mode.

Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the Max Group as 500 and the Overflow Action as Drop on port 1/0/3:

Switch#configure

Switch(config)#ipv6 mld snooping

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

Switch(config-if)#ipv6 mld snooping

Switch(config-if)#ipv6 mld snooping max-groups 500

Switch(config-if)#ipv6 mld snooping max-groups action drop

Switch(config-if)#show ipv6 mld snooping interface gigabitEthernet 1/0/3 **max-groups**

Port	Max-Groups	Overflow-Action
----	----------	----------
Gi1/0/3	500	Drop

Switch(config-if)#end

Switch#copy running-config startup-config

3.2.5 Configuring MLD Snooping Last Listener Query

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 mld snooping last-listener query-inteval** *interval* *interval* determines the interval between MASQs sent by the switch. The valid values are from 1 to 5 seconds.
Step 3	**ipv6 mld snooping last-listener query-count** *num* *num* determines the number of MASQs sent by the switch. The valid values are from 1 to 5.
Step 4	**show ipv6 mld snooping** Show the basic MLD snooping configuration.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the last listener query count as 5 and the last listener query interval as 5 seconds:

Switch#configure

Switch(config)#ipv6 mld snooping

Switch(config)#ipv6 mld snooping last-listener query-count 5

Switch(config)#ipv6 mld snooping last-listener query-interval 5

Switch(config)#show ipv6 mld snooping

MLD Snooping :Enable

Unknown Multicast :Pass

Last Query Times :5

Last Query Interval :5

Global Member Age Time :260

Global Router Age Time :300

Global Report Suppression :Disable

Enable Port:

Enable VLAN:

Switch(config)#end

Switch#copy running-config startup-config

3.2.6 Configuring MLD Snooping Parameters in the VLAN

Configuring Router Port Time and Member Port Time

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 mld snooping vlan-config** *vlan-id-list* **[rtime** *router-time* **| mtime** *member-time***]** *router-time* is the aging time of the router ports in the specified VLAN, ranging from 60 to 600 seconds. *member-time* is the aging time of the member ports in the specified VLAN, ranging from 60 to 600 seconds.
Step 3	**show ipv6 mld snooping vlan** *vlan-id* Show the basic MLD snooping configuration in the specified VLAN.
Step 4	**end** Return to privileged EXEC mode.

Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable MLD Snooping in VLAN 2 and VLAN 3, configure the router port time as 500 seconds and the member port time as 400 seconds:

Switch#configure

Switch(config)#ipv6 mld snooping

Switch(config)#ipv6 mld snooping vlan-config 2-3 **rtime** 500

Switch(config)#ipv6 mld snooping vlan-config 2-3 **mtime** 400

Switch(config)#show ipv6 mld snooping vlan 2

Vlan Id: 2

Router Time:500

Member Time:400

Static Router Port:None

Dynamic Router Port:None

Forbidden Router Port:None

Switch(config)#show ipv6 mld snooping vlan 3

Vlan Id: 3

Router Time:500

Member Time:400

Static Router Port:None

Dynamic Router Port:None

Forbidden Router Port:None

Switch(config)#end

Switch#copy running-config startup-config

Configuring Static Router Port

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 mld snooping vlan-config** *vlan-id-list* **[rport interface {gigabitEthernet** *port-list* **| port-channel** *port-channel-id***}]** *port-list* and *port-channel-id* are the static router ports in the specified VLAN.

Step 3	**show ipv6 mld snooping vlan** *vlan-id* Show the basic MLD snooping configuration in the specified VLAN.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable MLD Snooping in VLAN 2 and configure port 1/0/2 as the static router port:

Switch#configure

Switch(config)#ipv6 mld snooping

Switch(config)#ipv6 mld snooping vlan-config 2 **rport interface gigabitEthernet** 1/0/2

Switch(config)#show ipv6 mld snooping vlan 2

Vlan Id: 2

Router Time:0

Member Time:0

Static Router Port:Gi1/0/2

Dynamic Router Port:None

Forbidden Router Port:None

Switch(config)#end

Switch#copy running-config startup-config

Configuring Forbidden Router Port

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 mld snooping vlan-config** *vlan-id-list* **router-ports-forbidden interface {gigabitEthernet** *port-list* **| port-channel** *port-channel-id***}** *port-list* and *port-channel-id* are the ports that cannot become router ports in the specified VLAN.
Step 3	**show ipv6 mld snooping vlan** *vlan-id* Show the basic MLD snooping configuration in the specified VLAN.
Step 4	**end** Return to privileged EXEC mode.

Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable MLD Snooping in VLAN 2 and forbid port 1/0/4-6 from becoming router ports (port 1/0/4-6 will drop all multicast data from Layer 3 devices):

Switch#config

Switch(config)#ipv6 mld snooping

Switch(config)#ipv6 mld snooping vlan-config 2 **router-ports-forbidden interface gigabitEthernet** 1/0/4-6

Switch(config)#show ipv6 mld snooping vlan 2

Vlan Id: 2

Router Time:0

Member Time:0

Static Router Port:None

Dynamic Router Port:None

Forbidden Router Port:Gi1/0/4-6

Switch(config)#end

Switch#copy running-config startup-config

Configuring Static Multicast (Multicast IP and Forward Port)

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 mld snooping vlan-config** *vlan-id-list* **static** *ip* **interface {gigabitEthernet** *port-list* **| port-channel** *port-channel-id***}** *vlan-id-list* specifies the VLAN to be configured. *ip* specifies the static multicast IP address. *port-list* and *port-channel-id* specify the forward ports (member ports) bound to the static multicast IP address in the specified VLAN.
Step 3	**show ipv6 mld snooping groups static** Show the static MLD snooping configuration.
Step 4	**end** Return to privileged EXEC mode.

Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure ff01::1234:02 as the static multicast IP and specify port 1/0/9-10 as the forward ports:

Switch#configure

Switch(config)#ipv6 mld snooping

Switch(config)#ipv6 mld snooping vlan-config 2 **static** ff01::1234:02 **interface gigabitEthernet** 1/0/9-10

Switch(config)#show ipv6 mld snooping groups static

Multicast-ip	VLAN-id	Addr-type	Switch-port
----------	-------	---------	----------
ff01::1234:02	2	static	Gi1/0/9-10

Switch(config)#end

Switch#copy running-config startup-config

3.2.7 Configuring MLD Snooping Parameters in the Multicast VLAN

Configuring Router Port Time and Member Port Time

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 mld snooping multi-vlan-config** [*vlan-id*] **[rtime** *router-time* **| mtime** *member-time***]** *vlan-id* specifies the VLAN to be created or to be configured. *router-time* is the aging time of the router ports in the multicast VLAN, ranging from 60 to 600 seconds. *member-time* is the aging time of the member ports in the multicast VLAN, ranging from 60 to 600 seconds.
Step 3	**show ipv6 mld snooping multi-vlan** Show the MLD snooping configuration in the multicast VLAN.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure VLAN 5 as the multicast VLAN, set the router port time as 500 seconds and the member port time as 400 seconds:

Switch#configure

Switch(config)#ipv6 mld snooping

Switch(config)#ipv6 mld snooping multi-vlan-config 5 **rtime** 500

Switch(config)#ipv6 mld snooping multi-vlan-config 5 **mtime** 400

Switch(config)#show ipv6 mld snooping multi-vlan

Multicast Vlan:Enable

Vlan Id: 5

Router Time:500

Member Time:400

Replace Source IP:::

Static Router Port:None

Dynamic Router Port:None

Forbidden Router Port:None

Switch(config)#end

Switch#copy running-config startup-config

Configuring Static Router Port

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 mld snooping multi-vlan-config [***vlan-id***] [rport interface {gigabitEthernet** *port-list* **| port-channel** *port-channel-id***}]** *vlan-id* specifies the VLAN to be created or to be configured. *port-list* and *port-channel-id* are the static router ports in the multicast VLAN.
Step 3	**show ipv6 mld snooping multi-vlan** Show the MLD snooping configuration in the multicast VLAN.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure VLAN 5 as the multicast VLAN, and set port 1/0/5 as the static router port:

Switch#configure

Switch(config)#ipv6 mld snooping

Switch(config)#ipv6 mld snooping multi-vlan-config 5 **rport interface gigabitEthernet** 1/0/5

Switch(config)#show ipv6 mld snooping multi-vlan

Multicast Vlan:Enable

Vlan Id: 5

Router Time:300

Member Time:260

Replace Source IP:::

Static Router Port:Gi1/0/5

Dynamic Router Port:None

Forbidden Router Port:None

Switch(config)#end

Switch#copy running-config startup-config

Configuring Forbidden Router Port

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 mld snooping multi-vlan-config [***vlan-id***] router-ports-forbidden interface {gigabitEthernet** *port-list* **| port-channel** *port-channel-id***}** *vlan-id* specifies the multicast VLAN to be configured. *port-list* and *port-channel-id* are the ports that cannot become router ports in the multicast VLAN.
Step 3	**show ipv6 mld snooping multi-vlan** Show the MLD snooping configuration in the multicast VLAN.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure VLAN 5 as the multicast VLAN, and set port 1/0/6 as the forbidden router port:

Switch#configure

Switch(config)#ipv6 mld snooping

Switch(config)#ipv6 mld snooping multi-vlan-config 5 **router-ports-forbidden interface gigabitEthernet** 1/0/6

Switch(config)#show ipv6 mld snooping multi-vlan

Multicast Vlan:Enable

Vlan Id: 5

Router Time:300

Member Time:260

Replace Source IP:::

Static Router Port:None

Dynamic Router Port:None

Forbidden Router Port:Gi1/0/6

Switch(config)#end

Switch#copy running-config startup-config

Configuring Replace Source IP

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 mld snooping multi-vlan-config [***vlan-id***] replace-sourceip** *ip* *vlan-id* specifies the multicast VLAN to be configured. *ip* specifies the new source IP. The switch will replace the source IP in the MLD multicast data sent by the multicast VLAN with the IP address you enter.
Step 3	**show ipv6 mld snooping multi-vlan** Show the MLD snooping configuration in the multicast VLAN.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure VLAN 5 as the multicast VLAN and replace the source IP in the MLD packets sent by the switch with FE80::02FF:FFFF:FE00:0001:

Switch#configure

Switch(config)#ipv6 mld snooping

Switch(config)#ipv6 mld snooping multi-vlan-config 5 **replace-sourceip** fe80::02ff:ffff:fe00:0001

Switch(config)#show ipv6 mld snooping multi-vlan

Multicast Vlan:Enable

Vlan Id: 5

Router Time:300

Member Time:260

Replace Source IP:fe80::2ff:ffff:fe00:1

Static Router Port:None

Dynamic Router Port:None

Forbidden Router Port:None

Switch(config)#end

Switch#copy running-config startup-config

3.2.8 Configuring the Querier

Enabling MLD Querier

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 mld snooping querier vlan** *vlan-id* *vlan-id* specifies the VLAN to enable MLD Querier.
Step 3	**show ipv6 mld snooping querier** [**vlan** *vlan-id*] Show the MLD querier configuration.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable MLD Snooping and MLD Querier in VLAN 4:

Switch#configure

Switch(config)#ipv6 mld snooping

Switch(config)#ipv6 mld snooping querier vlan 4

Switch(config)#show ipv6 mld snooping querier

VLAN 4:

Maximum Response Time: 10

Query Interval: 60

General Query Source IP: fe80::2ff:ffff:fe00:1

Switch(config)#end

Switch#copy running-config startup-config

Configuring Query Interval, Max Response Time and General Query Source IP

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 mld snooping querier vlan** vlan-id **{query-interval** *interval* **| max-response-time** *response-time* **| general-query source-ip** *ip-addr***}** *vlan-id* specifies the VLAN where the querier is. *interval* is the interval between general query messages sent by the querier. *response-time* is the host's maximum response time to general query messages in a range of 1 to 25 seconds. *ip-addr* is the source IP address of the general query messages sent by the querier. It cannot be a multicast address or a broadcast address.
Step 3	**show ipv6 mld snooping querier** [**vlan** *vlan-id*] Show the detailed MLD querier configuration.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable MLD Snooping and MLD Querier in VLAN 4, set the query interval as 100 seconds, the max response time as 20 seconds, and the general query source IP as fe80::2ff:ffff:fe00:1:

Switch#configure

Switch(config)#ipv6 mld snooping

Switch(config)#ipv6 mld snooping querier vlan 4 **query-interval** 100

Switch(config)#ipv6 mld snooping querier vlan 4 **max-response-time** 20

Switch(config)#ipv6 mld snooping querier vlan 4 general-query source-ip fe80::2ff:ffff:fe00:1

Switch(config)#show ipv6 mld snooping querier

VLAN 4:

Maximum Response Time: 20

Query Interval: 100

General Query Source IP: fe80::2ff:ffff:fe00:1

Switch(config)#end

Switch#copy running-config startup-config

3.2.9 Configuring Multicast Filtering

Creating Profile

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 mld profile** *id* Create a new profile and enter profile configuration mode.
Step 3	**deny** **permit** Configure the profile's filtering mode. **permit** is similar to a whitelist, indicating that the switch only allow specific member ports to join specific multicast groups. **deny** is similar to a blacklist, indicating that the switch disallow specific member ports to join specific multicast groups.
Step 4	**range** *start-ip end-ip* Configure the range of multicast IP to be filtered. *start-ip*, *end-ip* are the start IP and end IP of the IP range respectively.
Step 5	**end** Return to privileged EXEC mode.

Step 6	**show ipv6 mld profile** [*id*] Show the detailed MLD profile configuration.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure Profile 1 so that the switch filters multicast data sent to ff01::1234:5-ff01::1234:8:

Switch#configure

Switch(config)#ipv6 mld snooping

Switch(config)#ipv6 mld profile 1

Switch(config-mld-profile)#deny

Switch(config-mld-profile)#range ff01::1234:5 ff01::1234:8

Switch(config-mld-profile)#show ipv6 mld profile

MLD Profile 1

deny

range ff01::1234:5 ff01::1234:8

Switch(config)#end

Switch#copy running-config startup-config

Binding Profile to the Port

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channe** *port-channel-list***}** Enter interface configuration mode
Step 3	**ipv6 mld filter** *profile-id* Bind *profile-id* to the specified port.
Step 4	**show ipv6 MLD profile** [*id*] Show the detailed MLD profile configuration.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to bind Profile 1 to port 1/0/2 so that port 1/0/2 filters multicast data sent to ff01::1234:5-ff01::1234:8:

Switch#configure

Switch(config)#ipv6 mld snooping

Switch(config)#ipv6 mld profile 1

Switch(config-mld-profile)#deny

Switch(config-mld-profile)#range ff01::1234:5 ff01::1234:8

Switch(config-mld-profile)#exit

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

Switch(config-if)#ipv6 mld snooping

Switch(config-if)#ipv6 mld filter 1

Switch(config-if)#show ipv6 mld profile

MLD Profile 1

deny

range ff01::1234:5 ff01::1234:8

Binding Port(s)

Gi1/0/2

Switch(config)#end

Switch#copy running-config startup-config

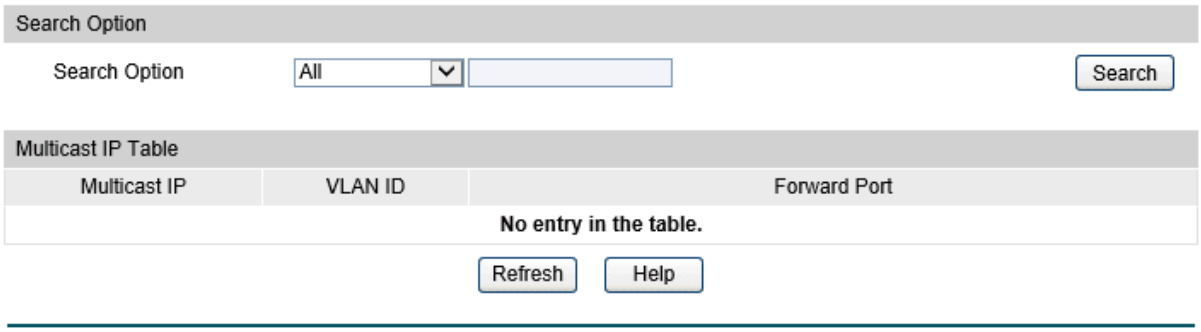
4 Viewing Multicast Snooping Configurations

4.1 Using the GUI

4.1.1 Viewing IPv4 Multicast Snooping Configurations

Choose the menu **Multicast > Multicast Table > IPv4 Multicast Table** to view all valid Multicast IP-VLAN-Port entries.

Figure 4-1 IPv4 Multicast Table



Search Option

Search Option	Search for specific multicast entries by using Multicast IP, VLAN ID and Forward Port.

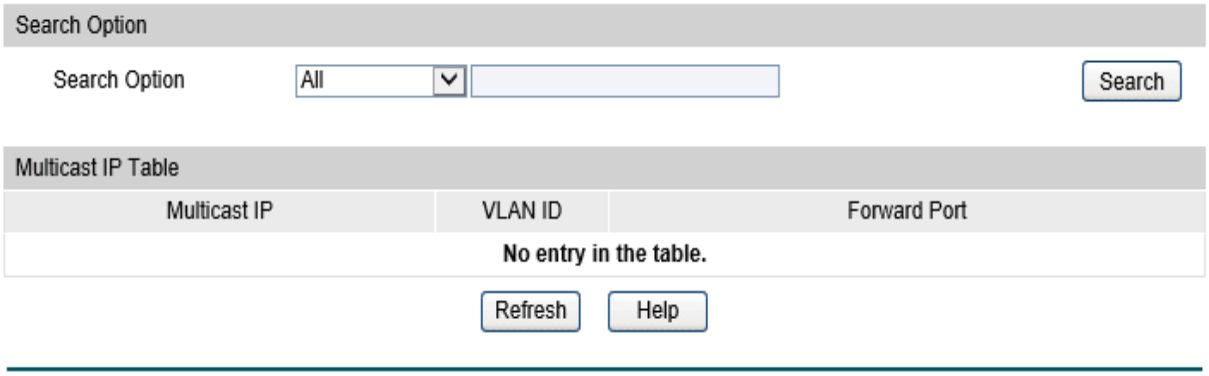
Multicast IP Table

Multicast IP	Multicast source IP.
VLAN ID	ID of the VLAN that the multicast group is in.
Forward Port	All ports in the multicast group, including router ports and member ports.

4.1.1 Viewing IPv6 Multicast Snooping Configurations

Choose the menu **Multicast > Multicast Table > IPv6 Multicast Table** to view all valid Multicast IP-VLAN-Port entries.

Figure 4-2 IPv6 Multicast Table



4.2 Using the CLI

4.2.1 Viewing IPv4 Multicast Snooping Configurations

show ip igmp snooping

Displays global settings of IGMP Snooping.

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

Displays settings of IGMP Snooping on the port(s).

port **|** *port-list* specifies the port(s) to display.

basic-config | *max-groups* | *packet-stat* displays the related IGMP configuration information.

show ip igmp snooping interface [port-channel [*lagid***]] {**basic-config | max-groups**}**

Displays settings of IGMP Snooping on the port-channel.

lagid specifies the LAG(s) to display.

basic-config | *max-groups* displays the related IGMP configuration information.

show ip igmp snooping vlan [*vlan-id***]**

Displays settings of IGMP Snooping in specific VLAN or all the VLANs.

show ip igmp snooping multi-vlan

Displays settings of IGMP Snooping in the multicast VLAN.

show ip igmp snooping groups vlan *vlan-id multicast_addr*

Displays information of specific multicast group in the specific VLAN.

show ip igmp snooping groups [vlan *vlan-id* **] [**count | dynamic | dynamic count | static | static count **]**

Displays information of specific multicast group in all VLANs or in the specific VLAN.

count: displays the number of multicast groups.

dynamic: displays information of all dynamic multicast groups.

dynamic count: displays the number of dynamic mu lticast groups.

static: displays information of all static multicast groups.

static count: displays the number of static multicast groups.

show ip igmp snooping querier [vlan *vlan-id* **]**

Displays information of IGMP Querier in all VLANs or in the specific VLAN.

show ip igmp profile [*id***]**

Displays settings in all profiles or in the specific profile.

clear ip igmp snooping statistics

Clear all statistics of all IGMP packets.

4.2.2 Viewing IPv6 Multicast Snooping Configurations

show ipv6 mld snooping

Displays global settings of MLD Snooping.

show ipv6 mld snooping interface [fastEthernet [*port* **|** *port-list***] | gigabitEthernet [***port* **|** *port-list***]] {**basic-config | max-groups | packet-stat**}**

Displays settings of MLD Snooping on the port.

port **|** *port-list:* specifies the port(s) to display.

basic-config | *max-groups* | *packet-stat* displays the related MLD configuration information.

show ipv6 mld snooping interface [port-channel [*lagid***]] {**basic-config | max-groups**}**

Displays settings of MLD Snooping on the port-channel.

lagid: specifies the LAG(s) to display.

basic-config | *max-groups:* displays the related MLD configuration information.

show ipv6 mld snooping vlan [*vlan-id***]**

Displays settings of MLD Snooping in specific VLAN or all the VLANs.

show ipv6 mld snooping multi-vlan

Displays settings of MLD Snooping in the multicast VLAN.

show ipv6 mld snooping groups vlan *vlan-id multicast_addr*

Displays information of specific multicast group in the specific VLAN.

show ipv6 mld snooping groups [vlan *vlan-id*] [count | dynamic | dynamic count | static | static count **]**

Displays information of specific multicast group in all VLANs or in the specific VLAN.

count displays the number of multicast groups.

dynamic displays information of all dynamic multicast groups.

dynamic count displays the number of dynamic multicast groups.

static displays information of all static multicast groups.

static count displays the number of static multicast groups.

show ipv6 mld snooping querier [vlan *vlan-id*]

Displays information of MLD Querier in all VLANs or in the specific VLAN.

show ipv6 mld profile [*id*]

Displays settings in all profiles or in the specific profile.

clear ipv6 mld snooping statistics

Clear all statistics of all MLD packets.

5 Configuration Examples

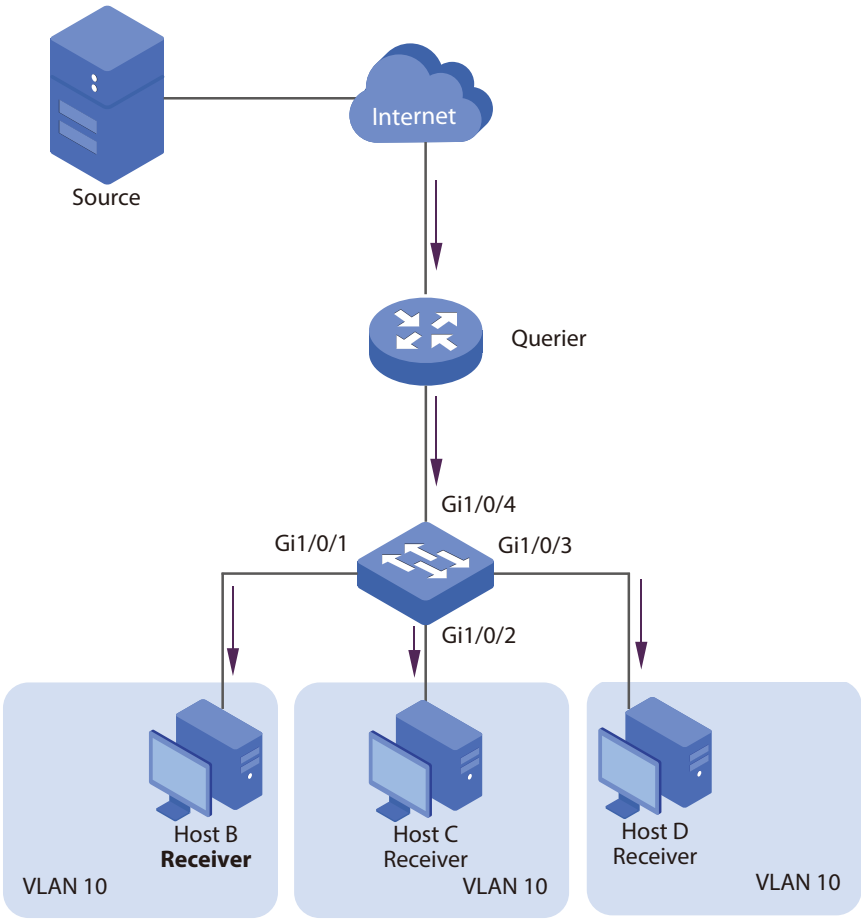
5.1 Example for Configuring Basic IGMP Snooping

5.1.1 Network Requirements

Host B, Host C and Host D are in the same VLAN of the switch. All of them want to receive multicast data sent to multicast group 225.1.1.1.

As shown in the following topology, Host B, Host C and Host D are connected to port 1/0/1, port 1/0/2 and port 1/0/3 respectively. Port 1/0/4 is the router port connected to the multicast querier.

Figure 5-1 Network Topology for Basic IGMP Snooping



5.1.2 Configuration Scheme

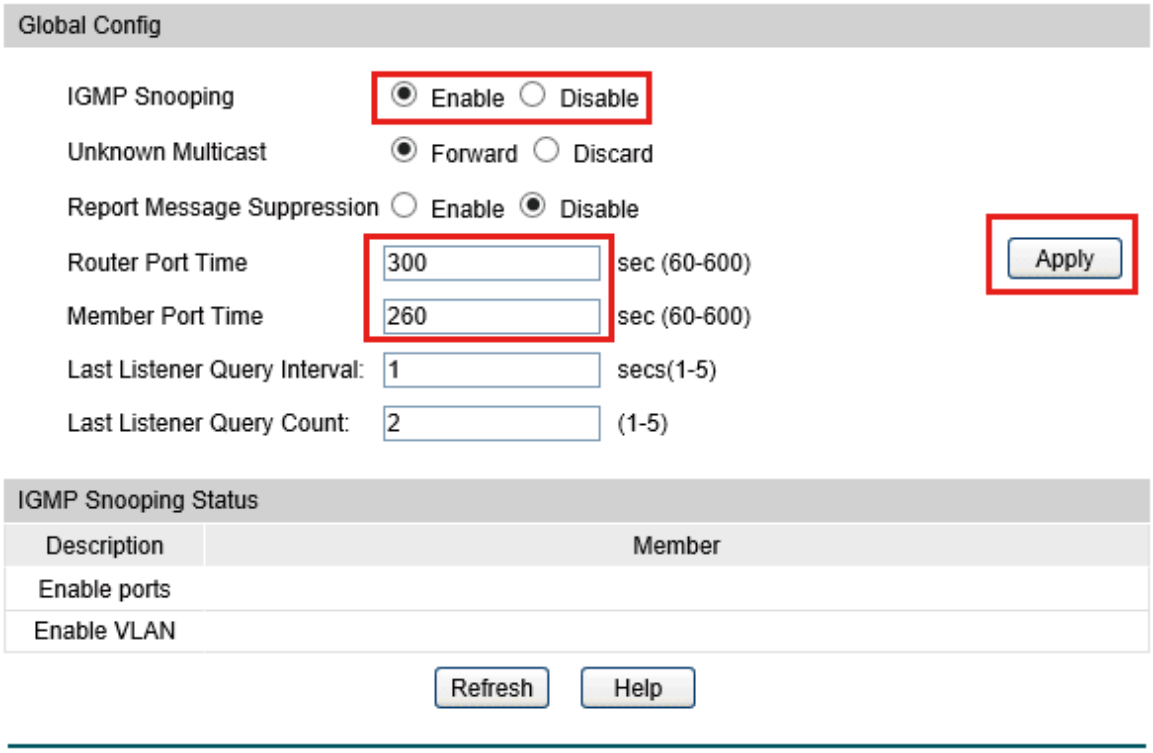
- Enable IGMP Snooping globally and on the port.
- Add the three member ports and the router port to a VLAN and configure their PVIDs.

Enable IGMP Snooping in the VLAN. Demonstrated with T2600G-28TS, this section provides configuration procedures in two ways: using the GUI and using the CLI.

5.1.3 Using the GUI

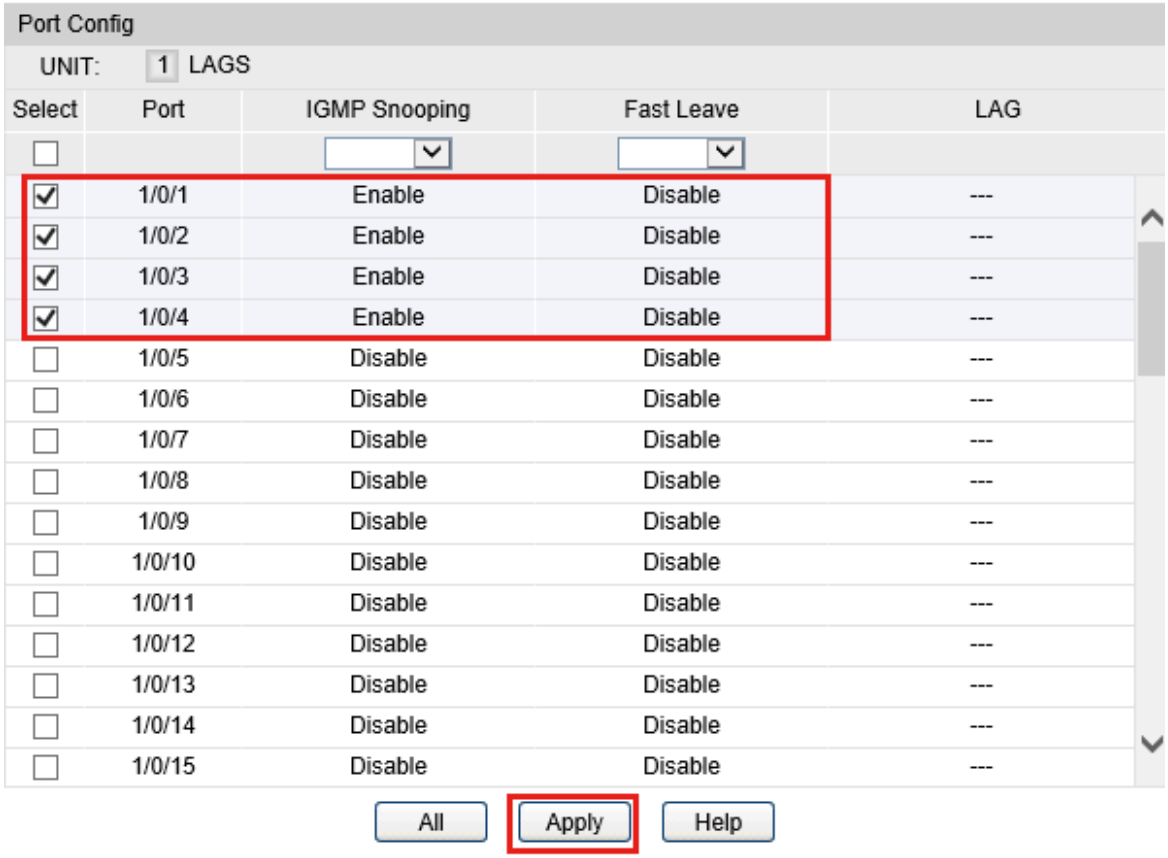
1) Choose the menu **Multicast > IGMP Snooping > Snooping Config** to load the following page. Enable IGMP Snooping globally, and keep the default values in the Router Port Time and Member Port Time fields.

Figure 5-2 Configure IGMP Snooping Globally



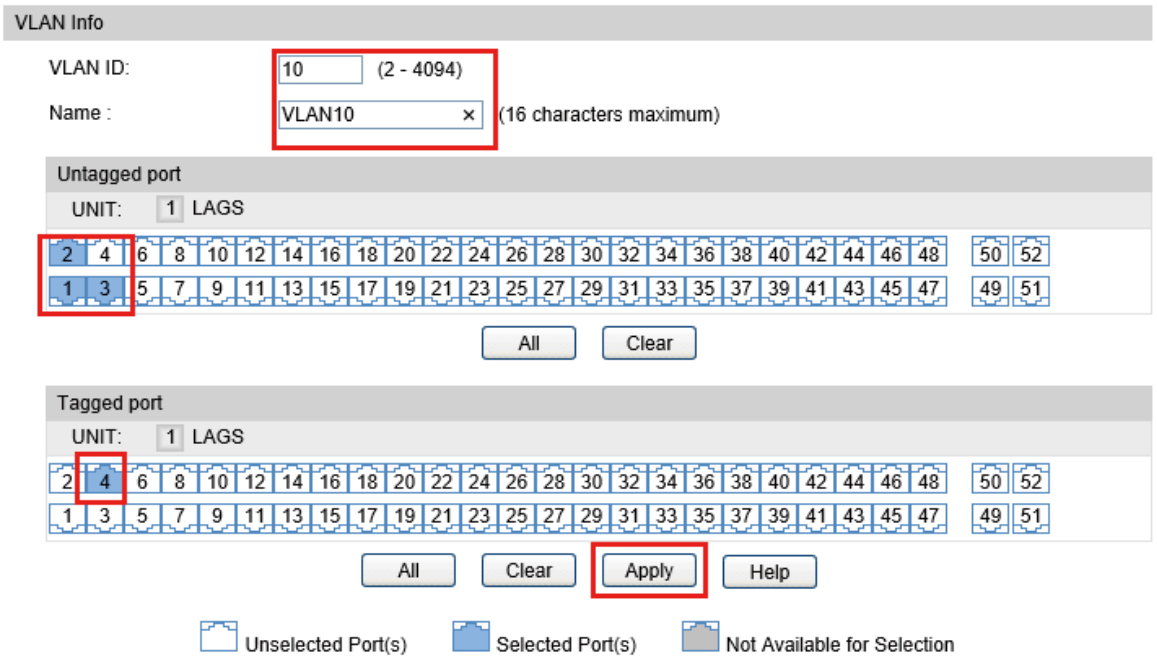
2) Choose the menu **Multicast > IGMP Snooping > Snooping Config** to load the following page. Enable IGMP Snooping on port 1/0/1-4.

Figure 5-3 Enable IGMP Snooping on the Ports



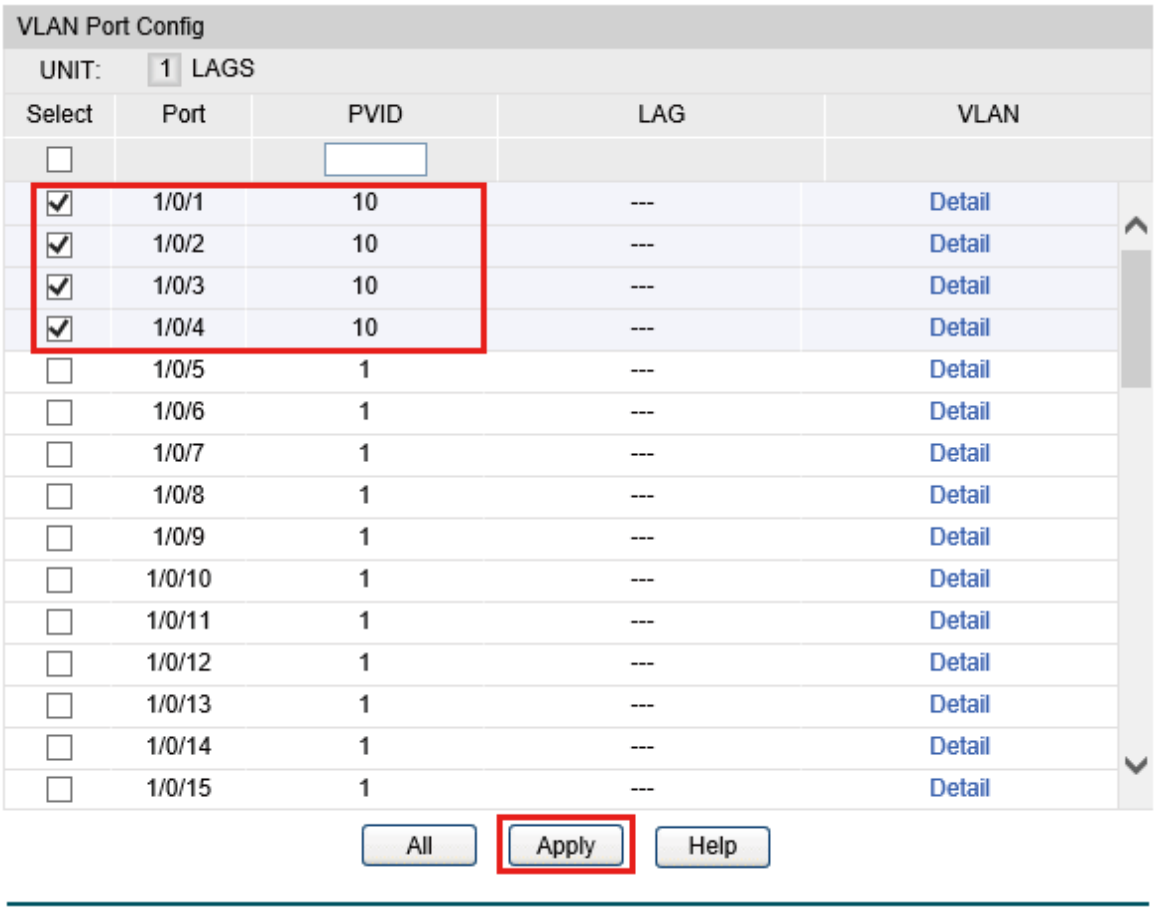
3) Choose the menu **VLAN > 802.1Q VLAN > VLAN Config** to load the following page. Create VLAN 10 and add Untagged port 1/0/1-3 and Tagged port 1/0/4 to VLAN 10.

Figure 5-4 Configure Link Type



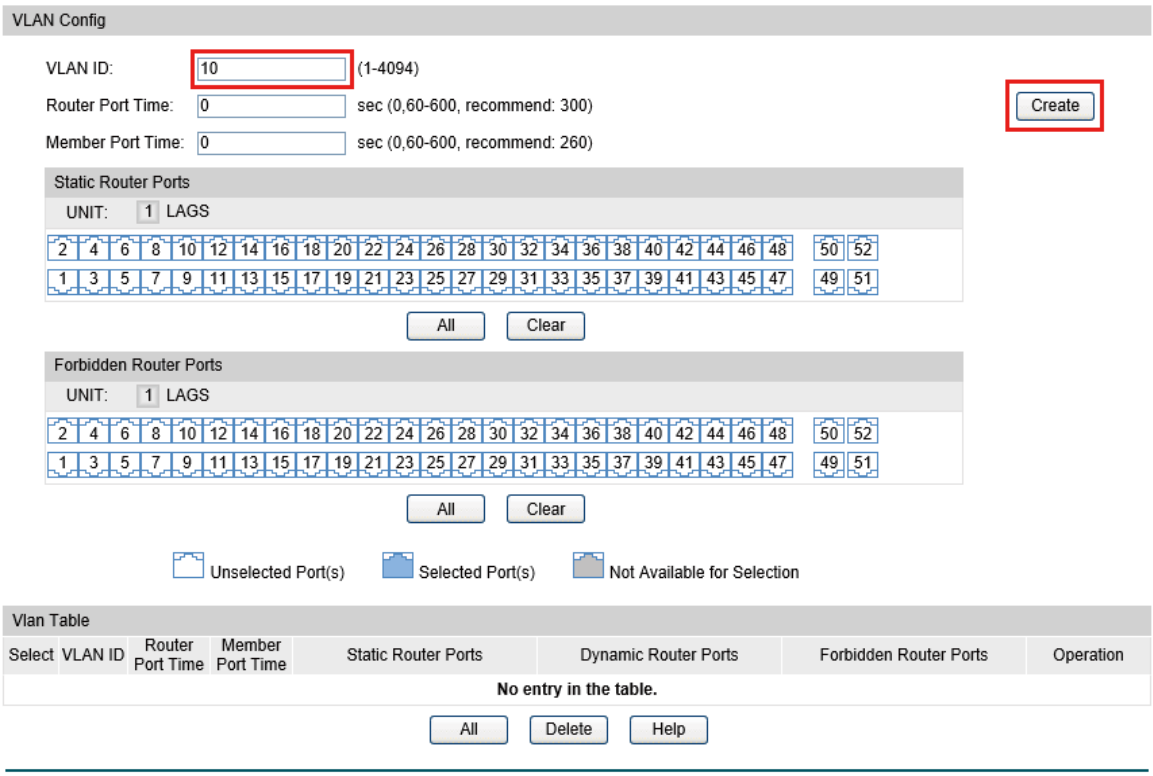
4) Choose the menu **VLAN > 802.1Q VLAN > Port Config** to load the following page. Configure the PVID of port 1/0/1-4 as 10.

Figure 5-5 Create VLAN and Add Member Ports



5) Choose the menu **Multicast > IGMP Snooping > VLAN Config** to load the following page. Enable IGMP Snooping in VLAN 10. Keep 0 as the Router Port Time and Member Port Time, which means the global settings will be used.

Figure 5-6 Enable IGMP Snooping in the VLAN



6) Click **Save Config** to save the settings.

5.1.4 Using the CLI

1) Enable IGMP Snooping globally.

Switch#configure

Switch(config)#ip igmp snooping

2) Enable IGMP Snooping on port 1/0/1-4.

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

Switch(config-if-range)#ip igmp snooping

Switch(config-if-range)#exit

3) Create VLAN 10.

Switch(config)#vlan 10

Switch(config-vlan)#name vlan10

Switch(config-vlan)#exit

4) Add port 1/0/1-3 to VLAN 10 and set the link type as untagged. Add port 1/0/4 to VLAN 10 and set the link type as tagged.

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

Switch(config-if-range)#switchport general allowed vlan 10 untagged

Switch(config-if-range)#exit

Switch(config)#interface gigabitEthernet 1/0/4

Switch(config-if)#switchport general allowed vlan 10 tagged

Switch(config-if)#exit

5) Set the PVID of port 1/0/1-4 as 10.

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

Switch(config-if-range)#switchport pvid 10

Switch(config-if-range)#exit

6) Enable IGMP Snooping in VLAN 10.

Switch(config)#ip igmp snooping vlan-config 10

7) Save the settings.

Switch(config)#end

Switch#copy running-config startup-config

Verify the Configurations

Show members in the VLAN:

Switch(config)#show vlan brief

VLAN	Name	Status	Ports
1	System-VLAN	active	Gi1/0/1, Gi1/0/2, Gi1/0/3, Gi1/0/4, Gi1/0/5, Gi1/0/6, Gi1/0/7, Gi1/0/8, ...
10	vlan10	active	Gi1/0/1, Gi1/0/2, Gi1/0/3, Gi1/0/4

Show status of IGMP Snooping globally, on the ports and in the VLAN:

Switch(config)#show ip igmp snooping

IGMP Snooping :Enable

Unknown Multicast :Pass

Last Query Times :2

Last Query Interval :1

Global Member Age Time :260

Global Router Age Time :300

Global Report Suppression :Disable

Global Authentication Accounting:Disable

Enable Port:Gi1/0/1-4

Enable VLAN:10

5.2 Example for Configuring Multicast VLAN

5.2.1 Network Requirements

Host B, Host C and Host D are in three different VLANs of the switch. All of them want to receive multicast data sent to multicast group 225.1.1.1.

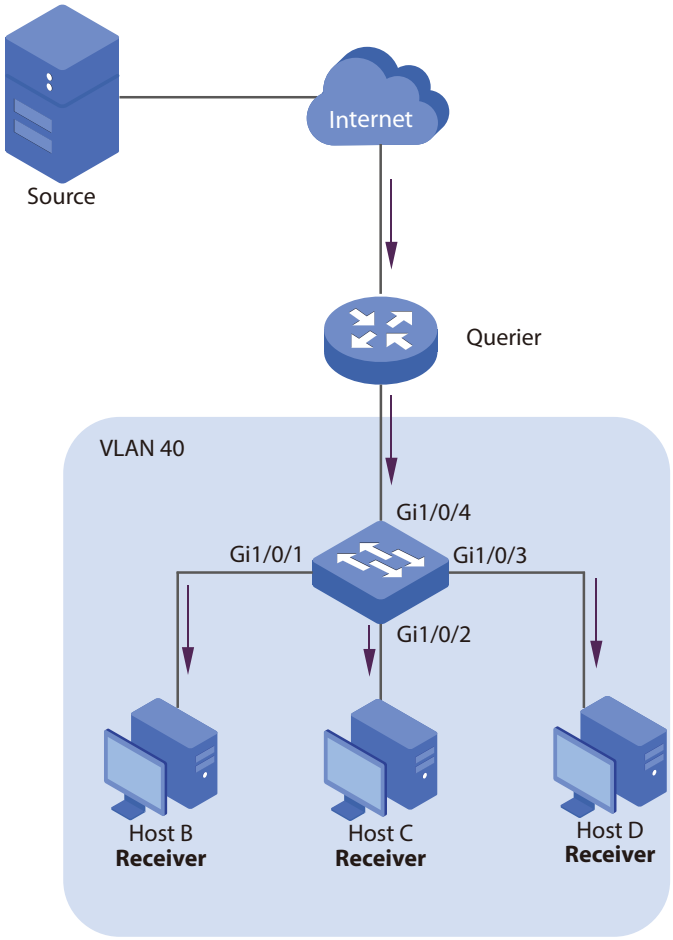
5.2.2 Configuration Scheme

Create a multicast VLAN and add the router port and ports connected to multicast members to the multicast VLAN. In this case, all multicast data will only be processed in the multicast VLAN.

5.2.3 Network Topology

As shown in the following network topology, Host B, Host C and Host D are connected to port 1/0/1, port 1/0/2 and port 1/0/3 respectively. Port 1/0/1, port 1/0/2 and port 1/0/3 belong to VLAN 10, VLAN 20 and VLAN 30 respectively. Port 1/0/4 is connected to the multicast network in the upper layer network. These 4 ports are all Untagged ports.

Figure 5-7 Network Topoloy for Multicast VLAN

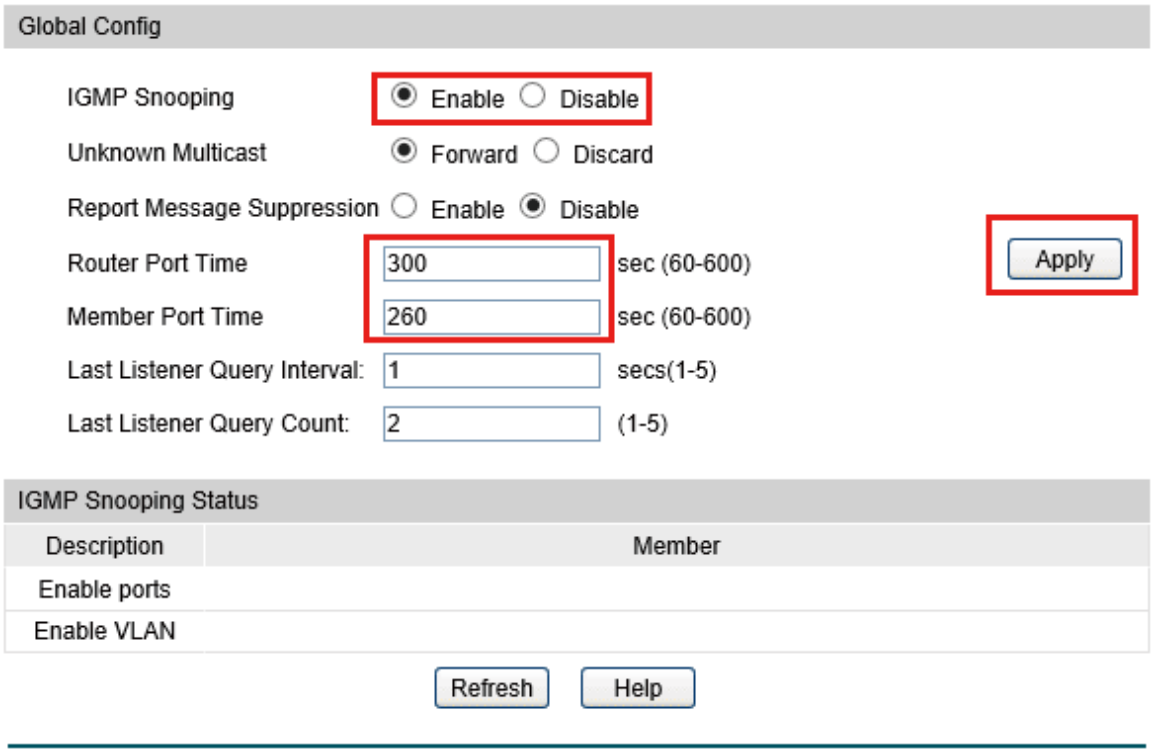


Demonstrated with T2600G-28TS, this section provides configuration procedures in two ways: using the GUI and using the CLI.

5.2.4 Using the GUI

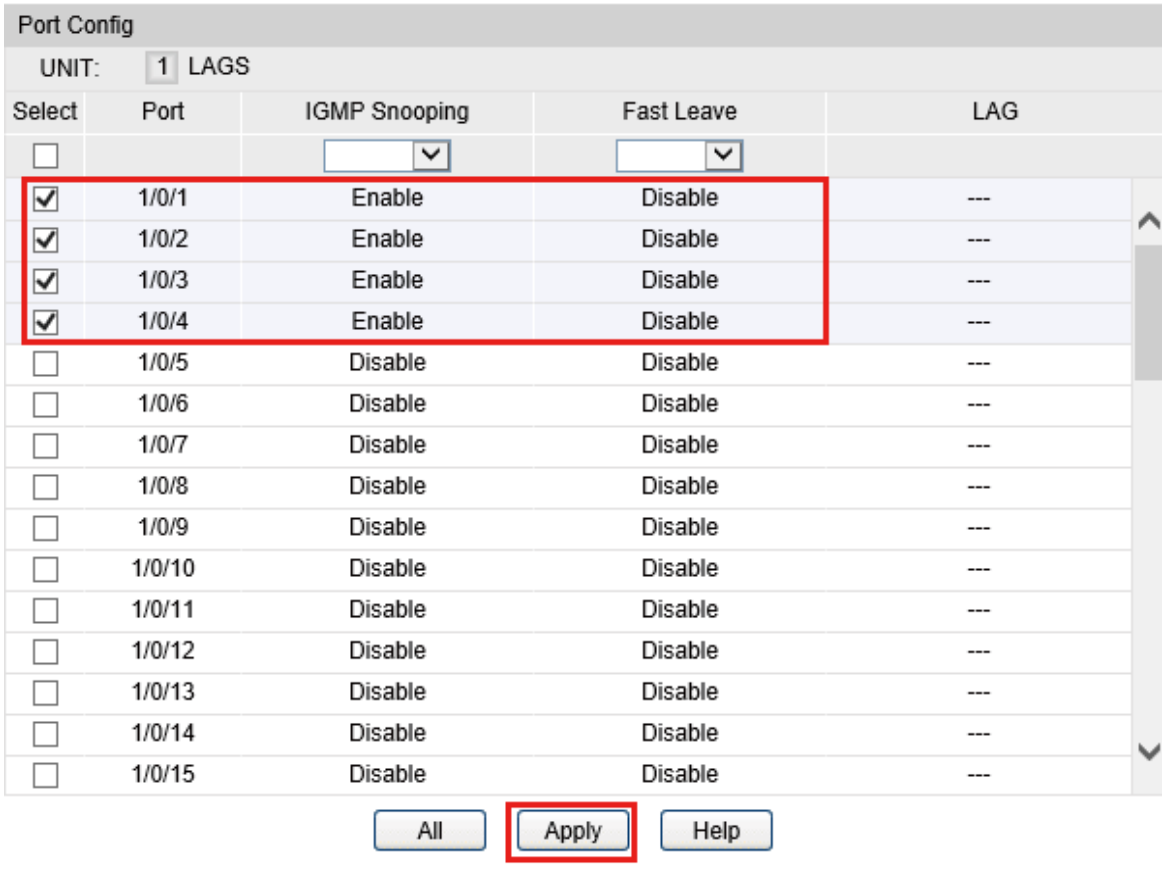
1) Choose the menu **Multicast > IGMP Snooping > Snooping Config** to load the following page. Enable IGMP Snooping globally, and keep the default values in the Router Port Time and Member Port Time fields.

Figure 5-8 Configure IGMP Snooping Globally



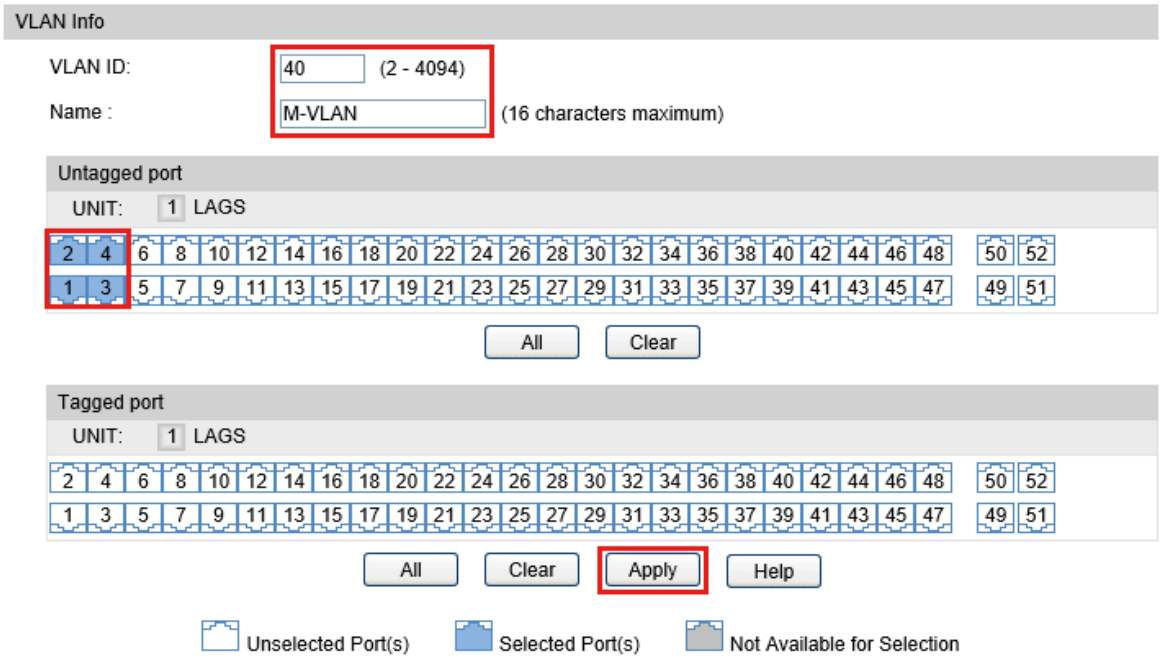
2) Choose the menu **Multicast > IGMP Snooping > Snooping Config** to load the following page. Enable IGMP Snooping on port 1/0/1-4.

Figure 5-9 Configure IGMP Snooping Globally



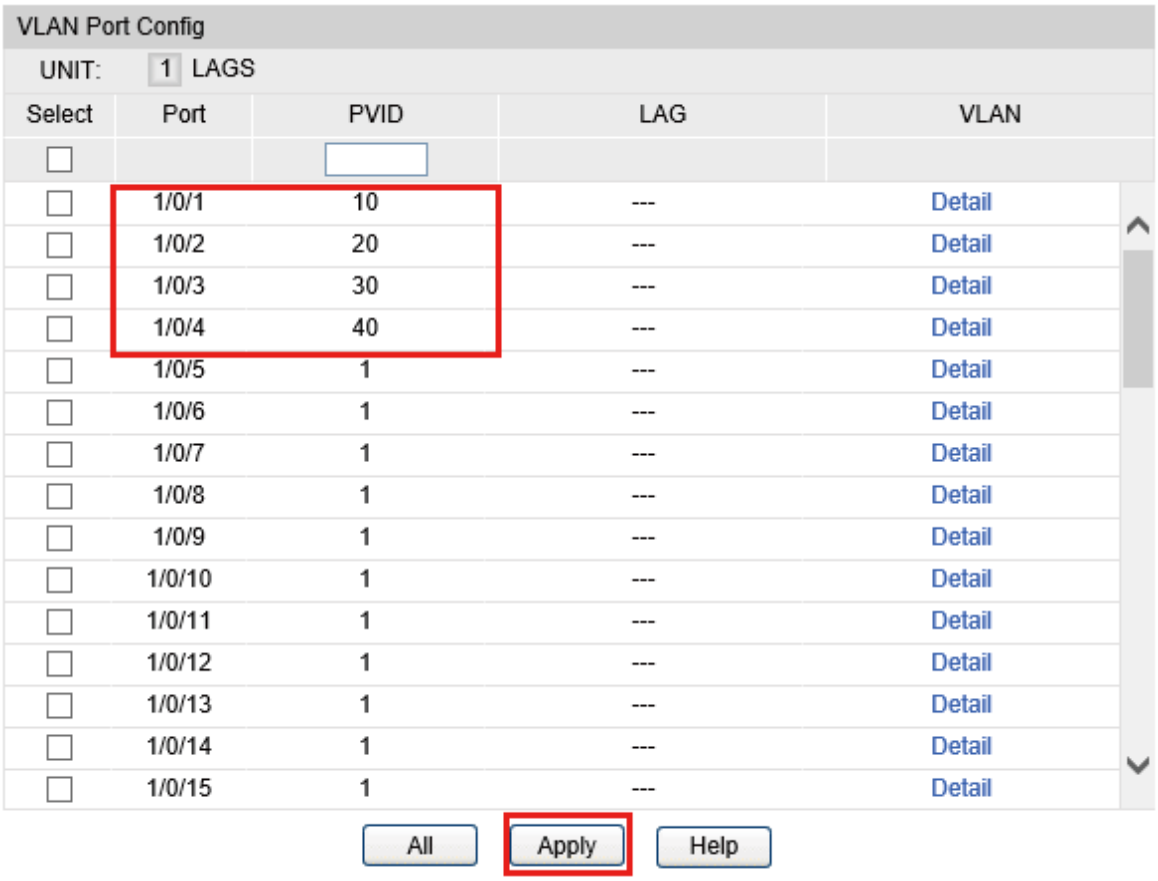
3) Choose the menu **VLAN > 802.1Q VLAN > VLAN Config** to load the following page. Create VLAN 40 and add Untagged port 1/0/1-4 to VLAN 40.

Figure 5-10 Configure Link Type



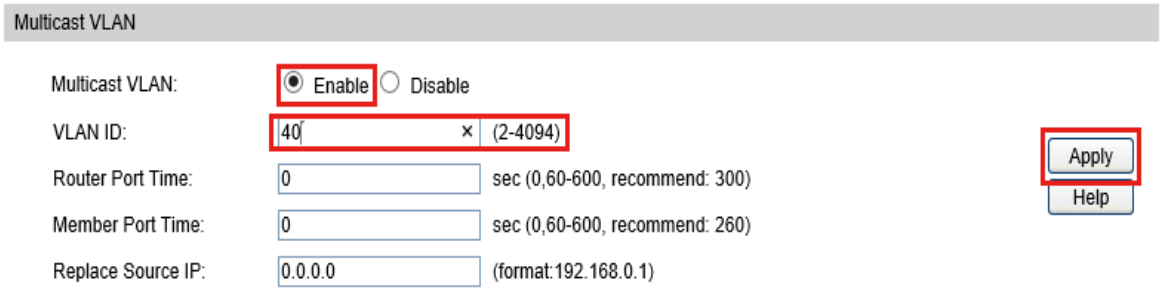
4) Choose the menu **VLAN > 802.1Q VLAN > Port Config** to load the following page. Configure the PVID of port 1/0/1 as 10, port 1/0/2 as 20, port 1/0/3 as 30 and port 1/0/4 as 40.

Figure 5-11 Create VLAN and Add Member Ports



5) Choose the menu **Multicast > IGMP Snooping > Multicast VLAN** to load the following page. Enable Multicast VLAN and configure VLAN 40 as the multicast VLAN. Keep Router Port Time and Member Port Time as 0.

Figure 5-12 Create Multicast VLAN



6) Click **Save Config** to save the settings.

5.2.5 Using the CLI

1) Enable IGMP Snooping Globally.

Switch#configure

Switch(config)#ip igmp snooping

2) Enable IGMP Snooping on port 1/0/1-4.

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

Switch(config-if-range)#ip igmp snooping

Switch(config-if-range)#exit

3) Create VLAN 10.

Switch(config)#vlan 10

Switch(config-vlan)#name vlan10

Switch(config-vlan)#exit

4) Add port 1/0/1-3 to VLAN 10 and set the link type as untagged. Add port 1/0/4 to VLAN 10 and set the link type as tagged.

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

Switch(config-if-range)#switchport general allowed vlan 10 untagged

Switch(config-if-range)#exit

Switch(config)#interface gigabitEthernet 1/0/4

Switch(config-if)#switchport general allowed vlan 10 tagged

Switch(config-if)#exit

5) Set the PVID of port 1/0/1-4 as 10.

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

Switch(config-if-range)#switchport pvid 10

Switch(config-if-range)#exit

6) Enable Multicast VLAN and configure VLAN 10 as the multicast VLAN.

Switch(config)#ip igmp snooping multi-vlan-config 10

7) Save the settings.

Switch(config)#end

Switch#copy running-config startup-config

Verify the Configurations

Switch(config)#show vlan brief

VLAN	Name	Status	Ports
1	System-VLAN	active	Gi1/0/1, Gi1/0/2, Gi1/0/3, Gi1/0/4, Gi1/0/5, Gi1/0/6, Gi1/0/7, Gi1/0/8, ...

10 vlan10 active Gi1/0/1, Gi1/0/2, Gi1/0/3, Gi1/0/4

Show status of IGMP Snooping globally, on the ports and in the multicast VLAN:

Switch(config)#show ip igmp snooping

IGMP Snooping :Enable

Unknown Multicast :Pass

Last Query Times :2

Last Query Interval :1

Global Member Age Time :260

Global Router Age Time :300

Global Report Suppression :Disable

Global Authentication Accounting:Disable

Enable Port:Gi1/0/1-4

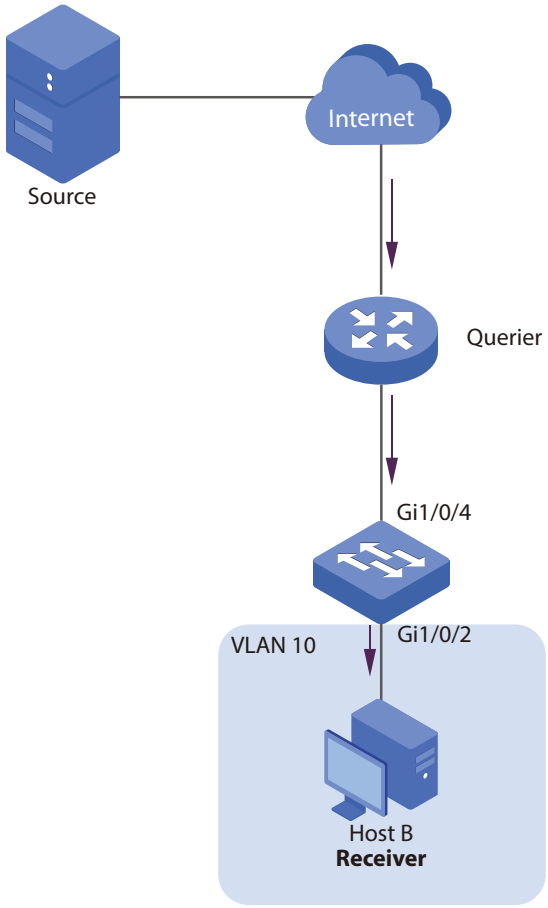
Enable VLAN:Multicast VLAN 10

5.3 Example for Configuring Unknown Multicast and Fast Leave

5.3.1 Network Requirement

A user experiences lag when he is changing channel on his IPTV. He wants solutions to this problem. As shown in the following network topology, port 1/0/4 on the switch is connected to the upper layer network, and port 1/0/2 is connected to Host B.

Figure 5-13 Network Topology for Unknow Multicast and Fast Leave



5.3.2 Configuration Scheme

After the channel is changed, the client (Host B) still receives irrelevant multicast data, the data from the previous channel and possibly other unknown multicast data, which increases the network load and results in network congestion. The solution to this problem is using Unknown Multicast and Fast Leave.

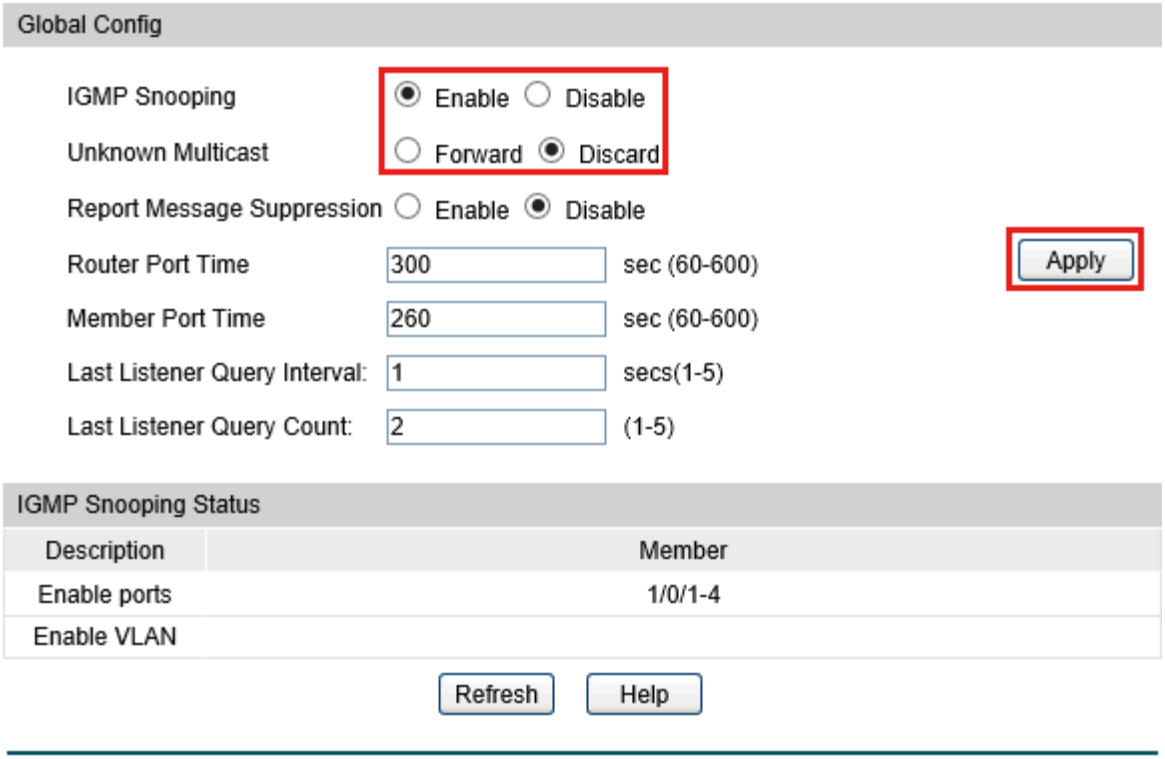
To avoid Host B from receiving irrelevant multicast data, the user can enable Fast Leave on port 1/0/2 and enable Unknown Multicast globally. To change channel, Host B sends a leave message about leaving the previous channel. The switch will then drop multicast data from the previous channel and all unknown multicast data, which ensures that Host B only receives multicast data from the new channel and that the multicast network is unimpeded.

Demonstrated with T2600G-28TS, this section provides configuration procedures in two ways: using the GUI and using the CLI.

5.3.3 Using the GUI

1) Choose the menu **Multicast > IGMP Snooping > Snooping Config** to load the following page. Enable IGMP Snooping globally and configure Unknown Multicast as Discard.

Figure 5-14 Configure IGMP Snooping Globally

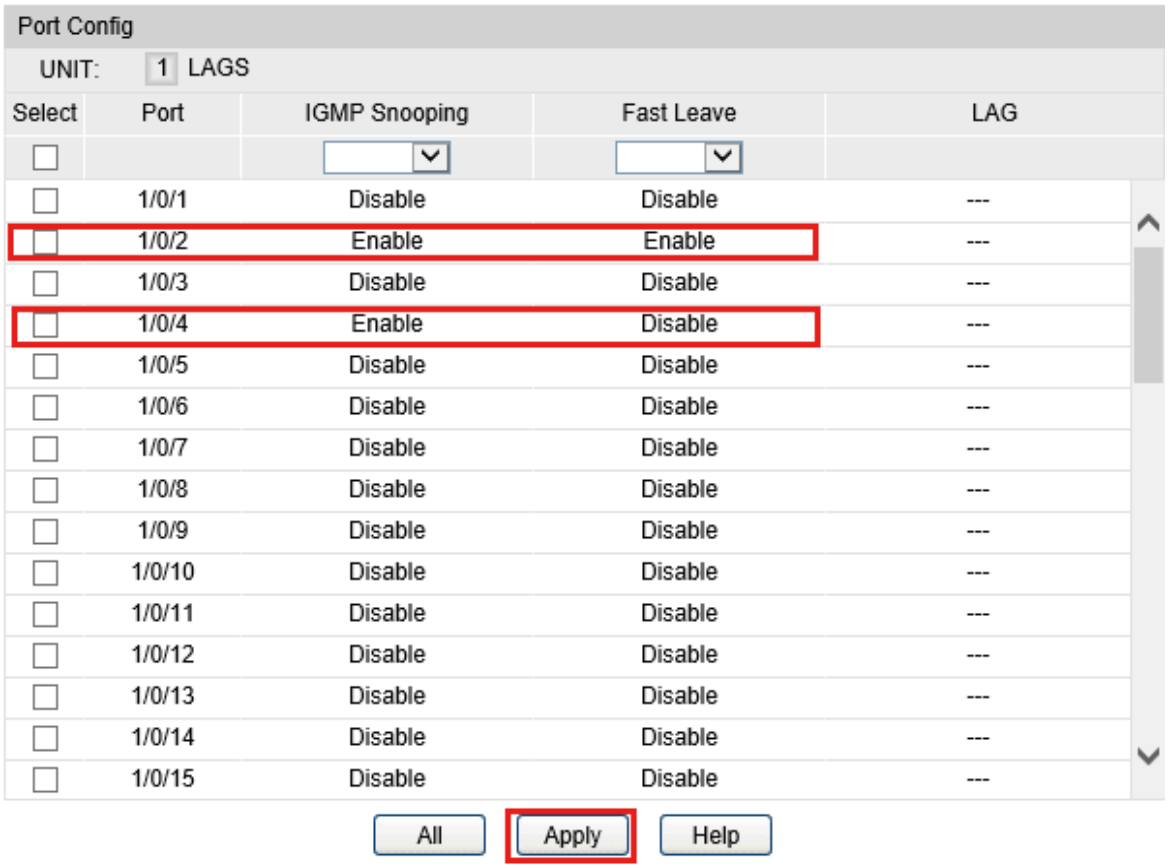


Note:

IGMP Snooping and MLD Snooping share the setting of Unknown Multicast, so you have to enable MLD Snooping globally on the **Multicast > MLD Snooping > Snooping Config** page at the same time.

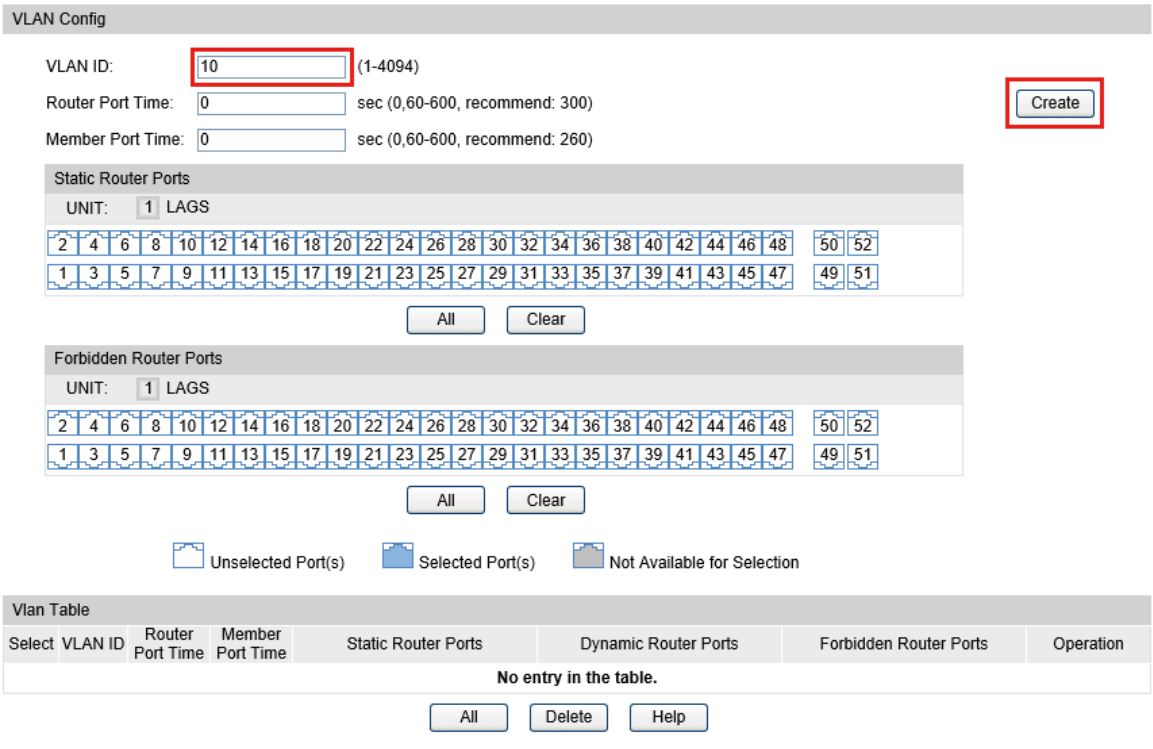
2) Choose the menu **Multicast > IGMP Snooping > Port Config** to load the following page. Enable IGMP Snooping on port 1/0/2 and port 1/0/4 and enable Fast Leave on port 1/0/2.

Figure 5-15 Configure IGMP Snooping Globally



3) Choose the menu **Multicast > IGMP Snooping > VLAN Config** to load the following page. Enable IGMP Snooping in VLAN 10.

Figure 5-16 Enable IGMP Snooping in the VLAN



4) Click **Save Config** to save the settings.

5.3.4 Using the CLI

1) Enable IGMP Snooping Globally.

   Switch#configure

   Switch(config)#ip igmp snooping

2) Configure Unknown Multicast as Discard globally.

   Switch(config)#ip igmp snooping drop unknown

3) Enable IGMP Snooping on port 1/0/2 and enable Fast Leave. On port 1/0/4, enable IGMP Snooping.

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

   Switch(config-if)#ip igmp snooping

   Switch(config-if)#ip igmp snooping immediate-leave

   Switch(config-if)#exit

   Switch(config)#interface gigabitEthernet 1/0/4

   Switch(config-if)#ip igmp snooping

   Switch(config-if)#exit

4) Enable IGMP Snooping in VLAN 10.

   Switch(config)#ip igmp snooping vlan-config 10

5) Save the settings.

   Switch(config)#end

   Switch#copy running-config startup-config

Verify the Configurations

Show global settings of IGMP Snooping:

Switch(config)#show ip igmp snooping

IGMP Snooping :Enable

Unknown Multicast :Discard

Last Query Times :2

Last Query Interval :1

Global Member Age Time :260

Global Router Age Time :300

Global Report Suppression :Disable

Global Authentication Accounting:Disable

Enable Port:Gi1/0/2,1/0/4

Enable VLAN:10

Show settings of IGMP Snooping on port 1/0/2:

Switch(config)#show ip igmp snooping interface gigabitEthernet 1/0/2 basic-config

Port IGMP-Snooping Fast-Leave

---- ------------ ----------

Gi1/0/2 enable enable

5.4 Example for Configuring Multicast Filtering

5.4.1 Network Requirements

Host B, Host C and Host D are in the same subnet. Host C and Host D only receive multicast data sent to 225.0.0.1, while Host B receives all multicast data except the one sent from 225.0.0.2.

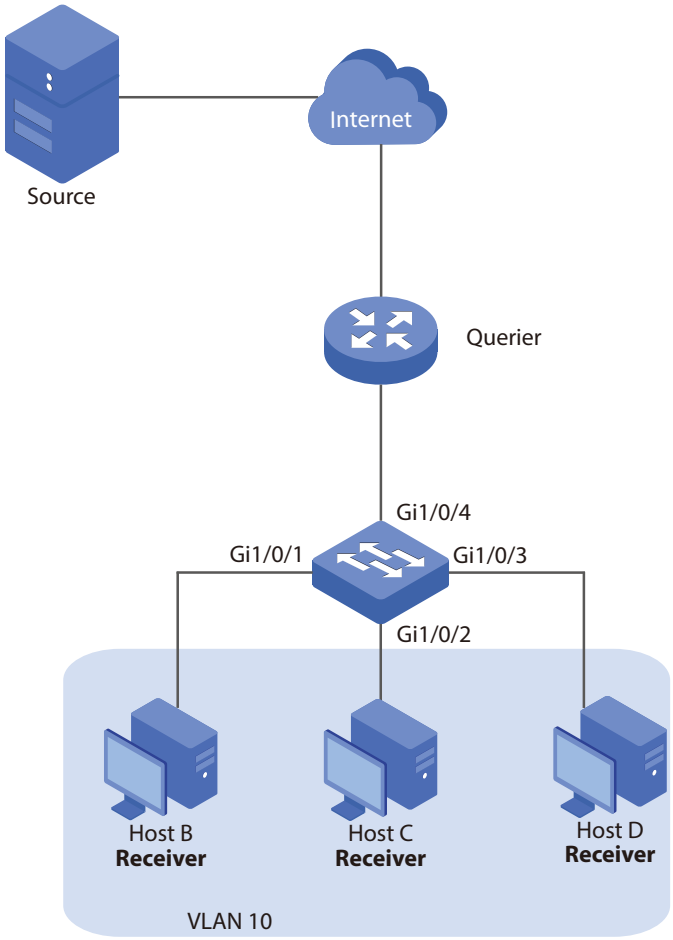
5.4.2 Configuration Scheme

With the functions for managing multicast groups, whitelist and blacklist mechanism (profile binding), the switch can only allow specific member ports to join specific multicast groups or disallow specific member ports to join specific multicast groups. You can achieve this filtering function by creating a profile and binding it to the corresponding member port.

5.4.3 Network Topology

As shown in the following network topology, Host B is connected to port 1/0/1, Host C is connected to port 1/0/2 and Host D is connected to port 1/0/3. They are all in VLAN 10.

Figure 5-17 Network Topology for Multicast Filtering



Demonstrated with T2600G-28TS, this section provides configuration procedures in two ways: using the GUI and using the CLI.

5.4.4 Using the GUI

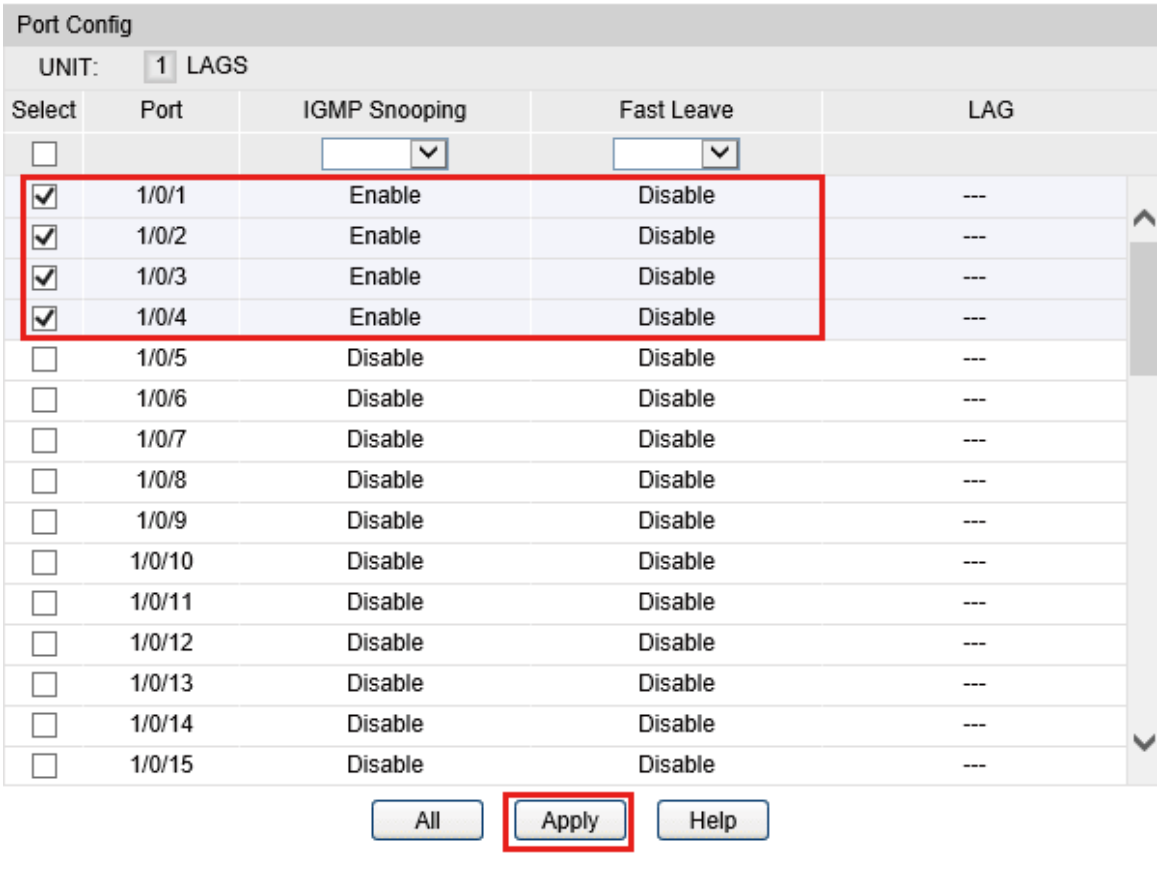
1) Choose the menu **Multicast > IGMP Snooping > Snooping Config** to load the following page. Enable IGMP Snooping globally, and keep the default values in the Router Port Time and Member Port Time fields.

Figure 5-18 Configure IGMP Snooping Globally



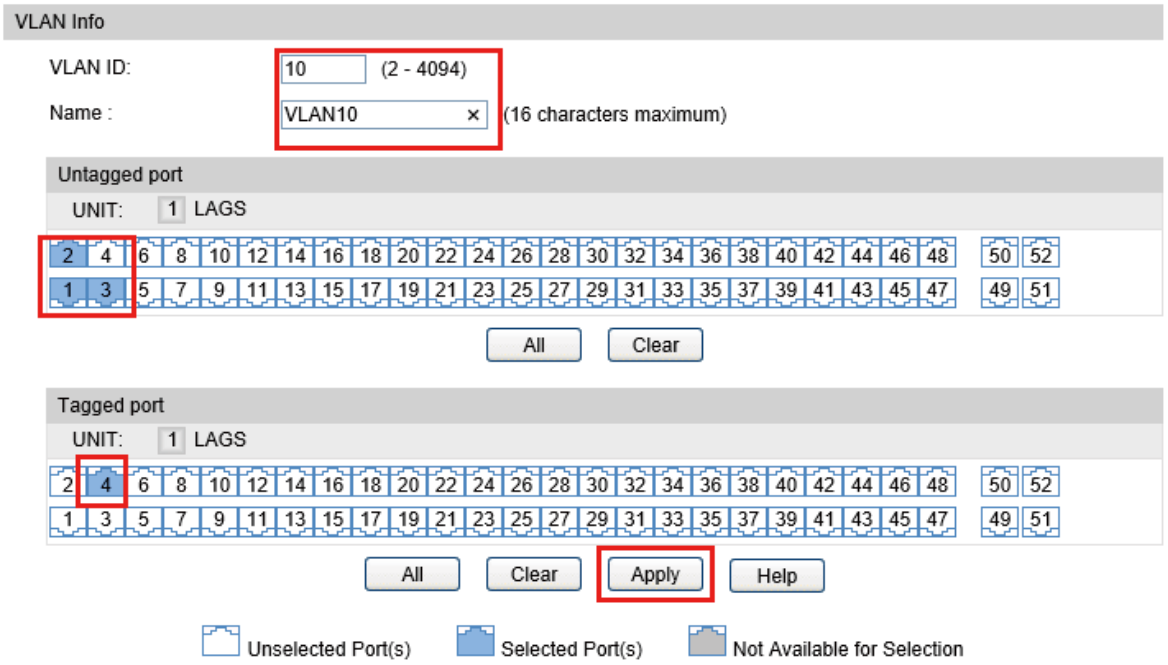
2) Choose the menu **Multicast > IGMP Snooping > Snooping Config** to load the following page.

Figure 5-19 Enable IGMP Snooping on the Port



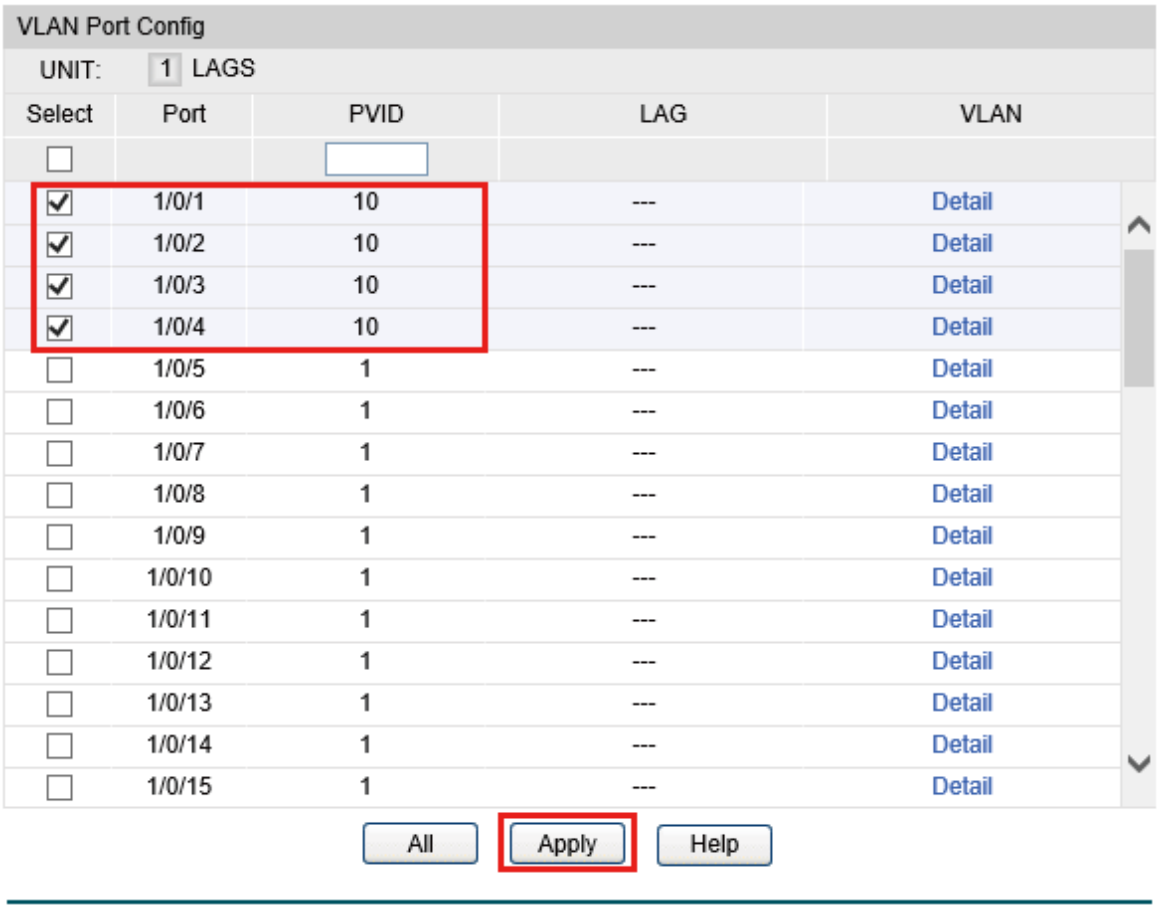
3) Choose the menu **VLAN > 802.1Q VLAN > VLAN Config** to load the following page. Create VLAN 10 and add Untagged port 1/0/1-3 and Tagged port 1/0/4 to VLAN 10.

Figure 5-20 Configure Link Type



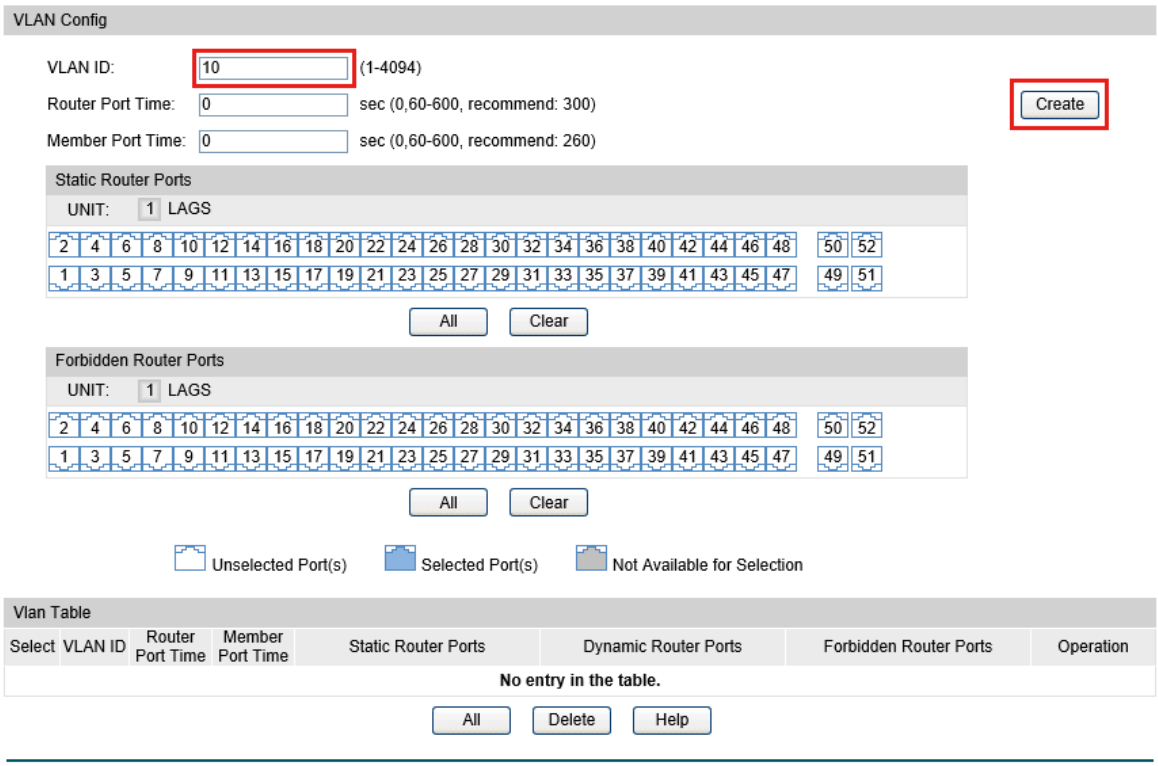
4) Choose the menu **VLAN > 802.1Q VLAN > Port** Config to load the following page. Configure the PVID of port 1/0/1-4 as 10.

Figure 5-21 Create VLAN and Add Member Ports



5) Choose the menu **Multicast > IGMP Snooping > VLAN Config** to load the following page. Enable IGMP Snooping in VLAN 10. Keep 0 as the Router Port Time and Member Port Time, which means the global settings will be used.

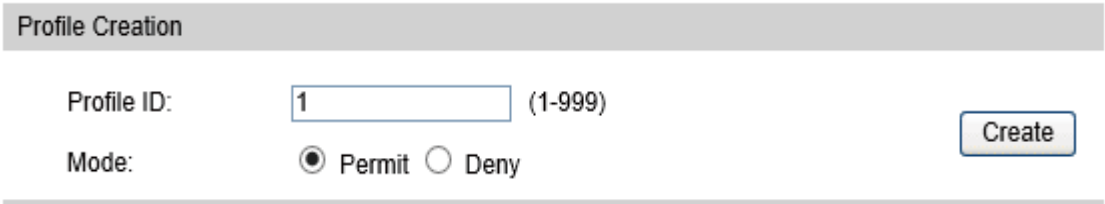
Figure 5-22 Enable IGMP Snooping in the VLAN



6) Specify the multicast data that Host C and Host D can receive.

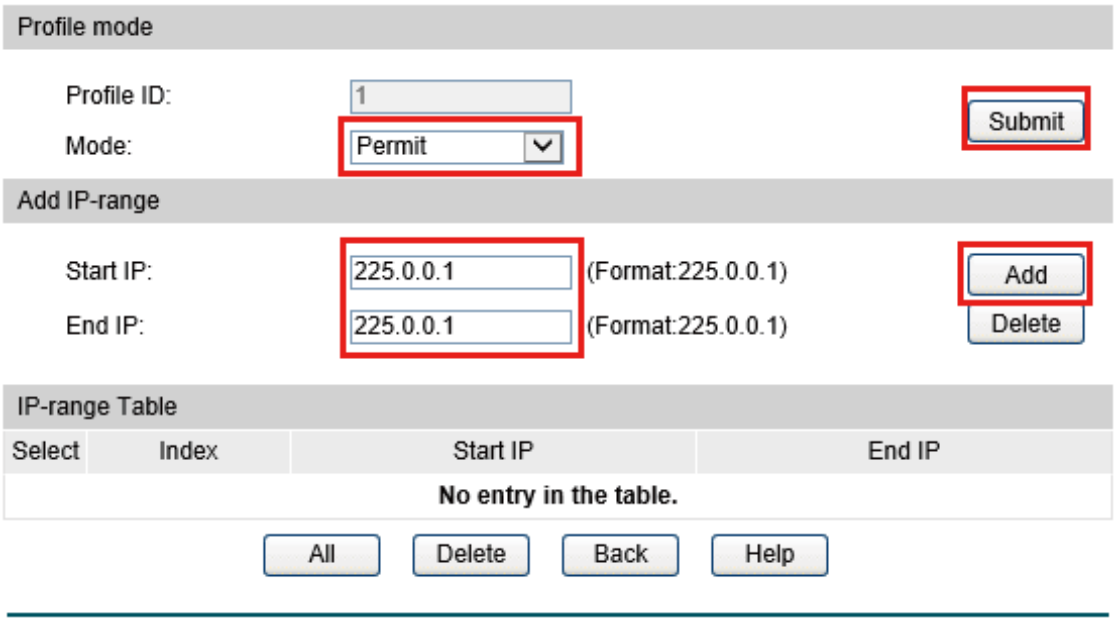
a. Choose the menu **Multicast > IGMP Snooping > Profile Config** to load the following page. Create Profile 1, select Permit as the Mode and click Create.

Figure 5-23 Create Profile 1



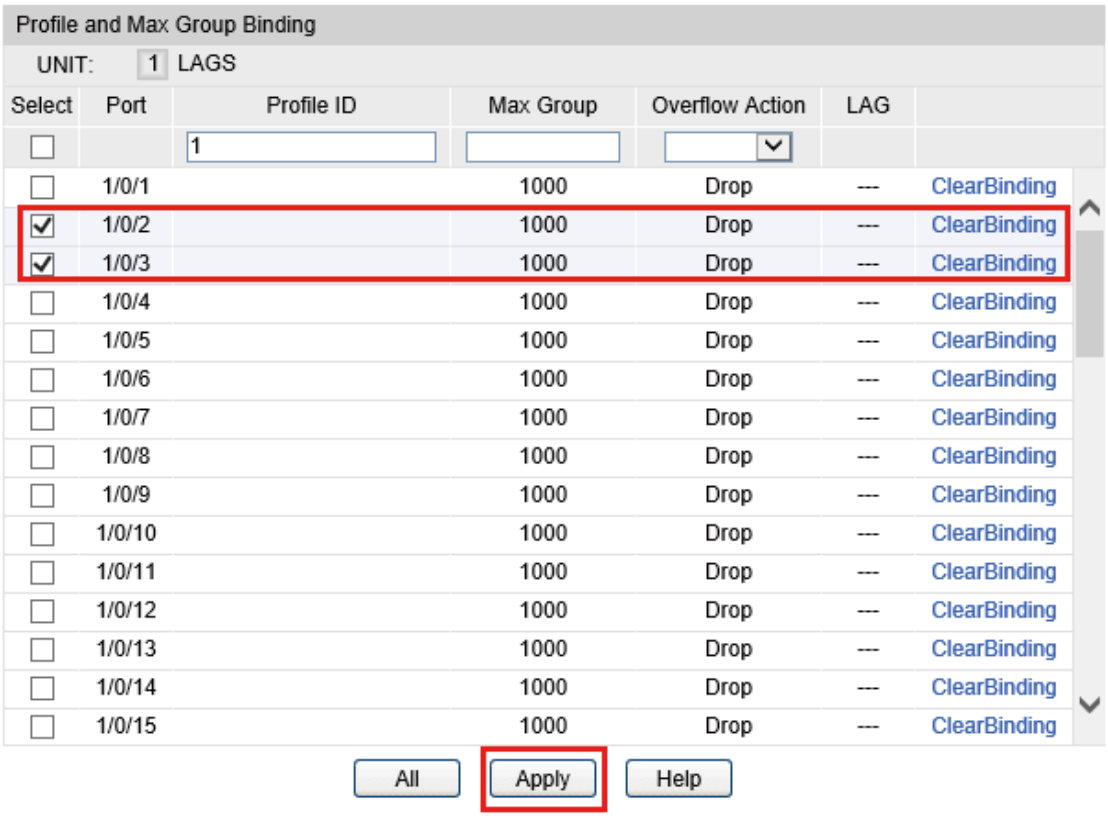
b. Choose the menu **Multicast > IGMP Snooping > Profile Config** to load the following page.

Figure 5-24 Edit Add IP-range in Profile 1



c. Choose the menu **Multicast > IGMP Snooping > Profile Binding** to load the following page. Select port 1/0/2 and port 1/0/3, enter 1 in the Profile ID field and click Apply to bind Profile 1 to these ports.

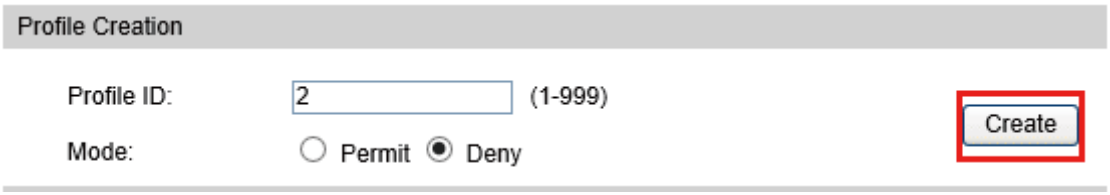
Figure 5-25 Bind Profile 1 to Port 1/0/2 and Port 1/0/3



7) Specify the multicast data that Host B can receive

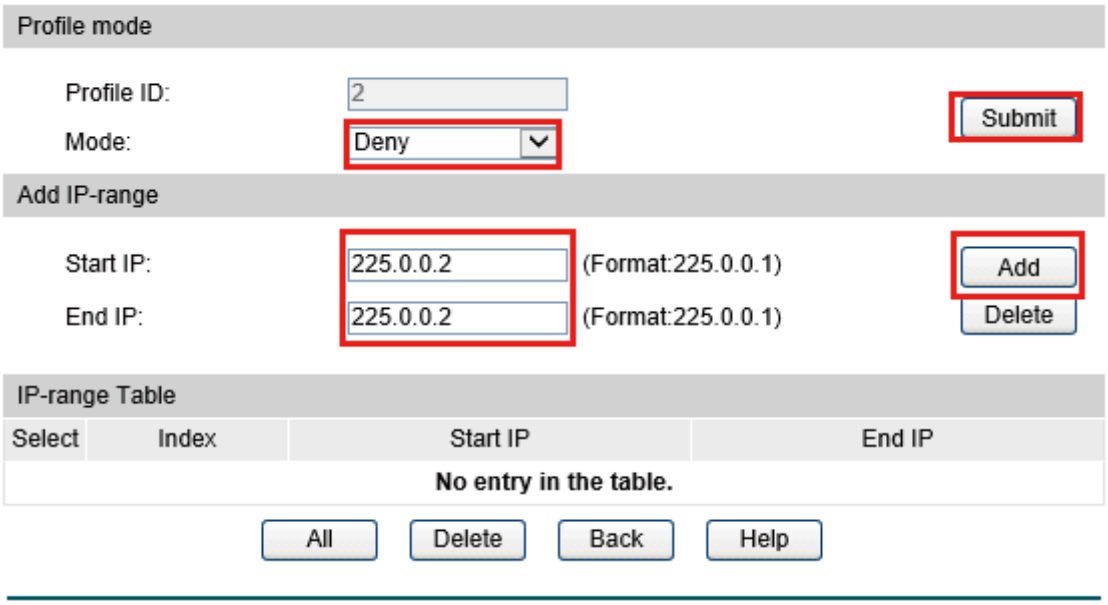
a. Choose the menu **Multicast > IGMP Snooping > Profile Config** to load the following page. Create Profile 2, select Deny as the Mode and click Create.

Figure 5-26 Profile 2



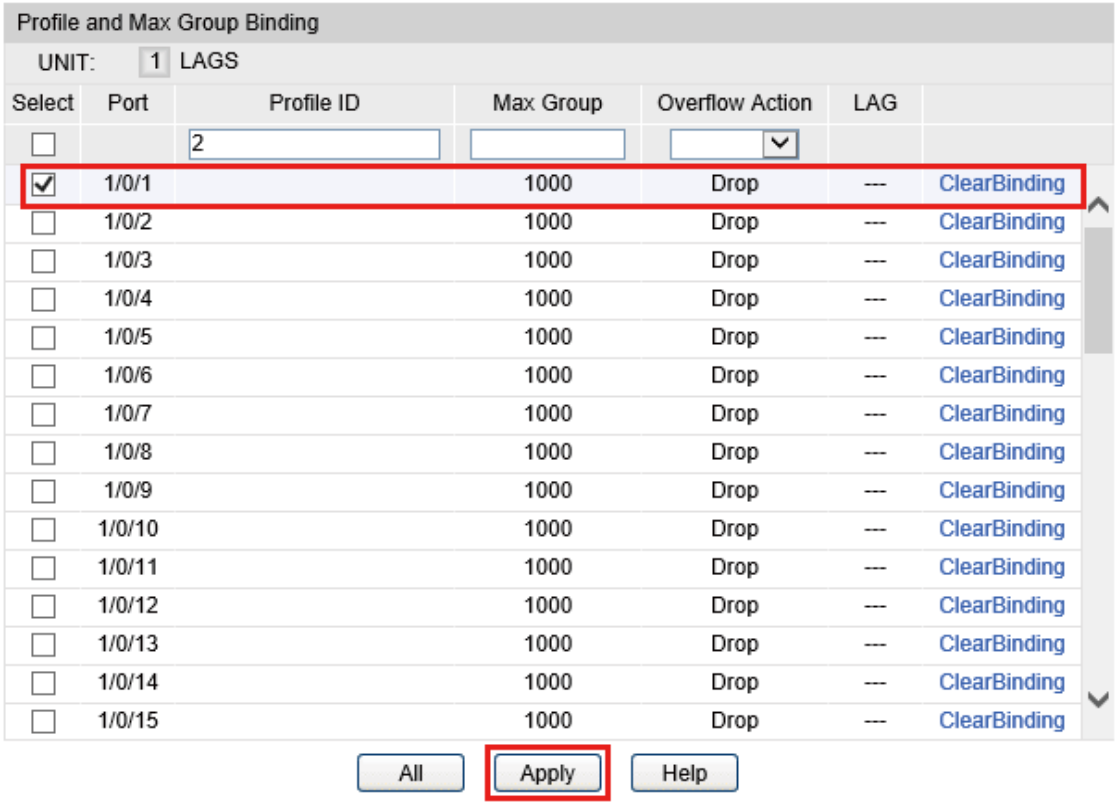
b. Choose the menu **Multicast > IGMP Snooping > Profile Config** to load the following page. In the IGMP Profile Info table, click Edit in the Profile 2 entry, enter 225.0.0.2 in both Start IP and End IP fields, and click Add.

Figure 5-27 Edit Add IP-range in Profile 2



c. Choose the menu **Multicast > IGMP Snooping > Profile Binding** to load the following page. Select port 1/0/1, enter 2 in the Profile ID field and click Apply to bind Profile 2 to this port.

Figure 5-28 Bind Profile 2 to Port 1/0/1



8) Click **Save Config** to save the settings.

5.4.5 Using the CLI

1) Enable IGMP Snooping Globally.

   Switch#configure

   Switch(config)#ip igmp snooping

2) Enable IGMP Snooping on port 1/0/1-4.

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

   Switch(config-if-range)#ip igmp snooping

   Switch(config-if-range)#exit

3) Create VLAN 10.

   Switch(config)#vlan 10

   Switch(config-vlan)#name vlan10

   Switch(config-vlan)#exit

4) Add port 1/0/1-3 to VLAN 10 and set the link type as untagged. Add port 1/0/4 to VLAN 10 and set the link type as tagged.

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

Switch(config-if-range)#switchport general allowed vlan 10 untagged

Switch(config-if-range)#exit

Switch(config)#interface gigabitEthernet 1/0/4

Switch(config-if)#switchport general allowed vlan 10 tagged

Switch(config-if)#exit

5) Set the PVID of port 1/0/1-4 as 10.

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

Switch(config-if-range)#switchport pvid 10

Switch(config-if-range)#exit

6) Enable IGMP Snooping in VLAN 10.

Switch(config)#ip igmp snooping vlan-config 10

Switch(config-if)#exit

7) Create Profile 1, configure the mode as permit, and add an IP range with both start IP and end IP being 225.0.0.1.

Switch(config)#ip igmp profile 1

Switch(config-igmp-profile)#permit

Switch(config-igmp-profile)#range 225.0.0.1 225.0.0.1

Switch(config-igmp-profile)#exit

8) Bind Profile 1 to Port 1/0/2 and Port 1/10/3.

Switch(config)#interface range gigabitEthernet 1/0/2-3

Switch(config-if-range)#ip igmp filter 1

Switch(config-if-range)#exit

9) Create Profile 2, configure the mode as deny, and add an IP range with both start IP and end IP being 225.0.0.2.

Switch(config)#ip igmp profile 2

Switch(config-igmp-profile)#deny

Switch(config-igmp-profile)#range 225.0.0.2 225.0.0.2

Switch(config-igmp-profile)#exit

10) Bind Profile 2 to Port 1/0/1.

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

Switch(config-if)#ip igmp filter 2

Switch(config-if)#exit

11) Save the settings.

```
Switch(config)#end
Switch#copy running-config startup-config
```

Verify the Configurations

Show global settings of IGMP Snooping:

```
Switch(config)#show ip igmp snooping
IGMP Snooping              :Enable
Unknown Multicast          :Pass
Last Query Times           :2
Last Query Interval        :1
Global Member Age Time     :260
Global Router Age Time     :300
Global Report Suppression  :Disable
Global Authentication Accounting:Disable
Enable Port:Gi1/0/1-4
Enable VLAN:10
```

Show all profile bindings:

```
Switch(config)#show ip igmp profile
IGMP Profile 1
  permit
  range 225.0.0.1 225.0.0.1
  Binding Port(s)
   Gi1/0/2-3
IGMP Profile 2
  deny
  range 225.0.0.2 225.0.0.2
  Binding Port(s)
   Gi1/0/1
```

6 Appendix: Default Parameters

6.1 Default Parameters for IGMP Snooping

Table 6-1 Default Parameters of IGMP Snooping

Function	Parameter	Default Setting
Global Settings of IGMP Snooping	IGMP Snooping	Disabled
	Unknown Multicast	Forward
	Report Message Suppression	Disabled
	Router Port Time	300 seconds
	Member Port Time	260 seconds
	Last Listener Query Interval	1 second
	Last Listener Query Count	2
IGMP Snooping Settings on the Port	IGMP Snooping	Disabled
	Fast Leave	Disabled
IGMP Snooping Settings in the VLAN	Enable or Not	Disabled
	Router Port Time	0, use global settings.
	Member Port Time	0, use global settings.
Multicast VLAN	Multicast VLAN	None
	Router Port Time	0, use global settings.
	Member Port Time	0, use global settings.
	Replace Source IP	0.0.0.0, indicating no replacement.
IGMP Snooping Querier	Enable or Not	Disabled
	Query Interval	60 seconds
	Max Response Time	10 seconds
	General Query Source IP	192.168.0.1

Function	Parameter	Default Setting
IGMP Accounting and Authentication	Global Settings of IGMP Accounting	Disabled
	IGMP Authentication	Disabled

6.2 Default Parameters for MLD Snooping

Table 6-2 Default Parameters of MLD Snooping

Function	Parameter	Default Setting
Global Settings of IGMP Snooping	MLD Snooping	Disabled
	Unknown Multicast	Forward
	Report Message Suppression	Disabled
	Router Port Time	300 seconds
	Member Port Time	260 seconds
	Last Listener Query Interval	1 second
	Last Listener Query Count	2
MLD Snooping on the Port	MLD Snooping	Disabled
	Fast Leave	Disabled
MLD Snooping in the VLAN	Enable or Not	Disabled
	Router Port Time	0, use global settings.
	Member Port Time	0, use global settings.
Multicast VLAN	Multicast VLAN	None
	Router Port Time	0, use global settings.
	Member Port Time	0, use global settings.
	Replace Source IP	::, indicating no replacement.

Function	Parameter	Default Setting
IGMP Snooping Querier	Enable or Not	Disabled
	Query Interval	60 seconds
	Max Response Time	10 seconds
	General Query Source IP	FE80::02FF:FFFF:FE00:0001

Part 18

Configuring Logical Interfaces

CHAPTERS

1. Overview
2. Logical Interfaces Configurations
3. Appendix: Default Parameters

1 Overview

Interfaces of a device are used to exchange data and interact with interfaces of other network devices. Interfaces are classified into physical interfaces and logical interfaces.

- Physical interfaces are the ports on the front panel or rear panel of the switch.
- Logical interfaces are manually configured and do not physically exist, such as loopback interfaces and routing interfaces.

This chapter introduces the configurations for logical interfaces. The supported types of logical interfaces are shown as below:

Table 1-1 Supported Types of Logical Interfaces

Type	Description
VLAN Interface	A Layer 3 interface with which different VLANs can communicate with each other.
Loopback Interface	An interface of which the status is always up.
Routed Port	A physical port configured as a Layer 3 port.
Port-channel Interface	Several Ethernet ports bound together and configured as a Layer 3 interface.

2 Logical Interfaces Configurations

To complete IPv4 interface configuration, follow these steps:

1) Create a Layer 3 interface
2) Configure IPv4 parameters of the created interface
3) View detailed information of the created interface

To complete IPv6 interface configuration, follow these steps:

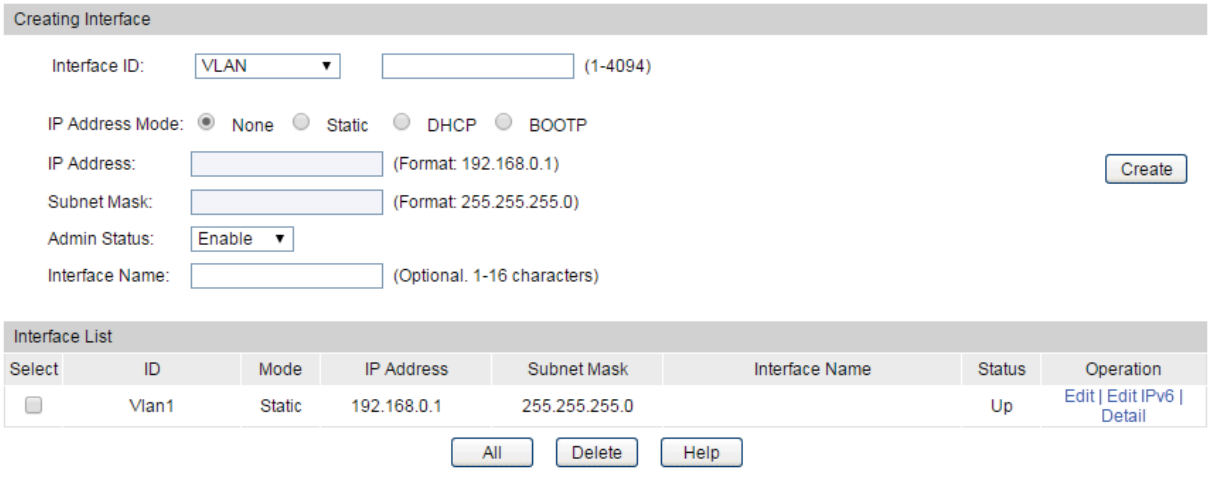
1) Create a Layer 3 interface
2) Configure IPv6 parameters of the created interface
3) View detailed information of the created interface

2.1 Using the GUI

2.1.1 Creating a Layer 3 Interface

Choose the menu **Routing> Interface > Interface Config** to load the following page.

Figure 2-1 Creating a Layer 3 Interface



1) In the **Creating Interface** section, specify an interface ID and configure relevant parameters for the interface according to your needs. Then click **Create**.

Interface ID	Select an interface type and enter the ID of the interface.

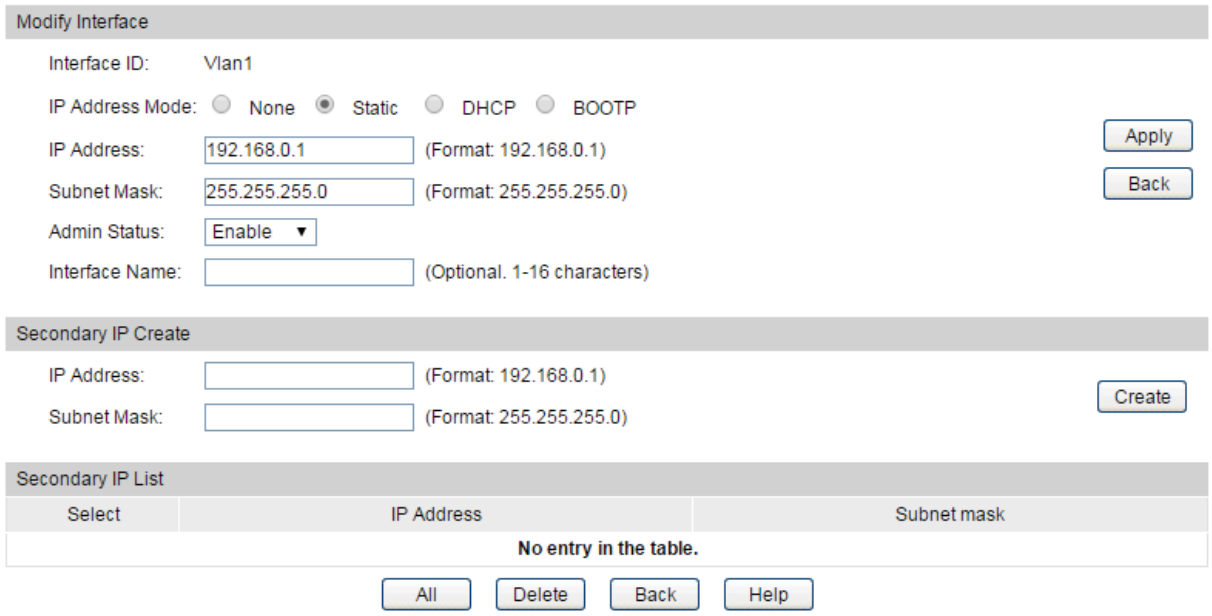
IP Address Mode	Specify the IP address assignment mode of the interface. **None:** No IP address will be assigned. **Static:** Assign an IP address manually. **DHCP:** Assign an IP address through DHCP . **BOOTP:** Assign an IP address through BOOTP.
IP Address	Specify the IP address of the interface if you choose "Static" as the IP address assignment mode.
Subnet Mask	Specify the subnet mask of the interface's IP address.
Admin Status	Enable or disable the interface's Layer 3 capabilities.
Interface Name	(Optional) Enter the name of the interface.

2) In the **Interface List** section, you can view the corresponding interface entry you create.

2.1.2 Configuring IPv4 Parameters of the Interface

In **Figure 2-1** you can view the corresponding interface entry you create in the **Interface List** section. On the corresponding interface entry, click **Edit** to load the following page and configure the IPv4 parameters of the interface.

Figure 2-2 Configuring the IPv4 Parameters



1) In the **Modify Interface** section, specify an interface ID and configure relevant parameters for the interface according to your actual needs. Then click **Apply**.

Interface ID	Select an interface type and enter the ID of the interface.

IP Address Mode	Specify the IP address assignment mode of the interface. **None:** No IP address will be assigned. **Static:** Assign an IP address manually. **DHCP:** Assign an IP address through DHCP . **BOOTP:** Assign an IP address through BOOTP.
IP Address	Specify the IP address of the interface if you choose "Static" as the IP address assignment mode.
Subnet Mask	Specify the subnet mask of the interface's IP address.
Admin Status	Enable or disable the interface's Layer 3 capabilities.
Interface Name	(Optional) Enter the name of the interface.

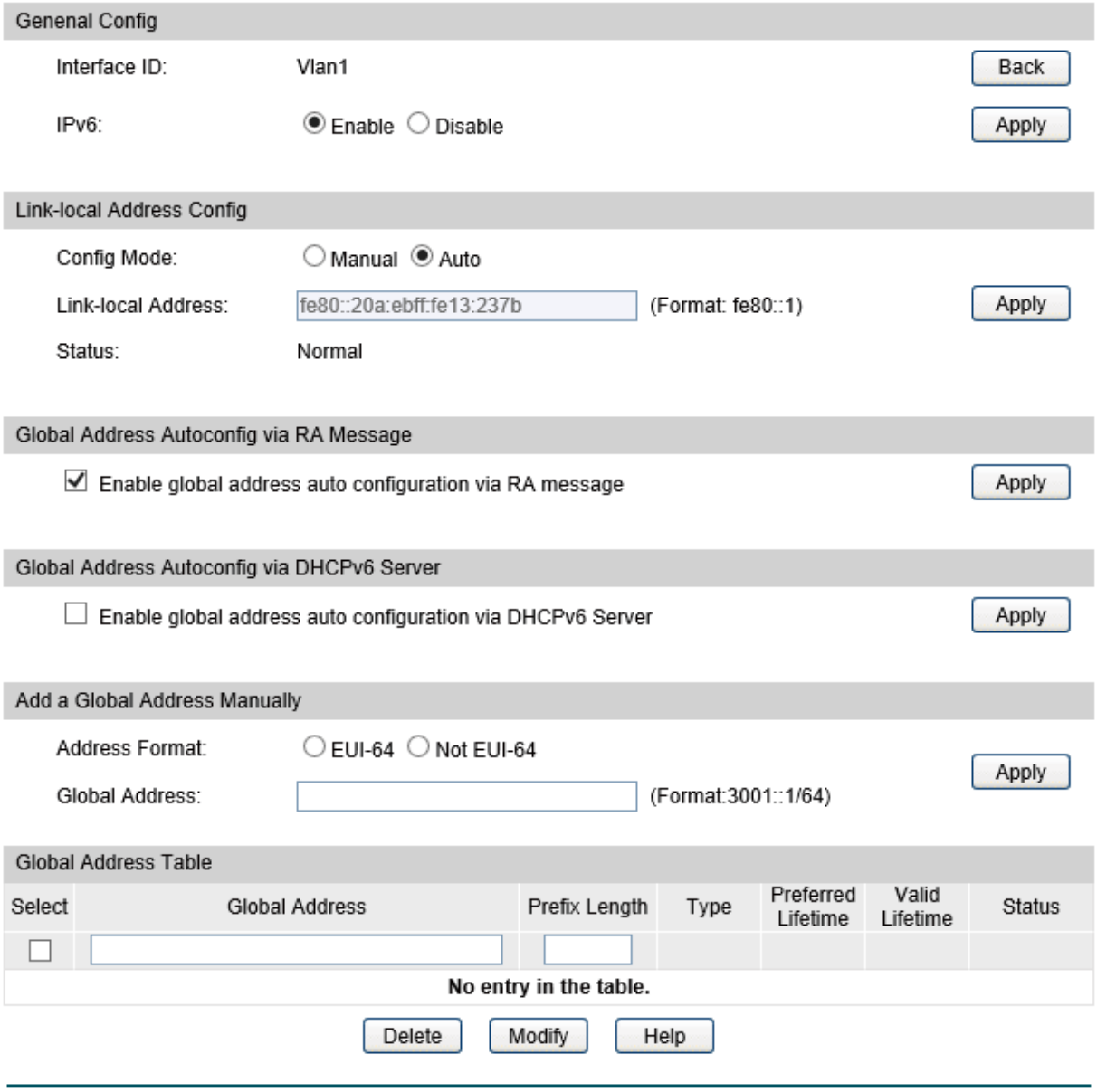
2) In the **Secondary IP Create** section, configure the secondary IP for the specified interface which allows you to have two logical subnets using one physical subnet. Then click **Create**.

3) In the **Secondary IP List** section, you can view the corresponding secondary IP entry you create.

2.1.3 Configuring IPv6 Parameters of the Interface

In **Figure 2-1**, you can view the corresponding interface entry you create in the **Interface List** section. On the corresponding interface entry, click **Edit IPv6** to load the following page and configure the IPv6 parameters of the interface.

Figure 2-3 Configuring the IPv6 Parameters



1) Enable IPv6 function on the interface of switch in the **General Config** section. Then click **Apply**.

Interface ID	Displays the interface ID.
IPv6	Enable or disable IPv6 function on the interface of switch.

2) Configure the IPv6 link-local address of the interface manually or automatically in the **Link-local Address Config** section. Then click **Apply**.

Config Mode	Select the link-local address configuration mode. **Manual:** With this option selected, you can assign a link-local address manually. **Auto:** With this option selected, the switch will generate a link-local address automatically.

Link-local Address	Enter a link-local address if you choose "Manual" as the link-local address configuration mode.
Status	Displays the status of the link-local address. **Normal:** Indicates that the link-local address is normal. **Try:** Indicates that the link-local address may be newly configured. **Repeat:** Indicates that the link-local address is duplicate. It is illegal to access the switch using the IPv6 address (including link-local and global address).

3) Configure one or more IPv6 global addresses of the interface via following three ways:

Via RA Message:

Enable global address auto configuration via RA message	With this option enabled, the switch automatically configures a global address and other information according to the address prefix and other configuration parameters from the received RA (Router Advertisement) message.

Via DHCPv6 Server:

Enable global address auto configuration via DHCPv6 Server	With this option enabled, the switch will try to obtain the global address from the DHCPv6 Server.

Manually:

Address Format	Select the global address format according to your needs. **EUI-64:** Indicates that you only need to specify an address prefix, then the system will create a global address automatically. **Not EUI-64:** Indicates that you have to specify an intact global address.
Global Address	When EUI-64 is selected, please input the address prefix here, otherwise, please input an intact IPv6 address here.

4) View the global address entry in the Global Address Table.

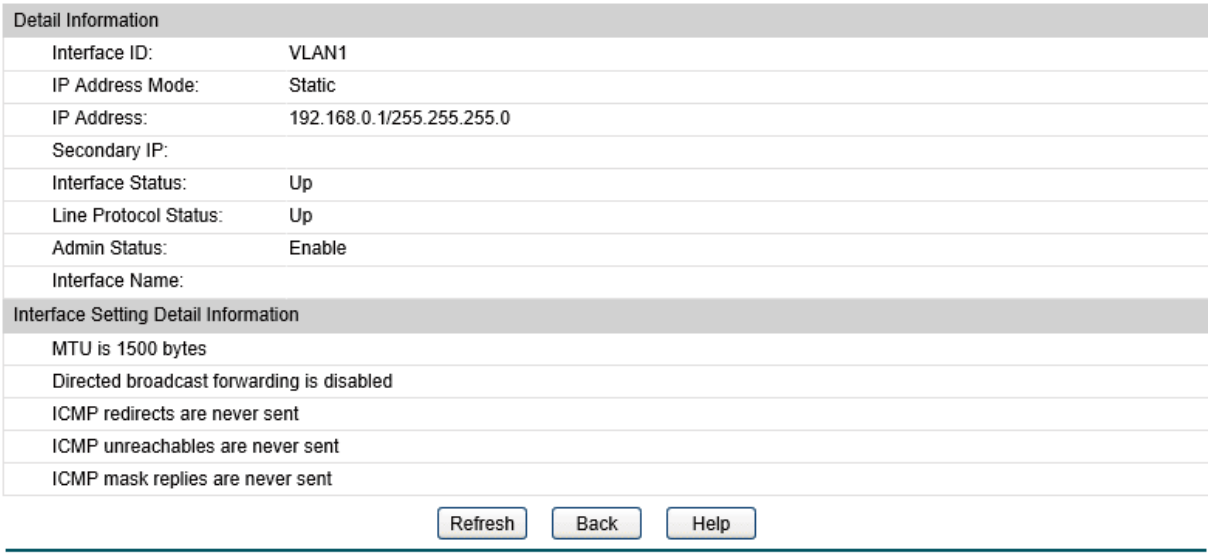
Global Address	View and modify the global address.
Prefix Length	View and modify the prefix length of the global address.
Type	Displays the configuration mode of the global address. **Manual:** Indicates that the corresponding address is configured manually. **Auto:** Indicates that the corresponding address is created automatically using the RA message or obtained from the DHCPv6 Server.
Preferred Lifetime	Displays the preferred lifetime of the global address.

Valid Lifetime	Displays the valid lifetime of the global address.
Status	Displays the status of the global address. **Normal:** Indicates that the global address is normal. **Try:** Indicates that the global address may be newly configured. **Repeat:** Indicates that the global address is duplicate. It is illegal to access the switch using this global address.

2.1.4 Viewing Detail Information of the Interface

In **Figure 2-1** you can view the corresponding interface entry you create in the **Interface List** section. On the corresponding interface entry, click **Detail** to load the following page and view the detail information of the interface.

Figure 2-4 Viewing the detail information of the interface



2.2 Using the CLI

2.2.1 Creating a Layer 3 Interface

Follow these steps to create a Layer 3 interface. You can create a VLAN interface, a loopback interface, a routed port or a port-channel interface according to your needs.

Step 1	**configure** Enter global configuration mode.

Step 2	Create a VLAN interface: **interface vlan** *vlan-id* *vlan-id*: Specify an IEEE 802.1Q VLAN ID that already exists, ranging from 1 to 4094. Create a loopback interface: **interface loopback {** *id* **}** *id:* Specify the ID of the loopback interface, ranging from 1 to 64. Create a routed port: **interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Enter interface configuration mode. *port*: Specify the Ethernet port number, for example 1/0/1. *port-list:* Specify the list of Ethernet ports, for example 1/0/1-3, 1/0/5. **no switchport** Switch the Layer 2 port into the Layer 3 routed port. Create a port-channel interface: **interface range port-channel** *port-channel-list* *port-channel-list:* The list of the port-channel interface, for example 1-3, 5.
Step 3	**description** *string* Specify a description to the Layer 3 interface, including VLAN interface, loopback interface, routed port and port-channel interface. *string:* The description of the Layer 3 interface, ranging from 1 to 32 characters.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create a VLAN interface with a description of VLAN-2.

Switch#configure

Switch(config)#interface vlan 2

Switch(config-if)#description VLAN-2

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.2 Configuring IPv4 Parameters of the Interface

Follow these steps to configure the IPv4 parameters of the interface.

Step 1	**configure** Enter global configuration mode.
Step 2	**interface** { *interface-type* } { *interface-number* } Enter layer 3 interface configuration mode. *interface-type*: Type of the layer 3 interface, including fastEthernet, gigabitEthernet, ten-gigabitEthernet, loopback and VLAN. *interface-number:* Number of the interface.
Step 3	Automatically assign an IP Address for the interface via DHCP or BOOTP: **ip address-alloc {** dhcp **|** bootp **}** Specify the IP Address assignment mode of the interface. dhcp: Specify the Layer 3 interface to obtain an IPv4 address from the DHCP Server. bootp: Specify the Layer 3 interface to obtain an IPv4 address from the BOOTP Server. Manually assign an IP Address for the interface: **ip address {** *ip-addr* **} {** *mask* **} [secondary]** Configure the IP address and subnet mask for the specified interface manually. *ip-addr*: Specify thse IP address of the Layer 3 interface. *mask*: Specify the subnet mask of the Layer 3 interface. **secondary:** Specify the interface's secondary IP address which allows you to have two logical subnets using one physical subnet. If this parameter is omitted here, the configured IP address is the interface's primary address.
Step 4	**show ip interface brief** Verify the summary information of the Layer 3 interfaces.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the IPv4 parameters of a routed port, including setting a static IP address for the port and enabling the Layer 3 capabilities:

Switch#configure

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

Switch(config-if)#no switchport

Switch(config-if)#ip address 192.168.0.100 255.255.255.0

Switch(config-if)#show ip interface brief

Interface	IP-Address	Method	Status	Protocol	Shutdown
Gi1/0/1	192.168.0.100/24	Static	Up	Up	no

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.3 Configuring IPv6 Parameters of the Interface

Follow these steps to configure the IPv6 parameters of the interface.

Step 1	**configure** Enter global configuration mode.
Step 2	**interface** { *interface-type* } { *interface-number* } Enter layer 3 interface configuration mode. *interface-type*: Type of the layer 3 interface, including fastEthernet, gigabitEthernet, ten-gigabitEthernet, loopback and VLAN. *interface-number:* Number of the interface.
Step 3	**ipv6 enable** Enable the IPv6 function on the speicified Layer 3 interface. By default, it is enabled on VLAN interface 1. IPv6 function can only be enabled on one Layer 3 interface at a time.
Step 4	Configure the IPv6 link-local address for the specified interface: Manually configure the ipv6 link-local address for the specified interface: **ipv6 address** *ipv6-addr* **link-local** *ipv6-addr*: Specify the link-local address of the interface. It should be a standardized IPv6 address with the prefix fe80::/10, otherwise this command will be invalid. Automatically configure the ipv6 link-local address for the specified interface: **ipv6 address autoconfig**

Step 5	Configure the IPv6 global address for the specified interface: Automatically configure the interface's global IPv6 address via RA message: **ipv6 address ra** Configure the interface's global IPv6 address according to the address prefix and other configuration parameters from its received RA (Router Advertisement) message. Automatically configure the interface's global IPv6 address via DHCPv6 server: **ipv6 address dhcp** Enable the DHCPv6 Client function. When this function is enabled, the Layer 3 interface will try to obtain the IPv6 address from DHCPv6 server. Manually configure the interface's global IPv6 address: **ipv6 address** *ipv6-addr* *ipv6-addr:* The Global IPv6 address with network prefix, for example 3ffe::1/64. **ipv6 address** *ipv6-addr* **eui-64** Specify a global IPv6 address with an extended unique identifier (EUI) in the low-order 64 bits of the IPv6 address. Specify only the network prefix; the last 64 bits are automatically computed from the switch MAC address. This enables IPv6 processing on the interface.
Step 6	**show ipv6 interface** Verify the configured ipv6 information of the interface.
Step 7	**end** Return to privileged EXEC mode.
Step 8	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable the IPv6 function and configure the IPv6 parameters of a vlan interface:

Switch#configure

Switch(config)#interface vlan 2

Switch(config-if)#ipv6 enable

Switch(config-if)#ipv6 address autoconfig

Switch(config-if)#ipv6 address dhcp

Switch(config-if)#show ipv6 interface

Vlan2 is up, line protocol is up

IPv6 is enable, Link-Local Address: fe80::20a:ebff:fe13:237b[NOR]

Global Address RA: Disable

Global Address DHCPv6: Enable

Global unicast address(es): ff02::1:ff13:237b

Joined group address(es): ff02::1

ICMP error messages limited to one every 1000 milliseconds

ICMP redirects are enable

MTU is 1500 bytes

ND DAD is enable, number of DAD attempts: 1

ND retrans timer is 1000 milliseconds

ND reachable time is 30000 milliseconds

Switch(config-if)#end

Switch#copy running-config startup-config

3 Appendix: Default Parameters

Default settings of interface are listed in the following tables.

Table 3-1 Configuring the IPv4 Parameters of the Interface

Parameter	Default Setting
Interface ID	VLAN
IP Address Mode	None
Admin Status	Enable
Recovery mode	Auto

Table 3-2 Configuring the IPv6 Parameters of the Interface

Parameter	Default Setting
IPv6	Disable On VLAN interface 1, it is enabled by default.
Config Mode	Auto
Enable global address auto configuration via RA message	Enable
Enable global address auto configuration via DHCPv6 Server	Disable

Part 19

Configuring Static Routing

CHAPTERS

1. Overview
2. IPv4 Static Routing Configuration
3. IPv6 Static Routing Configuration
4. Viewing Routing Table
5. Example for Static Routing
6. Appendix: Default Parameter

1 Overview

Static routing is a form of routing that is configured manually by adding non-aging entries into a routing table. The manually-configured routing information guides the router in forwarding data packets to the specific destination. On a simple network with a small number of devices, you only need to configure static routes to ensure that the devices from different subnets can communicate with each other. On a complex large-scale network, static routes ensure stable connectivity for important applications because the static routes remain unchanged even when the topology changes.

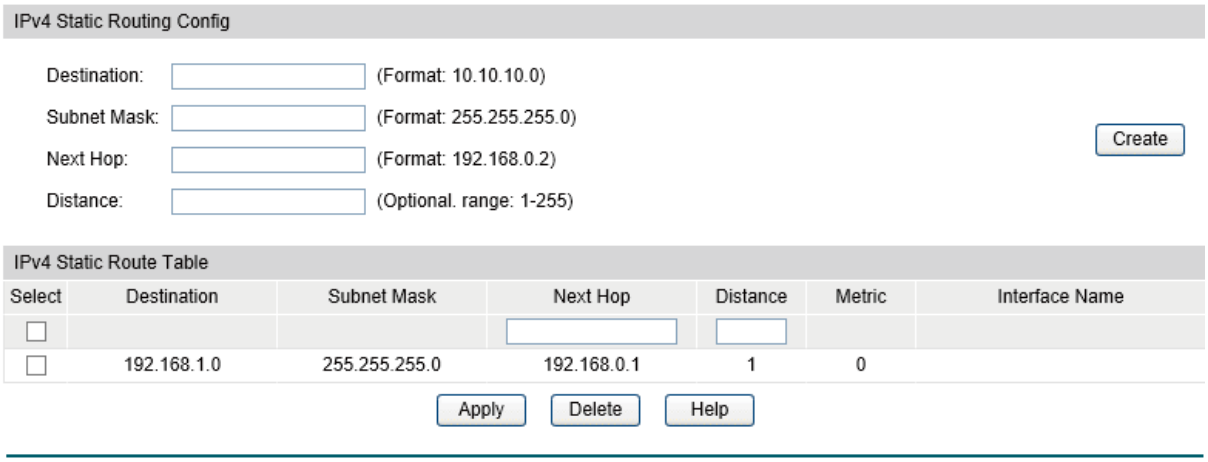
The switch supports IPv4 static routing and IPv6 static routing.

2 IPv4 Static Routing Configuration

2.1 Using the GUI

Choose the menu **Routing> Static Routing > IPv4 Static Routing Config** to load the following page.

Figure 2-1 Configuring the IPv4 Static Routing



1) In the **IPv4 Static Routing Config** section, configure the corresponding parameters to add an IPv4 static route. Then click **Create**.

Destination	Specify the destination IPv4 address of the packets.
Subnet Mask	Specify the subnet mask of the destination IPv4 address.
Next Hop	Specify the IPv4 gateway address to which the packet should be sent next.
Distance	Specify the administrative distance, which is a rating of the trustworthiness of the routing information. A higher value means a lower trust rating. When more than one routing protocols have routes to the same destination, only the route that has the shortest distance will be recorded in the IP routing table. The valid values are from 1 to 255 and the default value is 1.

2) In the **IPv4 Static Route Table** section, you can view and modify the IPv4 static routing entries.

2.2 Using the CLI

Follow these steps to create an IPv4 static route.

Step 1	**configure** Enter global configuration mode.
Step 2	**ip route {** *dest-address* **} {** *mask* **} {** *next-hop-address* **} [** *distance* **]** Add an IPv4 static route. *dest-address:* Specify the destination IPv4 address of the packets. *mask:* Specify the subnet mask of the destination IPv4 address. *next-hop-address:* Specify the IPv4 gateway address to which the packet should be sent next. *distance:* Specify the administrative distance, which is a rating of the trustworthiness of the routing information. A higher value means a lower trust rating. When more than one routing protocols have routes to the same destination, only the route that has the shortest distance will be recorded in the IP routing table. The valid values are from 1 to 255 and the default value is 1.
Step 3	**show ip route [** static | connected **]** Verify the IPv4 route entries of the specified type.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create an IPv4 static route with the destination IP address as 192.168.2.0, the subnet mask as 255.255.255.0 and the next-hop address as 192.168.0.2:

Switch#configure

Switch(config)#ip route 192.168.2.0 255.255.255.0 192.168.0.2

Switch(config)#show ip route

Codes: C - connected, S - static

* - candidate default

C 192.168.0.0/24 is directly connected, Vlan1

S 192.168.2.0/24 [1/0] via 192.168.0.2, Vlan1

Switch(config)#end

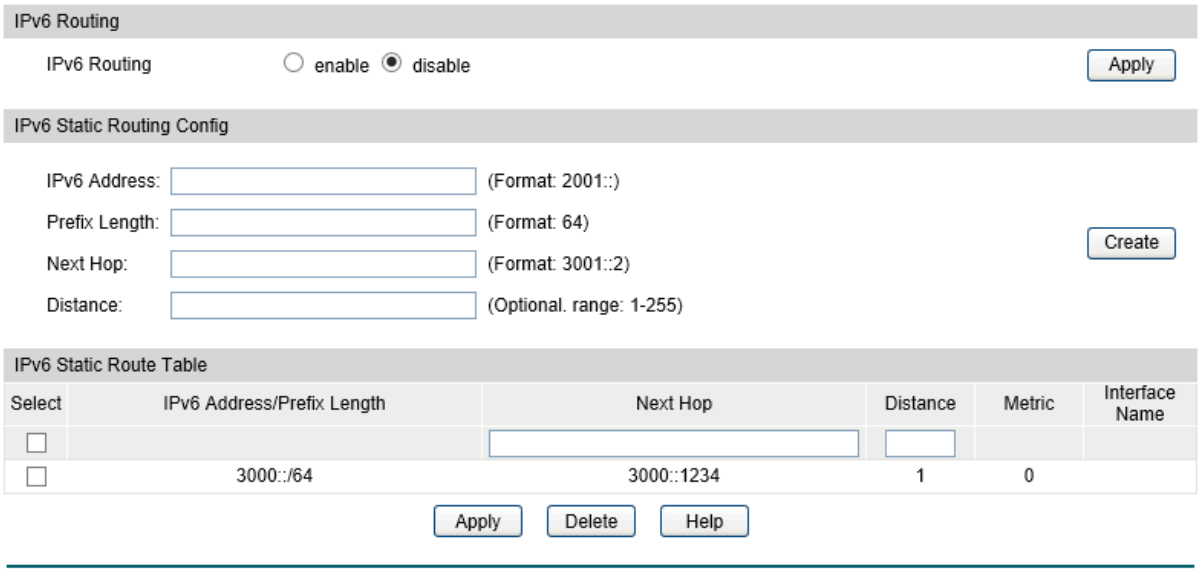
Switch#copy running-config startup-config

3 IPv6 Static Routing Configuration

3.1 Using the GUI

Choose the menu **Routing> Static Routing > IPv6 Static Routing Config** to load the following page.

Figure 3-1 Configuring the IPv6 Static Routing



1) In the **IPv6 Routing** section, enable IPv6 routing function and click **Apply**.
2) In the **IPv6 Static Routing Config** section, configure corresponding parameters to add an IPv6 static route. Then click **Create**.

IPv6 Address	Specify the destination IPv6 address of the packets.
Prefix Length	Specify the prefix length of the IPv6 address.
Next Hop	Specify the IPv6 gateway address to which the packet should be sent next.
Distance	Specify the administrative distance, which is a rating of the trustworthiness of the routing information. A higher value means a lower trust rating. When more than one routing protocols have routes to the same destination, only the route that has the shortest distance will be recorded in the IP routing table. The valid values are from 1 to 255 and the default value is 1.

3) In the **IPv6 Static Route Table** section, you can view and modify the IPv6 static routing entries.

3.2 Using the CLI

Follow these steps to enable IPv6 routing function and create an IPv6 static route.

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 routing** Enable the IPv6 routing function on the specified layer 3 interface.
Step 3	**ipv6 route {** *ipv6-dest-address* **} {** *next-hop-address* **} [** *distance* **]** Add an IPv6 static route. *ipv6-dest-address:* Specify the destination IPv6 address of the packets, in the format of X:X:X:X::X/<0-128>. *next-hop-address:* Specify the IPv6 gateway address to which the packet should be sent next. *distance:* Specify the administrative distance, which is a rating of the trustworthiness of the routing information. A higher value means a lower trust rating. When more than one routing protocols have routes to the same destination, only the route that has the shortest distance will be recorded in the IP routing table. The valid values are from 1 to 255 and the default value is 1.
Step 4	**show ipv6 route [** static | connected **]** Verify the IPv6 route entries of the specified type.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create an IPv6 static route with the destination IP address as 3200::/64 and the next-hop address as 3100::1234:

Switch#configure

Switch(config)#ipv6 route 3200::/64 3100::1234

Switch(config)#show ipv6 route static

Codes: C - connected, S - static

* - candidate default

C 3000::/64 is directly connected, Vlan1

S 3200::/64 [1/0] via 3100::1234, Vlan2

Switch(config)#end

Switch#copy running-config startup-config

4 Viewing Routing Table

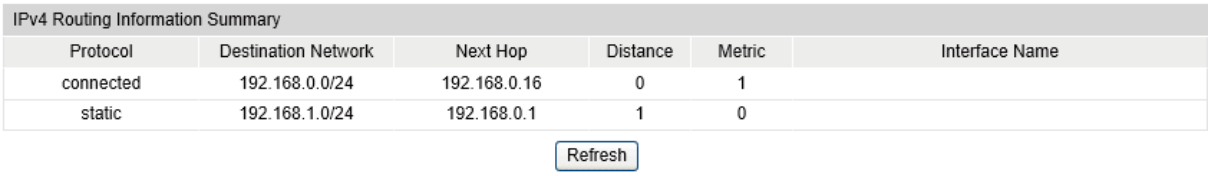
You can view routing tables to learn about the network topology. The switch supports IPv4 routing table and IPv6 routing table.

4.1 Using the GUI

4.1.1 Viewing IPv4 Routing Table

Choose the menu **Routing> Routing Table > IPv4 Routing Table** to load the following page.

Figure 4-1 Viewing IPv4 Routing Table



View the IPv4 routes in the **IPv4 Routing Information Summary** section.

Protocol	Displays the type of the route entry.
Destination Network	Displays the destination IP address and subnet mask.
Next Hop	Displays the IPv4 gateway address to which the packet should be sent next.
Distance	Displays the administrative distance which is a rating of the trustworthiness of a routing information. A higher value means a lower trust rating. When more than one routing protocols have routes to the same destination, only the route which has the smallest distance will be recorded in the IP routing table.
Metric	Displays the metric to reach the destination IP address.
Interface Name	Displays the gateway interface name.

4.1.2 Viewing IPv6 Routing Table

Choose the menu **Routing> Routing Table > IPv6 Routing Table** to load the following page.

Figure 4-2 Viewing IPv6 Routing Table



View the IPv6 routes in the **IPv6 Routing Information Summary** section.

Protocol	Displays the type of the route entry.
Destination Network	Displays the destination IP address and subnet mask.
Next Hop	Displays the IPv6 gateway address to which the packet should be sent next.
Distance	Displays the administrative distance which is a rating of the trustworthiness of a routing information. A higher value means a lower trust rating. When more than one routing protocols have routes to the same destination, only the route which has the smallest distance will be recorded in the IP routing table.
Metric	Displays the metric to reach the destination IP address.
Interface Name	Displays the gateway interface name.

4.2 Using the CLI

4.2.1 Viewing IPv4 Routing Table

On privileged EXEC mode or any other configuration mode, you can use the following command to view IPv4 routing table:

show ip route [static | connected **]**

View the IPv4 route entries of the specified type. If not specified, all types of route entries will be displayed.

static: View the static routes.

connected: View the connected routes.

4.2.2 Viewing IPv6 Routing Table

On privileged EXEC mode or any other configuration mode, you can use the following command to view IPv6 routing table:

show ipv6 route [static | connected **]**

View the IPv6 route entries of the specified type. If not specified, all types of route entries will be displayed.

static: View the static IPv6 routes.

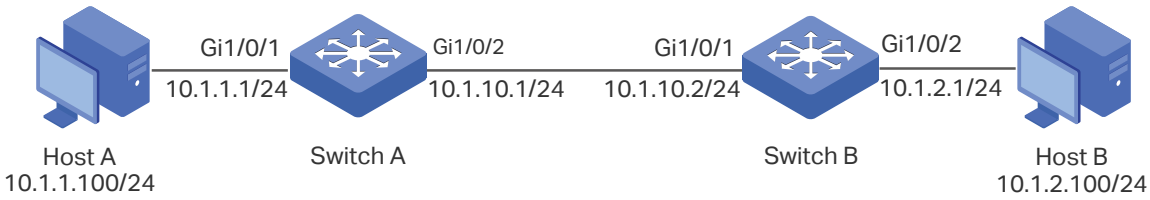
connected: View the connected IPv6 routes.

5 Example for Static Routing

5.1 Network Requirements

As shown below, Host A and Host B are on different network segments. To meet business needs, Host A and Host B need establish a connection without using dynamic routing protocols to ensure stable connectivity.

Figure 5-1 Network Topology



5.2 Configuration Scheme

To implement this requirement, you can configure the default gateway of host A as 10.1.1.1/24, the default gateway of host B as 10.1.2.1/24, and configure IPv4 static routes on Switch A and Switch B so that hosts on different network segments can communicate with each other.

Demonstrated with T2600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

5.3 Using the GUI

The configurations of Switch A and Switch B are similar. The following introductions take Switch A as an example.

1) Choose the menu **Routing> Interface > Interface Config** to load the following page. Create a routed port Gi1/0/1 with the mode as static, the IP address as 10.1.1.1, the mask as 255.255.255.0 and the admin status as Enable. Create a routed port Gi1/0/2 with the mode as static, the IP address as 10.1.10.1, the mask as 255.255.255.0 and the admin status as Enable.

Figure 5-2 Create a Routed Port Gi1/0/1 for Switch A

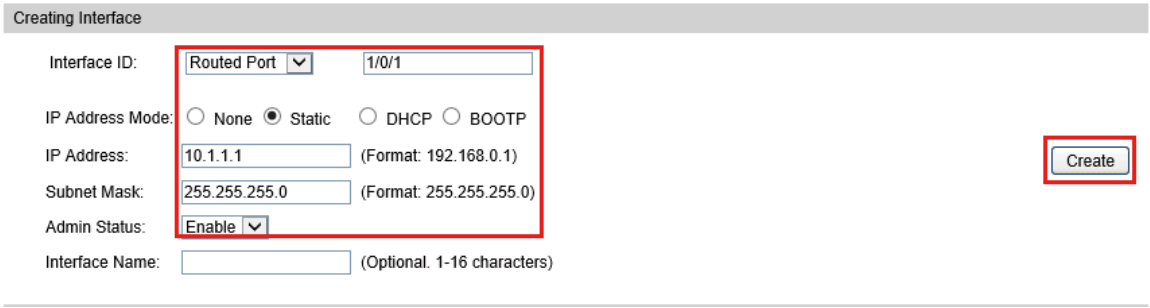
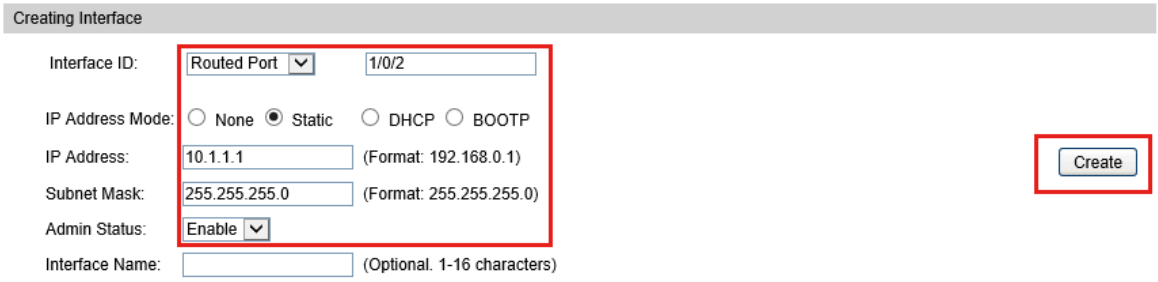
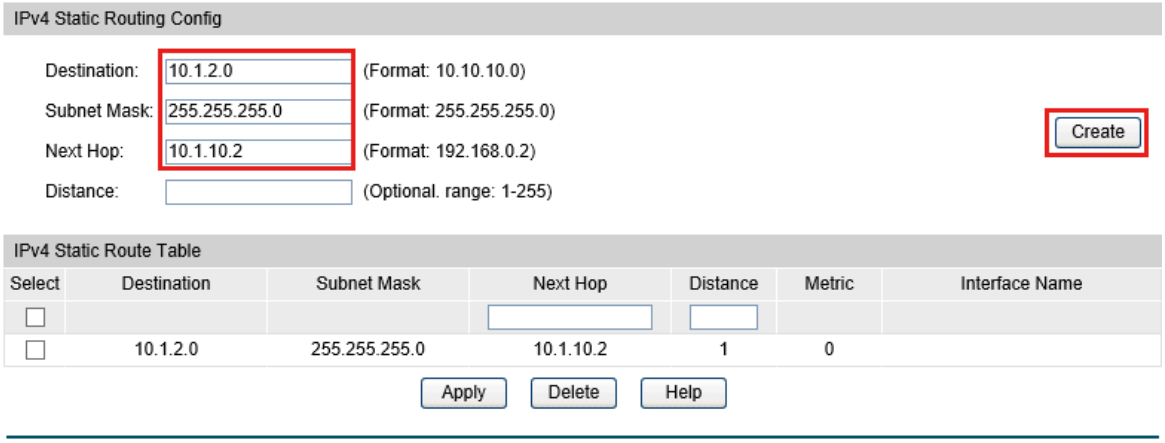


Figure 5-3 Create a Routed Port Gi1/0/2 for Switch A



2) Choose the menu **Routing> Static Routing > IPv4 Static Routing Config** to load the following page. Add a static route entry with the destination as 10.1.2.0, the subnet mask as 255.255.255.0 and the next hop as 10.1.10.2. For switch B, add a static route entry with the destination as 10.1.1.0, the subnet mask as 255.255.255.0 and the next hop as 10.1.10.1.

Figure 5-4 Add a Static Route for Switch A



5.4 Using the CLI

The configurations of Switch A and Switch B are similar. The following introductions take Switch A as an example.

1) Create a routed port Gi1/0/1 with the mode as static, the IP address as 10.1.1.1, the mask as 255.255.255.0 and the admin status as Enable. Create a routed port Gi1/0/2

with the mode as static, the IP address as 10.1.10.1, the mask as 255.255.255.0 and the admin status as Enable.

Switch_A#configure

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

Switch_A(config-if)#no switchport

Switch_A(config-if)#ip address 10.1.1.1 255.255.255.0

Switch_A(config-if)#exit

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

Switch_A(config-if)#no switchport

Switch_A(config-if)#ip address 10.1.10.1 255.255.255.0

2) Add a static route entry with the destination as 10.1.2.0, the subnet mask as 255.255.255.0 and the next hop as 10.1.10.2. For switch B, add a static route entry with the destination as 10.1.1.0, the subnet mask as 255.255.255.0 and the next hop as 10.1.10.1.

Switch_A#configure

Switch_A(config)#ip route 10.1.2.0 255.255.255.0 10.1.10.2

Switch_A(config)#end

Switch_A#copy running-config startup-config

Verify the Configurations

- Switch A

Verify the static routing configuration:

Switch_A#show ip route

Codes: C - connected, S - static

* - candidate default

C 10.1.1.0/24 is directly connected, Vlan10

C 10.1.10.0/24 is directly connected, Vlan20

S 10.1.2.0/24 [1/0] via 10.1.10.2, Vlan20

- Switch B

Verify the static routing configuration:

Switch_B#show ip route

Codes: C - connected, S - static

```
* - candidate default

C       10.1.2.0/24 is directly connected, Vlan30

C       10.1.10.0/24 is directly connected, Vlan20

S       10.1.1.0/24 [1/0] via 10.1.10.1, Vlan20
```

- Connectivity Between Switch A and Switch B

  Run the ping command on switch A to verify the connectivity:

```
Switch_A#ping 10.1.2.1

Pinging 10.1.2.1 with 64 bytes of data :

Reply from 10.1.2.1 : bytes=64 time<16ms TTL=64

Reply from 10.1.2.1 : bytes=64 time<16ms TTL=64

Reply from 10.1.2.1 : bytes=64 time<16ms TTL=64

Reply from 10.1.2.1 : bytes=64 time<16ms TTL=64

Ping statistics for 10.1.2.1:

Packets: Sent = 4 , Received = 4 , Lost = 0 (0% loss)

Approximate round trip times in milli-seconds:

Minimum = 1ms , Maximum = 3ms , Average = 1ms
```

6 Appendix: Default Parameter

Default setting of static routing is listed in the following table.

Table 6-1 Configuring Static Routing

Parameter	Default Setting
IPv6 Routing	Disable

Part 20

Configuring DHCP

CHAPTERS

1. DHCP
2. DHCP Server Configuration
3. DHCP Client Configuration
4. DHCP Relay Configuration
5. DHCP L2 Relay Configuration
6. Configuration Examples
7. Appendix: Default Parameters

1 DHCP

1.1 Overview

DHCP (Dynamic Host Configuration Protocol) is widely used in local area networks (LANs) to dynamically assign IP addresses and other network configuration parameters to network devices, which enhances the utilization of IP address.

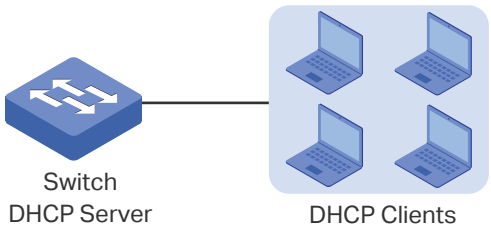
1.2 Supported Features

The supported DHCP features of the switch include DHCP Server, DHCP Client, DHCP Relay and DHCP L2 Relay.

DHCP Server

DHCP Server is used to dynamically assign IP addresses, and other parameters if needed, to clients in the local area network. As the following figure shows, the switch acts as a DHCP server and assigns IP addresses to the hosts.

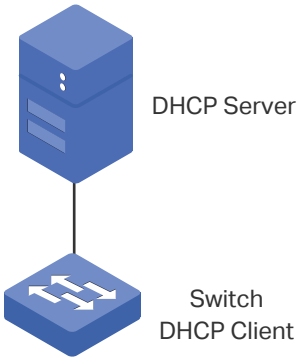
Figure 1-1 Application Scenario of DHCP Server



DHCP Client

A Layer 3 interface can be configured as a DHCP client. After configured, the Layer 3 interface can dynamically obtain IP address and other parameters from a DHCP server, which eases the network configuration and management. As the following figure shows, the switch acts as a DHCP client and dynamically obtain IP address from the DHCP server.

Figure 1-2 Application Scenario of DHCP Client



DHCP Relay

DHCP Relay is used to process and forward DHCP packets between different subnets or VLANs.

Since the client requests a dynamic IP address via broadcast, the basic network model of DHCP requires that the client and the server should be on the same LAN (on the same subnet and VLAN). Therefore, each LAN should be equipped with a DHCP server, thus increasing the costs of network construction.

DHCP Relay solves this problem. The DHCP Relay device acts as a relay agent and forwards DHCP packets between DHCP clients and DHCP servers on different LANs, so that DHCP clients on different LANs can share one DHCP server.

The switch supports two kinds of DHCP Relay: DHCP Interface Relay and DHCP VLAN Relay.

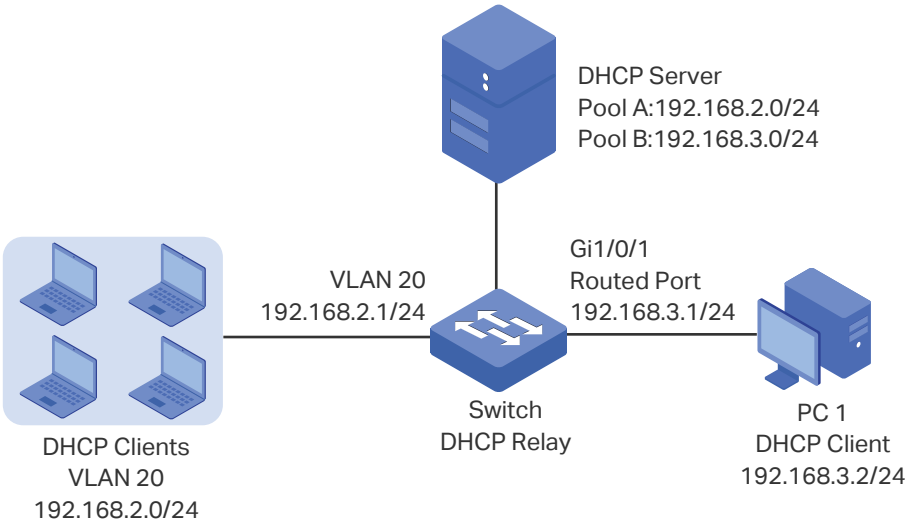
■ DHCP Interface Relay

DHCP Interface Relay is used to process and forward DHCP packets between different subnets.

Before DHCP Interface Relay configurations, you should configure IP addresses for the layer 3 interfaces connected to the clients. The layer 3 interface can be configured as either VLAN interface, routed port, or port channel interface according to your network scheme. When receiving DHCP packets from clients, the switch will fill the corresponding interface's IP address in the relay agent IP address field of the DHCP packets, and forwards the packets to the DHCP server. The DHCP server assigns IP addresses to the clients base on the relay agent IP address field.

As the following figure shows, the IP address for VLAN20 is 192.168.2.1/24 and for the routed port Gi1/0/1 is 192.168.3.1/24. With DHCP Interface VLAN configured, the switch uses IP address of VLAN 20 (192.168.2.1/24) when applying for IP addresses for clients in VLAN 20, and uses IP address of Gi1/0/1 (192.168.3.1/24) when applying for IP address for PC 1. As a result, the DHCP server will assign IP addresses in Pool A (the same subnet with the IP address of VLAN 20) to clients in VLAN 20, and assign IP address in Pool B (the same subnet with the Gi1/0/1) to PC 1.

Figure 1-3 Application Scenario of DHCP Interface Relay



DHCP VLAN Relay

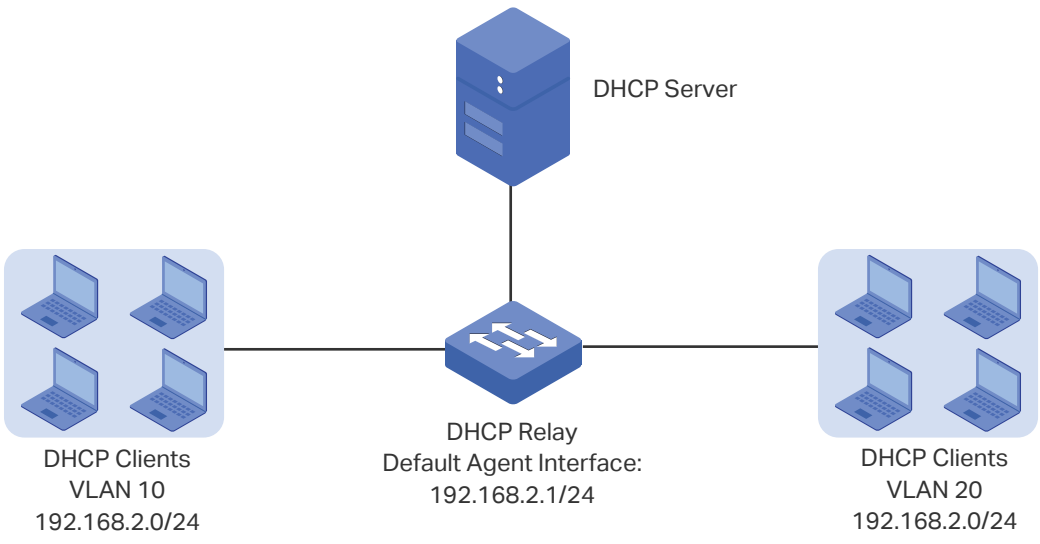
DHCP VLAN Relay allows clients in different VLANs to obtain IP addresses from the DHCP server using a single agent interface IP address.

In DHCP Interface Relay, to assign IP addresses to clients in different VLANs, you need to create a layer 3 interface for each VLAN to ensure the reachability.

In DHCP VLAN Relay, you can simply specify a layer 3 interface as default agent interface for all VLANs. The swith will fill this default agent interface's IP address in the relay agent IP address field of the DHCP packets from all VLANs.

As the following figure shows, no IP addresses are assigned to VLAN 10 and VLAN 20, but a default relay agent interface is configured with the IP address 192.168.2.1/24. The switch uses IP address of the default agent interface (192.168.2.1/24) to apply for IP addresses for clients in both VLAN 10 and VLAN 20. As a result, the DHCP server will assign IP addresses on 192.168.2.0/24 (the same subnet with the IP address of the default agent interface) to clients in both VLAN 10 and VLAN 20.

Figure 1-4 Application Scenario of DHCP VLAN Relay



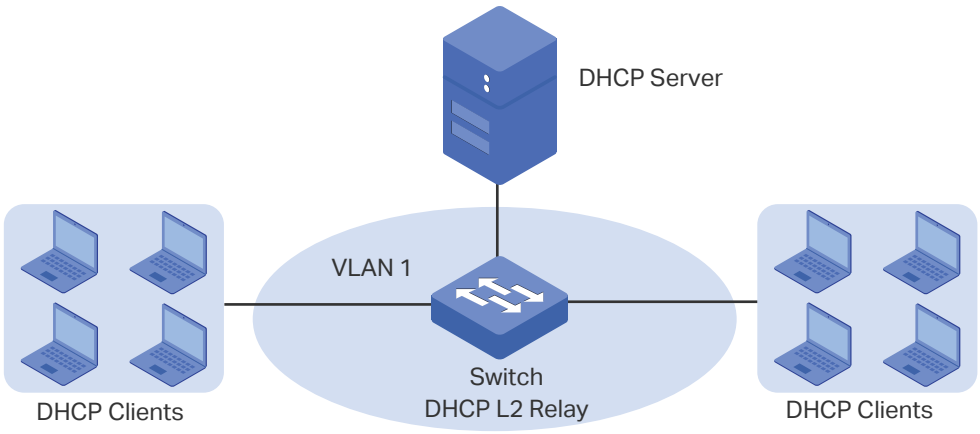
Note:

- If the VLAN already has an IP address, the switch will use the IP address of the VLAN as the relay agent IP address. The default relay agent IP address will not take effect.
- A routed port or port channel interface is not associated with a particular VLAN. DHCP VLAN relay will not work on routed ports or port channel interfaces.

DHCP L2 Relay

Unlike DHCP relay, DHCP L2 Relay is used in the situation that the DHCP server and client are in the same VLAN. In DHCP L2 Relay, in addition to normally assigning IP addresses to clients from the DHCP server, the switch can record the location information of the DHCP client using Option 82. The switch can add Option 82 to the DHCP request packet and then transmit the packet to the DHCP server. The DHCP server which supports Option 82 can set the distribution policy of IP addresses and the other parameters, providing a more flexible address distribution way.

Figure 1-5 Application Scenario of DHCP L2 Relay



2 DHCP Server Configuration

To complete DHCP server configuration, follow these steps:

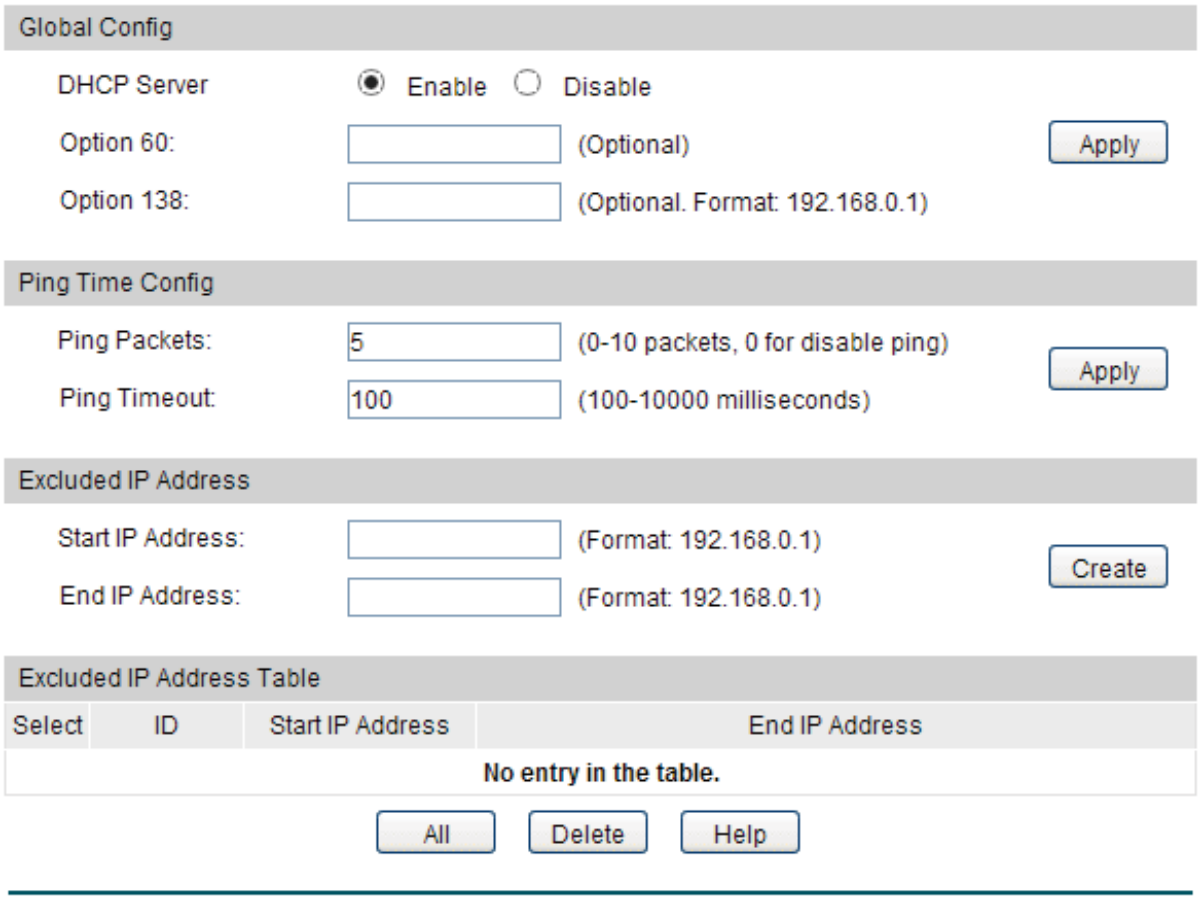
1) Enable the DHCP Server feature on the switch.
2) Configure the DHCP Server Pool.
3) For hosts that need static IP addresses, WWW server for example, bind the MAC address or client ID of the host to an IP address.

2.1 Using the GUI

2.1.1 Enabling DHCP Server

Choose the menu **Routing > DHCP Server > DHCP Server** to load the following page.

Figure 2-1 DHCP Server



Follow these steps to configure DHCP Server:

1) In the **Global Config** section, enable DHCP Server. Click **Apply**.

DHCP Server	Enable or disable DHCP Server. By default, it is disabled.

Option 60	(Optional) Specify the option 60 for device identification. Mostly it is used under the scenario where the APs (Access Points) apply for different IP addresses from different servers according to the needs. If an AP requests option 60, the server will respond a packet containing the option 60 configured here. And then the AP will compare the received option 60 with its own. If they are the same, the AP will accept the IP address assigned by the server, otherwise the assigned IP address will not be accepted.
Option 138	(Optional) Specify the option 138, which can be configured as the management IP address of an AC (Access Control) device. If the APs in the local network request this option, the server will respond a packet containing this option to inform the APs of the AC's IP address.

2) In the **Ping Time Config** section, configure Ping Packets and Ping Timeout for ping tests. Click **Apply**.

Ping Packets	Enter the number of ping packets the server can broadcast to test whether the IP address is occupied. The valid values are from 1 to 10, and the default is 1. When the switch is configured as a DHCP server to dynamically assign IP addresses to clients, the switch will deploy ping test to avoid IP address conflict resulted from assigning IP addresses repeatedly.
Ping Timeout	Specify the ping timeout period in milliseconds. It ranges from 100 to 10000 ms and the default is 100 ms. The DHCP server broadcasts an ICMP Echo Request (ping packet) to test whether an IP address is occupied or not. If there is no response within the ping timeout period, the server will broadcast the ping packet again. If the number of ping packets reaches the specified number and there is still no response, the server will assign the IP address. Otherwise, the server will record the IP address as a conflicted IP address and assign another IP address to the client.

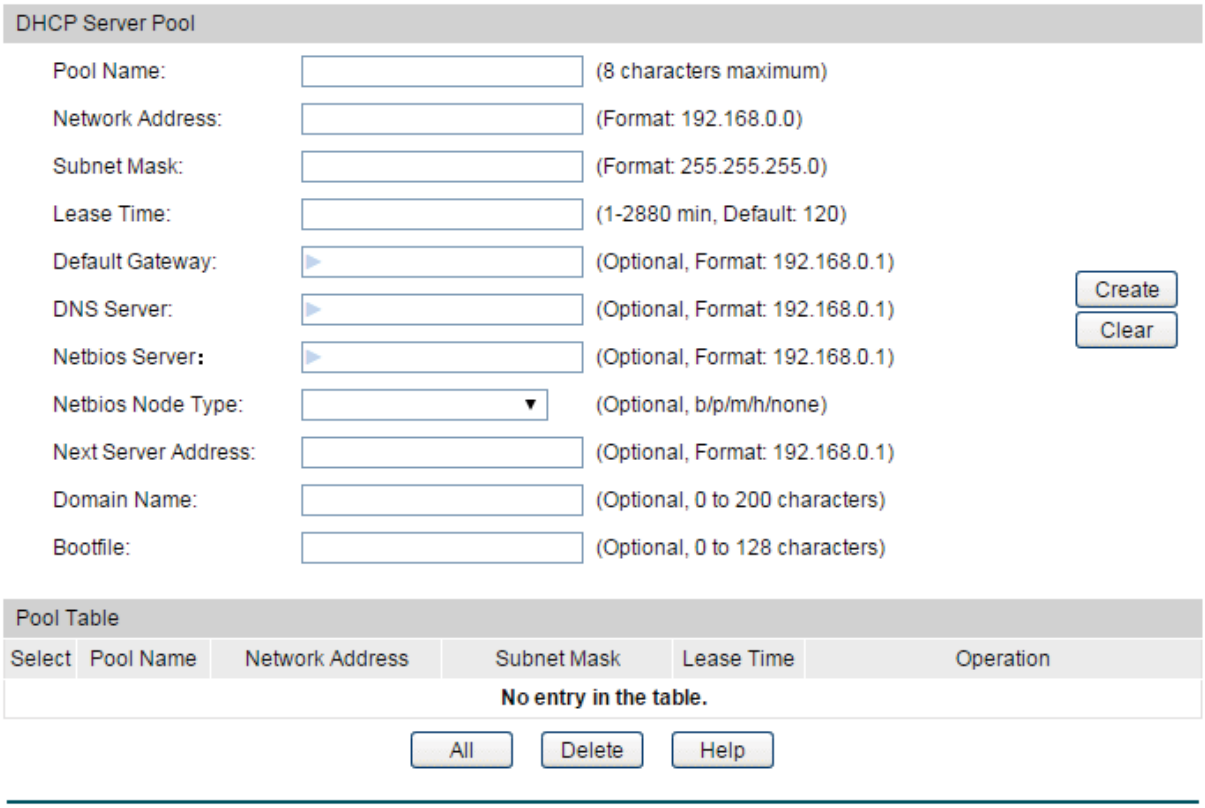
3) In the **Excluded IP Address** section, enter the Start IP Address and End IP Address to specify the range of reserved IP addresses. Click **Create**.

Start IP Address/ End IP Address	Specify the start IP address and end IP address of the excluded IP address range. If the start IP address and the end IP address are the same, the server excludes only one IP address. When configuring DHCP Server, you need to reserve certain IP addresses for each subnet, such as default gateway address, broadcast address and DNS server address.

2.1.2 Configuring DHCP Server Pool

Choose the menu **Routing > DHCP Server > Pool Setting** to load the following page.

Figure 2-2 Pool Setting



Follow these steps to configure DHCP Server Pool:

1) In the **DHCP Server Pool** section, configure the relevant parameters.

Pool Name	Specify a pool name for identification.
Network Address / Subnet Mask	Configure the network address and subnet mask of the DHCP server pool. The network address and subnet mask decide the range of the DHCP server pool. On the same subnet, all addresses can be assigned except the excluded addresses and addresses for special uses.
Lease Time	Specify how long the client can use the IP address assigned from this address pool. It ranges from 1 to 2880 minutes and the default is 120 minutes.
Default Gateway	(Optional) Configure the default gateway of the DHCP server pool. You can create up to 8 default gateways for each DHCP server pool. In general, you can configure the IP address of the VLAN interface as the default gateway address.

DNS Server	(Optional) Specify the DNS server of the DHCP server pool. You can specify up to 8 DNS servers for each DHCP server pool. In general, you can configure the IP address of the VLAN interface as the DNS server address.
Netbios Server	(Optional) Specify the NetBIOS name server. You can specify up to 8 NetBIOS servers for each DHCP server pool. When a DHCP client uses the Network NetBIOS (Basic Input Output System) protocol for communication, the host name must be mapped to IP address. NetBIOS name server can resolve host names to IP addresses.
Netbios Node Type	(Optional) Specify the Netbios type for the clients, which is the way of inquiring IP address resolution. The following options are provided: **b-node Broadcast**: The client sends query message via broadcast. **p-node Peer-to-Peer**: The client sends query message via unicast. **m-node Mixed**: The client sends query message via broadcast first. If it fails, the client will try again via unicast. **h-node Hybrid**: The client sends query message via unicast first. If it fails, the client will try again via broadcast.
Next Server Address	(Optional) Specify the IP address of a TFTP server for the clients. If needed, the clients can get the configuration file from the TFTP server for auto installation.
Domain Name	(Optional) Specify the domain name that the clients should use when resolving host names via DNS.
Bootfile	(Optional) Specify the name of the bootfile. If needed, the clients can get the bootfile from the TFTP server for auto installation.

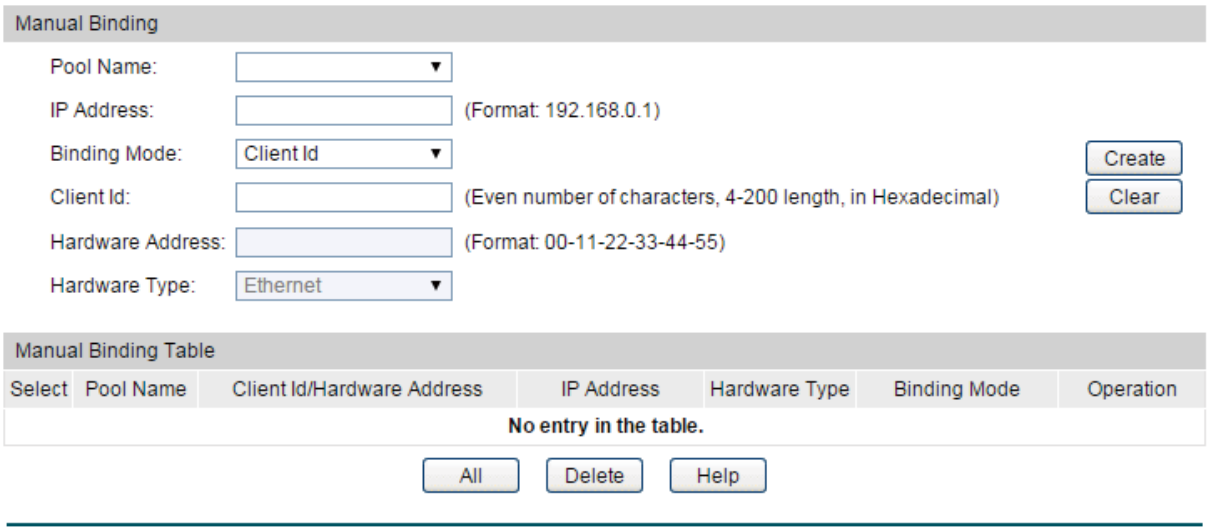
2) Click **Create**.

2.1.3 Configuring Manual Binding

Some hosts, WWW server for example, requires a static IP address. To satisfy this requirement, you can manually bind the MAC address or client ID of the host to an IP address, and the DHCP server will reserve the bound IP address to this host at all times.

Choose the menu **Routing > DHCP Server > Manual Binding** to load the following page.

Figure 2-3 Manual Binding



Follow these steps to configure Manual Binding:

1) In the **Manual Binding** section, select a pool name and enter the IP address to be bound. Select a binding mode and finish the configuration accordingly.

Pool Name	Select a DHCP server pool from the drop-down list.
IP Address	Enter the IP address to be bound to the host.
Binding Mode	Select a binding mode: **Client Id**: Bind the IP address to the client ID. **Client Id in ASCii**: Bind the IP address to the client ID in ASCII format. **Hardware Address**: Bind the IP address to the MAC address of the client.
Client Id	If you select Client ID as the binding mode, enter the client ID in this field.
Hardware Address	If you select Hardware Address as the binding mode, enter the MAC address in this field.
Hardware Type	If you select Hardware Address as the binding mode, select a hardware type. The hardware type includes Ethernet and IEEE802.

2) Click **Create**.

2.2 Using the CLI

2.2.1 Enabling DHCP Server

Follow these steps to enable DHCP Server and to configure ping packets and ping timeout.

Step 1	**configure** Enter global configuration mode.
Step 2	**service dhcp server** Enable DHCP Server.
Step 3	**ip dhcp server extend-option vendor-class-id** *class-id* (Optional) Specify the option 60 for server identification. If a client requests option 60, the server will respond a packet containing the option 60 configured here. And then the client will compare the received option 60 with its own. If they are the same, the client will accept the IP address assigned by the server, otherwise the assigned IP address will not be accepted. *class-id*: Specify the option 60.
Step 4	**ip dhcp server extend-option capwap-ac-ip** *ip-address* (Optional) Specify the option 138, which can be configured as the management IP address of an AC (Access Control) device. If the APs (Access Points) in the local network request this option, the server will respond a packet containing this option to inform the APs of the AC's IP address. *ip-address*: Specify the option 138.
Step 5	**ip dhcp server ping timeout** *value* Specify the ping timeout period. The DHCP server broadcasts an ICMP Echo Request (ping packet) to test whether an IP address is occupied or not. If there is no response within the ping timeout period, the server will broadcast the ping packet again. If the number of ping packets reaches the specified number and there is still no response, the server will assign the IP address. Otherwise, the server will record the IP address as a conflicted IP address and assign another IP address to the client. *value*: Specify the ping timeout period in milliseconds. It ranges from 100 to 10000 ms and the default is 100 ms.
Step 6	**ip dhcp server ping packets** *num* Specify the number of ping packets the server can broadcast to test whether the IP address is occupied. When the switch is configured as a DHCP server to dynamically assign IP addresses to clients, the switch will deploy ping test to avoid IP address conflict resulted from assigning IP addresses repeatedly. *num*: Enter the number of ping packets. The valid values are from 1 to 10, and the default is 1.

Step 7	**ip dhcp server exclude-address** *start-ip-address end-ip-address* Specify the start IP address and end IP address of the excluded IP address range. If the start IP address and the end IP address are the same, the server excludes only one IP address. When configuring DHCP Server, you need to reserve certain IP addresses for each subnet, such as default gateway address, broadcast address and DNS server address. *start-ip-address/end-ip-address*: Specify the start IP address and end IP address.
Step 8	**show ip dhcp server status** Verify the DHCP status, including whether it is enabled and the configuration of ping packet number and ping packet timeout.
Step 9	**show ip dhcp server extend-option** Verify the configuration of the extend options.
Step 10	**show ip dhcp server excluded-address** Verify the configuration of the excluded IP address.
Step 11	**end** Return to Privileged EXEC Mode.
Step 12	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable DHCP Server globally on Switch, configure the number of ping packets as 2 and configure the ping timeout period as 200 ms:

Switch#configure

Switch(config)#service dhcp server

Switch(config)#ip dhcp server ping packets 2

Switch(config)#ip dhcp server ping timeout 200

Switch(config)#show ip dhcp server status

DHCP server is enable.

Ping packet number: 2.

Ping packet timeout: 200 milliseconds.

Switch(config)#end

Switch#copy running-config startup-config

The following example shows how to configure the option 60 as abc and option 138 as 192.168.0.155:

Switch#configure

Switch(config)#ip dhcp server extend-option vendor-class-id abc

Switch(config)#ip dhcp server extend-option capwap-ac-ip 192.168.0.155

Switch(config)#show ip dhcp server extend-option

Option 60: abc

Option 138: 192.168.0.155

Switch(config)#end

Switch#copy running-config startup-config

The following example shows how to configure the 192.168.1.1 as the default gateway address and excluded IP address:

Switch#configure

Switch(config)#ip dhcp server excluded-address 192.168.1.1 192.168.1.1

Switch(config)#show ip dhcp server excluded-address

No.	Start IP Address	End IP Address
---	----------	----------
1	192.168.1.1	192.168.1.1

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Configuring DHCP Server Pool

Follow these steps to configure DHCP server pool:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip dhcp server pool** *pool-name* Configure a name for the DHCP server pool for identification. *pool-name*: Specify a pool name with 1 to 8 characters.

Step 3	**network** *network-address subnet-mask* Configure the network address and subnet mask of the DHCP server pool. The network address and subnet mask decide the range of the DHCP server pool. On the same subnet, all addresses can be assigned except the excluded addresses and addresses for special uses. *network-address*: Configure the network address of the DHCP server pool. *subnet-mask*: Configure the subnet mask of the DHCP server pool.
Step 4	**lease** *lease-time* Specify how long the client can use the IP address assigned from this address pool. *lease-time*: Enter the value of lease-time. It ranges from 1 to 2880 minutes and the default is 120 minutes.
Step 5	**default-gateway** *gateway-list* (Optional) Configure the default gateway of the DHCP server pool. In general, you can configure the IP address of the VLAN interface as the default gateway address. *gateway-list*: Specify the IP address of the default gateway. You can create up to 8 default gateways for each DHCP server pool.
Step 6	**dns-server** *dns-server-list* (Optional) Specify the DNS server of the DHCP server pool. In general, you can configure the IP address of the VLAN interface as the DNS server address. *dns-server-list*: Specify the IP address of the DNS server. You can specify up to 8 DNS servers for each DHCP server pool.
Step 7	**netbios-name-server** *NBNS-list* (Optional) Specify the NetBIOS name server. You can specify up to 8 NetBIOS servers for each DHCP server pool. When a DHCP client uses the Network NetBIOS (Basic Input Output System) protocol for communication, the host name must be mapped to IP address. NetBIOS name server can resolve host names to IP addresses. *NBNS-list*: Specify the IP address of the NetBIOS server. You can specify up to 8 NetBIOS servers for each DHCP server pool.
Step 8	**netbios-node-type** *type* (Optional) Specify the Netbios type for the clients, which is the way of inquiring IP address resolution. *type*: Specify the Netbios type. The following options are provided: **b-node Broadcast**: The client sends query message via broadcast. **p-node Peer-to-Peer**: The client sends query message via unicast. **m-node Mixed**: The client sends query message via broadcast first. If it fails, the client will try again via unicast. **h-node Hybrid**: The client sends query message via unicast first. If it fails, the client will try again via broadcast.

Step 9	**next-server** *ip-address* (Optional) Specify the IP address of a TFTP server for the clients. If needed, the clients can get the configuration file from the TFTP server for auto installation. *ip-address*: Specify the IP address of theTFTP server.
Step 10	**domain-name** *domainname* (Optional) Specify the domain name that the clients should use when resolving host names via DNS. *domainname*: Specify the domain name.
Step 11	**bootfile** *file-name* (Optional) Specify the name of the bootfile. If needed, the clients can get the bootfile from the TFTP server for auto installation. *file-name*: Specify the bootfile name.
Step 12	**show ip dhcp server pool** Verify the configuration of the DHCP server pool.
Step 13	**end** Return to Privileged EXEC Mode.
Step 14	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create a DHCP server pool and name it as pool1 and configure its network address as 192.168.1.0, subnet mask as 255.255.255.0, lease time as 180 minute, default gateway as 192.168.1.1, DNS server as 192.168.1.4, Netbios server as 192.168.1.19, Netbios type as broadcast, TFTP server as 192.168.1.30, domain name as com, and bootfile name as bootfile:

Switch#configure

Switch(config)#ip dhcp server pool pool1

Switch(dhcp-config)#network 192.168.1.0 255.255.255.0

Switch(dhcp-config)#lease 180

Switch(dhcp-config)#default-gateway 192.168.1.1

Switch(dhcp-config)#dns-server 192.168.1.4

Switch(dhcp-config)#netbios-name-server 192.168.1.19

Switch(dhcp-config)#netbios-node-type b-node

Switch(dhcp-config)#next server 192.168.1.30

Switch(dhcp-config)#domain-name com

Switch(dhcp-config)#bootfile bootfile

Switch(dhcp-config)#show ip dhcp server pool

Pool Name: pool1

Network Address: 192.168.1.0

Subenet Mask: 255.255.255.0

Lease Time: 180

Default Gateway: 192.168.1.1

DNS Server: 192.168.1.4

Netbios Server: 192.168.1.19

Netbios Node Type: b-node

Next Server Address: 192.168.1.30

Domain Name: com

Bootfile Name: bootfile

Switch(dhcp-config)#end

Switch#copy running-config startup-config

2.2.3 Configuring Manual Binding

Some hosts, WWW server for example, requires a static IP address. To satisfy this requirement, you can manually bind the MAC address or client ID of the host to an IP address, and the DHCP server will reserve the bound IP address to this host at all times.

Follow these steps to configure Manual Binding:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip dhcp server pool** *name* Create a DHCP server pool and enter DHCP configuration mode.

Step 3	Bind an IP address to a client: **address** *ip-address* **client-identifier** *client-id* Bind the specified IP address to the client with a specific hexadecimal client ID. *ip-address:* Specify the IP address to be bound. *client-id:* Specify the client ID in hexadecimal format. **address** *ip-address* **client-identifier** *client-id* **ascii** Bind the specified IP address to the client with a specific ASCII client ID. *ip-address:* Specify the IP address to be bound. *client-id:* Specify the client ID with ASCII characters. **address** *ip-address* **hardware-address** *hardware-address* **hardware-type** { ethernet | ieee802 } Bind the specified IP address to the client with a specific MAC address. *ip-address:* Specify the IP address to be bound. *hardware-address:* Enter the MAC address of the client. ethernet | ieee802*:* Specify a hardware type for the client, either Ethernet or IEEE802.
Step 4	**show ip dhcp server manual-binding** Verify the manual binding configuration.
Step 5	**end** Return to Privileged EXEC Mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to bind the IP address 192.168.1.33 in pool1 (on the subnet of 192.168.1.0) to the host with the MAC address 74:D4:68:22:3F:34:

Switch#config

Switch(config)#ip dhcp server pool pool1

Switch(dhcp-config)#address 192.168.1.33 **hardware-address** 74:d4:68:22:3f:34 **hardware-type ethernet**

Switch(dhcp-config)#show ip dhcp server manual-binding

Pool Name	Client Id/Hardware Address	IP Address	Hardware Type	Bind Mode
---	---	---	---	---
pool1	74:d4:68:22:3f:34	192.168.1.33	Ethernet	MAC Address

Switch(dhcp-config)#end

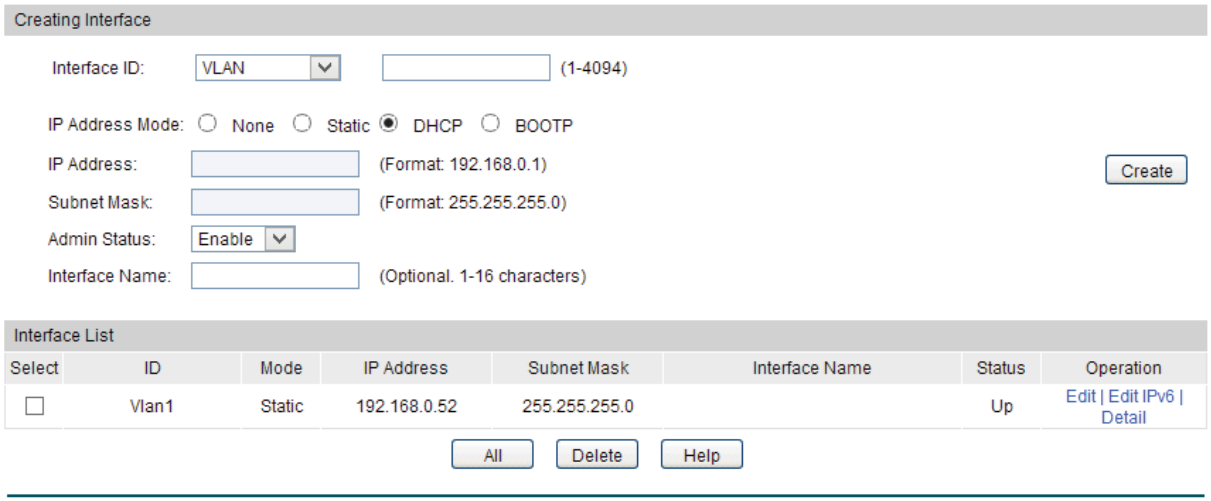
Switch#copy running-config startup-config

3 DHCP Client Configuration

3.1 Using the GUI

Choose the menu **Routing > Interface > Interface Config** to load the following page.

Figure 3-1 DHCP Client Configuration



Follow these steps to configure DHCP client:

1) In the **Creating Interface** section, select Interface VLAN or Routed Port as the interface type and enter the interface ID. Select DHCP or BOOTP as the IP Address Mode. Set the Admin Status as Enable, and enter the Interface Name (optional).

Interface ID	Select an interface type and enter the ID of the interface. If you select VLAN, enter a VLAN ID. If you select Routed port, enter a port number.
IP Address Mode	Select DHCP or BOOTP as the IP address assignment mode. **DHCP**: Assign an ip address for the interface through DHCP. **BOOTP**: Assign an ip address for the interface through BOOTP.
Admin Status	Enable or disable the interface's Layer 3 capabilities.
Interface Name	(Optional) Specify a name for the interface.

2) Click **Create**.

3.2 Using the CLI

Follow these steps to configure DHCP client.

Step 1	**configure** Enter global configuration mode.
Step 2	Enter interface configuration mode. **interface vlan** *vid* Enter VLAN interface configuration mode. *vid:* Specify the VLAN ID. **interface gigabitEthernet** *port* **no switchport** Enter interface configuration mode and configure the port as a layer-3 routed port. *port:* Specify the port number. **interface port-channel** *pid* **no switchport** Enter port-channel configuration mode and configure the port-channel as a layer-3 port-channel. *pid:* Specify the ID of the port-channel.
Step 3	**ip address-alloc** { dhcp | bootp } Enable DHCP or BOOTP IP address mode. dhcp: The specified Layer 3 interface can request the DHCP server to dynamically assign IP address and other network configuration parameters through DHCP mode. bootp: The specified Layer 3 interface can request the DHCP server to dynamically assign IP address and other network configuration parameters through BOOTP mode.
Step 4	**show ip interface brief** Verify the DHCP client configuration.
Step 5	**end** Return to Privileged EXEC Mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure port 1/0/5 as an Layer 3 interface, and to configure its IP address mode as DHCP:

Switch#configure

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

Switch(config-if)#no switchport

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

Switch(config-if)#show ip interface brief

Interface	IP-Address	Method	Status	Protocol	Shutdown
---	---	---	---	---	---
Gi1/0/5	192.168.0.100/24	DHCP	up	up	no

Switch(config-if)#end

Switch#copy running-config startup-config

4 DHCP Relay Configuration

To complete DHCP Relay configuration, follow these steps:

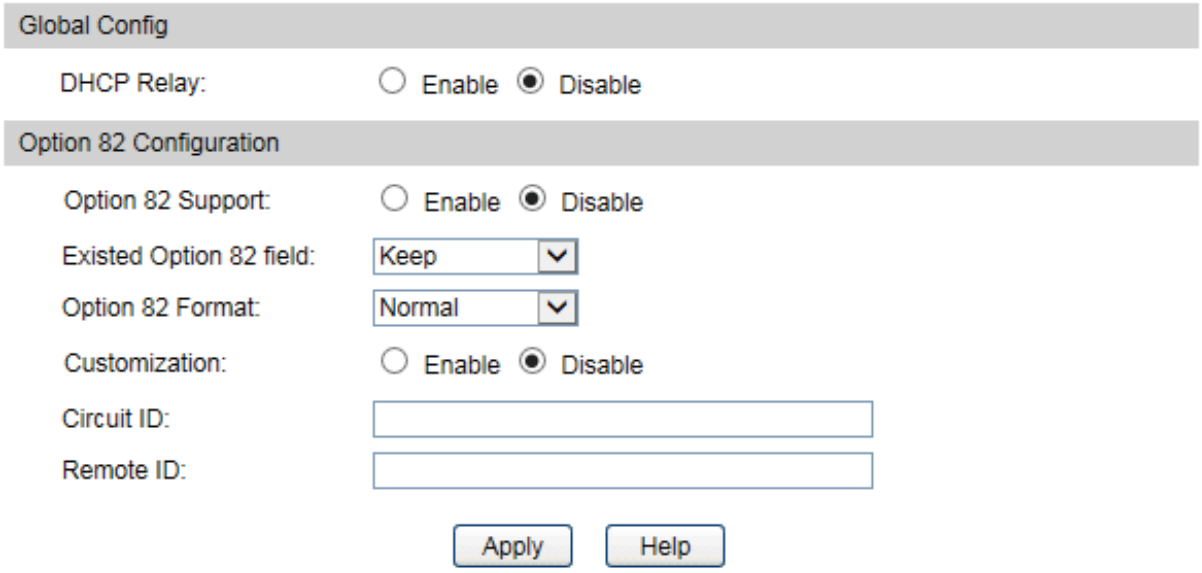
1) Enable DHCP Relay globally. Configure Option 82 if needed.
2) Enable DHCP Relay for ports.
3) Specify DHCP server for the Interface or VLAN.

4.1 Using the GUI

4.1.1 Enabling DHCP Relay globally and Configuring Option 82

Choose the menu **Routing > DHCP Relay > Global Config** to load the following page.

Figure 4-1 Enable DHCP Relay and Configure Option 82



Follow these steps to enable DHCP Relay and configure Option 82:

1) In the **Global Config** section, enable DHCP Relay.
2) (Optional) In the **Option 82 Configuration** section, configure Option 82.

DHCP Relay	Enable or disable DHCP Relay.
Option 82 Support	Select whether to enable Option 82 or not. By default, it is disabled. Option 82 is used to record the locations of the DHCP client, its Ethernet port and the VLAN, etc. If you need to record the accurate location of a client, you can enable Option 82 on the relay device closest to the client.

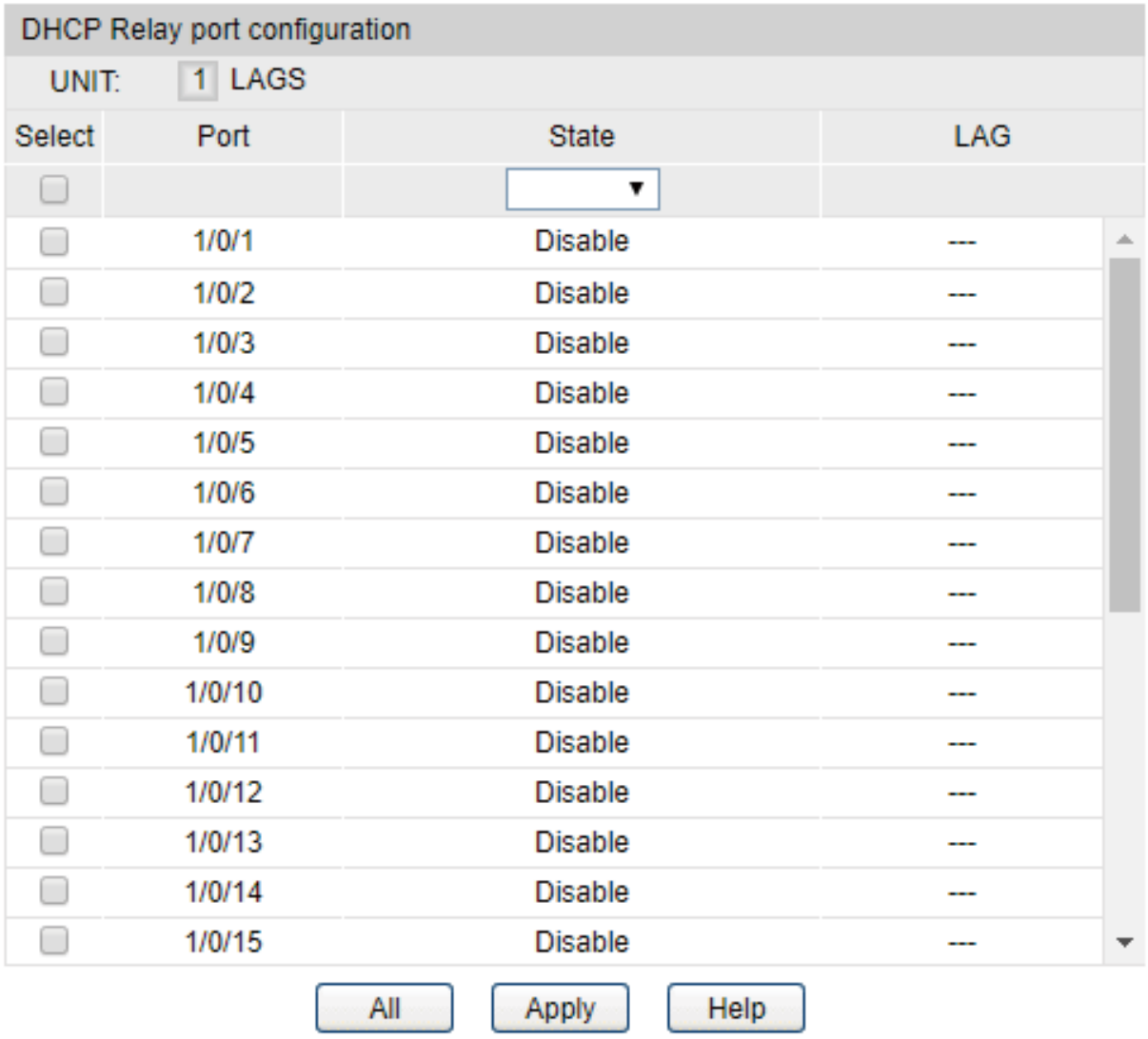
Existed Option 82 field	Select the operation for the Option 82 field of the DHCP request packets. **Keep**: Indicates keeping the Option 82 field of the packets. **Replace**: Indicates replacing the Option 82 field of the packets with the switch defined one. By default, the Circuit ID is defined to be the VLAN and the number of the port which receives the DHCP Request packets. The Remote ID is defined to be the MAC address of the DHCP Relay device which receives the DHCP Request packets. **Drop**: Indicates discarding the packets that include the Option 82 field.
Option 82 Format	Select the format of option 82 sub-option value field. **Normal:** Indicates that the format of sub-option value field is TLV (type-length-value). **Private:** Indicates that the format of sub-option value field is just value.
Customization	Select whether to enable Customization of Option 82 or not. When enabled, configure Option 82 information manually.
Circuit ID	Enter the customized circuit ID, which contains up to 64 characters. The circuit ID configurations of the switch and the DHCP server should be compatible with each other.
Remote ID	Enter the customized remote ID, which contains up to 64 characters. The remote ID configurations of the switch and the DHCP server should be compatible with each other.

3) Click **Apply**.

4.1.2 Enabling DHCP Relay for ports

Choose the menu **Routing > DHCP Relay > Port Config** to load the following page.

Figure 4-2 Enable DHCP Relay for ports



Follow these steps to enable DHCP Relay for ports:

1) Select and configure your desired ports.

UNIT:1/LAGS	Click **1** to configure physical ports. Click **LAGS** to configure LAGs.
State	With this option enabled, the port will enable DHCP Relay function. The ports connected to DHCP clients should be enabled. By default, it's disabled.

2) Click **Apply**.

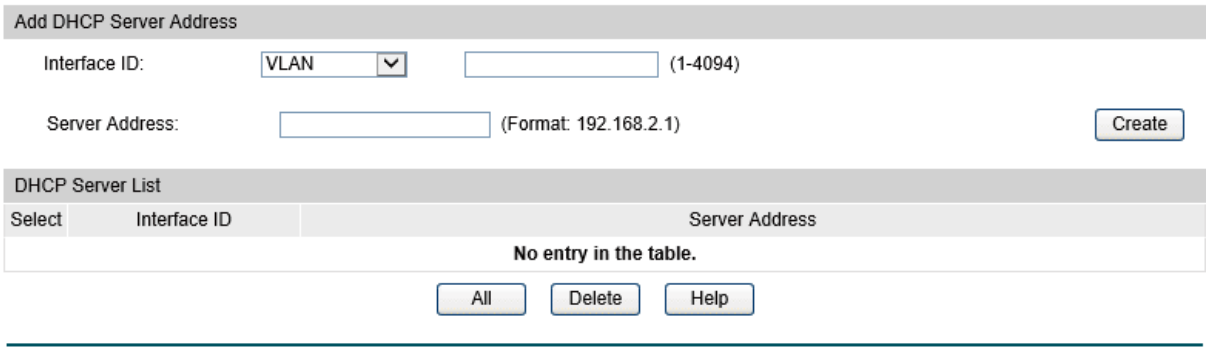
4.1.3 Specifying DHCP Server for the Interface or VLAN

You can specify DHCP server for an layer-3 interface or for a VLAN. The following respectively introduces how to configure DHCP Interface Relay and DHCP VLAN Relay.

- DHCP Interface Relay

Choose the menu **Routing > DHCP Relay > DHCP Interface Relay** to load the following page.

Figure 4-3 Specify DHCP Server for Layer-3 Interface



Follow these steps to specify DHCP Server for the interface:

1) In the **Add DHCP Server Address** section, select the interface type and enter the interface ID, and then enter the server address of the interface.

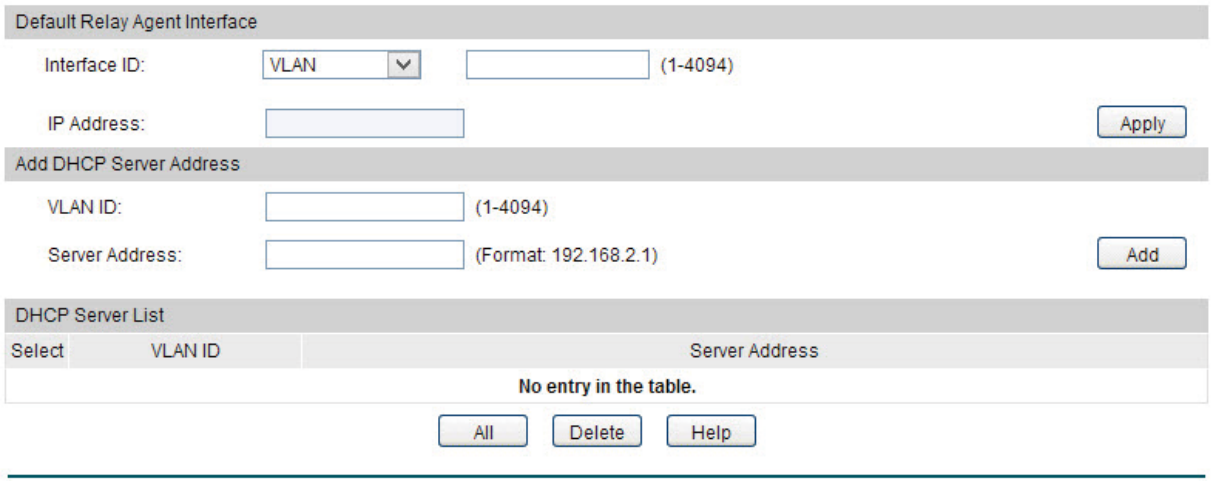
Interface ID	Specify the type and ID of the interface that is facing to the DHCP CLIENTS. The interface should be an existing layer 3 interface. For how to create a layer 3 interface, refer to *Configuring Logical Interfaces*.
Server Address	Enter the IP address of the DHCP server.

2) Click **Create** to specify the DHCP server for the interface.

- DHCP VLAN Relay

Choose the menu **Routing > DHCP Relay > DHCP VLAN Relay** to load the following page.

Figure 4-4 Specify DHCP Server for VLAN



Follow these steps to specify DHCP Server for the specific VLAN:

1) In the **Default Relay Agent Interface** section, specify the type and ID of the interface that needs to be configured as the default relay agent interface. Then click **Apply**.

Interface ID	Specify the type and ID of the interface that needs to be configured as the default relay agent interface. You can configure any existing layer 3 interface as the default relay agent interface. The DHCP server will assign IP addresses in the same subnet with this relay agent interface to the clients who use this relay agent interface to apply for IP addresses. For how to create layer 3 interface, refer to *Configuring Logical Interfaces*.
IP Address	Displays the IP address of this interface.

Note:

- If the VLAN already has an IP address, the switch will use the IP address of the VLAN as the relay agent IP address. The default relay agent IP address will not take effect.
- A routed port or port channel interface is not associated with a particular VLAN. DHCP VLAN relay will not work on routed ports or port channel interfaces.

2) In the **Add DHCP Server Address** section, specify the VLAN in which the clients needs IP addresses and the server address. Click **Add**.

VLAN ID	Specify the VLAN, in which the clients can get IP addresses from the DHCP server.
Server Address	Enter the IP address of the DHCP server.

4.2 Using the CLI

4.2.1 Enabling DHCP Relay globally

Follow these steps to enable DHCP Relay globally:

Step 1	**configure** Enter global configuration mode.
Step 2	**service dhcp relay** Enable DHCP Relay.
Step 3	**show ip dhcp relay** Verify the configuration of DHCP Relay.
Step 4	**end** Return to Privileged EXEC Mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable DHCP Relay:

Switch#configure

Switch(config)#service dhcp relay

Switch(config)#show ip dhcp relay

DHCP relay is enabled.

...

Switch(config)#end

Switch#copy running-config startup-config

4.2.2 (Optional) Configuring Option 82

Follow these steps to configure Option 82:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip dhcp relay information** Enable the Option 82 feature.

Step 3	**ip dhcp relay information policy** { keep | replace | drop } Configure how to process Option 82 information. keep: The switch will keep the Option 82 information in the packet. replace: The switch will replace the Option 82 information with the customized configurations on the switch. drop: The switch will drop the packets carrying Option 82 information
Step 4	**ip dhcp relay information format {** normal | private **}** Specify the format of option 82 sub-option value field. normal: Indicates that the format of sub-option value field is TLV (type-length-value). private: Indicates that the format of sub-option value field is just value.
Step 5	**ip dhcp relay information custom** Enable the Customization feature of Option 82.
Step 6	**ip dhcp relay information circuit-id** *circuit-id* If the Customization feature is enabled, specify the circuit ID. *circuit-id:* Specify the circuit ID with 1 to 63 characters including digits, English letters and underlines.
Step 7	**ip dhcp relay information remote-id** *remote-id* If the Customization feature is enabled, specify the remote ID. *remote-id:* Specify the remote ID with 1 to 32 characters including digits, English letters and underlines.
Step 8	**show ip dhcp relay** Verify the configuration of DHCP Relay.
Step 9	**end** Return to Privileged EXEC Mode.
Step 10	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable Option 82 and configure the process of Option 82 information as keep:

Switch#configure

Switch(config)#ip dhcp relay information

Switch(config)#ip dhcp relay information policy keep

Switch(config)#show ip dhcp relay

...

DHCP relay option 82 is enabled.

Existed option 82 field operation: keep.

...

Switch(config)#end

Switch#copy running-config startup-config

4.2.3 Enabling DHCP Relay for ports

After enabling DHCP relay globally, you need to enable DHCP relay for the ports connected to DHCP clients.

Follow these steps to enable DHCP Relay for ports:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-id-list* **}** Enter interface configuration mode.
Step 3	**ip dhcp relay enable** Enable DHCP relay for ports.
Step 4	**show ip dhcp relay interface [gigabitEthernet** *port* **| port-channel** *port-channel-id* **]** Verify the configuration of DHCP Relay for ports.
Step 5	**end** Return to Privileged EXEC Mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable DHCP Relay for port 1/0/2:

Switch#configure

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

Switch(config-if)#ip dhcp relay enable

Switch(config-if)#show ip dhcp relay interface gigabitEthernet 1/0/2

Interface State LAG

--------- ------- ---

Gi1/0/2 Enable N/A

...

Switch(config-if)#end

Switch#copy running-config startup-config

4.2.4 Specifying DHCP Server for Interface or VLAN

You can specify DHCP server for an layer-3 interface or for a VLAN. The following respectively introduces how to configure DHCP Interface Relay and DHCP VLAN Relay.

- DHCP Interface Relay

Follow these steps to DHCP Interface Relay:

Step 1	**configure** Enter global configuration mode.
Step 2	Enter Layer 3 interface configuration mode: **interface vlan** *vid* Enter VLAN interface configuration mode. *vid*:Specify the ID of the VLAN that will be configured as a DHCP relay agent. The valid values are from 1 to 4094. **interface { fastEthernet** *port* **| gigabitEthernet** *port* **}** **no switchport** Enter Routed Port interface configuration mode. *port:* Specify the ID of the routed port that will be configured as a DHCP relay agent. **interface port-channel** *lagid* Enter Port-channel configuration mode. *lagid:* Specify the ID of the LAG.
Step 3	**ip helper-address** *ip-addr* Specify DHCP server for the Layer 3 interface. *ip-addr:* Enter the IP address of the DHCP server.
Step 4	**show ip dhcp relay** Verify the configuration of DHCP Relay.

Step 5	**end** Return to Privileged EXEC Mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the DHCP server address as 192.168.1.7 on VLAN interface 66:

Switch#configure

Switch(config)#interface vlan 66

Switch(config-if)#ip helper-address 192.168.1.7

Switch(config-if)#show ip dhcp relay

...

DHCP relay helper address is configured on the following interfaces:

Interface	Helper address
----------	----------
VLAN 66	192.168.1.7

Switch(config-if)#end

Switch#copy running-config startup-config

- DHCP VLAN Relay

Follow these steps to configure DHCP VLAN Relay:

Step 1	**configure** Enter global configuration mode.

Step 2	Enter Layer 3 interface configuration mode: **interface vlan** *vid* Enter VLAN interface configuration mode. *vid*: Specify the ID of the VLAN that will be configured as the default relay agent interface. The valid values are from 1 to 4094. **interface loopback** *lid* Enter loopback configuration mode. *lid*: Specify the ID of the loopback interface that will be configured as the default relay agent interface. The valid values are from 1 to 64. **interface { fastEthernet** *port* **| gigabitEthernet** *port* **}** **no switchport** Enter Routed Port interface configuration mode. *port:* Specify the ID of the routed port that will be configured as the default relay agent interface. **interface port-channel** *lagid* Enter Port-channel configuration mode. *lagid:* Specify the ID of the LAG that will be configured as the default relay agent interface.
Step 3	**ip dhcp relay default-interface** Set the interface as the default relay agent interface. If the VLAN that the clients belong to does not have an IP address, the switch will use the IP address of this interface to fill in the relay agent IP address field of DHCP packets from the DHCP clients.
Step 4	**exit** Return to global configuration mode.
Step 5	**ip dhcp relay vlan** *vid* **helper-address** *ip-address* Specify the VLAN ID and the DHCP server. *vid:* Enter the ID of the VLAN, in which the hosts can dynamically get the IP addresses from the DHCP server. *ip-address:* Enter the IP address of the DHCP server.
Step 6	**show ip dhcp relay** Verify the configuration of DHCP Relay.
Step 7	**end** Return to Privileged EXEC Mode.
Step 8	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set the routed port 1/0/2 as the default relay agent interface and configure the DHCP server address as 192.168.1.8 on VLAN 10:

Switch#configure

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

Switch(config-if)# ip dhcp relay default-interface

Switch(config-if)#exit

Switch(config)#ip dhcp relay vlan 10 **helper-address** 192.168.1.8

Switch(config)#show ip dhcp relay

...

DHCP VLAN relay helper address is configured on the following vlan:

vlan Helper address

---------- --------------

VLAN 10 192.168.1.8

Switch(config)#end

Switch#copy running-config startup-config

5 DHCP L2 Relay Configuration

To complete DHCP L2 Relay configuration, follow these steps:

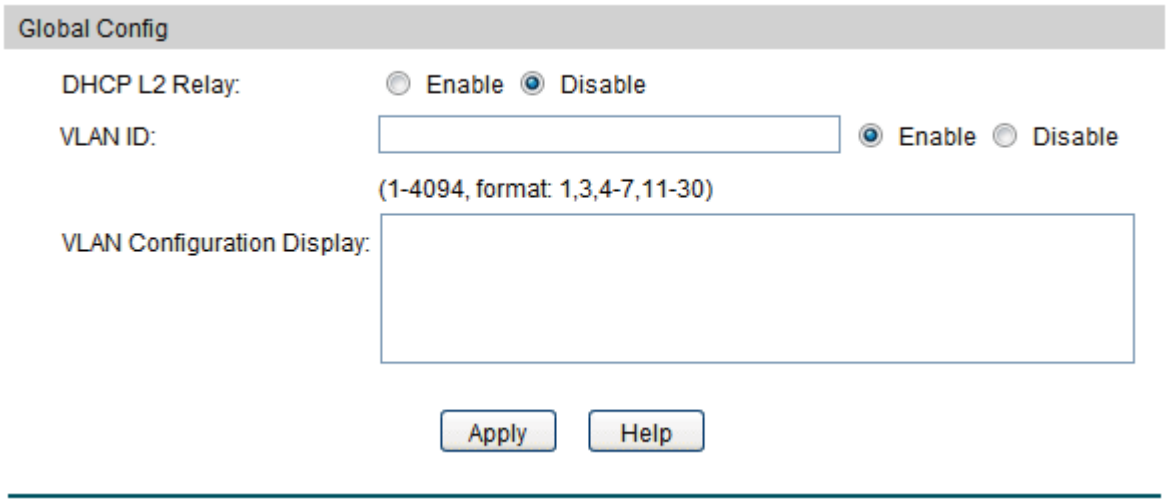
1) Enable DHCP L2 Relay.
2) Configure Option 82 for ports.

5.1 Using the GUI

5.1.1 Enabling DHCP L2 Relay

Choose the menu **Routing > DHCP L2 Relay > Global Config** to load the following page.

Figure 5-1 Enable DHCP L2 Relay



Follow these steps to enable DHCP L2 Relay globally and for the specified VLAN:

1) In the **Global Config** section, enable DHCP L2 Relay globally and for the desired VLANs.

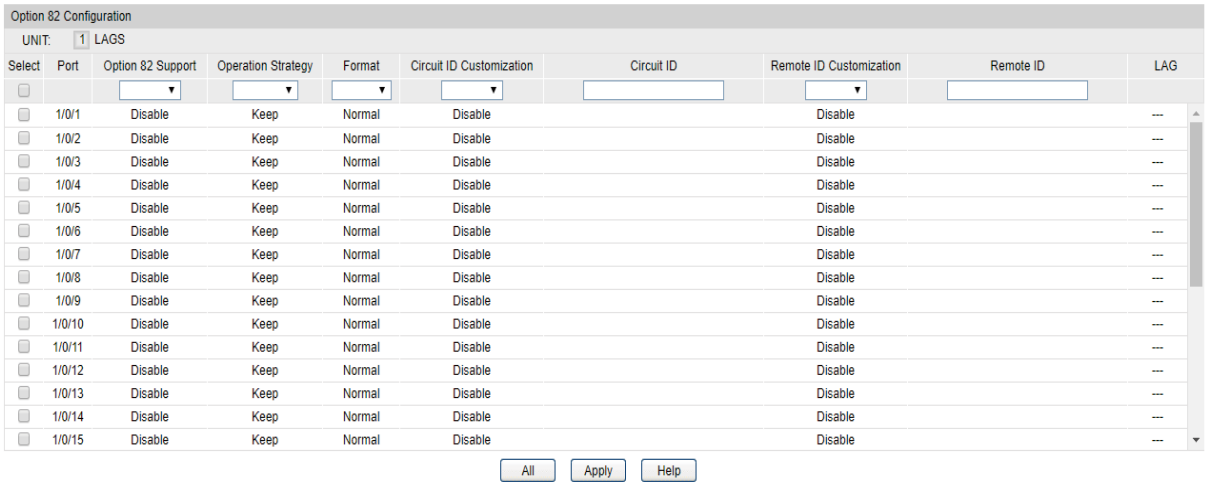
DHCP L2 Relay	Enable DHCP L2 Relay globally.
VLAN ID	Enter the VLAN ID or a list of VLAN IDs, and enable/disable DHCP L2 Relay function for the specified VLAN.
VLAN Configuration Display	Displays the VLAN IDs with DHCP L2 Relay funtion enabled.

2) Click **Apply**.

5.1.1 Configuring Option 82 for Ports

Choose the menu **Routing > DHCP L2 Relay > Option 82 Config** to load the following page.

Figure 5-2 Configure Option 82 for Ports



Follow these steps to enable DHCP Relay and configure Option 82:

1) Select one or more ports to configure Option 82.

Option 82 Support	Select whether to enable Option 82 or not. By default, it is disabled. Option 82 is used to record the DHCP client's location, Ethernet port and the VLAN, etc. If you need to record the accurate location of a client, you can enable Option 82 on the relay device which is closest to the client.
Operation Strategy	Select the operation for the Option 82 field of the DHCP request packets. **Keep**: Indicates keeping the Option 82 field of the packets. **Replace**: Indicates replacing the Option 82 field of the packets with the switch defined one. By default, the Circuit ID is defined to be the VLAN ID and the ID of the port which receives the DHCP Request packets. The Remote ID is defined to be the MAC address of the DHCP Relay device which receives the DHCP Request packets. **Drop**: Indicates discarding the packets that include the Option 82 field.
Format	Select the format of option 82 sub-option value field. **Normal:** Indicates that the format of sub-option value field is TLV (type-length-value). **Private:** Indicates that the format of sub-option value field is just value.
Circuit ID Customization	Enable or disable Customization of Option 82. If enabled, you need to configure Option 82 information manually; If disabled, the switch will automatically configure the VLAN ID and the ID of the port that receives the DHCP packets as the circuit ID.

Circuit ID	Enter the customized circuit ID, which contains up to 64 characters. The circuit ID configurations of the switch and the DHCP server should be compatible with each other.
Remote ID Customization	Enable or disable the switch to define the Option 82 sub-option Remote ID field. If it is enabled, you can manually configure the remote ID; if it is disabled, the switch will automatically configure the switch's MAC address as the remote ID.
Remote ID	Enter the customized remote ID, which contains up to 64 characters. The remote ID configurations of the switch and the DHCP server should be compatible with each other.

2) Click **Apply.**

5.2 Using the CLI

5.2.1 Enabling DHCP L2 Relay

Follow these steps to enable DHCP L2 Relay:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip dhcp l2relay** Enable DHCP L2 Relay.
Step 3	**ip dhcp l2relay vlan** *valn-list* Enable DHCP L2 Relay for specified VLANs. *vlan-list:* Specify the ID or ID list of the VLAN(s) to be enabled with DHCP L2 relay.
Step 5	**show ip dhcp l2relay** Verify the configuration of DHCP Relay.
Step 6	**end** Return to Privileged EXEC Mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable DHCP L2 Relay globally and for VLAN 2:

Switch#configure

Switch(config)#ip dhcp l2relay

Switch(config)#ip dhcp l2relay vlan 2

Switch(config)#show ip dhcp l2relay

Global Status: Enable

VLAN ID: 2

Switch(config)#end

Switch#copy running-config startup-config

5.2.2 Configuring Option 82 for Ports

Follow these steps to configure Option 82 for ports:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Enter interface configuration mode.
Step 3	**ip dhcp l2relay information option** Enable the Option 82 feature on the port.
Step 4	**ip dhcp l2relay information strategy {** keep | replace | drop **}** Specify the operation for the Option 82 field of the DHCP request packets from the Host. The following options are provided: keep: Indicates keeping the Option 82 field of the packets. replace: Indicates replacing the Option 82 field of the packets with one defined by switch. By default, the Circuit ID is defined to be the VLAN and the number of the port which receives the DHCP Request packets. The Remote ID is defined to be the MAC address of the DHCP Snooping device which receives the DHCP Request packets. drop: Indicates discarding the packets that include the Option 82 field.
Step 5	**ip dhcp l2relay information format {** normal | private **}** Specify the format of option 82 sub-option value field. normal: Indicates that the format of sub-option value field is TLV (type-length-value). private: Indicates that the format of sub-option value field is the value you configure for the related sub-option.
Step 6	**ip dhcp l2relay information circuit-id** *string* Configure the circuit ID. The circuit ID configurations of the switch and the DHCP server should be compatible with each other. *string:* Enter the circuit ID, which contains up to 64 characters.

Step 7	**ip dhcp l2relay information remote-id** *string* Configure the remote ID. The remote ID configurations of the switch and the DHCP server should be compatible with each other. *string:* Enter the remote ID, which contains up to 64 characters.
Step 8	**show ip dhcp l2relay interface { fastEthernet** *port* **| gigabitEthernet** *port* **| port-channel** *port-channel-id* **}** Verify the Option 82 configuration of the port.
Step 9	**end** Return to Privileged EXEC Mode.
Step 10	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable Option 82 on port 1/0/7 and configure the strategy as replace, the format as normal, the circuit-id as VLAN20 and the remote-id as Host1:

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/7

Switch(config-if)#ip dhcp l2relay information option

Switch(config-if)#ip dhcp l2relay information strategy replace

Switch(config-if)#ip dhcp l2relay information format normal

Switch(config-if)#ip dhcp l2relay information circuit-id VLAN20

Switch(config-if)#ip dhcp l2relay information remote-id Host1

Switch(config-if)#show ip dhcp l2relay interface gigabitEthernet 1/0/7

Interface	Option 82 Status	Operation Strategy	Format	Circuit ID	Remote ID	LAG
---	---	---	---	---	---	---
Gi1/0/7	Enable	Replace	Normal	VLAN20	Host1	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

6 Configuration Examples

6.1 Example for DHCP Server

6.1.1 Network Requirements

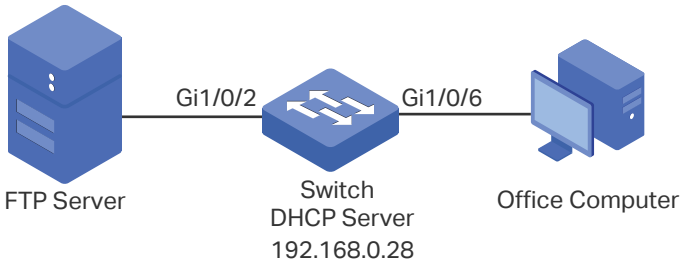
Now the switch in the office building needs to assign IP addresses to all connected devices. The connected devices include FTP servers which need static IP addresses, and office computers that can dynamically obtain IP addresses from the switch.

6.1.2 Configuration Scheme

To simplify the network topology, this chapter takes an FTP server and an office computer as an example. The FTP server and the office computer are connected to the switch. The switch acts as a DHCP server, assigning static IP address to the FTP server and dynamic IP address to the office computer.

As the following network topology shows, the IP address of the switch is 192.168.0.28, and both its gateway address and DNS server address are 192.168.0.1. Port 1/0/2 is connected to the FTP server and port 1/0/6 is connected to the office computer.

Figure 6-1 Network Topology for DHCP Server

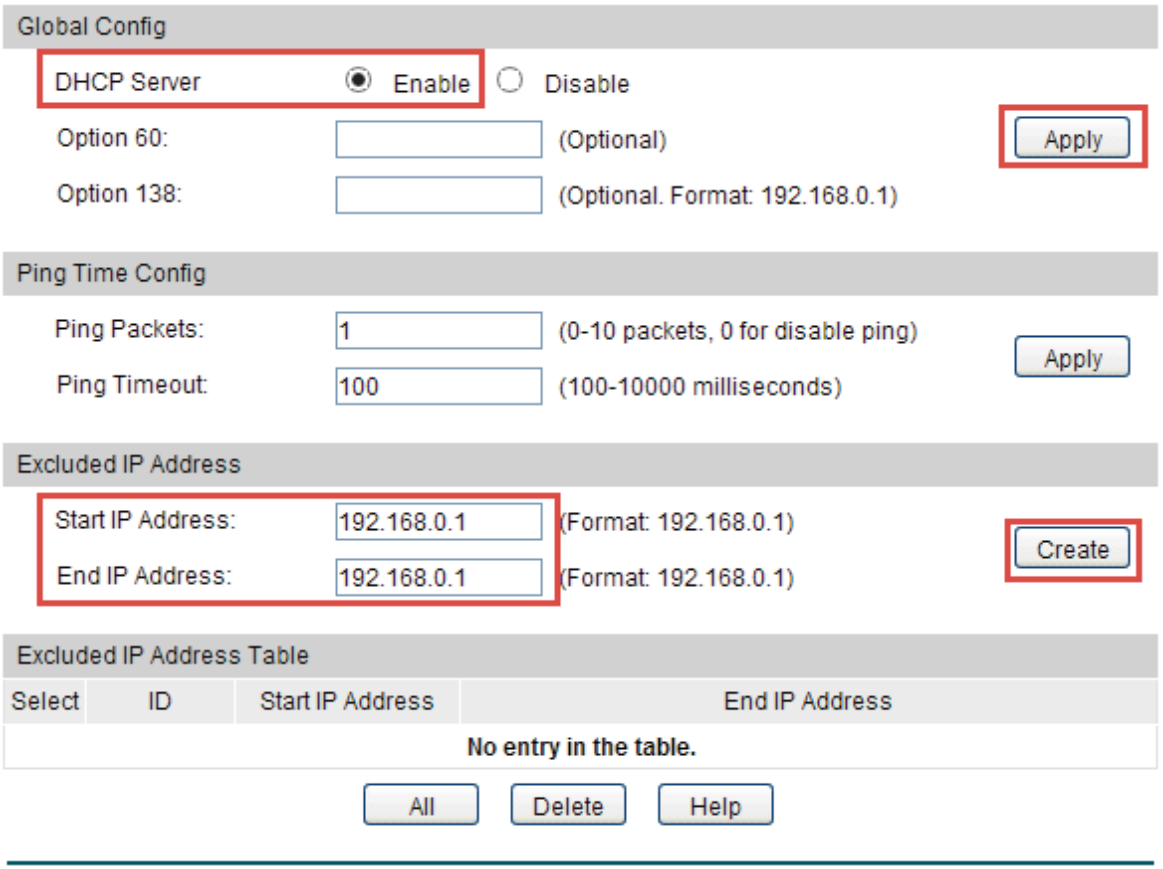


Demonstrated with T2600G-28TS, this chapter provides configuration procedures in two ways: using the GUI and using the CLI.

6.1.3 Using the GUI

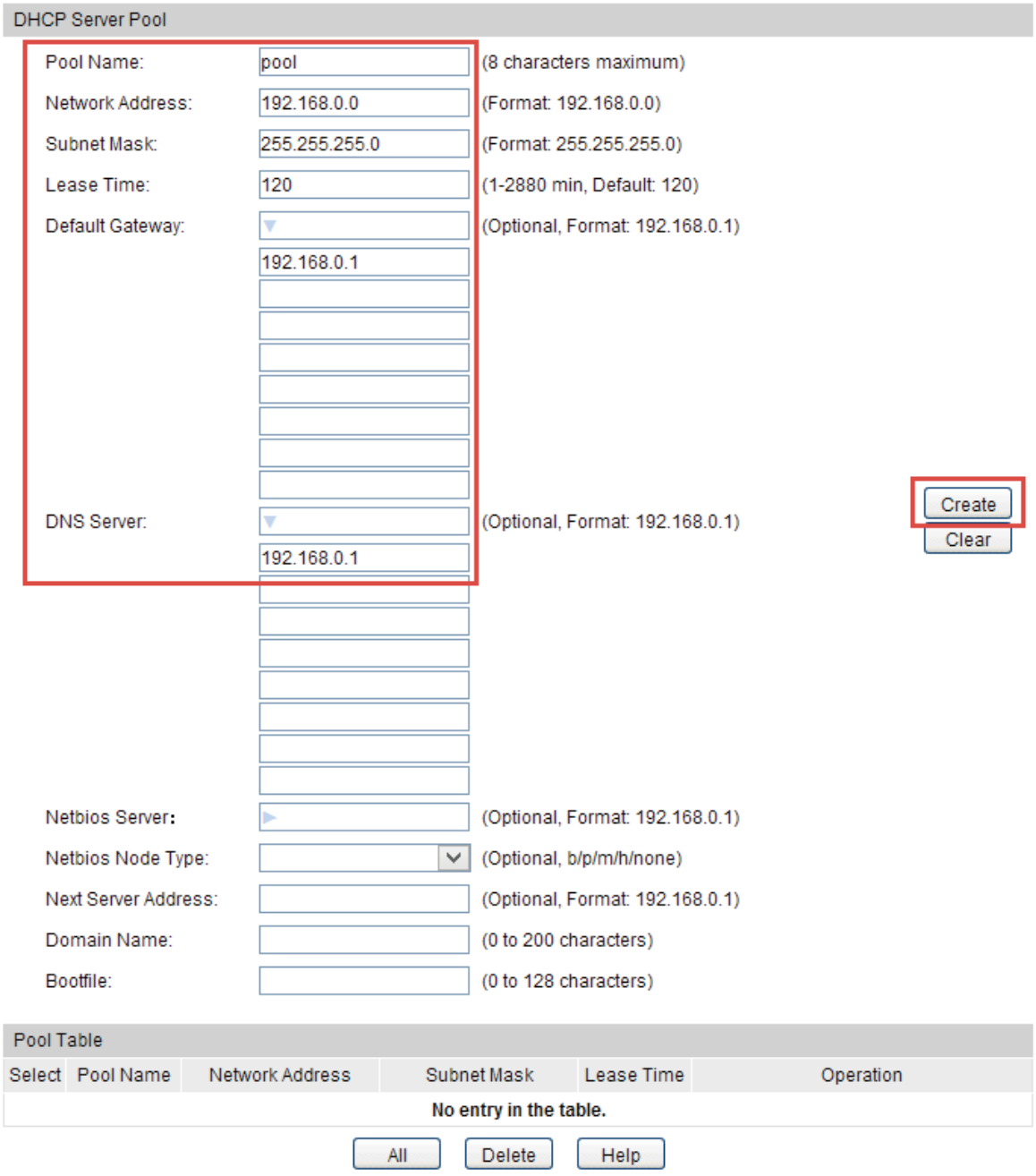
1) Choose the menu **Routing > DHCP Server > DHCP Server** to load the following page. In the **Global Config** section, enable DHCP Server. Because both the gateway address and DNS server address are 192.168.0.1, 192.168.0.1 should be configured as an excluded IP address in the **Excluded IP Address** section.

Figure 6-2 Configuring DHCP Server



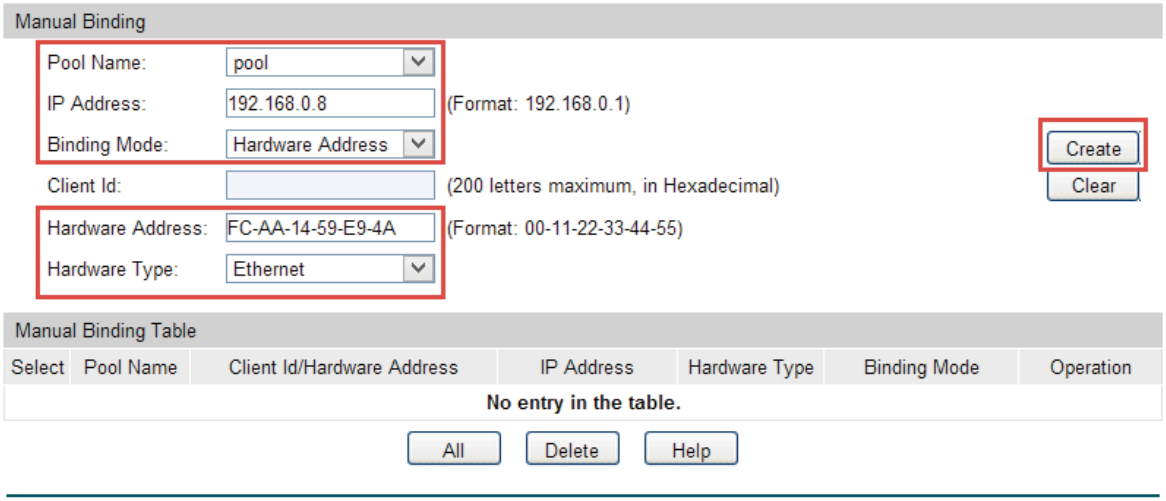
2) Choose the menu **Routing > DHCP Server > Pool Setting** to load the following page. Specify the Pool Name, Network Address, Subnet Mask, Lease Time, Default Gateway and DNS Server as shown below. Click **Create**.

Figure 6-3 Configuring DHCP Server Pool



3) Choose the menu **Routing > DHCP Server > Manual Binding** to load the following page. Select the DHCP server pool you just created, and enter the IP address of the FTP server in the IP Address field. Select Hardware Address as the binding mode, and enter the MAC address of the FTP server in the Hardware Address field. Select Ethernet as the Hardware Type. Click **Create**.

Figure 6-4 Configuring Manual Binding



6.1.4 Using the CLI

1) Enable DHCP Server.

Switch#configure

Switch(config)#service dhcp server

2) Specify the Pool Name, Network Address, Subnet Mask, Lease Time, Default Gateway, DNS Server and Exclude IP Address range.

Switch(config)#ip dhcp server pool pool

Switch(dhcp-config)#network 192.168.0.0 255.255.255.0

Switch(dhcp-config)#lease 120

Switch(dhcp-config)#default-gateway 192.168.0.1

Switch(dhcp-config)#dns-server 192.168.0.1

Switch(dhcp-config)#exit

Switch(config)#ip dhcp server excluded-address 192.168.0.1 192.168.0.1

3) Bind the specified IP address to the MAC address of the FTP server.

Switch(config)# ip dhcp server pool pool

Switch(dhcp-config)# address 192.168.0.8 **hardware-address** FC-AA-14-59-E9-4A **hardware-type ethernet**

Switch(dhcp-config)#end

Switch#copy running-config startup-config

Verify the Configuration

Switch#show ip dhcp server binding

IP Address	Client id/Hardware Address	Type	Lease Time Left
---	---	---	---
192.168.0.2	01-d43d-7ebf-615f	Automatic	01:57:27
192.168.0.8	01-fcaa-1459-e94a	Manual	Infinite

6.2 Example for DHCP Interface Relay

6.2.1 Network Requirements

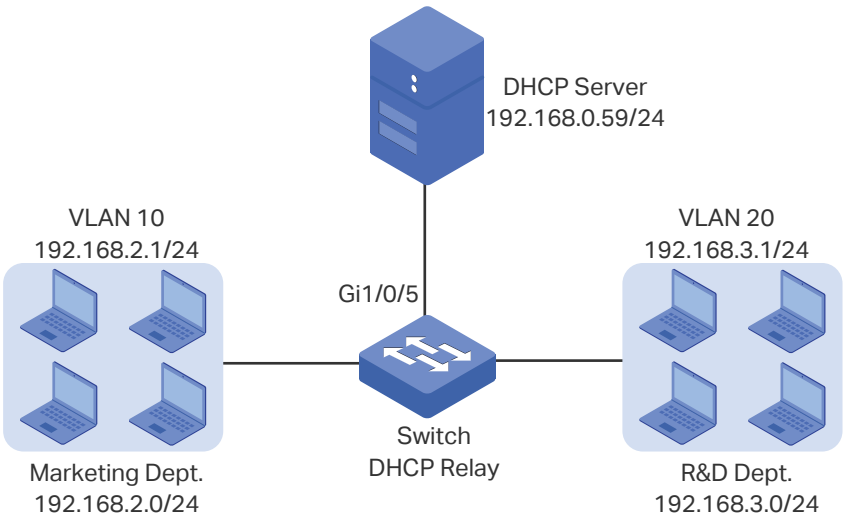
A company wants to assign IP addresses to all computers in two departments, and there is only one DHCP server available. It is required that computers in the same department should be on the same subnet, while computers in different departments should be on different subnets.

6.2.2 Configuration Scheme

In the given situation, the DHCP relay feature can satisfy the requirement because DHCP relay enables DHCP clients from different subnets to share one DHCP server. Make sure your DHCP server supports more than one DHCP address pool.

The network topology is as the following figure shows. Computers in the marketing department belong to VLAN 10 which is connected to the switch via port 1/0/8. The interface address of VLAN 10 is 192.168.2.1/24. Computers in the R&D department belong to VLAN 20 which is connected to the switch via port 1/0/16. The interface address of VLAN 20 is 192.168.3.1/24. The DHCP server is connected to the DHCP Relay switch via port 1/0/5, and its IP address is 192.168.0.59/24.

Figure 6-5 Network Topology for DHCP Relay



The overview of the configurations are as follows:

1) Before DHCP Relay configurations, create two DHCP address pools on the DHCP server, one is on 192.168.2.0/24 and the other is on 192.168.3.0/24. Then create static

routes or enable dynamic routing protocol like RIP on the DHCP server to make sure the DHCP server can reach these two networks.

2) Configure 802.1Q VLAN. Add all computers in the marketing department to VLAN 10, and add all computers in the R&D department to VLAN 20. For details, refer to *Configuring 802.1Q VLAN*.

3) Configure the interface address of the VLANs. For details, refer to *Configuring Logical Interfaces*.

4) Configure DHCP Relay on the switch. Enable DHCP Relay, and add DHCP server address to each VLAN. When these configurations are finished, the DHCP server can assign IP addresses to computers in the two departments, with each department on one subnet.

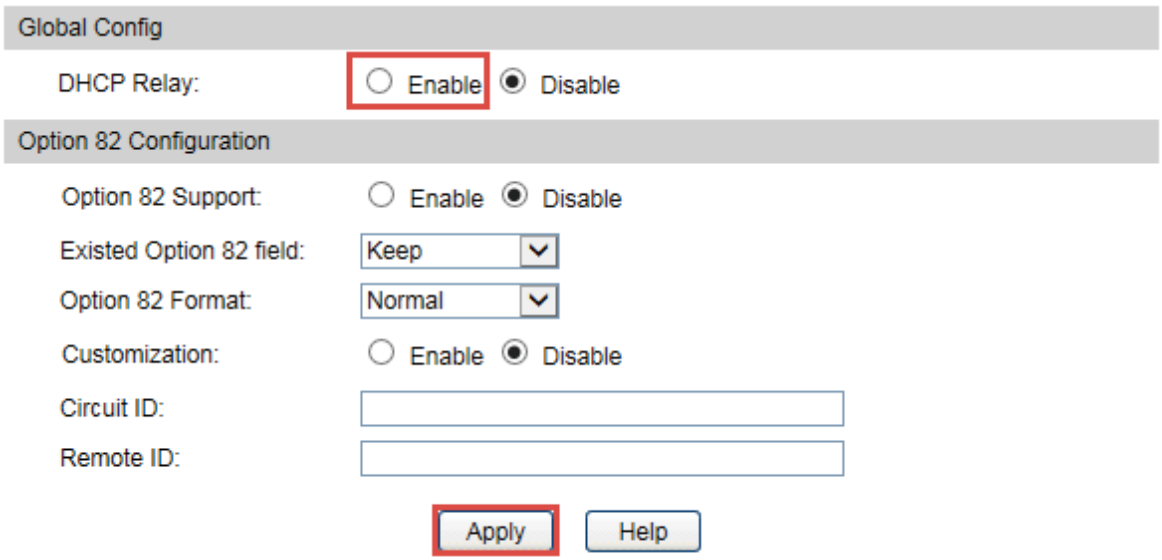
Demonstrated with T2600G-28TS, this chapter provides configuration procedures in two ways: using the GUI and using the CLI.

6.2.3 Using the GUI

Follow these steps to configure DHCP Relay:

1) Choose the menu **Routing > DHCP Relay > Global Config** to load the following page. In the **Global Config** section, enable DHCP Relay, and click **Apply**.

Figure 6-6 Enable DHCP Relay



2) Choose the menu **Routing > DHCP Relay > DHCP Interface Relay** to load the following page. In the **Add DHCP Server Address** section, add the DHCP server address to VLAN 10 and VLAN 20.

Figure 6-7 Specify DHCP Server for Interface VLAN 10

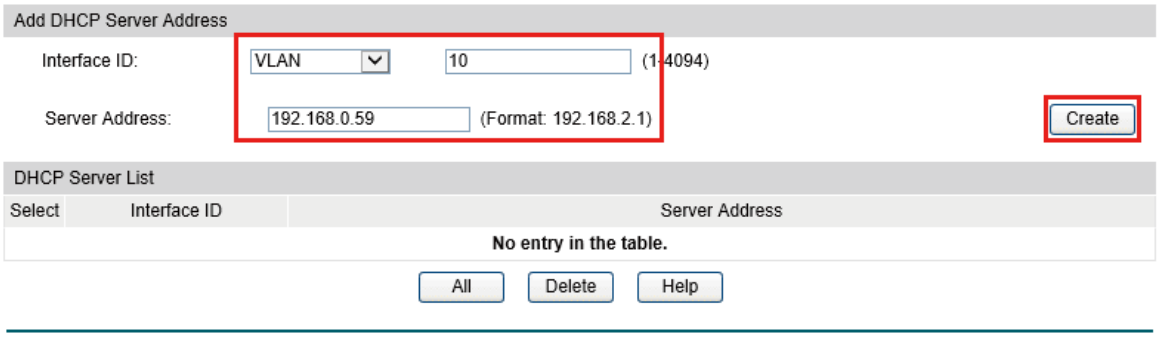
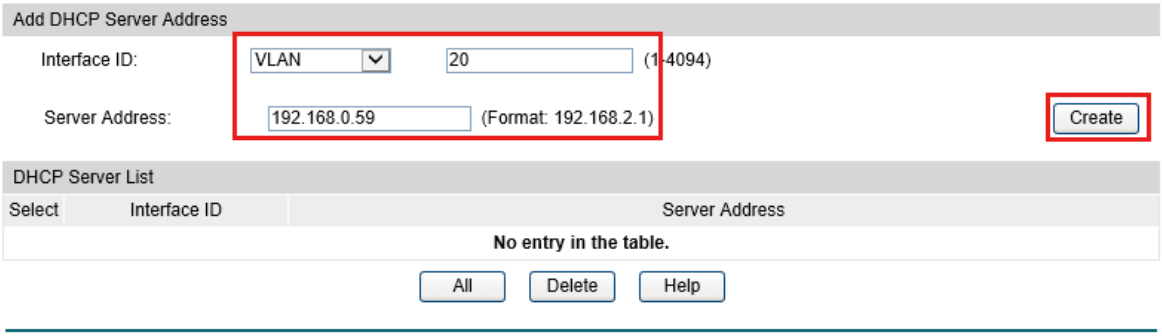


Figure 6-8 Specify DHCP Server for Interface VLAN 20



3) Click **Save Config** to save the settings.

6.2.4 Using the CLI

Follow these steps to configure DHCP Interface Relay:

1) Enable DHCP Relay.

Switch#configure

Switch(config)#service dhcp relay

2) Specify the DHCP server for the interface VLAN 10.

Switch(config)#interface vlan 10

Switch(config-if)#ip helper-address 192.168.0.59

Switch(config-if)#exit

3) Specify the DHCP server for interface VLAN 20

Switch(config)#interface vlan 20

Switch(config-if)#ip helper-address 192.168.0.59

Switch(config-if)#end

Switch#copy running-config startup-config

4) Verify the Configurations

Switch#show ip dhcp relay

DHCP relay is enabled

...

DHCP relay helper address is configured on the following interfaces:

Interface	Helper address
VLAN10	192.168.0.59
VLAN20	192.168.0.59

...

7 Appendix: Default Parameters

Default settings of DHCP Server are listed in the following table.

Table 7-1 Default Settings of DHCP Server

Parameter	Default Setting
Global Config	
DHCP Server	Disable
Option 60	None
Option 138	None
Ping Time Config	
Ping Packets	1
Ping Timeout	100 ms
Excluded IP Address	
Start IP Address	None
End IP Address	None
Pool Setting	
Pool Name	None
Network Address	None
Subnet Mask	None
Lease Time	120 min
Default Gateway	None
DNS Server	None
Netbios Server	None
Netbios Node Type	None
Next Server Address	None
Domain Name	None
Bootfile	None

Parameter	Default Setting
Manual Binding	
Pool Name	None
IP Address	None
Binding Mode	Client Id
Client Id	None
Hardware Address	None
Hardware Type	Ethernet

Default settings of DHCP Relay are listed in the following table.

Table 7-2 Default Settings of DHCP Relay

Parameter	Default Setting
DHCP Relay	
DHCP Relay	Disable
Option 82 Support	Disable
Existed Option 82 field	Keep
Option 82 Format	Normal
Customization	Disable
Circuit ID	None
Remote ID	None
DHCP Interface Relay	
Interface ID	None
Server Address	None
DHCP VLAN Relay	
Interface ID	None
VLAN ID	None
Server Address	None

Default settings of DHCP L2 Relay are listed in the following table.

Table 7-3 Default Settings of DHCP L2 Relay

Parameter	Default Setting
Global Config	
DHCP Relay	Disabled
VLAN Status	Disabled
Port Config	
Option 82 Support	Disabled
Option 82 Policy	Keep
Format	Normal
Circuit ID Customization	Disable
Circuit ID	None
Remote ID Customization	Disabled
Remote ID	None

Default setting of DHCP Client is listed in the following table.

Table 7-4 Default Setting of DHCP Client

Parameter	Default Setting
DHCP Client	Disable

Part 21

Configuring ARP

CHAPTERS

1. Overview
2. ARP Configurations

1 Overview

ARP (Address Resolution Protocol) is used to map IP addresses to MAC addresses. Taking an IP address as input, ARP learns the associated MAC address, and stores the IP-MAC address association in an ARP entry for rapid retrieval.

2 ARP Configurations

With ARP configurations, you can:

- View dynamic and static ARP entries.
- Add or delete static ARP entries.

2.1 Using the GUI

2.1.1 Viewing the ARP Entries

The ARP table consists of two kinds of ARP entries: dynamic and static.

- Dynamic Entry: Automatically learned and will be deleted after aging time.
- Static Entry: Added manually and will be remained unless modified or deleted manually.

Choose the menu **Routing > ARP > ARP Table** to load the following page.

Figure 2-1 Viewing the ARP Entries

ARP Table

Interface	IP Address	MAC Address	Type
Vlan1	192.168.0.73	00-0a-eb-00-13-01	DYNAMIC
Vlan1	192.168.0.18	00-0a-eb-13-12-47	DYNAMIC
Vlan1	192.168.0.226	00-0a-eb-13-23-97	DYNAMIC
Vlan1	192.168.0.61	f4-f2-6d-c3-28-62	DYNAMIC
Vlan1	192.168.0.117	00-0a-eb-13-12-3e	DYNAMIC
Vlan1	192.168.0.200	00-19-66-35-e1-b0	DYNAMIC
Vlan1	192.168.0.37	00-0a-eb-13-12-db	DYNAMIC

Refresh Help

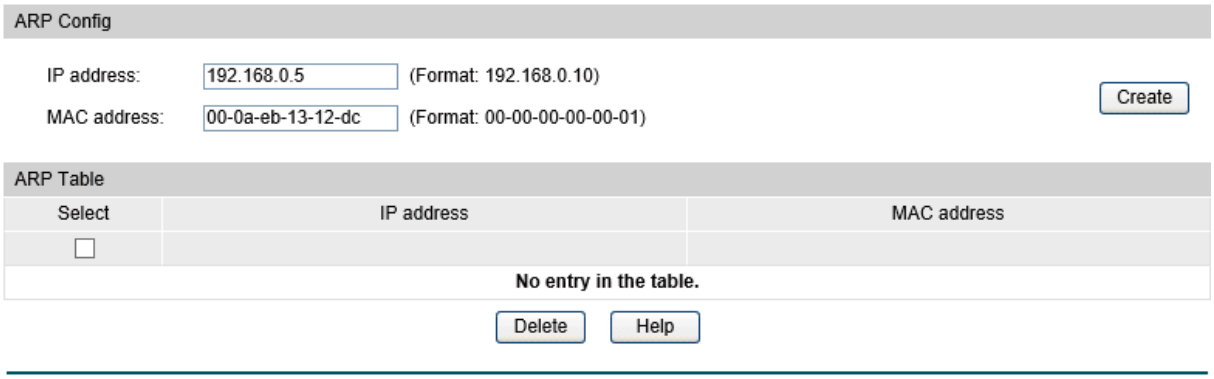
Interface	Displays the network interface of an ARP entry.
IP Address	Displays the IP address of an ARP entry.
MAC Address	Displays the MAC address of an ARP entry.
Type	Displays the type of an ARP entry. **STATIC**: A static ARP entry that will always be remained. **DYNAMIC**: A dynamic ARP entry that will be deleted after aging time.

2.1.2 Adding Static ARP Entries Manually

You can add desired static ARP entries by mannually specifying the IP addresses and MAC addresses.

Choose the menu **Routing > ARP > Static ARP** to load the following page.

Figure 2-2 Adding Static ARP Entries



Follow these steps to add static ARP Entries:

In the **ARP Config** section, enter the IP address and MAC address and click **Create**.

IP address	Specify the IP address.
MAC address	Specify the MAC address.

2.2 Using the CLI

2.2.1 Configuring ARP Function

- Adding Static ARP Entries

Follow these steps to add ARP entries:

Step 1	**configure** Enter global configuration mode.
Step 2	**arp** *ip mac type* Add a static ARP entry. *ip*: Enter the IP address of the static ARP entry. *mac:* Enter the MAC address of the static ARP entry. *type:* Enter the ARP type. Configure it as 'arpa'.

Step 3	**show arp** [*ip*] [*mac*] or **show ip arp** [*ip*] [*mac*] Verify the ARP entries. *ip*: Specify the IP address of your desired ARP entry. *mac:* Specify the MAC address of your desired ARP entry.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

This example shows how to create a static ARP entry with the IP as 192.168.0.1 and the MAC as 00:11:22:33:44:55:

Switch#configure

Switch(config)#arp 192.168.0.1 00:11:22:33:44:55 **arpa**

Switch(config)#show arp 192.168.0.1

Interface	Address	Hardware Addr	Type
Vlan1	192.168.0.1	00:11:22:33:44:55	STATIC

Switch(config)#end

Switch#copy running-config startup-config

■ Configuring the aging time of dynamic ARP entries

Follow these steps to configure the aging time of dynamic ARP entries:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list***}** Enter interface configuration mode. *port*| *port-list*: The number or the list of the Ethernet port that you want to configure. **interface vlan** *vlan-id* Enter interafce VLAN mode. *vlan-id:* Specify a vlan interface ID.

Step 3	**arp timeout** *timeout* Configure the ARP aging time of the VLAN interface or routed port . *timeout:* Specify the value of aging time, which ranges from 1 to 3000 in seconds. The default value is 600 seconds.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

This example shows how to configure the aging time of dynamic ARP entries as 1000 seconds for VLAN interface 2 :

Switch#configure

Switch(config)#interface vlan 2

Switch(config-if)#arp timeout 1000

Switch(config-if)#end

Switch#copy running-config startup-config

■ Clearing dynamic entries

Step 1	**end** Return to privileged EXEC mode.
Step 2	**clear arp-cache** Clear all the dynamic ARP entries.
Step 3	**copy running-config startup-config** Save the settings in the configuration file.

■ Viewing ARP Entries

On privileged EXEC mode or any other configuration mode, you can use the following command to view ARP entries:

show arp [*ip*] [*mac*]

or

show ip arp [*ip*] [*mac*]

Verify the active ARP entries.

ip: Specify the IP address of your desired ARP entry.

mac: Specify the MAC address of your desired ARP entry.

show ip arp { gigabitEthernet *port* **| port-channel** *lagid* **| vlan** *id* **}**

Verify the active ARP entries associated with a Layer 3 interface.

port: Specify the number of the routed port.

lagid: Specify the ID of the LAG.

id: Specify the VLAN interface ID.

Part 22

Configuring QoS

CHAPTERS

1. QoS
2. DiffServ Configuration
3. Bandwidth Control Configuration
4. Configuration Examples
5. Appendix: Default Parameters

1 QoS

1.1 Overview

With network scale expanding and applications developing, Internet traffic is dramatically increased, thus resulting in network congestion, packet drops and long transmission delay. Typically, networks treat all traffic equally on FIFO (First In First Out) delivery basis, but nowadays many special applications like VoD, video conferences, etc. require more bandwidth or shorter transmission delay to guarantee the performance.

With QoS (Quality of Service) technology, you can classify and prioritize network traffic to provide DiffServ (Differentiated Services) to certain types of traffic.

1.2 Supported Features

You can configure the DiffServ and bandwidth control features on the switch to maximize the network performance and bandwidth utilization.

DiffServ

The switch classifies the ingress packets, maps the packets to different priority queues and then forwards the packets according to specified scheduling algorithms to implement QoS function.

- Priority Mode: Three modes are supported, Port Priority, 802.1P Priority and DSCP Priority.
- Schedule Mode: Four schedule modes are supported, SP, WRR, SP+WRR and Equ.

Bandwidth Control

Bandwidth Control functions to control the traffic rate and broadcast flow on each port to ensure network performance.

- Rate limit functions to limit the ingress/egress traffic rate on each port. In this way, the network bandwidth can be reasonably distributed and utilized.
- Storm Control function allows the switch to filter broadcast packets, multicast packets and UL-frames (Unknown unicast frames) in the network. If the transmission rate of the packets exceeds the set rate, the packets will be automatically discarded to avoid network broadcast storm.

2 DiffServ Configuration

With class of service configurations, you can:

- Configure port priority
- Configure 802.1p priority
- Configure DSCP priority
- Specify the scheduler settings

Configuration Guidelines

- Select the priority mode that the ports trust according to your network requirements.

  A port can use only one priority to classify the ingress packets. Three priority modes are supported on the switch: Port Priority, 802.1P Priority and DSCP Priority.

  » Port Priority

  In this mode, the switch prioritizes packets according to their ingress ports, regardless of the packet field or type.

  » 802.1P Priority

  802.1P defines the first three bits in 802.1Q Tag as PRI field. The PRI values are from 0 to 7. 802.1P priority determines the priority of packets based on the PRI value.

  In this mode, the switch only prioritizes packets with VLAN tag, regardless of the IP header of the packets.

  » DSCP Priority

  DSCP priority determines the priority of packets based on the ToS (Type of Service) field in their IP header. RFC2474 re-defines the ToS field in the IP packet header as DS field. The first six bits (bit 0-bit 5) of the DS field is used to represent DSCP priority. The DSCP values are from 0 to 63.

  In this mode, the switch only prioritizes IP packets.

- Specify the 802.1p to queue mapping according to your needs.

  For 802.1p Priority, the packets will be forwarded according to the 802.1p to queue mapping directly.

  For Port Priority and DSCP Priority, the port priority and DSCP priority will first be mapped to the 8021p priority, and then mapped to the queue according to the 802.1p to queue mapping.

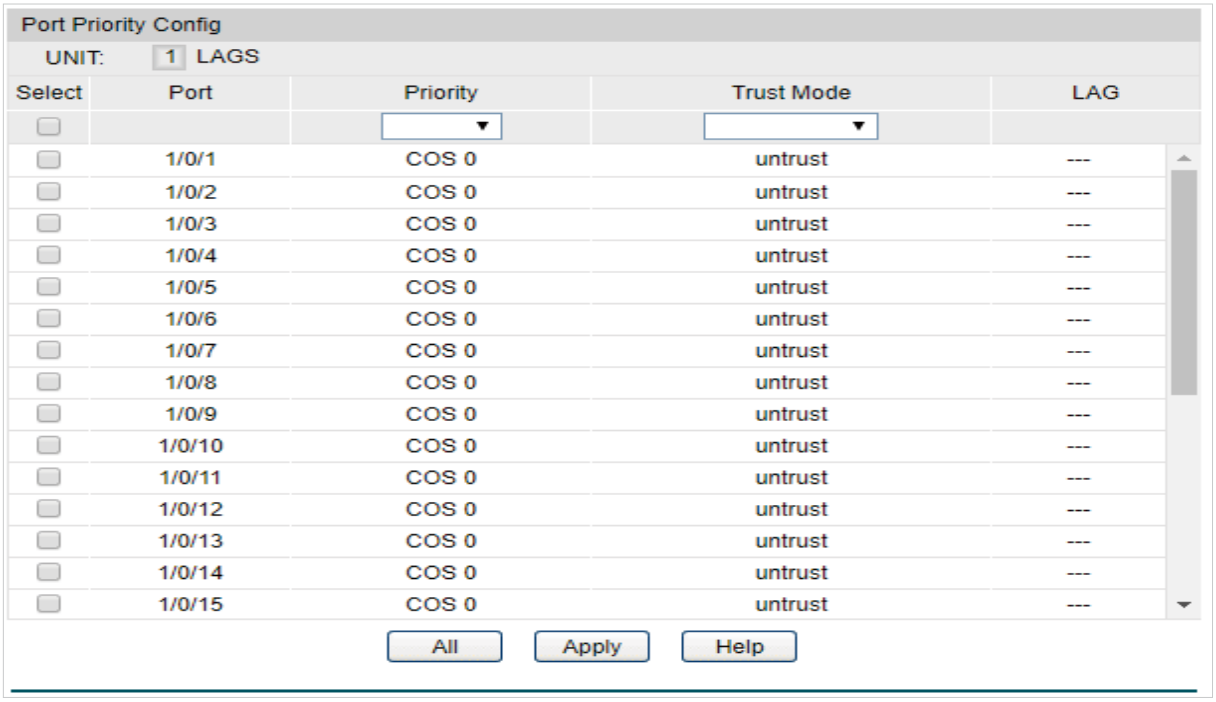
2.1 Using the GUI

2.1.1 Configuring Port Priority

- Configuring the Trust Mode and Port to 802.1p Mapping

Choose the menu **QoS > DiffServ > Port Priority** to load the following page.

Figure 2-1 Configuring the Trust Mode and Port to 802.1p Mapping



Follow these steps to configure the parameters of the port priority:

1) Select the desired ports, specify the 802.1p priority and set the **Trust Mode** as **untrust**.

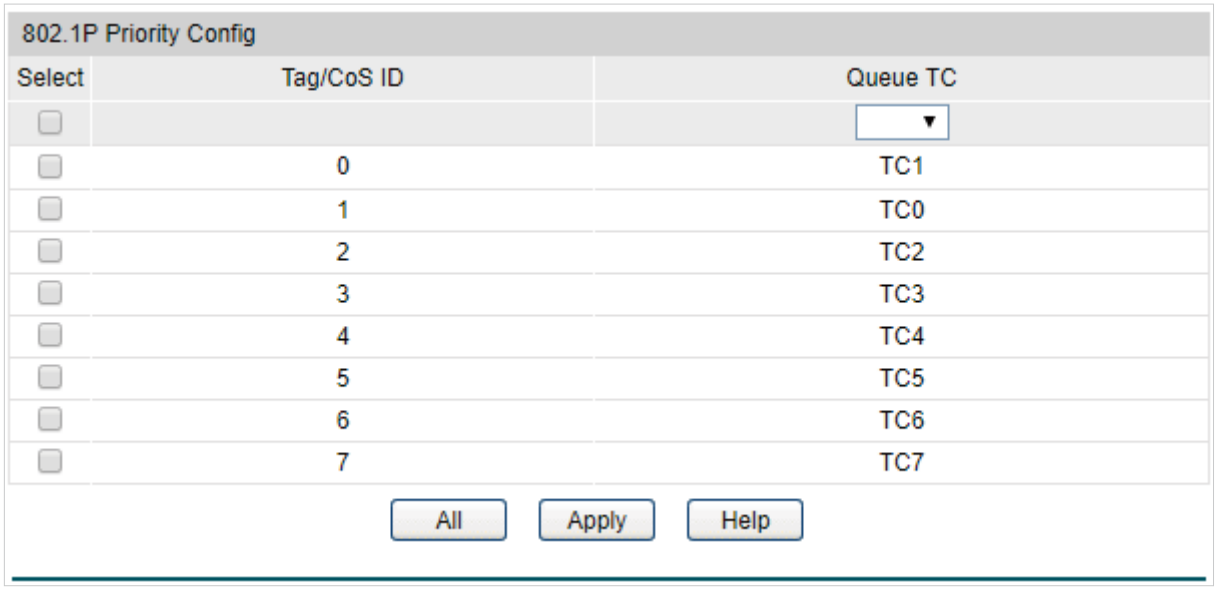
Priority	Specify the port to 802.1p mapping for the desired port. The ingress packets from one port are first mapped to 802.1p priority based on the port to 802.1p mapping, then to TC queues based on the 802.1p to queue mapping. The untagged packets from one port will be added an 802.1p priority value according to the port to 802.1p priority mapping.
Trust Mode	Select the **Trust Mode** as **untrust**. In this mode, the packets will be processed according to the port priority configuration.

2) Click **Apply**.

Configuring the 802.1P to Queue Mapping

Choose the menu **QoS > DiffServ > 802.1P Priority** to load the following page.

Figure 2-2 Configuring the 802.1p to Queue Mapping



Follow these steps to configure the 802.1P to Queue Mapping:

1) In the **802.1P Priority Config** section, configure the mappings.

Tag/CoS ID	Displays the number of 802.1p priority. In QoS, 802.1p priority is used to represent class of service.
Queue TC	Select the TC queue for the desired 802.1p priority. The packets with the desired 802.1p priority will be put in the corresponding queue.

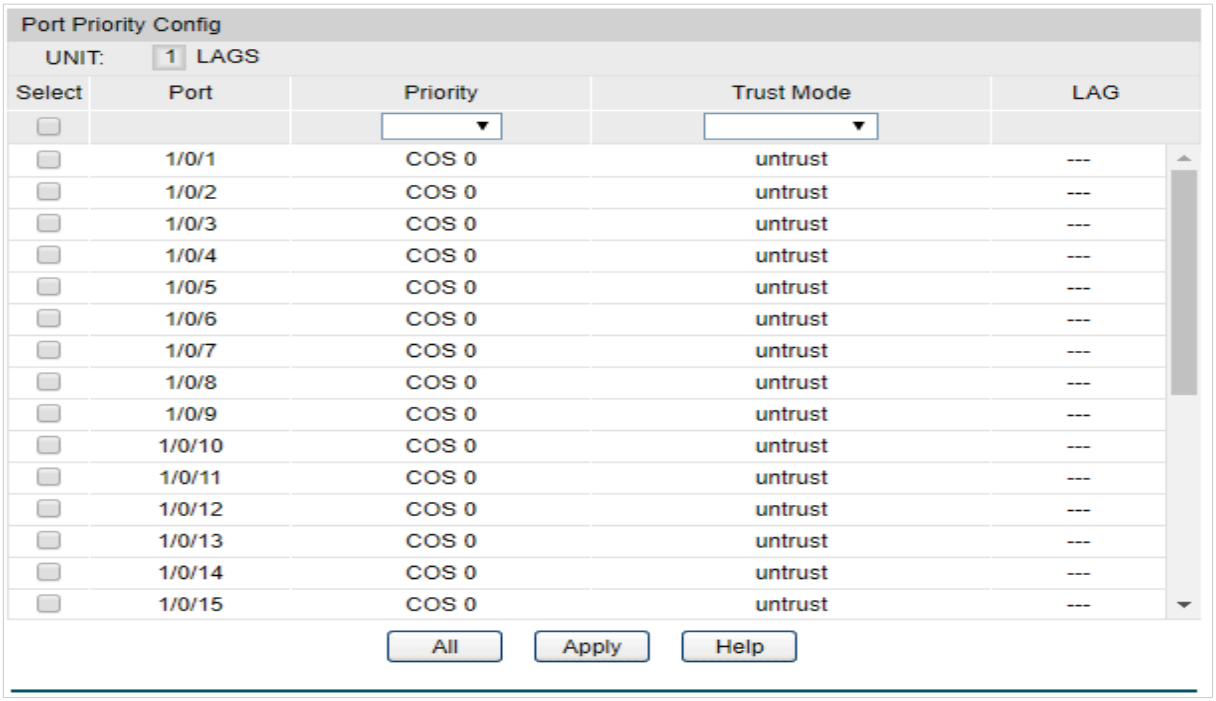
2) Click **Apply.**

2.1.2 Configuring 802.1P Priority

■ Configuring the Trust Mode

Choose the menu **QoS > DiffServ > Port Priority** to load the following page.

Figure 2-3 Configuring the Trust Mode



Follow these steps to configure the trust mode:

1) Select the desired ports and set the **Trust Mode** as **trust 802.1p**.

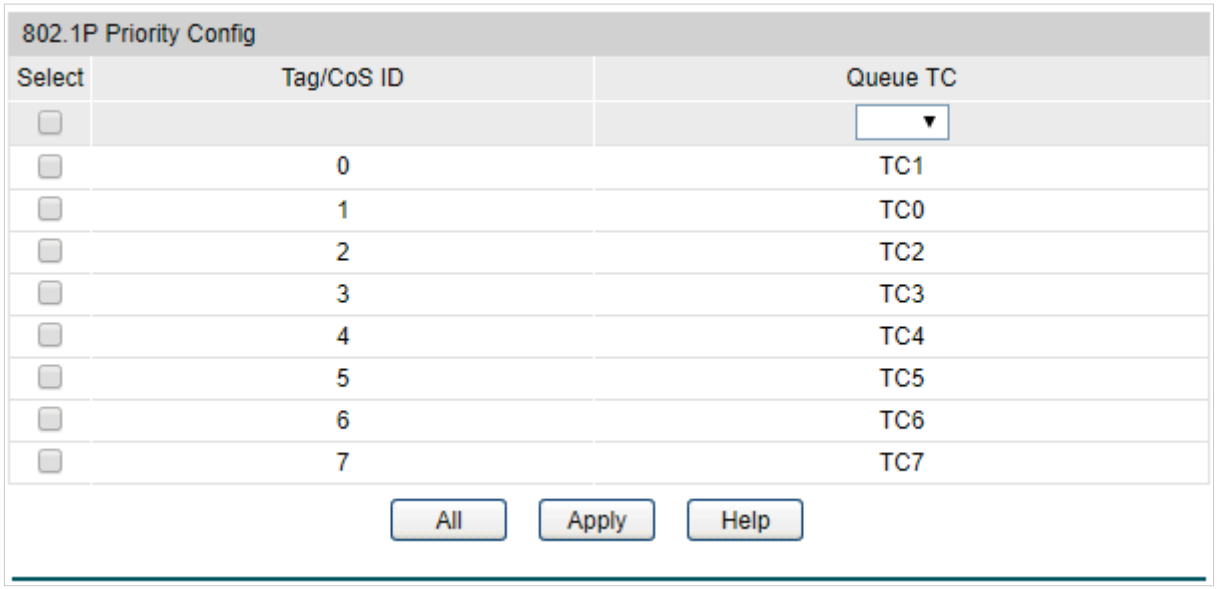
Trust Mode	Select the **Trust Mode** as **trust 802.1p**. In this mode, packets with VLAN tag will be processed according to the 802.1p priority configuration, and packets without VLAN tag will be processed according to the port priority configuration.

2) Click **Apply**.

Configuring the 802.1P to Queue Mapping

Choose the menu **QoS > DiffServ > 802.1P Priority** to load the following page.

Figure 2-4 Configuring the 802.1p to Queue Mapping



Follow these steps to configure the 802.1P to Queue Mapping:

1) In the **802.1P Priority Config** section, configure the mappings.

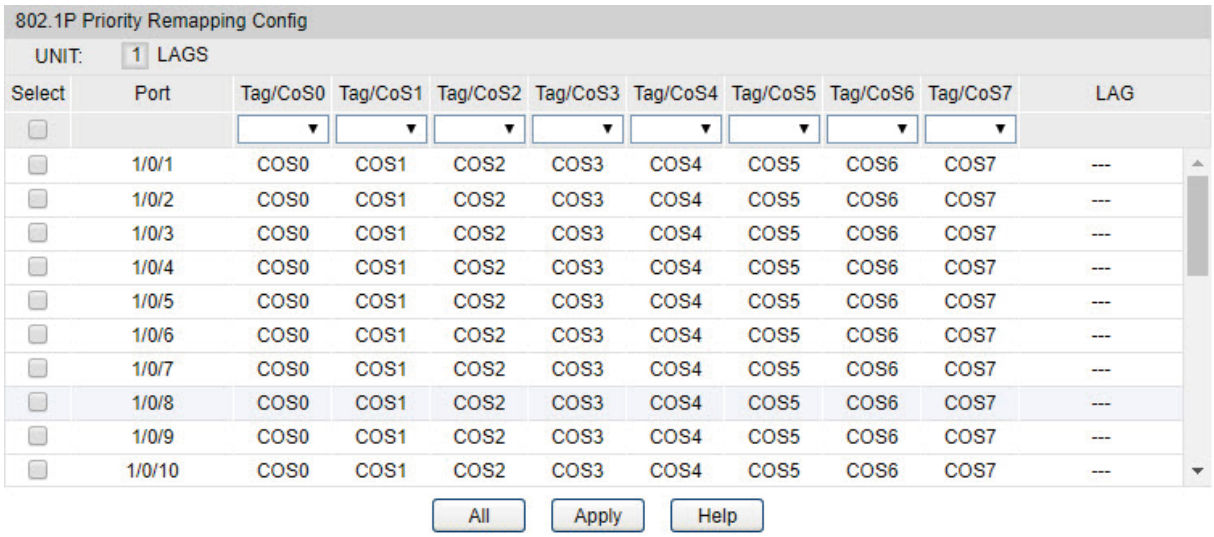
Tag/CoS ID	Displays the number of 802.1p priority. In QoS, 802.1p priority is used to represent class of service.
Queue TC	Select the TC queue for the desired 802.1p priority. The packets with the desired 802.1p priority will be put in the corresponding queue.

2) Click **Apply.**

(Optional) Configuring the 802.1P Priority Remapping

Choose the menu **QoS > DiffServ > 802.1P Priority Remapping** to load the following page.

Figure 2-5 Configuring the 802.1P Priority Remapping



Follow these steps to configure the 802.1P Priority Remapping:

1) In the **802.1P Priority Remapping Config** section, select the desired ports and configure the remapping.

Tag/CoS0-7	Select the number of 802.1p priority to which the desired 802.1p priority will be remapped. 802.1p Remap is used to modify the 802.1p priority of the ingress packets. When the switch detects the packets with desired 802.1p priority, it will modify the value of 802.1p priority according to the map.

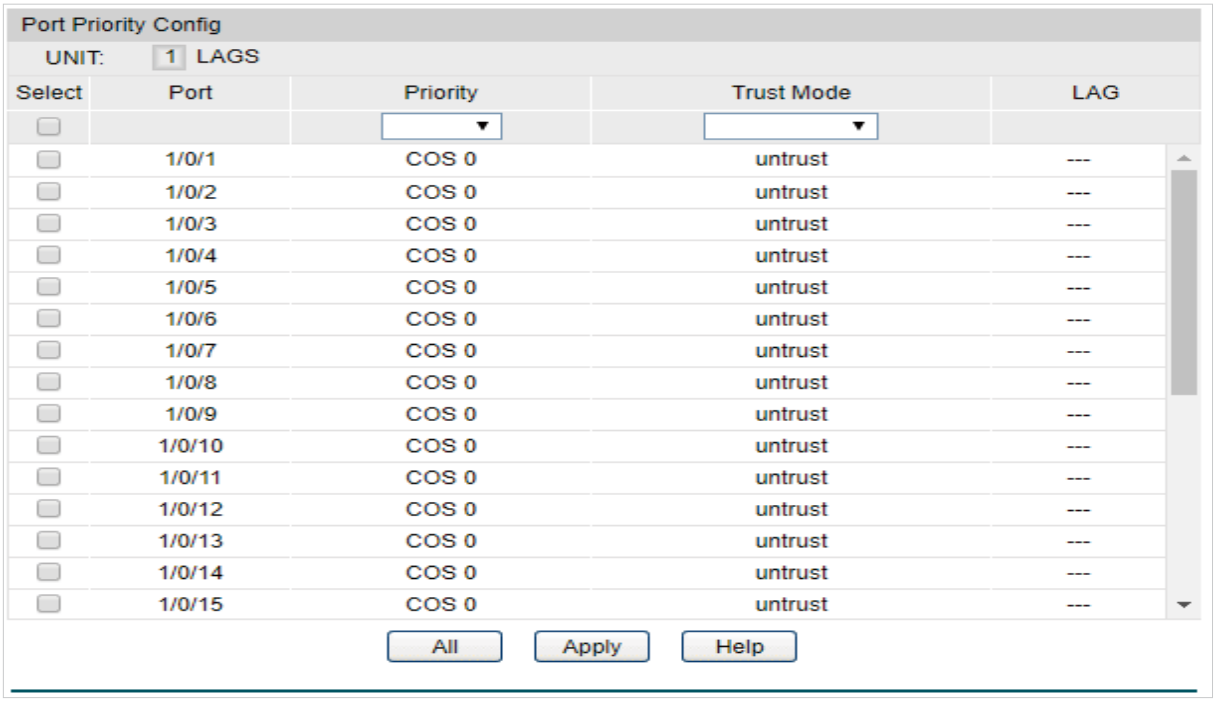
2) Click **Apply.**

2.1.3 Configuring DSCP Priority

■ Configuring the Trust Mode

Choose the menu **QoS > DiffServ > Port Priority** to load the following page.

Figure 2-6 Configuring the Trust Mode



Follow these steps to configure the trust mode:

1) Select the desired ports and set the **Trust Mode** as **trust DSCP**.

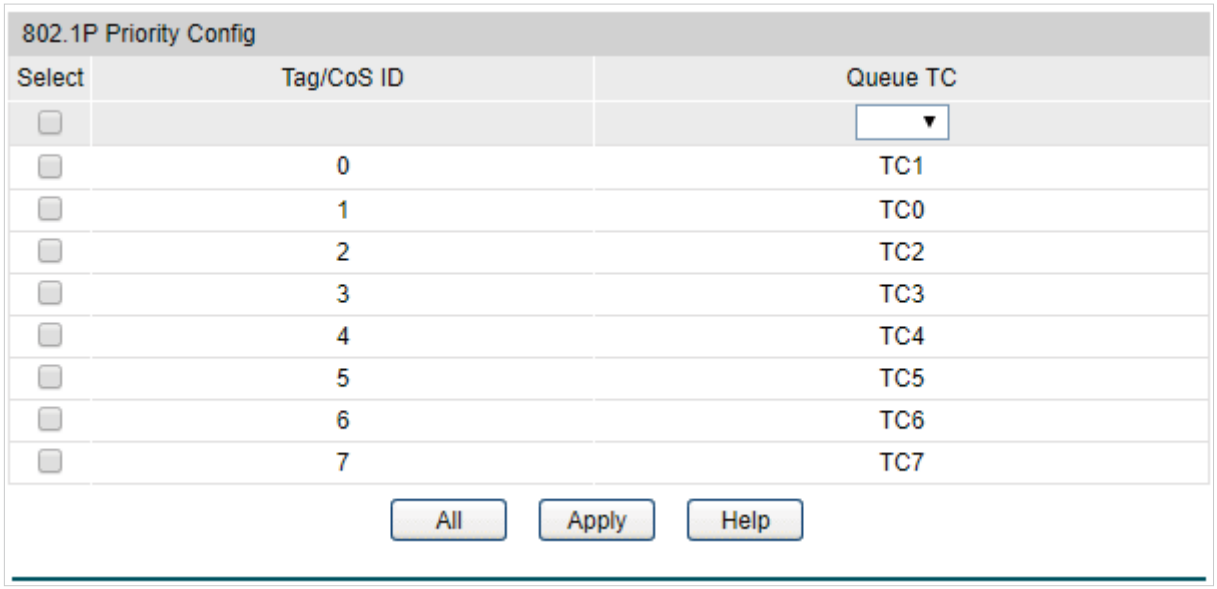
Trust Mode	Select the Trust mode as trust DSCP. In this mode, IP packets will be processed according to the DSCP Priority configuration, and other packets will be processed according to the port priority configuration

2) Click **Apply**.

Configuring the 802.1P to Queue Mapping

Choose the menu **QoS > DiffServ > 802.1P Priority** to load the following page.

Figure 2-7 Configuring the 802.1p to Queue Mapping



Follow these steps to configure the 802.1P to Queue Mapping:

1) In the **802.1P Priority Config** section, configure the mappings.

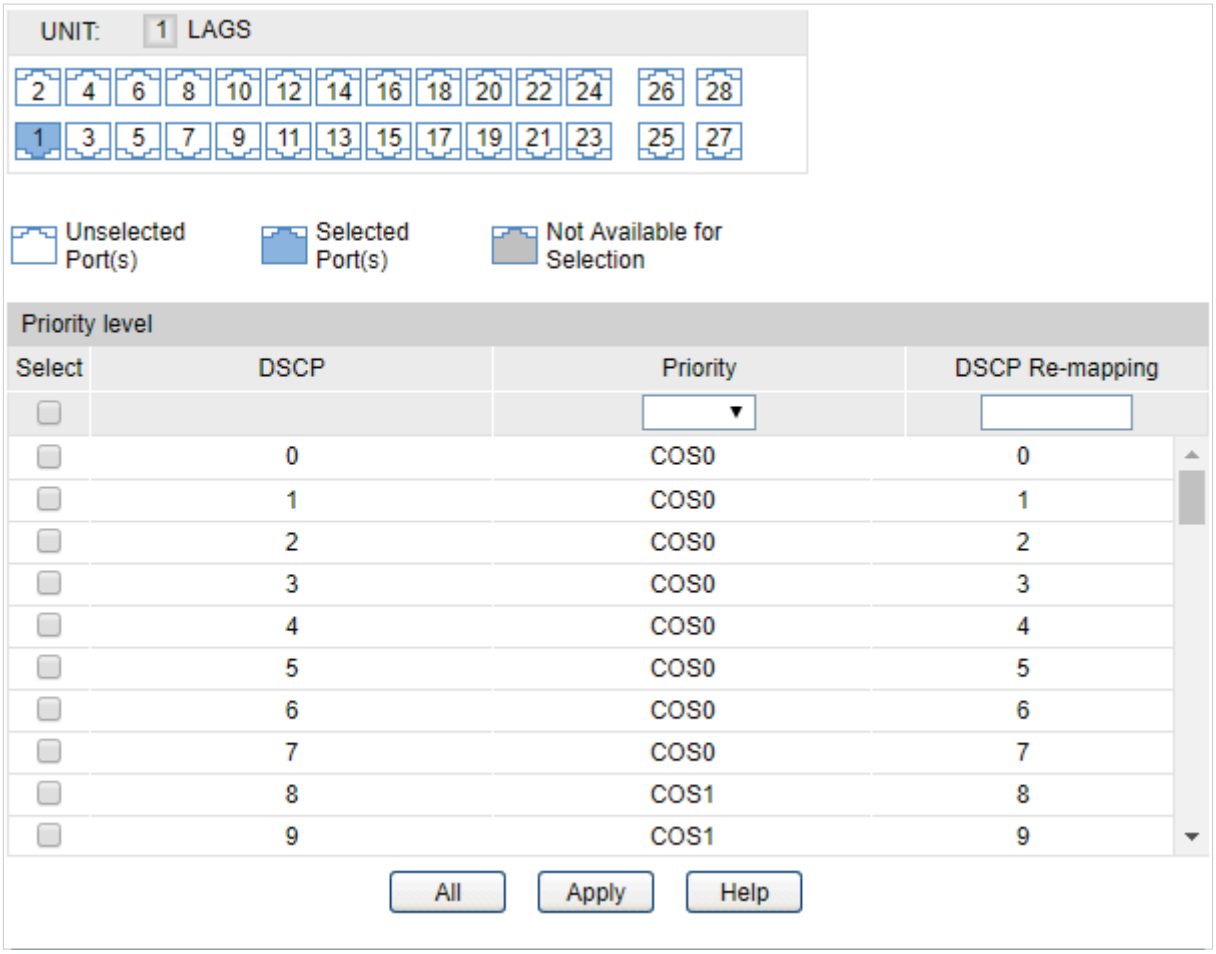
Tag/CoS ID	Displays the number of 802.1p priority. In QoS, 802.1p priority is used to represent class of service.
Queue TC	Select the TC queue for the desired 802.1p priority. The packets with the desired 802.1p priority will be put in the corresponding queue.

2) Click **Apply.**

Configuring the DSCP to 802.1p Mapping and the DSCP Remap

Choose the menu **QoS > DIffServ >DSCP Priority** to load the following page.

Figure 2-8 Configuring the DSCP to 802.1p Mapping and the DSCP Remap



Follow these steps to configure the DSCP Priority:

1) Select the desired port, configure the DSCP to 802.1p mapping and the DSCP remap.

DSCP	Displays the number of DSCP priority. DSCP Priority is used to classify the packets based on the value of DSCP, and map them to different queues. ToS (Type of Service) is a part of IP header, and DSCP uses the first six bits of ToS to represent the priority of IP packets. The DSCP values range from 0 to 63.
Priority	Specify the DSCP to 802.1p mapping for the desired port. The ingress packets are first mapped to 802.1p priority, then to TC queues according to the 802.1p to queue mappings.
DSCP Re-mapping	(Optional) Select the DSCP priority to which the desired DSCP priority will be remapped for the port. When the switch detects the packets with desired DSCP value, it will modify the packets' DSCP value according to the map.

2) Click **Apply**.

Note:

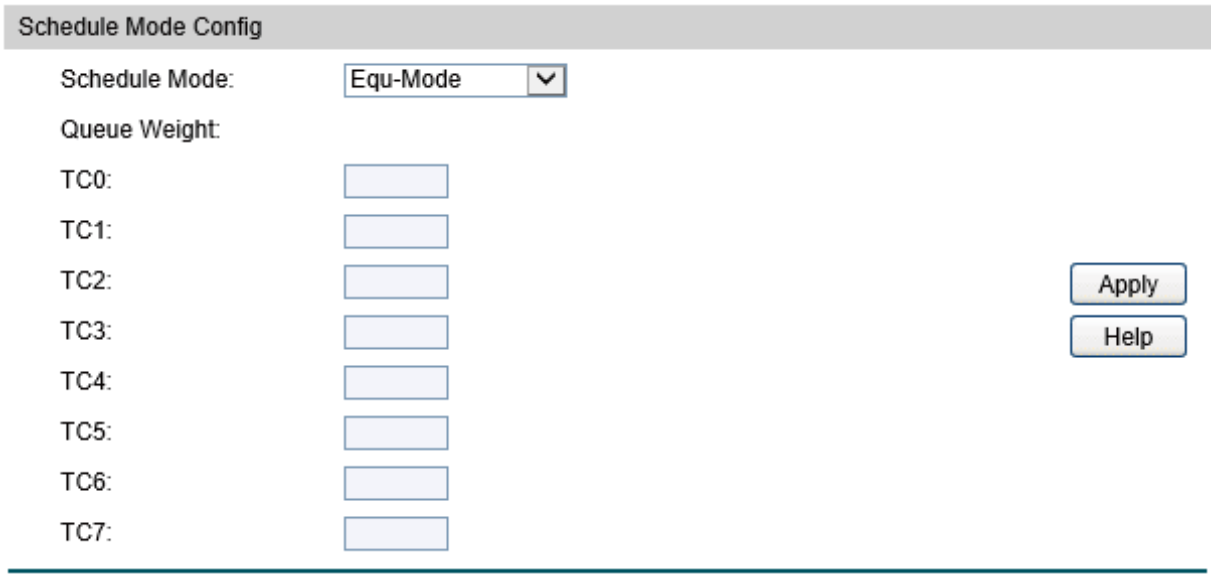
All the ports in the same LAG should be assigned with the same port priority.

2.1.4 Configuring Schedule Mode

Configure the schedule mode to control the forwarding sequence of different TC queues when congestion occurs.

Choose the menu **QoS > DiffServ > Schedule Mode** to load the following page.

Figure 2-9 Schedule Mode



Follow these steps to configure the schedule mode:

1) Select a schedule mode.

SP-Mode	Strict-Priority Mode. In this mode, the queue with higher priority will occupy the whole bandwidth. Packets in the queue with lower priority are sent only when the queue with higher priority is empty.
WRR-Mode	Weight Round Robin Mode. In this mode, packets in all the queues are sent in order based on the weight value for each queue. By default, the weight value ratio of TC0 to TC7 is 1:2:4: ... :127.
SP+WRR-Mode	Strict-Priority + Weight Round Robin Mode. In this mode, the switch provides two scheduling groups, SP group and WRR group. When scheduling queues, the switch allows the queues in the SP group to occupy the whole bandwidth following the SP mode. When the SP group is empty, the queues in the WRR group will take up the bandwidth according to their weight value ratio. By default, queue TC7 is in SP group and TC0, TC1...TC6 are in WRR group.
Equ-Mode	Equal-Mode. In this mode, all the queues occupy the bandwidth equally. The weight value ratio of all the queues is 1:1:1:1. Equ-Mode is selected by default.

2) (Optional) Configure the weight value of the each TC queue if the schedule mode is WRR of SP+WRR.

Queue Weight	Configure the weight value of the each TC queue. In WRR mode, the 8 queues will take up the bandwidth according to their ratio. The default values of TC0, TC1, TC2, TC3, TC4, TC5,TC6 and TC7 are 1, 2, 4, 8, 16, 32, 64 and 127 respectively. In SP+WRR mode, TC7 and the queue with its weight value set as 0 are in the SP group; other queues, with none-zero weight value, belong to the WRR group. In this SP+WRR scheduling mode, the queues in the SP group is scheduled preferentially (TC7>TC6>TC5>TC4>TC3>TC2>TC1>TC0 in strict priority). When there is no packets to be sent in the SP group, the queues in the WRR group will be scheduled according to the weight value of each queue. The default weight values of TC0, TC1, TC2, TC3, TC4, TC5 and TC6 are 1, 2, 4, 8, 16, 32 and 64 respectively, while the value of TC7 is 0 and non-configurable.

3) Click **Apply**.

Note:

With ACL Redirect feature, the switch maps all the packets that meet the configured ACL rules to the new TC queue, regardless of the mapping relations configured in this section.

2.2 Using CLI

2.2.1 Configuring Port Priority

- Configuring the Trust Mode and the port to 802.1P Mapping

Follow these steps to configure the trust mode and the port to 802.1P mapping:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Enter interface configuration mode.
Step 3	**qos trust mode** untrust Specify the trust mode of the port as untrust. In this mode, the packets will be processed according to the port priority configuration.

Step 4	**qos port-priority** *dot1p-priority* Specify the port to 802.1p priority mapping for the desired port. The ingress packets from one port are first mapped to 802.1p priority based on the port to 802.1p mapping, then to TC queues based on the 802.1p to queue mapping. The untagged packets from one port will be added an 802.1p priority value according to the port to 802.1p mapping. *dot1p-priority*: Specify the 802.1p priority ranging from 0 to 7. The default value is 0.
Step 5	**show qos trust-mode interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]** Verify the trust mode of the ports.
Step 6	**show qos port-priority interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]** Verify the port to 802.1p mappings.
Step 7	**end** Return to privileged EXEC mode.
Step 8	**copy running-config startup-config** Save the settings in the configuration file.

Configuring the 802.1P to Queue Mapping

Follow these steps to configure the 802.1P to queue mapping:

Step 1	**configure** Enter global configuration mode.
Step 2	**qos cos-map {***dot1p-priority***} {***tc-queue***}** Specify the 802.1p to queue mapping. The packets with the desired 802.1p priority will be put in the corresponding queues. By default, the 802.1p priority 0 to 7 is respectively mapped to TC-1, TC-0, TC-2, TC-3, TC-4, TC-5, TC-6, TC-7. *dot1p-priority*: Specify the 802.1p priority. The valid values are from 0 to 7. *tc-queue*: Specify the ID number of the TC queue. The valid values are from 0 to 7.
Step 3	**show qos cos-map** Verify the 802.1p to queue mappings.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the trust mode of port 1/0/1 as untrust, map the port 1/0/1 to 802.1p priority 1 and map 802.1p priority 1 to TC3:

Switch#configure

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

Switch(config-if)#qos trust mode untrust

Switch(config-if)#qos port-priority 1

Switch(config-if)#exit

Switch(config)#qos cos-map 1 3

Switch(config)#show qos trust-mode interface gigabitEthernet 1/0/1

```
Port       Trust Mode      LAG
--------   ---------       --------
Gi1/0/1    untrust         N/A
```

Switch(config)#show qos port-priority interface gigabitEthernet 1/0/1

```
Port       CoS Value       LAG
--------   ---------       --------
Gi1/0/1    CoS  1          N/A
```

Switch(config)#show qos cos-map

```
-----+-----+-----+-----+-----+-----+-----+----+----
Tag |0     |1     |2     |3     |4     |5     |6    |7
-----+-----+-----+-----+-----+-----+-----+----+----
TC   |TC0 |TC3 |TC2 |TC3 |TC4 |TC5 |TC6 |TC7
-----+-----+-----+-----+-----+-----+-----+----+----
```

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Configuring 802.1P Priority

- Configuring the Trust Mode

Follow these steps to configure the trust mode:

Step 1	**configure** Enter global configuration mode.

Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet port | range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Enter interface configuration mode.
Step 3	**qos trust mode** dot1p Specify the trust mode of the port as dot1p. In this mode, packets with VLAN tag will be processed according to the 802.1p priority configuration, and packets without VLAN tag will be processed according to the port priority configuration.
Step 4	**show qos trust-mode interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]** Verify the trust mode of the ports.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

Configuring the 802.1P to Queue Mapping and 802.1P Remap

Follow these steps to configure the 802.1p to queue mapping and 802.1p remap:

Step 1	**configure** Enter global configuration mode.
Step 2	**qos cos-map {***dot1p-priority***} {***tc-queue***}** Specify the 802.1p to queue mapping. The packets with the desired 802.1p priority will be put in the corresponding queues. By default, the 802.1p priority 0 to 7 is respectively mapped to TC-1, TC-0, TC-2, TC-3, TC-4, TC-5, TC-6, TC-7. *dot1p-priority*: Specify the 802.1p priority. The valid values are from 0 to 7. *tc-queue*: Specify the ID number of the TC queue. The valid values are from 0 to 7.
Step 3	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Enter interface configuration mode.
Step 4	**qos dot1p-remap {***dot1p-priority***} {***new-dot1p-priority***}** (Optional) Specify the 802.1p to 802.1p mappings. 802.1p Remap is used to modify the 802.1p priority of the ingress packets. When the switch detects the packets with desired 802.1p priority, it will modify the value of 802.1p priority according to the map. By default, the original 802.1p priority 0 is mapped to the 802.1p priority 0, the original 802.1p priority 1 is mapped to the 802.1p priority 1 and so on. *dot1p-priority*: Specify the original 802.1p priority. The valid values are from 0 to 7. *new-dot1p-priority*: Specify the new 802.1p priority. The valid values are from 0 to 7.

Step 5	**show qos cos-map** Verify the 802.1p to queue mappings.
Step 6	**show qos dot1p-remap interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]** Verify the 802.1p to 802.1p mappings of the ports.
Step 7	**end** Return to privileged EXEC mode.
Step 8	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the trust mode of port 1/0/1 as dot1p, map 802.1p priority 3 to TC4, and configure to map the original 802.1p 1 to 802.1p priority 3:

Switch#configure

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

Switch(config-if)#qos trust mode dot1p

Switch(config-if)#exit

Switch(config)#qos cos-map 3 4

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

Switch(config-if)#qos dot1p-remap 1 3

Switch(config-if)#show qos trust-mode interface gigabitEthernet 1/0/1

```
Port        Trust Mode      LAG
--------    ---------       --------
Gi1/0/1     trust 802.1P    N/A
```

Switch(config-if)#show qos cos-map

```
-----+-----+-----+-----+-----+-----+-----+----+----
Tag |0    |1    |2    |3    |4    |5    |6   |7
-----+-----+-----+-----+-----+-----+-----+----+----
TC  |TC0 |TC1 |TC2 |TC4 |TC4 |TC5 |TC6 |TC7
-----+-----+-----+-----+-----+-----+-----+----+----
```

Switch(config-if)#show qos dot1p-remap interface gigabitEthernet 1/0/1

```
Port        0   1   2   3   4   5   6   7   LAG
-----       ----- ----- ----- ----- ----- ----- ----- ----- -----
```

Gi1/0/1 0 **3** 2 3 4 5 6 7 N/A

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.3 Configuring DSCP Priority

■ Configuring the Trust Mode

Follow these steps to configure the trust mode:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** port **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Enter interface configuration mode.
Step 3	**qos trust mode** *dscp* Specify the trust mode of the port as dscp. In this mode, IP packets will be processed according to the DSCP priority configuration, and other packets will be processed according to the port priority configuration.
Step 4	**show qos trust-mode interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]** Verify the trust mode of the ports.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

■ Configuring the 802.1P to Queue Mapping

Follow these steps to configure the 802.1p to queue mapping:

Step 1	**configure** Enter global configuration mode.
Step 2	**qos cos-map {***dot1p-priority***} {***tc-queue***}** Specify the 802.1p to queue mapping. The packets with the desired 802.1p priority will be put in the corresponding queues. By default, the 802.1p priority 0 to 7 is respectively mapped to TC-1, TC-0, TC-2, TC-3, TC-4, TC-5, TC-6, TC-7. *dot1p-priority*: Specify the 802.1p priority. The valid values are from 0 to 7. *tc-queue*: Specify the ID number of the TC queue. The valid values are from 0 to 7.

Step 3	**show qos cos-map** Verify the 802.1p to queue mappings.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

Configuring the DSCP to 802.1P Mapping and DSCP Remap

Follow these steps to configure the DSCP to 802.1p mapping and DSCP remap:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Enter interface configuration mode.
Step 3	**qos dscp-map {***dscp-value-list***} {***dot1p-priority***}** Specify the DSCP to 802.1p mapping. The ingress packets with the desired DSCP priority are first mapped to 802.1p priority based on the DSCP to 802.1p mapping, then to TC queues based on the 802.1p to queue mapping. The untagged packets with the desired DSCP priority will be added an 802.1p priority value according to the DSCP to 802.1p mapping. By default, the DSCP priorities 0-7 are mapped to the 802.1p priority 0, the DSCP priorities 8-15 are mapped to the 802.1p priority 1 and so on. *dscp-value-list:* Specify the DSCP value list in the format of "1-3,5,7". The valid values are from 0 to 63. *dot1p-priority:* Specify the 802.1p priority. The valid values are from 0 to 7.
Step 4	**qos dscp-remap {***dscp-value-list***} {***dscp-remap-value***}** (Optional) Specify the DSCP to DSCP mappings for the ports. DSCP Remap is used to modify the DSCP priority of the ingress packets. When the switch detects the packets with the desired DSCP priority, it will modify the value of DSCP priority according to the map. By default, the original DSCP priority 0 is mapped to the DSCP priority 0, the original DSCP priority 1 is mapped to the DSCP priority 1 and so on. *dscp-value-list*: Specify the original DSCP priority list in the format of "1-3,5,7". The valid values are from 0 to 63. *dscp-remap-value*: Specify the new DSCP priority. The valid values are from 0 to 63.
Step 5	**show qos dscp-map interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]** Verify the DSCP to queue mappings.

Step 6	**show qos dscp-remap interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]** Verify the DSCP to DSCP remappings of the ports.
Step 7	**end** Return to privileged EXEC mode.
Step 8	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the trust mode of port 1/0/1 as dscp, map 802.1p priority 3 to TC4, map DSCP priority 1-3,5,7 to 802.1p priority 3, and configure to map the original DSCP priority 9 to DSCP priority 5:

Switch#configure

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

Switch(config-if)#qos trust mode dscp

Switch(config-if)#exit

Switch(config)#qos cos-map 3 4

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

Switch(config-if)#qos dscp-map 1-3,5,7 3

Switch(config-if)#qos dscp-remap 9 5

Switch(config-if)#show qos trust-mode interface gigabitEthernet 1/0/1

Port Trust Mode LAG

-------- --------- ------

Gi1/0/1 trust DSCP N/A

Switch(config-if)#show qos cos-map

-----+-----+-----+-----+-----+-----+-----+----+----

Tag |0 |1 |2 |**3** |4 |5 |6 |7

-----+-----+-----+-----+-----+-----+-----+----+----

TC |TC0 |TC1 |TC2 |**TC4** |TC4 |TC5 |TC6 |TC7

-----+-----+-----+-----+-----+-----+-----+----+----

Switch(config-if)#show qos dscp-map interface gigabitEthernet 1/0/1

Gi1/0/1----LAG: N/A

DSCP: 0 **1** **2** **3** 4 **5** 6 **7**

DSCP to 802.1P 0 **3** **3** **3** 0 **3** 0 **3**

---- ---- ---- ---- ---- ---- ---- ----

DSCP: 8 9 10 11 12 13 14 15

DSCP to 802.1P 1 1 1 1 1 1 1 1

---- ---- ---- ---- ---- ---- ---- ----

DSCP: 16 17 18 19 20 21 22 23

DSCP to 802.1P 2 2 2 2 2 2 2 2

---- ---- ---- ---- ---- ---- ---- ----

DSCP: 24 25 26 27 28 29 30 31

DSCP to 802.1P 3 3 3 3 3 3 3 3

---- ---- ---- ---- ---- ---- ---- ----

DSCP: 32 33 34 35 36 37 38 39

DSCP to 802.1P 4 4 4 4 4 4 4 4

---- ---- ---- ---- ---- ---- ---- ----

DSCP: 40 41 42 43 44 45 46 47

DSCP to 802.1P 5 5 5 5 5 5 5 5

---- ---- ---- ---- ---- ---- ---- ---

DSCP: 48 49 50 51 52 53 54 55

DSCP to 802.1P 6 6 6 6 6 6 6 6

---- ---- ---- ---- ---- ---- ---- ----

DSCP: 56 57 58 59 60 61 62 63

DSCP to 802.1P 7 7 7 7 7 7 7 7

---- ---- ---- ---- ---- ---- ---- ---

Switch(config-if)#show qos dscp-remap interface gigabitEthernet 1/0/1

Gi1/0/1----LAG: N/A

DSCP: 0 1 2 3 4 5 6 7

DSCP remap value 0 1 2 3 4 5 6 7

---- ---- ---- ---- ---- ---- ---- ----

DSCP: 8 **9** 10 11 12 13 14 15

DSCP remap value 8 **5** 10 11 12 13 14 15

	----	----	----	----	----	----	----	----
DSCP:	16	17	18	19	20	21	22	23
DSCP remap value	16	17	18	19	20	21	22	23
	----	----	----	----	----	----	----	----
DSCP:	24	25	26	27	28	29	30	31
DSCP remap value	24	25	26	27	28	29	30	31
	----	----	----	----	----	----	----	----
DSCP:	32	33	34	35	36	37	38	39
DSCP remap value	32	33	34	35	36	37	38	39
	----	----	----	----	----	----	----	----
DSCP:	40	41	42	43	44	45	46	47
DSCP remap value	40	41	42	43	44	45	46	47
	----	----	----	----	----	----	----	----
DSCP:	48	49	50	51	52	53	54	55
DSCP remap value	48	49	50	51	52	53	54	55
	----	----	----	----	----	----	----	----
DSCP:	56	57	58	59	60	61	62	63
DSCP remap value	56	57	58	59	60	61	62	63
	----	----	----	----	----	----	----	----

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.4 Configuring Schedule Mode

Follow these steps to configure the schedule mode to control the forwarding sequence of different TC queues when congestion occurs.

Step 1	**configure** Enter global configuration mode.

Step 2 **qos queue mode {**sp **|** wrr **|** spwrr **|** equ**}**

Configure the schedule mode of TC queues.

sp: The Strick Priority mode. In SP mode, the queue with higher priority will occupy the whole bandwidth. Packets in the queue with lower priority are sent only when the queue with higher priority is empty.

wrr: In WRR mode, packets in all the queues are sent in order based on the weight value for each queue. By default, the weight value ratio of TC0 to TC7 is 1:2:4:...:127.

spwrr: In SP+WRR mode, this switch provides two scheduling groups, SP group and WRR group. When scheduling queues, the switch allows the queues in the SP group to occupy the whole bandwidth following the SP mode. When the SP group is empty, the queues in the WRR group will take up the bandwidth according to their weight value ratio. By default, queue TC7 is in SP and TC0, TC1...TC6 are in WRR group.

equ: In Equ mode, all the queues occupy the bandwidth equally. The weight value ratio of all the queues is 1:1:1:1. It is the default schedule mode.

Step 3 **qos queue weight** { *tc-id* } { *weight-value* }

(Optional) Configure the weight value of each queue after the Schedule Mode is specified as WRR or SP+WRR.

tc-id: Specify the TC-ID. The valid values are from 0 to 7.

weight-value: Configure the weight value of the specified TC queue.

When the schedule mode is specified as WRR, the valid weight value are from 1 to 127. The 8 queues will take up the bandwidth according to their ratio. The default values of TC0, TC1, TC2, TC3, TC4, TC5,TC6 and TC7 are 1, 2, 4, 8, 16, 32, 64 and 127 respectively.

When the schedule mode is specified as SP+WRR, The valid weight values are from 0 to 127. TC7 and the queue with its weight value set as 0 are in the SP group; other queues, with none-zero weight value, belong to the WRR group. In this SP+WRR scheduling mode, the queues in the SP group is scheduled preferentially (TC6>TC5>TC4>TC3>TC2>TC1>TC0 in strict priority). When there is no packets to be sent in the SP group, the queues in the WRR group will be scheduled according to the weight value of each queue. The default weight values of TC0, TC1, TC2, TC3, TC4, TC5 and TC6 are 1, 2, 4, 8, 16, 32 and 64 respectively, while the value of TC7 is 0 and non-configurable.

Step 4 **show qos queue mode**

Verify the schedule mode configurations.

Step 5 **end**

Return to privileged EXEC mode.

Step 6 **copy running-config startup-config**

Save the settings in the configuration file.

Note:

With ACL Redirect feature, the switch maps all the packets that meet the configured ACL rules to the new TC queue, regardless of the mapping relations configured in this section.

The following example shows how to configure the schedule mode as WRR, with the weight values of TC0 to TC7 as 4, 7, 10, 13,16,19,22,25:

Switch#configure

Switch(config)#qos queue mode wrr

Switch(config)#qos queue weight 0 4

Switch(config)#qos queue weight 1 7

Switch(config)#qos queue weight 2 10

Switch(config)#qos queue weight 3 13

Switch(config)#qos queue weight 4 16

Switch(config)#qos queue weight 5 19

Switch(config)#qos queue weight 6 22

Switch(config)#qos queue weight 7 25

Switch(config)#show qos queue mode

----------+----------

Schedule Mode: WRR | Weight: TC0=4 TC1=7 TC2=10 TC3=13 TC4=16 TC5=19 TC6=22 TC7=25

----------+----------

Switch(config)#end

Switch#copy running-config startup-config

3 Bandwidth Control Configuration

To implement bandwidth control, you can:

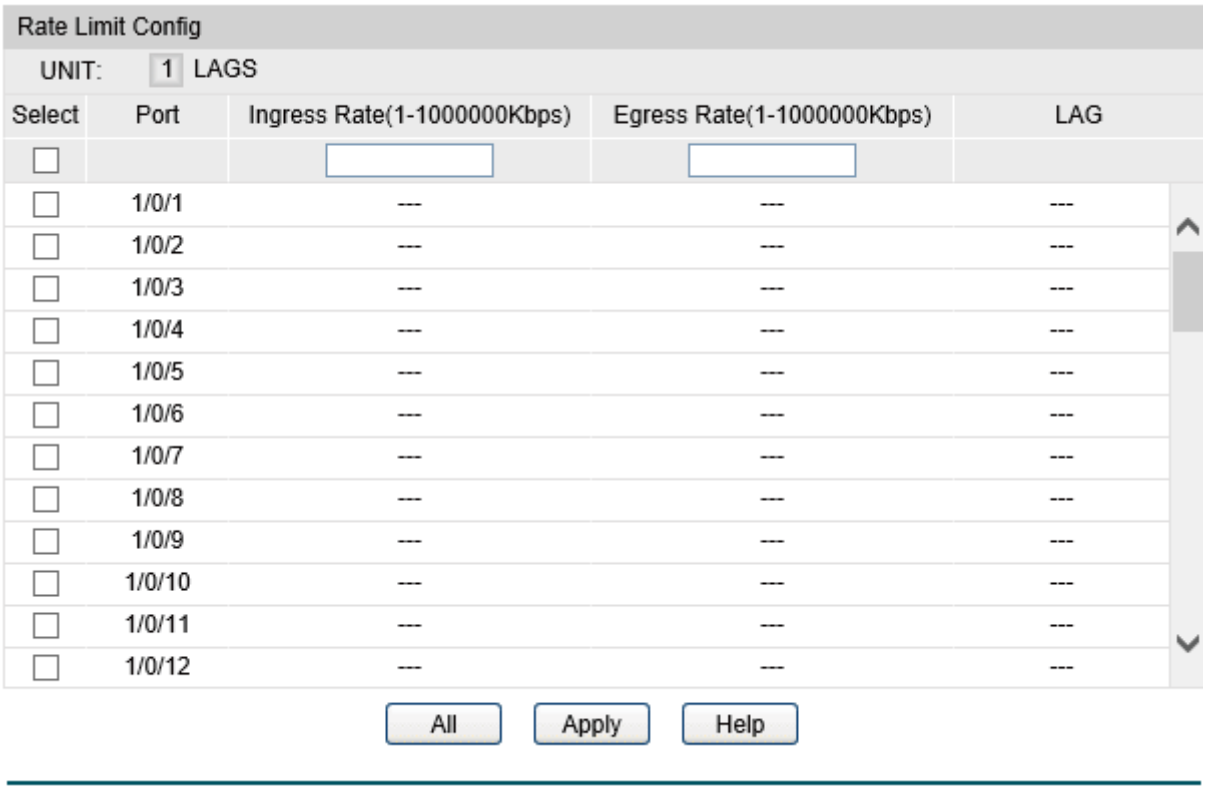
- Limit the ingress/egress traffic rate on each port by configuring the Rate Limit function;
- Limit the broadcast, multicast and UL frame forwarding rate on each port to avoid network broadcast storm by configuring the Storm Control function.

3.1 Using the GUI

3.1.1 Configuring Rate Limit

Choose the menu **QoS > Bandwidth Control > Rate Limit** to load the following page.

Figure 3-1 Rate Limit



Follow these steps to configure the Rate Limit function:

1) Configure the upper rate limit for the port to receive and send packets.

Ingress Rate (1-1000000Kbps)	Configure the upper rate limit for receiving packets on the port. The valid values are from 1 to 1000000 Kbps.

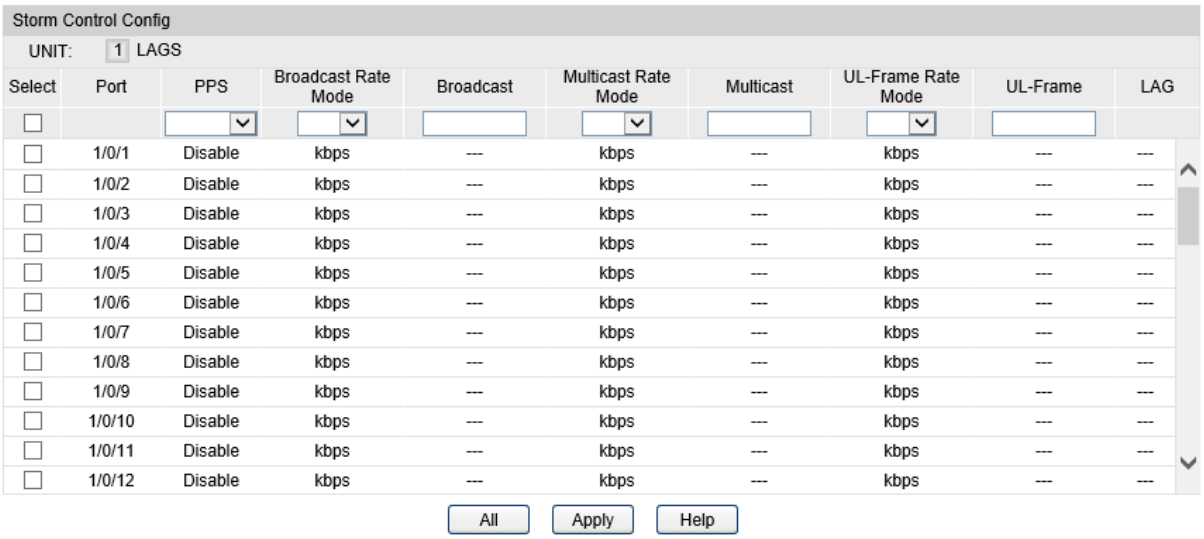
Egress Rate (1-1000000Kbps)	Configure the bandwidth for sending packets on the port. The valid values are from 1 to 1000000 Kbps.
LAG	Displays the aggregation group which the port is in.

2) Click **Apply**.

3.1.2 Configuring Storm Control

Choose the menu **QoS > Bandwidth Control > Storm Control** to load the following page.

Figure 3-2 Storm Control



Follow these steps to configure the Storm Control function:

1) Select the port(s) and configure the upper rate limit for forwarding broadcast packets, multicast packets and UL frames.

PPS	Enable or disable the PPS (Packets Per Second) mode on the port. With PPS enabled, the upper rate limit of the broadcast, multicast and UL-frame can only be specified in packets per second. With PPS disabled, the upper rate limit of the broadcast, multicast and UL-frame cannot be specified in packets per second.

Broadcast Rate Mode / Broadcast	To enable the broadcast rate control, select a broadcast rate mode and specify the upper rate limit for receiving broadcast packets in the **Broadcast** field. The packet traffic exceeding the rate will be discarded. The switch supports the following three rate modes: **kbps:** Specify the upper rate limit in kilo-bits per second, which ranges from 1 to 1000000 kbps. This mode is invalid if **PPS** is enabled. **ratio:** Specify the upper rate limit as a percentage of the bandwidth, which ranges from 1 to 100 percent. This mode is invalid if **PPS** is enabled. **pps:** Specify the upper rate limit in packets per second, which ranges from 1 to 1488000 packets per second. This mode is invalid if **PPS** is disabled. To disable the broadcast rate control, select **Disable** in the **Broadcast** field.
Multicast Rate Mode / Multicast	To enable the multicast rate control, select a multicast rate mode and specify the upper rate limit for receiving broadcast packets in the **Multicast** field. The packet traffic exceeding the rate will be discarded. The switch supports the following three rate modes: **kbps:** Specify the upper rate limit in kilo-bits per second, which ranges from 1 to 1000000 kbps. This mode is invalid if **PPS** is enabled. **ratio:** Specify the upper rate limit as a percentage of the bandwidth, which ranges from 1 to 100 percent. This mode is invalid if **PPS** is enabled. **pps:** Specify the upper rate limit in packets per second, which ranges from 1 to 1488000 packets per second. This mode is invalid if **PPS** is disabled. To disable the multicast rate control, select **Disable** in the **Multicast** field.
UL-Frame Rate Mode / UL-Frame	To enable the UL-Frame (Unknown unicast frame) rate control, select a UL-Frame rate mode and specify the upper rate limit for receiving UL-Frames in the **UL-Frame** field. The packet traffic exceeding the rate will be discarded. The switch supports the following three rate modes: **kbps:** Specify the upper rate limit in kilo-bits per second, which ranges from 1 to 1000000 kbps. This mode is invalid if **PPS** is enabled. **ratio:** Specify the upper rate limit as a percentage of the bandwidth, which ranges from 1 to 100 percent. This mode is invalid if **PPS** is enabled. **pps:** Specify the upper rate limit in packets per second, which ranges from 1 to 1488000 packets per second. This mode is invalid if **PPS** is disabled. To disable the UL-Frame rate control, select **Disable** in the **UL-Frame** field.
LAG	Displays the aggregation group which the port is in.

2) Click **Apply**.

Note:

- For ports in the same LAG, rate limit / storm control should be set to the same value to ensure a successful port aggregation.
- For one port, you cannot enable the Storm Control and the Rate limit at the same time.

3.2 Using the CLI

3.2.1 Configuring Rate Limit on Port

Configure the upper rate limit for the port to receive and send packets.

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *lag-id* **| range port-channel** *lag-list* **}** Enter interface configuration mode. *port* |*port-list*: The number or the list of the Ethernet port that you want to configure. *lag-id* |*lag-list:* The ID or the list of the LAG that you want to configure.
Step 3	**bandwidth {[ingress** *ingress-rate*] **[egress** *egress-rate*]**}** Configure the upper rate limit for the port to receive and send packets. *ingress-rate:* Configure the upper rate limit for receiving packets on the port. The valid values are from 1 to 1000000 Kbps. *egress-rate:* Configure the upper rate limit for sending packets on the port. The valid values are from 1 to 1000000 Kbps.
Step 4	**show bandwidth {interface [fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *lag-id* **| range port-channel** *lag-list* **]}** Verify the ingress/egress rate limit for forwarding packets on the port or LAG. If no port or LAG is specified, it displays the upper ingress/egress rate limit for all ports or LAGs.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the ingress-rate as 5120 Kbps and egress-rate as 1024 Kbps for port 1/0/5:

Switch#configure

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

Switch(config-if)#bandwidth ingress 5120 **egress** 1024

Switch(config-if)#show bandwidth interface gigabitEthernet 1/0/5

Port	IngressRate(Kbps)	EgressRate(Kbps)	LAG
---	---	---	---
Gi1/0/5	5120	1024	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

3.2.2 Configuring Storm Control

Configure the upper rate limit on the port for forwarding broadcast packets, multicast packets and unknown unicast frames.

Step 1	**configure** Enter global configuration mode
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *lag-id* **| range port-channel** *lag-list* **}** Enter interface configuration mode. *port* |*port-list*: The number or the list of the Ethernet port that you want to configure. *lag-id* |*lag-list:* The ID or the list of the LAG that you want to configure.

Step 3 Use the following commands to specify the upper rate limit of the broadcast packets, multicast packets and unknown unicast frames in pps:

storm-control pps

Configure the storm control mode as pps (packets per second) on the port. In PPS mode, the upper rate limit of the broadcast packets, multicast packets and unknown unicast frames can only be specified in packets per second.

storm-control {broadcast | multicast | unicast**} pps** *rate*

broadcast | multicast | unicast: Enable broadcast rate limit, multicast rate limit or unknown unicast rate limit on the port.

rate: Specify the upper rate limit for receiving broadcast packets, multicast packets and unknown unicast frames on the port. The packet traffic exceeding the rate will be discarded. The valid rate values are from 1 to 1488000 packets per second.

Use the following commands to specify the upper rate limit of the broadcast packets, multicast packets and unknown unicast frames in kbps or ratio:

no storm-control pps

Ensure the pps mode is disabled on the port.

storm-control {broadcast | multicast | unicast**} {**kbps | ratio**}** *rate*

broadcast | multicast | unicast: Enable broadcast packets rate limit, multicast packets rate limit or unknown unicast frames rate limit on the port.

kbps: Configure the storm control mode as kbps. In this mode, the upper rate limit is specified in kilo-bits per second.

ratio: Configure the storm control mode as ratio. In this mode, the upper rate limit is specified as a percentage of the bandwidth.

rate: Specify the upper rate limit for receiving broadcast packets, multicast packets and unknown unicast frames on the port. The packet traffic exceeding the rate will be discarded. For kbps, the valid rate values are from 1 to 1000000 kbps; for ratio, the valid rate values are from 1 to 100 percent.

Step 4 **show storm-control {interface [fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *lag-id* **| range port-channel** *lag-list***]}**

Verify the storm control configurations of the port or LAG. If no port or LAG is specified, it displays the storm control configuration for all ports or LAGs.

Step 5 **end**

Return to privileged EXEC mode.

Step 6 **copy running-config startup-config**

Save the settings in the configuration file.

The following example shows how to configure the upper rate limit of broadcast packets as 148800 pps on port 1/0/5:

Switch#configure

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

Switch(config-if)#storm-control pps

Switch(config-if)#storm-control broadcast **pps** 148800

Switch(config-if)#show storm-control interface gigabitEthernet 1/0/5

Port	BcRate	Mcate	UlRate	LAG
Gi1/0/5	pps 148800	pps 0	pps 0	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

The following example shows how to configure the upper rate limit of broadcast packets as 10240 kbps on port 1/0/5:

Switch#configure

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

Switch(config-if)#no storm-control pps

Switch(config-if)#storm-control broadcast kbps 10240

Switch(config-if)#show storm-control interface gigabitEthernet 1/0/5

Port	BcRate	Mcate	UlRate	LAG
Gi1/0/5	kbps 10240	kbps 0	kbps 0	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

4 Configuration Examples

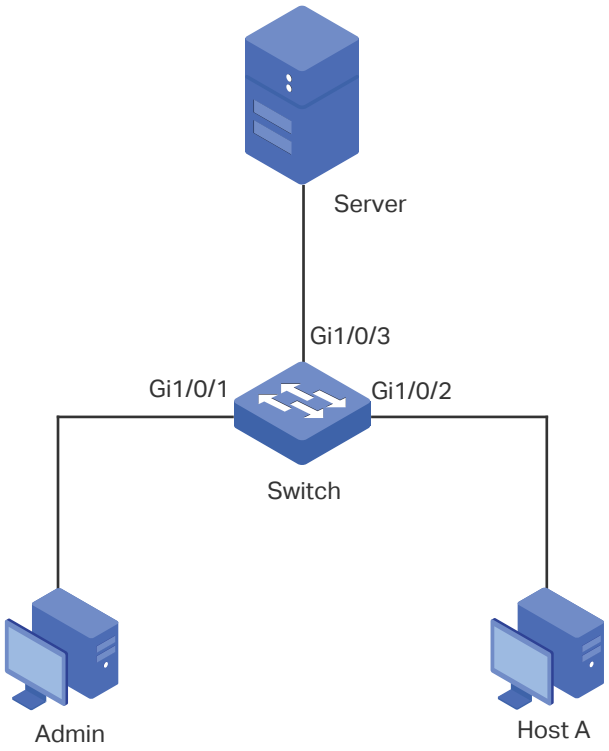
4.1 Example for Configuring SP Mode

4.1.1 Network Requirements

Two hosts, Admin and Host A, can access the local network server through the switch. Configure the switch to ensure the traffic from the Admin can be treated preferentially when congestion occurs. Only when the traffic from the Admin is completely forwarded will the traffic from Host A be forwarded.

The figure below shows the network topology.

Figure 4-1 QoS Application Topology



4.1.2 Configuration Scheme

The overview of the configuration is as follows:

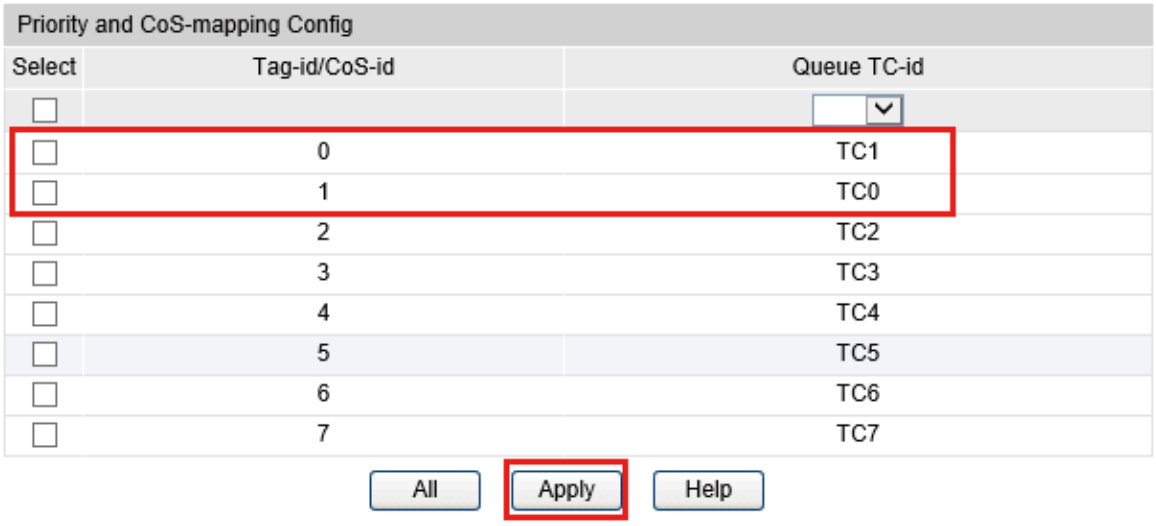
1) Configure the Port Priority for the two ports. Set Port 1/0/1 with higher priority.
2) Select SP schedule mode.

Demonstrated with T2600G-28TS, this chapter provides configuration procedures in two ways: using the GUI and using the CLI.

4.1.3 Using the GUI

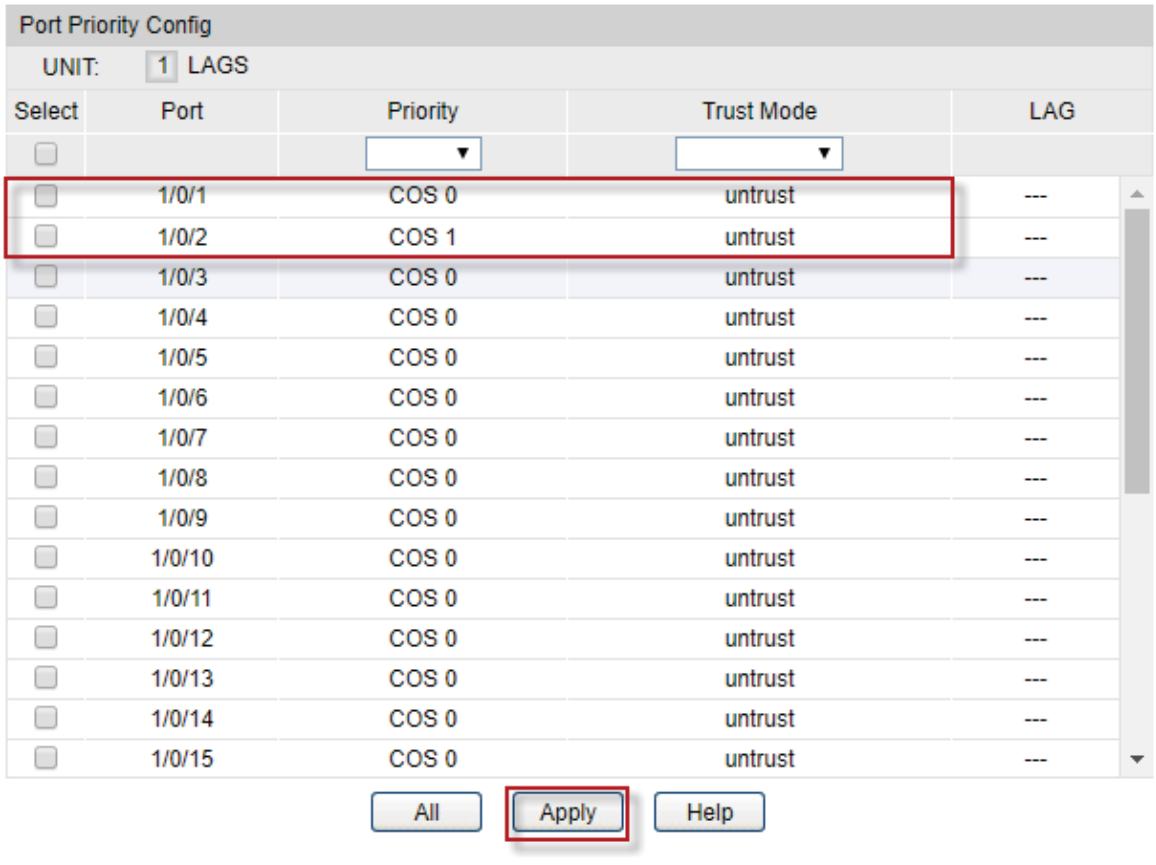
1) Choose **QoS > DiffServ > 802.1P Priority** to load the following page, and check the corresponding CoS-id of TC0 and TC1.

Figure 4-2 CoS-TC Mapping relations



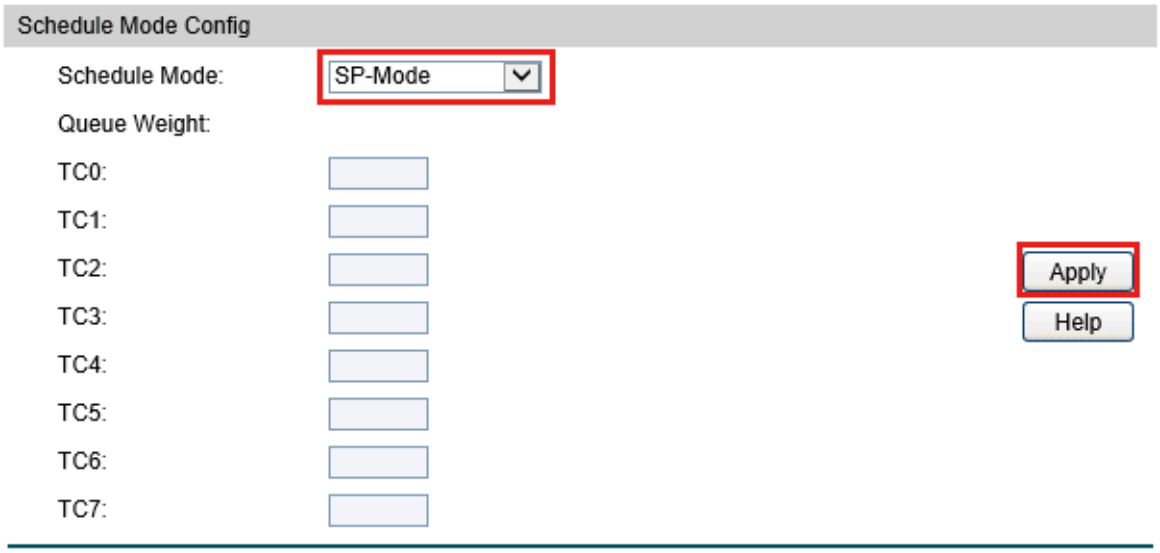
2) Choose **QoS > DiffServ > Port Priority** to load the following page, and set the priority for port 1/0/1 to CoS 0 (mapping to TC1) and priority for port 1/0/2 to CoS 1 (mapping to TC0). Set the **Trust Mode** as **untrust** for both port 1/0/1 and 1/0/2. Then click **Apply**.

Figure 4-3 Configure Port Priority



3) Choose **QoS > DiffServ > Schedule Mode** to load the following page, and select **SP-Mode** as the schedule mode. Click **Apply**.

Figure 4-4 Configure Schedule Mode



4.1.4 Using the CLI

1) Check the corresponding CoS-id of TC0 and TC1.

```
Switch#show qos cos-map
-----+-----+-----+----+-----+-----+-----+----+----
Tag |0    |1    |2   |3    |4    |5    |6   |7
-----+-----+-----+----+-----+-----+-----+----+----
TC  |TC1  |TC0  |TC2 |TC3  |TC4  |TC5  |TC6 |TC7
-----+-----+-----+----+-----+-----+-----+----+----
```

2) Set the priority for port 1/0/1 to CoS 0(mapping to TC1) and priority for port 1/0/2 to CoS 1(mapping to TC0). Set the trust-mode as untrust for both ports

```
Switch#configure
Switch(config)#interface gigabitEthernet 1/0/1
Switch(config-if)#qos port-priority 0
Switch(config-if)#qos tust mode untrust
Switch(config-if)#exit
Switch(config)#interface gigabitEthernet 1/0/2
Switch(config-if)#qos port-priority 1
Switch(config-if)#qos tust mode untrust
```

Switch(config-if)#exit

3) Select SP-Mode as the schedule mode and save the settings.

Switch(config)#qos queue mode sp

Switch(config)#exit

Switch#copy running-config startup-config

Verify the configuration

1) Verify the port-CoS mapping:

Switch(config)#show qos port-priority interface

Port	CoS Value	LAG
---	---	---
Gi1/0/1	0	N/A
Gi1/0/2	1	N/A

...

2) Verify the trust mode.

Switch(config)#show qos trust-mode interface

Port	Trust Mode	LAG
---	---	---
Gi1/0/1	untrust	N/A
Gi1/0/2	untrust	N/A

3) Verify the schedule mode.

Switch(config)#show qos queue mode

----------+----------

Scheduler Mode: SP | Weight: Unusable in sp mode.

----------+----------

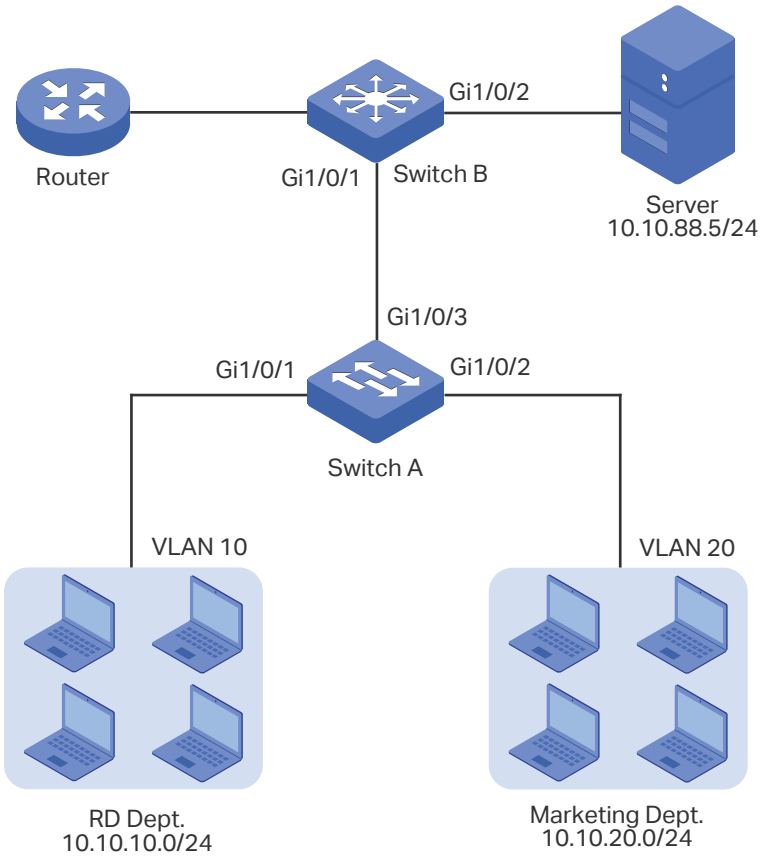
4.2 Example for Configuring WRR Mode

4.2.1 Network Requirements

Both RD department and Marketing department can access the local network server. Configure the switches to ensure the traffic from the two departments are forwarded based on the weight value ratio of 2:1 when congestion occurs.

The network topology is shown as the following figure. Switch A is an access layer switch, and Switch B is a layer 3 switch with ACL Redirect feature. RD department is connected to port 1/0/1 of Switch A. Marketing Department is connected to port 1/0/2 of Switch A, the server is connected to port 1/0/2 of Switch B and port 1/0/3 of Switch A is connected to port 1/0/1 of Switch B.

Figure 4-5 QoS Application Topology



4.2.2 Configuration Scheme

- Configure Switch A to add different VLAN tags to the packets from the two departments respectively.
- Configure Switch B to classify the incoming packets from the two departments according to the VLAN tags, and to map them into different TC queues. Configure the schedule mode as WRR-Mode to implement the QoS feature.

This chapter provides configuration procedures in two ways: using the GUI and using the CLI.

4.2.3 Using the GUI

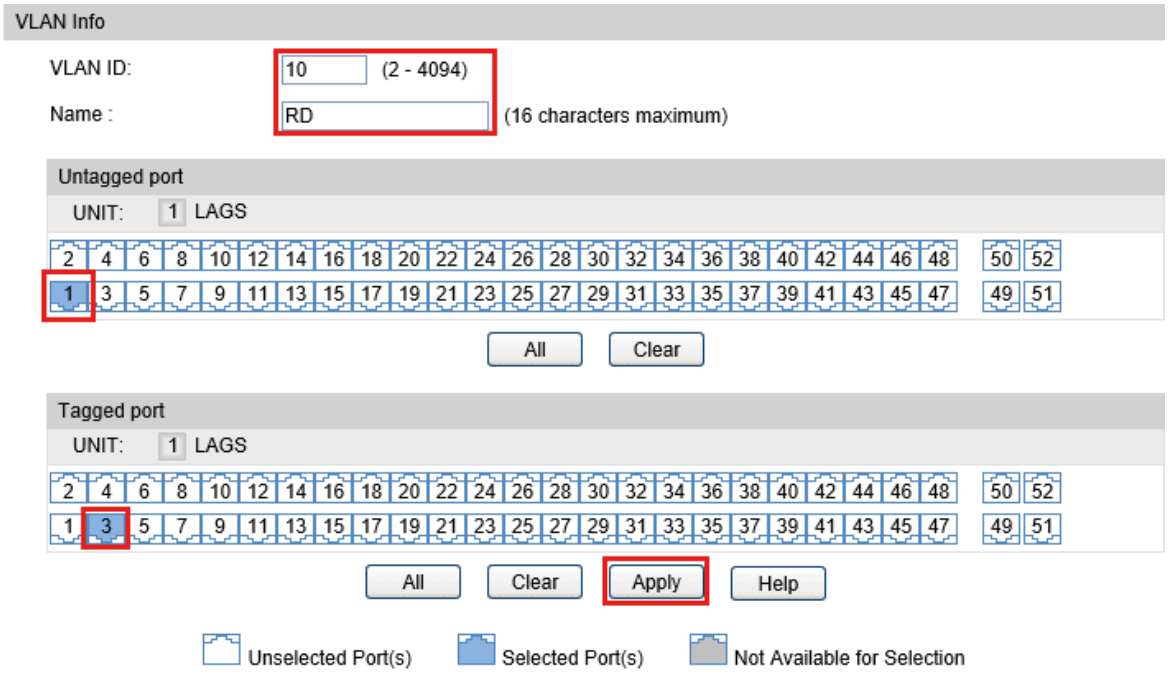
Note:

Before configuration, ensure network segments are reachable to each other.

- Configurations for Switch A (Demonstrated with T2600G-28TS)

1) Choose **VLAN > 802.1Q VLAN> VLAN Config**, and click **Create** to load the following page. Create VLAN 10 with the description of RD. Add port 1/0/1 as an untagged port and port 1/0/3 as a tagged port to VLAN 10. Then click **Apply**.

Figure 4-6 Configure VLAN 10



2) Click **Create** again to load the following page. Create VLAN 20 with the description of Marketing. Add port 1/0/2 as an untagged port and port 1/0/3 as a tagged port to VLAN 20. Then click **Apply**.

Figure 4-7 Configure VLAN 20

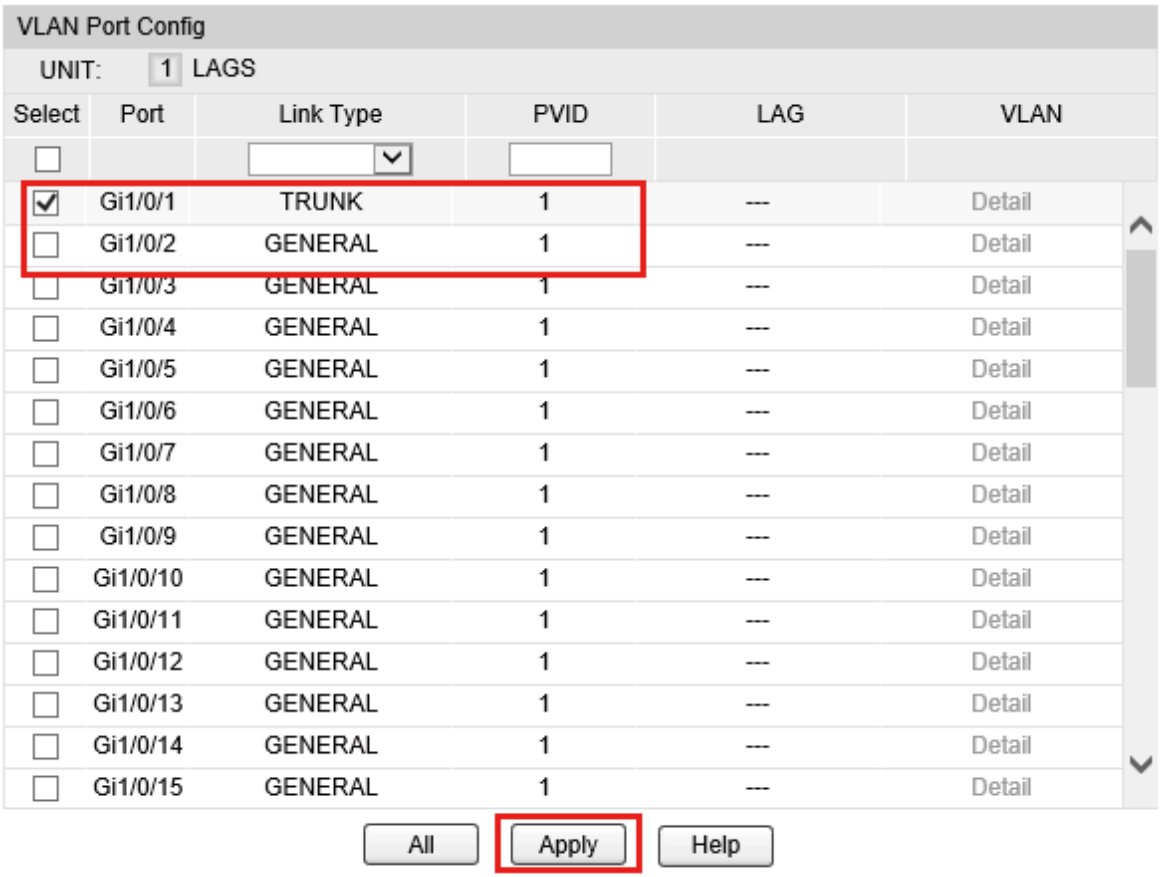


3) Click s**ave config** to save the settings.

- Configurations for Switch B (Demonstrated with T2600G-28TS)

1) Choose **VLAN > 802.1Q VLAN > Port Config** to load the following page. For port 1/0/1, set the Link Type as **TRUNK,** and for port 1/0/2, set the Link Type as **ACCESS**. Click **Apply**.

Figure 4-8 Configure the Port



2) Choose **VLAN > 802.1Q VLAN > VLAN Config** and click **Create** to load the following page. Create VLAN 10 and VLAN 20, and add port 1/0/1 to the two VLANs; create VLAN 30, and add port 1/0/2 to VLAN 30.

Figure 4-9 Configure VLAN 10

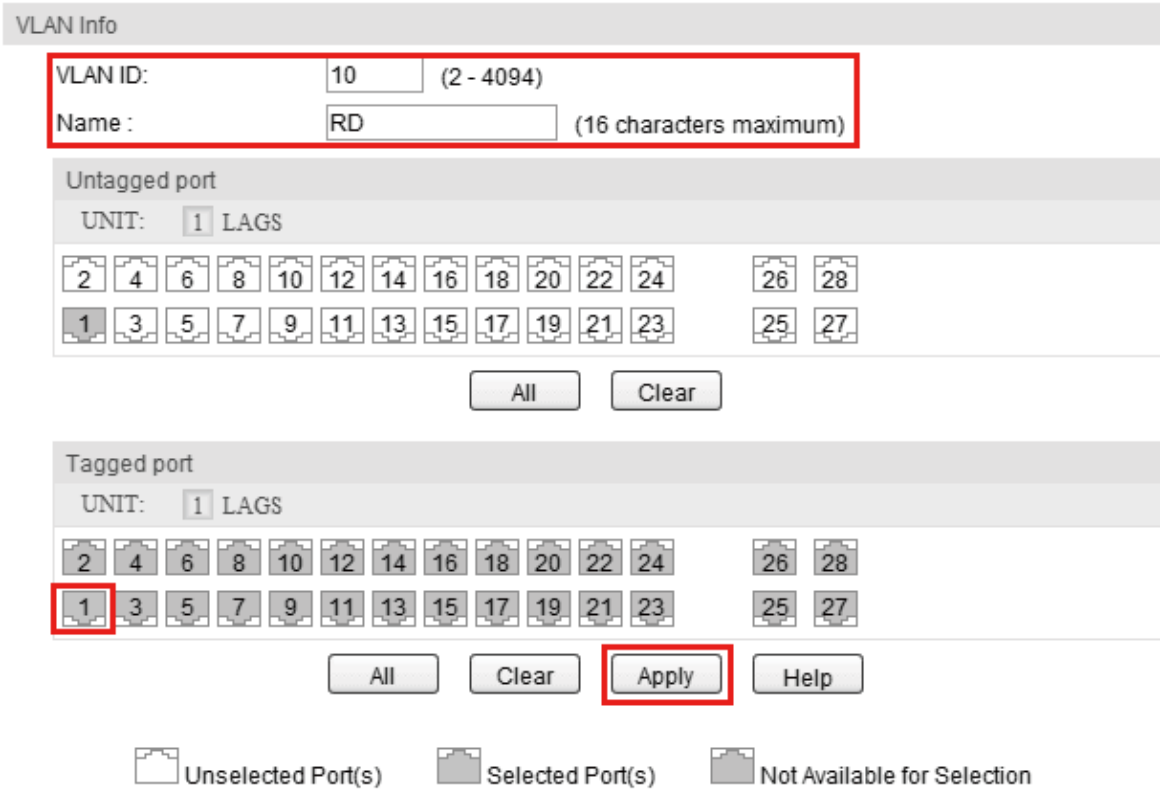


Figure 4-10 Configure VLAN 20

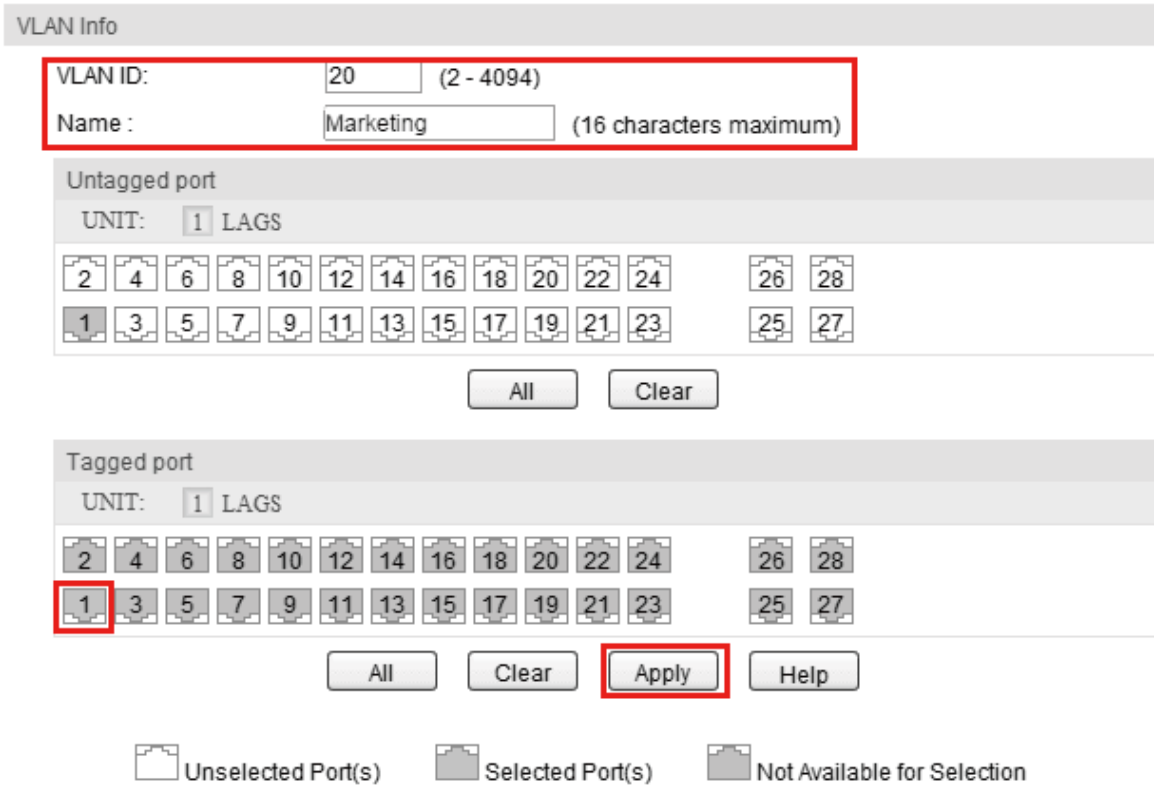
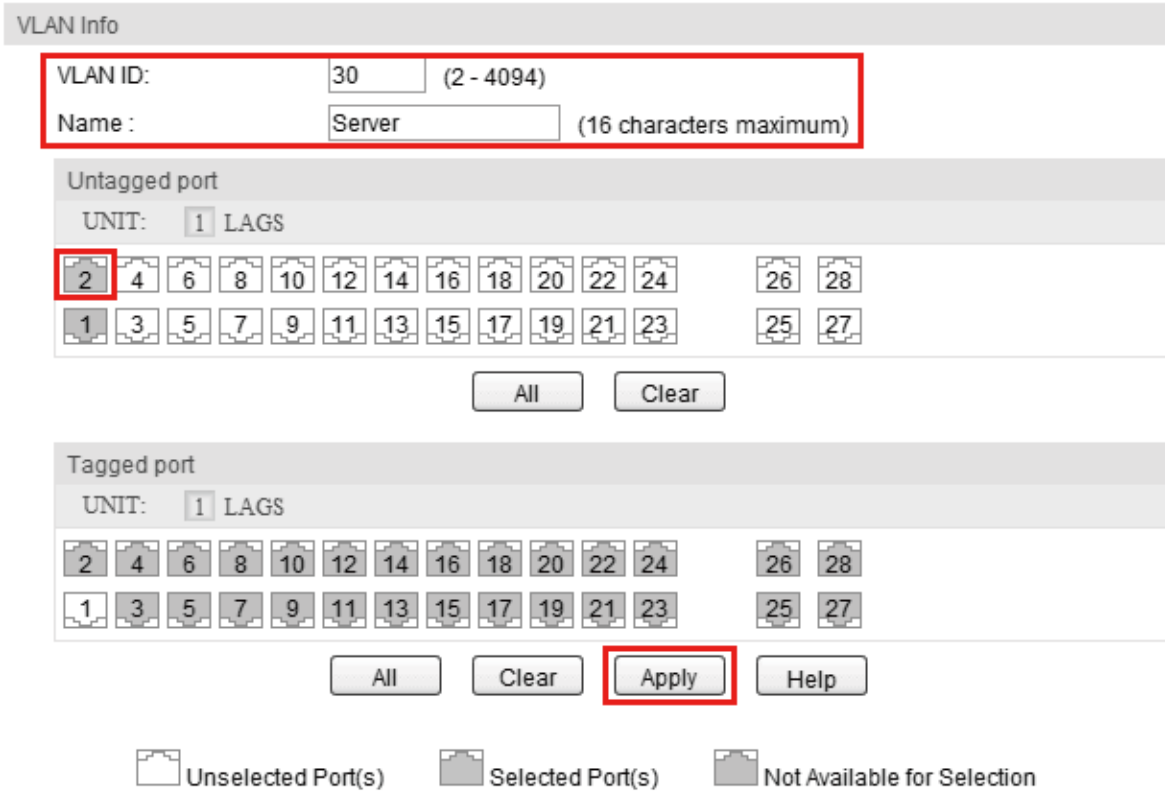


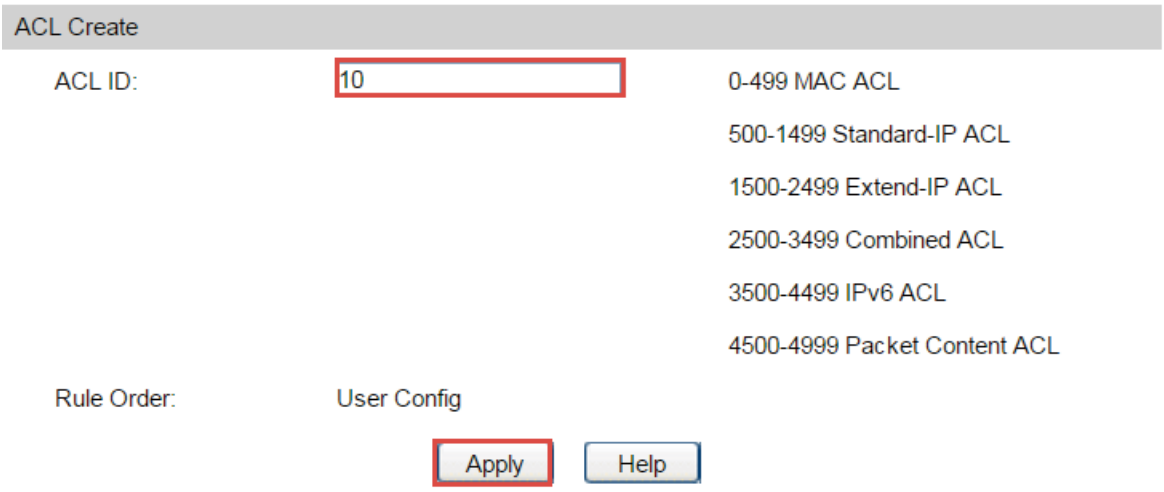
Figure 4-11 Configure VLAN30



3) Create MAC ACL 10 with its Rule ID as **1** and Operation as **Permit**.

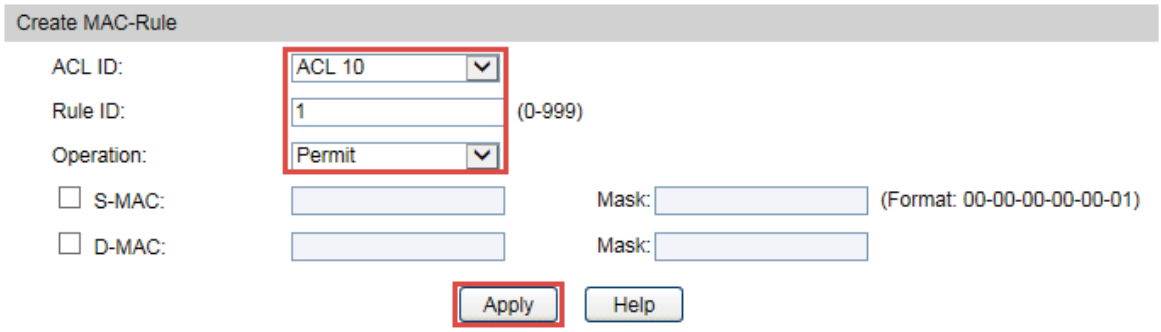
Choose **ACL> ACL Config > ACL Create** to load the following page. Create ACL 10, and click **Apply**.

Figure 4-12 Create MAC ACL 10



Choose **ACL> ACL Config > MAC ACL** to load the following page. Select ACL 10, specify the Rule ID as **1** and the Operation as **Permit**. Click **Apply**.

Figure 4-13 Create Rule 1



4) Create Policy RD and bind it to ACL 10, select **QoS Remark** and set Local Priority to **TC1**.

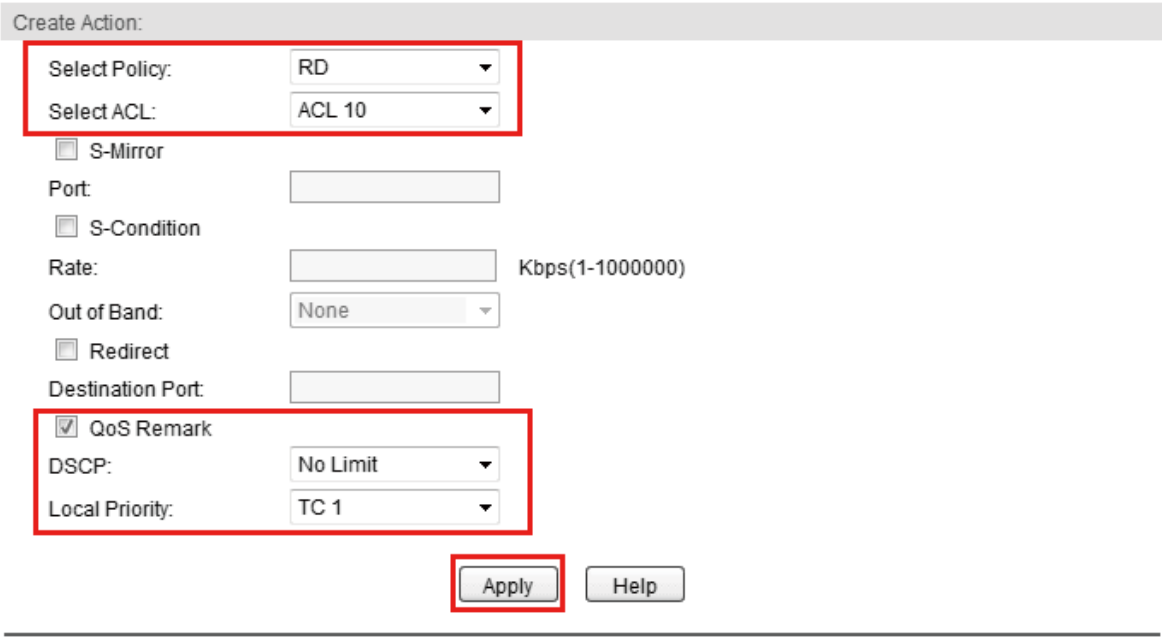
Choose **ACL > Policy Config > Policy Create** to load the following page. Create a policy with the Policy Name **RD** and click **Apply**.

Figure 4-14 Create Policy RD



Choose **ACL > Policy Config > Action Create** to load the following page. Select Policy RD, and ACL 10, click **QoS Remark** and set the Local Priority to **TC 1**. Click **Apply**.

Figure 4-15 Action Create



5) Create Policy Marketing and bind it to ACL 10, select **QoS Remark** and set Local Priority to **TC0**.

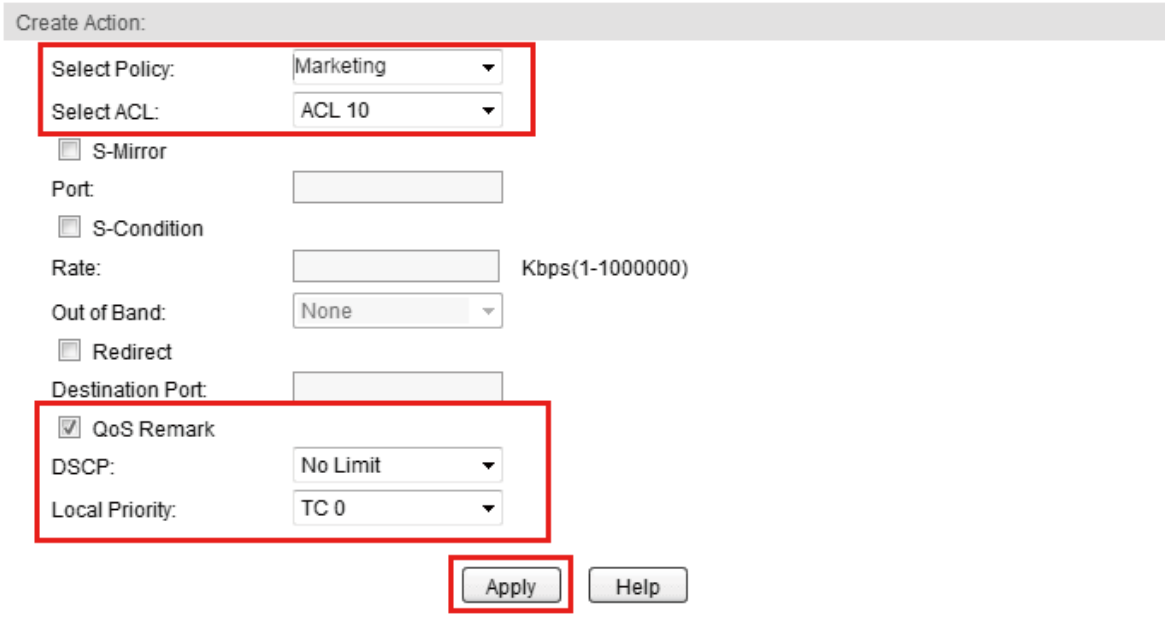
Choose **ACL > Policy Config > Policy Create** to load the following page. Create a policy with the Policy Name **Marketing** and click **Apply**.

Figure 4-16 Create Policy Marketing



Choose **ACL > Policy Config > Action Create** to load the following page. Select Policy Marketing, and ACL 10, click **QoS Remark** and set the Local Priority to **TC 0**. Click **Apply**.

Figure 4-17 Action Create



6) Choose **ACL > Policy Binding > VLAN Binding**. Bind Policy RD and Policy Marketing to VLAN10 and VLAN 20 respectively.

Figure 4-18 Bind Policy RD to VLAN 10

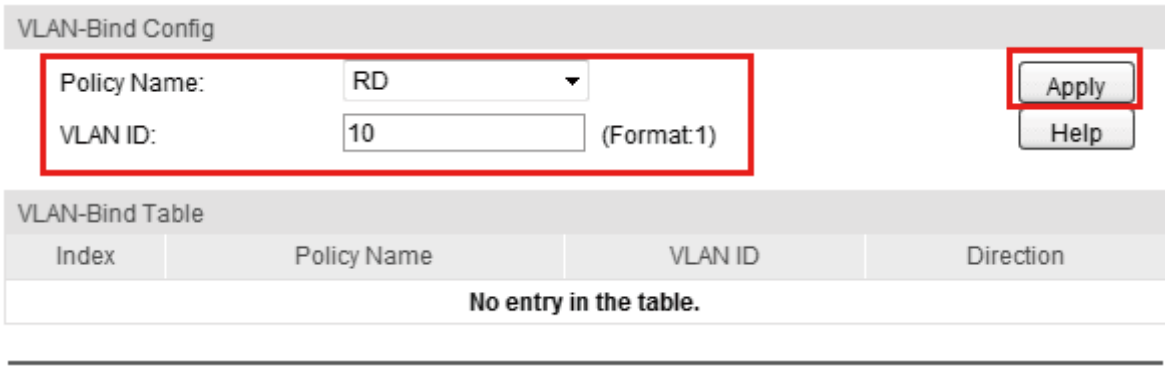
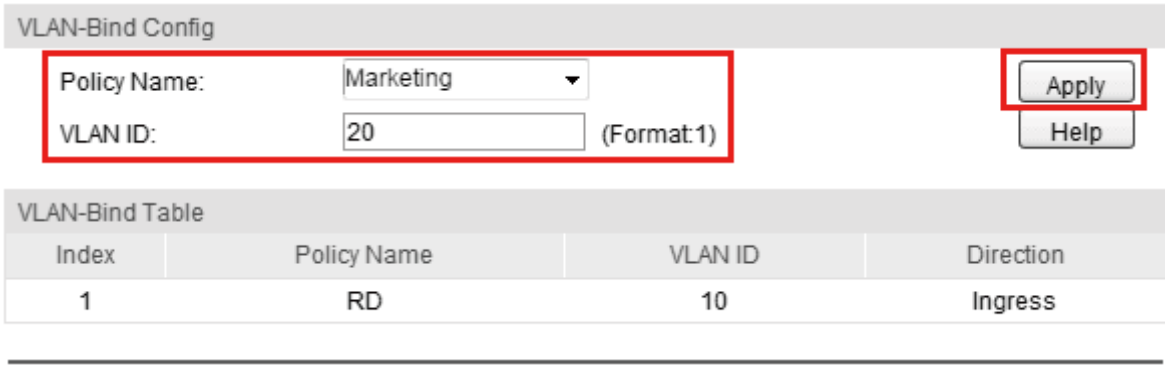


Figure 4-19 Bind Policy Marketing to VLAN 20



7) Choose **QoS > DiffServ > Schedule Mode**. Select **WRR-Mode** as the schedule mode, and click **Apply**. No configuration is required here because queues based on ACL rules have higher priority.

Figure 4-20 Configure Schedule Mode



8) Click **Save Config** to save the settings.

4.2.4 Using the CLI

Note:

Before configuration, ensure network segments are reachable to each other.

- Configurations for Switch A (Demonstrated with T1600G-52TS)

1) Create VLAN 10 with the name RD and VLAN 20 with the name Marketing.

```
Switch_A#configure
Switch_A(config)#vlan 10
Switch_A(config-vlan)#name RD
Switch_A(config-vlan)#exit
Switch_A(config)#vlan 20
Switch_A(config-vlan)#name Marketing
Switch_A(config-vlan)#exit
```

2) Set the port mode of port 1/0/1 and 1/0/2 as Untagged, and add them to VLAN 10 and VLAN 20 respectively. Set the port mode of port 1/0/3 and add it to both VLAN 10 and VLAN 20.

```
Switch_A(config)#interface gigabitEthernet 1/0/1
Switch_A(config-if)#switchport general allowed vlan 10 untagged
Switch_A(config-vlan)#exit
Switch_A(config)#interface gigabitEthernet 1/0/2
Switch_A(config-if)#switchport general allowed vlan 20 untagged
Switch_A(config-vlan)#exit
Switch_A(config)#interface gigabitEthernet 1/0/3
Switch_A(config-if)#switchport general allowed vlan 10,20  tagged
Switch_A(config-if)#end
Switch_A#copy running-config startup-config
```

- Configurations for For Switch B (Demonstrated with T2600G-28TS)

1) Create VLAN 10 and VLAN 20. Configure the Link Type of port 1/0/1 as **Trunk**, and add it to the two VLANs.

```
Switch_B#configure
Switch_B(config)#vlan 10
Switch_B(config-vlan)#name RD
Switch_B(config-vlan)exit
Switch_B(config)#vlan 20
Switch_B(config-vlan)#name Marketing
Switch_B(config-vlan)exit
Switch_B(config)#interface gigabitEthernet 1/0/1
Switch_B(config-if)#switchport mode trunk
Switch_B(config-if)#switchport trunk allowed vlan 10,20
Switch_B(config-if)#exit
```

2) Create VLAN 30. Configure the Link Type of port 1/0/2 as **Access**, and add it to VLAN 30.

```
Switch_B(config)#vlan 30
Switch_B(config-vlan)#name Server
Switch_B(config-vlan)exit
```

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

Switch_B(config-if)#switchport mode access

Switch_B(config-if)#switchport access vlan 30

Switch_B(config-if)#exit

3) Create MAC ACL 10 with its Rule ID as **1** and Operation as **Permit**.

Switch_B(config)#mac access-list 10

Switch_B(config-mac-acl)#rule 1 permit

Switch_B(config-mac-acl)#exit

4) Create Policy RD and bind it to ACL 10, enable **QoS Remark** and set Local Priority to **TC1**.

Switch_B(config)#access-list policy name RD

Switch_B(config)#access-list policy action RD 10

Switch_B(config-action)#qos-remark priority 1

Switch_B(config-action)#exit

5) Create Policy Marketing and bind it to ACL 10, enable **QoS Remark** and set Local Priority to **TC0**.

Switch_B(config)#access-list policy name Marketing

Switch_B(config)#access-list policy action Marketing 10

Switch_B(config-action)#qos-remark priority 0

Switch_B(config-action)#exit

6) Bind Policy RD and Policy Market to VLAN10 and VLAN 20 respectively.

Switch_B(config)#interface vlan 10

Switch_B(config-if)#access-list bind RD

Switch_B(config-if)#exit

Switch_B(config)#interface vlan 20

Switch_B(config-if)#access-list bind Marketing

Switch_B(config-if)#exit

7) Select **WRR-Mode** as the schedule mode and save the settings.

Switch_B(config)#qos queue mode wrr

Switch_B(config)#exit

Switch_B#copy running-config startup-config

Verify the configuration

- Switch A:

  Verify the VLAN members.

  Switch_B#show vlan

VLAN	Name	Status	Ports
1	System-VLAN	active	Gi1/0/3, Gi1/0/4, Gi1/0/5, Gi1/0/6, Gi1/0/7, Gi1/0/8, Gi1/0/9, Gi1/0/10, ... Gi1/0/49, Gi1/0/50, Gi1/0/51, Gi1/0/52
10	RD	active	Gi1/0/1, Gi1/0/3
20	Marketing	active	Gi1/0/2, Gi1/0/3

- Switch B:

  Verify ACL configuration:

  Switch_B#show access-list

  Mac access list 10

  1 permit

  Verify Policy and Action configuration:

  Switch_B(config)#show access-list policy

  Policy name : RD

  access-list 10 priority 1

  Policy name : Marketing

  access-list 10 priority 0

  Verify Policy binding:

  Switch_B#show access-list bind

Index	Policy Name	Interface/VID	Direction	Type
1	RD	10	Ingress	Vlan
2	Marketing	20	Ingress	Vlan

Verify the schedule mode.

```
Switch_B#show qos queue mode
----------------------+----------
Scheduler Mode | WRR
----------------------+----------
```

5 Appendix: Default Parameters

DiffServ

Table 5-1 DiffServ

Parameter	Default Setting
Port Priority	Enabled. Packets from all ports are mapped to the same TC queue.
802.1P Priority	Enabled. See Table 5-2 for Tag-id/CoS-id-TC mapping relations.
DSCP Priority	Disabled. See Table 5-3 for DSCP-CoS Mapping relations.
Schedule Mode	Equ-Mode.

Table 5-2 Tag-id/CoS-id-TC Mapping

Tag-id/CoS-id	TC Queues (8)
0	TC1
1	TC0
2	TC2
3	TC3
4	TC4
5	TC5
6	TC6
7	TC7

Table 5-3 DSCP-CoS Mapping

DSCP	CoS-id
0~7	CoS 0
8~15	CoS 1
16~23	CoS 2
24~31	CoS 3
32~39	CoS 4
40~47	CoS 5
48~55	CoS 6
56~63	CoS 7

Bandwidth Control

Table 5-4 Bandwidth Control

Parameter	Default Setting
Rate Limit	Disabled
Storm Control	Disabled

Part 23

Configuring Voice VLAN

CHAPTERS

1. Overview
2. Voice VLAN Configuration
3. Configuration Example
4. Appendix: Default Parameters

1 Overview

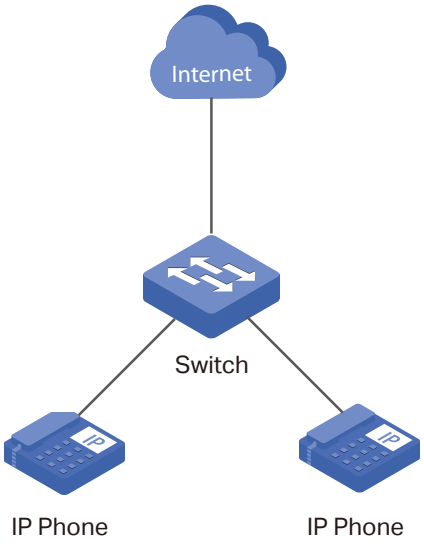
The voice VLAN feature is used to prioritize the transmission of voice traffic. Voice traffic is typically more time-sensitive than data traffic, and the voice quality can deteriorate a lot because of packet loss and delay. To ensure the high voice quality, you can configure the voice VLAN and set priority for voice traffic.

- Voice VLAN Modes on Ports

A voice VLAN can operate in two modes: manual mode and automatic mode.

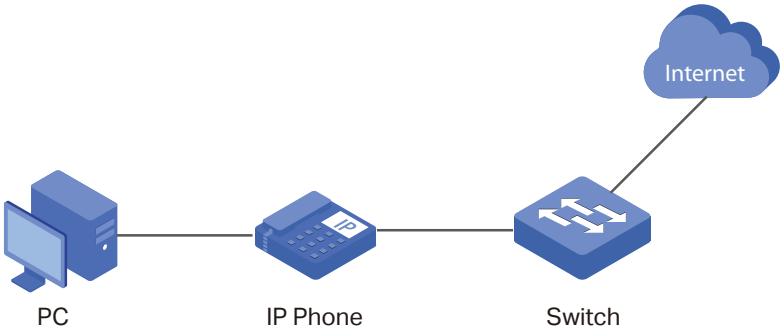
Manual mode: This mode is applicable when the switch port forwards voice traffic only. You manually add ports connecting IP phones to the voice VLAN; then the switch will apply priority rules to ensure the high priority of voice traffic.

Figure 1-1 Only Voice Traffic on One Port



Automatic mode: This mode is applicable when voice traffic and data traffic are transmitted on the same switch port. When a port receives a voice packet, the switch automatically adds the port to the voice VLAN and applies priority rules. The switch forwards voice traffic in the voice VLAN and data traffic in other VLANs.

Figure 1-2 Voice Traffic and Data Traffic on the Same Port



- OUI Address (Organizationally Unique Identifier Address)

The OUI address is used by the switch to determine whether a packet is a voice packet. An OUI address is the first 24 bits of a MAC address, and is assigned as a unique identifier by IEEE (Institute of Electrical and Electronics Engineers) to a device vendor. If the source MAC address of a packet complies with the OUI addresses in the switch, the switch identifies the packet as a voice packet and prioritizes it in transmission.

2 Voice VLAN Configuration

To complete the Voice VLAN configuration, follow these steps:

1) Create a VLAN.
2) Configure OUI addresses.
3) Configure Voice VLAN globally.
4) Configure Voice VLAN mode on ports.

Configuration Guidelines

- Before configuring voice VLAN, you need to create a VLAN for voice traffic. For details about VLAN Configuration, please refer to *Configuring 802.1Q VLAN*.
- VLAN 1 is a default VLAN and cannot be configured as the voice VLAN.
- Only one VLAN can be set as the voice VLAN on the switch.
- To apply the voice VLAN configuration, you may need to further configure PVID (Port VLAN ID) and the link type of the port which is connected to voice devices. We recommend that you choose the mode according to your needs and configure the port as the following table shows.

Table 2-1 Voice VLAN mode and Link Type of the Port

Traffic on One Port	Voice Traffic Type	Suggested Mode	Suggested Link Type and PVID
Voice traffic and data traffic	Tagged voice traffic	Automatic	PVID cannot be the voice VLAN ID.
	Untagged voice traffic		Not supported.
Voice traffic only	Tagged voice traffic	Manual	Tagged; PVID configuration is not required.
	Untagged voice traffic		Untagged; PVID should be the voice VLAN ID.

Because the voice VLAN in automatic mode supports only tagged voice traffic, you need to make sure traffic from the voice device is tagged. To do so, there are mainly two ways:

» You can configure the voice device to forward traffic with a voice VLAN tag.

» If your switch provides the LLDP-MED feature, you can also configure it to instruct the voice device to send tagged voice traffic. For details about LLDP-MED, please refer to *Configuring LLDP*.

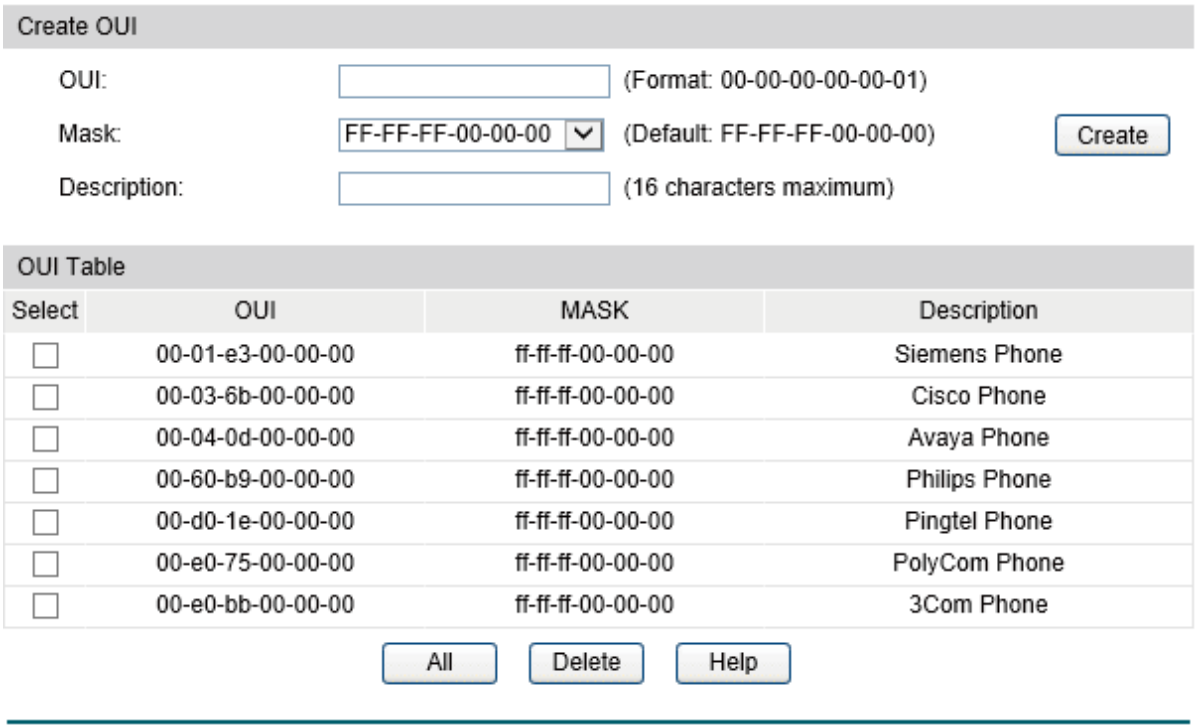
2.1 Using the GUI

2.1.1 Configuring OUI Addresses

If the OUI address of your voice device is not in the OUI table, you need to add the OUI address to the table.

Choose the menu **QoS > Voice VLAN > OUI Config** to load the following page.

Figure 2-1 Configuring OUI Addresses



Follow these steps to add OUI addresses:

1) Enter an OUI address and the corresponding mask, and give a description about the OUI address.

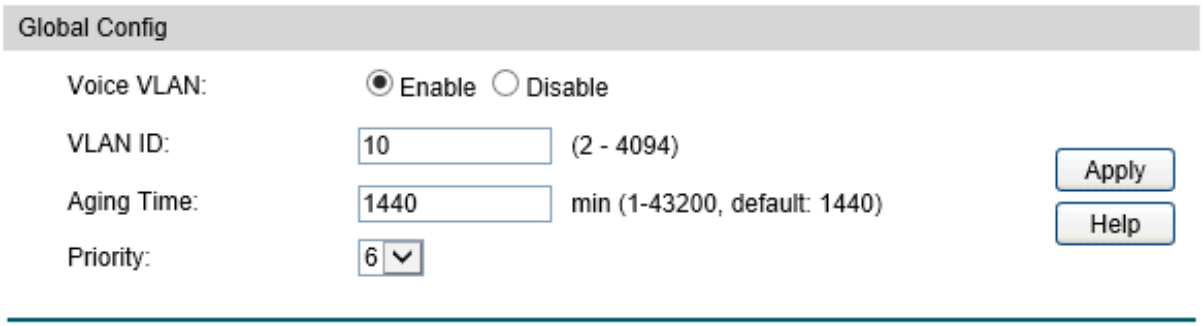
OUI	Enter the OUI address of your device.
Mask	Specify a mask to determine the depth of the OUI that the switch uses to check source addresses of received packets.
Description	Give an OUI address description for identification. The length is no more than 16 characters.

2) Click **Create** to add an OUI address to the table.

2.1.2 Configuring Voice VLAN Globally

Choose the menu **QoS > Voice VLAN > Global Config** to load the following page.

Figure 2-2 Configuring Voice VLAN Globally



Follow these steps to configure the voice VLAN globally:

1) Enable the voice VLAN feature, and enter a VLAN ID.

VLAN ID	Specify an existing VLAN as the voice VLAN.

2) Set the aging time for the voice VLAN.

Aging Time	Specify the length of time that a port remains in the voice VLAN after the port receives a voice packet. Aging time works only for ports in automatic voice VLAN mode. The range is 1 to 43200 minutes; the default is 1440 minutes.

3) Specify a priority for the voice VLAN.

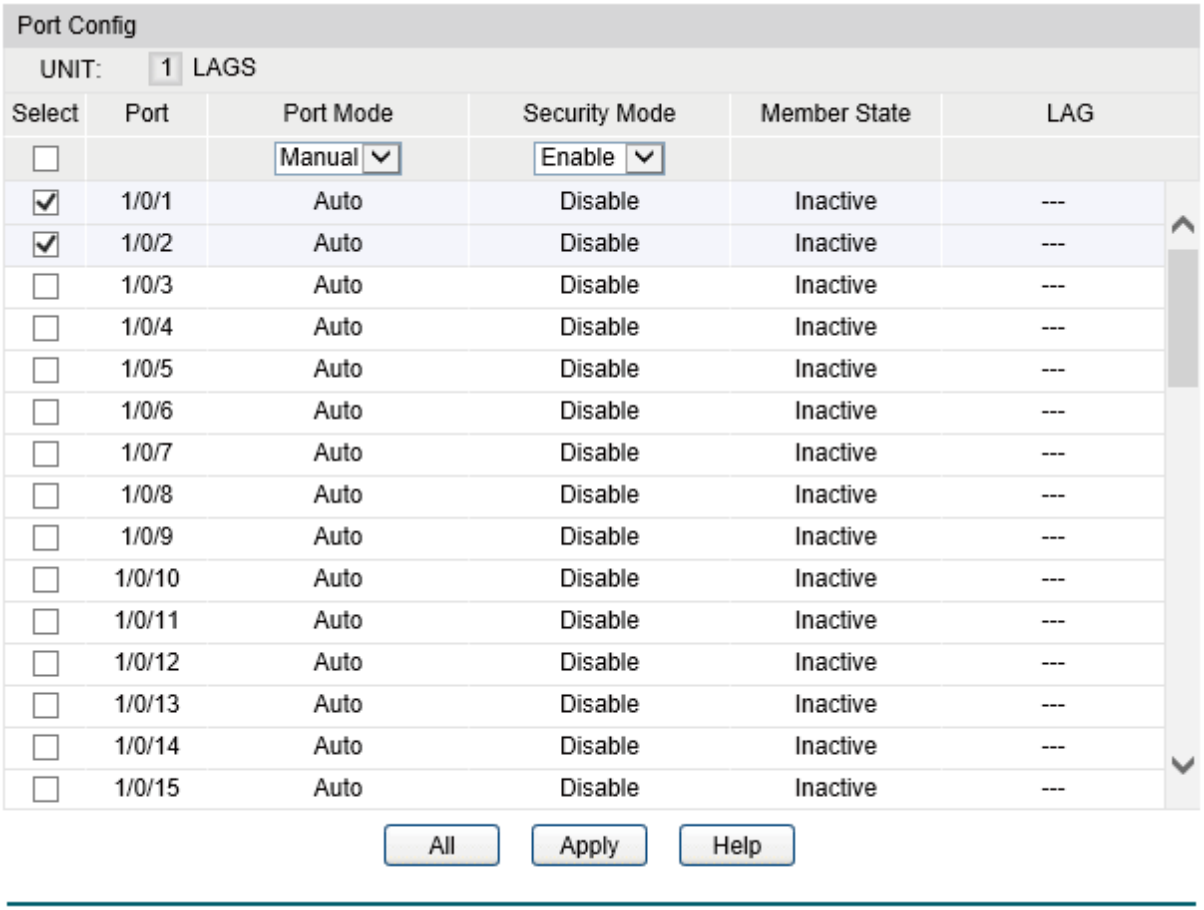
Priority	Specify the priority that will be assigned to voice packets. A bigger value means a higher priority. The range is 0 to 7; the default is 6. This is an IEEE 802.1p priority, and you can further configure its schedule mode if needed. For details about schedule mode, please refer to *Configuring QoS*.

4) Click **Apply**.

2.1.3 Configuring Voice VLAN Mode on Ports

Choose the menu **QoS > Voice VLAN > Port Config** to load the following page.

Figure 2-3 Configuring Voice VLAN Mode on Ports



Follow these steps to configure voice VLAN mode on ports:

1) Select your desired ports and choose the port mode.

Port Mode	Choose the way of adding the selected ports to the voice VLAN. **Auto**: When a port receives a voice packet whose resource MAC address matches an OUI address, the switch automatically adds the port to the voice VLAN. If you choose the Auto mode for the selected ports, make sure traffic from your voice device is tagged. **Manual**: You manually add the ports connecting voice devices to the voice VLAN.
Member State	Displays the current state of the ports that are connected to voice devices. **Active**: The corresponding port is in the voice VLAN. **Inactive**: The corresponding port is not in the voice VLAN.

2) Set the security mode for selected ports.

Security Mode	For packets that will be forwarded in the voice VLAN, you can configure the security mode to prevent malicious traffic with faked voice VLAN tag. For packets to other VLANs, how the switch processes the packets is determined by whether the selected ports permit the VLAN or not, independent of voice VLAN security mode. **Disable**: For packets to the voice VLAN, the switch does not check the source MAC address and the selected ports forward all these packets in the voice VLAN. The security mode is disabled by default. **Enable**: For packets to the voice VLAN, the selected ports forward only voice packets whose source MAC addresses match OUI addresses to the voice VLAN, and discard others. We recommend that you do not mix voice traffic with data traffic in the voice VLAN. If necessary, make sure the security mode is disabled.

3) Click **Apply**.

2.2 Using the CLI

Follow these steps to configure the voice VLAN:

Step 1	**configure** Enter global configuration mode.
Step 2	**show voice vlan oui** Check whether the OUI address of your voice device is in the OUI table.
Step 3	**voice vlan mac-address** *mac-addr* **mask** *mask* [**description** *descript*] If the OUI address of your voice device is not in the OUI table, add the OUI address to the table. *mac-addr*: Enter the OUI address of your device. *mask*: Specify a mask to determine the depth of the OUI that the switch uses to check source addresses of received packets. *descript:* Give an OUI address description for identification.
Step 4	**voice vlan priority** *pri* Set the priority for voice packets. *pri:* Specify the priority that will be tagged on voice packets. A bigger value means a higher priority. The range is 0 to 7; the default is 6. This is an IEEE 802.1p priority, and you can further configure its schedule mode if needed. For details about schedule mode, please refer to *Configuring QoS*.

Step 5	**voice vlan aging** *time* Set the aging time for ports in automatic voice VLAN mode. *time:* Specify the length of time that a port remains in the voice VLAN after the port receives a voice packet. Aging time works only for ports in automatic voice VLAN mode. The range is 1 to 43200 minutes; the default is 1440 minutes.
Step 6	**voice vlan** *vid* Specify an existing VLAN as the voice VLAN. *vid :* Enter the VLAN ID that you have created for the voice VLAN.
Step 7	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *lag-id* **| range port-channel** *lag-list* **}** Enter interface configuration mode. *port* |*port-list*: The number or the list of the Ethernet port that you want to configure. *lag-id* |*lag-list:* The ID or the list of the LAG that you want to configure.
Step 8	**switchport voice vlan mode** { auto | manual } Choose the way of adding the specified ports to the voice VLAN. auto: The switch automatically adds the specified ports to the voice VLAN when the ports receive voice packets. If you choose the auto mode for the specified ports, make sure traffic from your voice device is tagged. manual: You need to manually add the specified ports to the voice VLAN.
Step 9	**switchport voice vlan security** Enable the security feature. For packets to the voice VLAN, the selected ports forward only voice packets whose source MAC addresses match OUI addresses to the voice VLAN, and discard others. For packets to other VLANs, how the switch processes the packets is determined by whether the selected ports permit the VLAN or not, independent of voice VLAN security mode. We recommend that you do not mix voice traffic with data traffic in the voice VLAN. If necessary, make sure the security mode is disabled.
Step 10	**switchport general allowed vlan** *vid* { tagged | untagged } (For ports in manual voice VLAN mode) Add the specified ports to the voice VLAN. *vid:* Enter the voice VLAN ID to add the specified ports to the voice VLAN. tagged | untagged: Set the egress rule as tagged or untagged for the specified ports.
Step 11	**show voice vlan** Verify the global configuration of voice VLAN.
Step 12	**show voice vlan switchport** Verify the voice VLAN configuration of the ports.

Step 13	**end** Return to privileged EXEC mode.
Step 14	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set port 1/0/1 in manual voice VLAN mode. Configure the switch to forward voice traffic with an IEEE 802.1p priority of 5 and to transmit only voice traffic whose resource MAC address matches an OUI address in the voice VLAN :

Switch#configure

Switch(config)#vlan 10

Switch(config-vlan)#name VoiceVLAN

Switch(config-vlan)#exit

Switch(config)#voice vlan priority 5

Switch(config)#voice vlan 10

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

Switch(config-if)#switchport voice vlan mode manual

Switch(config-if)#switchport voice vlan security

Switch(config-if)#switchport general allowed vlan 10 untagged

Switch(config-if)#show voice vlan

Voice VLAN status: Enabled

VLAN ID: 10

Aging Time: 1440

Voice Priority: 5

Switch(config-if)#show voice vlan switchport

Port	Auto-mode	Security	State	LAG
Gi1/0/1	Manual	Enabled	Active	N/A
Gi1/0/2	Auto	Disabled	Inactive	N/A
Gi1/0/3	Auto	Disabled	Inactive	N/A

...

Switch(config-if)#end

Switch#copy running-config startup-config

3 Configuration Example

3.1 Network Requirements

The company plans to install IP phones in the office area and the meeting room, and has requirements as follows:

- In the office area
  - » IP phones share switch ports used by computers, because no more ports are available for IP phones.
  - » Transmit voice traffic in an exclusive path with high quality.
  - » Avoid attacks from malicious data flows.
- In the meeting room
  - » Transmit voice traffic in an exclusive path with high quality.
  - » Avoid attacks from malicious data flows.

3.2 Configuration Scheme

In the office area, IP phones share the same ports of the switch with computers and therefore occupy no more ports. To separate voice traffic from data traffic, configure LLDP-MED to instruct IP Phones to send traffic with the voice VLAN tag. Voice traffic is transmitted in the voice VLAN, and data traffic is transmitted in the default VLAN. Set ports that are connected to IP phones in automatic voice VLAN mode. Meanwhile, configure the voice VLAN to work in security mode and to forward only legal voice packets.

In the meeting room, the switch provides dedicated connections to IP phones. In this situation, IP phones do not need to send traffic with the voice VLAN tag. Set ports that are connected to IP phones in manual voice VLAN mode. Meanwhile, configure the voice VLAN to work in security mode and to forward only legal voice packets.

To ensure the high quality of voice traffic, configure all devices along the path to keep the priority of voice traffic and to coordinate with the voice VLAN configuration.

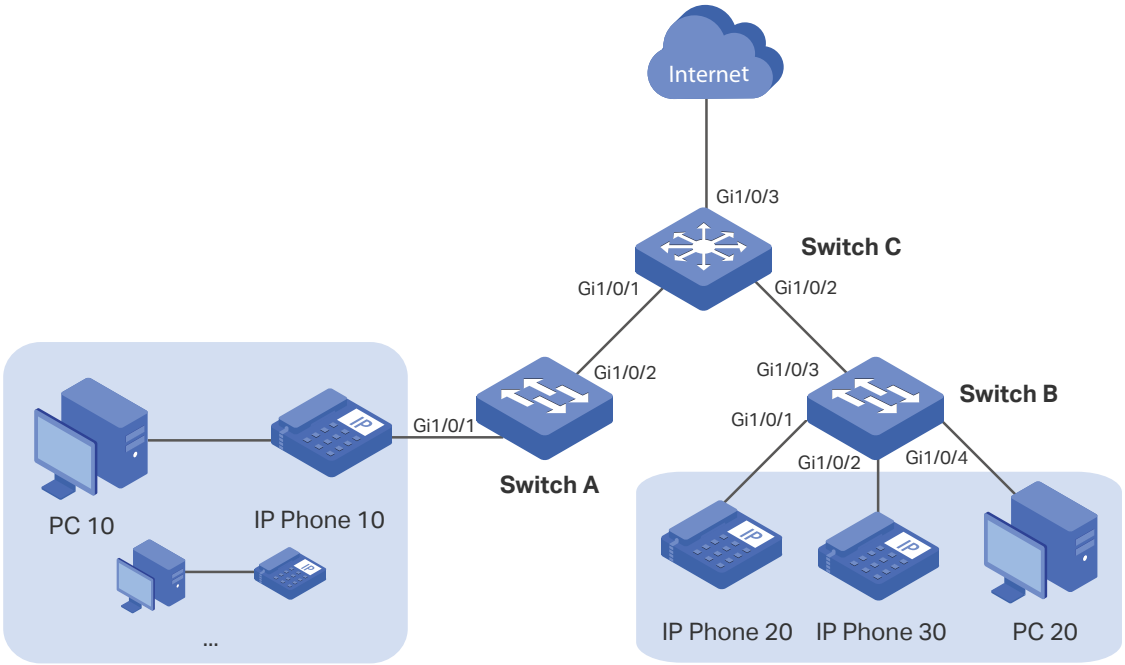
3.3 Network Topology

In the office area, IP phones are added to ports that are connected to computers on Switch A. These ports use the voice VLAN for voice traffic, and the default VLAN for data traffic.

In the meeting room, computers and IP phones are connected to different ports of Switch B. Ports connected to IP phones use the voice VLAN for voice traffic, and ports connected to computers use the default VLAN for data traffic.

Voice traffics from Switch A and Switch B are forwarded to voice gateway and Internet through Switch C.

Figure 3-1 Network Topology



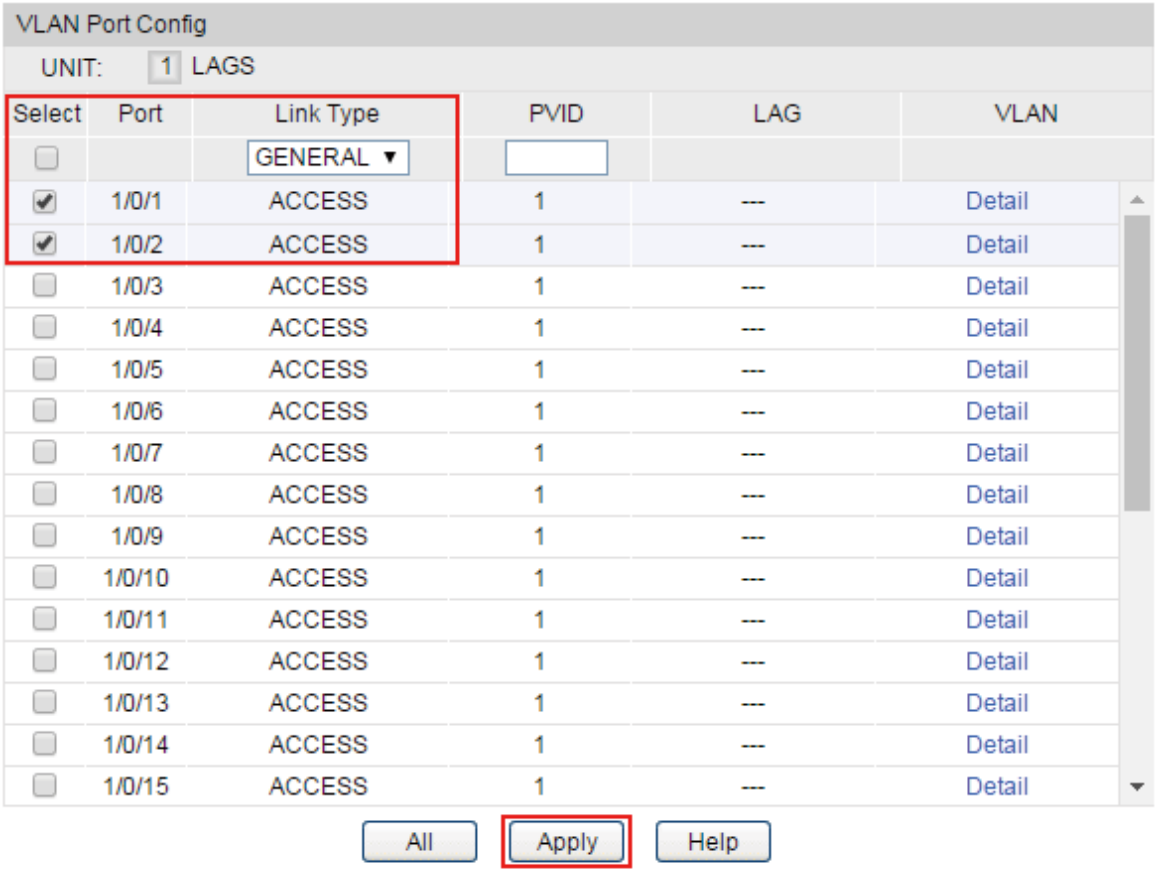
Demonstrated with T2600G-28TS, this chapter provides configuration procedures in two ways: using the GUI and using the CLI.

3.4 Using the GUI

- Configurations for Switch A

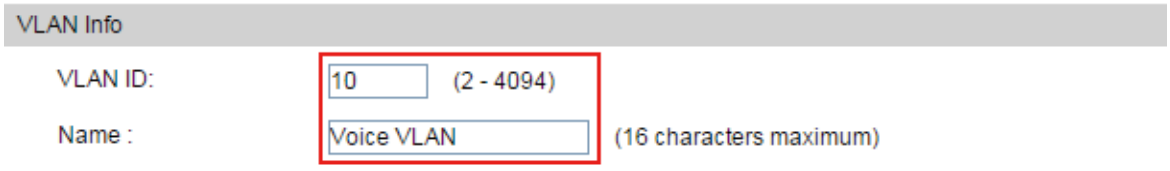
1) Choose the menu **VLAN > 802.1Q VLAN > Port Config** to load the following page. Set the link type of port1/0/1-2 as **General,** and click **Apply**.

Figure 3-2 Configuring the Link Type of port 1/0/1-2



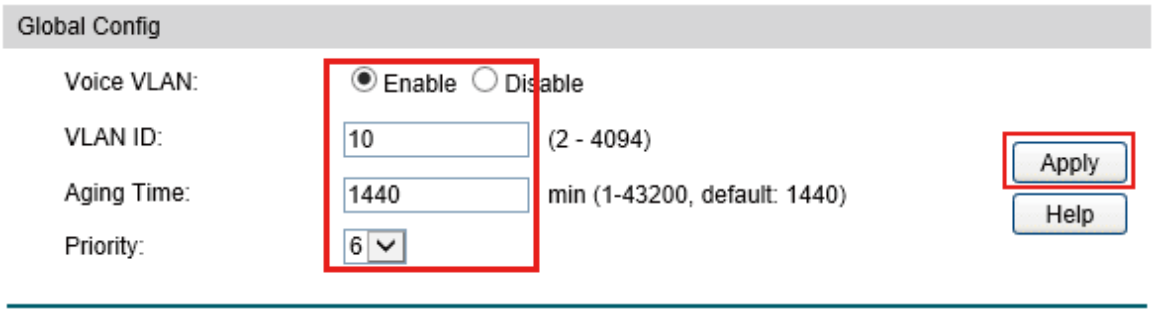
2) Choose the menu **VLAN > 802.1Q VLAN > VLAN Config** and click **Create** to load the following page. Create VLAN 10, and click **Apply**.

Figure 3-3 Creating a VLAN



3) Choose the menu **QoS > Voice VLAN > Global Config** to load the following page. Enable voice VLAN, enter 10 in the **VLAN ID** field and set aging time as 1440 minutes and priority as 6. Then click **Apply**.

Figure 3-4 Configuring Voice VLAN Globally



4) Choose the menu **QoS > Voice VLAN > Port Config** to load the following page. Select port 1/0/1, choose auto mode and enable security mode. Select port 1/0/2 and choose manual mode. Click **Apply**.

Figure 3-5 Configuring Voice VLAN Mode on Port 1/0/1

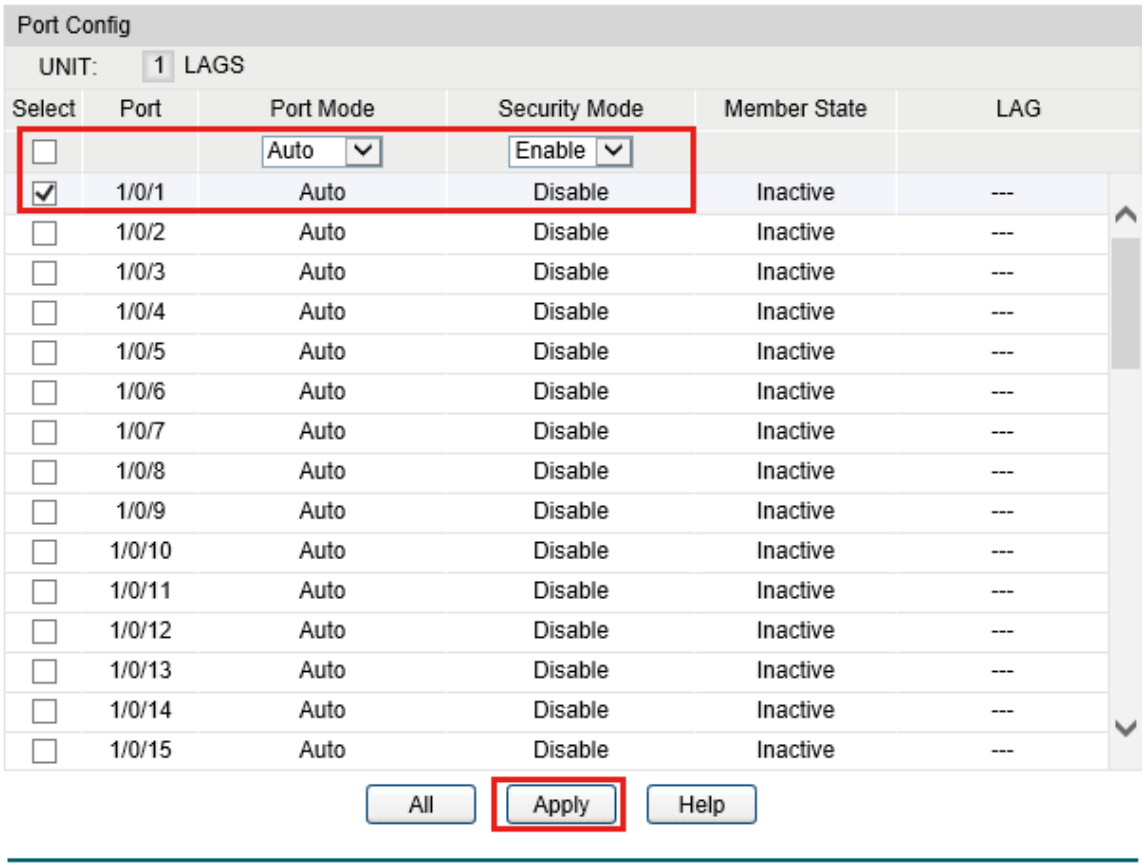
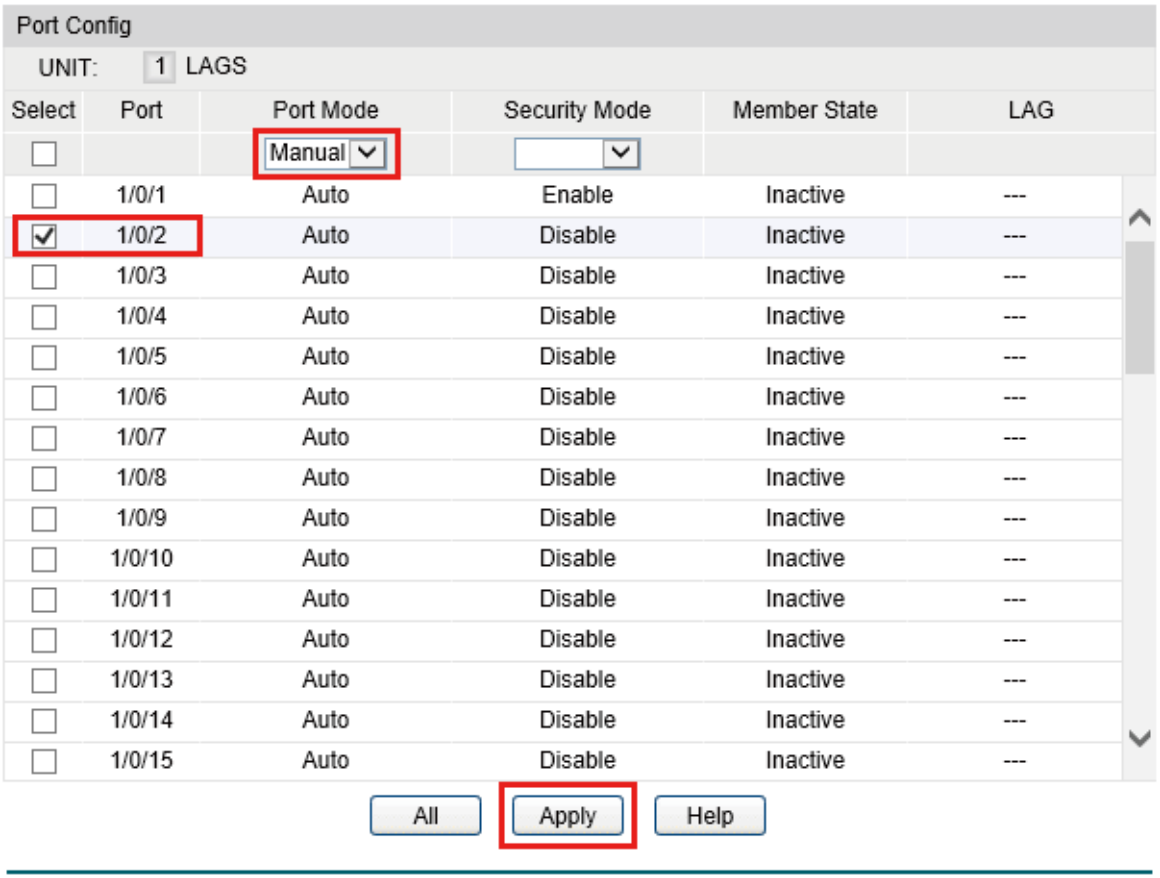
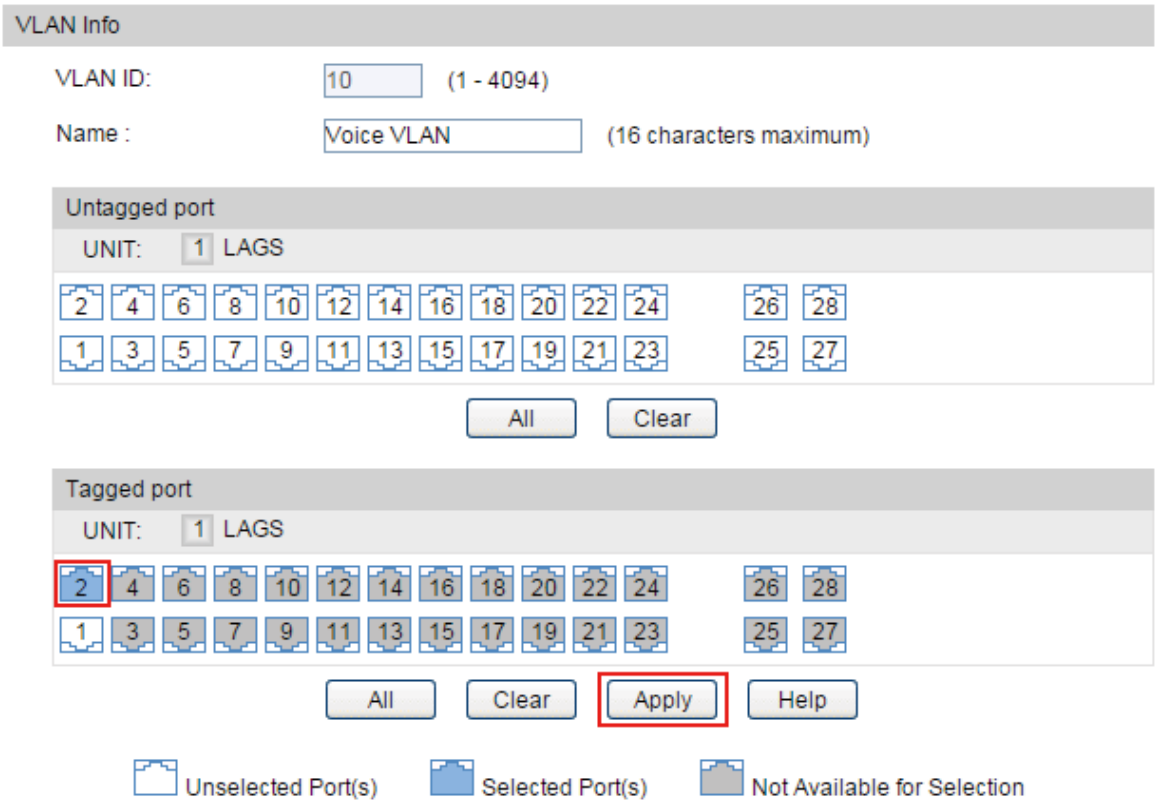


Figure 3-6 Configuring Voice VLAN Mode on Port 1/0/2



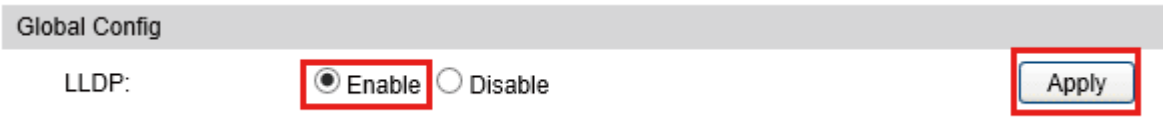
5) Choose the menu **VLAN > 802.1Q VLAN > VLAN Config** and edit VLAN 10 to load the following page. Add port 1/0/2 to the voice VLAN.

Figure 3-7 Adding Port 1/0/2 to the Voice VLAN



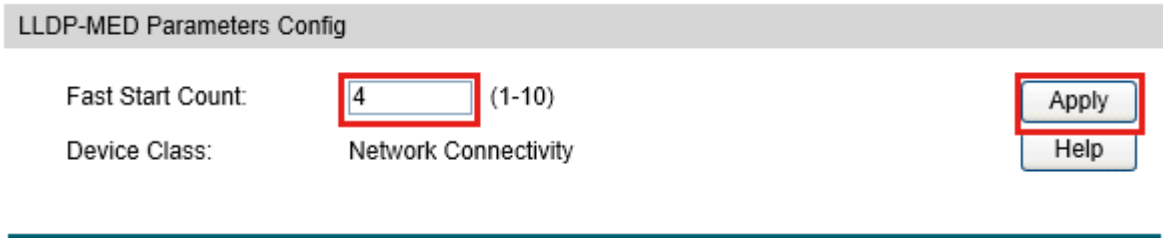
6) Choose the menu **LLDP > Basic Config> Global Config** to load the following page. Enable LLDP globally.

Figure 3-8 Enabling LLDP Globally



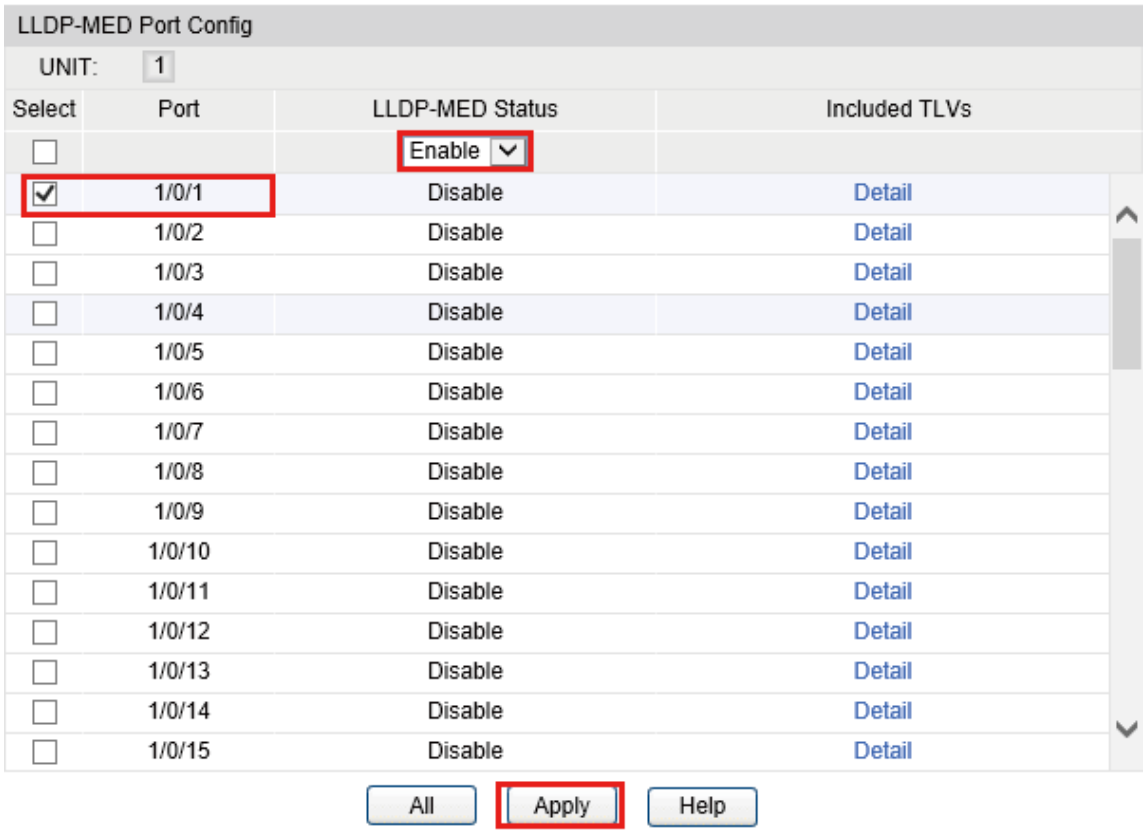
7) Choose the menu **LLDP > LLDP-MED> Global Config** to load the following page. Set fast start count as 4.

Figure 3-9 Configuring LLDP-MED Globally



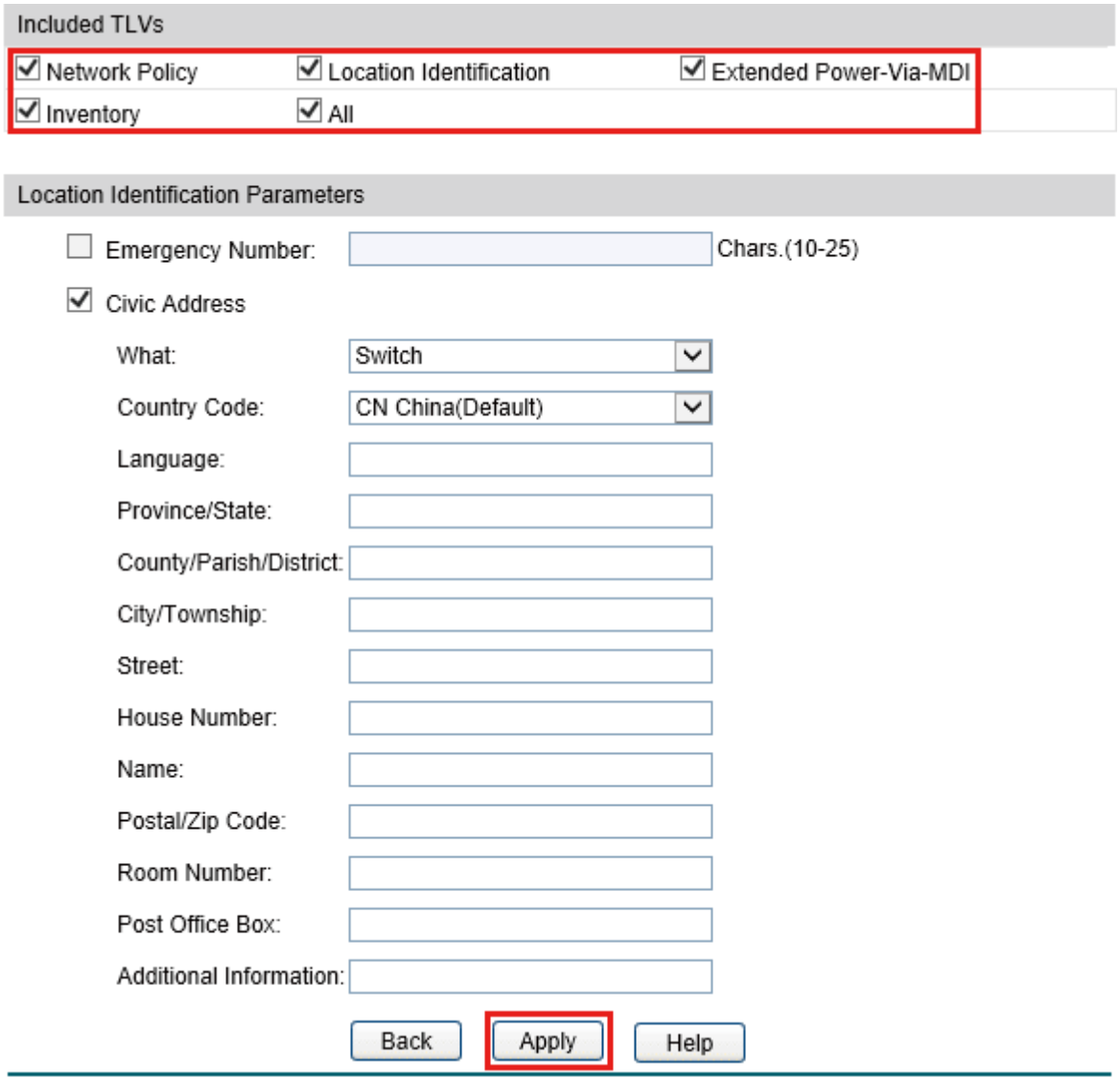
8) Choose the menu **LLDP > LLDP-MED> Port Config** to load the following page. Enable LLDP-MED on port 1/0/1.

Figure 3-10 Configuring LLDP-MED on Ports



Click **Detail** of port1/0/1 to load the following page. Configure the TLV information which will be carried in LLDP-MED frames and sent out by port 1/0/1. Select all TLVs, and configure location identification parameters.

Figure 3-11 Configuring TLVs



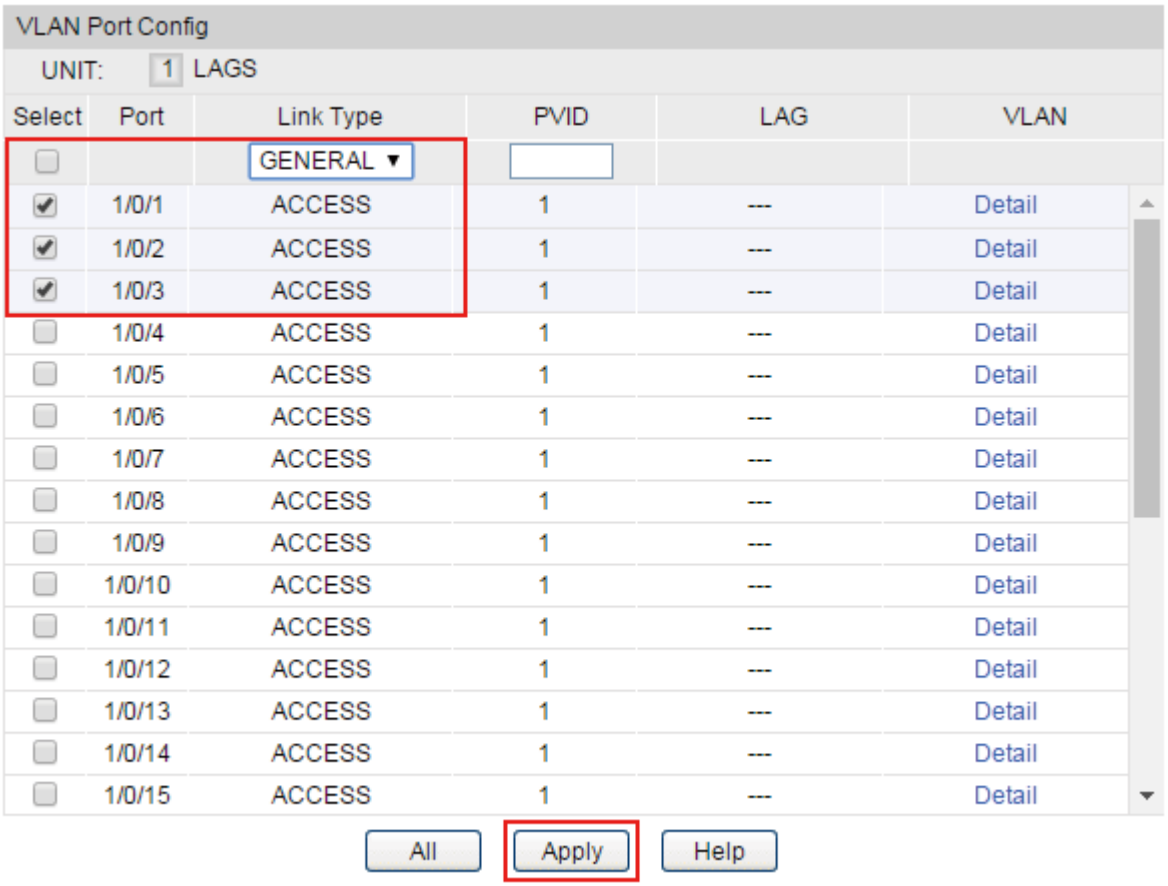
For details about LLDP-MED, please refer to *Configuring LLDP*.

9) Click **Save Config** to save the settings.

- Configurations for Switch B

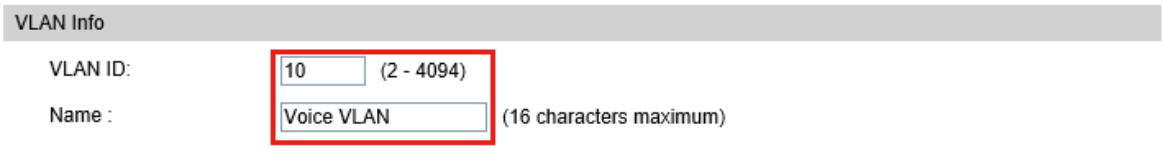
1) Choose the menu **VLAN > 802.1Q VLAN > Port Config** to load the following page. Configure the link type of ports 1/0/1-3 as General.

Figure 3-12 Configuring the Link Type of port 1/0/1-3



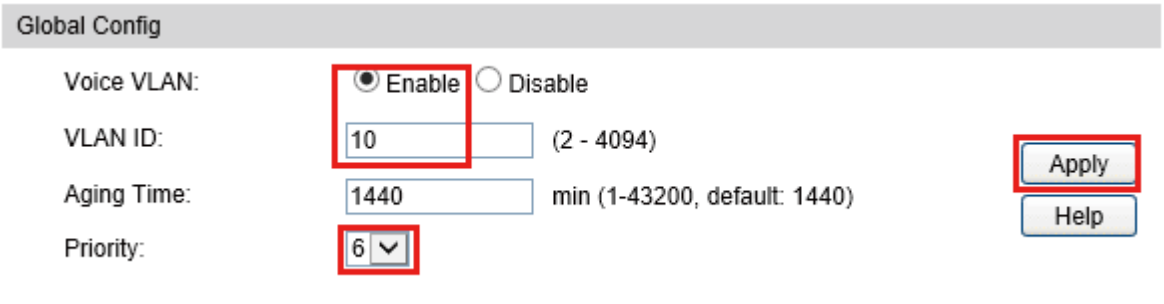
2) Choose the menu **VLAN > 802.1Q VLAN > VLAN Config** and click **Create** to load the following page. Create VLAN 10.

Figure 3-13 Creating a VLAN



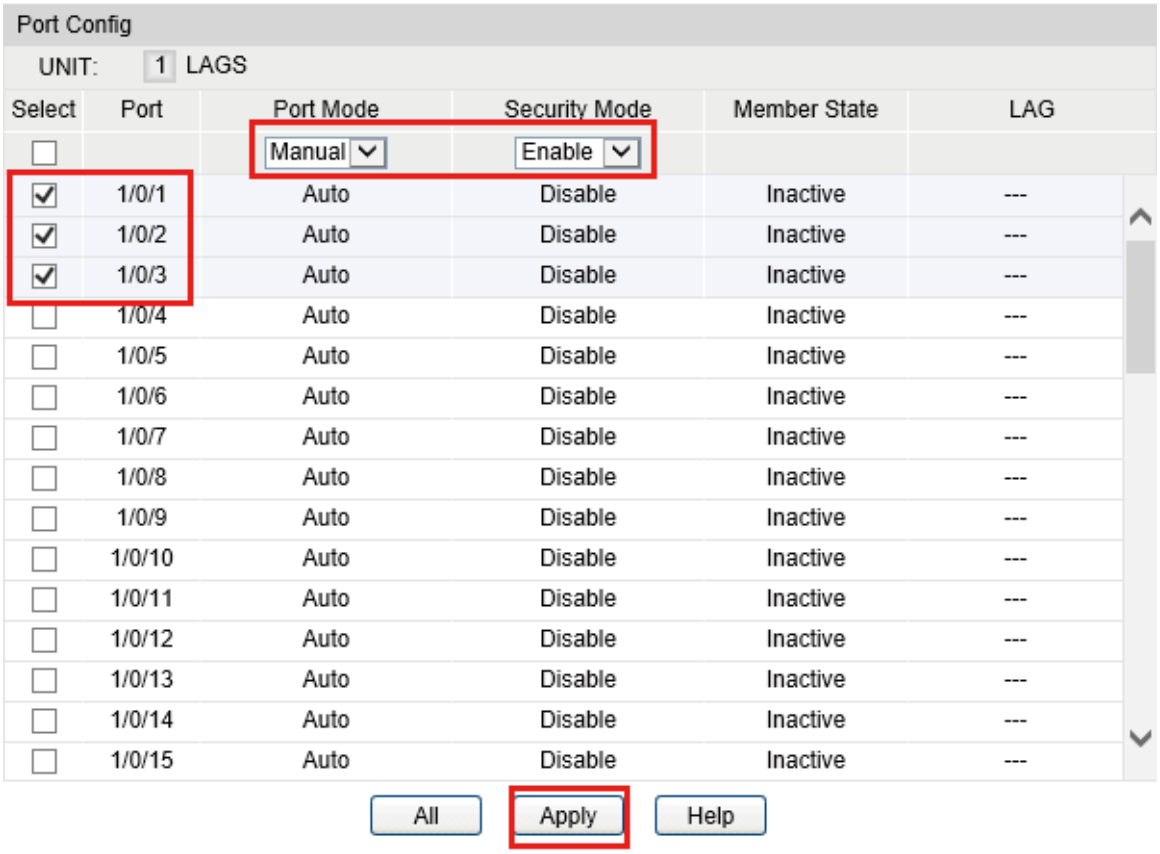
3) Choose the menu **QoS > Voice VLAN > Global Config** to load the following page. Enable voice VLAN, enter 10 in the **VLAN ID** field and set priority as 6.

Figure 3-14 Configuring Voice VLAN Globally



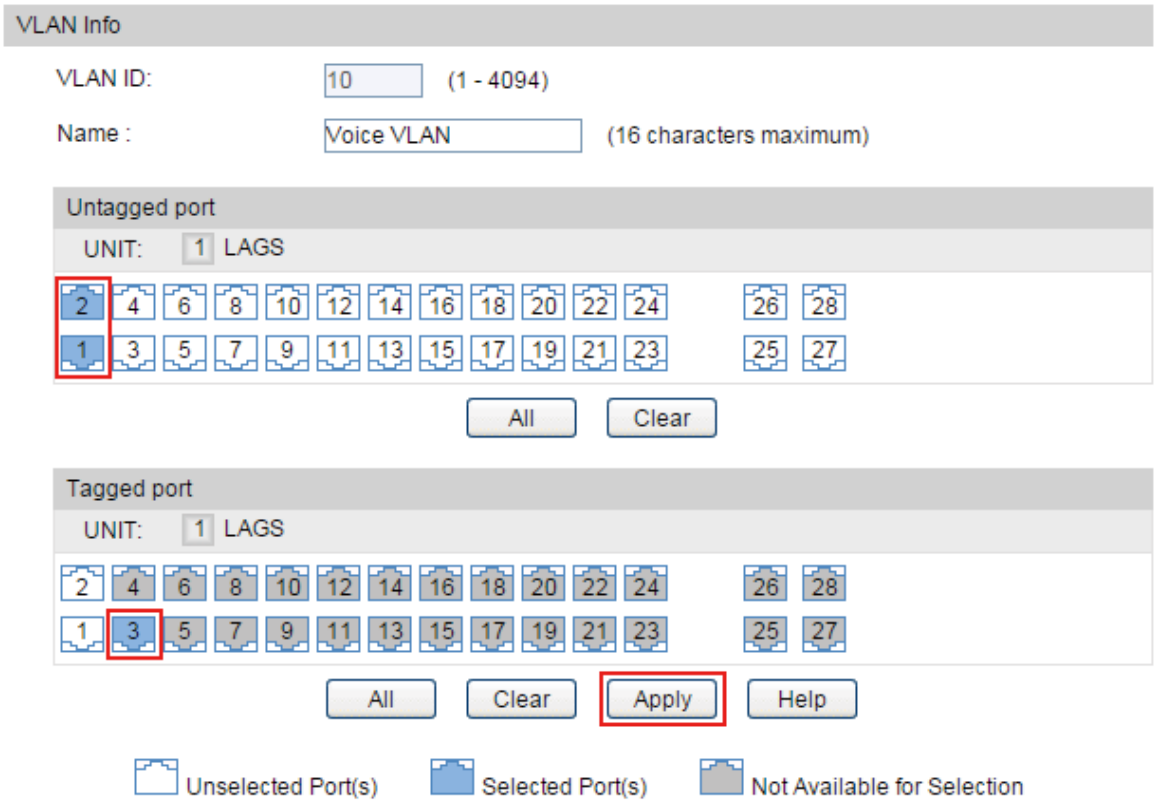
4) Choose the menu **QoS > Voice VLAN > Port Config** to load the following page. Select ports 1/0/1-3, choose manual mode and enable security mode. Click **Apply**.

Figure 3-15 Configuring Voice VLAN Mode on Ports



5) Choose the menu **VLAN > 802.1Q VLAN > VLAN Config** and edit VLAN 10 to load the following page. Add ports 1/0/1-3 to the voice VLAN. Click **Apply**.

Figure 3-16 Adding Ports to the Voice VLAN

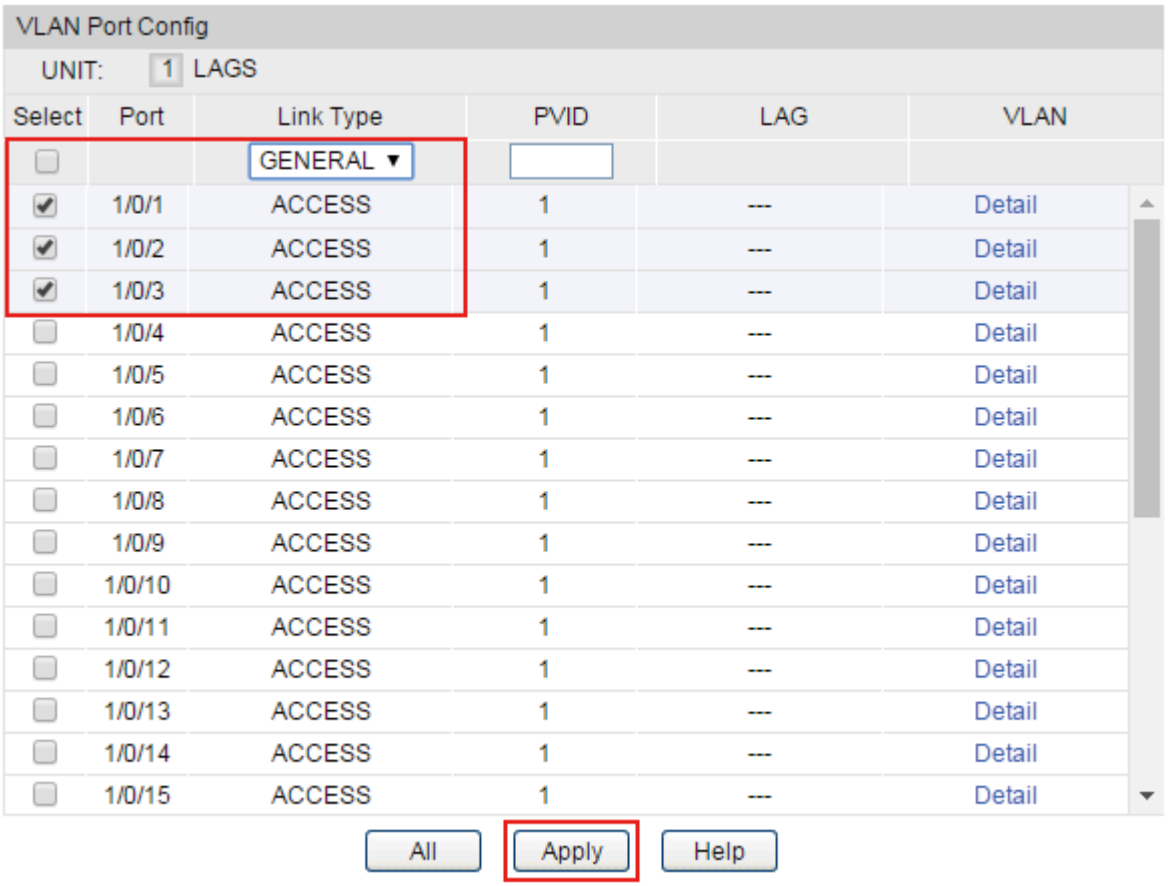


6) Click **Save Config** to save the settings.

- Configurations for Switch C

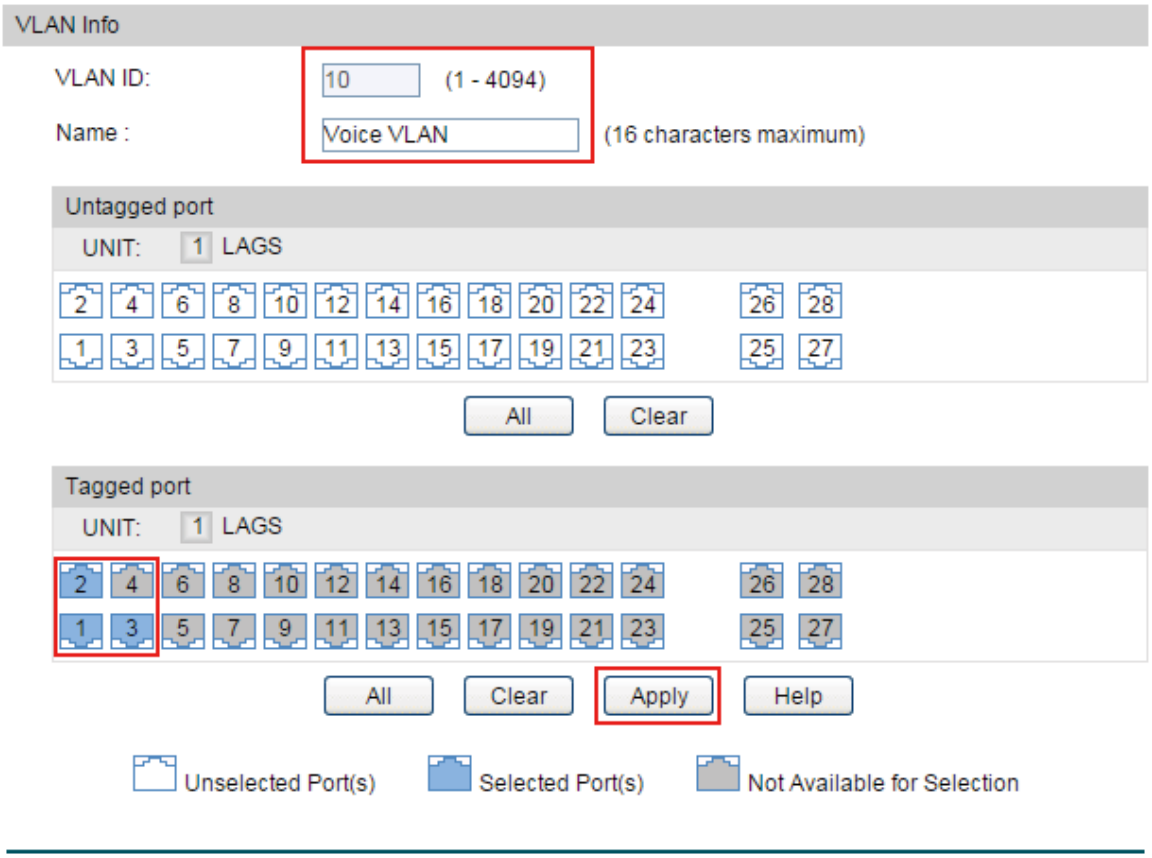
1) Choose the menu **VLAN > 802.1Q VLAN > Port Config** to load the following page. Configure the link type of ports 1/0/1-3 as General. Click **Apply**.

Figure 3-17 Configuring the Link Type of port 1/0/1-3



2) Choose the menu **VLAN > 802.1Q VLAN > VLAN Config** and click **Create** to load the following page. Create VLAN 10 and add ports 1/0/1-3 as tagged ports to the VLAN. Click **Apply**.

Figure 3-18 Creating a VLAN and Adding Ports to the VLAN



3) Click **Save Config** to save the settings.

3.5 Using the CLI

- Configurations for Switch A

1) Configure the link type of ports 1/0/1-2 as General.

Switch_A#configure

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

Switch_A(config-if-range)#switchport mode general

Switch_A(config-if-range)#exit

2) Create VLAN 10.

Switch_A(config)#vlan 10

Switch_A(config-vlan)#name VoiceVLAN

Switch_A(config-vlan)#exit

3) Configure the aging time as 1440 minutes for port in automatic voice VLAN mode, and set the 802.1p priority of voice packets as 6. Set VLAN 10 as the voice VLAN.

Switch_A(config)#voice vlan aging 1440

Switch_A(config)#voice vlan priority 6

Switch_A(config)#voice vlan 10

4) Configure port 1/0/1 to automatic voice VLAN mode and enable security mode.

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

Switch_A(config-if)#switchport voice vlan mode auto

Switch_A(config-if)#switchport voice vlan security

Switch_A(config-if)#exit

5) Configure port 1/0/2 to manual voice VLAN mode, and add it to the voice VLAN as a tagged port.

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

Switch_A(config-if)#switchport voice vlan mode manual

Switch_A(config-if)#switchport general allowed vlan 10 tagged

Switch_A(config-if)#exit

6) Enable LLDP globally and set the fast start count of LLDP-MED frame as 4.

Switch_A(config)#lldp

Switch_A(config)# lldp med-fast-count 4

7) Enable the LLDP-MED feature on port 1/0/1.

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

Switch_A(config-if)#lldp med-status

8) Select all MED TLVs to be carried in LLDP frames and sent out by port 1/0/1.

Switch_A(config-if)#lldp med-tlv-select all

9) Configure the location identification parameters for the IP phone on port 1/0/1. For details about LLDP-MED, please refer to *Configuring LLDP*.

Switch(config-if)#lldp med-location civic-address language English lci-city Vancouver street X _east_hastings_street postal-zipcode V6A1P9

Switch_A(config-if)#end

Switch_A#copy running-config startup-config

- Configurations for Switch B

1) Create VLAN 10.

Switch_B#configure

Switch_B(config)#vlan 10

Switch_B(config-vlan)#name VoiceVLAN

Switch_B(config-vlan)#exit

2) Set the 802.1p priority of voice packets as 6 and VLAN 10 as the voice VLAN.

Switch_B(config)#voice vlan priority 6

Switch_B(config)#voice vlan 10

3) Configure ports 1/0/1-3 to manual voice VLAN mode and enable security mode.

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

Switch_B(config-if-range)#switchport voice vlan mode manual

Switch_B(config-if-range)#switchport voice vlan security

Switch_B(config-if-range)#exit

4) For ports 1/0/1-2, set the link type as General and the egress rule as Untagged, and add them to the Voice VLAN.

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

Switch_B(config-if-range)#switchport mode general

Switch_B(config-if-range)#switchport general vlan 10 untagged

Switch_B(config-if-range)#exit

5) For ports 1/0/3, set the link type as General and the egress rule as Tagged, and add them to the Voice VLAN.

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

Switch_B(config-if)#switchport mode general

Switch_B(config-if)#switchport general allowed vlan 10 tagged

Switch_B(config-if)#end

Switch_B#copy running-config startup-config

- Configurations for Switch C

1) Create VLAN 10.

Switch_C#configure

Switch_C(config)#vlan 10

Switch_C(config-vlan)#name VoiceVLAN

Switch_C(config-vlan)#exit

2) For ports 1/0/1-3, set the link type as General and the egress rule as Tagged, and add them to the Voice VLAN.

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

Switch_C(config-if-range)#switchport mode general

```
Switch_C(config-if-range)#switchport general allowed vlan 10 tagged
Switch_C(config-if-range)#end
Switch_C#copy running-config startup-config
```

Verify the Configurations

- Switch A

Verify the global configuration of voice VLAN:

```
Switch_A#show voice vlan
 Voice VLAN status: Enabled
 VLAN ID: 10
 Aging Time: 1440
 Voice Priority: 6
```

Verify the voice VLAN configuration on the ports:

```
Switch_A#show voice vlan switchport
```

Port	Auto-mode	Security	State	LAG
Gi1/0/1	Auto	Enabled	Inactive	N/A
Gi1/0/2	Manual	Disabled	Active	N/A
Gi1/0/3	Auto	Disabled	Inactive	N/A

...

- Switch B

Verify the global configuration of voice VLAN:

```
Switch_B#show voice vlan
 Voice VLAN status: Enabled
 VLAN ID: 10
 Aging Time: 1440
 Voice Priority: 6
```

Verify the voice VLAN configuration on the ports:

```
Switch_B#show voice vlan switchport
```

```
Port     Auto-mode   Security    State     LAG
------   ----------  ----------  --------  ------
Gi1/0/1  Manual      Enabled     Active    N/A
Gi1/0/2  Manual      Enabled     Active    N/A
Gi1/0/3  Manual      Enabled     Active    N/A
...
```

- Switch C

  Verify the voice VLAN configuration for VLAN 10:

  Switch_C#show vlan id 10

```
VLAN   Name            Status    Ports
-----  --------------  --------  --------------------------------
10     VoiceVlan       active    Gi1/0/1, Gi1/0/2, Gi1/0/3
```

4 Appendix: Default Parameters

Default settings of voice VLAN are listed in the following tables.

Table 4-1 Default Settings of Global Configuration

Parameter	Default Setting
Voice VLAN	Disable
VLAN ID	None
Aging Time	1440 minutes
Priority	6

Table 4-2 Default Settings of Port Configuration

Parameter	Default Setting
Port Mode	Auto
Security Mode	Disable
Member State	Inactive

Table 4-3 Entries in the OUI Table

OUI	MASK	Description
00-01-e3-00-00-00	ff-ff-ff-00-00-00	Siemens Phone
00-03-6b-00-00-00	ff-ff-ff-00-00-00	Cisco Phone
00-04-0d-00-00-00	ff-ff-ff-00-00-00	Avaya Phone
00-60-b9-00-00-00	ff-ff-ff-00-00-00	Philips Phone
00-d0-1e-00-00-00	ff-ff-ff-00-00-00	Pingtel Phone
00-e0-75-00-00-00	ff-ff-ff-00-00-00	PolyCom Phone
00-e0-bb-00-00-00	ff-ff-ff-00-00-00	3Com Phone

Part 24

Configuring PoE

CHAPTERS

1. PoE
2. PoE Power Management Configurations
3. Time-Range Function Configurations
4. Example for PoE Configurations
5. Appendix: Default Parameters

Note:

Only T2600G-28MPS supports PoE feature.

1 PoE

1.1 Overview

Power over Ethernet (PoE) is a remote power supply function. With this function, the switch can supply power to the connected devices over twisted-pair cable.

Some devices such as IP phones, access points (APs) and cameras may be located far away from the AC power source in actual use. PoE can provide power for these devices without requiring to deploy power cables. This allows a single cable to provide both data connection and electric power to devices.

IEEE 802.3af and 802.3at are both PoE standards. The standard process of PoE power supply contains powered-device discovery, power administration, disconnect detection and optional power-device power classification.

PSE

Power sourcing equipment (PSE) is a device that provides power for PDs on the Ethernet, for example, the PoE switch. PSE can detect the PDs and determine the device power requirements.

PD

Powered device (PD) is a device receiving power from the PSE, for example, IP phones and access points. According to whether PDs comply with IEEE standard, they can be classified into standard PDs and non-standard PDs. Only standard PDs can be powered via TP-Link PoE switches.

1.2 Supported Features

PoE Power Management

PoE Power Management is used for users to manage the power the PoE switch supplied. The PoE switch allocates the power to the PDs according to your configurations.

Time-Range Function

The time-range function is used to set the power-on and power-off time range to save energy according to your actual use.

2 PoE Power Management Configurations

With PoE Power Management, you can:

- Configure the PoE parameters manually
- Configure the PoE parameters using the profile

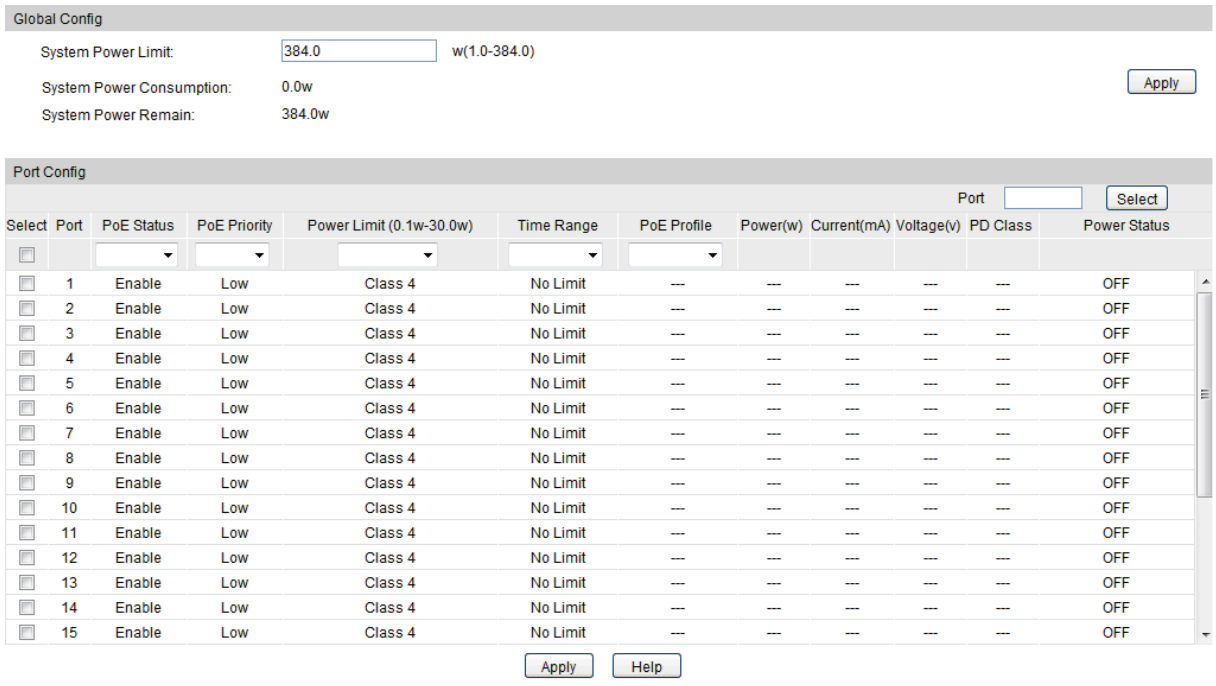
You can configure the PoE parameters one by one via configuring the PoE parameters manually. You can also set a profile with the desired parameters and bind the profile to the corresponding ports to quickly configure the PoE parameters.

2.1 Using the GUI

2.1.1 Configuring the PoE Parameters Manually

Choose the menu **PoE** > **PoE Config** > **PoE Config** to load the following page.

Figure 2-1 Configuring PoE Parameters Manually



Follow these steps to configure the basic PoE parameters:

1) In the **Global Config** section, specify the System Power Limit and click **Apply**.

System Power Limit	Specify the maximum power the PoE switch can supply.

System Power Consumption	Displays the real-time system power consumption of the PoE switch.
System Power Remain	Displays the real-time system remaining power of the PoE switch.

2) In the **Port Config** section, select the port you want to configure and specify the parameters. Click **Apply**.

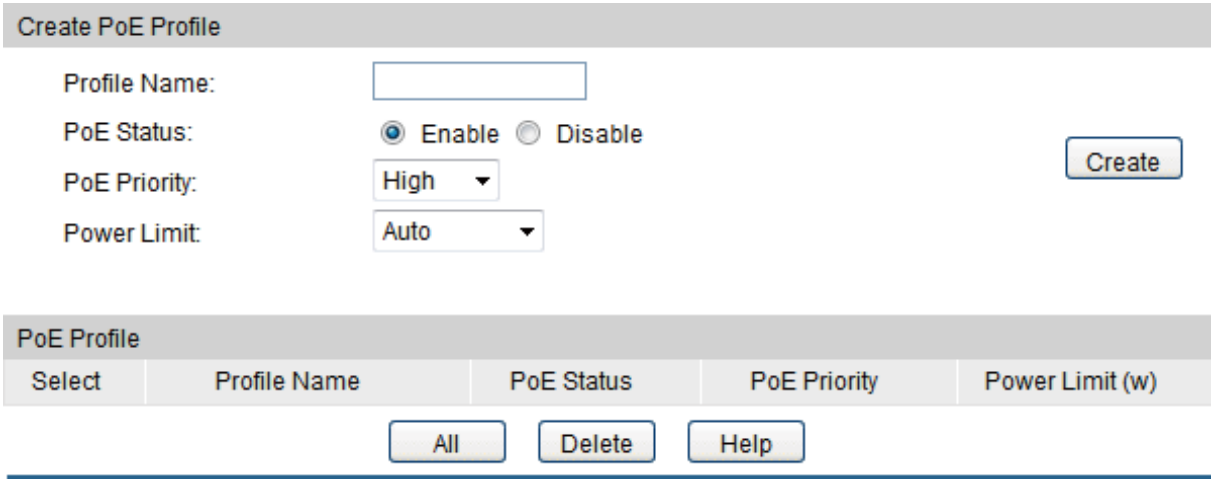
PoE Status	Enable or disable the PoE function for on corresponding port. The port can supply power to the PD when its status is enable.
PoE Priority	Select the priority level for the corresponding port. When the supply power exceeds the system power limit, the switch will power off PDs on low-priority ports to ensure stable running of other PDs.
Power Limit (0.1w-30.0w)	Specify the maximum power the corresponding port can supply. The following options are provided: **Auto**: The switch will allocate a value as the maximum power that the port can supply automatically. **Class1**: The maximum power that the port can supply is 4W. **Class2**: The maximum power that the port can supply is 7W. **Class3**: The maximum power that the port can supply is 15.4W. **Class4**: The maximum power that the port can supply is 30W. **Manual**: Enter a value manually.
Time Range	Select a time range, then the port will supply power only during the time range. For how to create a time range, refer to *Time Range Function Configurations*.
PoE Profile	A quick configuration method for the corresponding ports. If one profile is selected, you will not be able to modify PoE status, PoE priority or power limit manually. For how to create a profile, refer to *Configuring the PoE Parameters Using the Profile*.
Power(w)	Displays the port's real-time power supply.
Current(mA)	Displays the port's real-time current.
Voltage(v)	Displays the port's real-time voltage.
PD Class	Displays the class the linked PD belongs to.
Power Status	Displays the port's real-time power status.

2.1.2 Configuring the PoE Parameters Using the Profile

■ Creating a PoE Profile

Choose the menu **PoE** > **PoE Config** > **PoE Profile** to load the following page.

Figure 2-2 Create a PoE Profile



Follow these steps to create a PoE profile:

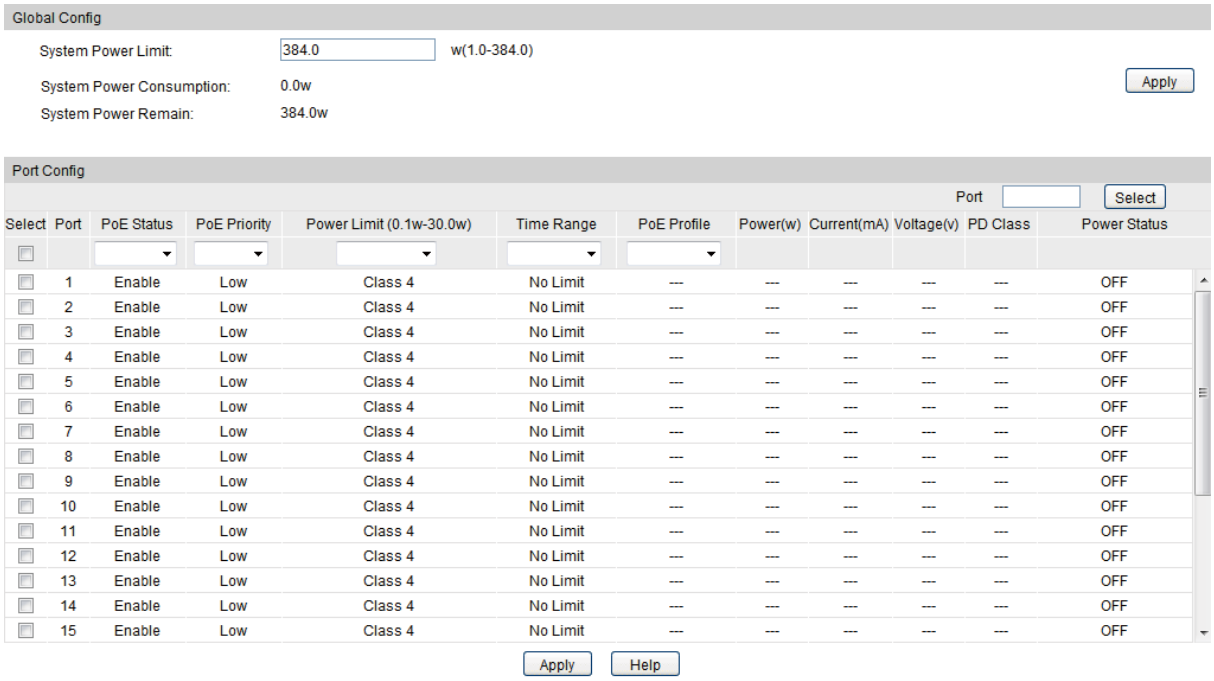
1) In the **Create PoE Profile** section, specify the desired configurations of the profile.

Profile Name	Specify a name for the PoE profile.
PoE Status	Specify the PoE status for the PoE profile.
PoE Priority	Specify the priority level for the PoE profile. The following options are provided: **High**, **Middle** and **Low**. When the supply power exceeds the system power limit, the switch will power off PDs on low-priority ports to ensure stable running of other PDs.
Power Limit	Specify the maximum power the port can supply for the PoE profile. The following options are provided: **Auto**: The switch will allocate a value as the maximum power that the port can supply automatically. **Class1**: The maximum power that the port can supply is 4W. **Class2**: The maximum power that the port can supply is 7W. **Class3**: The maximum power that the port can supply is 15.4W. **Class4**: The maximum power that the port can supply is 30W. **Manual**: Enter a value manually.

2) Click **Apply**.

Binding the Profile to the Corresponding Ports

Figure 2-3 Bind the Profile to the Corresponding Ports



Follow these steps to bind the profile to the corresponding ports:

1) In the **Global Config** section, specify the System Power Limit and click **Apply**.

System Power Limit	Specify the maximum power the PoE switch can supply.
System Power Consumption	Displays the real-time system power consumption of the PoE switch.
System Power Remain	Displays the real-time system remaining power of the PoE switch.

2) In the **Port Config** section, select a profile and bind it to the corresponding ports. Click **Apply**.

Port Select	Specify the port number and click **Select** to quick-select the corresponding entry. Only one port can be selected at a time.
Time Range	Select a time range, then the port will supply power only during the time range. For how to create a time range, refer to *Time Range Function Configurations*.
PoE Profile	Select the PoE profile set in the **PoE Profile** section for the desired port. If one profile is selected, you will not be able to modify PoE status, PoE priority or power limit manually.
Power(w)	Displays the port's real-time power supply.
Current(mA)	Displays the port's real-time current.

Voltage(v)	Displays the port's real-time voltage.
PD Class	Displays the class the linked PD belongs to.
Power Status	Displays the port's real-time power status.

2.2 Using the CLI

2.2.1 Configuring the PoE Parameters Manually

Follow these steps to configure the basic PoE parameters:

Step 1	**configure** Enter global configuration mode.
Step 2	**power inline consumption** *power-limit* Specify the the maximum power the PoE switch can supply globally. *power-limit*: Specify the maximum power the PoE switch can supply. It ranges from 1.0 to 384.0W, and the default value is 384.0W.
Step 3	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **}** Enter Interface Configuration mode. *port*: Specify the Ethernet port number, for example 1/0/1. *port-list:* Specify the list of Ethernet ports, for example 1/0/1-3, 1/0/5.
Step 4	**power inline supply {** enable **|** disable **}** Specify the PoE status for the corresponding port. enable **|** disable: Enable or disable the PoE function. By default, it is enable.
Step 5	**power inline priority {** low **|** middle **|** high **}** Specify the PoE priority for the corresponding port. low **|** middle **|** high: Select the priority level for the corresponding port. When the supply power exceeds the system power limit, the switch will power off PDs on low-priority ports to ensure stable running of other PDs. The default setting is low.
Step 6	**power inline consumption {** *power-limit* **|** auto **|** class1 **|** class2 **|** class3 **|** class4 **}** Specify the maximum power the corresponding port can supply. *power-limit* | auto | class1 | class2 | class3 | class4: Select or enter the maximum power the corresponding port can supply. The following options are provided: **Auto** represents that the switch will allocate the maximum power that the port can supply automatically. **Class1** represents 4W, **Class2** represents 7W, **Class3** represents 15.4W and **Class4** represents 30W, or you can enter a value manually. The value ranges from 1 to 300. It is in the unit of 0.1 watt. For instance, if you want to configure the maximum power as 5W, you should enter 50. By default, it is Class4.

Step 7	**show power inline** Verify the global PoE information of the system.
Step 8	**show power inline configuration interface [fastEthernet {** *port* **|** *port-list* **}	gigabitEthernet {** *port* **|** *port-list* **}]** Verify the PoE configuration of the corresponding port. *port*: Specify the Ethernet port number, for example 1/0/1. *port-list*: Specify the list of Ethernet ports, in the format of 1/0/1-3, 1/0/5.
Step 9	**show power inline information interface [fastEthernet {** *port* **|** *port-list* **}	gigabitEthernet {** *port* **|** *port-list* **}]** Verify the real-time PoE status of the corresponding port. *port*: Specify the Ethernet port number, for example 1/0/1. *port-list*: Specify the list of Ethernet ports, in the format of 1/0/1-3, 1/0/5.
Step 10	**end** Return to privileged EXEC mode.
Step 11	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set the system power limit as 160W. Set the priority as middle and set the power limit as class3 in the port 1/0/5.

Switch#configure

Switch(config)#power inline consumption 160

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

Switch(config-if)#power inline supply enable

Switch(config-if)#power inline priority middle

Switch(config-if)#power inline consumption class3

Switch(config-if)#show power inline

System Power Limit: 160.0w

System Power Consumption: 0.0w

System Power Remain: 160.0w

Switch(config-if)#show power inline configuration interface gigabitEthernet 1/0/5

Interface	PoE-Status	PoE-Prio	Power-Limit(w)	Time-Range	PoE-Profile
Gi1/0/5	Enable	Middle	Class3	No Limit	None

Switch(config-if)#show power inline information interface gigabitEthernet 1/0/5

Interface	Power(w)	Current(mA)	Voltage(v)	PD-Class	Power-Status
Gi1/0/5	1.3	26	53.5	Class 2	ON

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Configuring the PoE Parameters Using the Profile

Follow these steps to configure the PoE profile:

Step 1	**configure** Enter global configuration mode.
Step 2	**power profile** *name* **[supply {** enable **|** disable **} [priority {** low **|** middle **|** high **} [consumption {** *power-limit* **|** auto **|** class1 **|** class2 **|** class3 **|** class4 **}]]]** Create a PoE profile for the switch. In a profile, the PoE status, PoE priority and power limit are configured. You can bind a profile to the corresponding port to quickly configure the PoE function. *name*: Specify a name for the PoE profile. It ranges from 1 to 16 characters. If the name contains spaces, enclose the name in double quotes. enable **|** disable: Specify the PoE status for the profile. By default, it is enable. low **|** middle **|** high: Select the priority level for the profile. When the supply power exceeds the system power limit, the switch will power off PDs on low-priority ports to ensure stable running of other PDs. power-limit	auto	class1	class2	class3	class4: Select or enter the maximum power the corresponding port can supply. The following options are provided: **Auto** represents that the switch will assign a value of maximum power automatically. **Class1** represents 4W, **Class2** represents 7W, **Class3** represents 15.4W and **Class4** represents 30W or you can enter a value manually. The value ranges from 1 to 300. It is in the unit of 0.1 watt. For instance, if you want to configure the maximum power as 5W, you should enter 50.
Step 3	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **}** Enter Interface Configuration mode. *port*: Specify the Ethernet port number, for example 1/0/1. *port-list:* Specify the list of Ethernet ports, for example 1/0/1-3, 1/0/5.
Step 4	**power inline profile** *name* Bind a PoE profile to the desired port. If one profile is selected, you will not be able to modify PoE status, PoE priority or power limit manually. *name*: Specify the name of the PoE profile. If the name contains spaces, enclose the name in double quotes.

Step 5	**show power profile** Verify the defined PoE profile.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create a profile named profile1and bind the profile to the port 1/0/6.

Switch#configure

Switch(config)#power profile profile1 **supply** enable **priority** middle **consumption** class2

Switch(config)#show power profile

Index Name Status Priority Power-Limit(w)

----- ---------- ---------- --------- --------------

1 profile1 Enable Middle Class2

Switch(config)#interface gigabitEthernet 1/0/6

Switch(config-if)#power inline profile profile1

Switch(config-if)#show power inline configuration interface gigabitEthernet 1/0/6

Interface PoE-Status PoE-Prio Power-Limit(w) Time-Range PoE-Profile

---------- ---------- ---------- ------------ ------------ ----------------

Gi1/0/6 Enable Middle Class2 No Limit profile1

Switch(config-if)#end

Switch#copy running-config startup-config

3 Time-Range Function Configurations

With Time-Range configurations, you can:

- Create a time-range
- Configure the holiday parameters
- View the time-range table

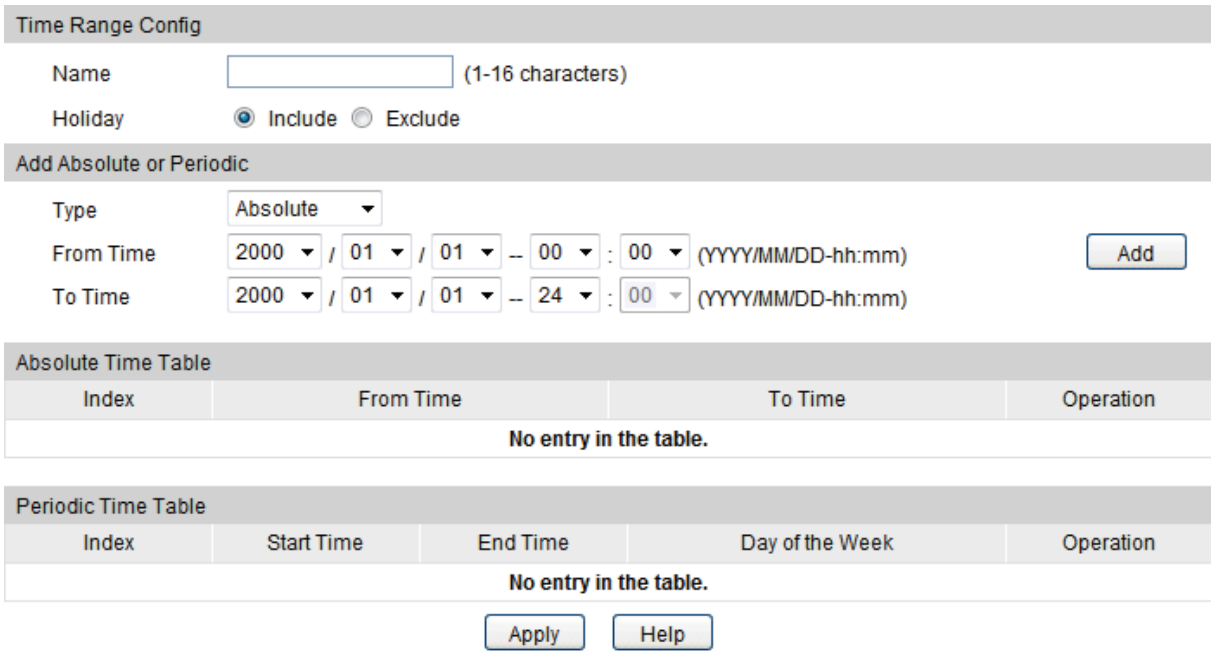
The time range here relies on the switch system clock; therefore, you need a reliable clock source. We recommend that you use Network Time Protocol (NTP) to synchronize the switch clock. For details, refer to *System Info Configurations* in *Managing System*.

3.1 Using the GUI

3.1.1 Creating a Time-Range

Choose the menu **PoE** > **Time-Range** > **Time-Range Create** to load the following page.

Figure 3-1 Creating a Time-Range



Follow these steps to create a time-range:

1) In the **Time Range Config** section, enter a name for the time-range and select to include or exclude the holiday in the time-range.

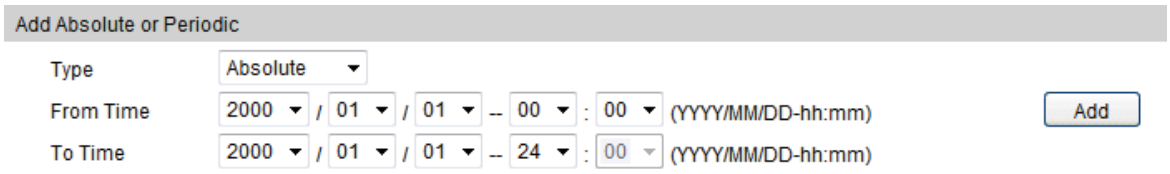
Name	Specify a name for the time-range.

Holiday	Select to **Include** or **Exclude** the holiday in a time-range. If **Exclude** is selected, the time-range will not take effect on holiday and the **PoE Status** is disabled. Otherwise, the time-range will not be affected by holiday.

2) In the **Add Absolute or Periodic** section, specify the parameters and click **Add**.

When the **Absolute** mode is selected, the following section will be shown.

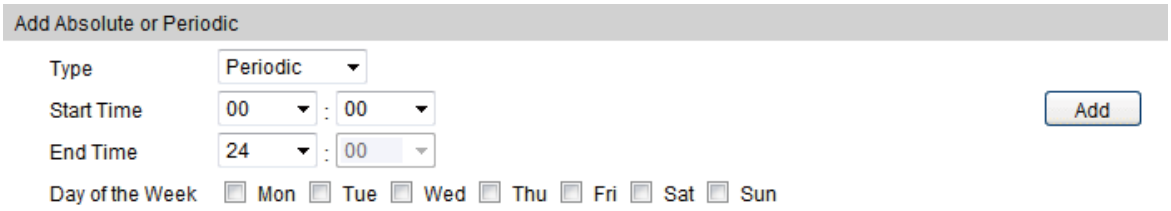
Figure 3-2 Absolute Mode



Type	Select **Absolute** time to configure.
From Time	Specify the starting time of the absolute mode.
To Time	Specify the ending time of the absolute mode.

When the **Periodic** mode is selected, the following section will be shown.

Figure 3-3 Periodic Mode



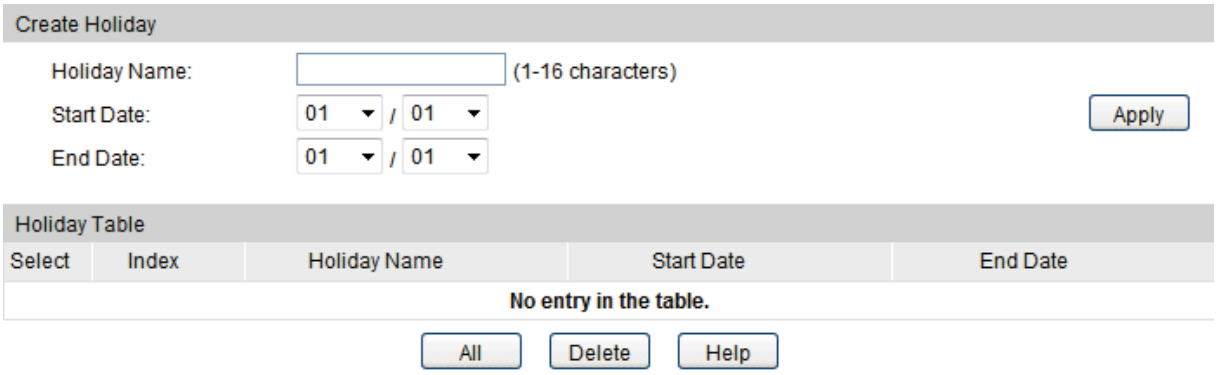
Type	Select **Periodic** time to configure.
Start Time	Specify the start time of the periodic mode.
End Time	Specify the end time of the periodic mode.
Day of the Week	Select day of the week for the periodic mode.

3) Click **Apply**.

3.1.2 Configuring the Holiday Parameters

Choose the menu **PoE** > **Time-Range** > **Holiday Config** to load the following page.

Figure 3-4 Configuring the Holiday Parameters



Follow these steps to configure the holiday parameters:

1) In the **Create Holiday** section, enter a name of the holiday and specify the time.

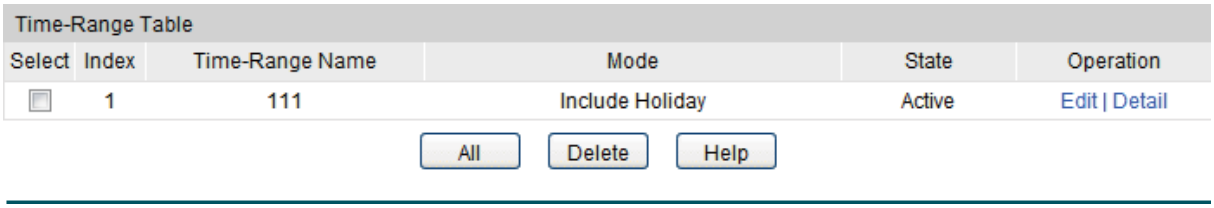
Holiday Name	Specify a name for the holiday time.
Start Date	Specify the starting time of the holiday.
End Date	Specify the ending time of the holiday.

2) Click **Apply**.

3.1.3 Viewing the Time-Range Table

Choose the menu **PoE** > **Time-Range** > **Time-Range Summary** to load the following page.

Figure 3-5 Viewing the Time-Range Table



Time-Range Name	Displays the name of the PoE time-range.
Mode	Displays the work mode of the time-range function.
State	Displays the state of the time-range function.
Operation	View or edit the configuration of the time-range function.

3.2 Using the CLI

3.2.1 Configuring a Time-Range

Follow these steps to create a time-range:

Step 1	**configure** Enter global configuration mode.
Step 2	**power time-range** *name* Create a time-range for the switch and enter Power Time-range Configuration Mode. *name*: Specify a name for the PoE time-range. It ranges from 1 to 16 characters. If the name contains spaces, enclose the name in double quotes.
Step 3	**holiday {** exclude **|** include **}** Specify the time-range including or excluding the holiday. exclude	include: Select to Include or Exclude the holiday in a time-range. If **Exclude** is selected, the time-range will not take effect on holiday and the **PoE Status** is disabled. Otherwise, the time-range will not be affected by holiday. By default, it is include.
Step 4	Use the following command to create a absolute time-range: **absolute from** *start-date* **to** *end-date* Specify the time range in absolute mode. *start-date*: Specify the starting time of the time-range in absolute mode. It is in the format of MM/DD/YYYY-HH:MM. By default, it is 2000/01/01-00:00. *end-date*: Specify the ending time of the time-range in absolute mode. It is in the format of MM/DD/YYYY-HH:MM. By default, it is 2099/12/31-24:00. Use the following command to create a periodic time-range: **periodic start** *start-time* **end** *end-time* **day-of-the-week** *day-of-the-week* Specify the time range in periodic mode. *start-time*: Specify the starting time in periodic mode. It is in the format of HH:MM. By default, it is 00:00. *end-time*: Specify the ending time in periodic mode. It is in the format of HH:MM. By default, it is 24:00. *day-of-the-week*: Specify the day in the week in periodic mode, ranging from 1 to 7. It is in the format of 1,3-4. By default, it is 1-7.
Step 5	**exit** Exit Power Time-range Configuration Mode.

Step 6	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **}** Enter Interface Configuration mode. *port*: Specify the Ethernet port number, for example 1/0/1. *port-list:* Specify the list of Ethernet ports, for example 1/0/1-3, 1/0/5.
Step 7	**power inline time-range** *name* Bind a time-range to the desired port. *name*: Specify the name of the PoE time-range.
Step 8	**show power time-range [** *name* **]** Verify the configuration of the time-range. *name*: Specify the name of the desired holiday. It ranges from 1 to 16 characters. If the name contains spaces, enclose the name in double quotes. All PoE time-range configurations will be displayed if the name is not specified.
Step 9	**end** Return to privileged EXEC mode.
Step 10	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create a time-range named time-range1. Select include to make the settings take affected on holiday. Set absolute mode from 2016/09/08-00:00 to 2016/09/10-24:00. Set the periodic mode from 01:00 to 23:00 in Friday. Bind the time-range to the port 1/0/7.

Switch#configure

Switch(config)#power time-range time-range1

Switch(config-time-range)#holiday include

Switch(config-time-range)#absolute from 09/08/2016-00:00 **to** 09/10/2016-24:00

Switch(config-time-range)#periodic start 01:00 **end** 23:00 **day-of-the-week** 5

Switch(config-time-range)#exit

Switch(config)#show power time-range time-range1

Time-range entry: time-range1 (Active)

holiday: include

number of absolute time: 1

1 - 09/08/2016-00:00 to 09/10/2016-24:00

number of periodic time: 1

1 - 01:00 to 23:00 on 5

Switch(config)#interface gigabitEthernet 1/0/7

Switch(config-if)#power inline time-range time-range1

Switch(config-if)#end

Switch#copy running-config startup-config

3.2.2 Configuring the Holiday Parameters

Follow these steps to configure the holiday parameters:

Step 1	**configure** Enter global configuration mode.
Step 2	**power holiday** *name* **start-date** *start-date* **end-date** *end-date* Create a time range for the holiday. *name*: Specify a name for the holiday. It ranges from 1 to 16 characters. If the name contains spaces, enclose the name in double quotes. *start-date*: Specify the starting time of the holiday in the format of MM/DD. *end-date*: Specify the ending time of the holiday in the format of MM/DD.
Step 3	**show power holiday** Verify the defined PoE holiday.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create a holiday named holiday1. Set the starting date as 08/16, set the ending date as 08/20.

Switch#configure

Switch(config)#power holiday holiday1 **start-date** 08/16 **end-date** 08/20

Switch(config)#show power holiday

Index	Holiday Name	Start-End
1	holiday1	08.16-08.20

Switch(config)#end

Switch#copy running-config startup-config

3.2.3 Viewing the Time-Range Table

On privileged EXEC mode or any other configuration mode, you can use the following command to view the time-range table:

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

Verify the defined PoE time-range.

name: Specify the name of the time-range desired. It ranges from 1 to 16 characters. If the name contains spaces, enclose the name in double quotes. All PoE time-range configurations will be displayed if the name is not specified.

The following example shows how to view the time-range table.

Switch#show power time-range

Time-range entry: office time (Active)

holiday: include

number of absolute time: 0

(01/01/2000-00:00 to 12/31/2099-24:00 by default)

number of periodic time: 1

1 - 08:30 to 18:00 on 1,2,3,4,5

Switch#end

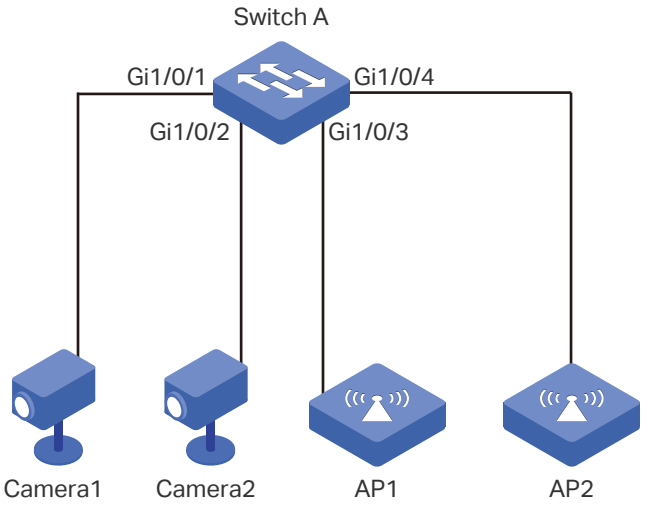
Switch#copy running-config startup-config

4 Example for PoE Configurations

4.1 Network Requirements

The network topology of a company is shown below. Camera1 and Camera2 work for the security of the company and cannot be power off all the time. AP1 and AP2 provide Internet service and only work in the daytime.

Figure 4-1 Network Topology



4.2 Configuring Scheme

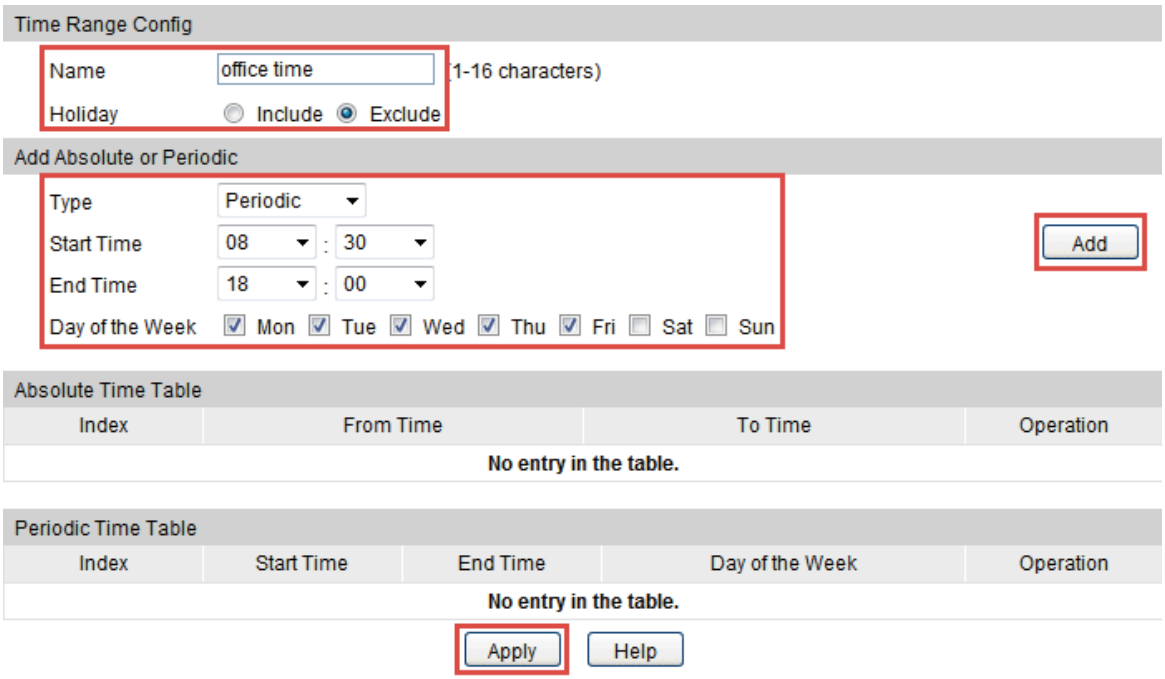
To implement this requirement, you can set a PoE time-range as the office time for example from 08:30 to 18:00. You can also set a holiday and make the time-range settings not be affected on holiday. Then apply the settings to port 1/0/3 and 1/0/4. Port 1/0/1 and 1/0/2 need to supply power all the time, so the time range configurations can be left at the default settings here.

4.3 Using the GUI

The configurations of Port1/0/4 is similar with the configuration of port 1/0/3. Here we take port 1/0/3 for example.

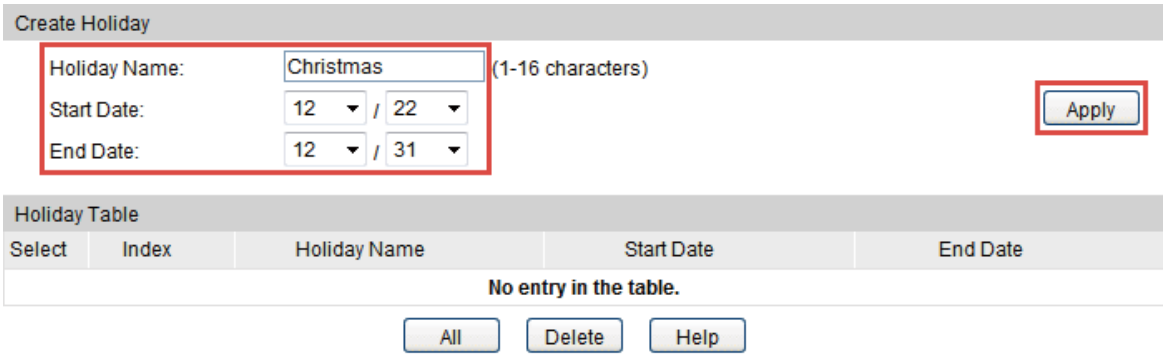
1) Choose the menu **PoE** > **Time-Range** > **Time-Range Create** to load the following page. Specify a name for the time-range and select **Exclude** to make the time-range settings not be affected on holiday. Set the time-range as periodic mode and add a time range that is from 08:30 to 18:00. Click **Apply**.

Figure 4-2 Create a Time-Range



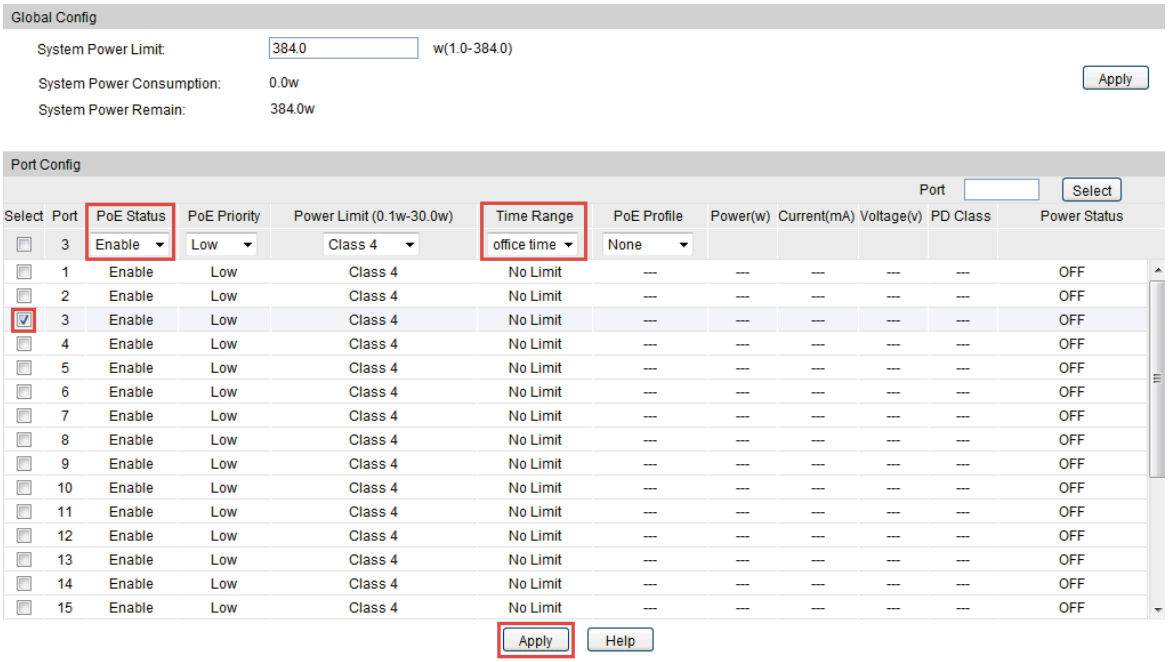
2) Choose the menu **PoE** > **Time-Range** > **Holiday Config** to load the following page. Specify a name for the holiday and set the starting date and ending date.

Figure 4-3 Configure the Holiday



3) Choose the menu **PoE** > **PoE Config** > **PoE Config** to load the following page. Select port 1/0/3 and enable the PoE function. Set the **Time Range** as office time. Click **Apply**.

Figure 4-4 Configure the Port



4.4 Using the CLI

The configurations of Port1/0/4 is similar with the configuration of port 1/0/3. Here we take port 1/0/3 for example.

1) Create a time-range.

   Switch_A#config

   Switch_A(config)#power time-range “office time”

   Switch_A(config-time-range)#holiday exclude

   Switch_A(config-time-range)#periodic start 08:30 end 23:00 day-of-the-week 1-5

   Switch_A(config-time-range)#exit

2) Create a holiday.

   Switch_A(config)#power holiday Christmas start-date 12/22 end-date 12/31

3) Enable the PoE function on the port 1/0/3. Specify the basic parameters for the port 1/0/3 and bind the time-range “office time” to the port.

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

   Switch_A(config-if)#power inline supply enable

   Switch_A(config-if)#power inline time-range “office time”

   Switch_A(config-if)#exit

   Switch_A(config-if)#end

```
Switch_A#copy running-config startup-config
```

Verify the Configuration

Verify the configuration of the holiday:

```
Switch_A(config)#show power holiday
Index    Holiday Name    Start-End
-----    ------------    ---------
1        Christmas       12.22-12.31
```

Verify the configuration of the time-range:

```
Switch_A(config)#show power time-range
 Time-range entry: office time (Active)
 holiday: exclude
 number of absolute time: 0
  (01/01/2000-00:00 to 12/31/2099-24:00 by default)
 number of periodic time: 1
  1 - 08:30 to 23:00 on 1,2,3,4,5
```

Verify the configuration of the PoE basic parameters:

```
Switch_A(config)#show power inline configuration interface gigabitEthernet 1/0/3
Interface  PoE-Status  PoE-Prio  Power-Limit(w)  Time-Range    PoE-Profile
---------  ----------  --------  --------------  ------------  ----------------
 Gi1/0/3   Enable      Low       Class4           office time  None
```

5 Appendix: Default Parameters

Table 5-1 Default Settings of PoE Configuration

Parameter	Default Setting
System Power Limit	384.0W
PoE Status	Enable
PoE Priority	Low
Power Limit (0.1w-30.0w)	Class 4
Time Range	No Limit
PoE Profile	None

Table 5-2 Default Settings of PoE Profile

Parameter	Default Setting
Profile Name	None
PoE Status	Enable
PoE Priority	High
Power Limit	Auto

Table 5-3 Default Settings of Time-Range Create

Parameter	Default Setting
Name	None
Holiday	Include
Type	Absolute
From Time	01/01/2000-00:00
To Time	01/01/2000-24:00

Table 5-4 Default Settings of Holiday Config

Parameter	Default Setting
Holiday Name	None
Start Date	01/01
End Date	01/01

Part 25

Configuring ACL

CHAPTERS

1. Overview
2. ACL Configuration
3. Configuration Example for ACL
4. Appendix: Default Parameters

1 Overview

1.1 Introduction

The rapid growth of network size and traffic brings challenges to network security and bandwidth allocation. Packet filtering can help prevent unauthorized access behaviors, limit network traffic and improve bandwidth use.

ACL (Access Control List) filters traffic as it passes through a switch, and permits or denies packets crossing specified interfaces or VLANs. It accurately identifies and processes the packets based on the ACL rules. In this way, ACL helps to limit network traffic, manage network access behaviors, forward packets to specified ports and more.

It is usually applied in the following situations:

- To prevent various network attacks, such as attacks on IP (Internet Protocol), TCP (Transmission Control Protocol), and ICMP (Internet Control Message Protocol) packets.
- To manage network access behaviors, such as controlling access to a network or to specific resources on your network.
- To limit network traffic and improve network performance by, for example, controlling the uploading and downloading bandwidth.

1.2 Supported Features

» ACL Binding

To“permit” or “deny” received packets, bind the ACL to a port or a VLAN so that the ACL takes effect on the port or VLAN. The packets that match a permit rule or deny rule will be forwarded or dropped.

» Policy Binding

Configure Policy if you need to further process the matched packets, through operations such as mirroring, rate-limiting, redirecting, or changing priority. The Policy takes effect after it is bound to a port or a VLAN.

2 ACL Configuration

To configure ACL Binding, follow these steps:

1) Configure a time-range during which the ACL is in effect.
2) Create a Policy and configure the policy action for packets that match the ACL rule.
3) Bind the ACL to a port or VLAN to make it effective.

To configure Policy Binding, follow these steps:

1) Configure a time-range during which the ACL takes effect.
2) Create an ACL and configure the rules to filter different packets.
3) Create a Policy and configure the policy action for packets that match the ACL rule.
4) Bind the Policy to a port or VLAN to make it effective.

Configuration Guidelines

- A packet “matches” an ACL rule when it meets the rule’s matching criteria. The resulting action will be either to “permit” or “deny”the packet that matches the rule.

- If no ACL rule is configured or no matching rule is found, the packets will be forwarded without being processed by the ACL.

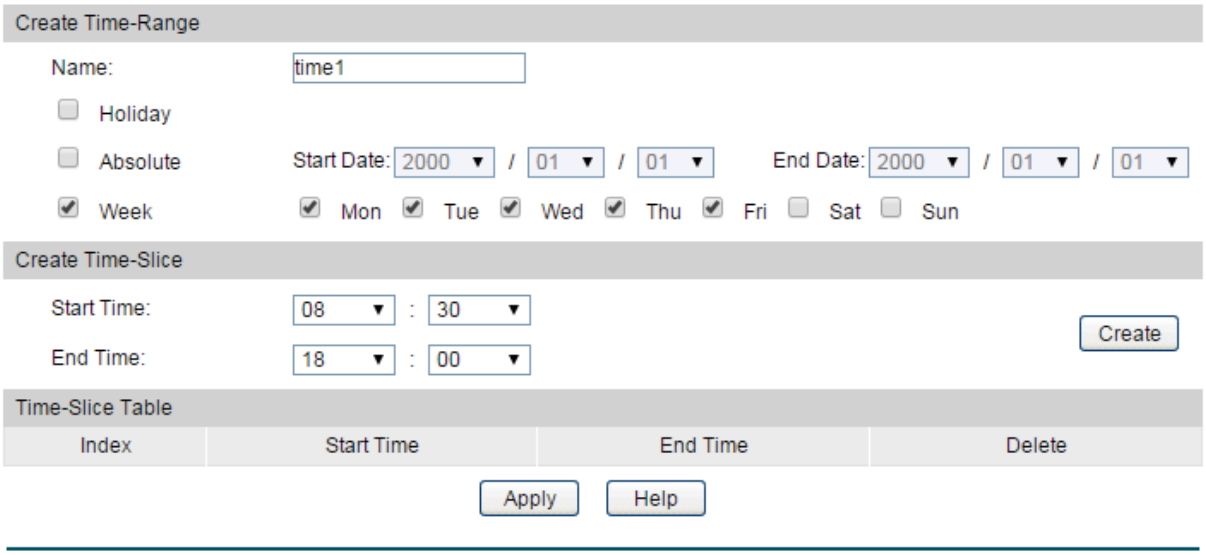
2.1 Using the GUI

2.1.1 Configuring Time-Range

Some ACL-based services or features may need to be limited to take effect only during a specified time period. In this case, you can configure time-range for the ACL.

Choose the menu **ACL > Time-Range > Time-Range Create** to load the following page.

Figure 2-1 Creating the Time-Range



Follow these steps to create the time-range:

1) In the **Create Time-Range** section, assign a name to the time-range, and then select a mode.

Name	Specify the name of the time-range.
Holiday	Configure time-range in Holiday mode. In this mode, the corresponding ACL rule takes effect only when the system date falls within the specified holiday time. For details, refer to Configuring Holiday
Absolute	Configure time-range in Absolute mode. In this mode, you can configure an absolute date range during which the corresponding ACL rule will take effect.
Week	Configure time-range in Week mode. In this mode, you can configure a cycle time range so the corresponding ACL rule will take effect on certain days each week.

2) In the **Create Time-Slice** section, configure the start and end time, then click **Create**.

Start Time / End Time	Enter the start and end time of a time-slice so that this ACL rule will take effect during specified time periods in the day.

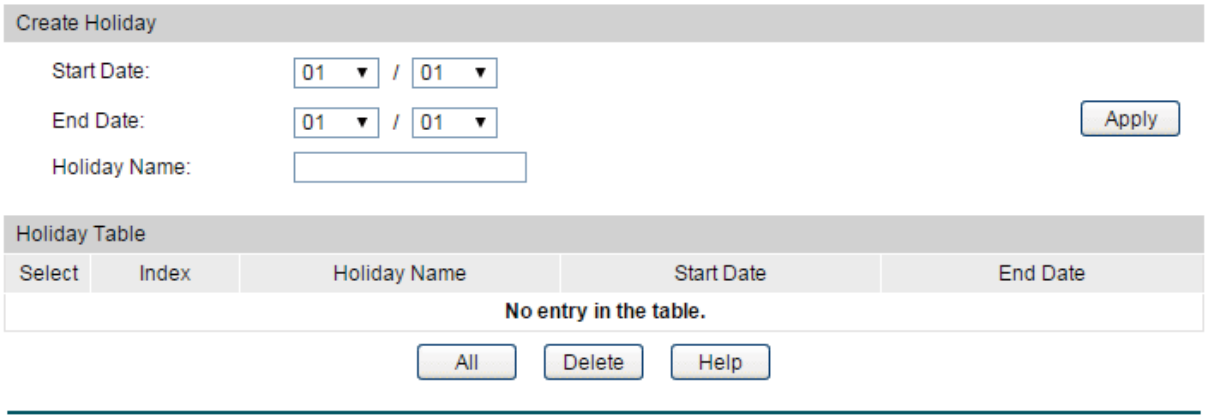
3) Click **Apply** to make the settings effective.

2.1.2 (Optional) Configuring Holiday

In Holiday mode, you need to configure specific dates for the holidays.

Choose the menu **ACL > Time-Range > Holiday Create** to load the following page.

Figure 2-2 Configuring the Holiday



Follow these steps to configure the holiday:

1) In the **Create Holiday** section, configure the start and end date, and assign a name to the holiday.

Start Date / End Date	Specify the start and end date of the holiday

2) Click **Apply** to make the settings effective.

2.1.3 Creating an ACL

You can create different types of ACL and define the rules based on source MAC or IP address, destination MAC or IP address, protocol type, port number and so on.

MAC ACL: MAC ACL uses source and destination MAC address for matching operations.

Standard-IP ACL: Standard-IP ACL uses source and destination IP address for matching operations.

Extended-IP ACL: Extended-IP ACL uses source and destination IP address, IP protocols and so on for matching operations.

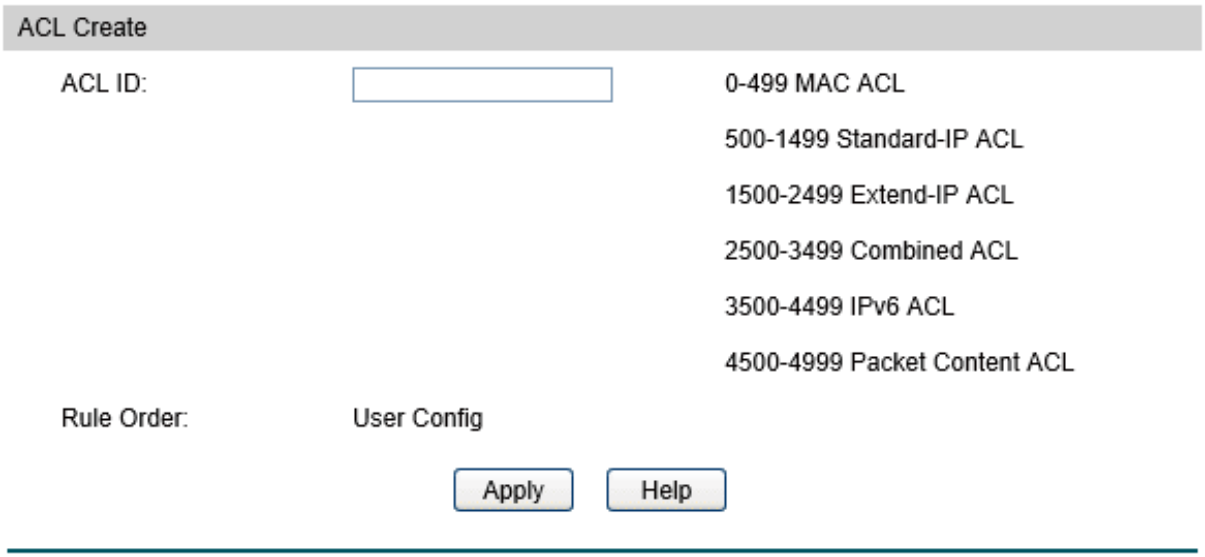
Combined ACL: Combined ACL uses source and destination MAC address, and source and destination IP address for matching operations.

IPv6 ACL: IPv6 ACL uses source and destination IPv6 address for matching operations.

Packet Content ACL: Packet Content ACL analyzes and processes 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.

Choose the menu **ACL > ACL Config > ACL Create** to load the following page.

Figure 2-3 Creating an ACL



Follow these steps to create an ACL:

1) In the **ACL Create** section, assign a name to the ACL.

ACL ID	Enter a number to identify the ACL

2) Click **Apply** to make the settings effective.

Note:

The supported ACL type and ID range varies on different switch models. Please refer to the on-screen information.

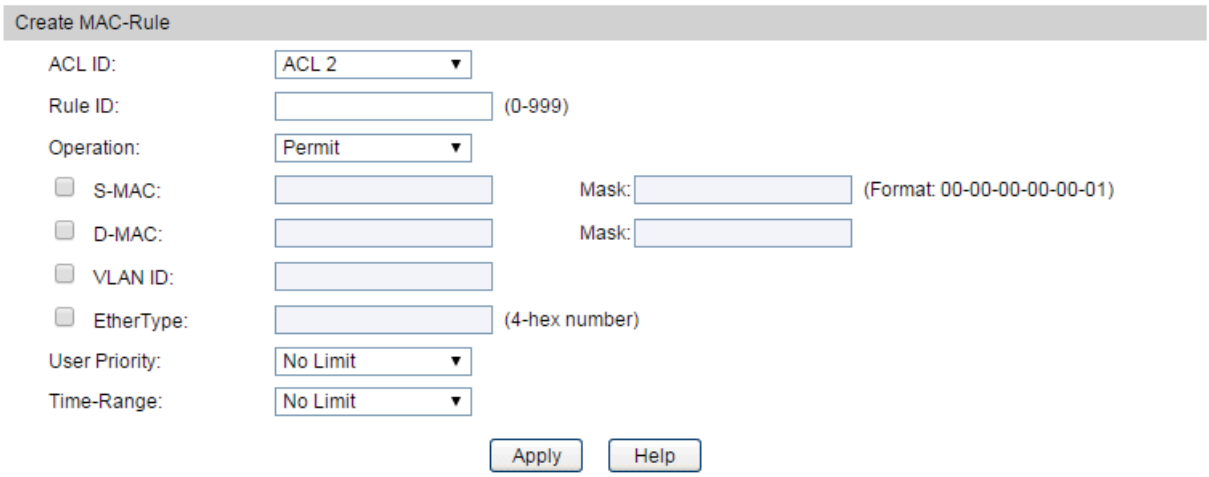
2.1.4 Configuring ACL Rules

Add rules to the ACL. For details, refer to MAC ACL Rule, Standard-IP ACL Rule, Extend-IP ACL Rule Combined ACL Rule, IPv6 ACL Rule and Packet Content ACL Rule.

Configuring the MAC ACL Rule

Choose the menu **ACL > ACL Config > MAC ACL** to load the following page.

Figure 2-4 Creating the MAC ACL



Follow these steps to create the MAC ACL:

1) Select an MAC ACL ID from the drop-down list, enter a Rule ID, then specify the operation for the matched packets.

ACL ID	Select an MAC ACL from the drop-down list.
Rule ID	Enter an ID number to identify the rule. It should not be the same as any existing MAC ACL Rule IDs.
Operation	Select an action to be taken when a packet matches the rule. **Permit**: To forward the matched packets. **Deny**: To discard the matched packets.

2) Define the rule's packet-matching criteria.

S-MAC/Mask	Enter the source MAC address with a mask. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
D-MAC/Mask	Enter the destination IP address with a mask. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
VLAN ID	Enter the ID number of the VLAN to which the ACL will apply.
EtherType	Specify the EtherType to be matched using 4 hexadecimal numbers.
User Priority	Specify the User Priority to be matched..

3) (Optional)Select a time-range from the drop-down list.

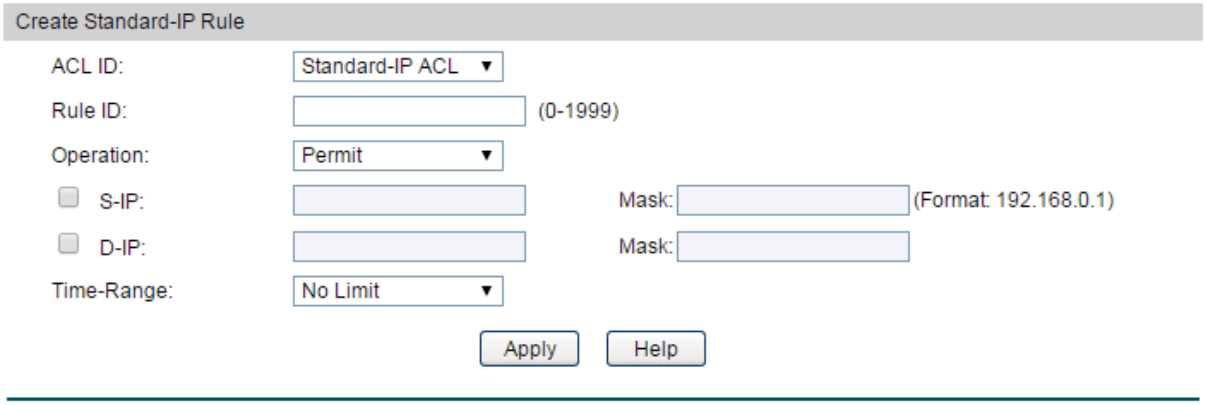
Time-Range	Select a time-range during which the rule will take effect. The default value is No Limit, which means the rule is always in effect..

4) Click **Apply** to make the settings effective.

Configuring the Standard-IP ACL Rule

Choose the menu **ACL > ACL Config > Standard-IP ACL** to load the following page.

Figure 2-5 Creating the Standard-IP ACL Rule



Follow these steps to create the Standard-IP ACL:

1) Select a Standard-IP ACL ID from the drop-down list, enter a Rule ID, then specify the operation for the matched packets.

ACL ID	Select a Standard-IP ACL from the drop-down list.
Rule ID	Enter an ID number to identify the rule. It should not be the same as any existing Standard-IP ACL Rule IDs.
Operation	Select an action to be taken when a packet matches the rule. **Permit**: To forward the matched packets. **Deny**: To discard the matched packets.

2) Define the rule's packet-matching criteria.

S-IP/Mask	Specify the source IP address with a mask. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
D-IP/Mask	Specify the destination IP address with a mask. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.

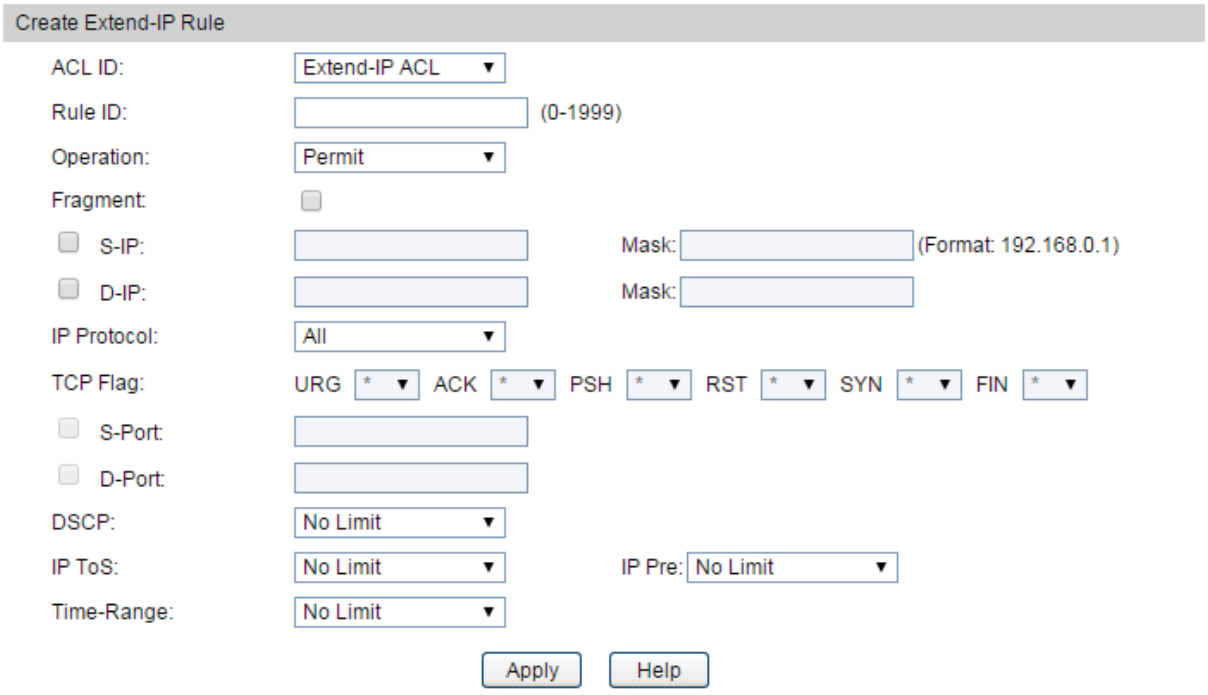
3) (Optional) Select a time-range from the drop-down list.

Time-Range	Select a time-range during which the rule will take effect. The default value is No Limit, which means the rule is always in effect.

Configuring the Extend-IP ACL Rule

Choose the menu **ACL > ACL Config > Extend-IP ACL** to load the following page.

Figure 2-6 Creating the Extend-IP ACL Rule



Follow these steps to create the Extend-IP ACL:

1) Select an Extend-IP ACL ID from the drop-down list, enter a Rule ID, then specify the operation for the matched packets.

ACL ID	Select a Extend-IP ACL from the drop-down list.
Rule ID	Enter an ID number to identify the rule. It should not be the same as any existing Extend-IP ACL Rule IDs.
Operation	Select an action to be taken when a packet matches the rule. **Permit**: To forward the matched packets. **Deny**: To discard the matched packets.

2) Define the rule's packet-matching criteria.

Fragment	Select the checkbox to make the rule valid for fragmented packets. When selected, the rule will apply to all fragmented packets and always permit to forward the last fragment of a packet.
S-IP/Mask	Specify the source IP address with a mask. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
D-IP/Mask	Specify the destination IP address with a mask. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.

IP Protocol	Select a protocol type from the drop-down list. The default is All, which indicates that packets of all protocols will be matched.
TCP Flag	If TCP protocol is selected, you can configure the TCP Flag to be used for the rule's matching operations. There are six flags and each has three options, which are *, 0 and 1. The default is *, which indicates that the flag is not used for matching operations. **URG**: Urgent flag. **ACK**: Acknowledge flag **PSH**: Push flag. **RST**: Reset flag. **SYN**: Synchronize flag. **FIN**: Finish flag
S-Port / D-Port	Enter the TCP/UDP source and destination port if TCP/UDP protocol is selected. The port number ranges from 0 to 65535.
DSCP	Specify a DSCP value to be matched between 0 and 63. The default is No Limit.
IP ToS	Specify an IP ToS value to be matched between 0 and 15. The default is No Limit.
IP Pre	Specify an IP Precedence value to be matched to be matched between 0 and 7. The default is No Limit.

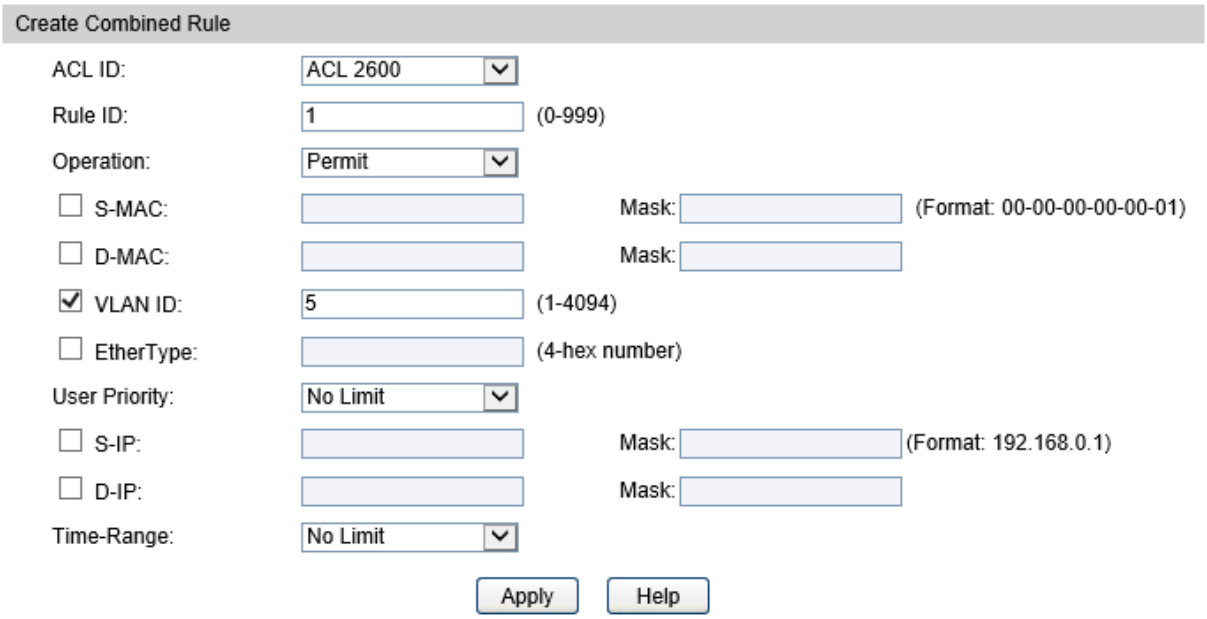
3) (Optional) Select a time-range from the drop-down list.

Time-Range	Select a time-range during which the rule will take effect. The default value is No Limit, which means the rule is always in effect.

Configuring the Combined ACL Rule

Choose the menu **ACL > ACL Config > Combined ACL** to load the following page.

Figure 2-7 Creating the Combined ACL Rule



Follow these steps to create the Combined ACL:

1) Select a Combined ACL ID from the drop-down list, enter a Rule ID, then specify the operation for the matched packets.

ACL ID	Select a Combined ACL from the drop-down list.
Rule ID	Enter an ID number to identify the rule. It should not be the same as any existing Combined ACL Rule IDs.
Operation	Select an action to be taken when a packet matches the rule. **Permit**: To forward the matched packets. **Deny**: To discard the matched packets.

2) Define the rule's packet-matching criteria.

S-MAC/Mask	Enter the source MAC address with a mask. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
D-MAC/Mask	Enter the destination IP address with a mask. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
VLAN ID	Enter the ID number of the VLAN to which the ACL will apply.
EtherType	Specify the EtherType to be matched using 4 hexadecimal numbers.
User Priority	Specify the User Priority to be matched.

S-IP/Mask	Specify the source IP address with a mask. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
D-IP/Mask	Specify the destination IP address with a mask. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.

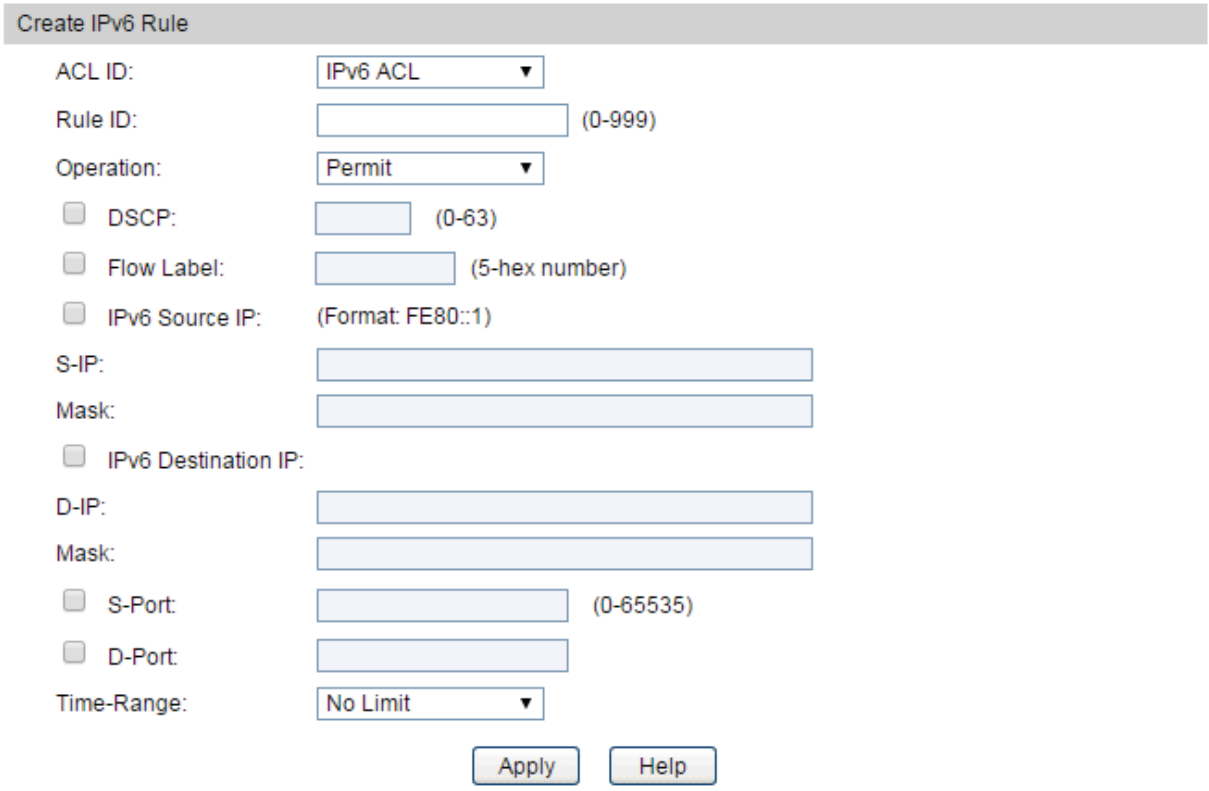
3) (Optional) Select a time-range from the drop-down list.

Time-Range	Select a time-range during which the rule will take effect. The default value is No Limit, which means the rule is always in effect.

Configuring the IPv6 ACL Rule

Choose the menu **ACL > ACL Config > IPv6 ACL** to load the following page.

Figure 2-8 Creating the IPv6 ACL Rule



Follow these steps to create the IPv6 ACL:

1) Select an IPv6 ACL ID from the drop-down list, enter a Rule ID, then specify the operation for the rule.

ACL ID	Select an IPv6 ACL from the drop-down list.
Rule ID	Enter an ID number to identify the rule. It should not be the same as any existing IPv6 ACL Rule IDs.

Operation	Select an action to be taken when a packet matches the rule. **Permit**: To forward the matched packets. **Deny**: To discard the matched packets.

2) Define the rule's packet-matching criteria.

DSCP	Specify a DSCP value to be matched.
Flow Label	Specify a Flow Label value to be matched.
IPv6 Source IP	When selected, enter the source IP address with a mask.
S-IP	Enter the source 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.
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 IP address mask specifies which bits in the source IPv6 address to match the rule. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
IPv6 Destination IP	When selected, enter the destination IPv6 address with a mask.
D-IP	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.
Mask	The mask is required if the destination IPv6 address is entered. Enter the complete mask (for example, ffff:ffff:0000:ffff). The IP address mask specifies which bits in the source IP address to match the rule. A value of 1 in the mask indicates that the corresponding bit in the address will be matched.
S-Port / D-Port	Enter the TCP/UDP source and destination port.

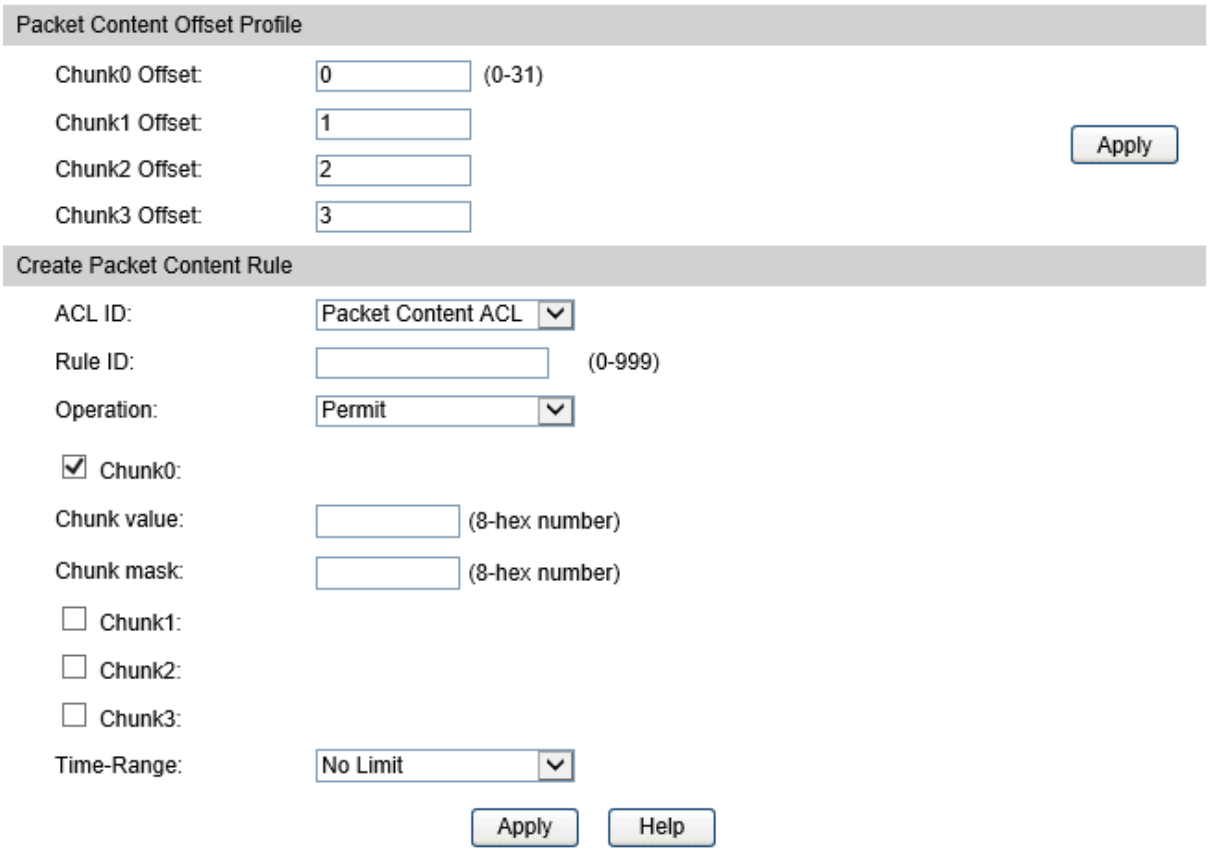
3) (Optional) Select a time-range from the drop-down list.

Time-Range	Select a time-range during which the rule will take effect. The default value is No Limit, which means the rule is always in effect.

Configuring the Packet Content ACL Rule

Choose the menu **ACL > ACL Config > Packet Content ACL** to load the following page.

Figure 2-9 Creating the Packet Content ACL Rule



Follow these steps to create the Packet Content ACL:

1) In **Packet Content Offset Profile** section, enter the offset of a chunk, all the 4 chunks must be set at the same time.

Chunk Offset	Enter the offset of a chunk, all the 4 chunks must be set at the same time. Offset 31 matches the 1, 2, 127, 128 bytes of the packet, offset 0 matches the 3,4,5,6 bytes of the packet, and so on, for the rest of the offset value.

2) In **Create Packet Content** section, select a Packet Content ACL from the drop-down list, enter a Rule ID, specify the operation for the rule, and define the rule's packet-matching criteria.

ACL ID	Select a Packet Content ACL from the drop-down list.
Rule ID	Enter an ID number to identify the rule. It should not be the same as any existing Packet Content ACL Rule IDs.
Operation	Select an action to be taken when a packet matches the rule. **Permit**: To forward the matched packets. **Deny**: To discard the matched packets.

Chunk0-Chunk3	Specify the EtherType to be matched using 4 hexadecimal numbers.
Chunk Value	Enter the 4-byte value in hexadecimal for the desired chunk, like '0000ffff'. The Packet Content ACL will check this chunk of packets to examine if the packets match the rule or not.
Chunk mask	Enter the 4-byte mask in hexadecimal for the desired chunk. The mask must be written completely in 4-byte hex mode, like '0000ffff'. The mask specifies which bits to match the rule.

3) (Optional) Select a time-range from the drop-down list.

Time-Range	Select a time-range during which the rule will take effect. The default value is No Limit, which means the rule is always in effect.

View the Rule Table

The rules in an ACL are listed in ascending order of configuration time, regardless of their rule IDs. By default, a rule configured earlier is listed before a rule configured later.

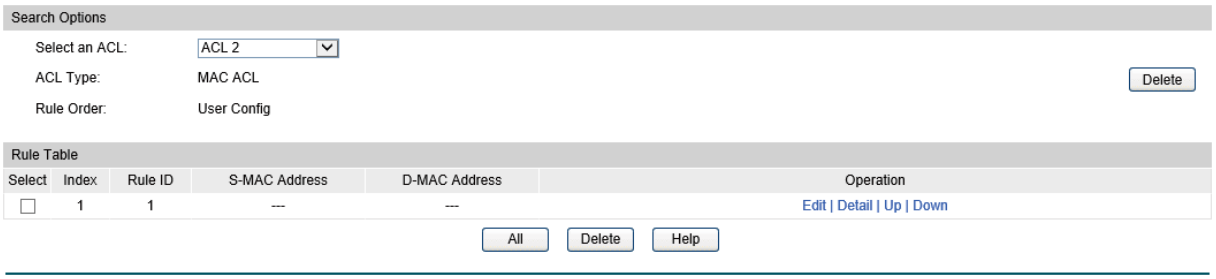
The switch matches a received packet with the rules in order. When a packet matches a rule, the device stops the match process and performs the action defined in the rule.

In the ACL rule table, you can view all the ACLs and their rules.

You can also delete an ACL or an ACL rule, or change the matching order if needed.

Choose the menu **ACL > ACL Config > ACL Summary** to load the following page.

Figure 2-10 ACL Information



2.1.5 Configuring Policy

Policy allows you to further process the matched packets through operations such as mirroring, rate-limiting, redirecting, or changing priority.

To configure the policy, follow these steps:

1) Create a policy.
2) Configure the action of the policy

Creating a Policy

Choose th menu **ACL > Policy Config > Policy Create** to load the following page.

Figure 2-11 Creating a Policy



Follow these steps to create a policy:

Enter a policy name, then click **Apply**.

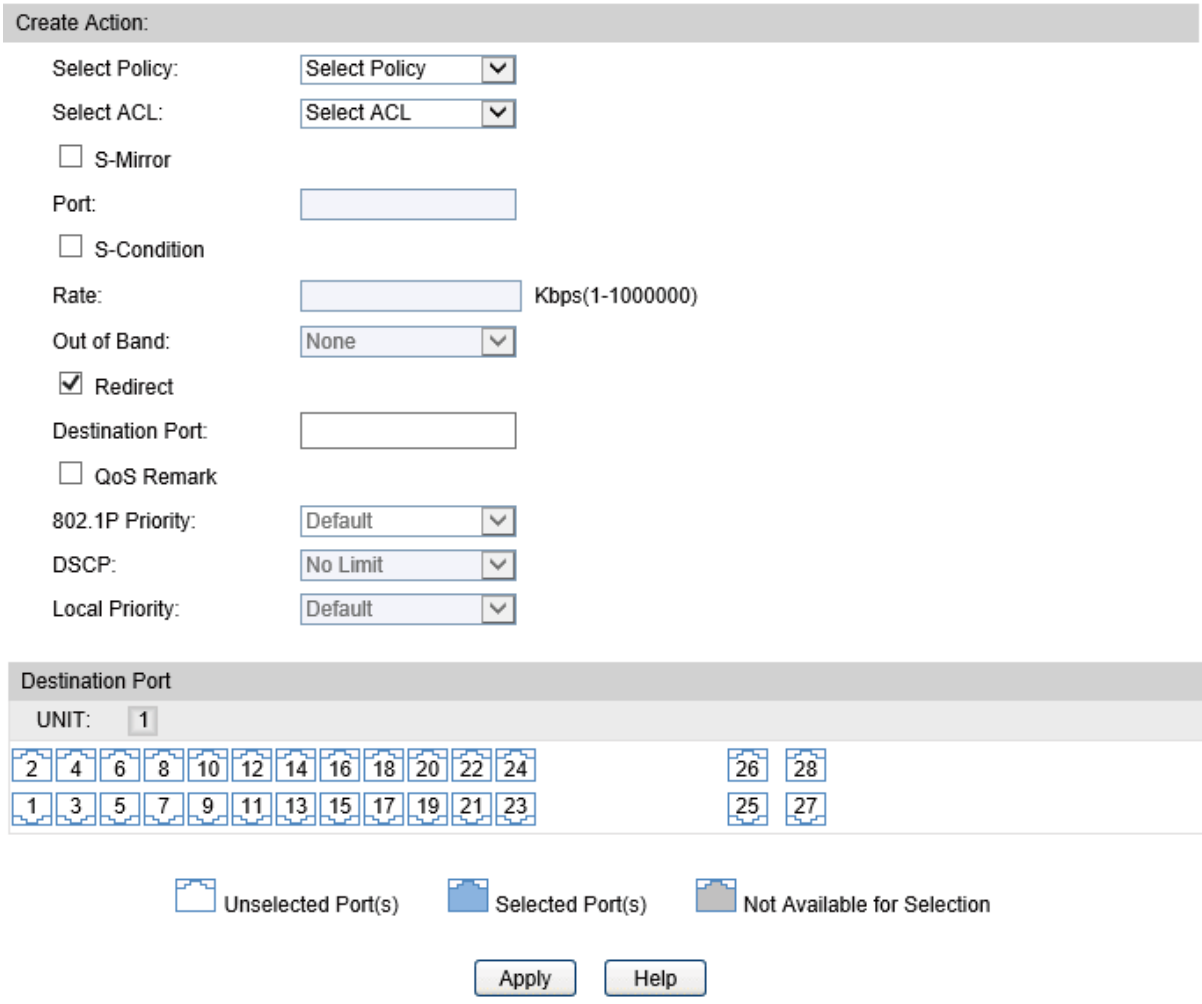
Policy Name	Enter a Policy Name between 1 and 16 characters.

Configuring the Action of the Policy

Apply an ACL to the policy and specify the action to be taken for the matched packets.

Choose the menu **ACL > Policy Config > Action Create** to load the following page.

Figure 2-12 Configuring the Action of the Policy



Follow these steps to configure the action of the policy:

1) Select your preferred policy and ACL.

Select Policy	Select a policy from the drop-down list.
Select ACL	Select an ACL to be applied to the policy.

2) Configure the actions to be taken for the matched packets.

S-Mirror	Configure port mirroring for the matched packets. Enter a destination port to which the packets will be mirrored.
Port	Enter a destination port.
S-Condition	Configure rate limiting for the matched packets.

Rate	Specify the transmission rate for the matched packets.
Out of Band	Select either “none” or “discard” as the action to be taken for packets whose rate is beyond the specified rate.
Redirect	Configure the redirect action for the matched packets.
Destination Port	Select a destination port to which the packets will be redirected.
QoS Remark	Configure QoS action for the matched packets.
802.1P Priority	Specify the 802.1p priority for the matched packets.
DSCP	Specify the DSCP region for the matched packets.
Local Priority	Specify the local priority for thematched packets.

3) Click **Apply** to make the settings effective.

2.1.6 Configuring the ACL Binding and Policy Binding

You can select ACL binding or Policy binding according to your needs.

An ACL or policy takes effect only after it is bound to a port or VLAN.

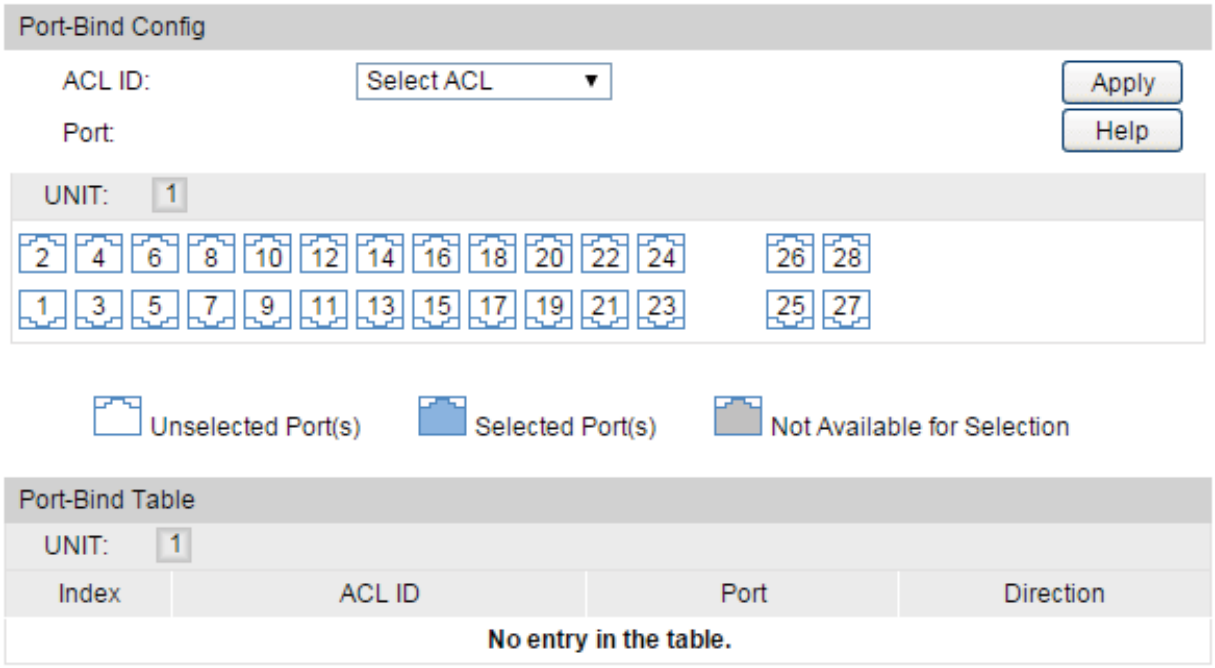
Configuring the ACL Binding

You can bind the ACL to a port or a VLAN. The received packets will then be matched and processed according to the ACL rules.

- Binding the ACL to a Port

Choose the menu **ACL > ACL Binding > Port Binding** to load the following page.

Figure 2-13 Binding the ACL to a Port



Follow these steps to bind the ACL to a Port:

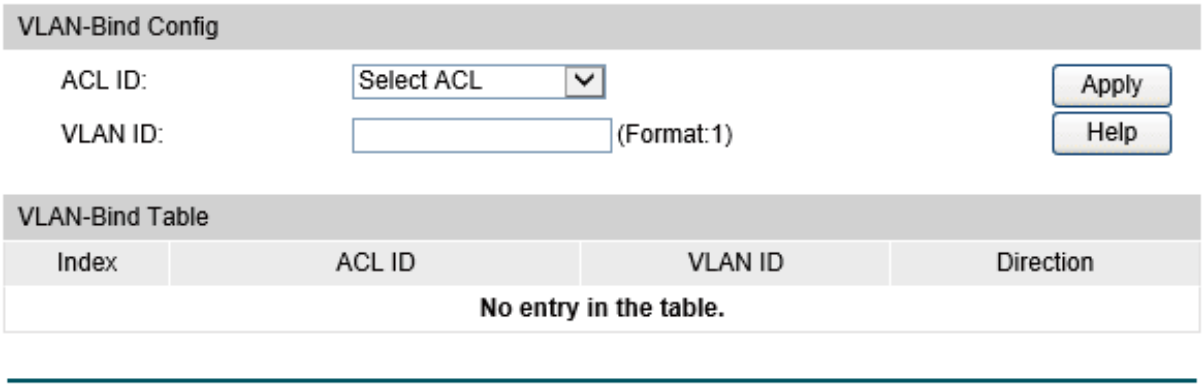
Select the ACL and the port, and click **Apply**.

ACL ID	Select an ACL from the drop-down list.

Binding the ACL to a VLAN

Choose the menu **ACL > ACL Binding > VLAN Binding** to load the following page.

Figure 2-14 Binding the ACL to a VLAN



Follow these steps to bind the ACL to a VLAN:

Select the ACL and enter the VLAN ID, and click **Apply**.

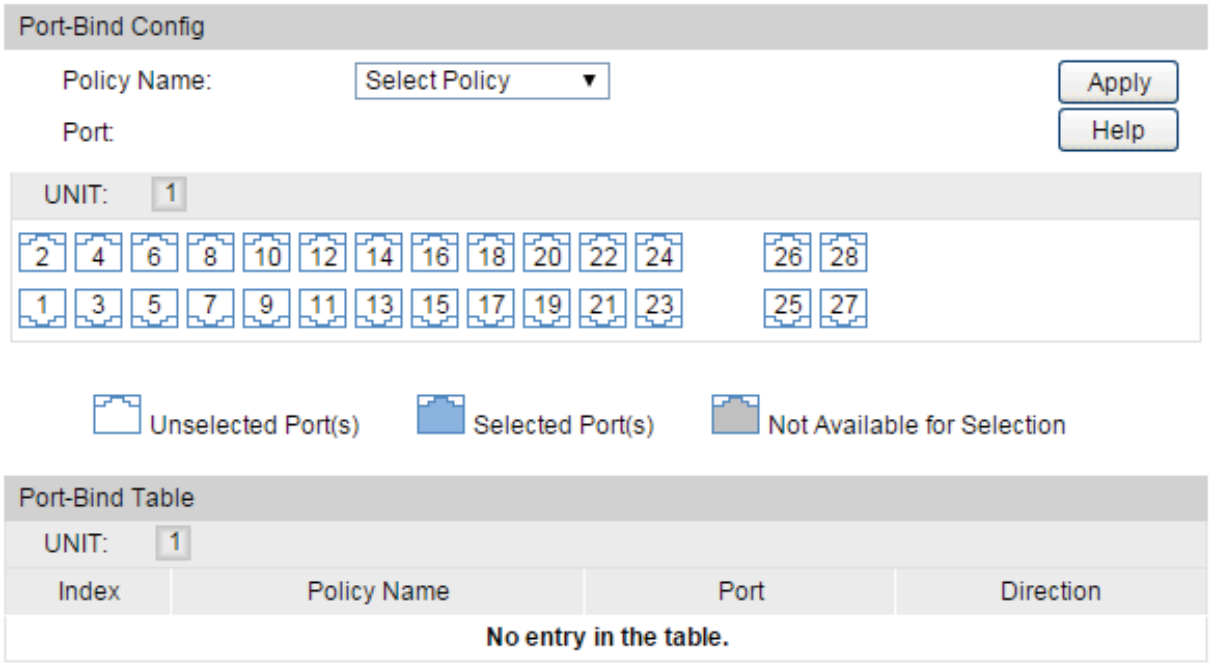
ACL ID	Select an ACL from the drop-down list. **Note**: Packet Content ACLs cannot be bound to any VLANs.
VLAN ID	Enter the VLAN ID.

Configuring the Policy Binding

You can bind the policy to a port or a VLAN. The received packets will then be matched and processed according to this policy.

■ Binding the Policy to a Port

Figure 2-15 Binding the policy to a Port



Follow these steps to bind the policy to a Port:

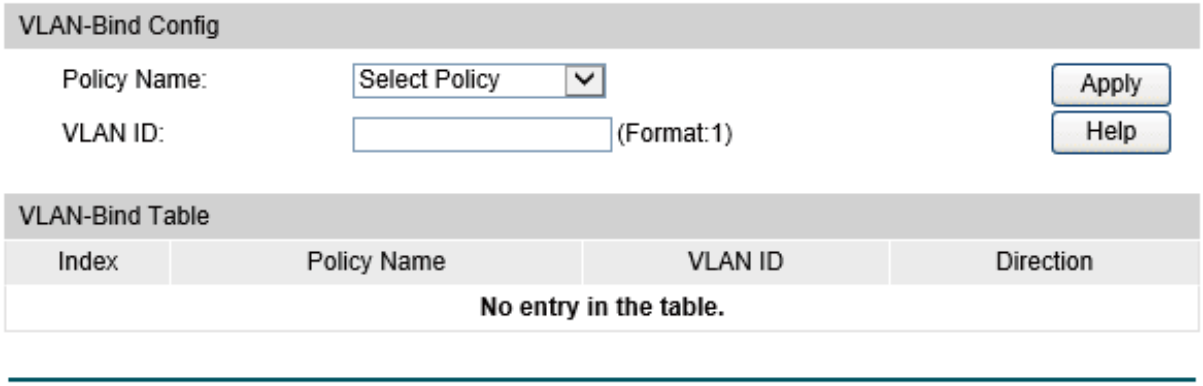
Select the policy and the port to be bound, and click **Apply**.

Policy Name	Select a Policy from the drop-down list.

■ Binding the Policy to a VLAN

Choose the menu **ACL > Policy Binding > VLAN Binding** to load the following page.

Figure 2-16 Binding the Policy to a VLAN



Follow these steps to bind the policy to a VLAN:

Select the ACL and enter the VLAN ID, and click **Apply**.

ACL ID	Select an ACL from the drop-down list. **Note**: Packet Content ACLs cannot be bound to any VLANs.
VLAN ID	Enter the VLAN ID.

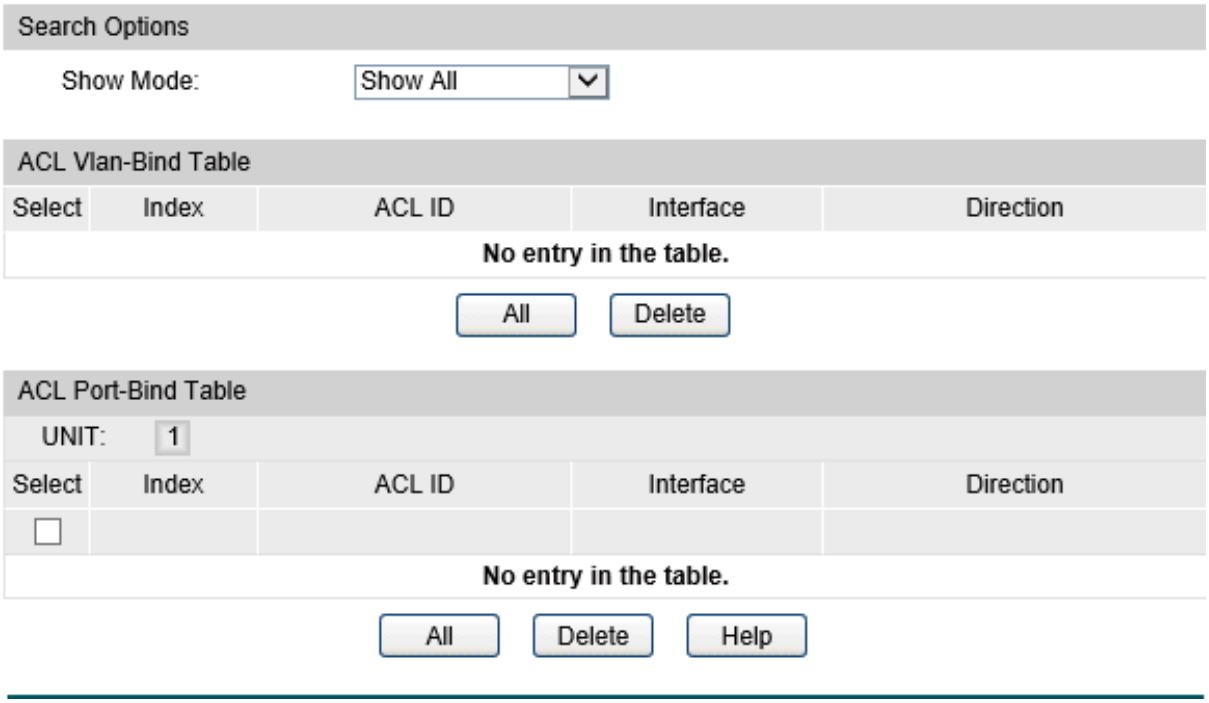
Verifying the Binding Configuration

Verifying the ACL Binding

You can view both port binding and VLAN binding entries in the table. You can also delete existing entries if needed.

Choose the menu **ACL > ACL Binding > Binding Table** to load the following page.

Figure 2-17 Verifying the ACL Binding

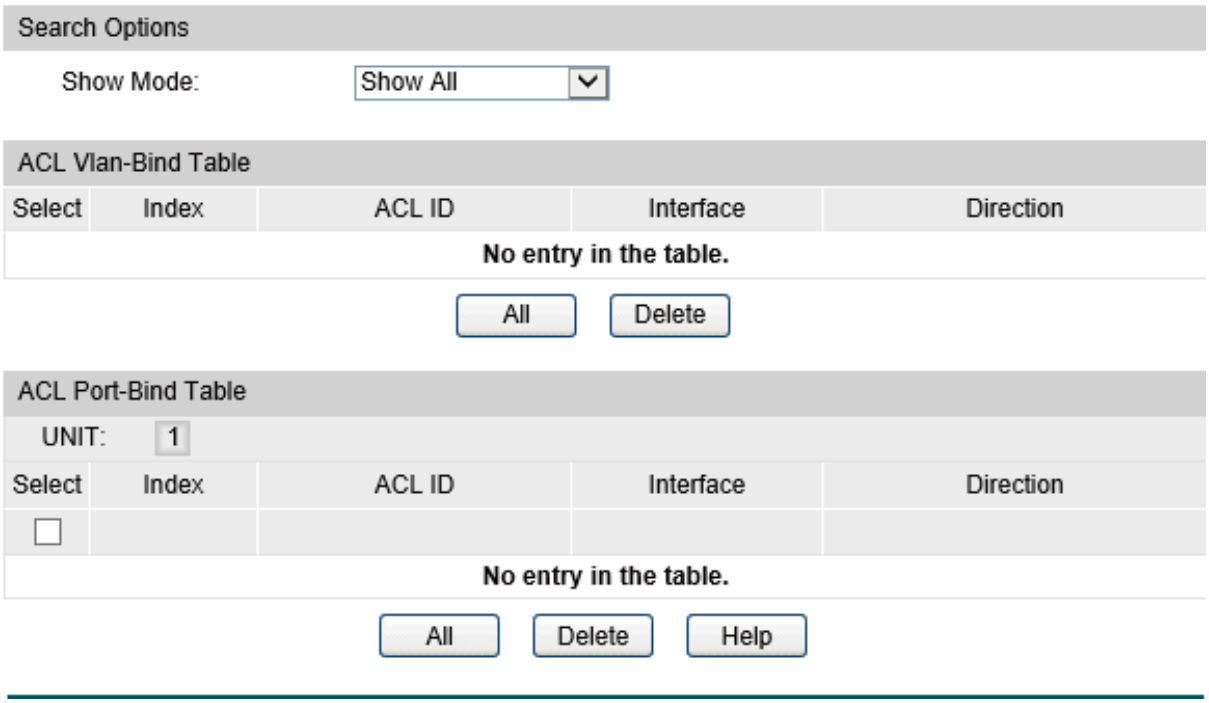


Verifying the Policy Binding

You can view both port binding and VLAN binding entries in the table. You can also delete existing entries if needed.

Choose the menu **ACL > Policy Binding > Binding Table** to load the following page.

Figure 2-18 Verifying the Policy Binding



2.2 Using the CLI

2.2.1 Configuring Time Range

Some services or features that use ACL need to be limited to a specified time period. In this case, you can configure time-range for the ACL.

Step 1	**configure** Enter global configuration mode.
Step 2	**time-range** *name* Add a time-range to make a rule effective only during a specified time period. *name*: Assign a name to the time-range using 1-16 characters.

Step 3	**absolute start** *start-date* **end** *end-date* (Optional) Configure time-range in Absolute mode. In this mode, the rule takes effect only during a specified period of time. *start-date:* Specify the start date in MM/DD/YYYY format. The default is 01/01/2000. *end-date:* Specify the start date in MM/DD/YYYY format. The default is 01/01/2000 **periodic** [**week-date** *week-day*] [**time-slice1** *time-slice*] [**time-slice2** *time-slice*] [**time-slice3** *time-slice*] [**time-slice4** *time-slice*] (Optional) Configure time-range in Week mode. In this mode, the rule takes effect only on certain days each week. *week-day:* Specify the cycle time range. You can enter 1-3,6 or descriptions such as daily, off-day or working-day. 1-3, 6 indicates Monday, Tuesday,Wednesday and Saturday; daily indicates every day; off-day indicates Saturday and Sunday, and working-day indicates Monday to Friday. By default, Week mode is disabled. *time-slice*: Add a time-slice in HH:MM-HH:MM format. You can add a maximum of four time-slices to each time-range. **holiday** (Optional) Configure time-range in Holiday mode. In this mode, the ACL rule is effective only during specified holiday times.
Step 4	**exit** Return to global configuration mode.
Step 5	**holiday** *name* **start-date** *start-date* **end-date** *end-date* In Holiday mode, specify the start and end date of the holiday time. *name*: Assign a name to the holiday using 1-16 characters. *start-date*: Specify the start date in MM/DD format, for example 05/01. *end-date*: Specify the end date in MM/DD format, for example 05/03
Step 6	**show time-range** (Optional) Display all time-range configurations. **show holiday** (Optional) Display all defined holiday times.
Step 7	**end** Return to privileged EXEC mode.
Step 8	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure time-range in Week mode. The ACL only takes effect at 08:30 am to 18:00 pm on Monday to Friday:

Switch#configure

Switch(config)#time-range work_time

Switch(config-time-range)#periodic week-date 1-5 **time-slice1** 08:30-18:00

Switch(config-time-range)#exit

Switch(config)#show time-range

Time-range entry: work_time(inactive)

periodic time-slice 08:30-18:00

periodic week-day 1,2,3,4,5

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Configuring ACL

Follow the steps to create different types of ACL and configure the ACL rules.

You can define the rules based on source or destination IP address, source or destination MAC address, protocol type, port number and others.

■ MAC ACL

Step 1	**configure** Enter global configuration mode.
Step 2	**mac access-list** *access-list-num* Input a MAC ACL ID to enter MAC Access-list mode. If it is a new ID , the ACL will be created before entering MAC Access-list mode. *access-list-num*: Enter an ACL ID between 0 and 499.

Step 3	**rule** *rule-id* {deny | permit} [[**smac** *source-mac*] **smask** *source-mac-mask*] [[**dmac** *destination-mac*] **dmask** *destination-mac-mask*] [**vid** *vlan-id*] [**type** ethernet-type] [**pri** *user-pri*] [**tseg** *time-segment*] Add a MAC ACL Rule. *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. *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. *vlan-id*: The VLAN ID ranges from 1 to 4094. ethernet-type: Specify an Ethernet-type with 4 hexadecimal numbers. *user-pri*: The user priority ranges from 0 to 7. The default is No Limit. *time-segment*: The name of the time-range. The default is No Limit.
Step 4	**exit** Return to global configuration mode.
Step 5	**show access-list** [*access-list-num*] Display the current ACL configuration. *access-list-num*: The ID number of the ACL.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create MAC ACL 50 and configure Rule 5 to permit packets with source MAC address 00:34:a2:d4:34:b5:

Switch#configure

Switch(config)#mac access-list 50

Switch(config-mac-acl)#rule 5 **permit smac** 00:34:a2:d4:34:b5 smask ff:ff:ff:ff:ff:ff

Switch(config-mac-acl)#exit

Switch(config)#show access-list 50

mac access list 50

rule 5 permit smac 00:34:a2:d4:34:b5 smask ff:ff:ff:ff:ff:ff

Switch(config)#end

Switch#copy running-config startup-config

■ Standard-IP ACL

Step 1	**configure** Enter global configuration mode.
Step 2	**access-list create** *access-list-num* Create an Standard-IP ACL. *access-list-num*: Enter an ACL ID. The ID ranges from 500 to 1499.
Step 3	**access-list standard** *acl-id* **rule** *rule-id* **{** deny **|** permit **} [[sip** *source-ip* **] smask** *source-ip-mask***] [[dip** *destination-ip* **] dmask** *destination-ip-mask* **] [tseg** *time-segment* **]** Add rules to the ACL. *acl-id:* The ID number of the ACL you have created. *rule-id*: Assign an ID to the rule. It cannot be the same as the existing Standard-IP Rule IDs. 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. *source-ip:* Enter the source IP address. *source-ip-mask*: Enter the mask of the source IP address. This is required if a source IP address is entered. *destination-ip:* Enter the destination IP address. *destination-ip-mask:* Enter the mask of the destination IP address. This is required if a destination IP address is entered. *time-segment:* The name of the time-range. The default is No Limit. **frag:** 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.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create Standard-IP ACL 600, and configure Rule 1 to permit packets with source IP address 192.168.1.100:

Switch#configure

Switch(config)#access-list create 600

Switch(config)#access-list standard 600 **rule** 1 **permit sip** 192.168.1.100 **smask** 255.255.255.255

Switch(config)#show access-list 600

Standard IP access list 600

rule 1 permit sip 192.168.1.100 smask 255.255.255.255

Switch(config)#end

Switch#copy running-config startup-config

■ Extend-IP ACL

Step 1	**configure** Enter global configuration mode.
Step 2	**access-list create** *access-list-num* Create an Extend-IP ACL *access-list-num*: Enter an ACL ID. The ID ranges from 1500 to 2499.

Step 3	**access-list extended** *acl-id* **rule** *rule-id* {deny | permit} [[**sip** source-ip] **smask** *source-ip-mask*] [[**dip** *destination-ip*] **dmask** *destination-ip-mask*] [**tseg** *time-segment*] [**frag** {disable | enable}] [**dscp** *dscp*] [**s-port** *s-port*] [**d-port** *d-port*] [**tcpflag** *tcpflag*] [**protocol** *protocol*] [**tos** *tos*] [**pre** *pre*] Add a rule for the ACL. *acl-id:* The ID number of the ACL you have created. *rule-id:* Assign an ID to the rule. It cannot be the same as the existing Extend-IP ACL Rule IDs. 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. *source-ip:* Enter the source IP address. *source-ip-mask:* Enter the mask of the source IP address. This is required if a source IP address is entered. *destination-ip:* Enter the destination IP address. *destination-ip-mask:* Enter the mask of the destination IP address. This is required if a destination IP address is entered. *time-segment:* The name of the time-range. The default is No Limit. **frag**: 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. *dscp:* Specify the DSCP value between 0 and 63. *s-port:* Enter the TCP/UDP source port if TCP/UDP protocol is selected. *d-port:* Enter the TCP/UDP destination port if TCP/UDP protocol is selected. *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) *protocol:* Specify a protocol type. *tos:* Specify the IP ToS to be matched. *pre:* Specify the IP Precedence to be matched.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create Extend-IP ACL 1700 and configure Rule 7 to deny Telnet packets with source IP192.168.2.100:

Switch#configure

Switch(config)#access-list create 1700

Switch(config)#access-list extended 1700 **rule** 7 **deny sip** 192.168.2.100 **smask** 255.255.255.255 **protocol** 6 **d-port** 23

Switch(config)#show access-list 1700

Extended IP access list 1700

rule 7 deny sip 192.168.2.100 smask 255.255.255.255 protocol 6 d-port 23

Switch(config)#end

Switch#copy running-config startup-config

■ Combined ACL

Step 1	**configure** Enter global configuration mode
Step 2	**access-list create** *access-list-num* Create a Combined ACL. *access-list-num*: Enter an ACL ID. The ID ranges from 2500 to 3499.
Step 3	**access-list combined** *acl-id* **rule** *rule-id* [permit|deny] [[**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** *dest-ip-address*] [**dip-mask** *dest-ip-mask*]] [**frag** {disable | enable}] [**tseg** *time-segment*] Add rules to the ACL. *acl-id*: The ID number of the ACL you have created. *rule-id*: Assign an ID to the rule. It should not be the same as any existing Combined ACL Rule IDs. permit|deny: 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. 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. ethertype: 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. **frag**: 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 . *time-segment*: The name of the time-range. The default is No Limit.

Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create Combined ACL 2600 and configure Rule 1 to deny packets with source IP address 192.168.3.100 in VLAN 2:

Switch#configure

Switch(config)#access-list create 2600

Switch(config)#access-list combined 2600 **rule** 1 **permit vid** 2 **sip** 192.168.3.100 **sip-mask** 255.255.255.255

Switch(config)#show access-list 2600

Combined access list 2600

rule 1 permit vid 2 sip 192.168.3.100 sip-mask 255.255.255.255

Switch(config)#end

Switch#copy running-config startup-config

- **IPv6 ACL**

Step 1	**configure** Enter global configuration mode
Step 2	**access-list ipv6** *access-list-num* Create an IPv6 ACL. *access-list-num*: Enter an ACL ID. The ID ranges from 3500 to 4499.

Step 3	**access-list ipv6** *acl-id* **rule** *rule-id* {permit | deny}[**dscp** *dscp-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-segment-name*] Add rules to the ACL. *acl-id:* The ID number of the ACL you have created. *rule-id:* Assign an ID to the rule. It should not be the same as any existing IPv6 Rule IDs. permit | deny: 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. *dscp-value*: Specify a DSCP value to be matched. *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-segment-name*: The name of the time-range. The default is No Limit.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create IPv6 ACL 3600 and configure Rule 1 to deny packets with source IPv6 address CDCD:910A:2222:5498:8475:1111:3900:2020:

Switch#configure

Switch(config)#access-list create 3600

Switch(config)#access-list ipv6 3600 **rule** 1 **deny sip** CDCD:910A:2222:5498:8475:1111:3900:2020 sip-mask ffff:ffff:ffff:ffff

Switch(config)#show access-list 3600

IPv6 access list 3600

rule 1 deny sip cdcd:910a:2222:5498:8475:1111:3900:2020 sip-mask ffff:ff

ff:ffff:ffff

Switch(config)#end

Switch#copy running-config startup-config

■ Packet Content ACL

Step 1	**configure** Enter global configuration mode
Step 2	**access-list create** *access-list-num* Create a Packet Content ACL. *access-list-num*: Enter an ACL ID. The ID ranges from 4500 to 4999.
Step 3	**access-list packet-content profile chunk-offset0** *offset0* **chunk-offset1** *offset1* **chunk-offset2** *offset2* **chunk-offset3** *offset3* Specify the offset of each chunk, all the 4 chunks must be set at the same time. *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 1, 2,127,128 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.
Step 4	**access-list packet-content config** *acl-id* **rule** *rule-id* **{**deny | permit**} [chunk0** *value* **mask0** *mask***] [chunk1** *value* **mask1** *mask***] [chunk2** *value* **mask2** *mask***] [chunk3** *value* **mask3** *mask***] [tseg** *tseg-name***]** Add rules to the ACL. *acl-id:* The ID number of the ACL you have created. *rule-id:* Assign an ID to the rule. It should not be the same as any existing Packet Content Rule IDs. permit | deny: 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. *value***:** Enter the 4-byte value in hexadecimal for the desired chunk, like '0000ffff'. The Packet Content ACL will check this chunk of packets to examine if the packets match the rule or not. *mask:* Enter the 4-byte mask in hexadecimal for the desired chunk. The mask must be written completely in 4-byte hex mode, like '0000ffff'. The mask specifies which bits to match the rule. *time-segment-name*: The name of the time-range. The default is No Limit.
Step 5	**end** Return to privileged EXEC mode.

Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create Packet Content ACL 4500, and deny the packets with the value of its chunk1 0x58:

Switch#configure

Switch(config)#access-list create 4500

Switch(config)#access-list packet-content profile chunk-offset0 offset0 **chunk-offset1** offset1 **chunk-offset2** offset2 **chunk-offset3** offset3

Switch(config)#packet-content config 4500 **rule** 10 deny **chunk**1 58 **mask1** ffffffff

Switch(config)#show access-list 4500

Packet content access list 4500

rule 10 deny chunk1 value 0x58 mask 0xffffffff

Switch(config)#end

Switch#copy running-config startup-config

2.2.3 Configuring Policy

Policy allows you to further process the matched packets through operations such as mirroring, rate-limiting, redirecting, or changing priority.

Follow the steps below to create a policy and configure the policy actions.

Step 1	**configure** Enter global configuration mode
Step 2	**access-list policy name** *name* Create a policy and assign it a name. *name*: Assign the policy a name with 1 to 16 characters.
Step 3	**access-list policy action** *policy-name acl-id* Apply an ACL to the policy. *policy-name*: The name of the policy. *acl-id*: The ID number of the ACL to be applied.

Step 4	**redirect interface** { **fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* } (Optional) Define the policy to redirect the matched packets to the desired port. *port*: The destination port to which the packets will be redirected. The default is All. **s-mirror interface** { **fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* } (Optional) Define the policy to mirror the matched packets to the desired port. *port*: The destination port to which the packets will be mirrored **s-condition rate** *rate* **osd** { none | discard } (Optional) Define the policy to monitor the rate of the matched packets *rate*: Specify a rate from 1 to 1000000 kbps. osd: Select either "none" or "discard" as the action action to be taken for the packets whose rate is beyond the specified rate. The default is None. **qos-remark dscp** *dscp* **priority** *pri* **dot1p** *pri* (Optional) Define the policy to remark priority for the matched packets. *dscp*: Specify the DSCP region for the data packets. The value ranges from 0 to 63. **priority** *pri*: Specify the local priority for the data packets. The value ranges from 0 to 7. **dot1p** *pri:* Specify the 802.1p priority for the data packets. The value ranges from 0 to 7.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

Create policy RD, apply ACL 600 to policy RD, and redirect the matched packets to port 1/0/4:

Switch#configure

Switch(config)#access-list policy name RD

Switch(config)#access-list policy action RD 600

Switch(config-action)#redirect interface gigabitEthernet 1/0/4

Switch(config-action)#exit

Switch(config)#show access-list policy RD

Policy name : RD

access-list 600 redirect-port Gi1/0/4

Switch(config)#end

Switch#copy running-config startup-config

2.2.4 ACL Binding and Policy Binding

You can select ACL binding or Policy binding according to your needs. An ACL Rule and policy takes effect only after they are bound to a port or VLAN.

- Policy Binding

You can bind the policy to a port or a VLAN, then the received packets will be matched and operated based on the policy.

Step 1	**configure** Enter global configuration mode
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** **access-list bind** *policy-name* (Optional) Enter layer 2 interface configuration mode and bind the policy to the port. *port*: The port to which the policy will bind. *policy-name*: The name of the policy. **interface vlan** *vlan-id* **access-list bind** *policy-name* (Optional) Enter layer 3 interface configuration mode and bind the policy to the VLAN. **Note**: Packet Content ACLs cannot be bound to any VLANs. *vlan-id*: The VLAN to which the policy will bind. *policy-name*: The name of the policy.
Step 3	**end** Return to privileged EXEC mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to bind policy 1 to port 2 and policy 2 to VLAN 2:

Switch#configure

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

Switch(config-if)#access-list bind 1

Switch(config-if)#exit

Switch(config)#interface vlan 2

Switch(config-if)#access-list bind 2

Switch(config-if)#exit

Switch(config)#show access-list bind

Index	Policy Name	Interface/VID	Direction	Type
-----	----------	----------	--------	----
1	1	Gi1/0/2	Ingress	Port
2	2	2	Ingress	Vlan
Index	ACL ID	Interface/VID	Direction	Type
-----	----------	----------	--------	----

Switch(config)#end

Switch#copy running-config startup-config

- ACL Binding

You can bind the ACL to a port or a VLAN. The received packets will then be matched and processed according to the ACL rules.

Step 1	**configure** Enter global configuration mode
Step 2	**interface** { **fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* } **access-list bind acl** *acl-id* (Optional) Enter layer 2 interface configuration mode and bind the ACL to the port. *port*: The port to which the ACL will bind. *acl-id*: The ID number of the ACL. **interface vlan** *vlan-id* **access-list bind acl** *acl-id* (Optional) Enter layer 3 interface configuration mode and bind the ACL to the VLAN. **Note**: Packet Content ACLs cannot be bound to any VLANs. *vlan-id*: The VLAN to which the ACL will bind. *acl-id*: The ID number of the ACL.
Step 3	**end** Return to privileged EXEC mode.

Step 4	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to bind ACL 1 to port 3 and ACL 2 to VLAN 4:

Switch#configure

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

Switch(config-if)#access-list bind acl 1

Switch(config-if)#exit

Switch(config)#interface vlan 4

Switch(config-if)#access-list bind acl 2

Switch(config-if)#exit

Switch(config)#show access-list bind

Index	Policy Name	Interface/VID	Direction	Type
-----	----------	----------	--------	----
Index	ACL ID	Interface/VID	Direction	Type
-----	----------	----------	-------	----
1	1	Gi1/0/3	Ingress	Port
2	2	4	Ingress	Vlan

Switch(config)#end

Switch#copy running-config startup-config

3 Configuration Example for ACL

3.1 Network Requirements

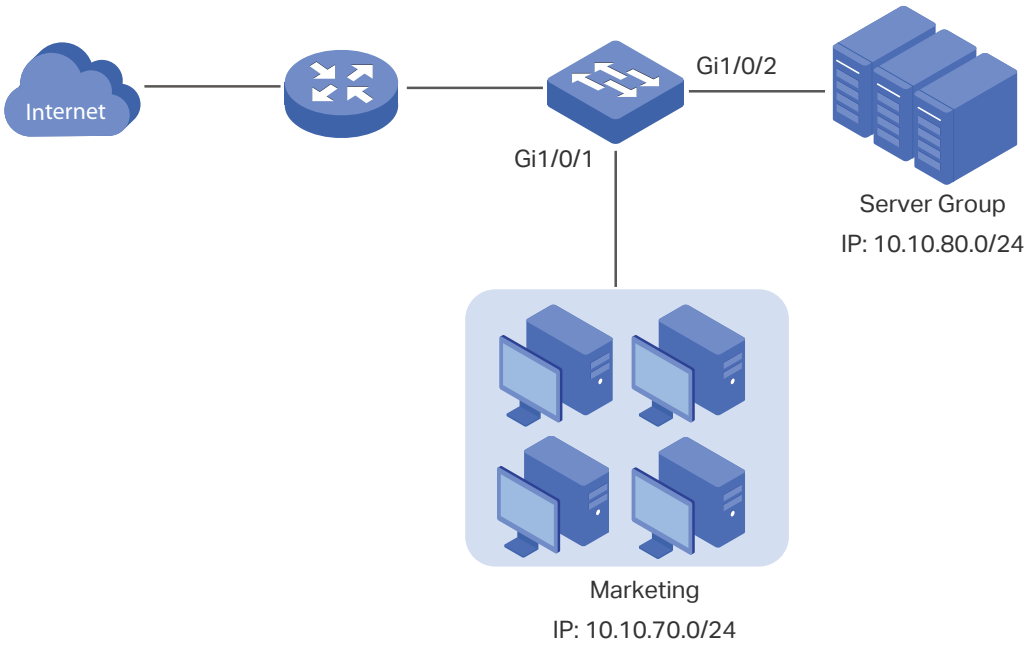
A company's internal server group can provide different types of services. It is required that:

- the Marketing department can only access internal server group in the intranet.
- the Marketing department can only visit http and https websites on the internet.

3.2 Network Topology

As is shown below, computers in the Marketing department are connected to the switch via port 1/0/1 , and the internal server group is connected to the switch via port 1/0/2.

Figure 3-1 Network Topology



3.3 Configuration Scheme

To meet the requirements above, you can set up packet filtering by creating an Extend-IP ACL and configuring rules for it.

- Configuring ACL

1) Configure a permit rule to match packets with source IP address 10.10.70.0/24, and destination IP address 10.10.80.0/24. This rule allows the Marketing department to access internal network servers from intranet.
2) Configure permit rules to match the packets with source IP address 10.10.70.0/24, and destination ports TCP 80, TCP 443 and TCP/UDP 53. These allow the Marketing department to visit http and https websites on the internet.
3) Configure a deny rule to match the packets with source IP address 10.10.70.0. This rule blocks other network services.

The switch matches the packets with the rules in order, starting with Rule 1. If a packet matches a rule, the switch stops the matching process and initiates the action defined in the rule.

- Binding Configuration

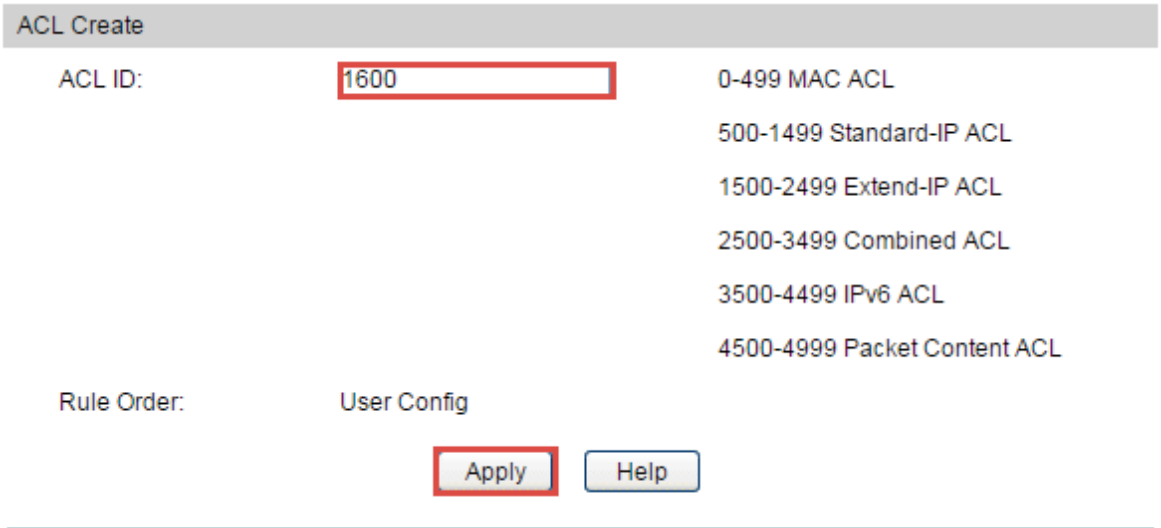
Apply the Extend-IP ACL to a Policy and bind the Policy to port 1/0/1 so that the ACL rules will apply to the Marketing department only.

Demonstrated with T2600G-28TS, the following sections explain the configuration procedure in two ways: using the GUI and using the CLI.

3.4 Using the GUI

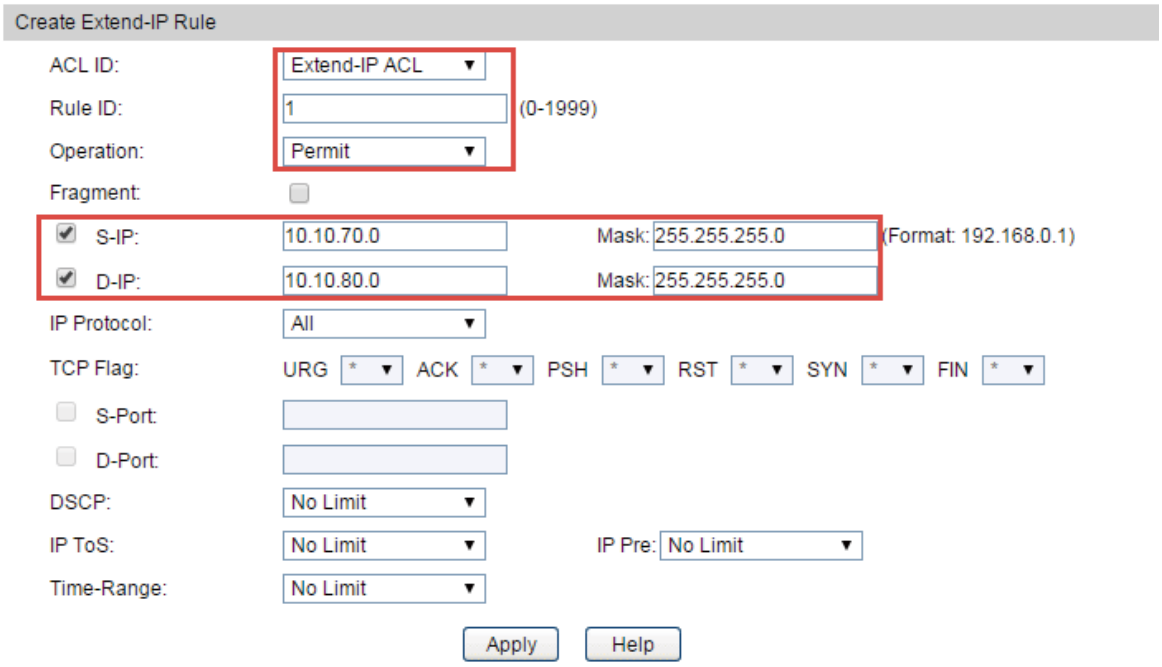
1) Choose the menu **ACL > ACL Config > ACL** Create to load the following page. Then create Extend- IP ACL 1600.

Figure 3-2 Creating an Extend-IP ACL



2) Choose the menu **ACL > ACL Config > Extend-IP ACL** to load the the following page. Configure Rule 1 to match packets with the source IP address 10.10.70.0/24 and destination IP address 10.10.80.0/24.

Figure 3-3 Configuring Rule 1



3) Choose the menu **ACL > ACL Config > Extend-IP ACL** to load the the following page. Configure rule 2 and rule 3 to permit packets with source IP 10.10.70.0 and destination port TCP 80 (http service port) and UDP 443 (https service port).

Figure 3-4 Configuring Rule 2

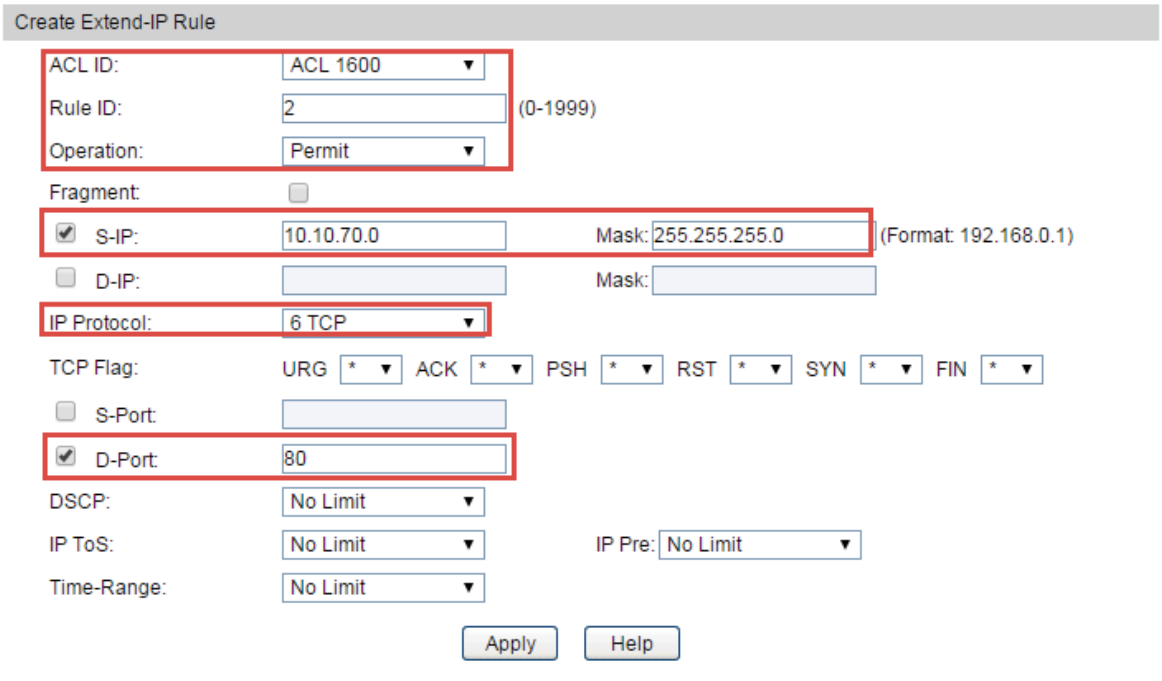
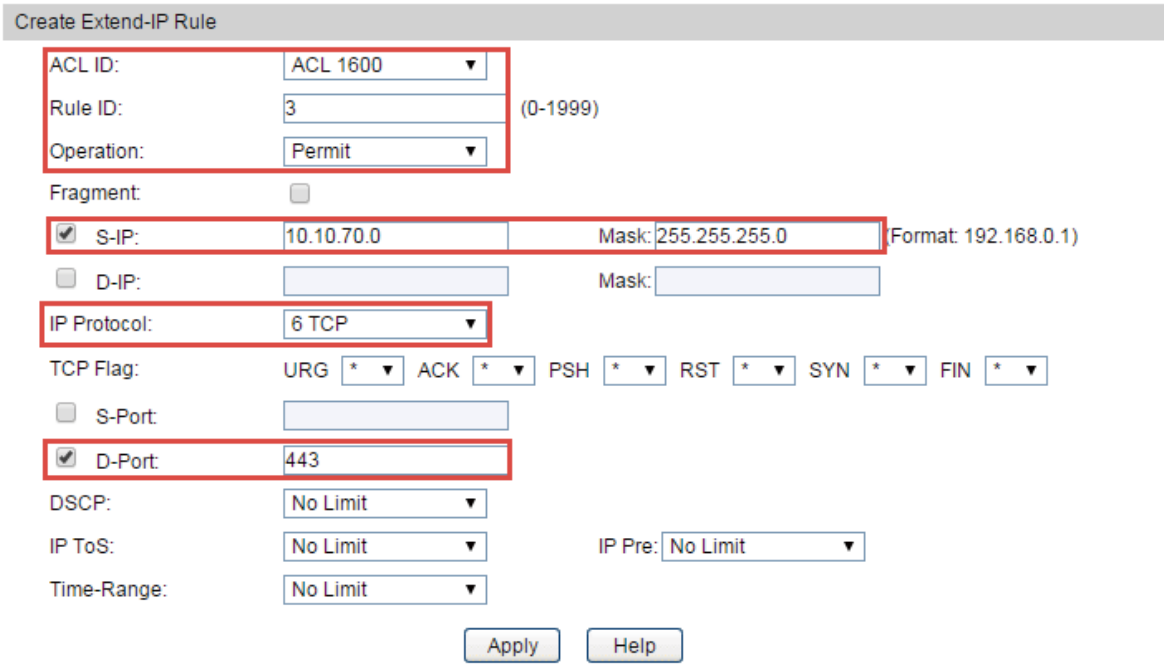


Figure 3-5 Configuring Rule 3



4) Choose the menu **ACL > ACL Config > Extend-IP ACL** to load the following page. Configure Rule 4 and Rule 5 to permit packets with source IP 10.10.70.0 and with destination port TCP 53 or UDP 53 (DNS service port).

Figure 3-6 Configuring Rule 4

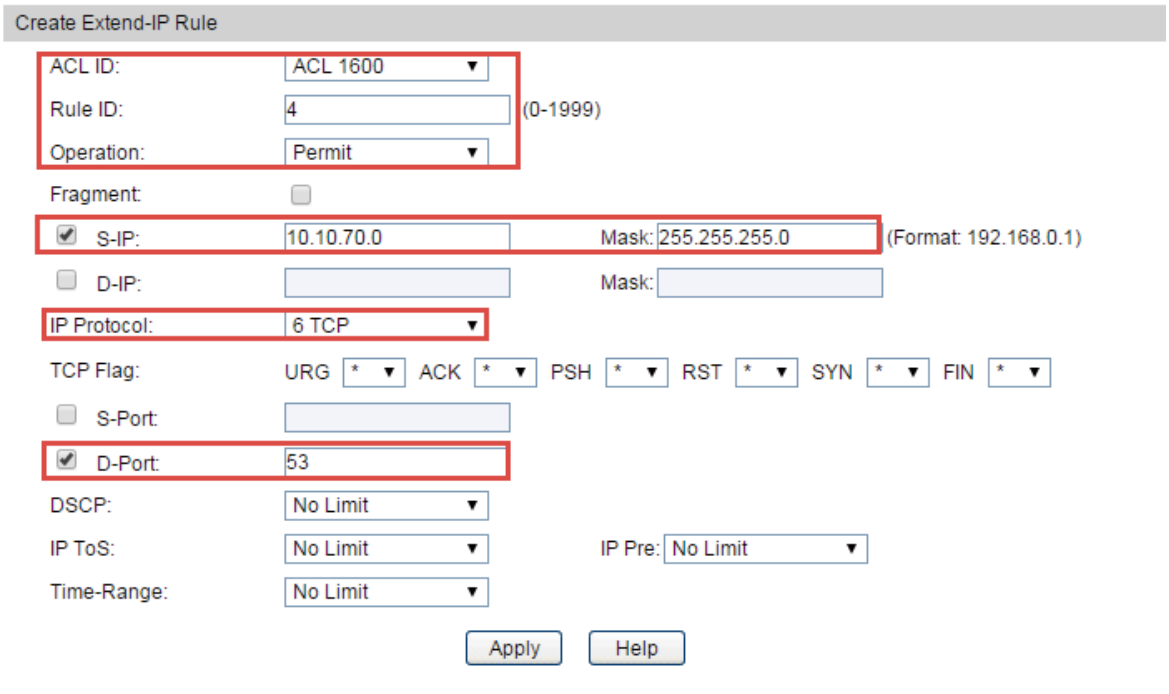
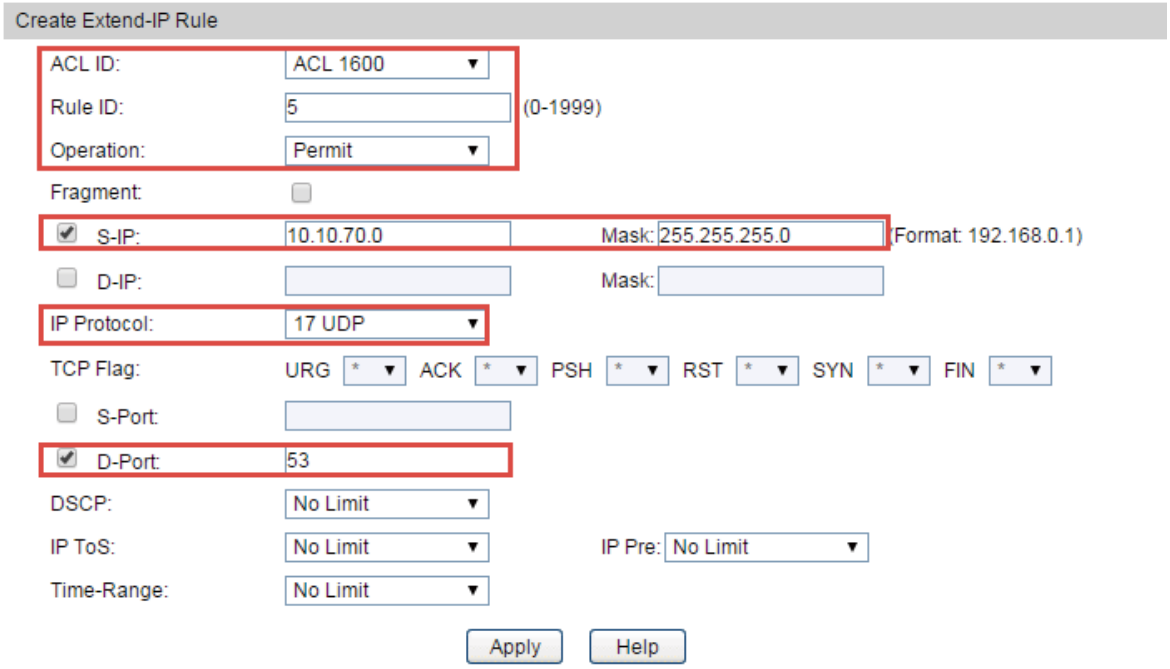
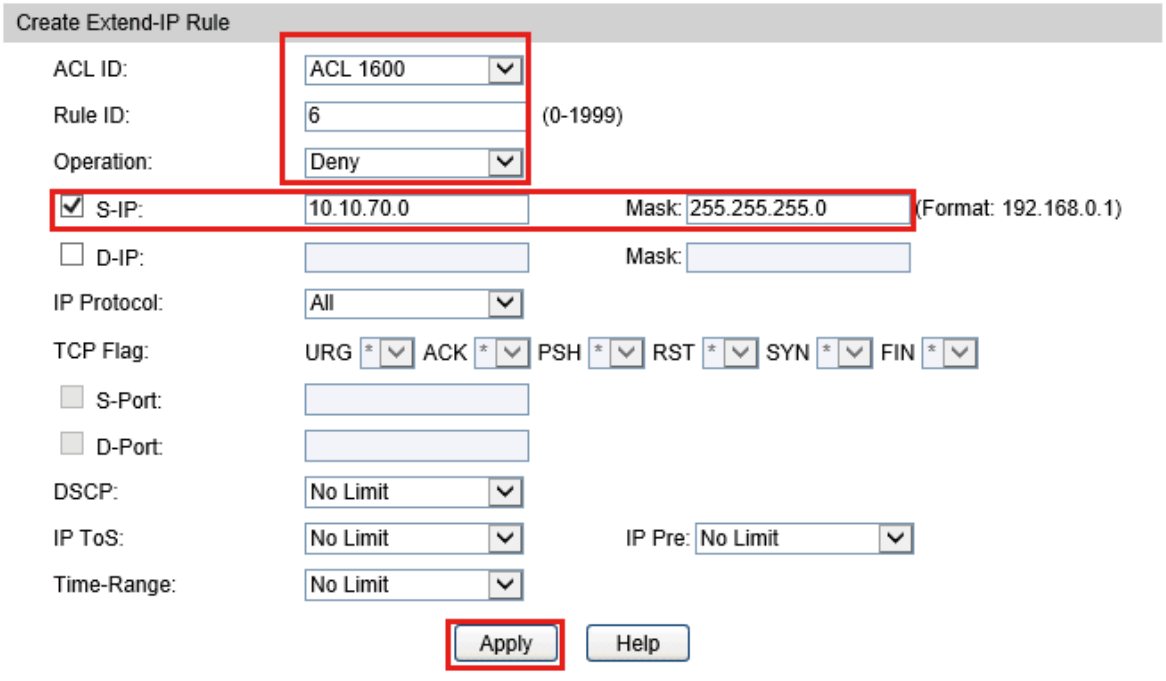


Figure 3-7 Configuring Rule 5



5) Choose the menu **ACL > ACL Config > Extend-IP ACL** to load the following page. Configure Rule 6 to deny packets with source IP 10.10.70.0.

Figure 3-8 Configuring Rule 6



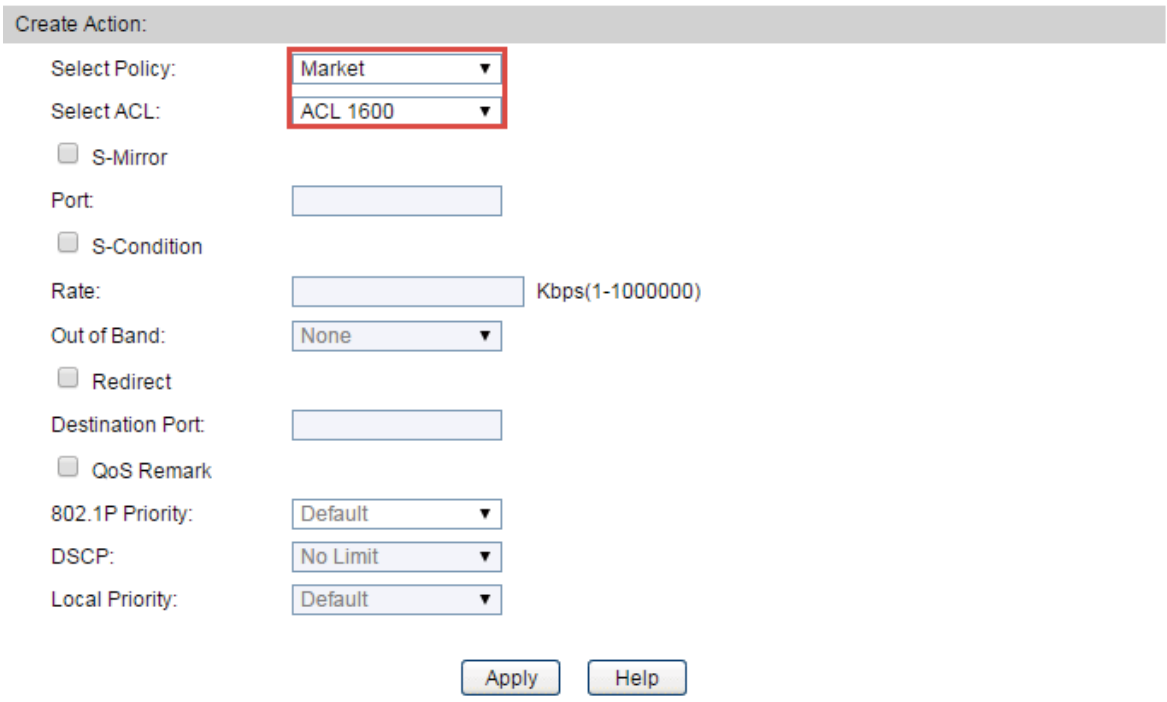
6) Choose the menu **ACL > Policy Config > Policy Create** to load the the following page. Then create Policy Market.

Figure 3-9 Creating the Policy



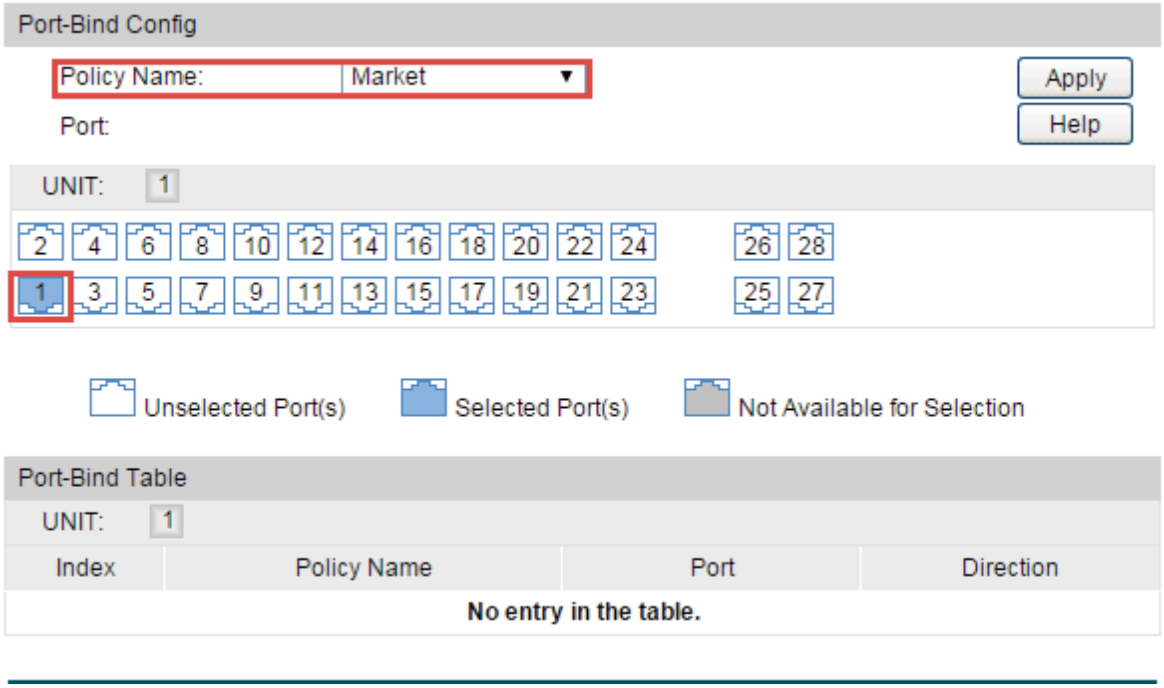
7) Choose the menu **ACL > Policy Config > Action Create** to load the the following page. Then apply ACL 1600 to Policy Market.

Figure 3-10 Applying the ACL to the Policy



8) Choose the menu **ACL > Policy Binding > Port Binding** to load the the following page. Bind Policy Market to port 1/0/1 to make it take effect.

Figure 3-11 Binding the Policy to Port 1/0/1



9) Click **Save Config** to save the settings.

3.5 Using the CLI

1) Create Extended-IP ACL 1600.

   Switch#configure

   Switch(config)#access-list create 1600

2) Configure rule 1 to permit packets with source IP 10.10.70.0 and destination IP 10.10.80.0.

   Switch(config)#access-list extended 1600 rule 1 permit sip 10.10.70.0 smask 255.255.255.0 dip 10.10.80.0 dmask 255.255.255.0

3) Configure Rule 2 and Rule 3 to permit packets with source IP 10.10.70.0, and destination port TCP 80 (http service port) or TCP 443 (https service port).

   Switch(config)#access-list extended 1600 rule 2 permit sip 10.10.70.0 smask 255.255.255.0 protocol 6 d-port 80

   Switch(config)#access-list extended 1600 rule 3 permit sip 10.10.70.0 smask 255.255.255.0 protocol 6 d-port 443

4) Configure Rule 4 and Rule 5 to permit packets with source IP 10.10.70.0, and destination port TCP53 or UDP 53.

   Switch(config)#access-list extended 1600 rule 4 permit sip 10.10.70.0 smask 255.255.255.0 protocol 6 d-port 53

Switch(config)#access-list extended 1600 rule 5 permit sip 10.10.70.0 smask 255.255.255.0 protocol 17 d-port 53

5) Configure Rule 6 to deny packets with source IP 10.10.70.0.

Switch(config)#access-list extended 1600 rule 6 deny sip 10.10.70.0 smask 255.255.255.0

6) Create Policy Market, and then apply ACL 1600 to it.

Switch(config)#access-list policy name Market

Switch(config)#access-list policy action Market 1600

Switch(config-action)#exit

7) Bind Policy Market to Port 1.

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

Switch(config-if)#access-list bind Market

Switch(config-if)#exit

Switch(config)#end

Switch#copy running-config startup-config

Verify the Configurations

Verify the

Extended IP access list 1600

rule 1 permit sip 10.10.70.0 smask 255.255.255.0 dip 10.10.80.0 dmask 255.255.255.0

rule 2 permit sip 10.10.70.0 smask 255.255.255.0 protocol 6 d-port 80

rule 3 permit sip 10.10.70.0 smask 255.255.255.0 protocol 6 d-port 443

rule 4 permit sip 10.10.70.0 smask 255.255.255.0 protocol 6 d-port 53

rule 5 permit sip 10.10.70.0 smask 255.255.255.0 protocol 17 d-port 53

rule 6 deny sip 10.10.70.0 smask 255.255.255.0

Switch(config)#show access-list bind

Index	Policy Name	Interface/VID	Direction	Type
1	Market	Gi1/0/1	Ingress	Port

Index	ACL ID	Interface/VID	Direction	Type

4 Appendix: Default Parameters

For MAC ACL:

Parameter	Default Setting
Operation	Permit
User Priority	No Limit
Time-Range	No Limit

For Standard-IP ACL:

Parameter	Default Setting
Operation	Permit
Time-Range	No Limit

For Extend-IP ACL:

Parameter	Default Setting
Operation	Permit
IP Protocol	All
DSCP	No Limit
IP ToS	No Limit
IP Pre	No Limit
Time-Range	No Limit

For IPv6 ACL:

Parameter	Default Setting
Operation	Permit
Time-Range	No Limit

For Combined ACL:

Parameter	Default Setting
Operation	Permit
Time-Range	No Limit

For Packet Content ACL:

Parameter	Default Setting
Operation	Permit
Time-Range	No Limit

Part 26

Configuring Network Security

CHAPTERS

1. Network Security
2. IP-MAC Binding Configurations
3. IPv6-MAC Binding Configurations
4. DHCP Snooping Configuration
5. DHCPv6 Snooping Configuration
6. ARP Inspection Configurations
7. ND Detection Configuration
8. IP Source Guard Configuration
9. DoS Defend Configuration
10. 802.1X Configuration
11. PPPoE ID-Insertion Configuration
12. AAA Configuration
13. DHCP Server Filter Configuration
14. NetBIOS Filtering Configuration
15. Configuration Examples
16. Appendix: Default Parameters

1 Network Security

1.1 Overview

Network Security provides multiple protection measures for the network. Users can configure the security functions according to their needs.

1.2 Supported Features

The switch supports multiple network security features, for example, IP-MAC Binding, DHCP Snooping, ARP Inspection and so on.

IP-MAC Binding

IP-MAC Binding is used to bind the IP address, MAC address, VLAN ID and the connected port number of the specified host. Basing on the IP-MAC binding table, the switch can prevent the ARP cheating attacks with the ARP Detection feature and filter the packets that don't match the binding entries with the IP Source Guard feature.

The binding entries can be manually configured, or learned by ARP scanning or DHCP snooping.

IPv6-MAC Binding

IPv6-MAC Binding is used to bind the IPv6 address, MAC address, VLAN ID and the connected port number of the specified host. Basing on the IPv6-MAC binding table, the switch can prevent the ND attacks with the ND Detection feature and filter the IPv6 packets that don't match the binding entries with the IP Source Guard feature.

The binding entries can be manually configured, or learned by ND Snooping or DHCPv6 snooping.

DHCP Snooping

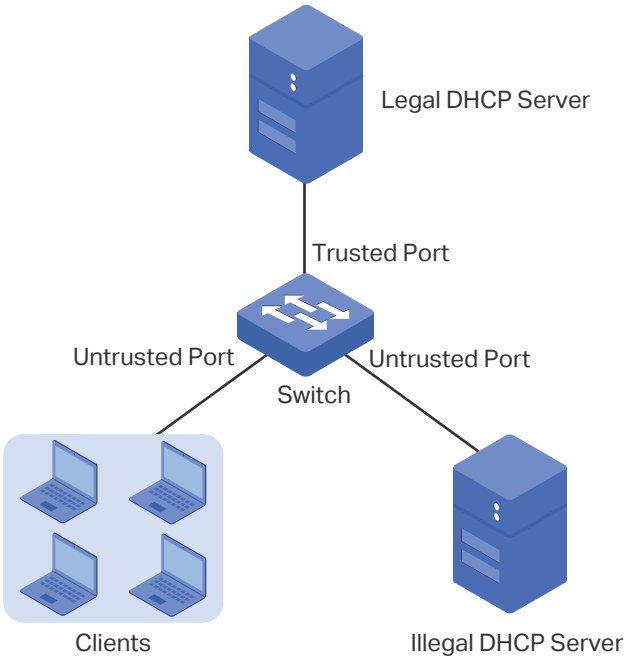
DHCP Snooping supports the basic DHCP security feature and the Option 82 feature.

- Basic DHCP Security

During the working process of DHCP, generally there is no authentication mechanism between the DHCP server and the clients. If there are several DHCP servers on the network, security problems and network interference will happen. DHCP Snooping resolves this problem.

As the following figure shows, the port connected to the legal DHCP server should be configured as a trusted port, and other ports should be configured as untrusted ports. When receiving the DHCP discover or DHCP request packets, the switch forwards them to the legal DHCP server only through the trusted port. When receiving the respond packets, the switch will determine whether to send or not depending on the type of receiving port: packets received from the trusted port will be forwarded, otherwise they will be discarded. DHCP Snooping ensures that users get IP addresses only from the legal DHCP server, enhancing the network security.

Figure 1-1 Network Topology of Basic DHCP Security



Additionally, with DHCP Snooping, the switch can monitor the IP address obtaining process of each client host and record the IP address, MAC address, VLAN ID and the connected port number of the host for automatic binding.

DHCPv6 Snooping

DHCPv6 Snooping is similar with DHCP Snooping introduced above. It ensures that users get IPv6 addresses from the legal DHCPv6 server and enhances the network security. Besides, with DHCPv6 Snooping, the switch can monitor the IPv6 address obtaining process of each client host and record the IPv6 address, MAC address, VLAN ID and the connected port number of the host for automatic binding.

ARP Inspection

In an actual complex network, there are high security risks during ARP implementation procedure. The cheating attacks against ARP, such as imitating gateway, cheating gateway, cheating terminal hosts and ARP flooding attack, frequently occur to the network. ARP Inspection can prevent the network from these ARP attacks.

- Prevent ARP Cheating Attacks

Based on the predefined IP-MAC Binding entries, the ARP Inspection can be configured to detect the ARP packets and filter the illegal ones so as to prevent the network from ARP cheating attacks.

- Prevent ARP Flooding Attack

With the ARP Defend feature the switch can terminate receiving the ARP packets for 300 seconds when the transmission speed of the legal ARP packet on the port exceeds the defined value so as to avoid ARP flooding attack.

ND Detection

Because of the absence of security mechanism, IPv6 ND (Neighbor Discovery) protocol is easy to be exploited by attackers. ND detection feature uses the entries in the IPv6-MAC binding table to filter the forged ND packets and prevent the ND attacks.

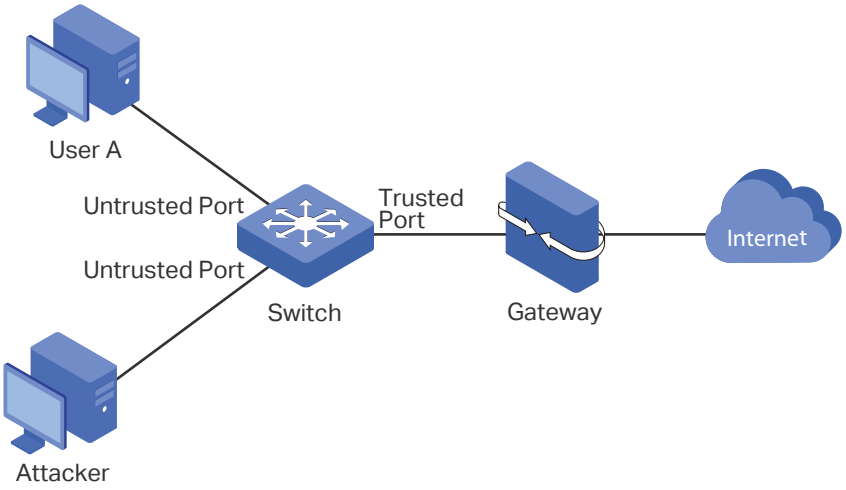
The application topology of ND Detection is as the following figure shows. the port that is connected to the gateway should be configured as trusted port, and other ports should be configured as untrusted ports. The forwarding principles of ND packets are as follows:

- All ND packets received on the trusted port will be forwarded without checked.

- RS (Router Solicitation) and NS (Neighbor Solicitation) packets with their source IPv6 addresses unspecified, such as the RS packet for IPv6 address request and the NS packet for duplicate address detection, will not be checked on both kinds of ports.

- RA (Router Advertisement) and RR (Router Redirect) packets received on the untrusted port will be discarded directly, and other ND packets will be checked: The switch will use the IPv6-MAC binding table to compare the IPv6 address, MAC address, VLAN ID and receiving port between the entry and the ND packet. If a match is found, the ND packet is considered legal and will be forwarded; if no match is found, the ND packet is considered illegal and will be discarded.

Figure 1-2 Network Topology of ND Detection



IP Source Guard

IP Source Guard is to filter the IP packets and IPv6 packets based on the IP-MAC Binding table and IPv6 MAC-Binding table. Only the packets that match the binding rules are permitted, which enhances the network security.

DoS Defend

The DoS (Denial of Service) defend feature provides protection against DoS attacks. DoS attacks occupy the network bandwidth maliciously by sending numerous service requests to the hosts. It results in an abnormal service or breakdown of the network.

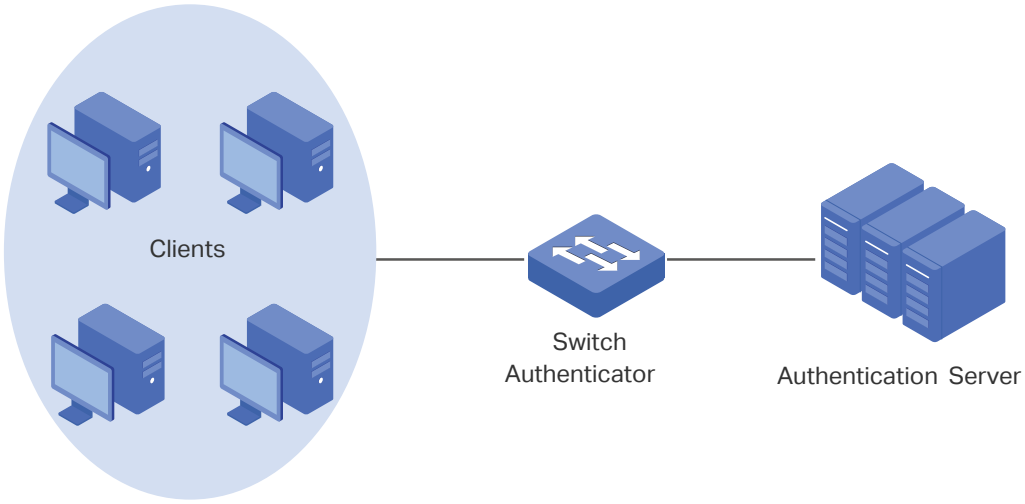
With DoS Defend feature, the switch can analyze the specific fields of the IP packets, distinguish the malicious DoS attack packets and discard them directly. Also, DoS Defend feature can limit the transmission rate of legal packets. When the number of legal packets exceeds the threshold value and may incur a breakdown of the network, the switch will discard the packets.

802.1X

802.1X protocol is a protocol for port-based Network Access Control. It is used to authenticate and control access from devices connected to the ports. If the device connected to the port is authenticated by the authentication server successfully, its request to access the LAN will be accepted; if not, its request will be denied.

802.1X authentication uses the typical client-server model which contains three device roles: client/supplicant, authenticator and authentication server. This is described in the figure below:

Figure 1-3 802.1X Authentication Model



- Client

A client, usually a computer, is connected to the authenticator via a physical port. We recommend that you install TP-Link 802.1X authentication client software on the client hosts, enabling them to request 802.1X authentication to access the LAN.

- Authenticator

An authenticator is usually a network device that supports 802.1X protocol. As the above figure shows, the switch is an authenticator.

The authenticator acts as an intermediate proxy between the client and the authentication server. The authenticator requests user information from the client and sends it to the authentication server; also, the authenticator obtains responses from the authentication server and send them to the client. The authenticator allows authenticated clients to access the LAN through the connected ports but denies the unauthenticated clients.

- Authentication Server

The authentication server is usually the host running the RADIUS server program. It stores information of clients, confirms whether a client is legal and informs the authenticator whether a client is authenticated.

PPPoE ID-Insertion

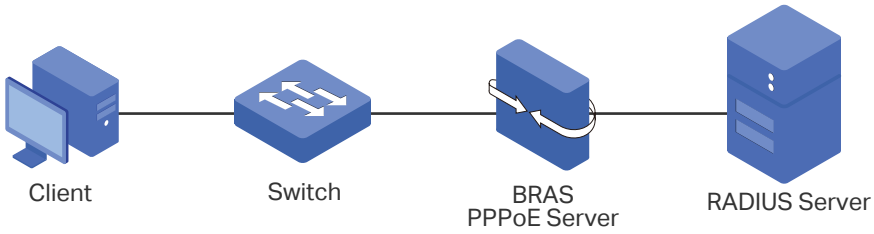
In common PPPoE dialup mode, when users dial up through PPPoE, they can access the network as long as their accounts are authenticated successfully on the RADIUS server. As a result, the illegal users can embezzle the accounts to access the Internet.

PPPoE ID-Insertion provides a way to resolve this problem. With this feature enabled, the switch attaches a tag to the PPPoE Active Discovery packets received from the client, and sends it to the BRAS (Broadband Remote Access Server). The tag records the client information, such as the connected port number and the MAC address of the client. The

BRAS uses the tag as a NAS-Port-ID attribute in the RADIUS packet and send it to the RADIUS server for PPP (Point-to-Point Protocol) authentication. If the tag information is different from the configured one, the authentication will fail. In this way, the illegal users cannot embezzle the accounts of legal users to access the Internet.

Additionally, after receiving the PPPoE Active Discovery Offer packet or Session-confirmation packet from the BRAS, the switch will remove the tag in the packet and send it to the client.

Figure 1-4 Network Topology of PPPoE ID-Insertion

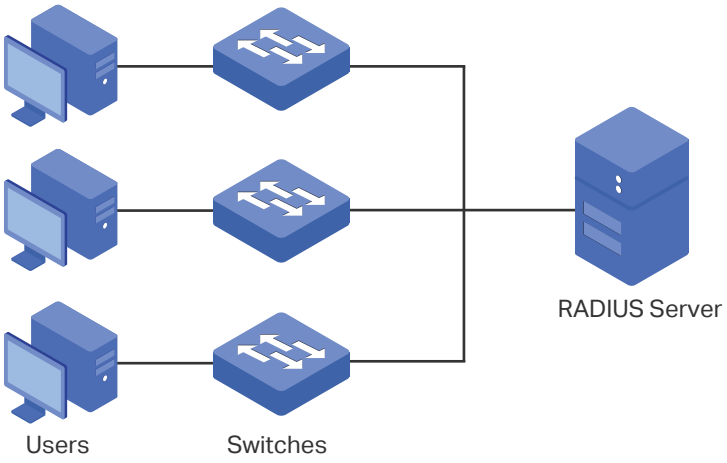


AAA

AAA stands for authentication, authorization and accounting. On TP-Link switches, this feature is mainly used to authenticate the users trying to log in to the switch or get administrative privileges. The administrator can create guest accounts and an Enable password for other users. The guests do not have administrative privileges without the Enable password provided.

AAA provides a safe and efficient authentication method. The authentication can be processed locally on the switch or centrally on the RADIUS/TACACS+ server(s). As the following figure shows, the network administrator can centrally configure the management accounts of the switches on the RADIUS server and use this server to authenticate the users trying to access the switch or get administrative privileges.

Figure 1-5 Network Topology of AAA



DHCP Server Filter

DHCP Server Filter function will check whether DHCP packets are legal and discard the illegal ones accoding to the DHCP Server Permit Entry Table configured manually. This function ensures that users get IP addresses only from the legal DHCP server and enhances the network security.

NetBIOS Filtering

NetBIOS Filtering function can block the network communication on computers which use NetBIOS over TCP/IP, thus enhancing the network security.

2 IP-MAC Binding Configurations

You can complete IP-MAC binding in two ways:

- Manual Binding
- Dynamical Binding (including ARP Scanning and DHCP Snooping)

Additionally, you can search the specified entries in the Binding Table.

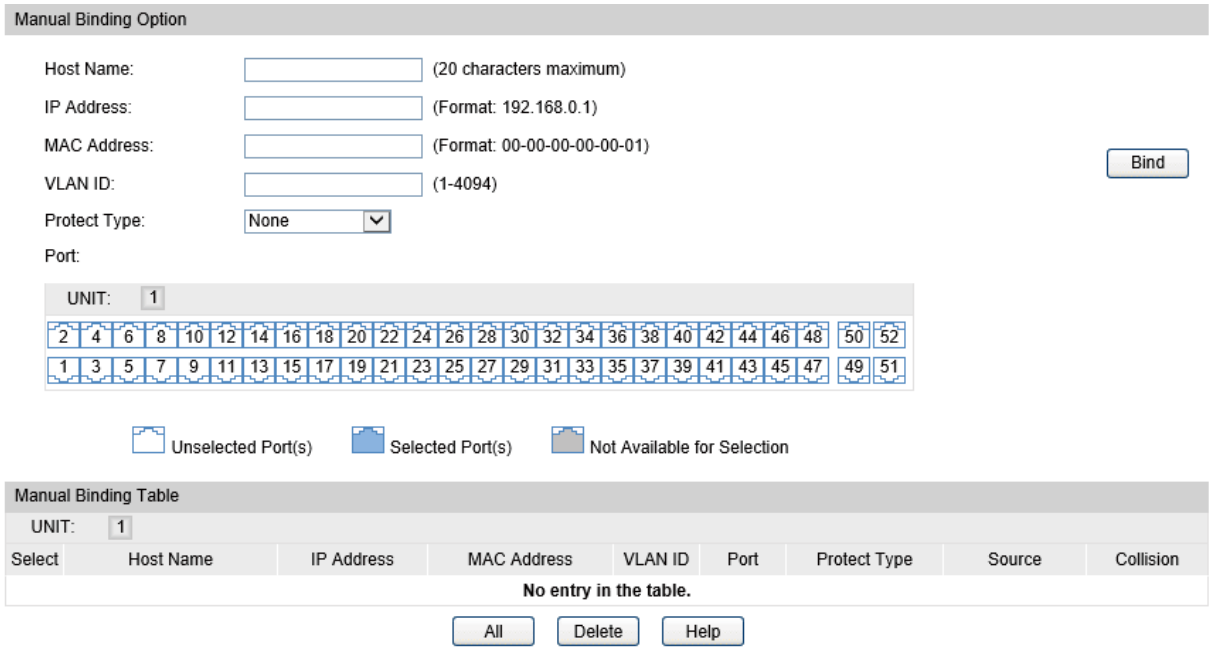
2.1 Using the GUI

2.1.1 Binding Entries Manually

You can manually bind the IP address, MAC address, VLAN ID and the Port number together on the condition that you have got the related information of the hosts on the network.

Choose the menu **Network Security > IP-MAC Binding > Manual Binding** to load the following page.

Figure 2-1 Manual Binding



In the **Manual Binding Option** section, follow these steps to configure IP-MAC Binding:

1) Enter the following information to specify a host.

Host Name	Enter the host name for identification.
IP Address	Enter the IP address.
MAC Address	Enter the MAC address.
VLAN ID	Enter the VLAN ID.

2) Select protect type for the entry.

Protect Type	Select the protect type for the entry: **None**: This entry will not be applied to any feature. **ARP Detection**: This entry will be applied to the ARP Detection feature. **IP Source Guard**: This entry will be applied to the IP Source Guard feature. **All**: This entry will be applied to both the features.

3) Select the port that is connected to this host.

4) Click **Bind**.

2.1.2 Binding Entries Dynamically

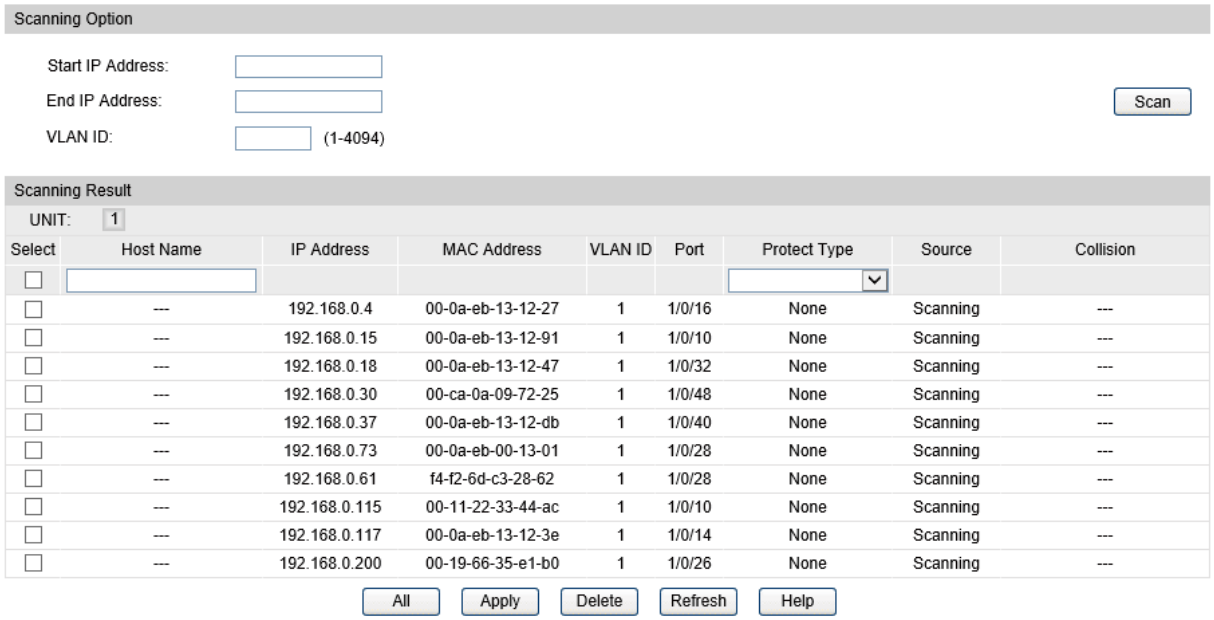
The binding entries can be dynamically learned from ARP Scanning and DHCP Snooping.

- ARP Scanning

With ARP Scanning, the switch sends the ARP request packets of the specified IP field to the hosts. Upon receiving the ARP reply packet, the switch can get the IP address, MAC address, VLAN ID and the connected port number of the host. You can bind these entries conveniently.

Choose the menu **Network Security > IP-MAC Binding > ARP Scanning** to load the following page.

Figure 2-2 ARP Scanning



Follow these steps to configure IP-MAC Binding via ARP scanning:

1) In the **Scanning Option** section, specify an IP address range and a VLAN ID. Then click **Scan** to scan the entries in the specified IP address range and VLAN.

Start IP Address/ End IP Address	Specify an IP range by entering a start and end IP address.
VLAN ID	Specify a VLAN ID.

2) In the **Scanning Result** section, select one or more entries and configure the relevant parameters. Then click **Apply**.

Host Name	Enter a host name for identification.
IP Address	Displays the IP address.
MAC Address	Displays the MAC address.
VLAN ID	Displays the VLAN ID.
Port	Displays the port number.

Protect Type	Select the protect type for the entry: **None**: This entry will not be applied to any feature. **ARP Detection**: This entry will be applied to the ARP Detection feature. **IP Source Guard**: This entry will be applied to the IP Source Guard feature. **All**: This entry will be applied to both the features.
Source	Displays the source of the entry.
Collision	Displays the collision status of the entry. **Warning**: The collision entries have the same IP address and MAC address, and all the collision entries are valid. This kind of collision may be caused by the MSTP function. **Critical**: The collision entries have the same IP address but different MAC addresses. For the collision entries learned from the same source, only the newly added entry will be valid. For the collision entries learned from different sources, only the entry with the highest priority will be valid. The priority of different entry types, from high to low, is Manually, ARP Scanning and DHCP Snooping.

- DHCP Snooping

With DHCP Snooping enabled, the switch can monitor the IP address obtaining process of the host, and record the IP address, MAC address, VLAN ID and the connected port number of the host.

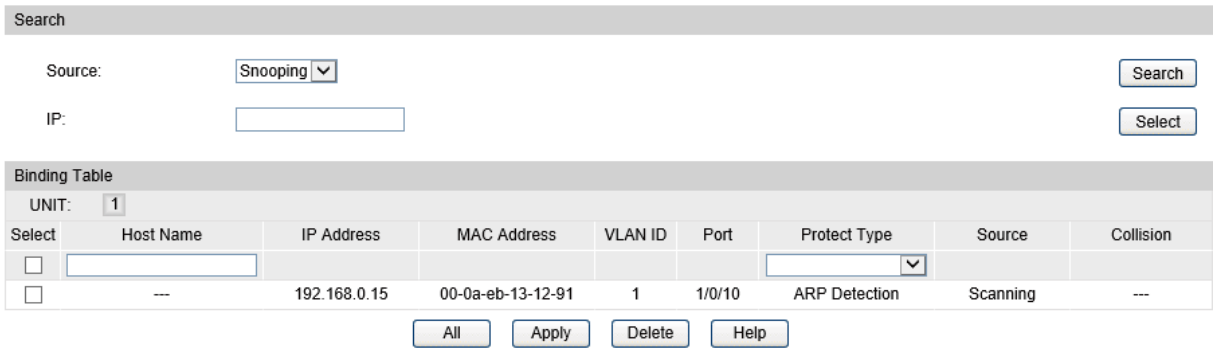
For instructions on how to configure DHCP Snooping, refer to *DHCP Snooping Configurations*.

2.1.3 Viewing the Binding Entries

With the Binding Table, you can view and search the specified binding entries.

Choose the menu **Network Security > IP-MAC Binding > Binding Table** to load the following page.

Figure 2-3 Binding Table



In the **Search** section, specify the search criteria to search your desired entries.

Source	Select the source of the entry and click **Search**. **All**: Displays the entries from all sources. **Manual**: Displays the manually bound entries. **Scanning**: Displays the binding entries learned from ARP Scanning. **Snooping**: Displays the binding entries learned from DHCP Snooping.
IP:	Enter an IP address and click **Search** to search the specific entry.

In the **Binding Table** section, you can view the searched entries. Additionally, you can configure the host name and protect type for one or more entries, and click **Apply**.

Host Name	Enter a host name for identification.
IP Address	Displays the IP address.
MAC Address	Displays the MAC address.
VLAN ID	Displays the VLAN ID.
Port	Displays the port number.
Protect Type	Select the protect type for the entry: **None**: This entry will not be applied to any feature. **ARP Detection**: This entry will be applied to the ARP Detection feature. **IP Source Guard**: This entry will be applied to the IP Source Guard feature. **All**: This entry will be applied to both the features.
Source	Displays the source of the entry.
Collision	Displays the collision status of the entry. **Warning**: The collision entries have the same IP address and MAC address, and all the collision entries are valid. This kind of collision may be caused by the MSTP function. **Critical**: The collision entries have the same IP address but different MAC addresses. For the collision entries learned from the same source, only the newly added entry will be valid. For the collision entries learned form different sources, only the entry with the highest priority will be valid. The priority of different entry types, from high to low, is Manually, ARP Scanning and DHCP Snooping.

2.2 Using the CLI

Binding entries via ARP scanning is not supported by the CLI; Binding entries via DHCP Snooping is introduced in *DHCP Snooping Configurations*. The following sections introduce how to bind entries manually and view the binding entries.

2.2.1 Binding Entries Manually

You can manually bind the IP address, MAC address, VLAN ID and the Port number together on the condition that you have got the related information of the hosts.

Follow these steps to manually bind entries:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip source binding** *hostname ip-addr mac-addr* **vlan** *vlan-id* **interface gigabitEthernet** *port* **{** none | arp-detection | ip-verify-source | both **} [forced-source {**arp-scanning | dhcp-snooping**}]** Manually bind the host name, IP address, MAC address, VLAN ID and port number of the host, and configure the protect type for the host. In addition, you can change the source of the entry as ARP Scanning or DHCP Snooping. *hostname*: Specify a name for the host. It contains 20 characters at most. *ip-addr*: Enter the IP address of the host. *mac-addr*: Enter the MAC address of the host, in the format of xx:xx:xx:xx:xx:xx. *vlan-id*: Enter the VLAN ID of the host. *port*: Enter the number of the port on which the host is connected. none | arp-detection | ip-verify-source | both: Specify the protect type for the entry. None indicates this entry will not be applied to ARP Detection; arp-detection indicates this entry will be applied to ARP Detection. arp-scanning | dhcp-snooping: Change the source of the entry to ARP Scanning or DHCP Snooping.
Step 3	**show ip source binding** Verify the binding entry.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to bind an entry with the hostname host1, IP address 192.168.0.55, MAC address AA-BB-CC-DD-EE-FF, VLAN ID 10, port number 1/0/5, and enable this entry for the ARP detection feature.

Switch#configure

Switch(config)#ip source binding host1 192.168.0.55 aa:bb:cc:dd:ee:ff **vlan** 10 **interface gigabitEthernet** 1/0/5 arp-detection

Switch(config)#show ip source binding

U	No.	Host	IP-Addr	MAC-Addr	VID	Port	ACL	Col.
--	---	-------	--------	--------	------	-----	------	-----
1	1	host1	192.168.0.55	aa:bb:cc:dd:ee:ff	10	Gi1/0/5	ARP-D	

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Viewing Binding Entries

On privileged EXEC mode or any other configuration mode, you can use the following command to view binding entries:

show ip source binding

View the information of binding entries, including the host name, IP address, MAC address, VLAN ID, port number, protect type and collision status.

There are two types of collision status: Warning and Critical.

Warning: The collision entries have the same IP address and MAC address, and all the collision entries are valid. This kind of collision may be caused by the MSTP function.

Critical: The collision entries have the same IP address but different MAC addresses. For the collision entries learned from the same source, only the newly added entry will be valid. For the collision entries learned different sources, only the entry with the highest priority will be valid. The priority of different entry types, from high to low, is Manually, ARP Scanning and DHCP Snooping.

3 IPv6-MAC Binding Configurations

You can complete IPv6-MAC binding in two ways:

- Manual Binding
- Dynamical Binding (including ND Snooping and DHCPv6 Snooping)

Additionally, you can search the specified entries in the Binding Table.

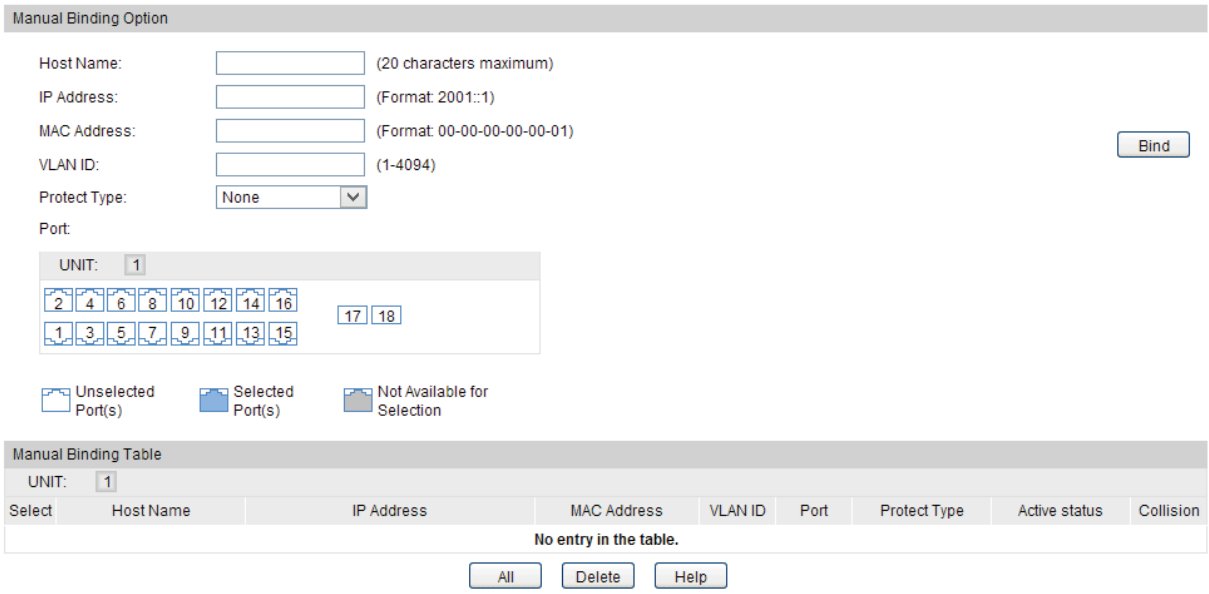
3.1 Using the GUI

3.1.1 Binding Entries Manually

You can manually bind the IPv6 address, MAC address, VLAN ID and the Port number together on the condition that you have got the related information of the hosts on the network.

Choose the menu **Network Security > IPv6-MAC Binding > Manual Binding** to load the following page.

Figure 3-1 Manual Binding



In the **Manual Binding Option** section, follow these steps to configure IPv6-MAC Binding:

1) Enter the following information to specify a host.

Host Name	Enter the host name for identification.
IP Address	Enter the IP address.
MAC Address	Enter the MAC address.
VLAN ID	Enter the VLAN ID.

2) Select protect type for the entry.

Protect Type	Select the protect type for the entry: **None**: This entry will not be applied to any feature. **ND Detection**: This entry will be applied to the ND Detection feature. **IP Source Guard**: This entry will be applied to the IP Source Guard feature. **All**: This entry will be applied to both ND Detection and IP Source Guard.

3) Select the port that is connected to this host.
4) Click **Bind**.

3.1.2 Binding Entries Dynamically

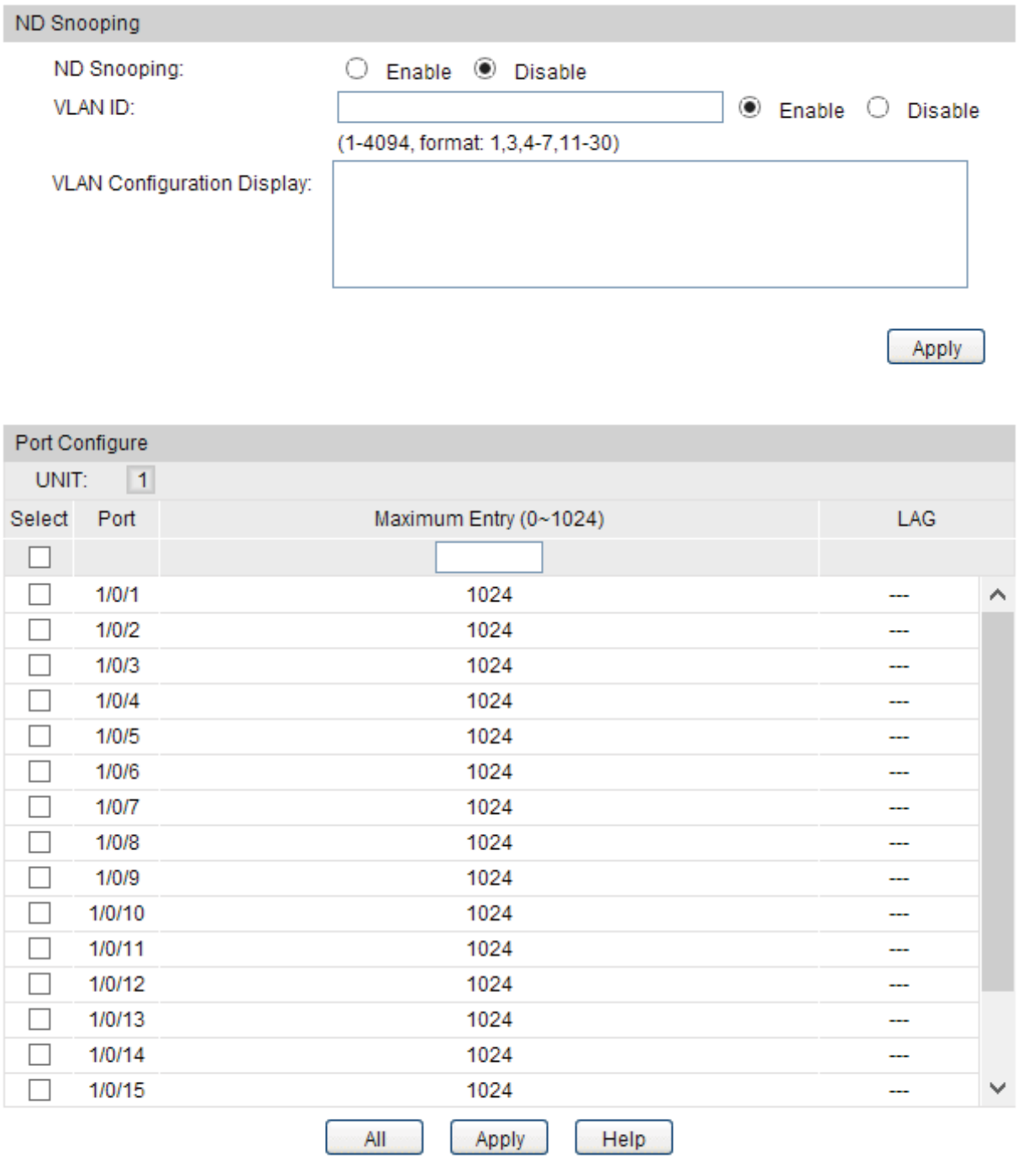
The binding entries can be dynamically learned from ND Snooping and DHCPv6 Snooping.

- ND Snooping

With ND Snooping, the switch monitors the ND packets, and records the IPv6 addresses, MAC addresses, VLAN IDs and the connected port numbers of the IPv6 hosts. You can bind these entries conveniently.

Choose the menu **Network Security > IPV6-MAC Binding > ND Snooping** to load the following page.

Figure 3-2 ND Snooping



Follow these steps to configure IPv6-MAC Binding via ND Snooping:

1) In the **ND Snooping** section, enable ND Snooping globally and on the specified VLAN(s). Then click **Apply**.

ND Snooping	Enable ND Snooping Globally.

VLAN ID	Specify one or more VLAN IDs to enable ND Snooping on the VLAN(s).
VLAN Configuration Display	Displays the VLANs that have been enabled with ND Snooping.

2) In the **Port Configure** section, select one or more ports and configure the maximum number of entries that can be learned on this port via ND Snooping. Then click **Apply**.

Maximum Entry (0~1024)	Configure the maximum number of ND binding entries a port can learn via ND snooping. The valid values are from 0 to 1024, and the default is 1024.
LAG	Displays the LAG that the port is in.

- DHCPv6 Snooping

With DHCPv6 Snooping enabled, the switch can monitor the IPv6 address obtaining process of the host, and record the IPv6 address, MAC address, VLAN ID and the connected port number of the host.

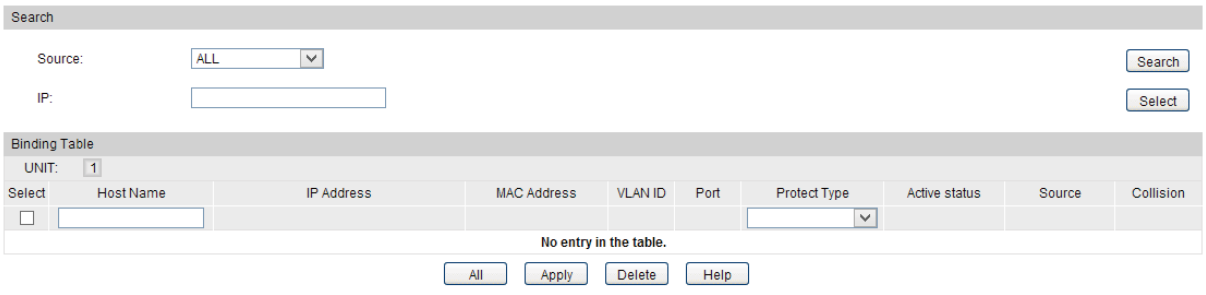
For instructions on how to configure DHCPv6 Snooping, refer to DHCPv6 Snooping Configuration.

3.1.3 Viewing the Binding Entries

With the Binding Table, you can view and search the specified binding entries.

Choose the menu **Network Security > IPv6-MAC Binding > Binding Table** to load the following page.

Figure 3-3 Binding Table



In the **Search** section, specify the search criteria to search your desired entries.

Source	Select the source of the entry and click **Search**. **All**: Displays the entries from all sources. **Manual**: Displays the manually bound entries. **ND Snooping**: Displays the binding entries learned from ND Snooping. **DHCP Snooping**: Displays the binding entries learned from DHCP Snooping.

IP	Enter an IP address and click **Search** to search the specific entry.

In the **Binding Table** section, you can view the search results. Additionally, you can configure the host name and protect type for one or more entries, and click **Apply**.

Host Name	Enter a host name for identification.
IP Address	Displays the IPv6 address.
MAC Address	Displays the MAC address.
VLAN ID	Displays the VLAN ID.
Port	Displays the port number.
Protect Type	Select the protect type for the entry: **None**: This entry will not be applied to any feature. **ND Detection**: This entry will be applied to the ND Detection feature. **IP Source Guard**: This entry will be applied to the IP Source Guard feature. **All**: This entry will be applied to both ND Detection and IP Source Guard.
Active Status	Displays whether the binding entries are valid for each feature. **ND Detection**: The entries are valid for ND Detection. **IP Source Guard**: The entries are valid for IP Source Guard. **All:** The entries are valid for both ND Detection and IP Source Guard. **None**: The entries are valid for no feature.
Source	Displays the source of the entry.
Collision	Displays the collision status of the entry. **Warning**: The collision entries have the same IPv6 address and MAC address, and all the collision entries are valid. This kind of collision may be caused by the MSTP function. **Critical**: The collision entries have the same IPv6 address but different MAC addresses. For the collision entries learned from the same source, only the newly added entry will be valid. For the collision entries learned form different sources, only the entry with the highest priority will be valid. The priority of different entry types, from high to low, is Manually, DHCP Snooping and ND Snooping.

3.2 Using the CLI

Binding entries via DHCPv6 Snooping is introduced in DHCPv6 Snooping Configuration. The following sections introduce how to bind entries manually and via ND Snooping, and how to view the binding entries.

3.2.1 Binding Entries Manually

You can manually bind the IPv6 address, MAC address, VLAN ID and the Port number together on the condition that you have got the related information of the hosts.

Follow these steps to manually bind entries:

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 source binding** *hostname ipv6-addr mac-addr* **vlan** *vlan-id* **interface{ fastEthernet** *port* **| gigabitEthernet** *port* **} {** none | nd-detection | ipv6-verify-source | both **}** Manually bind the host name, IPv6 address, MAC address, VLAN ID and port number of the host, and configure the protect type for the host. *hostname*: Specify a name for the host. It contains 20 characters at most. *ipv6-addr*: Enter the IPv6 address of the host, in the format of X:X:X:X::X. *mac-addr*: Enter the MAC address of the host, in the format of xx:xx:xx:xx:xx:xx. *vlan-id*: Enter the VLAN ID of the host. *port*: Enter the number of the port on which the host is connected. none | nd-detection | ipv6-verify-source | both: Specify the protect type for the entry. None indicates this entry will not be applied to any feature; nd-detection indicates this entry will be applied to ND Detection; ipv6-verify-source indicates this entry will be applied to IP Source Guard; both indicates this entry will be applied to both ND Detection and IP Source Guard.
Step 3	**show ipv6 source binding** Verify the binding entry.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

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#configure

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

Switch(config)#show ipv6 source binding

U	No.	Host	IP-Addr	MAC-Addr	VID	Port	ACL	Active	Source	Col.
-	---	----	-------	--------	---	----	---	-----	------	----
1	1	host1	2001:0:9d38:90d5::34	aa:bb:cc:dd:ee:ff	10	Gi1/0/5	ND-D	ND-D	Manual	

Switch(config)#end

Switch#copy running-config startup-config

3.2.2 Binding Entries via ND Snooping

Follow these steps to bind entries via ND Snooping:

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 nd snooping** Globally enable ND Snooping.
Step 3	**ipv6 nd snooping vlan** *vlan-range* Enable ND Snooping on the specified VLAN. *vlan-range:* Enter the vlan range in the format of 1-3, 5.
Step 4	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **}** Enter interface configuration mode.
Step 5	**ipv6 nd snooping max-entries** *value* Configure the maximum number of ND binding entries a port can learn via ND snooping. *value:* Enter the maximum number of ND binding entries a port can learn via ND snooping. The valid values are from 0 to 1024, and the default is 1024.
Step 6	**show ipv6 nd snooping** Verify the global configuration of IPv6 ND Snooping
Step 7	**show ipv6 nd snooping interface { fastEthernet** *port* **| gigabitEthernet** *port* **}** Verify the IPv6 ND Snooping configuration of the specific port.

Step 8	**end** Return to privileged EXEC mode.
Step 9	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable ND Snooping globally and on VLAN 1.

Switch#configure

Switch(config)#ipv6 nd snooping

Switch(config)#ipv6 nd snooping vlan 1

Switch(config)#show ipv6 nd snooping

Global Status: Enable

VLAN ID: 1

Switch(config)#end

Switch#copy running-config startup-config

The following example shows how to configure the maximum number of entries that can be learned on port 1/0/1:

Switch#configure

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

Switch(config-if)#ipv6 nd snooping max-entries 1000

Switch(config-if)#show ipv6 nd snooping interface gigabitEthernet 1/0/1

Interface max-entries LAG

--------- ---------- -----

Gi1/0/1 1000 N/A

Switch(config-if)#end

Switch#copy running-config startup-config

3.2.3 Viewing Binding Entries

On privileged EXEC mode or any other configuration mode, you can use the following command to view binding entries:

show ipv6 source binding

View the information of binding entries, including the host name, IPv6 address, MAC address, VLAN ID, port number, protect type, source and collision status.

There are two types of collision status: Warning and Critical.

Warning: The collision entries have the same IPv6 address and MAC address, and all the collision entries are valid. This kind of collision may be caused by the MSTP function.

Critical: The collision entries have the same IPv6 address but different MAC addresses. For the collision entries learned from the same source, only the newly added entry will be valid. For the collision entries learned different sources, only the entry with the highest priority will be valid. The priority of different entry types, from high to low, is Manually, DHCPv6 Snooping and ND Snooping.

4 DHCP Snooping Configuration

To complete DHCP Snooping configuration, follow these steps:

1) Enable DHCP Snooping on VLAN.
2) Configure DHCP Snooping on the specified port.

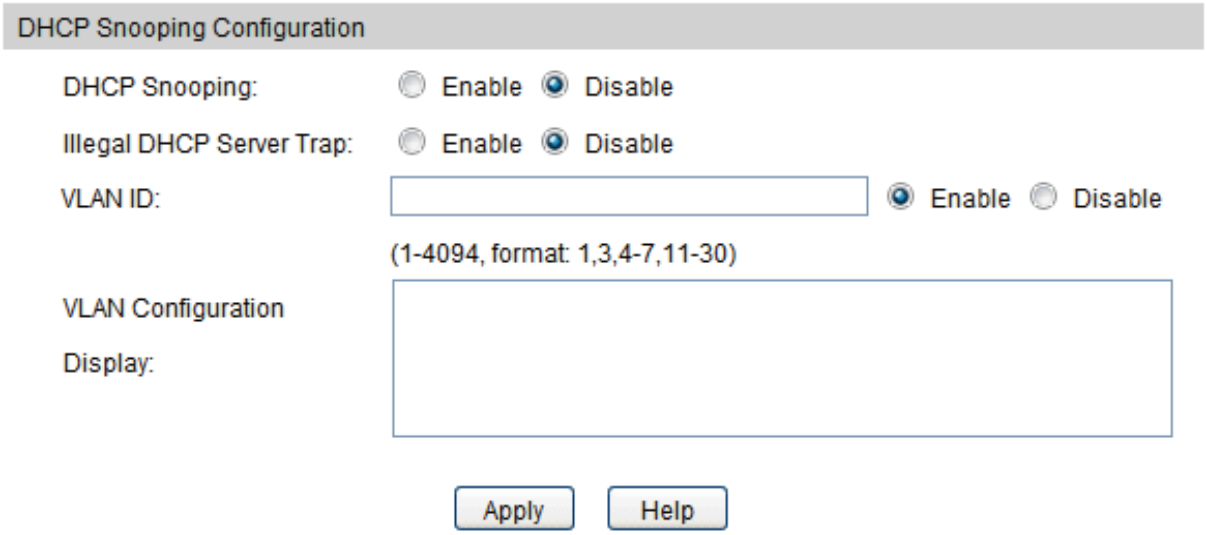
Tips: The switch can dynamically bind the entries via DHCP Snooping after step 1 and step 2 are completed. By default, the binding entries are applied to ARP Detection.

4.1 Using the GUI

4.1.1 Enabling DHCP Snooping on VLAN

Choose the menu **Network Security > DHCP Snooping > Global Config** to load the following page.

Figure 4-1 Global Config



Follow these steps to enable DHCP Snooping:

1) Globally enable DHCP Snooping.

2) Configure the Illegal DHCP Server Trap feature.

Illegal DHCP Server Trap	Enable Illegal DHCP Server Trap feature to send snmp trap message when untrusted port has received DHCP Server packets.

4) Enable DHCP Snooping on a VLAN or range of VLANs.

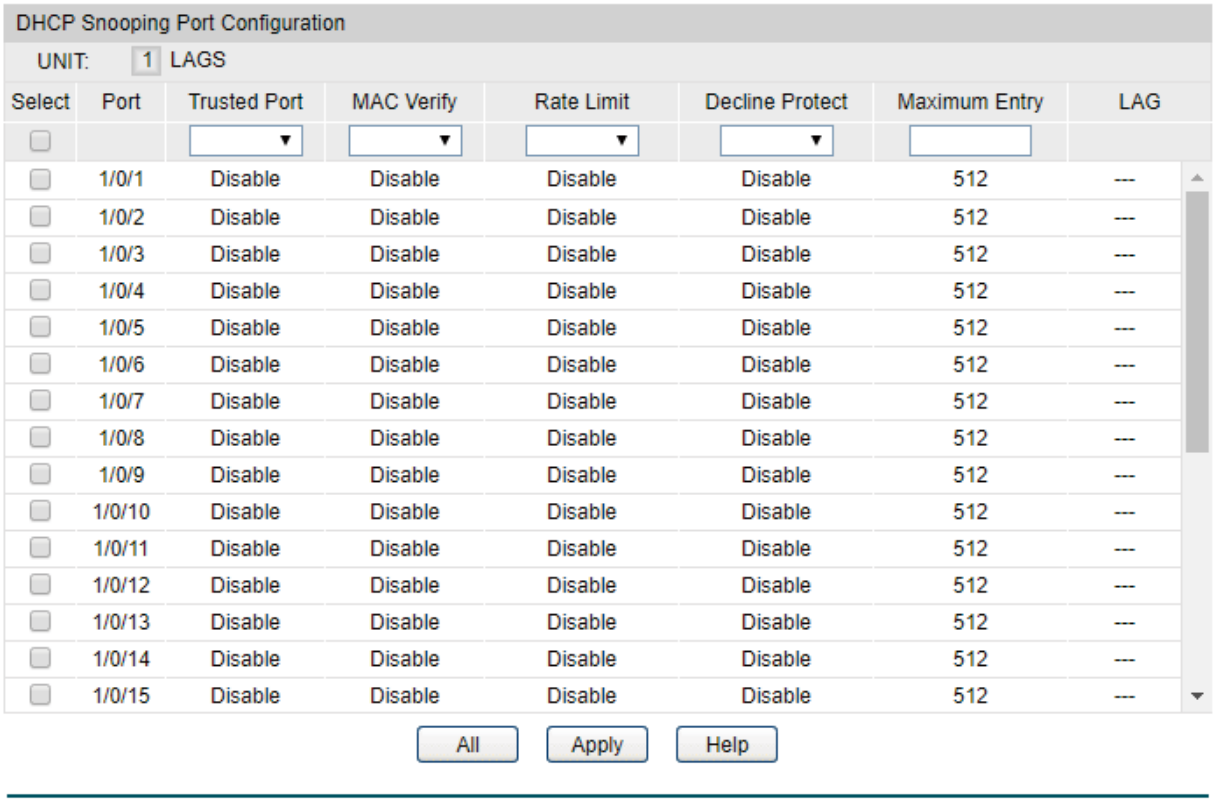
VLAN ID	Specify the VLAN ID in the format shown on the page.
VLAN Configuration Display	Displays the VLANs that have been enabled with DHCP Snooping.

5) Click **Apply**.

4.1.2 Configuring DHCP Snooping on Ports

Choose the menu **Network Security > DHCP Snooping > Port Config** to load the following page.

Figure 4-2 Port Config



Follow these steps to configure DHCP Snooping on the specified port:

1) Select one or more ports and configure the parameters.

Trusted Port	Select Enable to set the port that is connected to the DHCP server as a trusted port. Select Disable to set the other ports as untrusted ports.
MAC Verify	Enable or disable the MAC Verify feature. There are two fields in the DHCP packet that contain the MAC address of the host. The MAC Verify feature compares the two fields of a DHCP packet and discards the packet if the two fields are different. This prevents the IP address resource on the DHCP server from being exhausted by forged MAC addresses.
Rate Limit	Select to enable the rate limit feature and specify the maximum number of DHCP packets that can be forwarded on the port per second. The excessive DHCP packets will be discarded.

Decline Protect	Select to enable the decline protect feature and specify the maximum number of DHCP Decline packets that can be forwarded on the port per second. The excessive DHCP Decline packets will be discarded.
Maximum Entry	Configure the maximum number of binding entries a port can learn via DHCP snooping
LAG	Displays the LAG that the port is in.

2) Click **Apply**.

4.2 Using the CLI

4.2.1 Enabling DHCP Snooping on VLAN

Follow these steps to globally configure DHCP Snooping:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip dhcp snooping** Globally enable DHCP Snooping.
Step 3	**snmp-server traps security dhcp-snoop** Enable Illegal DHCP Server Trap feature to send snmp trap message when untrusted port has received DHCP Server packets.
Step 4	**ip dhcp snooping vlan** *vlan-range* Enable DHCP Snooping on the specified VLAN. *vlan-range:* Enter the vlan range in the format of 1-3, 5.
Step 5	**show ip dhcp snooping** Verify global configuration of DHCP Snooping.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable DHCP Snooping globally and on VLAN 5:

Switch#configure

Switch(config)#ip dhcp snooping

Switch(config)#ip dhcp snooping vlan 5

Switch(config)#show ip dhcp snooping

Global Status: Enable

VLAN ID: 5

Switch(config-if)#end

Switch#copy running-config startup-config

4.2.2 Configuring DHCP Snooping on Ports

Follow these steps to configure DHCP Snooping on the specified ports.

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| interface port-channel** *port-channel-id* **| interface range port-channel** *port-channel-id-list* **}** Enter interface configuration mode.
Step 3	**ip dhcp snooping trust** Set the port that is connected to the DHCP server as a trusted port. The switch can forward the DHCP packets on the trusted port and discard the DHCP response packets on the distrusted port, so as to ensure that users get proper IP addresses from the legal DHCP server.
Step 4	**ip dhcp snooping mac-verify** Enable the MAC Verify feature. There are two fields in the DHCP packet that contain the MAC address of the host. The MAC Verify feature compares the two fields of a DHCP packet and discards the packet if the two fields are different. This prevents the IP address resource on the DHCP server from being exhausted by forged MAC addresses.
Step 5	**ip dhcp snooping limit rate** *value* Enable the limit rate feature and specify the maximum number of DHCP messages that can be forwarded on the port per second. The excessive DHCP packets will be discarded. *value:* Specify the limit rate value. The following options are provided: 0, 5,10,15,20,25 and 30 (packets/second). The default value is 0, which indicates disabling limit rate.
Step 6	**ip dhcp snooping decline rate** *value* Enable the decline protect feature and specify the maximum number of Decline packets can be forwarded per second on the port. The excessive DHCP Decline packets will be discarded. *value:* Specify the limit rate value of Decline packets. The following options are provided: 0, 5,10,15,20,25 and 30 (packets/second). The default value is 0, which indicates disabling this feature.

Step 7	**ip dhcp snooping max-entries** *value* Configure the maximum number of binding entries the port can learn via DHCP snooping. value: Enter the value of maximum number of entries. The valid values are from 0 to 512.
Step 8	**show ip dhcp snooping interface** [**gigabitEthernet** *port* | **port-channel** *port-channel-id*] Verify the DHCP Snooping configuration of the port.
Step 9	**end** Return to privileged EXEC mode.
Step 10	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure port 1/0/1 as a trusted port, enable the MAC verify feature, and set the limit rate as 10 pps and decline rate as 20 pps on this port:

Switch#configure

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

Switch(config-if)#ip dhcp snooping trust

Switch(config-if)#ip dhcp snooping mac-verify

Switch(config-if)#ip dhcp snooping limit rate 10

Switch(config-if)#ip dhcp snooping decline rate 20

Switch(config-if)#show ip dhcp snooping interface gigabitEthernet 1/0/1

Interface	Trusted	MAC-Verify	Limit-Rate	Dec-rate	LAG
---	---	---	---	---	---
Gi1/0/1	Enable	Enable	10	20	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

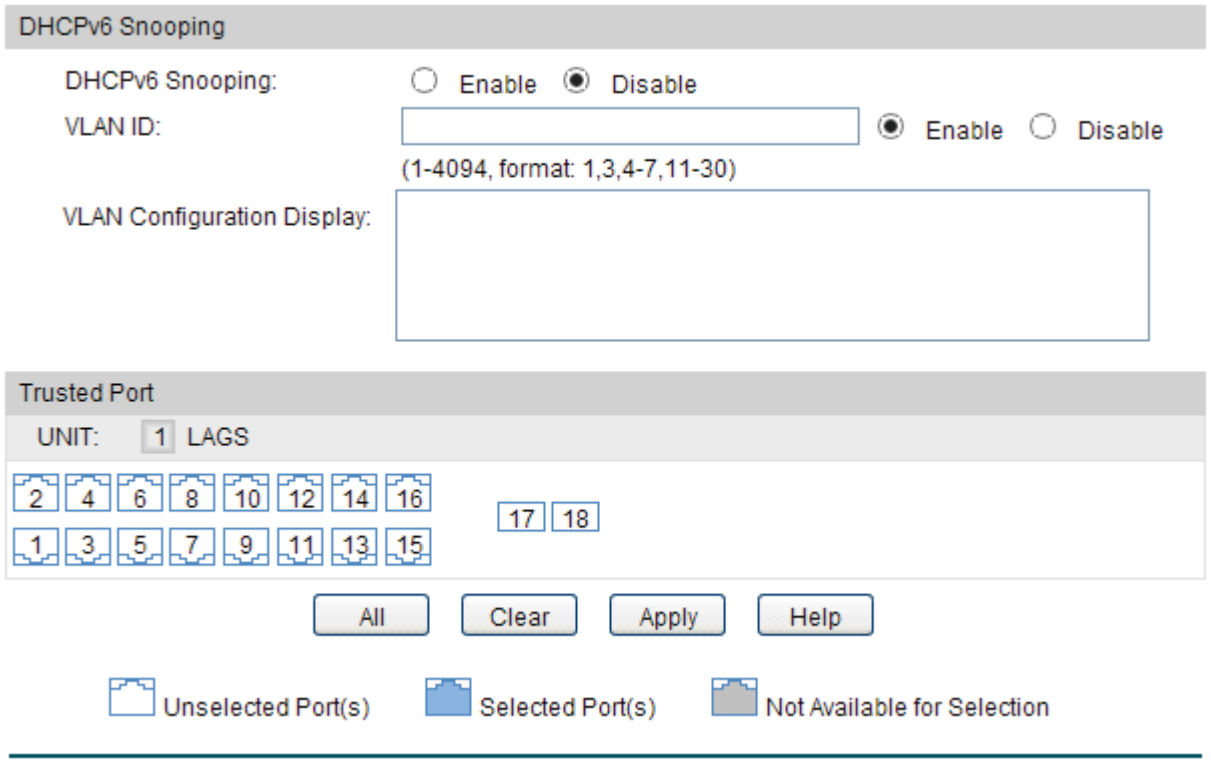
5 DHCPv6 Snooping Configuration

Tips: The switch can dynamically bind the entries via DHCPv6 Snooping after DHCPv6 Snooping is configured. By default, the binding entries are applied to both IP Source Guard and ND Detection.

5.1 Using the GUI

Choose the menu **Network Security > DHCPv6 Snooping > DHCPv6 Snooping** to load the following page.

Figure 5-1 DHCPv6 Snooping



Follow these steps to configure DHCPv6 Snooping:

1) In the **DHCPv6 Snooping** section, enable DHCPv6 Snooping globally and specify one or more VLAN IDs to enable DHCPv6 Snooping on the VLAN(s).

DHCPv6 Snooping	Globally enable DHCPv6 Snooping.
VLAN ID	Specify the VLAN ID(s) in the format shown on the page.
VLAN Configuration Display	Displays the VLANs that have been enabled with DHCPv6 Snooping.

2) In the **Trusted Port** section, select the port that is connected to the DHCPv6 server as a trusted port, and the other unselected ports are the untrusted by default.

3) Click **Apply**.

5.2 Using the CLI

Follow these steps to configure DHCPv6 Snooping:

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 dhcp snooping** Globally enable DHCPv6 Snooping.
Step 3	**ipv6 dhcp snooping vlan** *vlan-range* Enable DHCPv6 Snooping on the specified VLAN. *vlan-range:* Enter the vlan range in the format of 1-3, 5.
Step 4	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| interface port-channel** *port-channel-id* **| interface range port-channel** *port-channel-id-list* **}** Enter interface configuration mode.
Step 5	**ipv6 dhcp snooping trust** Configure the port(s) as trusted port(s). Generally, the port that is connected to the DHCPv6 server is configured as a trusted port.
Step 6	**show ipv6 dhcp snooping** Verify the global DHCPv6 DHCP Snooping configuration.
Step 7	**show ipv6 dhcp snooping interface { fastEthernet** *port* **| gigabitEthernet** *port* **| port-channel** *port-channel-id* **}** Verify the DHCPv6 Snooping configuration of the port.
Step 8	**end** Return to privileged EXEC mode.
Step 9	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable DHCP Snooping globally and on VLAN 5, and configure port 1/0/1 as a trusted port:

Switch#configure

Switch(config)#ipv6 dhcp snooping

Switch(config)#ipv6 dhcp snooping vlan 5

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

Switch(config-if)#ipv6 dhcp snooping trust

Switch(config-if)#show ipv6 dhcp snooping

Global Status: Enable

VLAN ID: 5

Switch(config-if)#show ipv6 dhcp snooping interface gigabitEthernet 1/0/1

Interface Trusted LAG

--------- ------- ---

Gi1/0/1 Enable N/A

Switch(config-if)#end

Switch#copy running-config startup-config

6 ARP Inspection Configurations

With ARP Inspection configurations, you can:

- Configure ARP Detection
- Configure ARP Defend
- View ARP Statistics

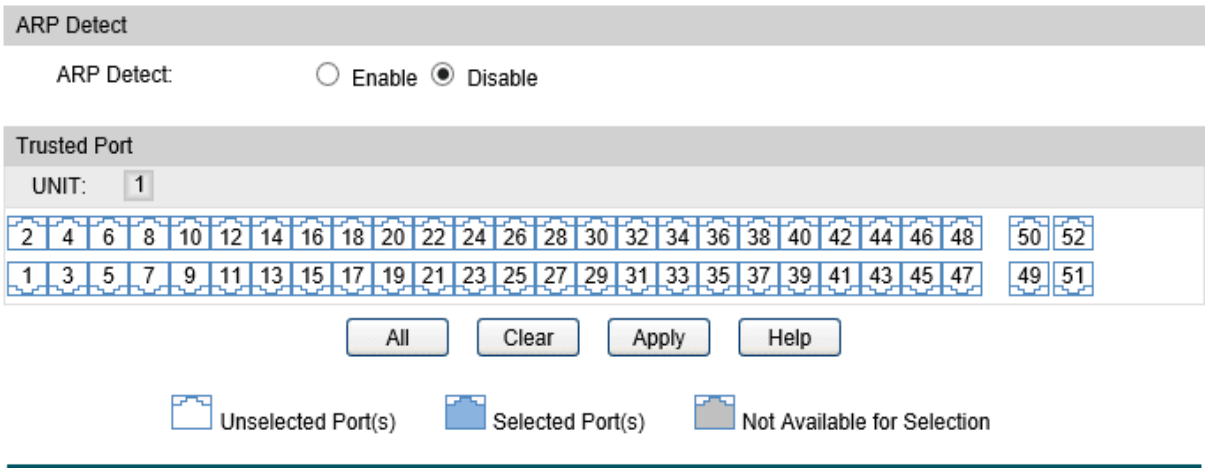
6.1 Using the GUI

6.1.1 Configuring ARP Detection

The ARP Detection feature allows the switch to detect the ARP packets based on the binding entries in the IP-MAC Binding Table and filter out the illegal ARP packets. Before configuring ARP Detection, complete IP-MAC Binding configuration. For details, refer to *IP-MAC Binding Configurations*.

Choose the menu **Network Security > ARP Inspection > ARP Detect** to load the following page.

Figure 6-1 ARP Detect



Follow these steps to configure ARP Detection:

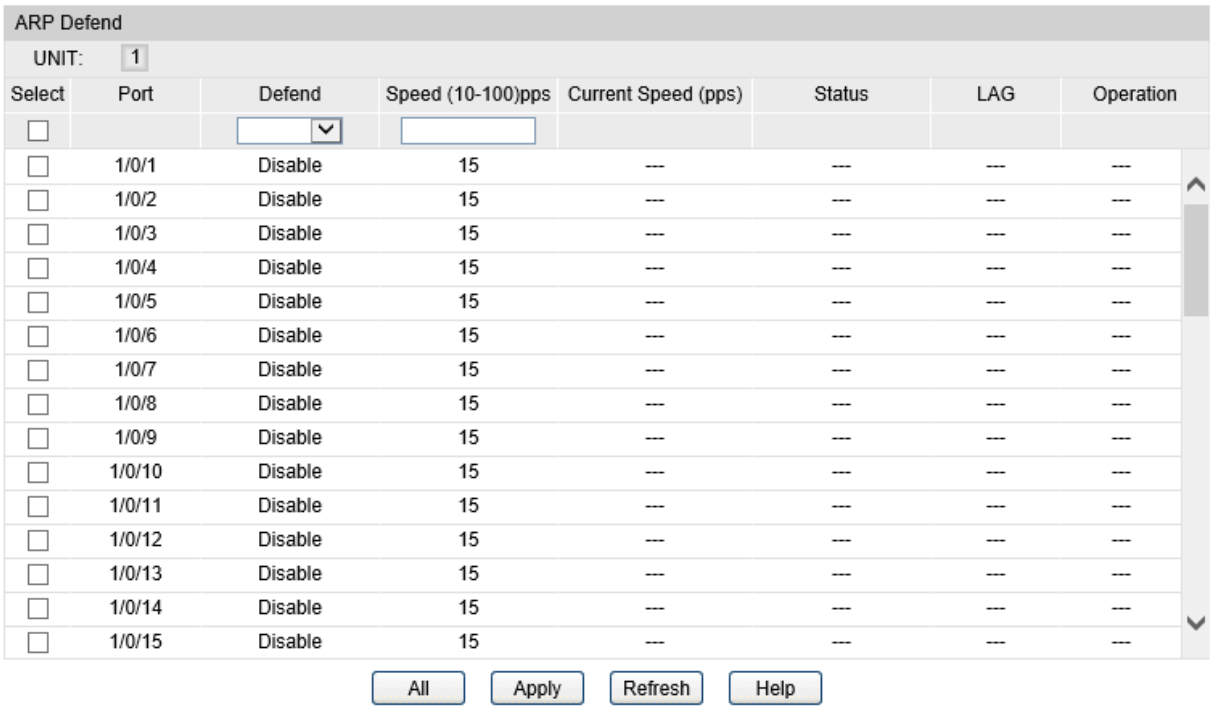
1) In the **ARP Detect** section, enable the ARP Detection feature.
2) In the **Trusted Port** section, select one or more ports to be configured as the trusted port(s), on which the ARP Detection function will be inactive. The specific ports, such as up-link ports and routing ports are suggested to be set as trusted.
3) Click **Apply**.

6.1.2 Configuring ARP Defend

With ARP Defend enabled, the switch can terminate receiving the ARP packets for 300 seconds when the transmission speed of the legal ARP packet on the port exceeds the defined value so as to avoid ARP Attack flood.

Choose the menu **Network Security > ARP Inspection > ARP Defend** to load the following page.

Figure 6-2 ARP Defend



Follow these steps to configure ARP Defend:

1) Select one or more ports and configure the parameters.

Defend	Enable the ARP Defend feature.
Speed (10-100) pps	Specify the maximum number of the ARP packets that can be received on the port per second. The valid values are from 10 to 100 pps (packet/second), and the default value is 15.
Current Speed (pps)	Displays the current speed of receiving the ARP packets on the port.
Status	Displays the status of the ARP attack: **Normal**: The forwarding of ARP packets on the port is normal. **Drop ARP300sec**: The speed of receiving the ARP packets has exceeded the specified value, and the port will drop the received ARP packets in the next 300 seconds.
LAG	Displays the LAG that the port is in.
Operation	Click the **Recover** button to restore the port to the normal status. The ARP Defend for this port will be re-enabled.

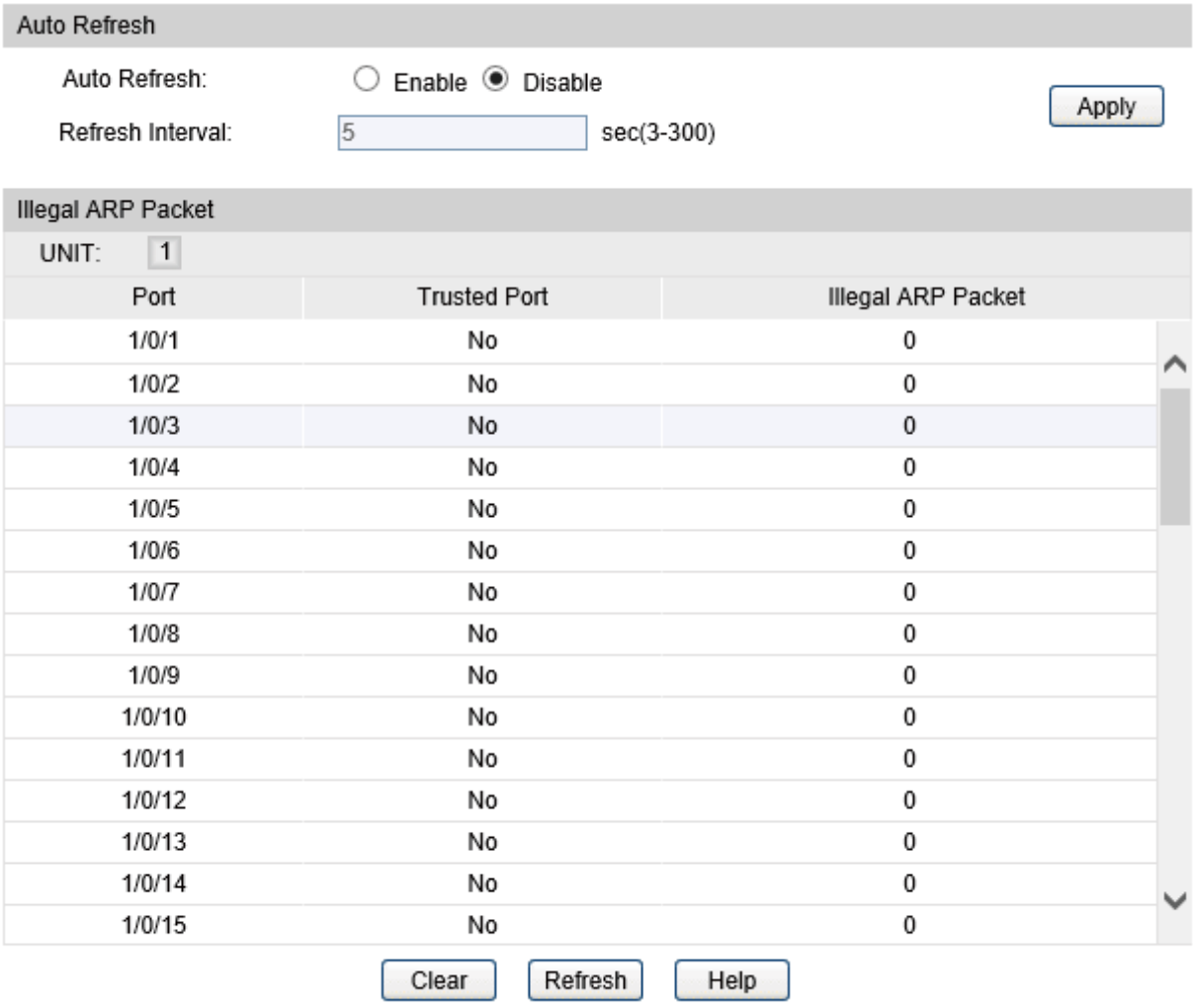
2) Click **Apply**.

6.1.3 Viewing ARP Statistics

You can view the number of the illegal ARP packets received on each port, which facilitates you to locate the network malfunction and take the related protection measures.

Choose the menu **Network Security > ARP Inspection > ARP Statistics** to load the following page.

Figure 6-3 ARP Statistics



In the **Auto Refresh** section, you can enable the auto refresh feature and specify the refresh interval, and thus the web page will be automatically refreshed.

In the **Illegal ARP Packet** section, you can view the number of illegal ARP packets on each port.

Trusted Port	Indicates whether the port is an ARP trusted port or not.
Illegal ARP Packet	Displays the number of the received illegal ARP packets.

6.2 Using the CLI

6.2.1 Configuring ARP Detection

The ARP Detection feature allows the switch to detect the ARP packets basing on the binding entries in the IP-MAC Binding Table and filter the illegal ARP packets. Before configuring ARP Detection, complete IP-MAC Binding configuration. For details, refer to *IP-MAC Binding Configurations*.

Follow these steps to configure ARP Detection:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip arp inspection** Globally enable the ARP Detection feature.
Step 3	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **}** Enter interface configuration mode.
Step 4	**ip arp inspection trust** Configure the port as a trusted port, on which the ARP Detection function will not take effect. The specific ports, such as up-linked ports and routing ports are suggested to be set as trusted ports.
Step 5	**show ip arp inspection** Verify the ARP Inspection configuration.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to globally enable ARP Detection and configure port 1/0/1 as a trusted port.

Switch#configure

Switch(config)#ip arp inspection

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

Switch(config-if)#ip arp inspection trust

Switch(config-if)#show ip arp inspection

ARP detection global status: Enabled

Port Trusted

Gi1/0/1 YES

Gi1/0/2 NO

...

Switch(config-if)#end

Switch#copy running-config startup-config

6.2.2 Configuring ARP Defend

With ARP Defend enabled, the switch can terminate receiving the ARP packets for 300 seconds when the transmission speed of the legal ARP packet on the port exceeds the defined value so as to avoid ARP Attack flood.

Follow these steps to configure ARP Defend:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **}** Enter interface configuration mode.
Step 3	**ip arp inspection** Enable the ARP defend feature on the port.
Step 4	**ip arp inspection limit-rate** *value* Specify the maximum number of the ARP packets can be received on the port per second. *value:* Specify the limit rate value. The valid values are from 10 to 100 pps (packets/second), and the default value is 15.
Step 5	**show ip arp inspection interface** (Optional) View the configurations and status of the ports.
Step 6	**ip arp inspection recover** (Optional) For ports which the speed of receiving ARP packets has exceeded the limit, use this command to restore the port from Discard status to Normal status.
Step 7	**end** Return to privileged EXEC mode.
Step 8	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable ARP Defend and configure the ARP inspection limit-rate as 20 pps on port 1/0/2:

Switch#configure

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

Switch(config-if)#ip arp inspection

Switch(config-if)#ip arp inspection limit-rate 20

Switch(config-if)#show ip arp inspection interface gigabitEthernet 1/0/2

Port	OverSpeed	Rate	Current	Status	LAG
Gi1/0/2	Enabled	20	N/A	Normal	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

The following example shows how to restore the port 1/0/1 that is in Discard status to Normal status:

Switch#configure

Switch(config)#show ip arp inspection interface

Port	OverSpeed	Rate	Current	Status	LAG
Gi1/0/1	Enabled	15	N/A	Discard,290s	N/A
Gi1/0/2	Enabled	15	N/A	Normal	N/A

...

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

Switch(config-if)#ip arp recover

Switch(config-if)#show ip arp inspection interface gigabitEthernet 1/0/1

Port	OverSpeed	Rate	Current	Status	LAG
Gi1/0/1	Disabled	15	N/A	Normal	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

6.2.3 Viewing ARP Statistics

On privileged EXEC mode or any other configuration mode, you can use the following command to view ARP statistics:

show ip arp inspection statistics

View the ARP statistics on each port, including whether the port is trusted port and the number of received ARP packets on the port.

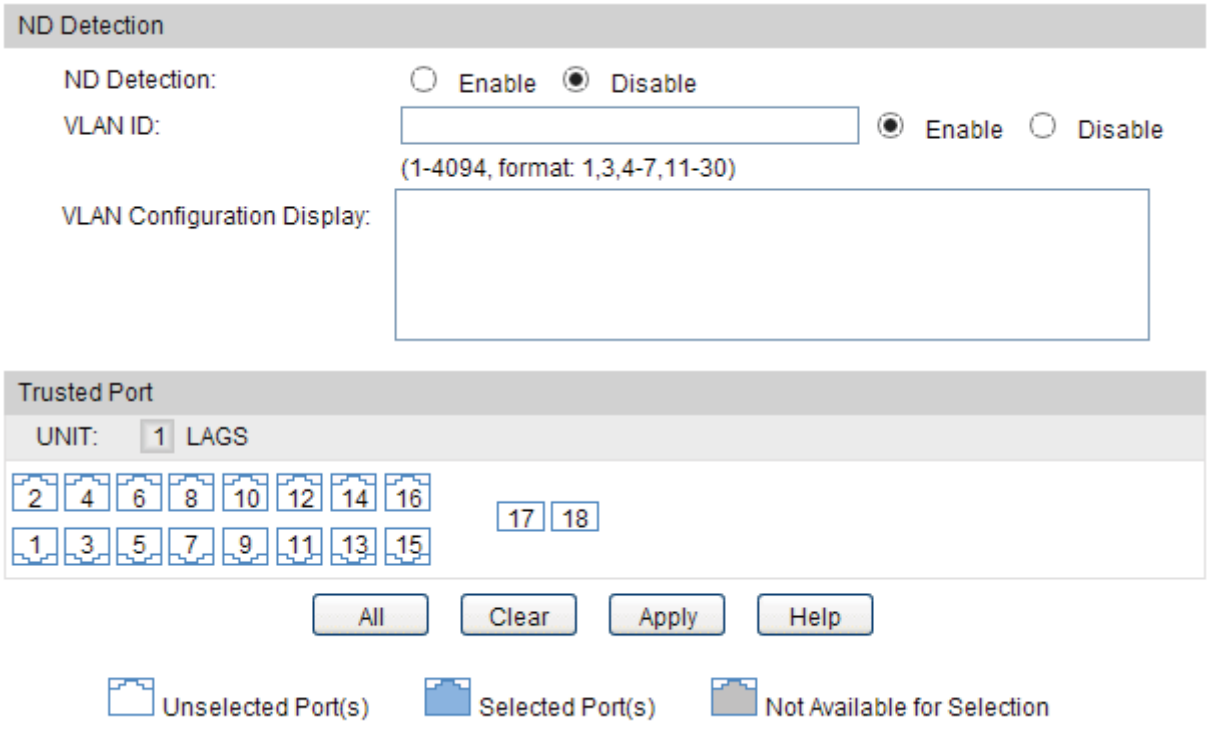
7 ND Detection Configuration

7.1 Using the GUI

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.

Choose the menu **Network Security > ND Detection > ND Detection** to load the following page.

Figure 7-1 ND Detection



Follow these steps to configure ND Detection:

1) In the **ND Detection** section, enable ND Detection globally and specify one or more

VLAN IDs to enable DHCPv6 Snooping on the VLAN(s).

ND Detection	Globally enable ND Detection.
VLAN ID	Specify the VLAN ID(s) in the format shown on the page.
VLAN Configuration Display	Displays the VLANs that have been enabled with ND Detection.

2) In the **Trusted Port** section, select one or more ports to be configured as the trusted port(s), on which the ND packets will not be checked. The specific ports, such as up-link ports and routing ports are suggested to be set as trusted.

3) Click **Apply**.

7.2 Using the CLI

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.

Follow these steps to configure ND Detection:

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 nd detection** Globally enable the ND Detection feature.
Step 3	**ipv6 nd detection vlan** *vlan-range* Enable ND Detection on the specified VLAN. *vlan-range:* Enter the vlan range in the format of 1-3, 5.
Step 4	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-id-list* **}** Enter interface configuration mode.
Step 5	**ipv6 nd detection trust** Configure the port as a trusted port, on which the ND packets will not be checked. The specific ports, such as up-linked ports and routing ports are suggested to be set as trusted ports.
Step 6	**show ipv6 nd detection** Verify the global ND Detection configuration.

Step 7	**show ipv6 nd detection interface { fastEthernet** *port* **| gigabitEthernet** *port* **| port-channel** *port-channel-id* **}** Verify the global ND Detection configuration of the port.
Step 8	**end** Return to privileged EXEC mode.
Step 9	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable ND Detection globally and on VLAN 1, and configure port 1/0/1 as trusted port:

Switch#configure

Switch(config)#ipv6 nd detection

Switch(config)#ipv6 nd detection vlan 1

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

Switch(config-if)#ipv6 nd detection trust

Switch(config-if)#show ipv6 nd detection

Global Status: Enable

VLAN ID: 1

Switch(config-if)#show ipv6 nd detection interface gigabitEthernet 1/0/1

Interface Trusted LAG

--------- ------- ---

Gi1/0/1 Enable N/A

Switch(config-if)#end

Switch#copy running-config startup-config

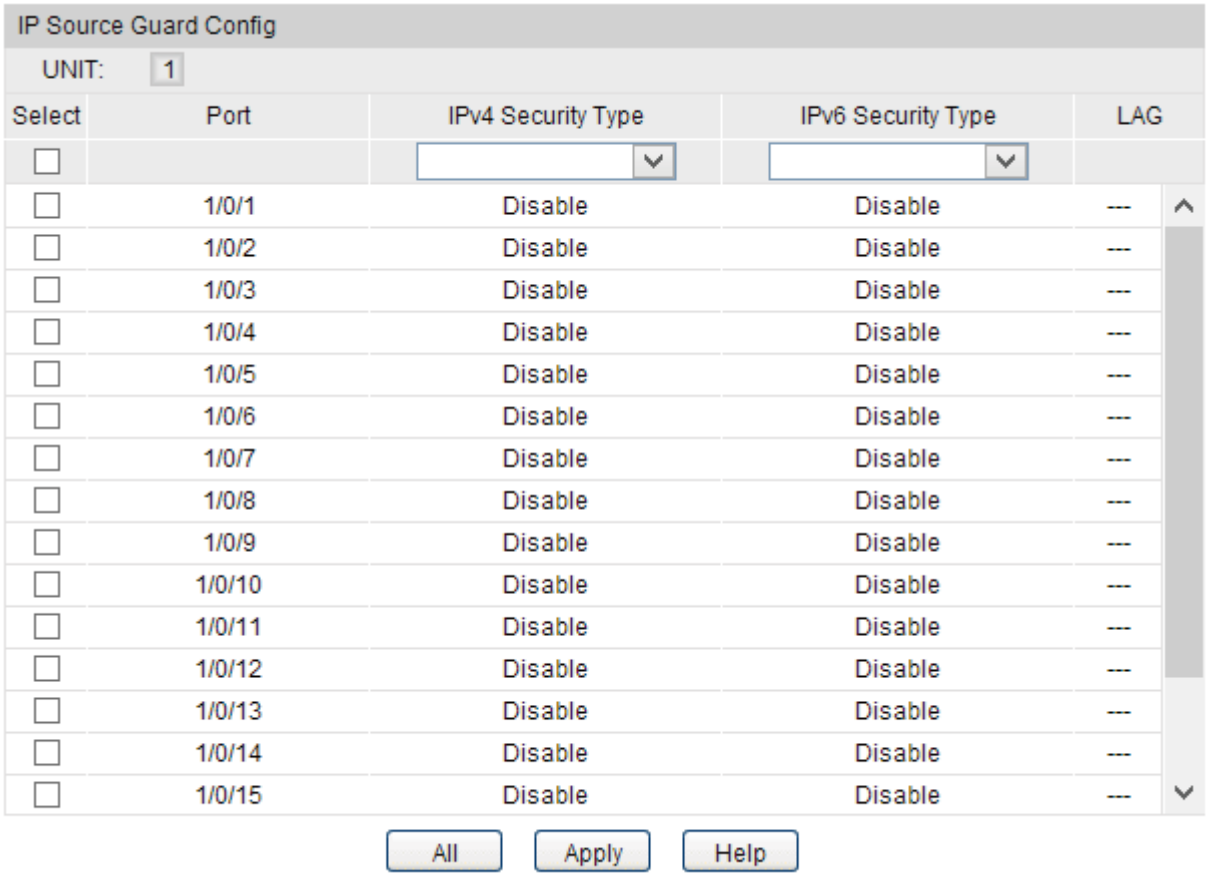
8 IP Source Guard Configuration

8.1 Using the GUI

The IP Source Guard feature allows the switch to filter the packets that do not match the rules of IP-MAC Binding Table or IPv6-MAC Binding Table. Before configuring IP Source Guard, complete IP-MAC Binding or IPv6-MAC Binding configuration. For details, refer to *IP-MAC Binding Configurations* and IPv6-MAC Binding Configurations.

Choose the menu **Network Security > IP Source Guard > IP Source Guard** to load the following page.

Figure 8-1 IP Source Guard



Follow these steps to configure IP Source Guard:

1) Select one or more ports and configure IP Source Guard on the port(s).

IPv4 Security Type	Select Security Type on the port for IPv4 packets. The following options are provided: **Disable**: The IP Source Guard feature is disabled on the port. **SIP+MAC**: Only the packet with its source IP address, source MAC address and port number matching the IP-MAC binding rules can be processed, otherwise the packet will be discarded.
IPv6 Security Type	Select the Security Type on the port for IPv6 packets. The following options are provided: **Disable**: The IP Source Guard feature is disabled on the port. **SIPv6+MAC**: Only the packet with its source IPv6 address, source MAC address and port number matching the IPv6-MAC binding rules can be processed, otherwise the packet will be discarded.
LAG	Displays the LAG that the port is in.

2) Click **Apply**.

8.2 Using the CLI

The IP Source Guard feature allows the switch to filter the packets that do not match the rules of IP-MAC Binding Table or IPv6-MAC Binding Table. Before configuring IP Source Guard, complete IP-MAC Binding or IPv6-MAC Binding configurations. For details, refer to *IP-MAC Binding Configurations* and IPv6-MAC Binding Configurations.

Follow these steps to configure IP Source Guard:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **}** Enter interface configuration mode.
Step 3	Enable IP Source Guard on the port for IPv4 packets, IPv6 packets or both. **ip verify source {** sip+mac **}** Enable IP Source Guard for IPv4 packets. sip+mac*:* Only the packet with its source IP address, source MAC address and port number matching the IP-MAC binding rules can be processed, otherwise the packet will be discarded. **ipv6 verify source {** sipv6+mac **}** Enable IP Source Guard for IPv6 packets. sipv6+mac*:* Only the packet with its source IPv6 address, source MAC address and port number matching the IPv6-MAC binding rules can be processed, otherwise the packet will be discarded.
Step 4	Verify the IP Source Guard configuration on the specified port. **show ip verify source interface gigabitEthernet** *port* Verify the IP Source Guard configuration for IPv4 packets. **show ipv6 verify source interface gigabitEthernet** *port* Verify the IP Source Guard configuration for IPv6 packets.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable IP Source Guard on port 1/0/1 for IPv6 packets:

Switch#configure

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

Switch(config-if)#ipv6 verify source sipv6+mac

Switch(config-if)#show ipv6 verify source interface gigabitEthernet 1/0/1

Port	Security-Type	LAG
----	----------	----
Gi1/0/1	SIPv6+MAC	N/A

Switch(config-if)#end

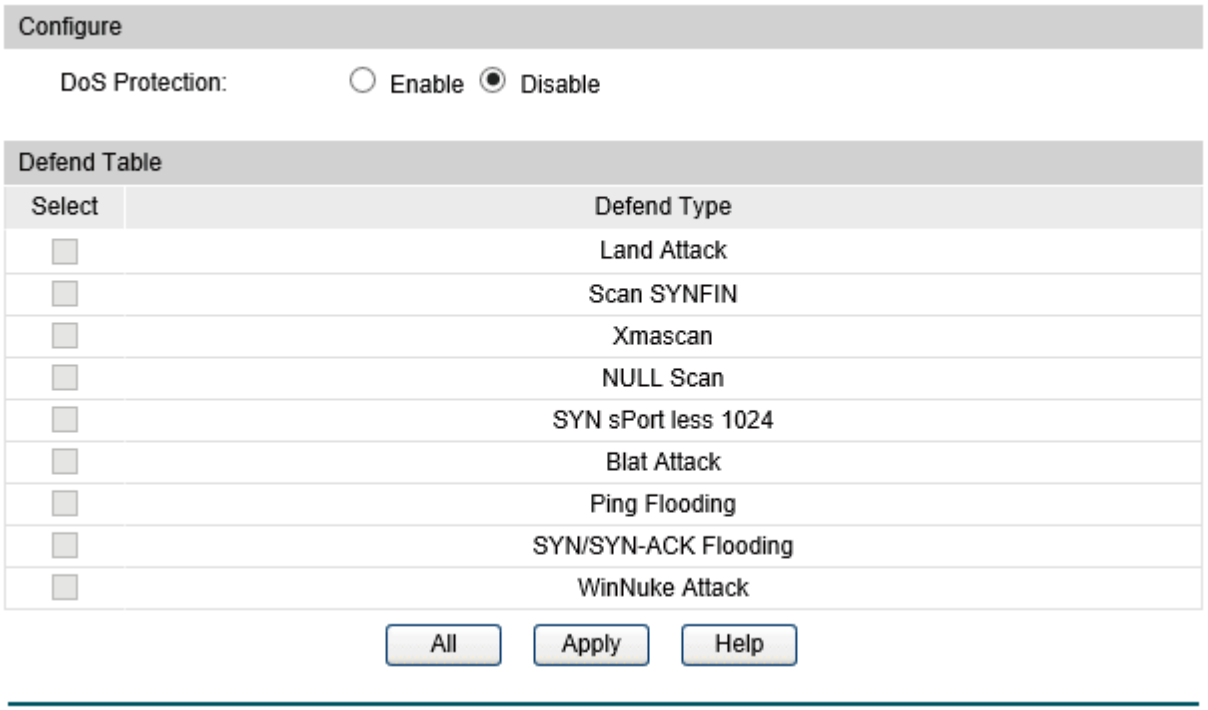
Switch#copy running-config startup-config

9 DoS Defend Configuration

9.1 Using the GUI

Choose the menu **Network Security > DoS Defend > DoS Defend** to load the following page.

Figure 9-1 Dos Defend



Follow these steps to configure DoS Defend:

1) In the **Configure** section, enable DoS Protection.
2) In the **Defend Table** section, select one or more defend types according to your needs. The following table introduces each type of DoS attack.

Land Attack	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.
Xmascan	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.
SYN sPort less 1024	The attacker sends the illegal packet with its TCP SYN field set to 1 and source port smaller than 1024.
Blat Attack	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 Flooding	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/SYN-ACK Flooding	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.
WinNuke Attack	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.

3) Click **Apply**.

9.2 Using the CLI

Follow these steps to configure DoS Defend:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip dos-prevent** Globally enable the DoS defend feature.

Step 3	**ip dos-prevent type {** land | scan-synfin | xma-scan | null-scan | port-less-1024 | blat | ping-flood | syn-flood | win-nuke **}** Configure one or more defend types according to your needs. The types of DoS attack are introduced as follows. land: The attacker sends a specific fake SYN (synchronous) packet to the destination host. Because both 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, a 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 the control fields set to 0 are considered as the illegal packets. 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 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: An Operation System with bugs cannot process the URG (Urgent Pointer) of TCP packets. If the attacker sends TCP packets to port139 (NetBIOS) of the host with Operation System bugs, it will cause blue screen.
Step 4	**show ip dos-prevent** Verify the Dos Defend configuration.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable the DoS Defend type named land:

Switch#configure

Switch(config)#ip dos-prevent

Switch(config)#ip dos-prevent type land

Switch(config)#show ip dos-prevent

Type	Status
---	---
Land Attack	Enabled
Scan SYNFIN	Disabled
Xmascan	Disabled

...

Switch(config)#end

Switch#copy running-config startup-config

10 802.1X Configuration

To complete the 802.1X configuration, follow these steps:

1) Configure the RADIUS server.
2) Configure 802.1X globally.
3) Configure 802.1X on ports.

Configuration Guidelines

802.1X authentication and Port Security cannot be enabled at the same time. Before enabling 802.1X authentication, make sure that Port Security is disabled.

10.1 Using the GUI

10.1.1 Configuring the RADIUS Server

Enable AAA function on the switch, configure the parameters of RADIUS sever and configure the RADIUS server group.

- Enabling AAA function

Choose the menu **Network Security > AAA > Global Config** to load the following page.

Figure 10-1 Enable AAA Function

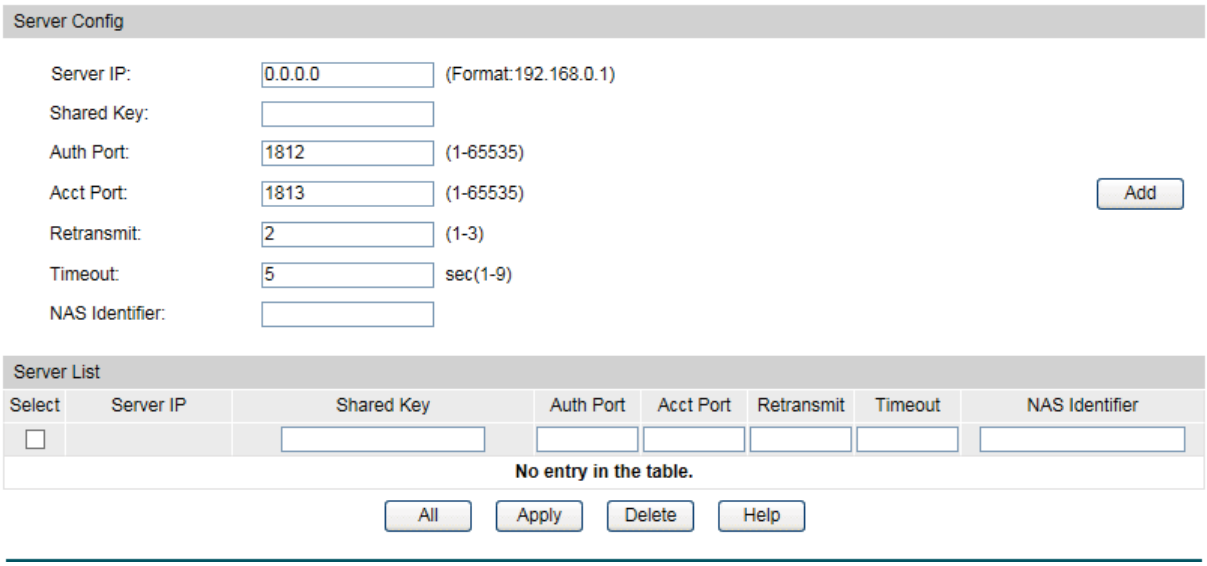


In the **Global Config** section, enable AAA function on the switch and click **Apply**.

Adding the RADIUS Server

Choose the menu **Network Security > AAA > RADIUS Config** to load the following page.

Figure 10-2 RADIUS Config



Follow these steps to create a protocol template:

1) In the **Server Config** section, configure the parameters of RADIUS server.
2) Click **Apply**.

Server IP	Enter the IP address of the server running the RADIUS secure protocol.
Shared Key	Enter the shared key between the RADIUS server and the switch. The RADIUS server and the switch use the key string to encrypt passwords and exchange responses.
Auth Port	Specify the UDP destination port on the RADIUS server for authentication requests. The default setting is 1812.
Acct Port	Specify the UDP destination port on the RADIUS server for accounting requests. The default setting is 1813.
Retransmit	Specify the number of times a request is resent to the server if the server does not respond. The default setting is 2.
Timeout	Specify the time interval that the switch waits for the server to reply before resending. The default setting is 5 seconds.

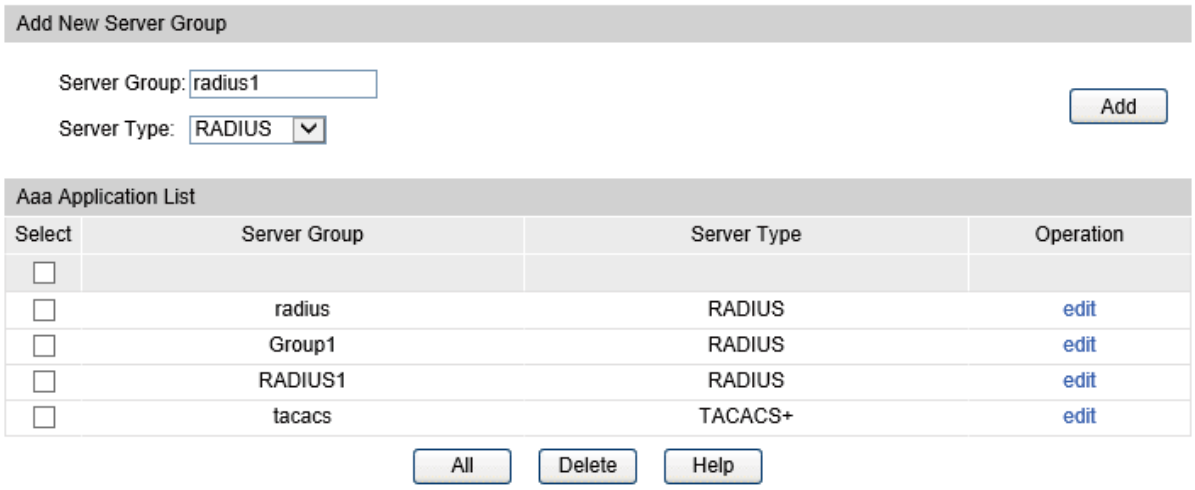
NAS Identifier	Specify the name of the NAS (Network Access Server) to be contained in RADIUS packets for identification. It ranges from 1 to 31 characters. The default value is the MAC address of the switch. Generally, the NAS indicates the switch itself.

Configuring the RADIUS Server Group

You can configure the radius servers for authentication and accounting. If multiple radius servers are available, you are suggested to add them to different server groups respectively for authentication and accounting.

Choose the menu **Network Security > AAA > Server Group** to load the following page.

Figure 10-3 Adding a Server Group



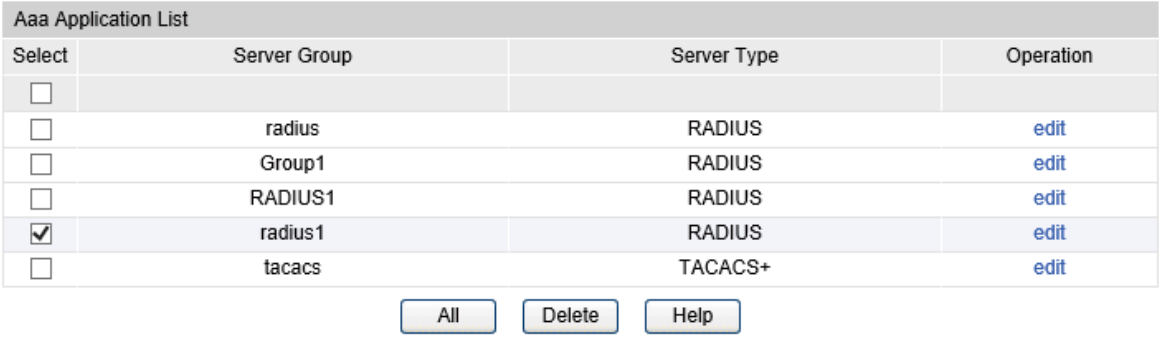
Follow these steps to create a protocol template:

1) In the **Add New Server Group** section, specify the name and server type for the new server group, and click **Add**.

Server Group:	Specify the name of the new server group.
Server Type:	Select the type of the server group as RADIUS.

2) Select the newly added group, and click **edit** in the **Operation** column.

Figure 10-4 Edit the Group



3) Select the server to be added to the group from the **Server IP** drop-down list . Then click **Add** to add this server to the server group.

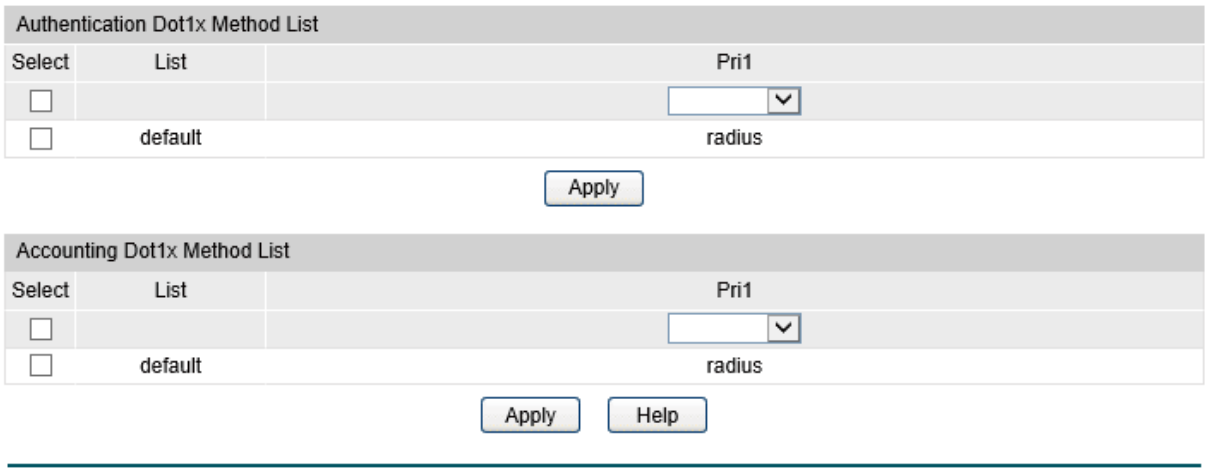
Figure 10-5 Add Server to Group



Configuring the Dot1x List

Choose the menu **Network Security > AAA > Dot1x List** to load the following page.

Figure 10-6 Configuring the Dot1x List



Follow these steps to configure RADIUS server groups for 802.1X authentication and accounting:

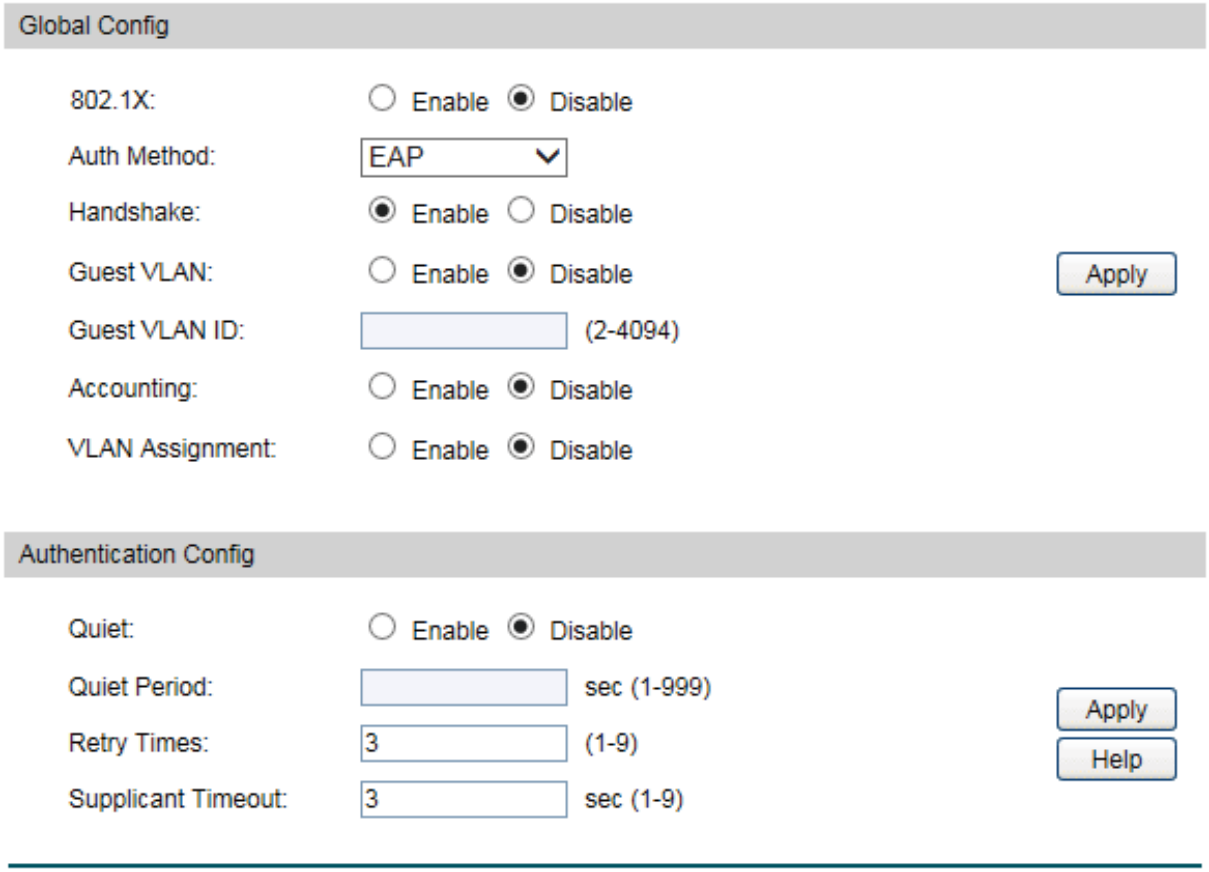
1) In the **Authentication Dot1x Method List** section, select an existing RADIUS server group for authentication from the Pri1 drop-down list and click **Apply**.

2) In the **Accounting Dot1x Method List** section, select an existing RADIUS server group for accounting from the Pri1 drop-down list and click **Apply**.

10.1.2 Configuring 802.1X Globally

Choose the menu **Network Security > 802.1X > Global Config** to load the following page.

Figure 10-7 Global Config



Follow these steps to configure 802.1X global parameters:

1) In the **Global Config** section, enable 802.1X globally and click **Apply**.

Auth Method	Select the 802.1X authentication method. **PAP**: The 802.1X authentication system uses EAP packets to exchange information between the switch and the client. The transmission of EAP (Extensible Authentication Protocol) packets is terminated at the switch and the EAP packets are converted to other protocol (such as RADIUS) packets, and transmitted to the authentication server. **EAP**: The 802.1X authentication system uses EAP packets to exchange information between the switch and the client. The EAP packets with authentication data are encapsulated in the advanced protocol (such as RADIUS) packets, and transmitted to the authentication server.
Handshake	Enable or disable the Handshake feature. The Handshake feature is used to detect the connection status between the TP-Link 802.1X Client and the switch. Please disable Handshake feature if you are using other client softwares instead of TP-Link 802.1X Client.

Guest VLAN	Select whether to enable Guest VLAN. By default, it is disabled. If the Guest VLAN is enabled, a port can access resources in the guest VLAN even though the port is not yet authenticated; if guest VLAN is disabled and the port is not authenticated, the port cannot visit any resource in the LAN.
Guest VLAN ID	Enter the guest VLAN's ID. It must be an existing VLAN with the ID ranging from 2 to 4094.
Accounting	Enable or disable 802.1X accounting feature.
VLAN Assignment	Enable or disable the 802.1X VLAN assignment feature. 802.1x VLAN assignment is a technology allowing the RADIUS server to send the VLAN assignment to the port when the port is authenticated. If the assigned VLAN does not exist on the switch, the switch will create the related VLAN automatically, add the authenticated port to the VLAN and change the PVID based on the assigned VLAN. If the assigned VLAN exists on the switch, the switch will directly add the authenticated port to the related VLAN and change the PVID instead of creating a new VLAN. If no VLAN is supplied by the RADIUS server or if 802.1x authentication is disabled, the port will be in its original VLAN after successful authentication.

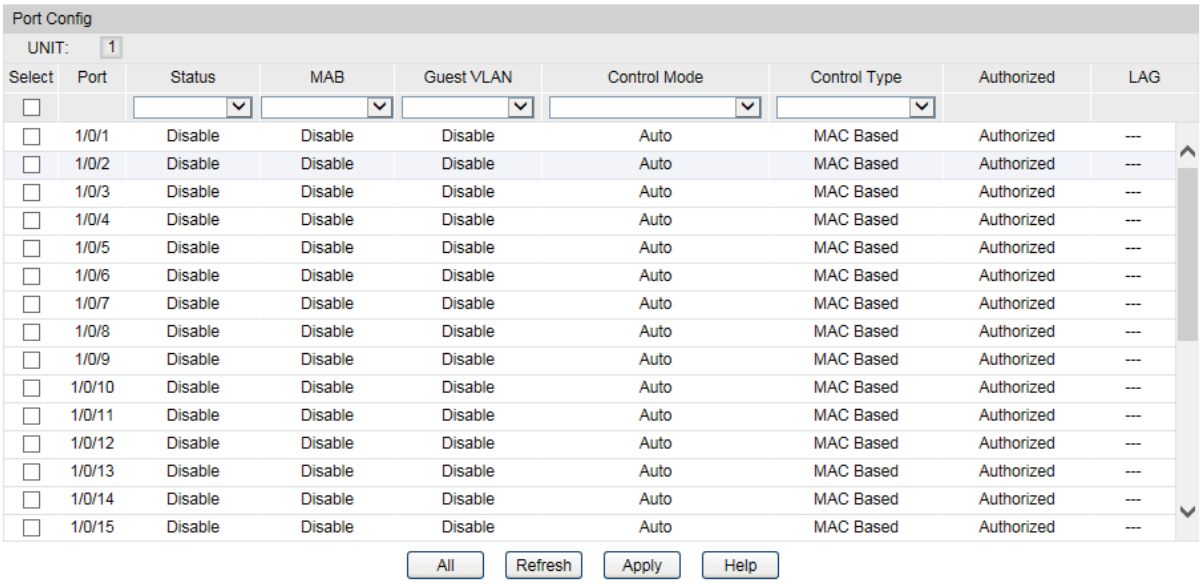
2) In the **Authentication Config** section, enable Quiet, configure the Quiet timer, and click **Apply**.

Quiet	Enable or disable the Quiet timer.
Quiet Period	Specify the Quiet Period. It ranges from 1 to 999 seconds and the default time is 10 seconds. The quiet period starts after the authentication fails. During the quiet period, the switch does not process authentication requests from the same client.
Retry Times	Specify the maximum number of attempts to send the authentication packet. It ranges from 1 to 9 times and the default is 3 times.
Supplicant Timeout	Specify the maximum time which the switch waits for a response from the client. It ranges from 1 to 9 seconds and the default time is 3 seconds. If the switch does not receive any reply from the client within the specified time, it will resend the request.

10.1.3 Configuring 802.1X on Ports

Choose the menu **Network Security > 802.1X > Port Config** to load the following page.

Figure 10-8 Port Config



Configure 802.1X authentication on the desired port and click **Apply**.

Status	Enable 802.1X authentication on the port.
Guest VLAN	Select whether to enable Guest VLAN on the port.
MAB	Select whether to enable the MAB (MAC-Based Authentication Bypass) feature for the port. With MAB feature enabled, the switch automatically sends the authentication server a RADIUS access request frame with the client's MAC address as the username and password. It is also necessary to configure the RADIUS server with the client's information for authentication. You can enable this feature on IEEE 802.1x ports connected to devices without 802.1X capability. For example, most printers, IP phones and fax machines do not have 802.1X capability.
Control Mode	Select the Control Mode for the port. By default, it is Auto. **Auto**: If this option is selected, the port can access the network only when it is authenticated. **Force-Authorized**: If this option is selected, the port can access the network without authentication. **Force-Unauthorized**: If this option is selected, the port can never be authenticated.
Control Type	Select the Control Type for the port. By default, it is MAC Based. **MAC Based**: All clients connected to the port need to be authenticated. **Port Based**: If a client connected to the port is authenticated, other clients can access the LAN without authentication.

Authorized	Displays whether the port is authorized or not.
LAG	Displays the LAG the port belongs to.

Note:

If a port is in an LAG, its 802.1X authentication function cannot be enabled. Also, a port with 802.1X authentication enabled cannot be added to any LAG.

10.2 Using the CLI

10.2.1 Configuring the RADIUS Server

Follow these steps to configure RADIUS:

Step 1	**configure** Enter global configuration mode.
Step 2	**aaa enable** Enable the AAA function globally.
Step 3	**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* **}]** Add the RADIUS server and configure the related parameters as needed. **host** *ip-address*: Enter the IP address of the server running the RADIUS protocol. **auth-port** *port-id*: Specify the UDP destination port on the RADIUS server for authentication requests. The default setting is 1812. **acct-port** *port-id:* Specify the UDP destination port on the RADIUS server for accounting requests. The default setting is 1813. Generally, the accounting feature is not used in the authentication account management. **timeout** *time*: Specify the time interval that the switch waits for the server to reply before resending. The valid values are from 1 to 9 seconds and the default setting is 5 seconds. **retransmit** *number*: Specify the number of times a request is resent to the server if the server does not respond. The valid values are from 1 to 3 and the default setting is 2. **nas-id** *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. **key {** [0] *string* **|** 7 *encrypted-string* **}**: Specify the shared key. 0 and 7 prevent 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 server, which contains 31 characters at most. *encrypted-string* is a symmetric encrypted key with a fixed length, which you can copy from the configuration file of another switch. The key or encrypted-key you configured here will be displayed in the encrypted form.

Step 4	**aaa group** radius *group-name* Create a radius server group. radius: Specify the group type as radius. *group-name*: Specify a name for the group.
Step 5	**server** *ip-address* Add the existing servers to the server group. *ip-address*: Specify IP address of the server to be added to the group.
Step 6	**exit** Return to global configuration mode.
Step 7	**aaa authentication dot1x default** { *method* } Select the radius group for 802.1X authentication. *method:* Specify the radius group for 802.1X authentication. **aaa accounting dot1x default** { *method* } Select the radius group for 802.1X accounting. *method:* Specify the radius group for 802.1X accounting. Note: If multiple radius servers are available, you are suggested to add them to different server groups respectively for authentication and accounting.
Step 8	**show aaa global** (Optional) Verify the global configuration of AAA.
Step 9	**show radius-server** (Optional) Verify the configuration of RADIUS server.
Step 10	**show aaa group** [*group-name*] (Optional) Verify the configuration of server group.
Step 11	**show aaa authentication** dot1x (Optional) Verify the authentication method list.
Step 12	**show aaa accounting** dot1x (Optional) Verify the accounting method list.
Step 13	**end** Return to privileged EXEC mode.
Step 14	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable AAA, add a RADIUS server to the server group named radius1, and apply this server group to the 802.1X authentication. The IP address of

the RADIUS server is 192.168.0.100; the shared key is 123456; the authentication port is 1812; the accounting port is 1813.

Switch#configure

Switch(config)#aaa enable

Switch(config)#radius-server host 192.168.0.100 **key** 123456 **auth-port** 1812 **acct-port** 1813

Switch(config)#aaa group radius radius1

Switch(aaa-group)#server 192.168.0.100

Switch(aaa-group)#exit

Switch(config)#aaa authentication dot1x default radius1

Switch(config)#aaa accounting dot1x default radius1

Switch(config)#show radius-server

Server Ip	Auth Port	Acct Port	Timeout	Retransmit	NAS Identifier	Shared key
192.168.0.100	1812	1813	5	2	000AEB132397	123456

Switch(config)#show aaa group radius1

192.168.0.100

Switch(config)#show aaa authentication dot1x

Methodlist	pri1	pri2	pri3	pri4
default	radius1	--	--	--

Switch(config)#show aaa accounting dot1x

Methodlist	pri1	pri2	pri3	pri4
default	radius1	--	--	--

Switch(config)#show aaa global

AAA global status: Enable

Switch(config)#end

Switch#copy running-config startup-config

10.2.2 Configuring 802.1X Globally

Follow these steps to configure 802.1X globally:

Step 1	**configure** Enter global configuration mode.
Step 2	**dot1x system-auth-control** Enable 802.1X authentication globally.
Step 3	**dot1x auth-method** { pap | eap } Configure the 802.1X authentication method. pap: Specify the authentication method as PAP. If this option is selected, the 802.1X authentication system uses EAP (Extensible Authentication Protocol) packets to exchange information between the switch and the client. The transmission of EAP packets is terminated at the switch and the EAP packets are converted to other protocol (such as RADIUS) packets, and transmitted to the authentication server. eap: Specify the authentication method as EAP. If this option is selected, the 802.1X authentication system uses EAP packets to exchange information between the switch and the client. The EAP packets with authentication data are encapsulated in the advanced protocol (such as RADIUS) packets, and transmitted to the authentication server.
Step 4	**dot1x guest-vlan** *vid* (Optional) Enable guest VLAN globally. *vid:* Specify the ID of the VLAN to be configured as the guest VLAN. It must be an existing VLAN with the ID ranging from 2 to 4094. Clients in the guest VLAN can only access resources from specific VLANs.
Step 5	**dot1x quiet-period** [time] (Optional) Enable the quiet feature for 802.1X authentication and configure the quiet period. time: Set a value between 1 and 999 seconds for the quiet period. It is 10 seconds by default. The quiet period starts after the authentication fails. During the quiet period, the switch does not process authentication requests from the same client.
Step 6	**dot1x vlan-assignment** (Optional) Enable or disable the 802.1X VLAN assignment feature. 802.1x VLAN assignment is a technology allowing the RADIUS server to send the VLAN assignment to the port when the port is authenticated. If the assigned VLAN does not exist on the switch, the switch will create the related VLAN automatically, add the authenticated port to the VLAN and change the PVID based on the assigned VLAN. If the assigned VLAN exists on the switch, the switch will directly add the authenticated port to the related VLAN and change the PVID instead of creating a new VLAN. If no VLAN is supplied by the RADIUS server or if 802.1x authentication is disabled, the port will be in its original VLAN after successful authentication.

Step 7	**dot1x timeout supplicant-timeout** *time* Configure the supplicant timeout period. *time:* Specify the maximum time for which the switch waits for response from the client. It ranges from 1 to 9 seconds and the default time is 3 seconds. If the switch does not receive any reply from the client within the specified time, it will resend the request.
Step 8	**dot1x max-reauth-req** *times* Specify the maximum number of attempts to send the authentication packet for the client. *times:* The maximum attempts for the client to send the authentication packet. It ranges from 1 to 9 and the default is 3.
Step 9	**show dot1x global** (Optional) Verify global configurations of 802.1X.
Step 10	**end** Return to privileged EXEC mode.
Step 11	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable 802.1X authentication, configure PAP as the authentication method and keep other parameters as default:

Switch#configure

Switch(config)#dot1x system-auth-control

Switch(config)#dot1x auth-method pap

Switch(config)#show dot1x global

802.1X State: Enabled

Authentication Method: PAP

Handshake State: Enabled

Guest VLAN State: Disabled

Guest VLAN ID: N/A

802.1X Accounting State: Disabled

802.1X VLAN Assignment State: Disabled

Quiet-period State: Disable

Quiet-period Timer: 10 sec.

Max Retry-times For RADIUS Packet: 3

Supplicant Timeout: 3 sec.

Switch(config)#end

Switch#copy running-config startup-config

10.2.3 Configuring 802.1X on Ports

Follow these steps to configure the port:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list***}** Enter interface configuration mode. *port:* Enter the ID of the port to be configured.
Step 3	**dot1x** Enable 802.1X authentication for the port.
Step 4	**dot1x mab** Enable the MAB (MAC-Based Authentication Bypass) feature for the port. With MAB feature enabled, the switch automatically sends the authentication server a RADIUS access request frame with the client's MAC address as the username and password. It is also necessary to configure the RADIUS server with the client's information for authentication. You can enable this feature on IEEE 802.1x ports connected to devices without 802.1X capability. For example, most printers, IP phones and fax machines do not have 802.1X capability.
Step 5	**dot1x port-method** { mac-based | port-based } Configure the control type for the port. By default, it is mac-based. mac-based**:** All clients connected to the port need to be authenticated. port-based**:** If a client connected to the port is authenticated, other clients can access the LAN without authentication.
Step 6	**dot1x guest-vlan** (Optional) Enable guest VLAN on the port. Note: Before enabling guest VLAN, the control type of the port should be configured as port-based.

Step 7	**dot1x port-control** { auto | authorized-force | unauthorized-force } Configure the control mode for the port. By default, it is auto. auto: If this option is selected, the port can access the network only when it is authenticated. authorized-force: If this option is selected, the port can access the network without authentication. unauthorized-force: If this option is selected, the port can never be authenticated.
Step 8	**show dot1x interface [fastEthernet** *port* **|gigabitEthernet** *port* **| ten-gigabitEthernet** *port***]** (Optional) Verify the configurations of 802.1X authentication on the port. *port:* Enter the ID of the port to be configured. If no specific port is entered, the switch will show configurations of all ports.
Step 9	**end** Return to privileged EXEC mode.
Step 10	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable 802.1X authentication on port 1/0/2, configure the control type as port-based, and configure the control mode as auto:

Switch#configure

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

Switch(config-if)#dot1x

Switch(config-if)#dot1x port-method port-based

Switch(config-if)#dot1x port-control auto

Switch(config-if)#show dot1x interface gigabitEthernet 1/0/2

Port	State	MAB State	GuestVLAN	PortControl	PortMethod	Authorized	LAG
----	---------	---------	---------	--------	--------	------------	---
Gi1/0/2	enabled	disabled	disabled	auto	port-based	unauthorized	N/A

Switch(config-if)#end

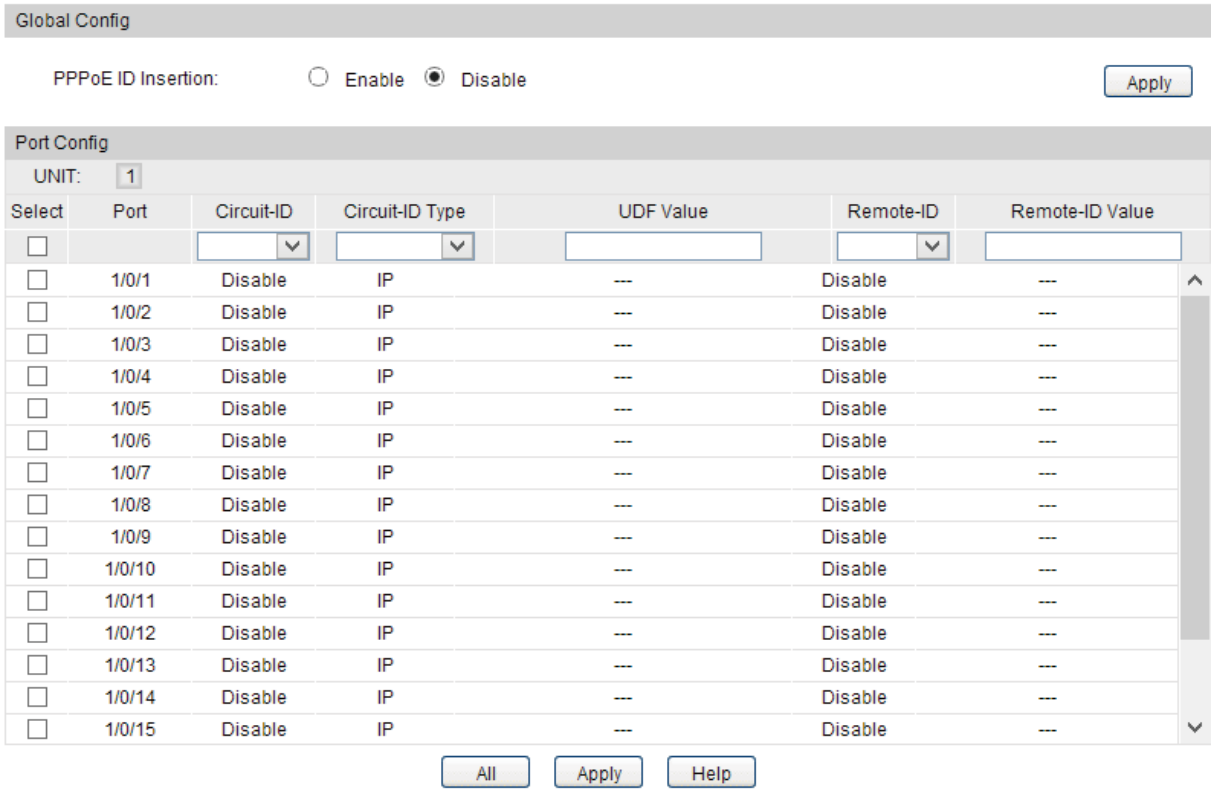
Switch#copy running-config startup-config

11 PPPoE ID-Insertion Configuration

11.1 Using the GUI

Choose the menu **Network Security > PPPoE > PPPoE ID Insertion** to load the following page.

Figure 11-1 PPPoE ID Insertion



Follow these steps to configure PPPoE ID-Insertion:

1) In the **Global Config** section, enable PPPoE ID Insertion and click **Apply**.
2) In the **Port Config** section, select one or more ports, and configure the relevant parameters. Then click **Apply**.

Circuit-ID	Enable or disable the Circuit-ID Insertion feature. With this option enabled, the switch will insert a Circuit ID to the received PPPoE Discovery packet on this port.

Circuit-ID Type	Select the type of the Circuit ID. The following options are provided: **IP**: The circuit ID includes the following three parts: the source MAC address of the received packet, the IP address of the switch and the port number. This is the default value. **MAC**: The circuit ID includes the following three parts: the source MAC address of the packet, the MAC address of the switch and the port number. **UDF**: The circuit ID includes the following three parts: the source MAC address of the packet, the user-specified string and the port number. **UDF ONLY**: Only the user specified string will be used to encode the Circuit-ID option.
UDF Value	If UDF or UDF ONLY is selected, specify a string with at most 40 characters to encode the Circuit-id option.
Remote-ID	Enable or disable the Remote-ID Insertion feature. With this option enabled, the switch will insert a Remote ID to the received PPPoE Discovery packet on this port.
Remote-ID Value	Specify a string with at most 40 characters to encode the Remote-id option.

11.2 Using the CLI

Follow these steps to configure PPPoE ID-Insertion:

Step 1	**configure** Enter global configuration mode.
Step 2	**pppoe id-insertion** Globally enable the PPPoE ID-Insertion feature.
Step 3	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **}** Enter interface configuration mode.
Step 4	**pppoe circuit-id** Enable Circuit-ID Insertion feature, and the switch will insert a Circuit ID to the received PPPoE Discovery packet on this port.

Step 5	**pppoe circuit-id type {** mac | ip | udf [*Value*] | udf-only [*Value*] **}** Specify the type of the Circuit ID. The following options are provided: mac: The source MAC address of the packet, the MAC address of the switch and the port number will be used to encode the Circuit-ID option. ip: The circuit ID includes the following three parts: the source MAC address of the received packet, the IP address of the switch and the port number. This is the default value. udf [*Value*]: Specify a string with at most 40 characters. The circuit ID includes the following three parts: the source MAC address of the packet, the user-specified string and the port number. udf-only [*Value*]: Specify a string with at most of 40 characters. Only the specified string will be used to encode the Circuit-ID option.
Step 6	**pppoe remote-id** [*Value*] Enable Remote-ID Insertion feature and specify the Remote ID. *Value*: Specify a string with at most 40 characters. The source MAC address of the packet and the specified string will be used to encode the Remote-ID option.
Step 7	**show pppoe id-insertion global** Verify the global configuration of PPPoE ID-Insertion.
Step 8	**show pppoe id-insertion interface { fastEthernet** *port* **| gigabitEthernet** *port* **}** Verify the configuration of PPPoE ID-Insertion for the specific port.
Step 9	**end** Return to privileged EXEC mode.
Step 10	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable PPPoE ID-Insertion globally and on port 1/0/1, and configure the Circuit-ID as 123 without other information and Remote-ID as host1.

Switch#configure

Switch(config)#pppoe id-insertion

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

Switch(config-if)#pppoe circuit-id

Switch(config-if)#pppoe circuit-id type udf-only 123

Switch(config-if)#pppoe remote-id host1

Switch(config-if)#show pppoe id-insertion global

PPPoE ID Insertion State: Enabled

Switch(config-if)#show pppoe id-insertion interface gigabitEthernet 1/0/1

Port	Circuit-ID	C-ID Type	C-ID Value(UDF)	Remote-ID	R-ID Value
Gi1/0/1	Enabled	UDF-ONLY	123	Enabled	host1

Switch(config-if)#end

Switch#copy running-config startup-config

12 AAA Configuration

In the AAA feature, the authentication can be processed locally on the switch or centrally on the RADIUS/TACACS+ server(s). To ensure the stability of the authentication system, you can configure multiple servers and authentication methods at the same time. This chapter introduces how to configure this kind of comprehensive authentication in AAA.

To complete the configuration, follow these steps:

1) Globally enable AAA.
2) Add the servers.
3) Configure the server groups.
4) Configure the method list.
5) Configure the AAA application list.
6) Configure the login account and the Enable password.

Configuration Guidelines

The basic concepts and working mechanism of AAA are as follows:

- Server Group

Multiple servers running the same protocol can be added to a server group, and the servers in the group will authenticate the users in the order they are added. The server that is first added to the group has the highest priority, and is responsible for authentication under normal circumstances. If the first one breaks down or doesn't respond to the authentication request for some reason, the second sever will start working for authentication, and so on.

- Method List

A server group is regarded as a method, and the local authentication is another method. Several methods can be configured to form a method list. The switch uses the first method in the method list to authenticate the user, and if that method fails to respond, the

switch selects the next method. This process continues until the user has a successful communication with a method or until all defined methods are exhausted. If the authentication succeeds or the secure server or the local switch denies the user's access, the authentication process stops and no other methods are attempted.

Two types of method list are provided: Login method list for users of all types to access the switch, and Enable method list for guests to get administrative privileges.

- AAA Application List

The switch supports the following access applications: Console, Telnet, SSH and HTTP. You can select the configured authentication method lists for each application.

12.1 Using the GUI

12.1.1 Globally Enabling AAA

Choose the menu **Network Security > AAA > Global Conifg** to load the following page.

Figure 12-1 Global Configuration



Follow these steps to globally enable AAA:

1) In the **Global Config** section, enable AAA.
2) Click **Apply**.

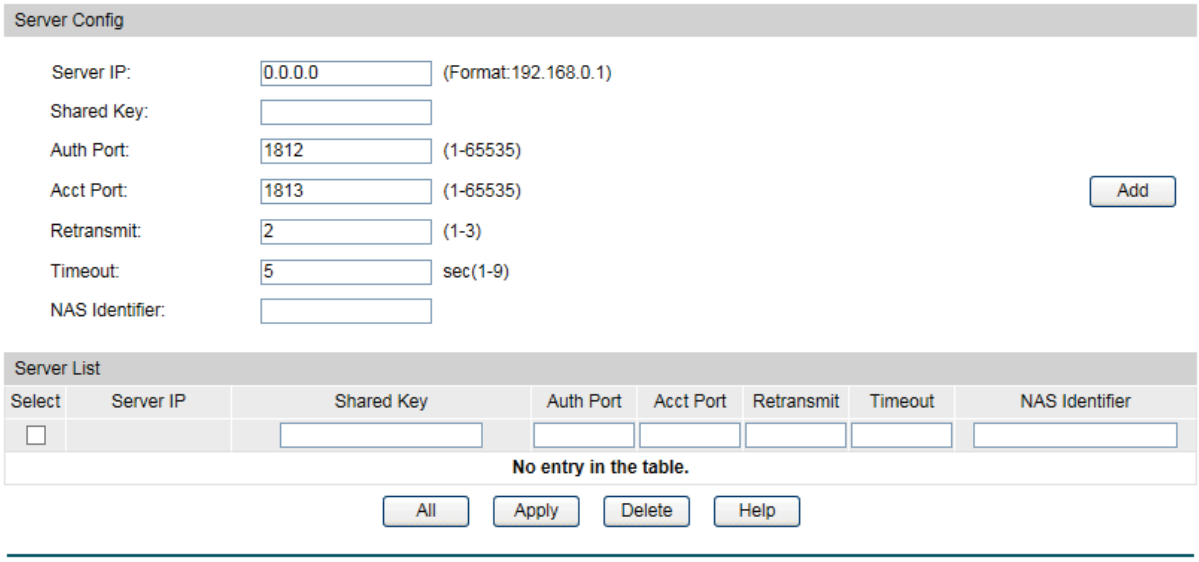
12.1.2 Adding Servers

You can add one or more RADIUS/TACACS+ servers on the switch for authentication. If multiple servers are added, the server that is first added to the group has the highest priority and authenticates the users trying to access the switch. The others act as backup servers in case the first one breaks down.

Adding RADIUS Server

Choose the menu **Network Security > AAA > RADIUS Conifg** to load the following page.

Figure 12-2 RADIUS Server Configuration



Follow these steps to add a RADIUS server:

1) In the **Server Config** section, configure the following parameters.

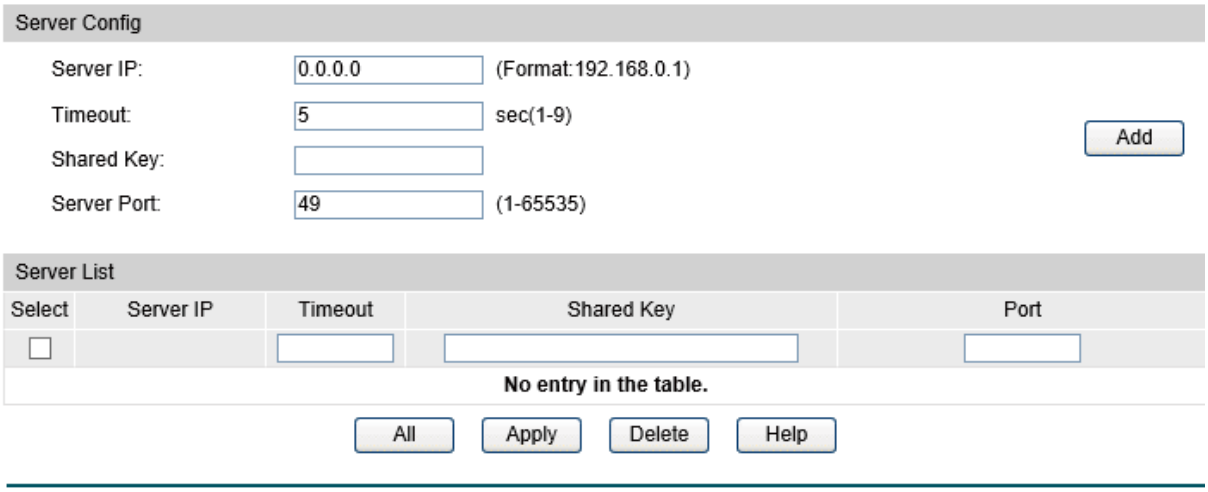
Server IP	Enter the IP address of the server running the RADIUS secure protocol.
Shared Key	Enter the shared key between the RADIUS server and the switch. The RADIUS server and the switch use the key string to encrypt passwords and exchange responses.
Auth Port	Specify the UDP destination port on the RADIUS server for authentication requests. The default setting is 1812.
Acct Port	Specify the UDP destination port on the RADIUS server for accounting requests. The default setting is 1813. Usually, it is used in the 802.1X feature.
Retransmit	Specify the number of times a request is resent to the server if the server does not respond. The default setting is 2.
Timeout	Specify the time interval that the switch waits for the server to reply before resending. The default setting is 5 seconds.
NAS Identifier	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.

2) Click **Add** to add the RADIUS server on the switch.

Adding TACACS+ Server

Choose the menu **Network Security > AAA > TACACS+ Conifg** to load the following page.

Figure 12-3 TACACS+ Server Configuration



Follow these steps to add a TACACS+ server:

1) In the **Server Config** section, configure the following parameters.

Server IP	Enter the IP address of the server running the TACACS+ secure protocol.
Timeout	Specify the time interval that the switch waits for the server to reply before resending. The default setting is 5 seconds.
Shared Key	Enter the shared key between the TACACS+ server and the switch. The TACACS+ server and the switch use the key string to encrypt passwords and exchange responses.
Server Port	Specify the TCP port used on the TACACS+ server for AAA. The default setting is 49.

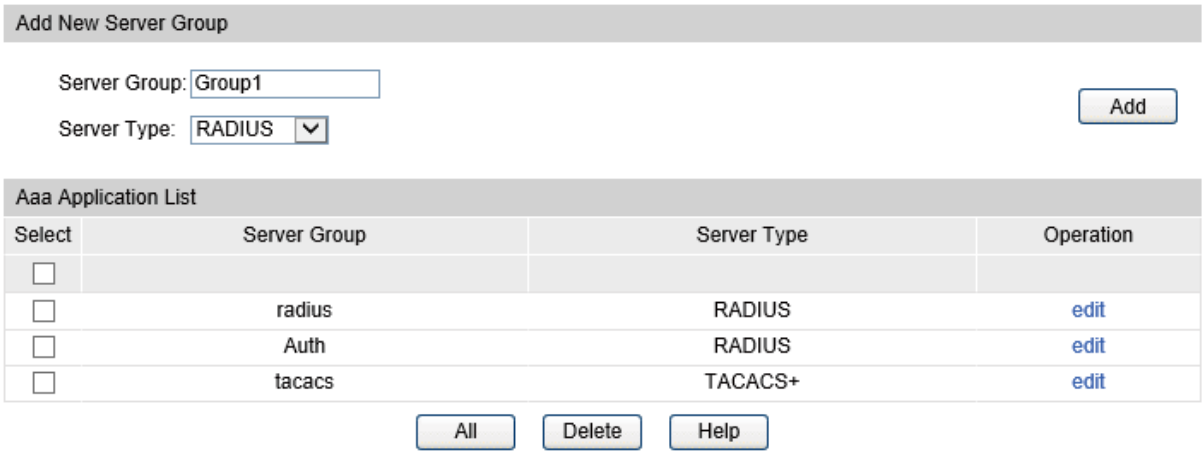
2) Click **Add** to add the TACACS+ server on the switch.

12.1.3 Configuring Server Groups

The switch has two built-in server groups, one for RADIUS servers and the other for TACACS+ servers. The servers running the same protocol are automatically added to the default server group. You can add new server groups as needed.

Choose the menu **Network Security > AAA > Server Group** to load the following page.

Figure 12-4 Add New Server Group



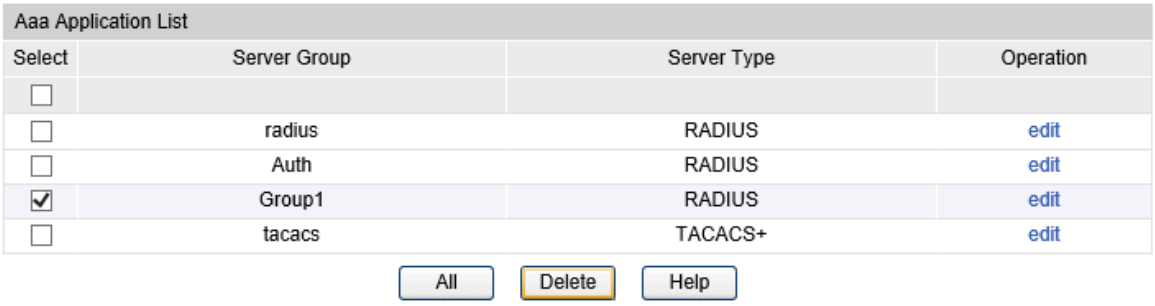
The two default server groups in the list cannot be edited or deleted. You can follow these steps to configure a new server group:

1) In the **Add New Server Group** section, configure the group name and the server type, and click **Add** to add the new server group.

Server Group	Specify a name for the server group.
Server Type	Select the server type for the group. The following options are provided: RADIUS and TACACS+.

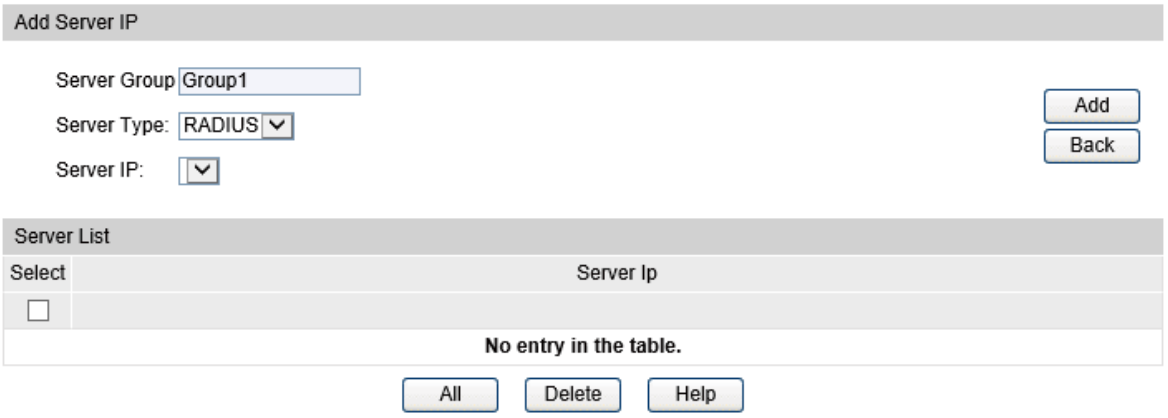
2) Select the newly added group, and click **edit** in the **Operation** column.

Figure 12-5 Edit the Group



3) Select the server to be added to the group from the **Server IP** drop-down list . Then click **Add** to add this server to the server group.

Figure 12-6 Add Server to Group

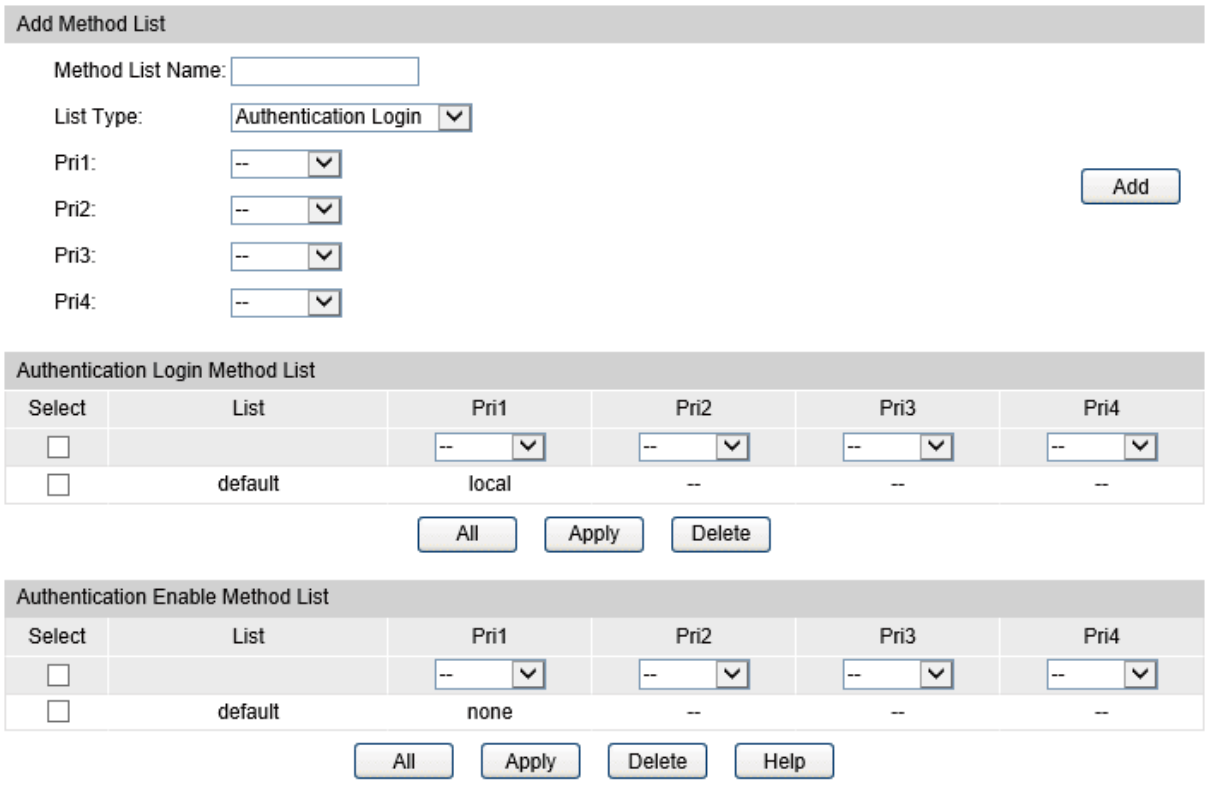


12.1.4 Configuring the Method List

A method list describes the authentication methods and their sequence to authenticate the users. The switch supports Login Method List for users of all types to gain access to the switch, and Enable Method List for guests to get administrative privileges.

Choose the menu **Network Security > AAA > Method List** to load the following page.

Figure 12-7 Add New Method



There are two default methods respectively for the Login authentication and the Enable authentication.

You can edit the default methods or follow these steps to add a new method:

1) In the **Add Method List** section, configure the parameters for the method to be added.

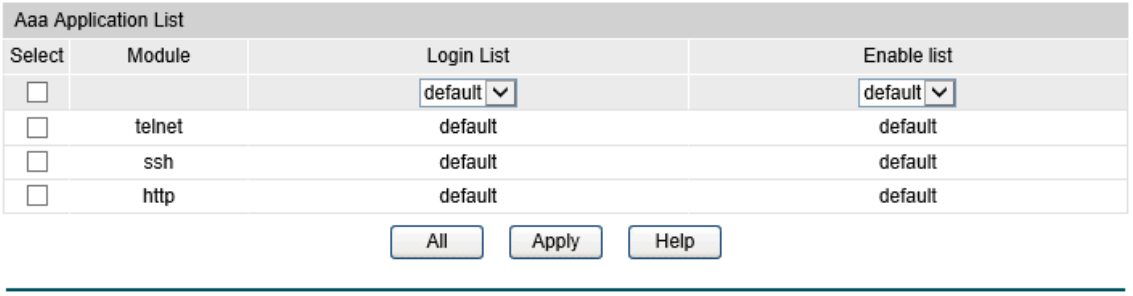
Method List Name	Specify a name for the method.
List Type	Select the authentication type. The following options are provided: Authentication Login and Authentication Enable.
Pri1- Pri4	Specify the authentication methods in order. The method with priority 1 authenticates a user first, the method with priority 2 is tried if the previous method does not respond, and so on. **local**: Use the local database in the switch for authentication. **none**: No authentication is used. **radius**: Use the remote RADIUS server/server groups for authentication. **tacacs**: Use the remote TACACS+ server/server groups for authentication. **Other user-defined server groups**: Use the user-defined server groups for authentication.

2) Click **Add** to add the new method.

12.1.5 Configuring the AAA Application List

Choose the menu **Network Security > AAA > Global Config** to load the following page.

Figure 12-8 Configure Application List



Follow these steps to configure the AAA application list.

1) In the **AAA Application List** section, select an access application and configure the Login list and Enable list.

Module	Displays the configurable applications on the switch: console, telnet, ssh and http.
Login List	Select a previously configured Login method list. This method list will authenticate the users trying to log in to the switch.
Enable List	Select a previously configured Enable method list. This method list will authenticate the users trying to get administrative privileges.

2) Click **Apply**.

12.1.6 Configuring Login Account and Enable Password

The login account and Enable password can be configured locally on the switch or centrally on the RADIUS/TACACS+ server(s).

- On the Switch

The local username and password for login can be configured in the User Management feature. For details, refer to *Managing System*.

To configure the local Enable password for getting administrative privileges, choose the menu **Network Security > AAA > Global Config** to load the following page.

Figure 12-9 Configure Enable Password



Specify the Enable password in the **Enable Admin** section, and click **Apply**.

Tips: The logged-in guests can enter the Enable password on this page to get administrative privileges.

- On the Server

The accounts created by the RADIUS/TACACS+ server can only view the configurations and some network information without the Enable password.

Some configuration principles on the server are as follows:

- For Login authentication configuration, more than one login account can be created on the server. Besides, both the user name and password can be customized.

- For Enable password configuration:

  On RADIUS server, the user name should be set as **$enable$**, and the Enable password is customizable. All the users trying to get administrative privileges share this Enable password.

  On TACACS+ server, configure the value of "enable 15" as the Enable password in the configuration file. All the users trying to get administrative privileges share this Enable password.

12.2 Using the CLI

12.2.1 Globally Enabling AAA

Follow these steps to globally enable AAA:

Step 1	**configure** Enter global configuration mode.
Step 2	**aaa enable** Globally enable the AAA feature.
Step 3	**show aaa global** Verify the global configuration of AAA.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to globally enable AAA:

Switch#configure

Switch(config)#aaa enable

Switch(config)#show aaa global

AAA global status: Enable

...

Switch(config)#end

Switch#copy running-config startup-config

12.2.2 Adding Servers

You can add one or more RADIUS/TACACS+ servers on the switch for authentication. If multiple servers are added, the server with the highest priority authenticates the users trying to access the switch, and the others act as backup servers in case the first one breaks down.

- Adding RADIUS Server

Follow these steps to add RADIUS server on the switch:

Step 1	**configure** Enter global configuration mode.
Step 2	**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* **}]** Add the RADIUS server and configure the related parameters as needed. **host** *ip-address*: Enter the IP address of the server running the RADIUS protocol. **auth-port** *port-id*: Specify the UDP destination port on the RADIUS server for authentication requests. The default setting is 1812. **acct-port** *port-id:* Specify the UDP destination port on the RADIUS server for accounting requests. The default setting is 1813. Usually, it is used in the 802.1X feature. **timeout** *time*: Specify the time interval that the switch waits for the server to reply before resending. The valid values are from 1 to 9 seconds and the default setting is 5 seconds. **retransmit** *number*: Specify the number of times a request is resent to the server if the server does not respond. The valid values are from 1 to 3 and the default setting is 2. **nas-id** *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. **key {** [0] *string* **|** 7 *encrypted-string* **}**: Specify the shared key. 0 and 7 represent 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 server, which contains 31 characters at most. *encrypted-string* is a symmetric encrypted key with a fixed length, which you can copy from the configuration file of another switch. The key or encrypted-key you configure here will be displayed in the encrypted form.
Step 3	**show radius-server** Verify the configuration of RADIUS server.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to add a RADIUS server on the switch. Set the IP address of the server as 192.168.0.10, the authentication port as 1812, the shared key as 123456, the timeout as 8 seconds and the retransmit number as 3.

Switch#configure

Switch(config)#radius-server host 192.168.0.10 **auth-port** 1812 **timeout** 8 **retransmit** 3 **key** 123456

Switch(config)#show radius-server

Server Ip	Auth Port	Acct Port	Timeout	Retransmit	NAS Identifier	Shared key

192.168.0.10 1812 1813 5 2 000AEB132397 123456

Switch(config)#end

Switch#copy running-config startup-config

Adding TACACS+ Server

Follow these steps to add TACACS+ server on the switch:

Step 1	**configure** Enter global configuration mode.
Step 2	**tacacs-server host** *ip-address* **[port** *port-id* **] [timeout** *time* **] [key {** [0] *string* **|** 7 *encrypted-string* **}]** Add the RADIUS server and configure the related parameters as needed. **host** *ip-address*: Enter the IP address of the server running the TACACS+ protocol. **port** *port-id*: Specify the TCP destination port on the TACACS+ server for authentication requests. The default setting is 49. **timeout** *time*: Specify the time interval that the switch waits for the server to reply before resending. The valid values are from 1 to 9 seconds and the default setting is 5 seconds. **key {** [0] *string* **|** 7 *encrypted-string* **}**: Specify the shared key. 0 and 7 represent 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 server, which contains 31 characters at most. *encrypted-string* is a symmetric encrypted key with a fixed length, which you can copy from the configuration file of another switch. The key or encrypted-key you configured here will be displayed in the encrypted form.
Step 3	**show tacacs-server** Verify the configuration of TACACS+ server.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to add a TACACS+server on the switch. Set the IP address of the server as 192.168.0.20, the authentication port as 49, the shared key as 123456, and the timeout as 8 seconds.

Switch#configure

Switch(config)#tacacs-server host 192.168.0.20 **auth-port** 49 **timeout** 8 **key** 123456

Switch(config)#show tacacs-server

Server Ip	Port	Timeout	Shared key
192.168.0.20	49	8	123456

Switch(config)#end

Switch#copy running-config startup-config

12.2.3 Configuring Server Groups

The switch has two built-in server groups, one for RADIUS and the other for TACACS+. The servers running the same protocol are automatically added to the default server group. You can add new server groups as needed.

The two default server groups cannot be deleted or edited. Follow these steps to add a server group:

Step 1	**configure** Enter global configuration mode.
Step 2	**aaa group {** radius | tacacs **}** *group-name* Create a server group. radius | tacacs: Specify the group type. *group-name*: Specify a name for the group.
Step 3	**server** *ip-address* Add the existing servers to the server group. *ip-address*: Specify IP address of the server to be added to the group.
Step 4	**show aaa group** [*group-name*] Verify the configuration of server group.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create a RADIUS server group named RADIUS1 and add the existing two RADIUS servers whose IP address is 192.168.0.10 and 192.168.0.20 to the group.

Switch#configure

Switch(config)#aaa group radius RADIUS1

Switch(aaa-group)#server 192.168.0.10

Switch(aaa-group)#server 192.168.0.20

Switch(aaa-group)#show aaa group RADIUS1

192.168.0.10

192.168.0.20

Switch(aaa-group)#end

Switch#copy running-config startup-config

12.2.4 Configuring the Method List

A method list describes the authentication methods and their sequence to authenticate the users. The switch supports Login Method List for users of all types to gain access to the switch, and Enable Method List for guests to get administrative privileges.

Follow these steps to configure the method list:

Step 1	**configure** Enter global configuration mode.
Step 2	**aaa authentication login {** *method-list* **} {** *method1* **} [** *method2* **] [** *method3* **] [** *method4* **]** Configure a login method list. *method-list*: Specify a name for the method list. *method1/method2/method3/method4*: Specify the authentication methods in order. The first method authenticates a user first, the second method is tried if the previous method does not respond, and so on. The default methods include radius, tacacs, local and none. None means no authentication is used for login.
Step 3	**aaa authentication enable {** *method-list* **} {** *method1* **} [** *method2* **] [** *method3* **] [** *method4* **]** Configure an Enable password method list. *method-list*: Specify a name for the method list. *method1/method2/method3/method4*: Specify the authentication methods in order. The default methods include radius, tacacs, local and none. None means no authentication is used for getting administrative privileges.
Step 4	**show aaa authentication** [login | enable] Verify the configuration method list.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create a Login method list named Login1, and configure the method 1 as the default radius server group and the method 2 as local.

Switch#configure

Switch(config)##aaa authentication login Login1 radius local

Switch(config)#show aaa authentication login

Methodlist	pri1	pri2	pri3	pri4
default	local	--	--	--
Login1	radius	local	--	--

Switch(config)#end

Switch#copy running-config startup-config

The following example shows how to create an Enable method list named Enable1, and configure the method 1 as the default radius server group and the method 2 as local.

Switch#configure

Switch(config)##aaa authentication enable Enable1 radius local

Switch(config)#show aaa authentication enable

Methodlist	pri1	pri2	pri3	pri4
default	local	--	--	--
Enable1	radius	local	--	--

Switch(config)#end

Switch#copy running-config startup-config

12.2.5 Configuring the AAA Application List

You can configure authentication method lists on the following access applications: Console, Telnet, SSH and HTTP.

- Console

Follow these steps to apply the Login and Enable method lists for the application Console:

Step 1	**configure** Enter global configuration mode.

Step 2	**line console** *linenum* Enter line configuration mode. *linenum*: Enter 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.
Step 3	**login authentication {** *method-list* **}** Apply the Login method list for the application Console. *method-list*: Specify the name of the Login method list.
Step 4	**enable authentication {** *method-list* **}** Apply the Enable method list for the application Console. *method-list*: Specify the name of the Enable method list.
Step 5	**show aaa global** Verify the configuration of application list.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to apply the existing Login method list named Login1 and Enable method list named Enable1 for the application Console.

Switch#configure

Switch(config)#line console 0

Switch(config-line)#login authentication Login1

Switch(config-line)#enable authentication Enable1

Switch(config-line)#show aaa global

...

Module	Login List	Enable List
Console	Login1	Enable1
Telnet	default	default
Ssh	default	default
Http	default	default

Switch(config-line)#end

Switch#copy running-config startup-config

Telnet

Follow these steps to apply the Login and Enable method lists for the application Telnet:

Step 1	**configure** Enter global configuration mode.
Step 2	**line telnet** Enter line configuration mode.
Step 3	**login authentication {** *method-list* **}** Apply the Login method list for the application Telnet. *method-list*: Specify the name of the Login method list.
Step 4	**enable authentication {** *method-list* **}** Apply the Enable method list for the application Telnet. *method-list*: Specify the name of the Enable method list.
Step 5	**show aaa global** Verify the configuration of application list.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to apply the existing Login method list named Login1 and Enable method list named Enable1 for the application Telnet.

Switch#configure

Switch(config)#line telnet

Switch(config-line)#login authentication Login1

Switch(config-line)#enable authentication Enable1

Switch(config-line)#show aaa global

...

Module	Login List	Enable List
Console	default	default
Telnet	Login1	Enable1
Ssh	default	default

Http default default

Switch(config-line)#end

Switch#copy running-config startup-config

- SSH

Follow these steps to apply the Login and Enable method lists for the application SSH:

Step 1	**configure** Enter global configuration mode.
Step 2	**line ssh** Enter line configuration mode.
Step 3	**login authentication {** *method-list* **}** Apply the Login method list for the application SSH. *method-list*: Specify the name of the Login method list.
Step 4	**enable authentication {** *method-list* **}** Apply the Enable method list for the application SSH. *method-list*: Specify the name of the Enable method list.
Step 5	**show aaa global** Verify the configuration of application list.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to apply the existing Login method list named Login1 and Enable method list named Enable1 for the application SSH.

Switch#configure

Switch(config)#line ssh

Switch(config-line)#login authentication Login1

Switch(config-line)#enable authentication Enable1

Switch(config-line)#show aaa global

...

Module Login List Enable List

Console default default

Telnet default default

Ssh Login1 Enable1

Http default default

Switch(config-line)#end

Switch#copy running-config startup-config

- HTTP

Follow these steps to apply the Login and Enable method lists for the application HTTP:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip http login authentication {** *method-list* **}** Apply the Login method list for the application HTTP. *method-list*: Specify the name of the Login method list.
Step 3	**ip http enable authentication {** *method-list* **}** Apply the Enable method list for the application HTTP. *method-list*: Specify the name of the Enable method list.
Step 4	**show aaa global** Verify the configuration of application list.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to apply the existing Login method list named Login1 and Enable method list named Enable1 for the application HTTP:

Switch#configure

Switch(config)#ip http login authentication Login1

Switch(config)#ip http enable authentication Enable1

Switch(config)#show aaa global

...

Module Login List Enable List

Console	default	default
Telnet	default	default
Ssh	default	default
Http	Login1	Enable1

Switch(config)#end

Switch#copy running-config startup-config

12.2.6 Configuring Login Account and Enable Password

The login account and Enable password can be configured locally on the switch or centrally on the RADIUS/TACACS+ server(s).

- On the Switch

The local username and password for login can be configured in the User Management feature. For details, refer to *Managing System*.

To configure the local Enable password for getting administrative privileges, follow these steps:

Step 1	**configure** Enter global configuration mode.
Step 2	**enable admin password {** [0] *password* **|** 7 *encrypted-password* **}** Set the Enable password. This command uses symmetric encryption. 0 and 7 represent 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. *password* is a string from 1 to 31 alphanumeric characters or symbols. *encrypted-password* is a symmetric encrypted key with a fixed length, which you can copy from the configuration file of another switch. The key or encrypted-key you configured here will be displayed in the encrypted form. **enable admin secret {** [0] *password* **|** 5 *encrypted-password* **}** Set the Enable password. This command uses MD5 encryption. 0 and 5 are the encryption type. 0 indicates that an unencrypted key will follow. 5 indicates that an MD5 encrypted password with fixed length will follow. By default, the encryption type is 0. *password* is a string from 1 to 31 alphanumeric characters or symbols. *encrypted-password* is an MD5 encrypted password with fixed length, which you can copy from another switch's configuration file.
Step 3	**end** Return to privileged EXEC mode.

Step 4	**copy running-config startup-config** Save the settings in the configuration file.

On the Server

The accounts created by the RADIUS/TACACS+ server can only view the configurations and some network information without the Enable password.

Some configuration principles on the server are as follows:

- For Login authentication configuration, more than one login account can be created on the server. Besides, both the user name and password can be customized.

- For Enable password configuration:

  On RADIUS server, the user name should be set as **$enable$**, and the Enable password is customizable. All the users trying to get administrative privileges share this Enable password.

  On TACACS+ server, configure the value of "enable 15" as the Enable password in the configuration file. All the users trying to get administrative privileges share this Enable password.

Tips: The logged-in guests can get administrative privileges by using the command **enable-admin** and providing the Enable password.

13 DHCP Server Filter Configuration

To complete DHCP Server Filter Configuration, follow these steps:

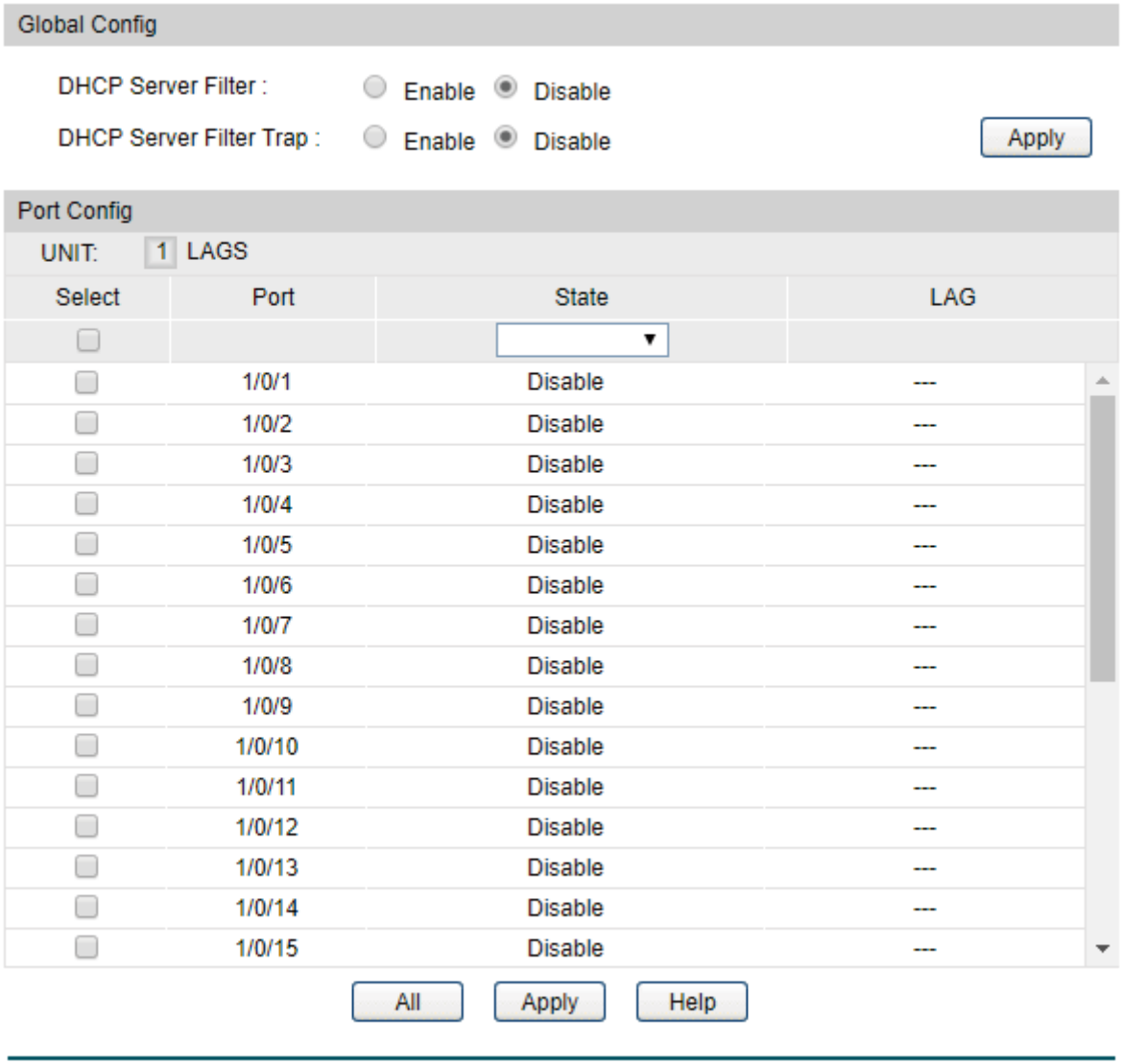
1) Enable DHCP Server Filter. Enable DHCP Server Filter Trap if needed.
2) Configure the DHCP Server Permit Entry.

13.1 Using the GUI

13.1.1 Enabling DHCP Server Filter

Choose the menu **Network Security > DHCP Server Filter > DHCP Server Filter Config** to load the following page.

Figure 13-1 DHCP Server Filter Config



Follow these steps to enable DHCP Server Filter:

1) In the **Global Config** section, enable DHCP Server Filter. Enable DHCP Server Filter Trap if needed. Click **Apply**.

DHCP Server Filter	Enable or disable DHCP Server Filter globally. By default, it is disabled.
DHCP Server Filter Trap	Enable or disable DHCP Server Filter trap. The switch will send an SNMP trap message when receiving an illegal DHCP packet.

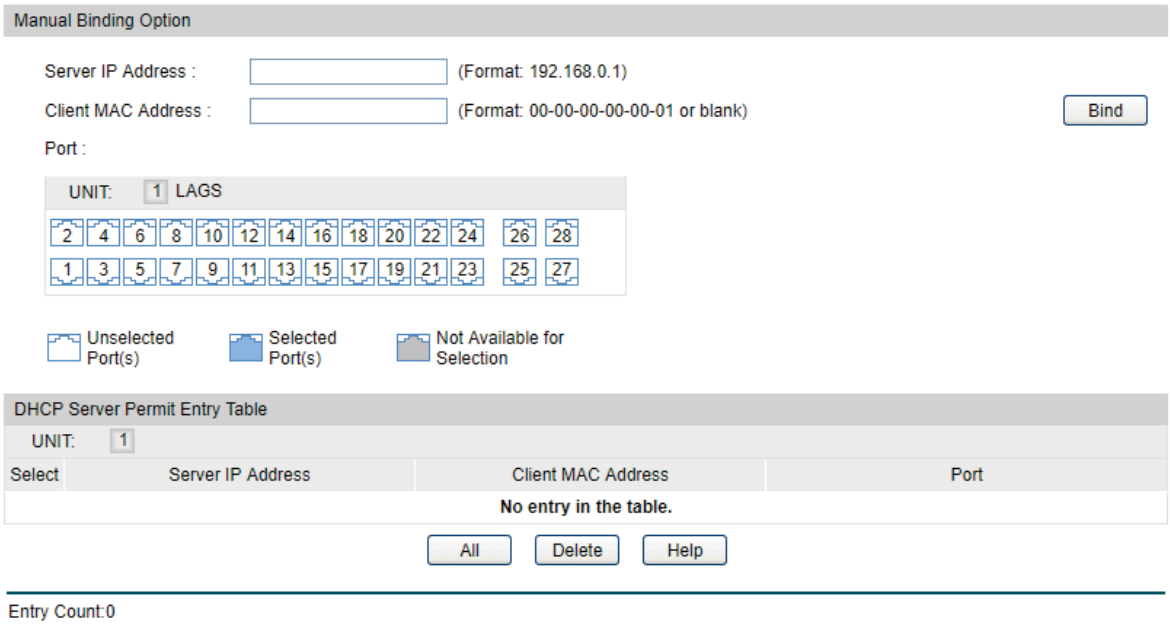
2) In the **Port Config** section, enable DHCP Server Filter for the desired ports. Click **Apply**.

UNIT:1/LAGS	Click **1** to configure physical ports. Click **LAGS** to configure LAGs.
State	With this option enabled, the port will enable DHCP Server Filter function. By default, it's disabled.

13.1.2 Configuring the DHCP Server Permit Entry

Choose the menu **Network Security > DHCP Server Filter > DHCP Server Permit Entry** to load the following page.

Figure 13-2 DHCP Server Permit Entry



Follow these steps to configure the DHCP Server Permit Entry:

1) In the **Manual Binding Option** section, bind **Server IP Address**, **Client MAC Address**, and **Port** manually.

Server IP Address	Enter the IP Address of the legal DHCP Server. Only the DHCP Server packets from the legal DHCP Server can pass the switch.

Client MAC Address	Enter the MAC Address of the legal DHCP client. Leaving it blank means all. Only the DHCP Server packets sent to the legal DHCP client can pass the switch.
Port	Select the port connected to the DHCP Server.

2) Click **Bind.**

13.2 Using the CLI

13.2.1 Enabling DHCP Server Filter globally

Follow these steps to enable DHCP Relay globally:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip dhcp filter** Enable DHCP server filter globally.
Step 3	**snmp-server traps security dhcp-filter** (Optional)Enable DHCP Server Filter Trap.
Step 3	**show ip dhcp filter** Verify the global configuration of DHCP filter.
Step 4	**end** Return to Privileged EXEC Mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable DHCP Relay:

Switch#configure

Switch(config)#ip dhcp filter

Switch(config)#show ip dhcp filter

Global Status: Enable

...

Switch(config)#end

Switch#copy running-config startup-config

13.2.2 Enabling DHCP Server Filter for ports

Follow these steps to enable DHCP Server Filter for ports:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-id-list* **}** Enter interface configuration mode.
Step 3	**ip dhcp filter** Enable DHCP server filter for ports.
Step 4	**show ip dhcp filter interface [gigabitEthernet** *port* **| port-channel** *port-channel-id* **]** Verify the configuration of DHCP server filter for ports.
Step 5	**end** Return to Privileged EXEC Mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable DHCP Server FIlter for port 1/0/2.

Switch#configure

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

Switch(config-if)#ip dhcp filter

Switch(config-if)#show ip dhcp filter interface gigabitEthernet 1/0/2

Interface state LAG

--------- ------- ---

Gi1/0/2 Enable N/A

...

Switch(config)#end

Switch#copy running-config startup-config

13.2.3 Configuring the DHCP Server Permit Entry

Follow these steps to configure DHCP Server Permit Entry:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip dhcp filter server permit-entry server-ip** *ipAddr* **client-mac** *macAddr* **interface { gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **}** Bind DHCP Server IP, client MAC address, and port manually:
Step 3	**show ip dhcp filter server permit-entry** Verify the DHCP Server Permit Entry configuration.
Step 4	**end** Return to Privileged EXEC Mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the DHCP Server Permit Entry by binding DHCP server IP 192.168.0.30, MAC Address aa:aa:aa:aa:aa:aa, and port 1/0/2 manually.

Switch#configure

Switch(config)#ip dhcp filter server permit-entry server-ip 192.168.0.30 **client-mac** aa:aa:aa:aa:aa:aa **interface gigabitEthernet** 1/0/2

Switch(config)#show ip dhcp filter server permit-entry

Server IP	Client MAC	Interface
192.168.0.30	aa:aa:aa:aa:aa:aa	Gi1/0/2

Switch(config)#end

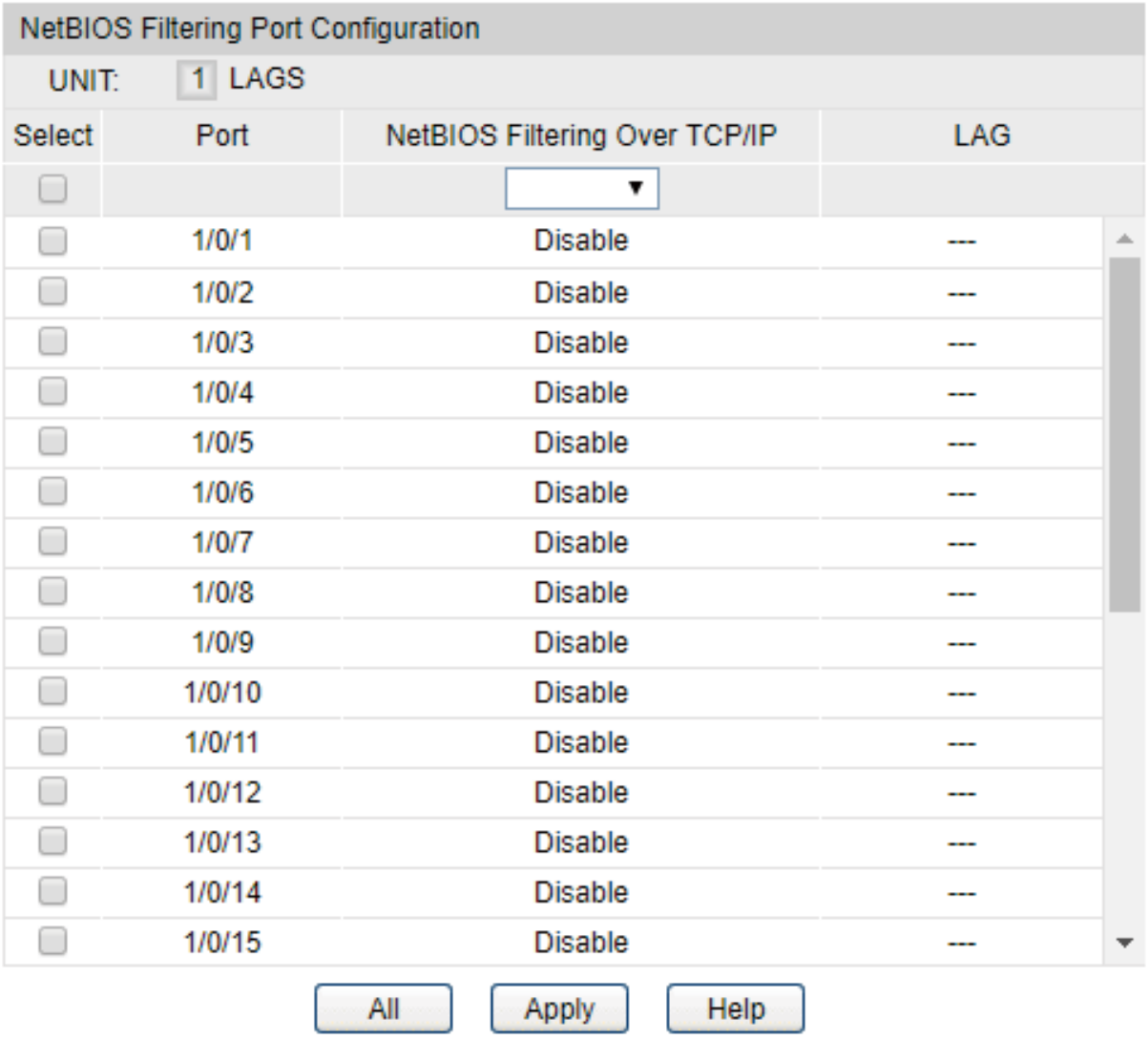
Switch#copy running-config startup-config

14 NetBIOS Filtering Configuration

14.1 Using the GUI

Choose the menu **Network Security > NetBIOS Filtering> NetBIOS Filtering** to load the following page.

Figure 14-1 NetBIOS Filtering Port Configuration



Follow these steps to configure NetBIOS Filtering:

1) Select the ports and enable NetBIOS Filtering Over TCP/IP for ports.

UNIT:1/LAGS	Click **1** to configure physical ports. Click **LAGS** to configure LAGs.

NetBIOS Filtering over TCP/IP	With this option enabled, the port will enable NetBIOS Filtering Over TCP/IP function. The switch will block all the network conmmunication using NetBIOS over TCP/IP on the port. By default, it's disabled.

2) Click **Apply.**

14.2 Using the CLI

Follow these steps to configure NetBIOS Filtering:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface { gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-id-list* **}** Enter interface configuration mode.
Step 3	**netbios filter** Enable NetBIOS Filtering for ports.
Step 4	**show netbios filter [interface gigabitEthernet** *port* **| interface port-channel** *port-channel-id***]** Verify the configuration of NetBIOS Filtering for ports.
Step 5	**end** Return to Privileged EXEC Mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable NetBIOS Filtering on port 1/0/2:

Switch#configure

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

Switch(config-if)#netbios filter

Switch(config-if)#show netbios filter interface gigabitEthernet 1/0/2

Interface NetBIOS Filtering Over TCP/IP LAG

--------- ---------- ---

Gi1/0/2 Enable N/A

Switch(config)#end

Switch#copy running-config startup-config

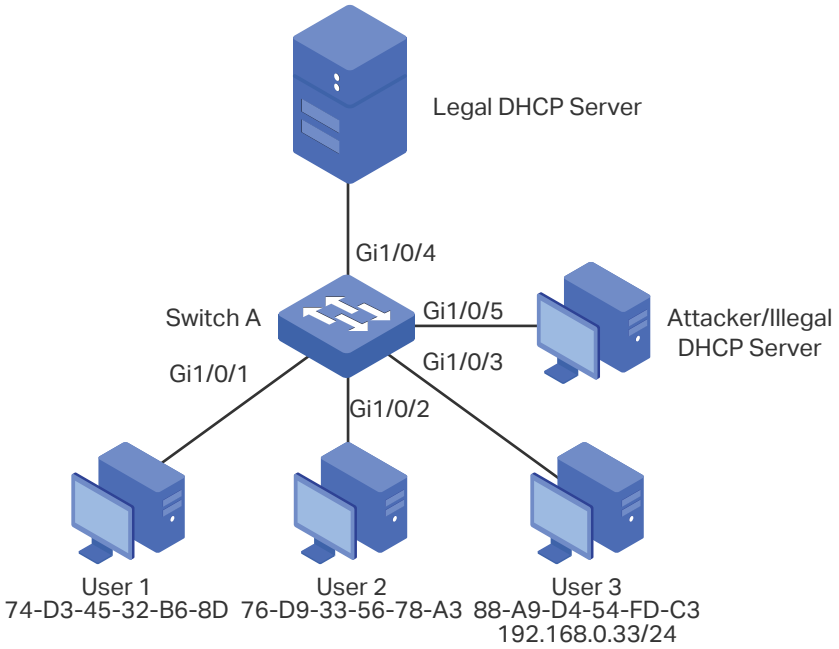
15 Configuration Examples

15.1 Example for DHCP Snooping and ARP Detection

15.1.1 Network Requirements

As shown below, User 1 and User 2 get IP addresses from the legal DHCP server, and User 3 has a static IP address. All of them are in the default VLAN 1. Now, untrusted DHCP packets need to be filtered to ensure that the DHCP clients (User 1 and User 2) can get the IP addresses from the legal DHCP server. Additionally, the network needs to be prevented from ARP attacks.

Figure 15-1 Network Topology



15.1.2 Configuration Scheme

To meet these requirements, you can configure DHCP Snooping to filter the untrusted DHCP packets from the illegal DHCP server and configure ARP Detection and ARP Defend to prevent the network from ARP attacks.

The overview of configuration is as follows:

1) Configure DHCP Snooping on Switch A. Set port 1/0/4 that is connected to the legal DHCP server as the trusted port and other ports as untrusted ports. So that the illegal DHCP server on any other port cannot assign IP addresses for the clients.

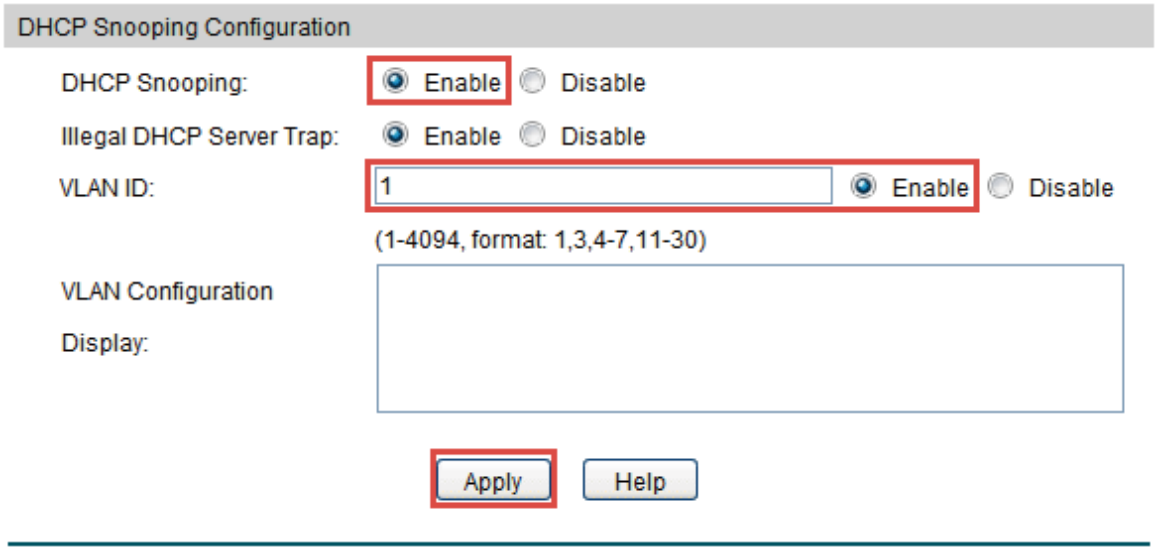
2) Configure IP-MAC Binding on Switch A. The binding entries for User 1 and User 2 will be automatically learned via DHCP Snooping, and you need to manually bind the entry for User 3.
3) Enable ARP Detection on Switch A to prevent ARP cheating attacks.
4) Configure ARP Defend on Switch A to limit the speed of receiving the legal ARP packets on each port, thus to prevent ARP flooding attacks.

Demonstrated with T2600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

15.1.3 Using the GUI

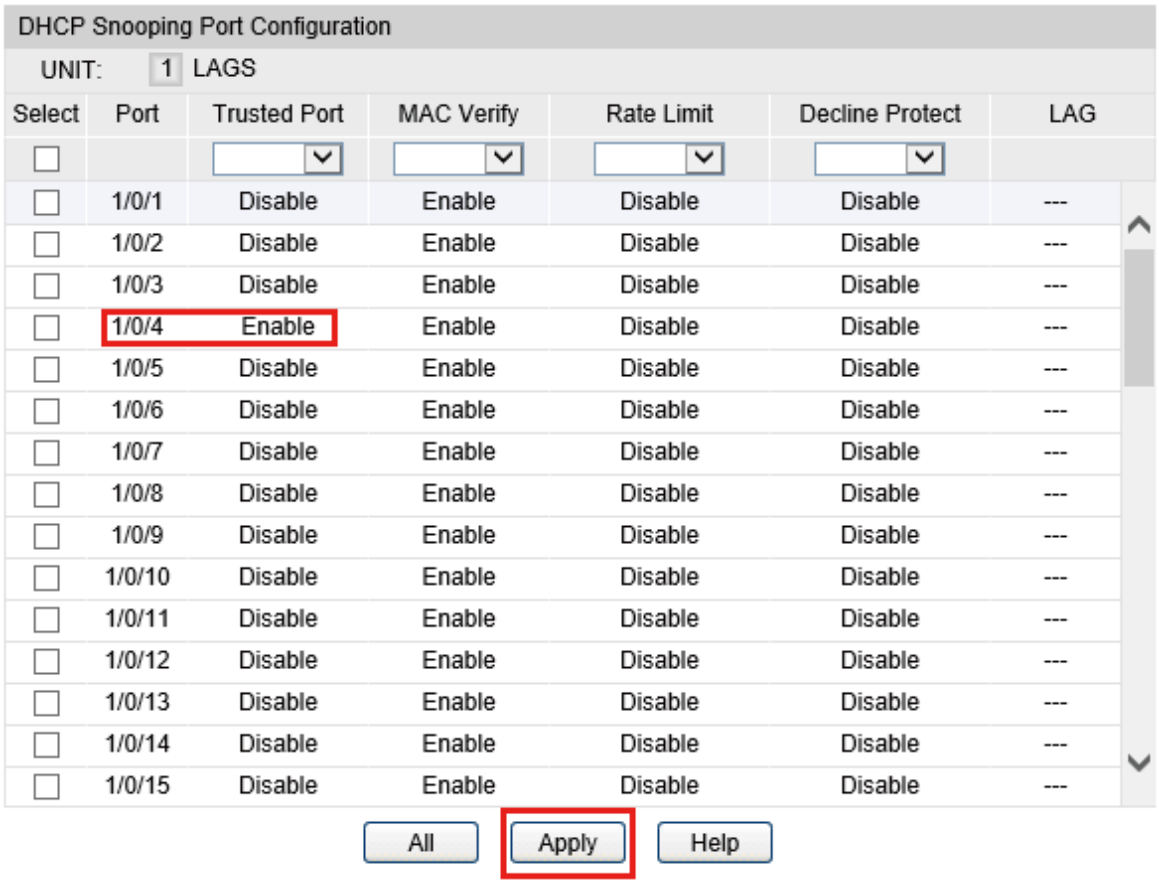
1) Choose the menu **Network Security > DHCP Snooping > Global Config** to load the following page. Because all users are in the default VLAN 1, enable DHCP Snooping on VLAN 1. Click **Apply**.

Figure 15-2 Global Config



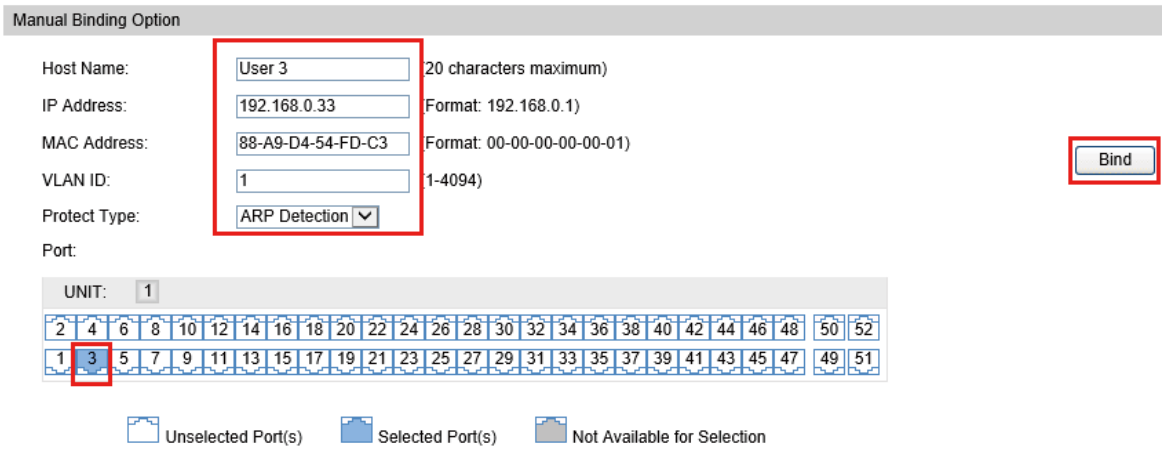
2) Choose the menu **Network Security > DHCP Snooping > Port Config** to load the following page. Set port 1/0/4 as the trusted port and ports 1/0/1-port1/0/3 as untrusted ports, and click **Apply**.

Figure 15-3 Port Config



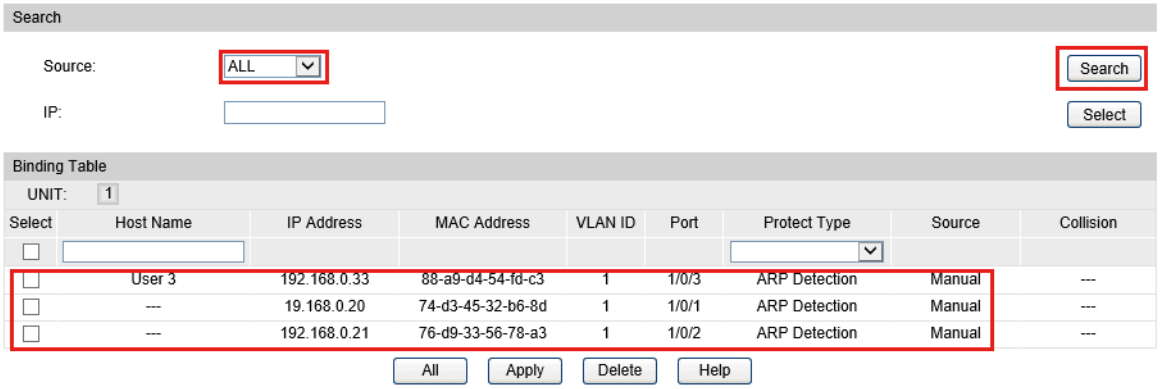
3) Choose the menu **Network Security > IP-MAC Binding > Manual Binding** to load the following page. Enter the host name, IP address, MAC address and VLAN ID of User 3, select ARP Detection as the protect type, and select port 1/0/3 on the panel. Click **Bind**.

Figure 15-4 Manual Binding



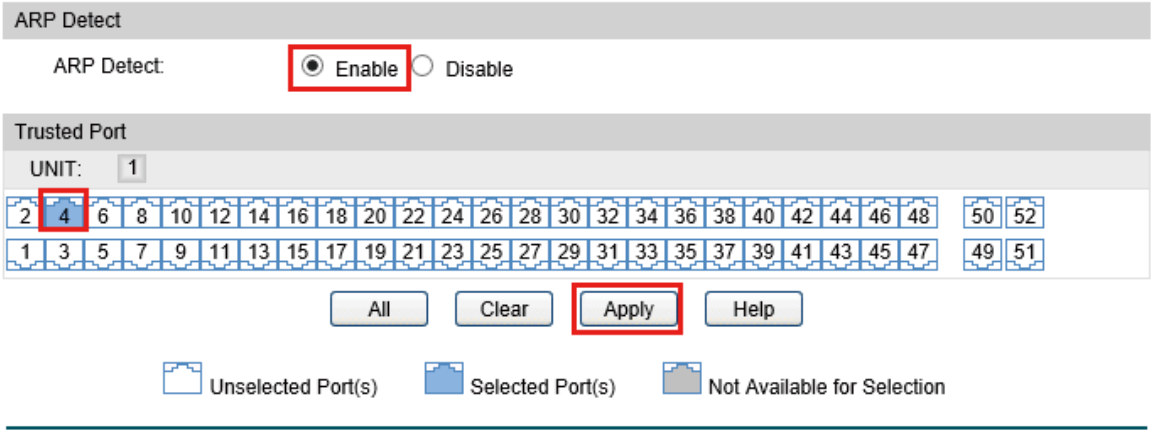
4) Choose the menu **Network Security > IP-MAC Binding > Binding Table** to load the following page. Select Source type as All, and click **Search** to view all the entries that have been bound.

Figure 15-5 Binding Table



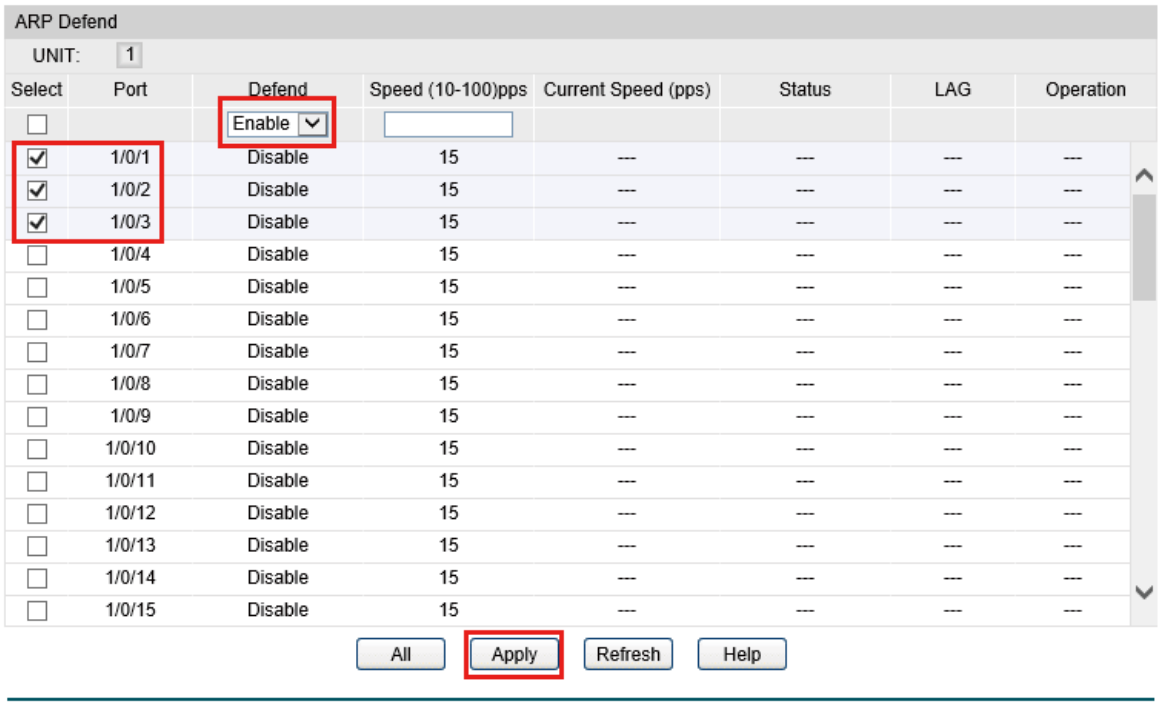
5) Choose the menu **Network Security > ARP Inspection > ARP Detect** to load the following page. Enable ARP Detection and set ports 1/0/4 as trusted port. Click **Apply**.

Figure 15-6 ARP Detect



6) Choose the menu **Network Security > ARP Inspection > ARP Defend** to load the following page. Enable ARP Defend for ports 1/0/1-3 and click **Apply**.

Figure 15-7 ARP Defend



7) Click **Save Config** to save the settings.

15.1.4 Using the CLI

1) Enable DHCP Snooping globally and on VLAN 1.

   Switch_A#configure

   Switch_A(config)#ip dhcp snooping

   Switch_A(config)#ip dhcp snooping vlan 1

2) Configure port 1/0/4 as a trusted port.

   Switch_A(config)#interface gigabitEthernet 1/0/4

   Switch_A(config-if)#ip dhcp snooping trust

   Switch_A(config-if)#exit

3) Manually bind the entry for User 3.

   Switch_A(config)#ip source binding User3 192.168.0.33 88:a9:d4:54:fd:c3 vlan 1 interface gigabitEthernet 1/0/3 arp-detection

4) Enable ARP Detection globally and set port 1/0/4 as a trusted port.

   Switch_A(config)#ip arp inspection

   Switch_A(config)#interface gigabitEthernet 1/0/4

   Switch_A(config-if)#ip arp inspection trust

Switch_A(config-if)#exit

5) Configure ARP Defend on ports 1/0/1-3.

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

Switch_A(config-if-range)#ip arp inspection

Switch_A(config-if-range)#ip arp inspection limit-rate 15

Switch_A(config-if-range)#end

Switch_A#copy running-config startup-config

6) Verify the Configuration

Verify the configuration of DHCP Snooping:

Switch_A#show ip dhcp snooping

Global Status: Enable

VLAN ID: 1

Switch_A#show ip dhcp snooping interface

Interface	Trusted	MAC-Verify	Limit-Rate	Dec-rate	LAG
---	---	---	---	---	---
Gi1/0/1	Disable	Enable	0	0	N/A
Gi1/0/2	Disable	Enable	0	0	N/A
Gi1/0/3	Disable	Enable	0	0	N/A
Gi1/0/4	Enable	Enable	0	0	N/A

...

Verify the IP-MAC Binding entries:

Switch_A#show ip source binding

U	No.	Host	IP-Addr	MAC-Addr	VID	Port	ACL	Col.
--	---	---	---	---	---	---	---	--
1	1	User1	192.168.0.20	74:d3:45:32:6b:8d	1	Gi1/0/1	ARP-D	
1	2	User2	192.168.0.21	76:d9:33:56:78:a3	1	Gi1/0/2	ARP-D	
1	3	User3	192.168.0.33	88:a9:d4:54:fd:c3	1	Gi1/0/3	ARP-D	

Verify the configuration of ARP Detection:

```
Switch_A#show ip arp inspection
ARP detection global status: Enabled
Port        Trusted
Gi1/0/1     NO
Gi1/0/2     NO
Gi1/0/3     NO
Gi1/0/4     YES
...
```

Verify the configuration of ARP Defend:

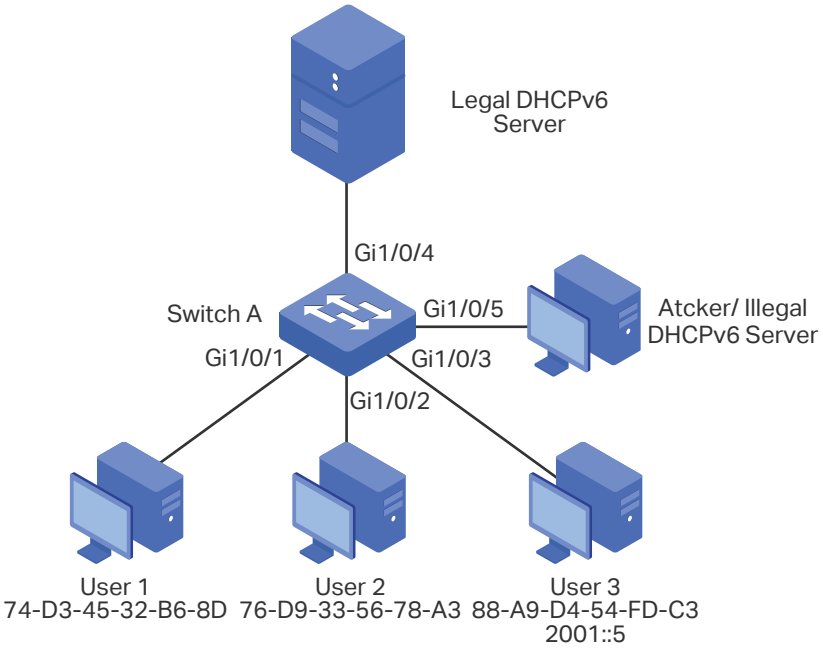
```
Switch_A#show ip arp inspection interface
Port      OverSpeed  Rate  Current   Status     LAG
Gi1/0/1   Enabled    15    N/A       Normal     N/A
Gi1/0/2   Enabled    15    N/A       Normal     N/A
Gi1/0/3   Enabled    15    N/A       Normal     N/A
Gi1/0/4   Disabled   15    N/A       N/A        N/A
...
```

15.2 Example for DHCPv6 Snooping and ND Detection

15.2.1 Network Requirements

As shown below, User 1 and User 2 get IPv6 addresses from the DHCPv6 server, and User 3 has a static IPv6 address. All of them are in the default VLAN 1. Now, untrusted DHCPv6 packets need to be filtered to ensure that the DHCPv6 clients (User 1 and User 2) can get the IPv6 addresses from the legal DHCPv6 server. Additionally, the network needs to be prevented from ND attacks.

Figure 15-8 Network Topology



15.2.2 Configuration Scheme

To meet these requirements, you can configure DHCPv6 Snooping to filter the untrusted DHCPv6 packets from the illegal DHCPv6 server and configure ND Detection to prevent the network from ND attacks. The overview of configuration is as follows:

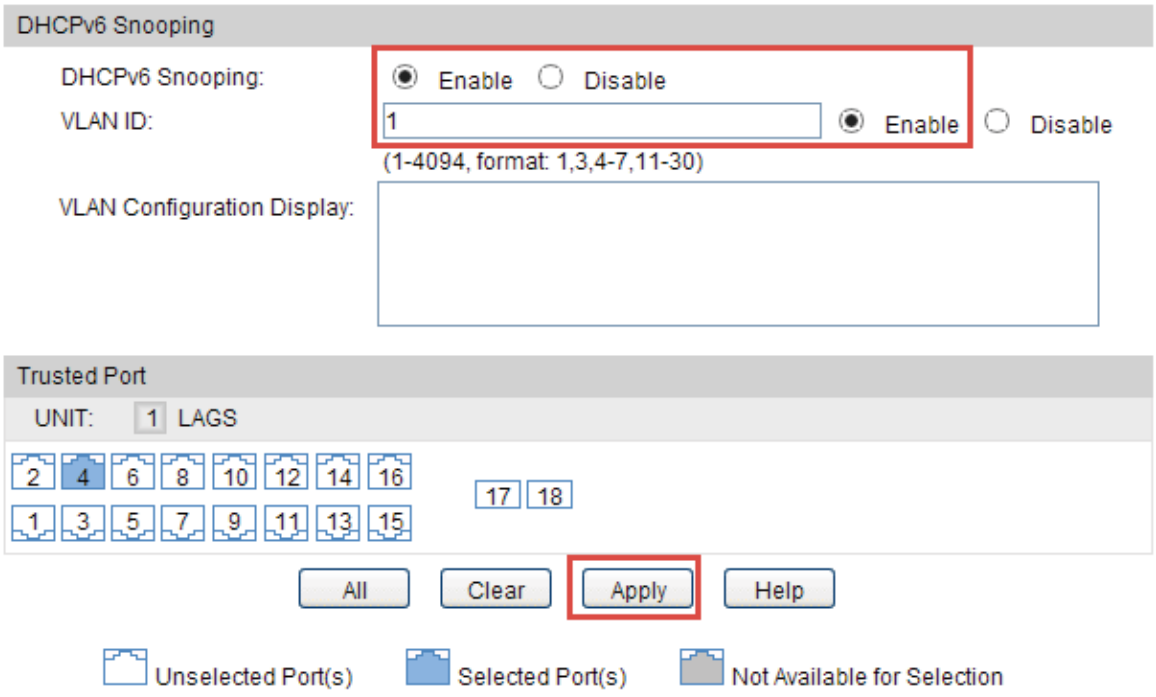
1) Configure DHCPv6 Snooping on Switch A. Set port 1/0/4 that is connected to the illegal DHCPv6 server as the trusted port and other ports as untrusted ports. So that the illegal DHCPv6 server on any other port cannot assign IPv6 addresses for the clients.
2) Configure IPv6-MAC Binding on Switch A. The binding entries for User 1 and User 2 will be automatically learned via DHCPv6 Snooping, and you need to manually bind the entry for User 3.
3) Enable ND Detection on Switch A to prevent ND attacks.

Demonstrated with T2600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

15.2.3 Using the GUI

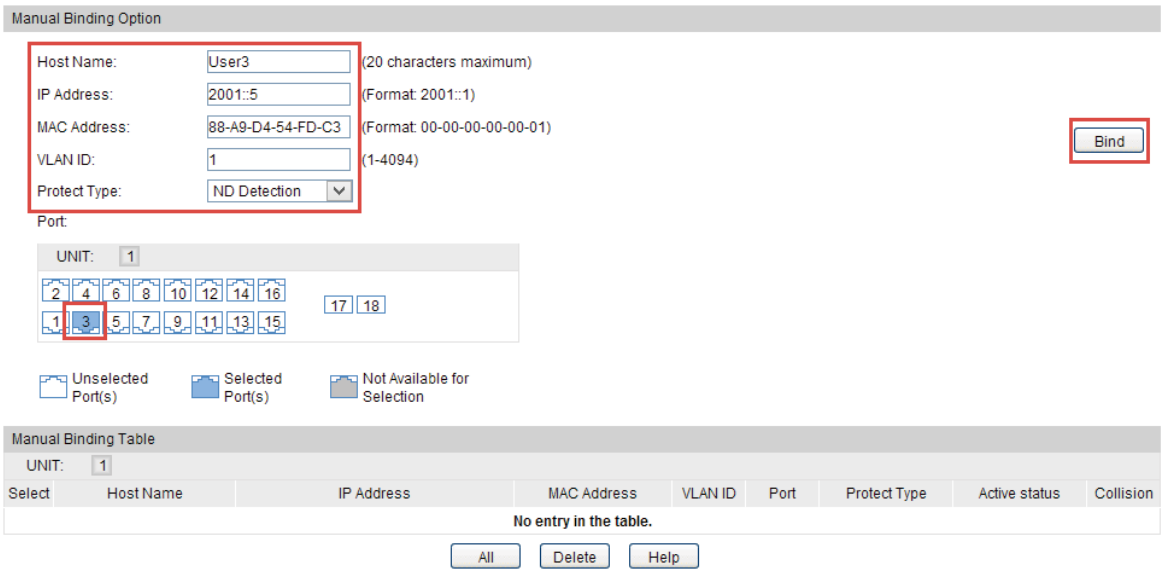
1) Choose the menu **Network Security > DHCPv6 Snooping > Global Config** to load the following page. Because all users are in the default VLAN 1, enable DHCPv6 Snooping on VLAN 1. Set port 1/0/4 as a trusted port. Click **Apply**. After that, the IPv6-MAC binding entries of the DHCPv6 clients will be automatically learned via DHCPv6 Snooping.

Figure 15-9 Global Config



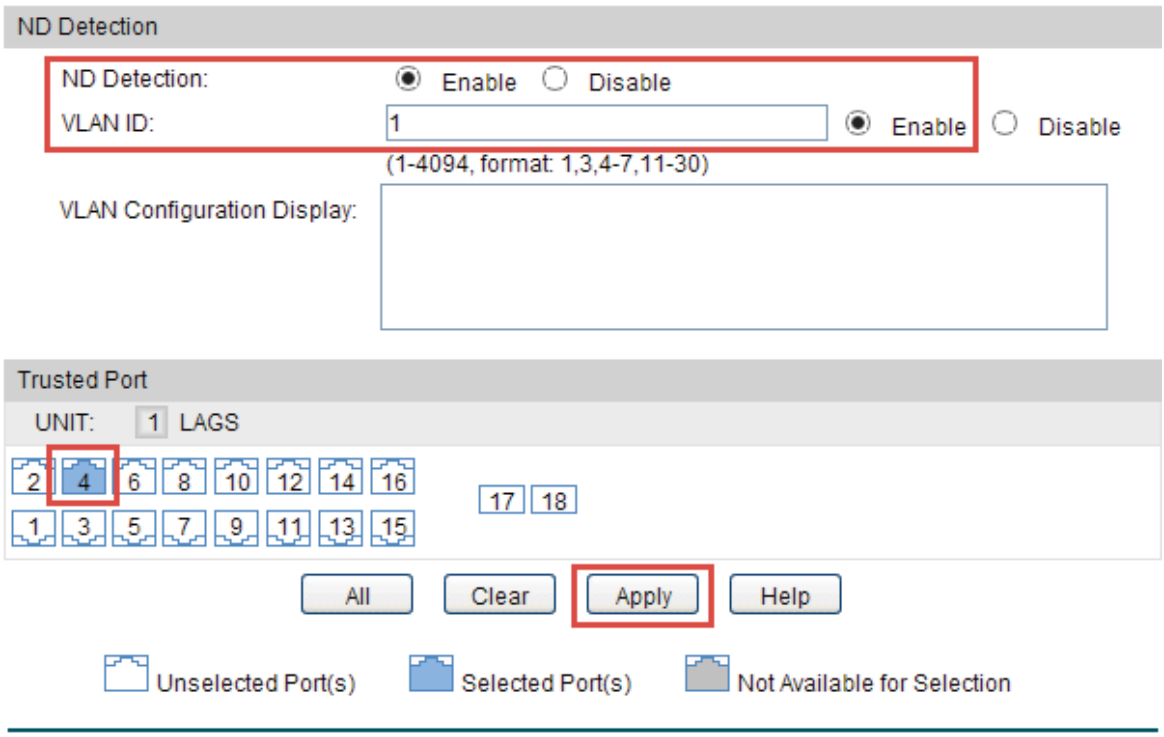
2) Choose the menu **Network Security > IP-MAC Binding > Manual Binding** to load the following page. Enter the host name, IP address, MAC address and VLAN ID of User 3, select ARP Detection as the protect type, and select port 1/0/3 on the panel. Click **Bind**.

Figure 15-10 Manual Binding



3) Choose the menu **Network Security > ND Detection > ND Detection** to load the following page. Because all users are in the default VLAN 1, enable ND Detection on VLAN 1. Set port 1/0/4 as a trusted port. Click **Apply**.

Figure 15-11 ND Detection



4) Click **Save Config** to save the settings.

15.2.4 Using the CLI

1) Enable DHCPv6 Snooping globally and on VLAN 1.

   Switch_A#configure

   Switch_A(config)#ipv6 dhcp snooping

   Switch_A(config)#ipv6 dhcp snooping vlan 1

2) Configure port 1/0/4 as a trusted port.

   Switch_A(config)#interface gigabitEthernet 1/0/4

   Switch_A(config-if)#ipv6 dhcp snooping trust

   Switch_A(config-if)#exit

3) Manually bind the entry for User 3.

   Switch_A(config)#ipv6 source binding User3 2001::5 88:a9:d4:54:fd:c3 vlan 1 interface gigabitEthernet 1/0/3 nd-detection

4) Enable ND Detection on VLAN 1 and set port 1/0/4 as a trusted port.

   Switch_A(config)#ipv6 nd detection

   Switch_A(config)#ipv6 nd detection vlan 1

   Switch_A(config)#interface gigabitEthernet 1/0/4

Switch_A(config-if)#ipv6 nd detection trust

Switch_A(config-if)#end

Switch_A#copy running-config startup-config

Verify the Configuration

Verify the configuration of DHCPv6 Snooping:

Switch_A#show ipv6 dhcp snooping

Global Status: Enable

VLAN ID: 1

Switch_A#show ipv6 dhcp snooping interface

Interface	Trusted	LAG
Gi1/0/1	Disable	N/A
Gi1/0/2	Disable	N/A
Gi1/0/3	Disable	N/A
Gi1/0/4	Enable	N/A
Gi1/0/5	Disable	N/A

...

Verify the IPv6-MAC Binding entries:

Switch_A#show ipv6 source binding

U	No.	Host	IP-Addr	MAC-Addr	VID	Port	ACL	Active	Source	Col.
1	1	User1	2001::2	74:d3:45:32:b6:8d	1	Gi1/0/1	Both	ND-D	ND Snooping	
1	2	User2	2001::3	76:d9:33:56:78:a3	1	Gi1/0/2	Both	ND-D	ND Snooping	
1	3	User3	2001::5	88:a9:d4:54:fd:c3	1	Gi1/0/3	ND-D	ND-D	Manual	

Verify the configuration of ND Detection:

Switch_A#show ipv6 nd detection

Global Status: Enable

VLAN ID: 1

Switch_A#show ipv6 nd detection interface

Interface Trusted LAG

--------- ------- ----

Gi1/0/1 Disable N/A

Gi1/0/2 Disable N/A

Gi1/0/3 Disable N/A

Gi1/0/4 Enable N/A

Gi1/0/5 Disable N/A

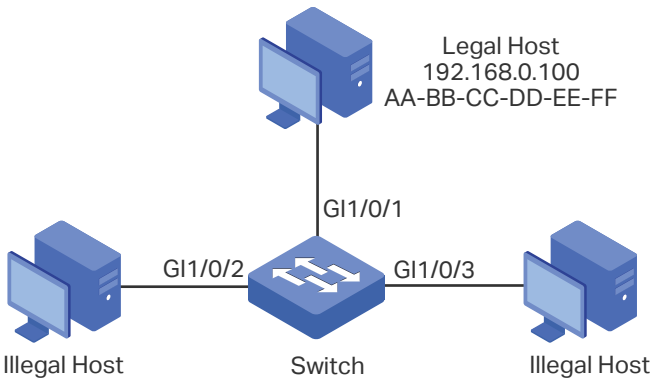
...

15.3 Example for IP Source Guard

15.3.1 Network Requirements

As shown below, the legal host connects to the switch via port 1/0/1 and belongs to the default VLAN 1. It is required that only the legal host can access the network via port 1/0/1, and other unknown hosts will be blocked when trying to access the network via ports 1/0/1-3.

Figure 15-12 Network Topology



15.3.2 Configuration Scheme

To implement this requirement, you can use IP-MAC Binding and IP Source Guard to filter out the packets received from the unknown hosts. The overview of configuration on the switch is as follows:

1) Bind the MAC address, IP address, connected port number and VLAN ID of the legal host with IP-MAC Binding.

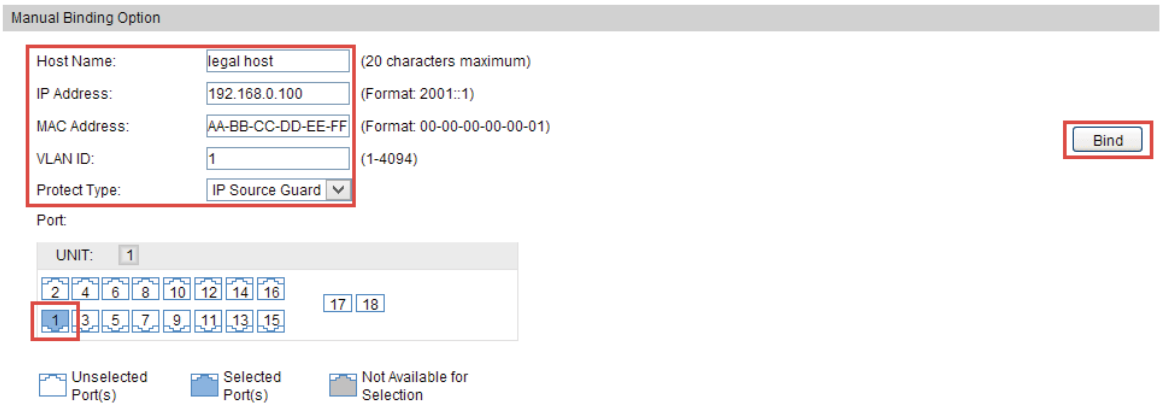
2) Enable IP Source Guard on ports 1/0/1-3.

Demonstrated with T2600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

15.3.3 Using the GUI

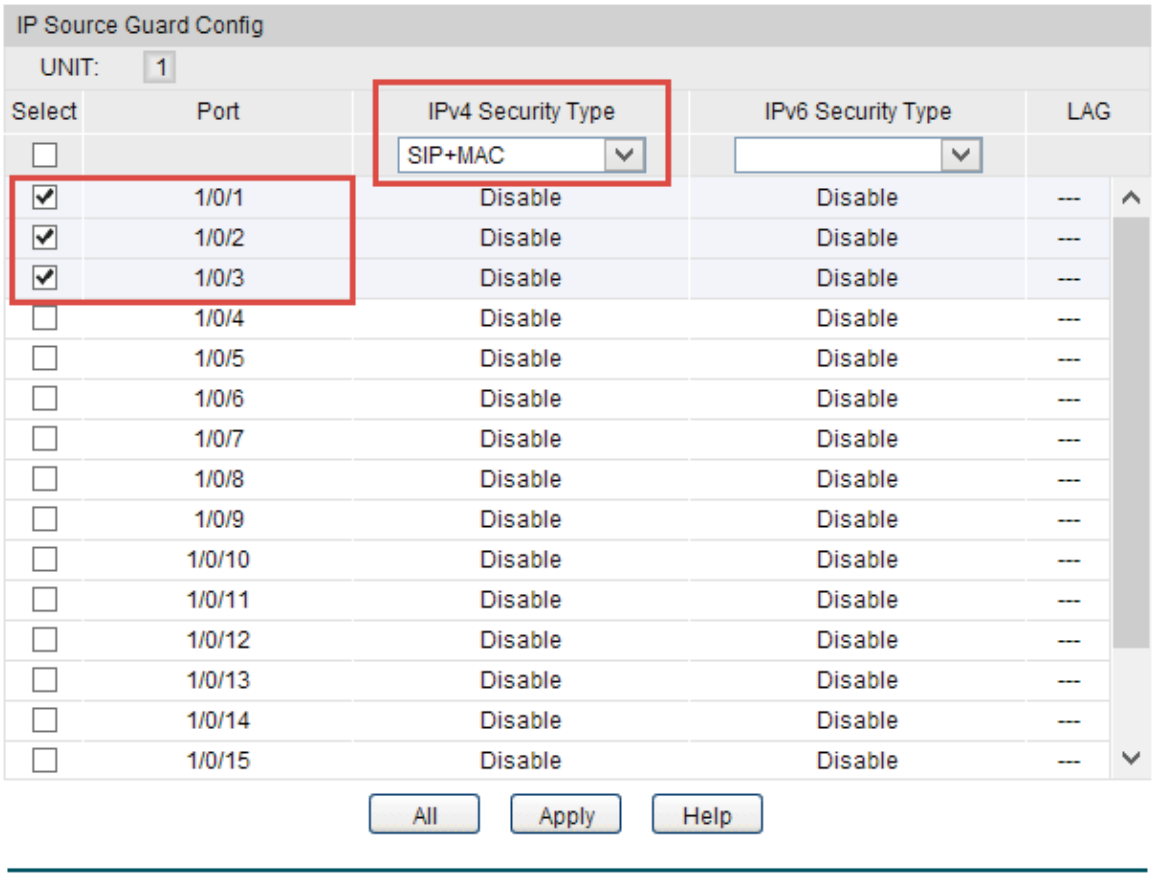
1) Choose the menu **Network Security > IP-MAC Binding > Manual Binding** to load the following page. Specify the host name, IP address, MAC address, VLAN ID of the host, select Protect Type as IP Source Guard, and select port 1/0/1. Click **Bind**.

Figure 15-13 Manual Binding



2) Choose the menu **Network Security > IP Source Guard> IP Source Guard** to load the following page. Select ports 1/0/1-3, configure the IPv4 Security Type as SIP+MAC, and click **Apply**. Then the switch will check the packets received from ports 1/0/1-3

Figure 15-14 IP Source Guard



3) Click **Save Config** to save the settings.

15.3.4 Using the CLI

1) Manually bind the IP address, MAC address, VLAN ID and connected port number of the host, and apply this entry to the IP Source Guard feature.

   Switch#configure

   Switch(config)#ip source binding legal-host 192.168.0.100 aa:bb:cc:dd:ee:ff vlan 1 interface gigabitEthernet 1/0/1 ip-verify-source

2) Enable IP Source Guard on ports 1/0/1-3.

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

   Switch(config-if-range)#ip verify source sip+mac

   Switch(config-if-range)#end

   Switch#copy running-config startup-config

Verify the Configuration

Verify the binding entry:

Switch#show ip source binding

U	No.	Host	IP-Addr	MAC-Addr	VID	Port	ACL	Col.
-	---	----	-------------	--------	---	-------	------	----
1	1	legal-host	192.168.0.100	aa:bb:cc:dd:ee:ff	1	Gi1/0/1	IP-V-S	

Notice:

1. Here,'Col.'stands for 'Collision';'ARP-D' for 'ARP-Detection',and'IP-V-S' for 'IP-Verify-Source'.

2. 'No.' stands for the actual index of each entry in the binding-table.They may not actually in the order of 1,2,3,...

Verify the configuration of IP Source Guard:

Switch#show ip verify source

Port	Security-Type	LAG
Gi1/0/1	SIP+MAC	N/A
Gi1/0/2	SIP+MAC	N/A
Gi1/0/3	SIP+MAC	N/A

...

15.4 Example for 802.1X

15.4.1 Network Requirements

The network administrator wants to control access from the end users (clients) in the company. It is required that all clients need to be authenticated separately and that only the authenticated clients can access the Internet.

15.4.2 Configuration Scheme

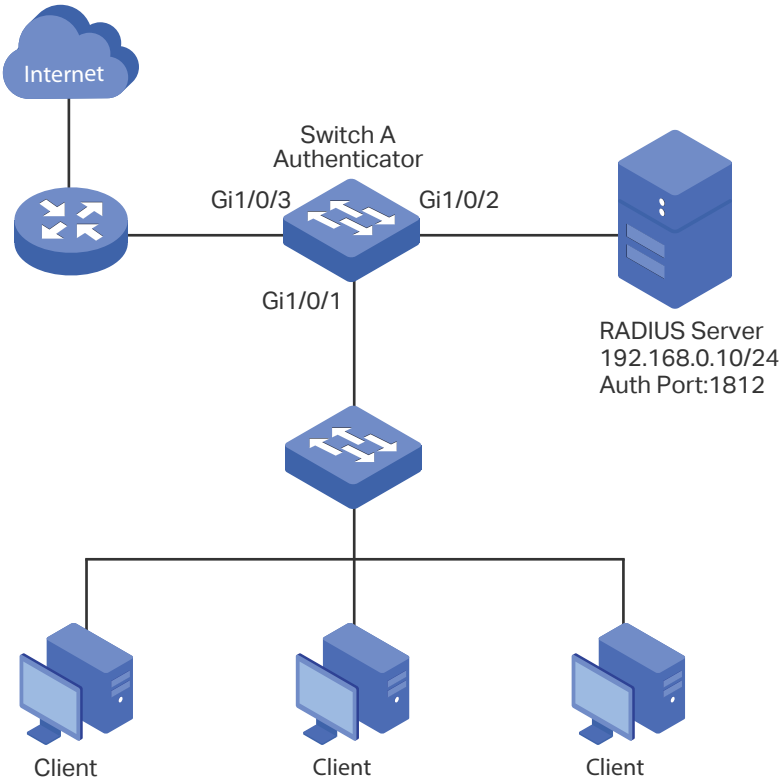
- To authenticate clients separately, enable 802.1X authentication, configure the control mode as auto, and set the control type as MAC based.
- Enable 802.1X authentication on the ports connected to clients.

- Keep 802.1X authentication disabled on ports connected to the authentication server and the Internet, which ensures unrestricted connections between the switch and the authentication server or the Internet.

15.4.3 Network Topology

As shown in the following figure, Switch A acts as the authenticator. Port 1/0/1 is connected to the client, port 1/0/2 is connected to the RADIUS server, and port 1/0/3 is connected to the Internet.

Figure 15-15 Network Topology



Demonstrated with T2600G-28TS acting as the authenticator, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

15.4.4 Using the GUI

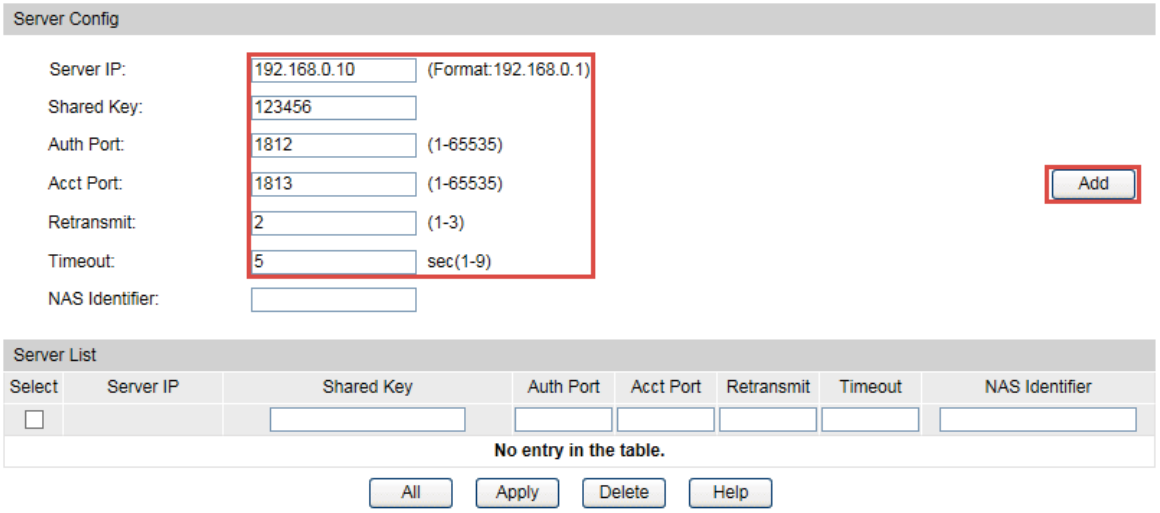
1) Choose the menu **Network Security > AAA > Global Config** to load the following page. Enable AAA function globally on the switch.

Figure 15-16 Enable AAA Function



2) Choose the menu **Network Security > AAA > RADIUS Config** to load the following page. Configure the parameters of the RADIUS server.

Figure 15-17 RADIUS Config



3) Choose the menu **Network Security > AAA > Server Group** to load the following page. In the **Add New Server Group** section, specify the group name as radius1 and the server type as RADIUS. Click **Add** to create the server group.

Figure 15-18 Create Server Group



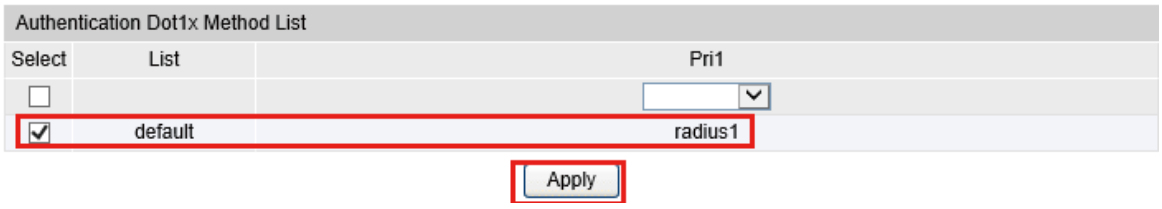
4) On the same page, select the newly created server group and click **edit** to load the following page. Select 192.168.0.10 from the drop-down list, and click **Add** to add the server to the group.

Figure 15-19 Add Servers to Server Group



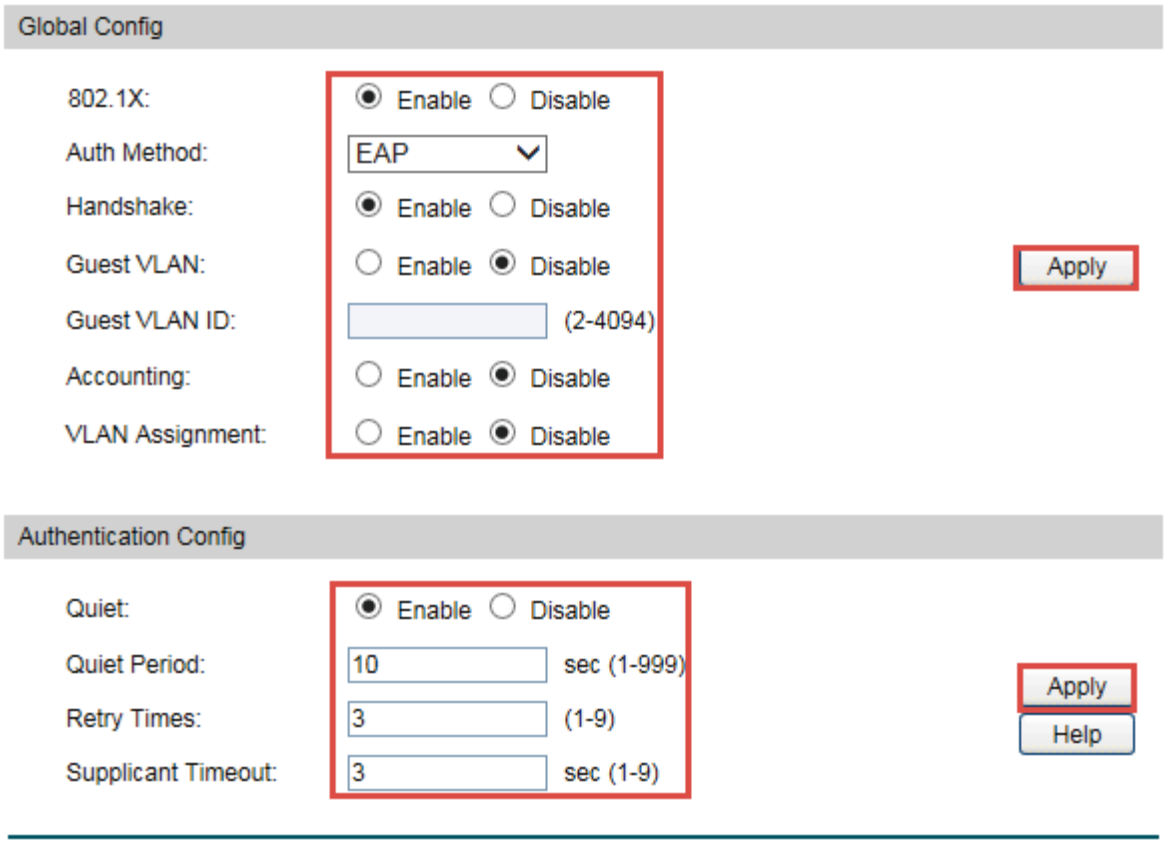
5) Choose the menu **Network Security > AAA > Dot1x List** to load the following page. In the **Authentication Dot1x Method List** section, select radius1 as the radius server group for authentication, and click **Apply**.

Figure 15-20 Configure Authentication RADIUS Server



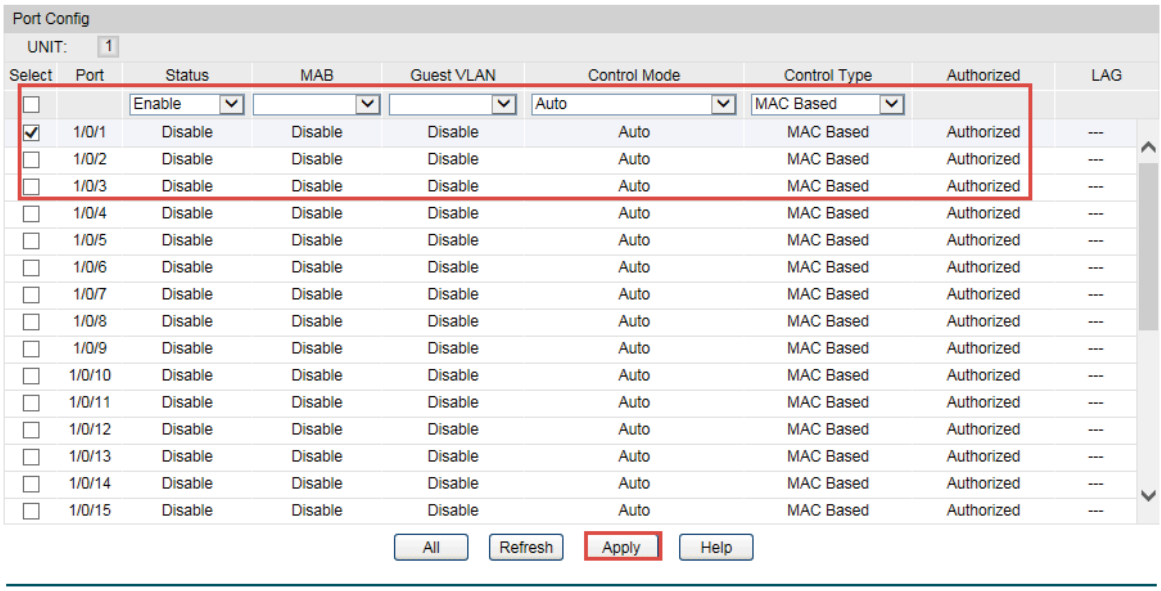
6) Choose the menu **Network Security > 802.1X Authentication > Global Config** to load the following page. Enable 802.1X authentication and configure the Authentication Method as EAP. Enable the Quiet feature and then keep the default authentication settings.

Figure 15-21 Global Config



7) Choose the menu **Network Security > 802.1X Authentication > Port Config** to load the following page. For port 1/0/1, enable 802.1X authentication, set the Control Mode as auto and set the Control Type as MAC Based; For port 1/0/2 and port 1/0/3, disable 802.1X authentication.

Figure 15-22 Port Config



8) Click **Save Config** to save the settings.

15.4.5 Using the CLI

1) Enable AAA function globally and configure the RADIUS parameters.

Switch_A(config)#aaa enable

Switch_A(config)#radius-server host 192.168.0.10 auth-port 1812 key 123456

Switch_A(config)#aaa group radius radius1

Switch_A(aaa-group)#server 192.168.0.10

Switch_A(aaa-group)#exit

Switch_A(config)#aaa authentication dot1x default radius1

Switch_A(config)#end

Switch_A#copy running-config startup-config

2) Globally enable 802.1X authentication and set the authentication method; enable the quiet feature and configure relevant parameters.

Switch_A#configure

Switch_A(config)#dot1x system-auth-control

Switch_A(config)#dot1x auth-method eap

Switch_A(config)#dot1x quiet-period

3) Disable 802.1X authentication on port 1/0/2 and port 1/0/3. Enable 802.1X authentication on port 1/0/1, set the control mode as auto, and set the control type as MAC based.

```
Switch_A(config)#interface gigabitEthernet 1/0/2
Switch_A(config-if)#no dot1x
Switch_A(config-if)#exit
Switch_A(config)#interface gigabitEthernet 1/0/3
Switch_A(config-if)#no dot1x
Switch_A(config-if)#exit
Switch_A(config)#interface gigabitEthernet 1/0/1
Switch_A(config-if)#dot1x
Switch_A(config-if)#dot1x port-method mac-based
Switch_A(config-if)#dot1x port-control auto
Switch_A(config-if)#exit
```

Verify the Configurations

Verify the global configurations of 802.1X authentication:

```
Switch_A#show dot1x global
802.1X State:                   Enabled
Authentication Method:          EAP
Handshake State:                Enabled
Guest VLAN State:               Disabled
Guest VLAN ID:                  N/A
802.1X Accounting State: Disabled
802.1X VLAN Assignment State:   Disabled
Quiet-period State:             Enabled
Quiet-period Timer:             10 sec.
Max Retry-times For RADIUS Packet: 3
Supplicant Timeout:             3 sec.
```

Verify the configurations of 802.1X authentication on the port:

```
Switch_A#show dot1x interface
Port      State    MAB State  GuestVLAN  PortControl  PortMethod   Authorized  LAG
----      ------   ---------  ---------  -----------  ----------   ----------  ---
Gi1/0/1   enabled  disabled   disabled       auto       mac-based    authorized  N/A
Gi1/0/2   disabled disabled   disabled       auto       mac-based    authorized  N/A
Gi1/0/3   disabled disabled   disabled       auto       mac-based    authorized  N/A
...
```

Verify the configurations of RADIUS :

```
Switch_A#show aaa global
 AAA global status:        Enable
 Module          Login List        Enable List
 Console         default           default
 Telnet          default           default
 Ssh             default           default
 Http            default           default
Switch_A#show aaa authentication dot1x
        Methodlist     pri1         pri2         pri3         pri4
        default        radius1      --           --           --
Switch_A#show aaa group radius1
192.168.0.10
```

15.5 Example for AAA

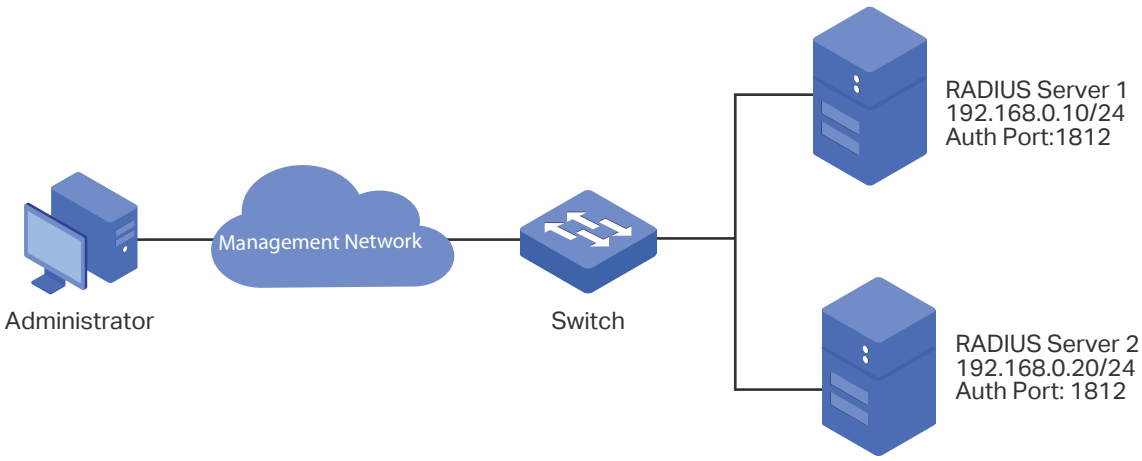
15.5.1 Network Requirements

As shown below, the switch needs to be managed remotely via Telnet. In addition, the senior administrator of the company wants to create an account for the less senior administrators, who can only view the configurations and some network information without the Enable password provided.

Two RADIUS servers are deployed in the network to provide a safer authenticate method for the administrators trying to log in or get administrative privileges. If RADIUS Server 1

breaks down and doesn't respond to the authentication request, RADIUS Server 2 will work, so as to ensure the stability of the authentication system.

Figure 15-23 Network Topology



15.5.2 Configuration Scheme

To implement this requirement, the senior administrator can create the login account and the Enable password on the two RADIUS servers, and configure the AAA feature on the switch. The IP addresses of the two RADIUS servers are 192.168.0.10/24 and 192.168.0.20/24; the authentication port number is 1812; the shared key is 123456.

The overview of configuration on the switch is as follows:

1) Globally enable AAA.

1) Add the two RADIUS servers on the switch.

2) Create a new RADIUS server group and add the two servers to the group. Make sure that RADIUS Server 1 is the first server for authentication.

3) Configure the method list.

4) Configure the AAA application list.

Demonstrated with T2600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

15.5.3 Using the GUI

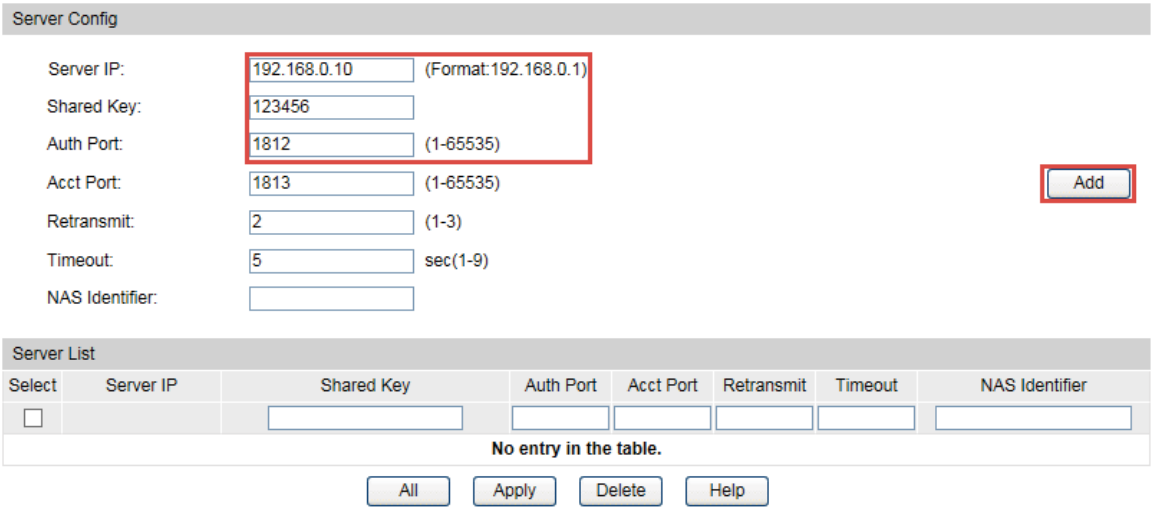
1) Choose the menu **Network Security > AAA > Global Config** to load the following page. In the **Global Config** section, enable AAA and click **Apply.**

Figure 15-24 Global Config



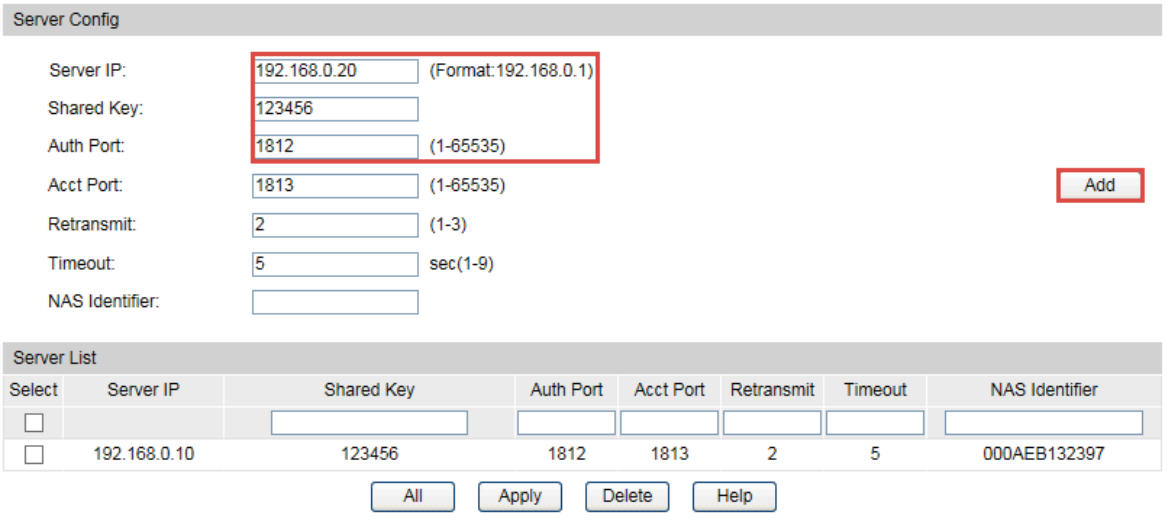
2) Choose the menu **Network Security > AAA > RADIUS Server** to load the following page. Configure the Server IP as 192.168.0.10, the Shared Key as 123456, the Auth Port as 1812, and keep the other parameters as default. Click **Add** to add RADIUS Server 1 on the switch.

Figure 15-25 Add RADIUS Server 1



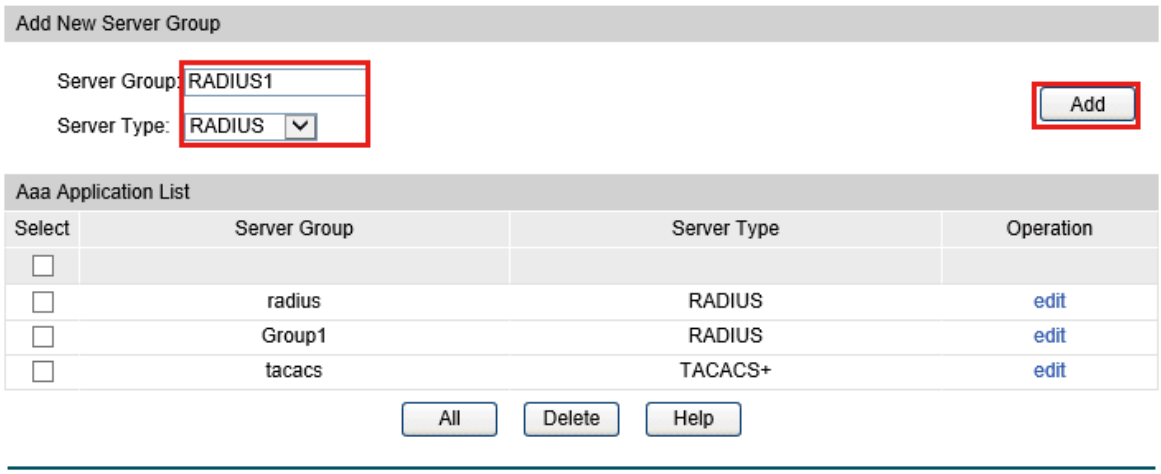
3) On the same page, configure the Server IP as 192.168.0.20, the Shared Key as 123456, the Auth Port as 1812, and keep the other parameters as default. Click **Add** to add RADIUS Server 2 on the switch.

Figure 15-26 Add RADIUS Server 2



4) Choose the menu **Network Security > AAA > Server Group** to load the following page. In the **Add New Server Group** section, specify the group name as RADIUS1 and the server type as RADIUS. Click **Add** to create the server group.

Figure 15-27 Create Server Group



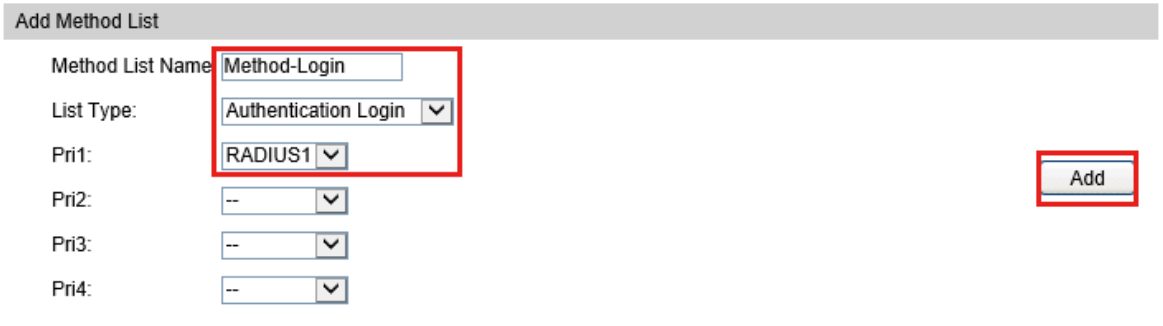
5) On the same page, select the newly created server group and click **edit** to load the following page. Select 192.168.0.10 from the drop-down list, and click **Add** to add RADIUS Server 1 to the group. Then select 192.168.0.20 from the drop-down list, and click **Add** to add RADIUS Server 2 to the group.

Figure 15-28 Add Servers to Server Group



6) Choose the menu **Network Security > AAA > Method List** to load the following page. Specify the Method List Name as Method-Login, select the List Type as Authentication Login, and select the Pri1 as RADIUS1. Click **Add** to set the method list for the Login authentication.

Figure 15-29 Configure Login Method List



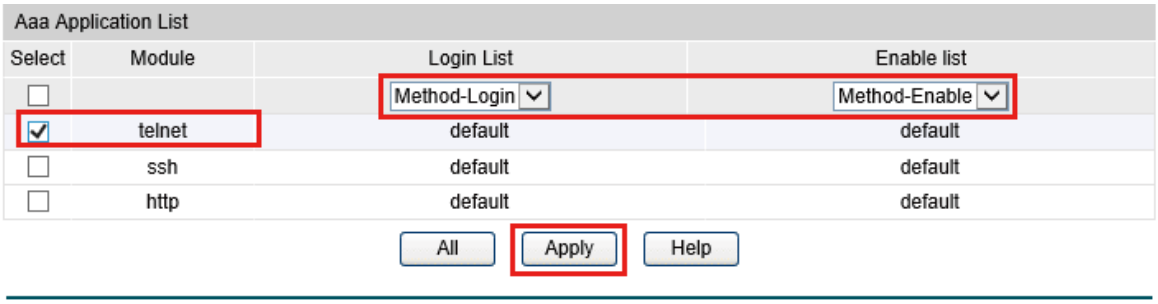
7) On the same page, specify the Method List Name as Method-Enable, select the List Type as Authentication Enable, and select the Pri1 as RADIUS1. Click **Add** to set the method list for the Enable password authentication.

Figure 15-30 Configure Enable Method List



8) Choose the menu **Network Security > AAA > Global Config** to load the following page. In the **AAA Application List** section, select telnet and configure the Login List as Method-Login and Enable List as Method-Enable. Then click **Apply**.

Figure 15-31 Configure AAA Application List



9) Click **Save Config** to save the settings.

15.5.4 Using the CLI

1) Enable AAA globally.

Switch#configure

Switch(config)#aaa enable

2) Add RADIUS Server 1 and RADIUS Server 2 on the switch.

Switch(config)#radius-server host 192.168.0.10 auth-port 1812 key 123456

Switch(config)#radius-server host 192.168.0.20 auth-port 1812 key 123456

3) Create a new server group named RADIUS1 and add the two RADIUS servers to the server group.

Switch(config)#aaa group radius RADIUS1

Switch(aaa-group)#server 192.168.0.10

Switch(aaa-group)#server 192.168.0.20

Switch(aaa-group)#exit

4) Create two method lists: Method-Login and Method-Enable, and configure the server group RADIUS1 as the authentication method for the two method lists.

Switch(config)#aaa authentication login Method-Login RADIUS1

Switch(config)#aaa authentication enable Method-Enable RADIUS1

5) Configure Method-Login and Method-Enable as the authentication method for the Telnet application.

Switch(config)#line telnet

Switch(config-line)#login authentication Method-Login

Switch(config-line)#enable authentication Method-Enable

Switch(config-line)#end

Switch#copy running-config startup-config

Verify the Configuration

Verify the configuration of the RADIUS servers:

Switch#show radius-server

Server Ip	Auth Port	Acct Port	Timeout	Retransmit	NAS Identifier	Shared key
192.168.0.10	1812	1813	5	2	000AEB132397	123456
192.168.0.20	1812	1813	5	2	000AEB132397	123456

Verify the configuration of server group RADIUS1:

Switch#show aaa group RADIUS1

192.168.0.10

192.168.0.20

Verify the configuration of the method lists:

Switch#show aaa authentication

Authentication Login Methodlist:

Methodlist	pri1	pri2	pri3	pri4
default	local	--	--	--
Method-Login	RADIUS1	--	--	--

Authentication Enable Methodlist:

Methodlist	pri1	pri2	pri3	pri4
default	none	--	--	--
Method-Enable	RADIUS1	--	--	--

...

Verify the status of the AAA feature and the configuration of the AAA application list:

Switch#show aaa global

AAA global status: Enable

Module	Login List	Enable List
Console	default	default
Telnet	Method-Login	Method-Enable
SSH	default	default
Http	default	default

16 Appendix: Default Parameters

Default settings of Network Security are listed in the following tables.

Table 16-1 IP-MAC Binding

Parameter	Defualt Setting
Protect Type	For Manual Binding: None For ARP Scanning: None For DHCP Snooping: All

Table 16-2 IPv6-MAC Binding

Parameter	Default Setting
Protect Type	For Manual Binding: None For ND Snooping: All For DHCPv6 Snooping: All

Table 16-3 ND Snooping

Parameter	Default Setting
ND Snooping	Disable
VLAN ID	None
Maximum Entry	1024

Table 16-4 DHCP Snooping

Parameter	Default Setting
Global Config	
DHCP Snooping	Disable
VLAN ID	Disable
Port Config	
Trusted Port	Disable
MAC Verify	Enable

Parameter	Default Setting
Rate Limit	Disable
Decline Protect	Disable
Option 82 Config	
Option 82 Support	Disable
Operation Strategy	Keep
Option 82 Format	Normal
Circuit ID Customization	Disable
Circuit ID	None
Remote ID Customization	Disable
Remote ID	None

Table 16-5 DHCPv6 Snooping

Parameter	Default Setting
Global Config	
DHCPv6 Snooping	Disable
VLAN ID	Disable
Trusted Port	None

Table 16-6 ARP Inspection

Parameter	Default Setting
ARP Detect	
ARP Detect	Disable
Trusted Port	None
ARP Defend	
Defend	Disable
Speed	15 pps
ARP Statistics	

Parameter	Default Setting
Auto Refresh	Disable
Refresh Interval	5 seconds

Table 16-7 ND Detection

Parameter	Default Setting
ND Detection	Disable
VLAN ID	Disable
Trusted Port	None

Table 16-8 IP Source Guard

Parameter	Default Setting
IPv4 Security Type	Disable
IPv6 Security Type	Disable

Table 16-9 DoS Defend

Parameter	Default Setting
DoS Defend	Disable

Table 16-10 802.1X

Parameter	Default Setting
Global Config	
802.1X Authentication	Disable
Auth Method	EAP
Handshake	Enable
Guest VLAN	Disable
Accounting	Disable
VLAN Assignment	Disable

Parameter	Default Setting
Quiet Feature	
Quiet Feature	Disable
Quiet Period	10 seconds
Retry Times	3
Supplicant Timeout	3 seconds
Port Config	
802.1X Status	Disable
MAB	Disable
Guest VLAN	Disable
Control Mode	Auto
Control Type	MAC Based
Dot1X List	
Authentication Dot1x Method List	List Name: default Pri1: radius
Accounting Dot1x Method List	List Name: default Pri1:radius

Table 16-11 PPPoE ID-Insertion

Parameter	Default Setting
Global Config	
PPPoE ID-Insertion	Disable
Port Config	
Circuit-ID	Disable
Circuit-ID Type	IP
UDF Value	None
Remote-ID	Disable
Remote-ID Value	None

Table 16-12 AAA

Parameter	Defualt Setting
Global Config	
AAA	Disable
RADIUS Config	
Server IP	None
Shared Key	None
Auth Port	1812
Acct Port	1813
Retransmit	2
Timeout	5 seconds
NAS Identifier	The MAC address of the switch.
TACACS+ Config	
Server IP	None
Timeout	5 seconds
Shared Key	None
Port	49
Server Group: There are two default server groups: radius and tacacs.	
Method List	
Authentication Login Method List	List name: default Pri1: local
Authentication Enable Method List	List name: default Pri1: none
AAA Application List	
console	Login List: default Enable List: default

Parameter	Defualt Setting
telnet	Login List: default Enable List: default
ssh	Login List: default Enable List: default
http	Login List: default Enable List: default

Table 16-13 DHCP Server FIlter

Parameter	Default Setting
Global Config	
DHCP Server Filter	Disable
DHCP Server Filter Trap	Disable
Port Config	
State	Disable

Table 16-14 NetBIOS Filtering

Parameter	Default Setting
NetBIOS Filtering Port Configuration	
NetBIOS Filtering Over TCP/IP	Disable

Part 27

Configuring LLDP

CHAPTERS

1. LLDP
2. LLDP Configurations
3. LLDP-MED Configurations
4. Viewing LLDP Settings
5. Viewing LLDP-MED Settings
6. Configuration Example
7. Appendix: Default Parameters

1 LLDP

1.1 Overview

LLDP (Link Layer Discovery Protocol) is a neighbor discovery protocol that is used for network devices to advertise information about themselves to other devices on the network. This protocol is a standard IEEE 802.1ab defined protocol and runs over the Layer 2 (the data-link layer) , which allows for interoperability between network devices of different vendors.

With the LLDP feature, network administrators can get the managed network devices' information from the switch or the NMS (Network Management System), which can help them know about the network topology, examine the network connectivity and troubleshoot the network faults.

LLDP-MED (Media Endpoint Discovery) is an extension of LLDP that is used to advertise information between network devices and media endpoints. It is specially used together with Voice VLAN to allow VoIP (Voice over Internet Protocol) device to access the network. VoIP devices can use LLDP-MED for auto-configuration to minimize the configuration effort.

1.2 Supported Features

The switch supports LLDP and LLDP-MED.

LLDP allows the local device to encapsulate its management address, device ID, interface ID and other information into a LLDPDU (Link Layer Discovery Protocol Data Unit) and periodically advertise this LLDPDU to its neighbor devices on the network. The neighbors store the received LLDPDU in a standard MIB (Management Information Base), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP-MED allows the network device to send its information including Voice VLAN information, PoE (Power over Ethernet) capacity and etc. to the media endpoint devices for auto-configuration. The media endpoint devices (IP phones) receive the Voice VLAN information and finish the auto-configuration, then send the voice traffic carrying VLAN tag, which can provide preferential treatment to the voice traffic in the Voice VLAN.

2 LLDP Configurations

With LLDP configurations, you can:

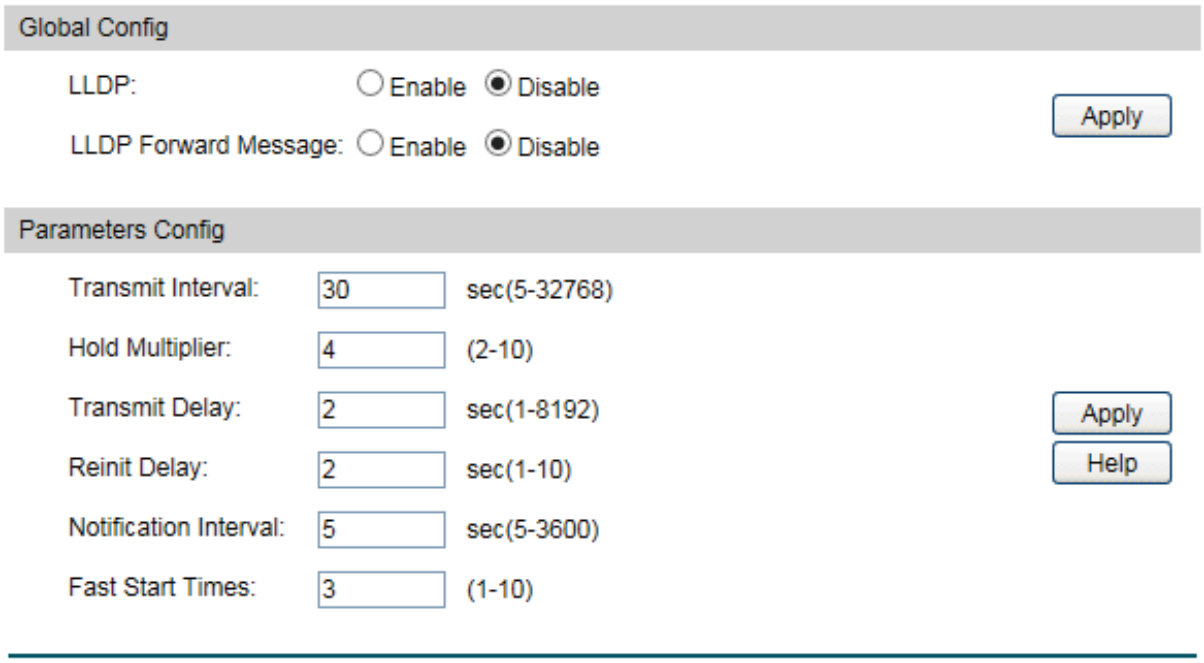
1) Enable the LLDP feature on the switch.
2) (Optional) Configure the LLDP feature globally.
3) (Optional) Configure the LLDP feature for the interface.

2.1 Using the GUI

2.1.1 Global Config

Choose the **LLDP** > **Basic Config** > **Global Config** to load the following page.

Figure 2-1 Global Config



Follow these steps to enable LLDP and configure the LLDP feature globally.

1) In the **Global Config** section, enable LLDP. You can also enable the switch to forward LLDP messages when LLDP function is disabled. Click **Apply**.

LLDP	Enable or disable LLDP function globally.
LLDP Forward Message	Enable or disable the switch to forward LLDP messages when LLDP function is disabled.

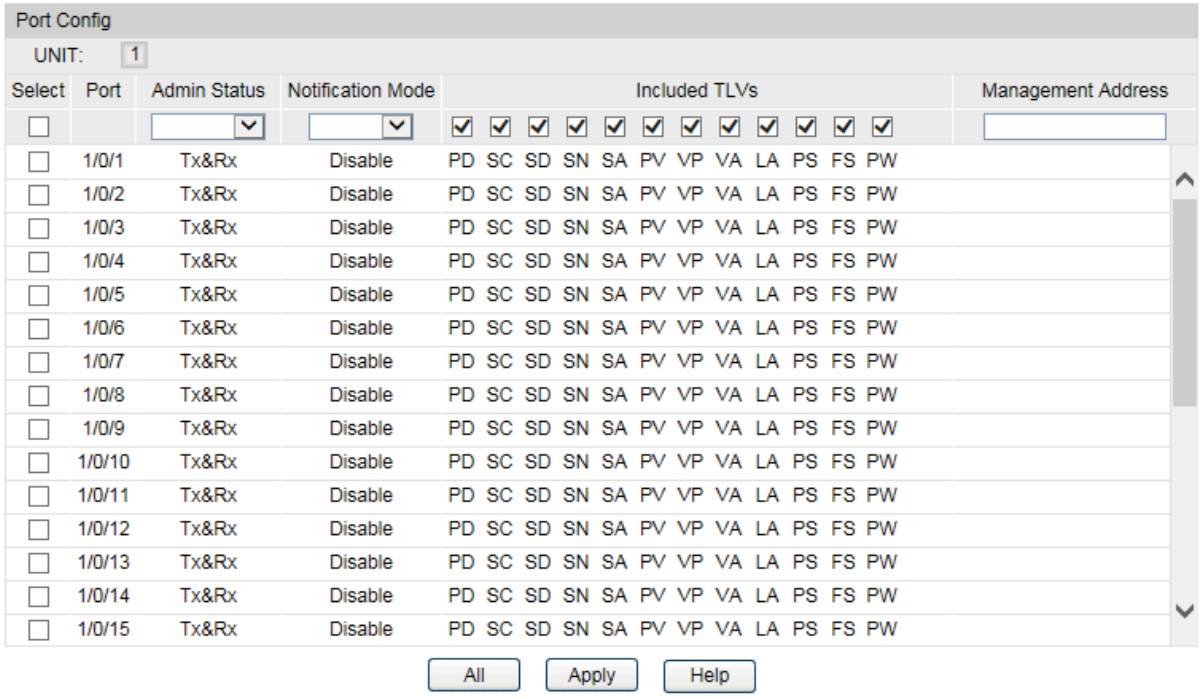
3) In the **Parameters Config** section, configure the LLDP parameters. Click **Apply**.

Transmit Interval	Enter the interval between successive LLDP packets that are periodically sent from the local device to its neighbors. The default is 30 seconds.
Hold Multiplier	Specify the amount of time the neighbor device should hold the received information before discarding it. The default is 4. TTL (Time to Live) = Hold Multiplier * Transmit Interval.
Transmit Delay	Specify the amount of time that the local device waits before sending another LLDP packet to its neighbors. When the local information changes, the local device will send LLDP packets to inform its neighbors. If frequent changes occur to the local device, LLDP packets will flood. After specifying a transmit delay time, the local device will wait for a delay time to send LLDP packets when changes occur to avoid frequent LLDP packet forwarding. The default is 2 seconds.
Reinit Delay	Specify the delay time that the local port waits before changing its Admin Status. When a local port's Admin Status changes, the local device will send Trap messages. After specifying a reinit delay time, the local device will wait for a delay time to send Trap messages to avoid frequent Trap forwarding. The default is 2 seconds.
Notification Interval	Enter the interval between successive Trap messages that are periodically sent from the local device to the NMS. The default is 5 seconds.
Fast Start Times	Specify the number of LLDP packets that the local port sends when its Admin Status changes from Disable (or Rx_Only) to Tx&RX (or Tx_Only). The default is 3. In this case, the local device will shorten the Transmit Interval of LLDP packets to 1 second to make it quickly discovered by its neighbors. After the specified number of LLDP packets are sent, the Transmit Interval will be restored to the specified value.

2.1.2 Port Config

Choose th menu **LLDP** > **Basic Config** > **Policy Config** to load the following page.

Figure 2-2 Port Config



Follow these steps to configure the LLDP feature for the interface.

1) Select the desired port and set its Admin Status and Notification Mode.

Admin Status	Set Admin Status for the port to deal with LLDP packets. Tx&Rx: The port will transmit LLDP packets and process the received LLDP packets. Rx_Only: The port will only process the received LLDP packets but not transmit LLDP packets. Tx_Only: The port will only transmit LLDP packets but not process the received LLDP packets. Disable: The port will not transmitLLDP packets or process the received LLDP packets.
Notification Mode	Select whether to enable SNMP on the port. If it is enabled, the local device will send Trap messages to inform the NMS when the local information changes.

2) Select the TLVs (Type/Length/Value) included in the LLDP packets according to your needs.

Included TLVs	Configure the TLVs included in the outgoing LLDP packets. TP-Link supports the following TLVs: PD: Used to advertise the port description defined by the IEEE 802 LAN station. SC: Used to advertise the supported functions and whether or not these functions are enabled. SD: Used to advertise the system's description including the full name and version identification of the system's hardware type, software operating system, and networking software. SN: Used to advertise the system name. SA: Used to advertise the local device's management address to make it possible to be managed by SNMP. PV: Used to advertise the 802.1Q VLAN ID of the port. VP: Used to advertise the protocol VLAN ID of the port. VA: Used to advertise the name of the VLAN which the port is in. LA: Used to advertise whether the link is capable of being aggregated, whether the link is currently in an aggregation, and the port ID when it is in an aggregation. PS: Used to advertise the port's attributes including the duplex and bit-rate capability of the sending IEEE 802.3 LAN node that is connected to the physical medium, the current duplex and bit-rate settings of the sending IEEE 802.3 LAN node and whether these settings are the result of auto-negotiation during link initiation or of manual set override action. FS: Used to advertise the maximum frame size capability of the implemented MAC and PHY. PW: Used to advertise the port's PoE (Power over Ethernet) support capabilities.

3) Optional. Configure the port's management address for identifying the devices.

2.2 Using the CLI

2.2.1 Global Config

Enable the LLDP feature on the switch and configure the LLDP parameters.

Step 1	**configure** Enter global configuration mode.
Step 2	**lldp** Enable the LLDP feature on the switch.

Step 3	**lldp forward_message** (Optional) Enable the switch to forward LLDP messages when LLDP function is disabled.
Step 4	**lldp hold-multiplier** (Optional) Specify the amount of time the neighbor device should hold the received information before discarding it. The default is 4. TTL (Time to Live) = Hold Multiplier * Transmit Interval.
Step 5	**lldp timer { tx-interval** *tx-interval* **| tx-delay** *tx-delay* **| reinit-delay** *reinit-delay* **| notify-interval** *notify-interval* **| fast-count** *fast-count* **}** (Optional) Configure the timers for LLDP packet forwarding. *tx-interval:* Enter the interval between successive LLDP packets that are periodically sent from the local device to its neighbors. *tx-delay:* Specify the amount of time that the local device waits before sending another LLDP packet to its neighbors. The default is 2 seconds. *reinit-delay:* Specify the amount of time that the local device waits before sending another LLDP packet to its neighbors. The default is 2 seconds. *notify-interval:* Enter the interval between successive Trap messages that are periodically sent from the local device to the NMS. The default is 5 seconds. *fast-count:* Specify the number of packets that the local port sends when its Admin Status changes. The default is 3.
Step 6	**show lldp** Display the LLDP information.
Step 7	**end** Return to Privileged EXEC Mode.
Step 8	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the following parameters, lldp timer=4, tx-interval=30 seconds, tx-delay=2 seconds, reinit-delay=3 seconds, notify-iInterval=5 seconds, fast-count=3.

Switch#configure

Switch(config)#lldp

Switch(config)#lldp hold-multiplier 4

Switch(config)#lldp timer tx-interval 30 **tx-delay** 2 **reinit-delay** 3 **notify-interval** 5 **fast-count** 3

Switch(config)#show lldp

LLDP Status: Enabled

LLDP Forward Message: Disabled

Tx Interval: 30 seconds

TTL Multiplier: 4

Tx Delay: 2 seconds

Initialization Delay: 2 seconds

Trap Notification Interval: 5 seconds

Fast-packet Count: 3

LLDP-MED Fast Start Repeat Count: 4

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Port Config

Select the desired port and set its Admin Status, Notification Mode and the TLVs included in the LLDP packets.

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Enter interface configuration mode.
Step 3	**lldp receive** (Optional) Set the mode for the port to receive LLDP packets. It is enabled by default.
Step 4	**lldp transmit** (Optional) Set the mode for the port to send LLDP packets. It is enabled by default.
Step 5	**lldp snmp-trap** (Optional) Enable the Notification Mode feature on the port. If it is enabled, the local device will send Trap messages to inform the SNMP server when local information changes. It is disabled by default.
Step 6	**lldp tlv-select** (Optional) Configure the TLVs included in the outgoing LLDP packets. By default, the outgoing LLDP packets include all TLVs.
Step 7	**lldp management-address {** *ip-address* **}** Optional. Specify the port's management IP address. The NMS uses management addresses to identify the devices.

Step 8	**show lldp interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}** Display LLDP configuration of the corresponding port.
Step 9	**end** Return to Privileged EXEC Mode.
Step 10	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the port 1/0/1. The port can receive and transmit LLDP packets, its notification mode is enabled and the outgoing LLDP packets include all TLVs.

Switch#configure

Switch(config)#lldp

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

Switch(config-if)#lldp receive

Switch(config-if)#lldp transmit

Switch(config-if)#lldp snmp-trap

Switch(config-if)#lldp tlv-select all

Switch(config-if)#show lldp interface gigabitEthernet 1/0/1

LLDP interface config:

gigabitEthernet 1/0/1:

Admin Status: TxRx

SNMP Trap: Enabled

TLV Status

--- ------

Port-Description Yes

System-Capability Yes

System-Description Yes

System-Name Yes

Management-Address Yes

Port-VLAN-ID Yes

Protocol-VLAN-ID Yes

VLAN-Name Yes

Link-Aggregation Yes

MAC-Physic Yes

Max-Frame-Size Yes

Power Yes

Switch(config-if)#end

Switch#copy running-config startup-config

3 LLDP-MED Configurations

With LLDP-MED configurations, you can:

1) Configure the LLDP-MED feature globally.
2) Enable and configure the LLDP-MED feature on the interface.

Configuration Guidelines

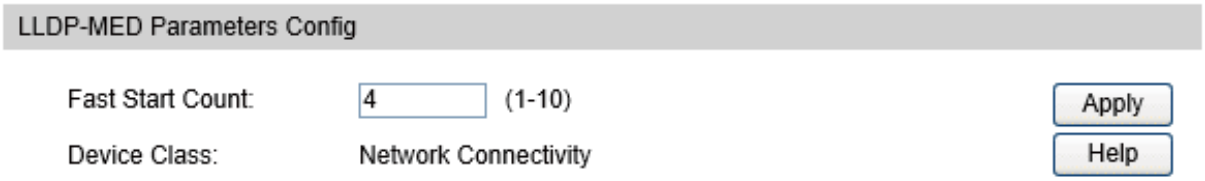
LLDP-MED is used together with Voice VLAN to implement VoIP access. Besides the configuration of LLDP-MED feature, you also need configure the Voice VLAN feature. Refer to *Configuring Voice VLAN* for detailed instructions.

3.1 Using the GUI

3.1.1 Global Config

Choose the **LLDP** > **LLDP-MED**> **Global Config** to load the following page.

Figure 3-1 LLDP-MED Parameters Config



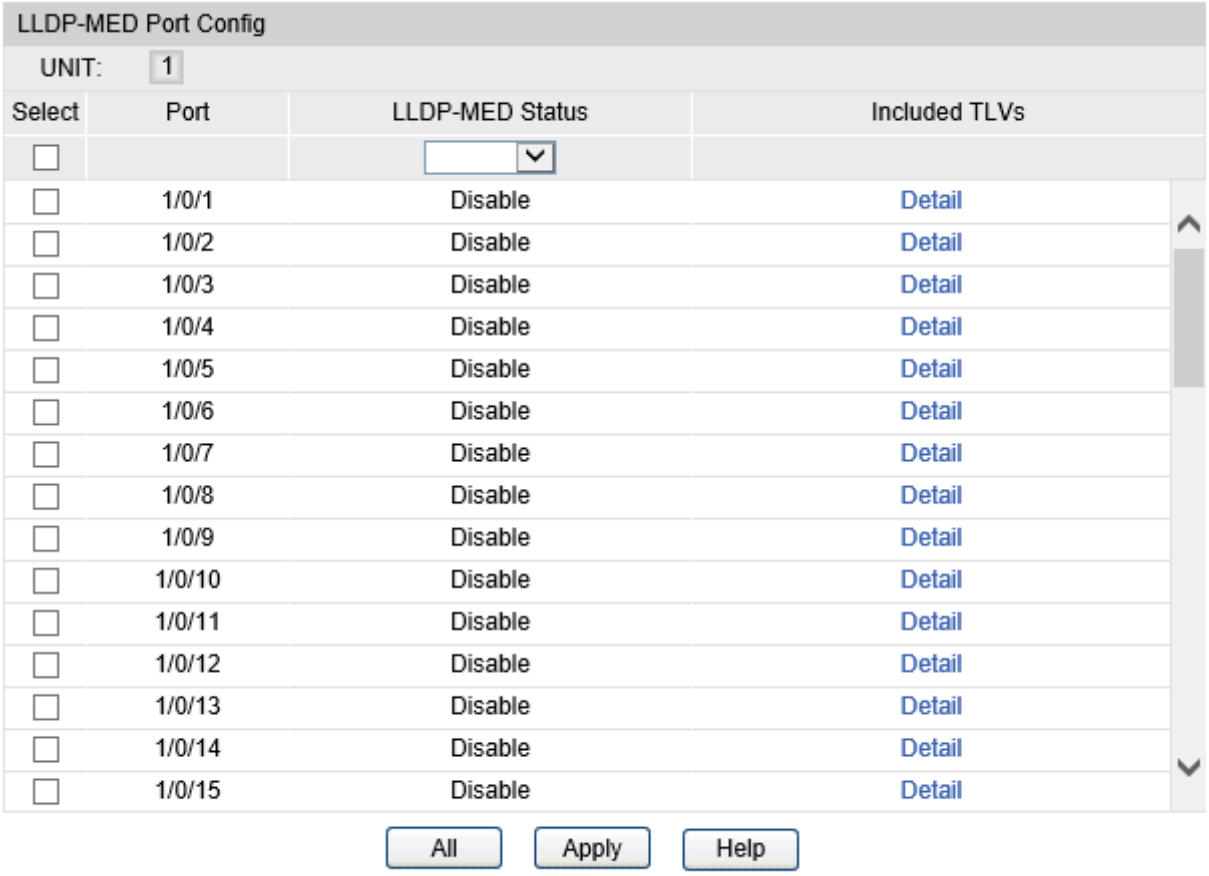
Configure the Fast Start Count and view the current device class. Click **Apply**.

Fast Start Count	Specify the number of successive LLDP-MED frames that the local device sends when fast start mechanism is activated. The default is 4. If the LLDP-MED status on the port is changed from Disable to Enable, the fast start mechanism will be activated, and the local device will send the specified number of LLDP packets carrying LLDP-MED information. After that, the Transmit Interval will be restored to the specified value.
Device Class	Display the current device class. LLDP-MED defines two device classes, Network Connectivity Device and Endpoint Device. The switch is a Network Connectivity device.

3.1.2 Port Config

Choose th menu **LLDP** > **LLDP-MED** > **Policy Config** to load the following page.

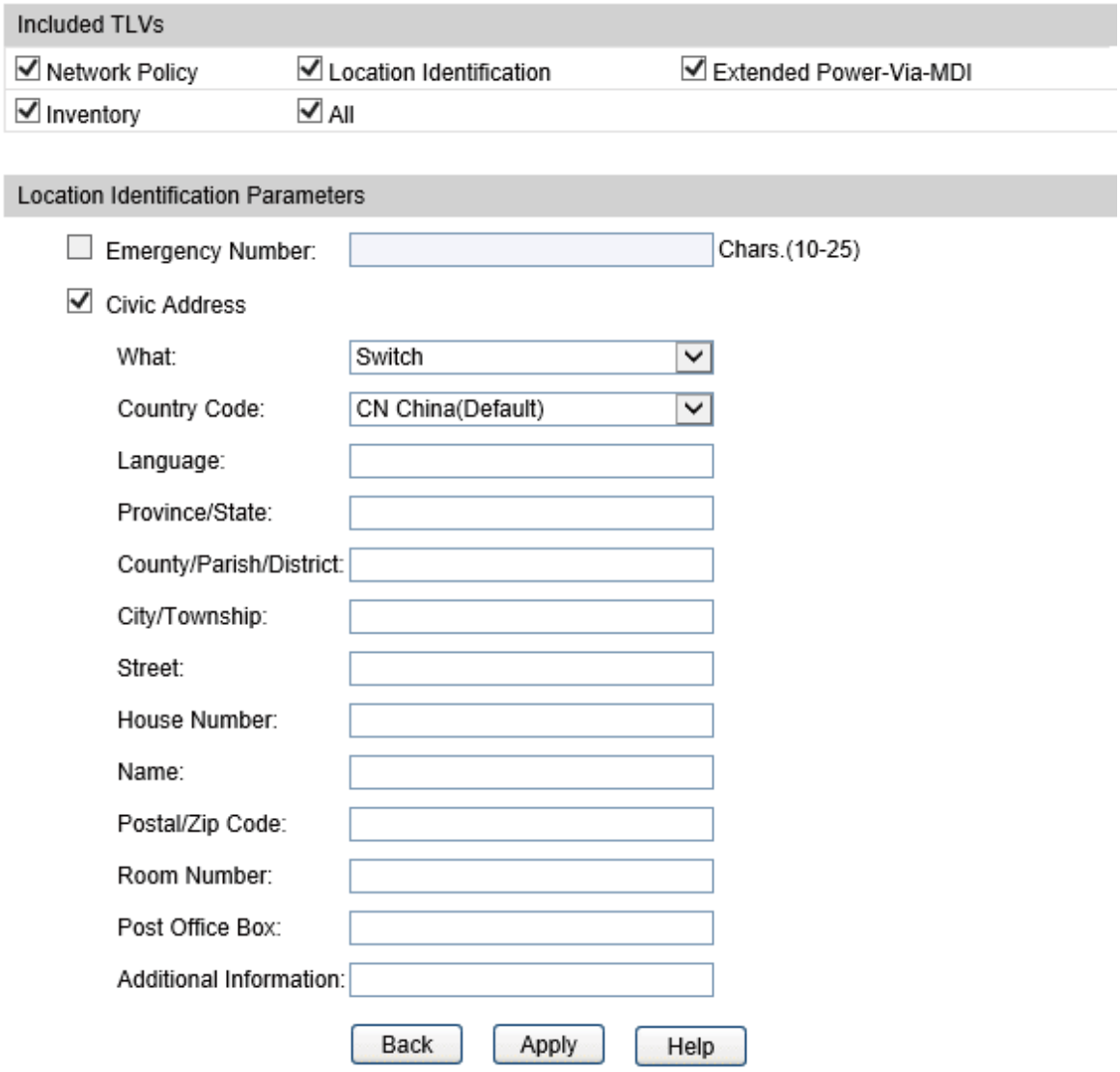
Figure 3-2 LLDP-MED Port Config



Follow these steps to enable LLDP-MED:

1) Select the desired port and enble LLDP-MED. Click **Apply**.
2) Click **Detail** to enter the following page. Configure the TLVs included in the outgoing LLDP packets. If **Location Identification** is selected, you need configure the Emergency Number or select Civic Address to configure the details. Click **Apply**.

Figure 3-3 LLDP-MED Port Config-Detail



Network Policy	Used to advertise VLAN configuration and the associated Layer 2 and Layer 3 attributes of the port to the Endpoint devices.
Location Identification	Used to assign the location identifier information to the Endpoint devices. If this option is selected, you can configure the emergency number or the detailed address of the Endpoint device in the Location Identification Parameters section.
Extended Power-Via-MDI	Used to advertise the detailed PoE information including power supply priority and supply status between LLDP-MED Endpoint devices and Network Connectivity devices.
Inventory	Used to advertise the inventory information. The Inventory TLV set contains seven basic Inventory management TLVs, that is, Hardware Revision TLV, Firmware Revision TLV, Software Revision TLV, Serial Number TLV, Manufacturer Name TLV, Model Name TLV and Asset ID TLV.
Emergency Number	Configure the emergency number to call CAMA or PSAP. The number should contain 10-25 characters.

Civic Address	Configure the address of the audio device in the IETF defined address format. What: Specify the role type of the local device, DHCP Server, Switch or LLDP-MED Endpoint. Country Code: Enter the country code defined by ISO 3166 , for example, CN, US. Language, Province/State etc.: Enter the regular details.

3.2 Using the CLI

3.2.1 Global Config

Step 1	**configure** Enter global configuration mode.
Step 2	**lldp** Enable the LLDP feature on the switch.
Step 3	**lldp med-fast-count** *count* (Optional) Specify the number of successive LLDP-MED frames that the local device sends when fast start mechanism is activated. When the fast start mechanism is activated, the local device will send the specified number of LLDP packets carrying LLDP-MED information. *count:* The valid value are from 1 to 10. The default is 4.
Step 4	**show lldp** Display the LLDP information.
Step 5	**end** Return to Privileged EXEC Mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure LLDP-MED fast count as 4:

Switch#configure

Switch(config)#lldp

Switch(config)#lldp med-fast-count 4

Switch(config)#show lldp

LLDP Status: Enabled

Tx Interval: 30 seconds

TTL Multiplier: 4

Tx Delay: 2 seconds

Initialization Delay: 2 seconds

Trap Notification Interval: 5 seconds

Fast-packet Count: 3

LLDP-MED Fast Start Repeat Count: 4

Switch(config)#end

Switch#copy running-config startup-config

3.2.2 Port Config

Select the desired port, enable LLDP-MED and select the TLVs (Type/Length/Value) included in the outgoing LLDP packets according to your needs.

Step 1	**configure** Enter global configuration mode.
Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Enter interface configuration mode.
Step 3	**lldp med-status** (Optional) Enable the LLDP-MED on the port. It is disabled by default.
Step 4	**lldp med-tlv-select { [inventory-management] [location] [network-policy] [power-management] [all] }** (Optional) Configure the LLDP-MED TLVs included in the outgoing LLDP packets. By default, the outgoing LLDP packets include all TLVs. If LLDP-MED Location TLV is selected, configure the parameters as follows: **lldp med-location {emergency-number** *identifier* **| civic-address [language** *language* **| province-state** *province-state* **| lci-county-name** *county* **| lci-city** *city* **| street** *street* **| house-number** *house-number* **| name** *name* **| postal-zipcode** *postal-zipcode* **| room-number** *room-number* **| post-office-box** *post-office-box* **| additional** *additional* **| country-code** *country-code* **| what { dhcp-server | endpoint | switch }] }** Configure the LLDP-MED Location TLV included in the outgoing LLDP packets. Used to assign the location identifier information to the Endpoint devices. *identifier:* Configure the emergency number to call CAMA or PSAP. The number should contain 10-25 characters. *language,province-state,county.etc:* Configure the address in the IETF defined address format.
Step 5	**show lldp interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}** Display LLDP configuration of the corresponding port.

Step 6	**end** Return to Privileged EXEC Mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable LLDP-MED on port 1/0/1, configure the LLDP-MED TLVs included in the outgoing LLDP packets.

Switch(config)#lldp

Switch(config)#lldp med-fast-count 4

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

Switch(config-if)#lldp med-status

Switch(config-if)#lldp med-tlv-select all

Switch(config-if)#show lldp interface gigabitEthernet 1/0/1

LLDP interface config:

gigabitEthernet 1/0/1:

Admin Status: TxRx

SNMP Trap: Enabled

TLV Status

--- ------

Port-Description Yes

System-Capability Yes

System-Description Yes

System-Name Yes

Management-Address Yes

Port-VLAN-ID Yes

Protocol-VLAN-ID Yes

VLAN-Name Yes

Link-Aggregation Yes

MAC-Physic Yes

Max-Frame-Size Yes

Power Yes

LLDP-MED Status: Enabled

TLV Status

--- ------

Network Policy Yes

Location Identification Yes

Extended Power Via MDI Yes

Inventory Management Yes

Switch(config)#end

Switch#copy running-config startup-config

4 Viewing LLDP Settings

This chapter introduces how to view the LLDP settings on the local device.

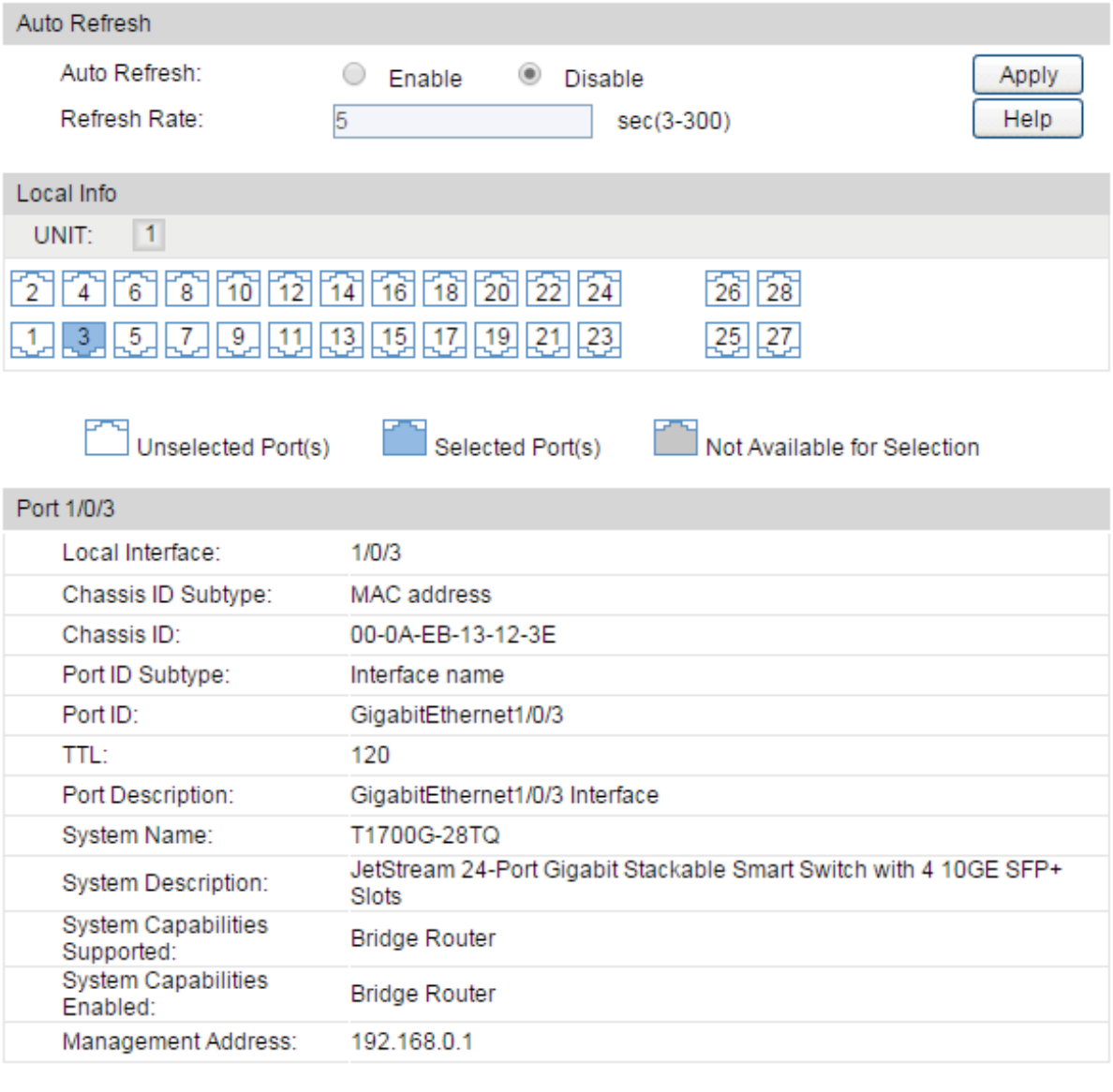
4.1 Using GUI

4.1.1 Viewing LLDP Device Info

- Viewing the Local Info

Choose the menu **LLDP** > **Device Info** > **Local Info** to load the following page.

Figure 4-1 Local Info



Follow these steps to view the local information:

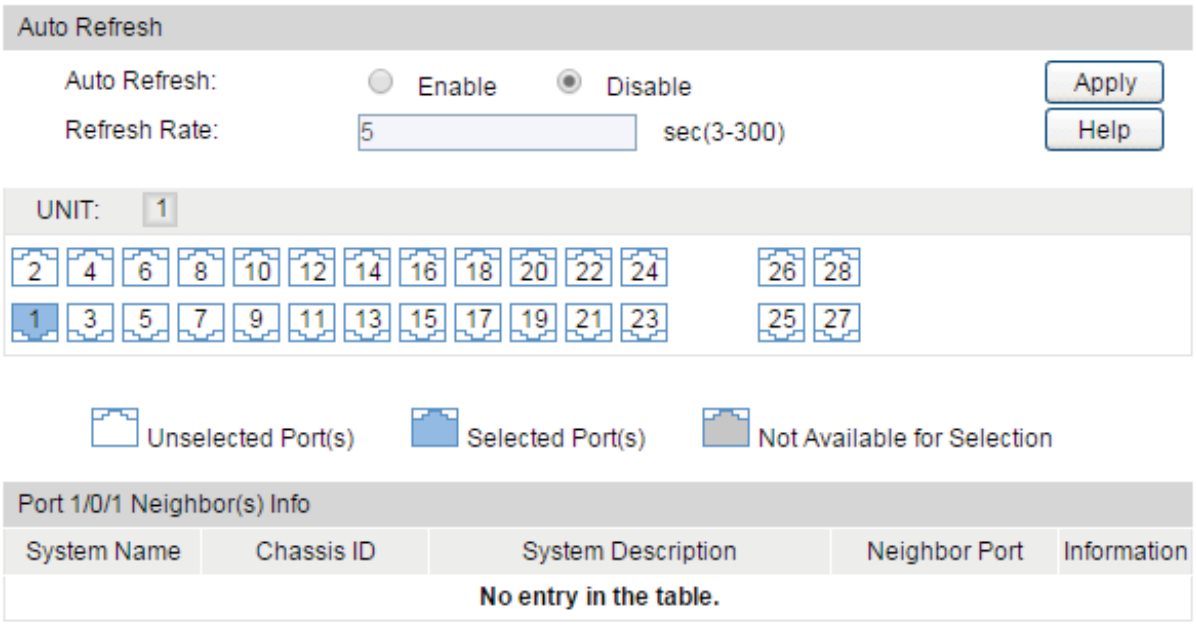
1) In the **Auto Refresh** section, enable the Auto Refresh feature and set the Refresh Rate according to your needs. Click **Apply**.
2) In the **Local Info** section, select the desired port and view its associated local device information.

Local Interface	Displays the local port ID.
Chassis ID Subtype	Displays the Chassis ID type.
Chassis ID	Displays the value of the Chassis ID.
Port ID Subtype	Displays the Port ID type.
Port ID	Displays the value of the Port ID.
TTL	Specify the amount of time the neighbor device should hold the received information before discarding it.
Port Description	Displays the description of the local port.
System Name	Displays the system name of the local device.
System Description	Displays the system description of the local device.
System Capabilities Supported	Displays the supported capabilities of the local system.
System Capabilities Enabled	Displays the primary functions of the local device.
Management Address	Displays the management address of the local device.

Viewing the Neighbor Info

Choose the menu **LLDP** > **Device Info** > **Neighbor Info** to load the following page.

Figure 4-2 Neighbor Info



Follow these steps to view the neighbor information:

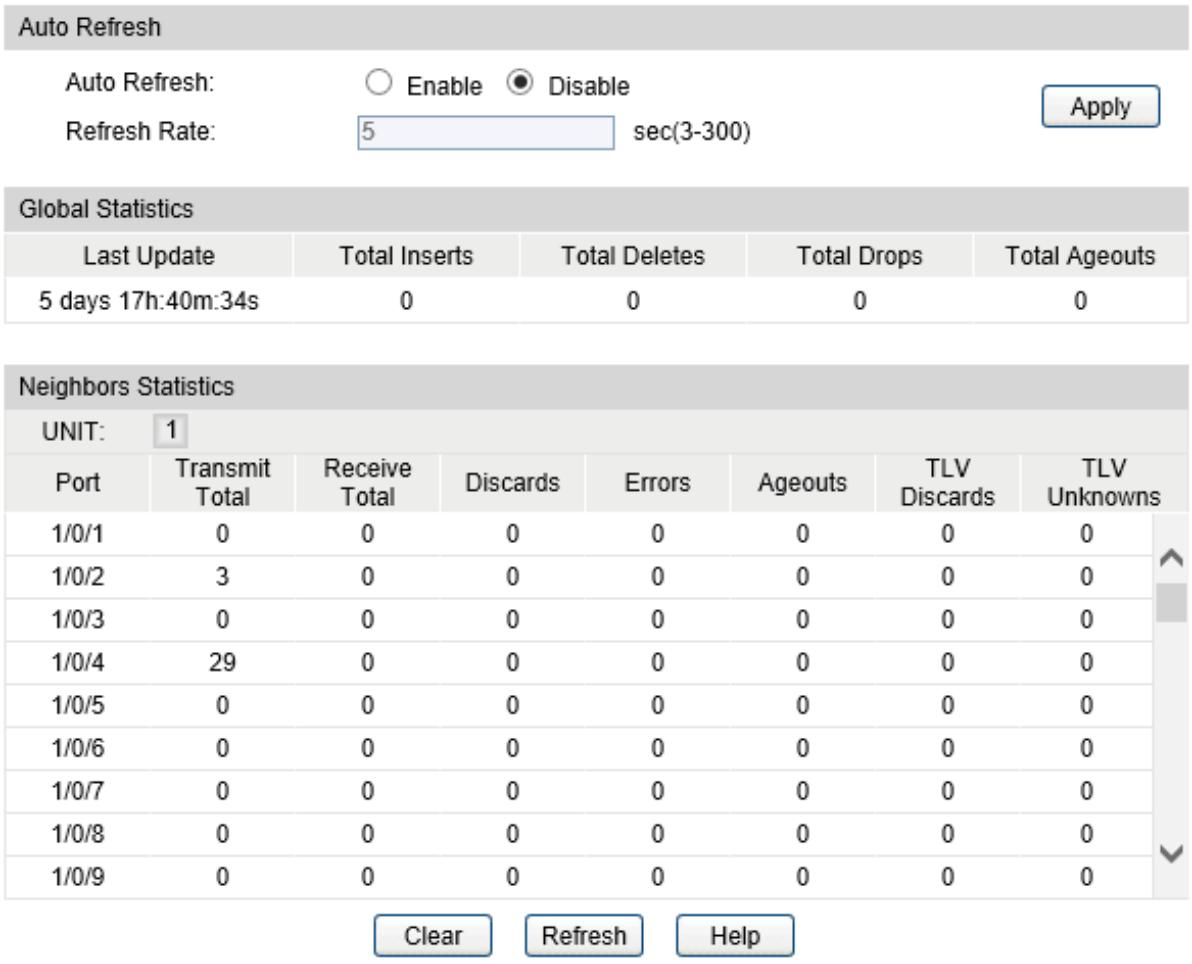
1) In the **Auto Refresh** section, enable the Auto Refresh feature and set the Refresh Rate according to your needs. Click **Apply**.
2) In the **Local Info** section, select the desired port and view its associated neighbor device information.

System Name	Displays the system name of the neighbor device.
Chassis ID	Displays the Chassis ID of the neighbor device.
System Description	Displays the system description of the neighbor device.
Neighbor Port	Displays the port ID of the neighbor device which is connected to the local port.
Information	Click to view the details of the neighbor device.

4.1.2 Viewing LLDP Statistics

Choose the menu **LLDP** > **Device Statistics** > **Statistics Info** to load the following page.

Figure 4-3 Static Info



Follow these steps to view LLDP statistics:

1) In the **Auto Refresh** section, enable the Auto Refresh feature and set the Refresh Rate according to your needs. Click **Apply**.

2) In the **Global Statistics** section, view the global statistics of the local device.

Last Update	Displays the time when the statistics updated.
Total Inserts	Displays the latest number of neighbors the local device has created.
Total Deletes	Displays the latest number of neighbors the local device has removed.
Total Drops	Displays the latest number of neighbors the local device has discarded.
Total Ageouts	Displays the latest number of neighbors that have aged out on the local device.

3) In the **Neighbors Statistics** section, view the statistics of the corresponding port.

Transmit Total	Displays the total number of the LLDP packets sent via the port.
Receive Total	Displays the total number of the LLDP packets received via the port.
Discards	Displays the total number of the LLDP packets discarded by the port.
Errors	Displays the total number of the error LLDP packets received via the port.
Ageouts	Displays the number of the aged out neighbors that are connected to the port.
TLV Discards	Displays the total number of the TLVs discarded by the port when receiving LLDP packets.
TLV Unknowns	Displays the total number of the unknown TLVs included in the received LLDP packets.

4.2 Using CLI

Viewing the Local Info

show lldp local-information interface { fastEthernet *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}**

View the LLDP details of a specific port or all the ports on the local device.

Viewing the Neighbor Info

show lldp neighbor-information interface { fastEthernet *port* **| gigabitEthernet** *port* **| ten gigabitEthernet** *port* **}**

Display the information of the neighbor device which is connected to the port.

Viewing LLDP Statistics

show lldp traffic interface { fastEthernet *port* **| gigabitEthernet** *port* **| tengigabitEthernet** *port* **}**

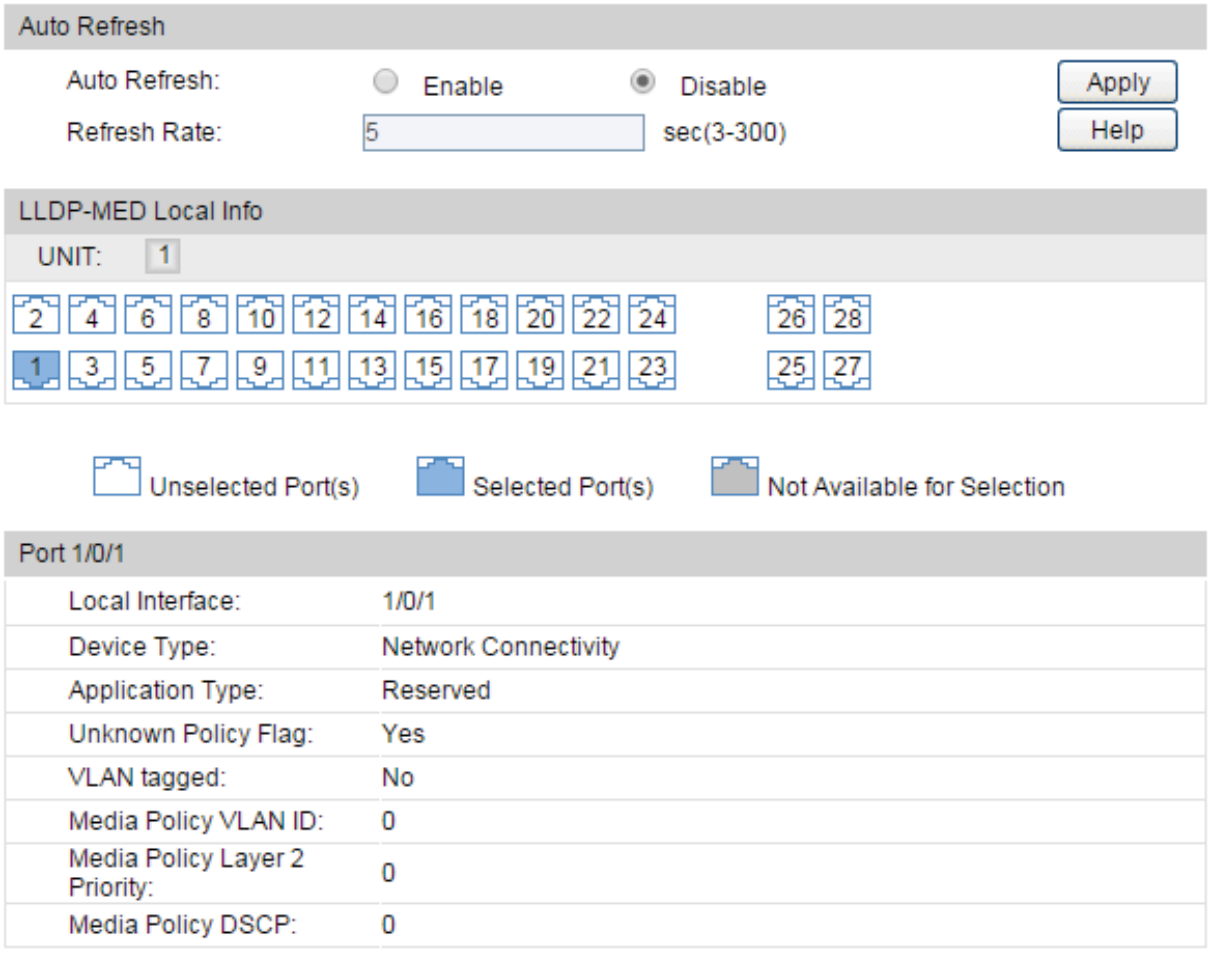
View the statistics of the corresponding port on the local device.

5 Viewing LLDP-MED Settings

5.1 Using GUI

- Viewing the Local Info

Figure 5-1 LLDP-MED Local Info



Follow these steps to view LLDP-MED local information:

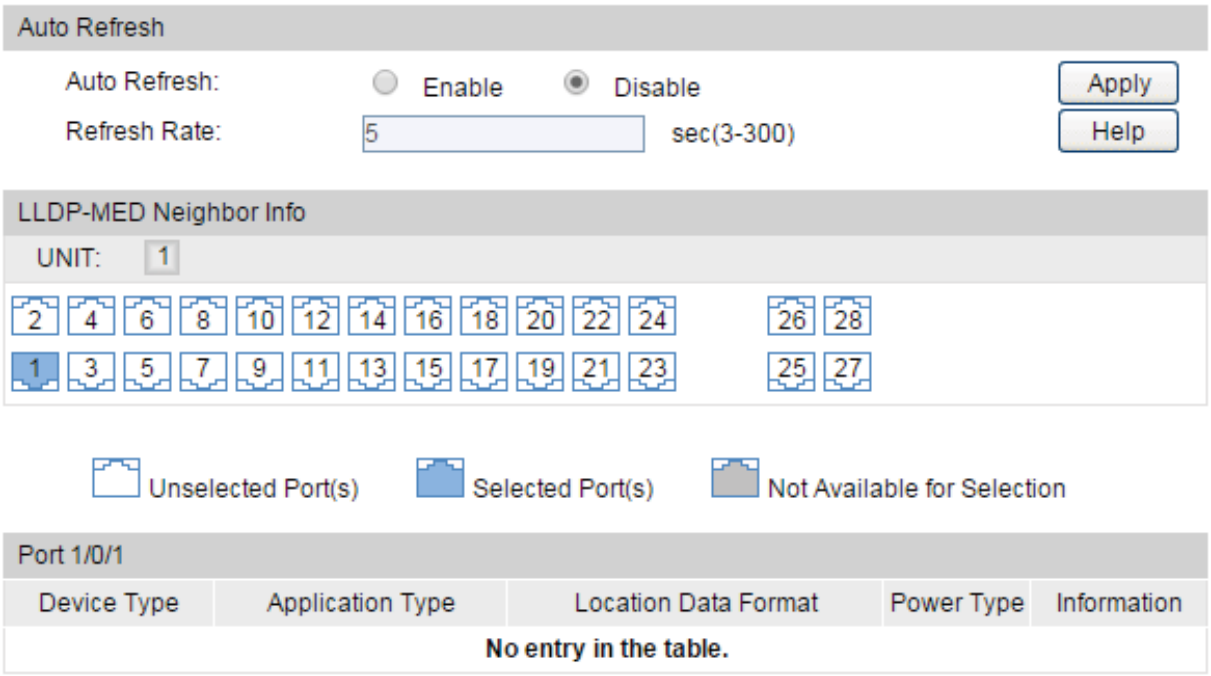
1) In the **Auto Refresh** section, enable the Auto Refresh feature and set the Refresh Rate according to your needs. Click **Apply**.
2) In the **LLDP-MED Local Info** section, select the desired port and view the LLDP-MED settings.

Local Interface	Displays the local port ID.
Device Type	Displays the local device type defined by LLDP-MED.LLDP-MED.

Application Type	Displays the supported applications of the local device.
Unknown Policy Flag	Displays the unknown location settings included in the network policy TLV.
VLAN tagged	Displays the VLAN Tag type of the applications, tagged or untagged.
Media Policy VLAN ID	Displays the 802.1Q VLAN ID of the port.
Media Policy Layer 2 Priority	Displays the Layer 2 priority used in the specific application.
Media Policy DSCP	Displays the DSCP value used in the specific application.

Viewing the Neighbor Info

Figure 5-2 LLDP-MED Neighbor Info



Follow these steps to view LLDP-MED neighgbor information:

1) In the **Auto Refresh** section, enable the Auto Refresh feature and set the Refresh Rate according to your needs. Click **Apply**.
2) In the **LLDP-MED Neighbor Info** section, select the desired port and view the LLDP-MED settings.

Device Type	Displays the LLDP-MED device type of the neighbor device.

Application Type	Displays the application type of the neighbor device.
Location Data Format	Displays the location type of the neighbor device.
Power Type	Displays the power type of the neighbor device.
Information	View more LLDP-MED details of the neighbor device.

5.2 Using CLI

Viewing the Local Info

show lldp local-information interface { fastEthernet *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}**

View the LLDP details of a specific port or all the ports on the local device.

Viewing the Neighbor Info

show lldp neighbor-information interface { fastEthernet *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}**

Display the information of the neighbor device which is connected to the port.

Viewing LLDP Statistics

show lldp traffic interface { fastEthernet *port* **| gigabitEthernet** *port* **| tengigabitEthernet** *port* **}**

View the statistics of the corresponding port.

6 Configuration Example

6.1 Example for Configuring LLDP

6.1.1 Network Requirements

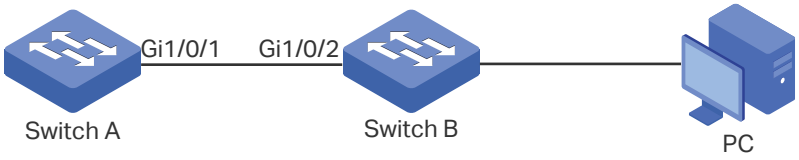
The network administrator needs view the information of the devices in the company network to know about the link situation and network topology so that he can troubleshoot the potential network faults in advance.

6.1.2 Network Topology

Exampled with the following situation:

Port Gi1/0/1 on Switch A is directly connected to port Gi1/0/2 on Switch B. Switch B is directly connected to the PC. The administrator can view the device information using the NMS.

Figure 6-1 LLDP Network Topology



6.1.3 Configuration Scheme

LLDP can meet the network requirements. Enable the LLDP feature globally on Switch A and Switch B. Configure the related LLDP parameters on the corresponding ports.

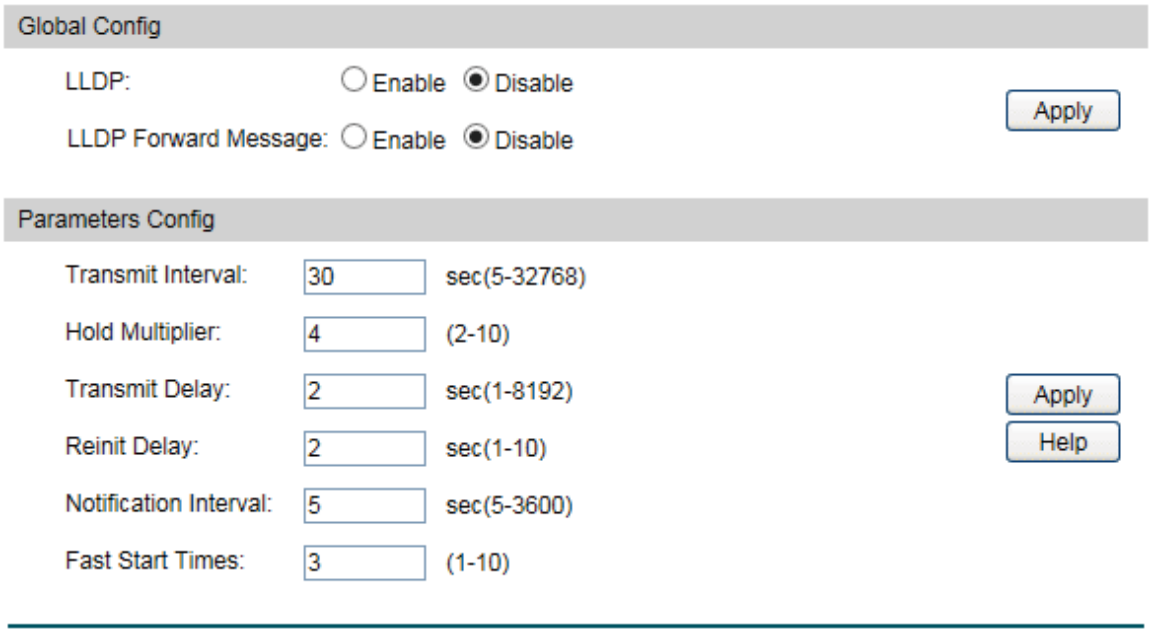
Configuring Switch A and Switch B:

The configurations of Switch A and Switch B are similar. The following introductions take Switch A as an example. Demonstrated with T2600G-28TS, this chapter provides configuration procedures in two ways: using the GUI and using the CLI.

6.1.4 Using the GUI

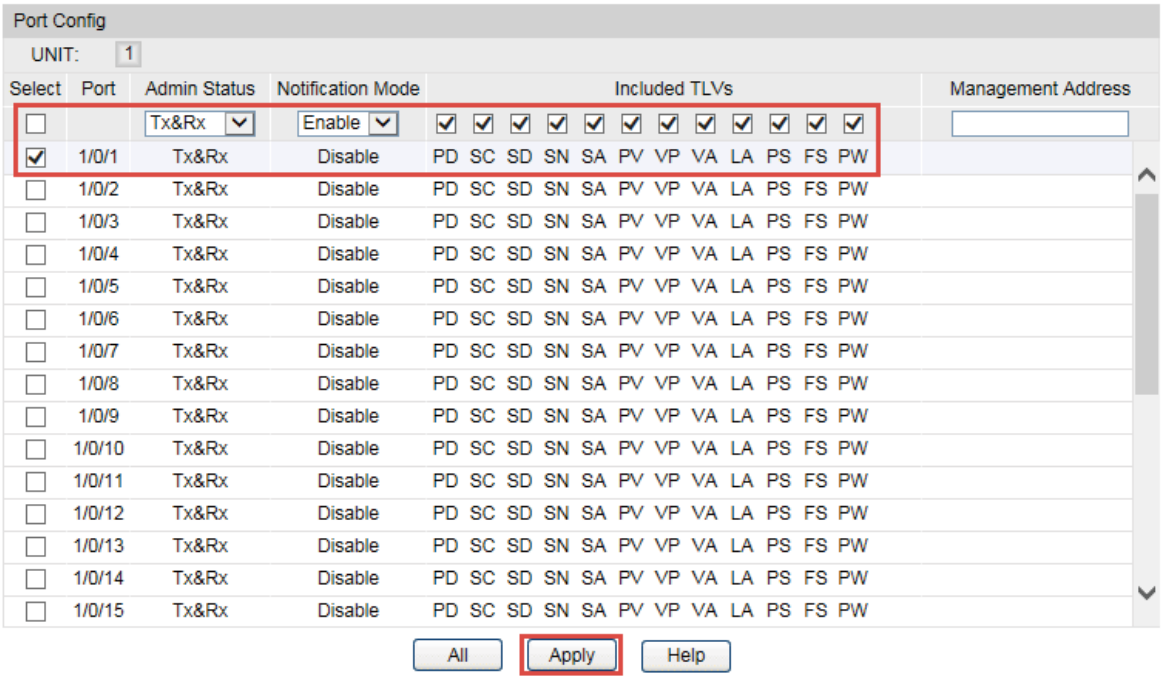
1) Choose the menu **LLDP** > **Basic Config** > **Global Config** to load the following page. Enable LLDP globally and configure the related parameters. Here we take the default settings as an example.

Figure 6-2 LLDP Global Config



2) Choose the menu **LLDP** > **Basic Config** > **Port Config** to load the following page. Set the Admin Status of port Gi1/0/1 to Tx&Rx, enable Notification Mode and configure all the TLVs included in the outgoing LLDP packets.

Figure 6-3 LLDP Port Config



6.1.5 Using CLI

1) Enable LLDP globally and configure the corresponding parameters.

```
Switch_A#configure
Switch_A(config)#lldp
```

Switch_A(config)#lldp hold-multiplier 4

Switch_A(config)#lldp timer tx-interval 30 tx-delay 2 reinit-delay 3 notify-interval 5 fast-count 3

2) Set the Admin Status of port Gi1/0/1 to Tx&Rx, enable Notification Mode and configure all the TLVs included in the outgoing LLDP packets.

Switch_A#configure

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

Switch_A(config-if)#lldp receive

Switch_A(config-if)#lldp transmit

Switch_A(config-if)#lldp snmp-trap

Switch_A(config-if)#lldp tlv-select all

Switch_A(config-if)#end

Switch_A#copy running-config startup-config

Verify the Configurations

View LLDP settings globally

Switch_A#show lldp

LLDP Status:	Enabled
LLDP Forward Message:	Disabled
Tx Interval:	30 seconds
TTL Multiplier:	4
Tx Delay:	2 seconds
Initialization Delay:	2 seconds
Trap Notification Interval:	5 seconds
Fast-packet Count:	3
LLDP-MED Fast Start Repeat Count:	4

View LLDP settings on each port

Switch_A#show lldp interface gigabitEthernet 1/0/1

LLDP interface config:

gigabitEthernet 1/0/1:

Admin Status:	TxRx
SNMP Trap:	Enabled

TLV	Status
Port-Description	Yes
System-Capability	Yes
System-Description	Yes
System-Name	Yes
Management-Address	Yes
Port-VLAN-ID	Yes
Protocol-VLAN-ID	Yes
VLAN-Name	Yes
Link-Aggregation	Yes
MAC-Physic	Yes
Max-Frame-Size	Yes
Power	Yes

LLDP-MED Status: Disabled

TLV	Status
Network Policy	Yes
Location Identification	Yes
Extended Power Via MDI	Yes
Inventory Management	Yes

View the Local Info

Switch_A#show lldp local-information interface gigabitEthernet 1/0/1

LLDP local Information:

gigabitEthernet 1/0/1:

Chassis type:	MAC address
Chassis ID:	00:0A:EB:13:23:97
Port ID type:	Interface name
Port ID:	GigabitEthernet1/0/1
Port description:	GigabitEthernet1/0/1 Interface

TTL: 120

System name: T2600G-28TS

System description: JetStream 24-Port Gigabit L2 Managed Switch with 4 SFP Slots

System capabilities supported: Bridge Router

System capabilities enabled: Bridge Router

Management address type: ipv4

Management address: 192.168.0.226

Management address interface type: IfIndex

Management address interface ID: 1

Management address OID: 0

Port VLAN ID(PVID): 1

Port and protocol VLAN ID(PPVID): 0

Port and protocol VLAN supported: Yes

Port and protocol VLAN enabled: No

VLAN name of VLAN 1: System-VLAN

Protocol identity:

Auto-negotiation supported: Yes

Auto-negotiation enabled: Yes

OperMau: speed(1000)/duplex(Full)

Link aggregation supported: Yes

Link aggregation enabled: No

Aggregation port ID: 0

Power port class: PD

PSE power supported: No

PSE power enabled: No

PSE pairs control ability: No

Maximum frame size: 1518

LLDP-MED Capabilities: Capabilities

Network Policy

Location Identification

Inventory

Device Type: Network Connectivity

Application type: Reserved

Unknown policy: Yes

Tagged: No

VLAN ID: 0

Layer 2 Priority: 0

DSCP: 0

Location Data Format: Civic Address LCI

- What: Switch

- Country Code: CN

Hardware Revision: T2600G-28TS 2.0

Firmware Revision: Reserved

Software Revision: 2.0.0 Build 20160905 Rel.74744(s)

Serial Number: Reserved

Manufacturer Name: TP-Link

Model Name: T2600G-28TS 2.0

Asset ID: unknown

View the Neighbor Info

Switch_A#show lldp neighbor-information interface gigabitEthernet 1/0/1

LLDP Neighbor Information:

gigabitEthernet 1/0/1:

Neighbor index 1:

Chassis type: MAC address

Chassis ID: 00:0A:EB:13:18:2D

Port ID type: Interface name

Port ID: GigabitEthernet1/0/2

Port description: GigabitEthernet1/0/2 Interface

TTL: 120

System name:	T1600G-52PS
System description:	JetStream 48-Port Gigabit Smart PoE Switch with 4 SFP Slots
System capabilities supported:	Bridge Router
System capabilities enabled:	Bridge Router
Management address type:	ipv4
Management address:	192.168.0.1
Management address interface type:	IfIndex
Management address interface ID:	1
Management address OID:	0
Port VLAN ID(PVID):	1
Port and protocol VLAN ID(PPVID):	0
Port and protocol VLAN supported:	Yes
Port and protocol VLAN enabled:	No
VLAN name of VLAN 1:	System-VLAN
Protocol identity:	
Auto-negotiation supported:	Yes
Auto-negotiation enabled:	Yes
OperMau:	speed(1000)/duplex(Full)
Link aggregation supported:	Yes
Link aggregation enabled:	No
Aggregation port ID:	0
Power port class:	PSE
PSE power supported:	Yes
PSE power enabled:	Yes
PSE pairs control ability:	No

6.2 Example for Configuring LLDP-MED

6.2.1 Network Requirements

The marketing department needs establish the voice conversation with the field office. They want to install IP phones in their office and meet the following requirements:

- Save the switch ports for more IP phones due to the limited number of the ports on the switch in the office;
- The voice traffic is transmitted in a separate VLAN to guarantee the voice quality.
- The IP phones can finish the Voice VLAN configuration automatically to minimize the configuration effort.

6.2.2 Configuration Scheme

To save the limited ports on the switch, connect the IP phone and the PC in a series, then the IP phone and PC can share the same port on the switch.

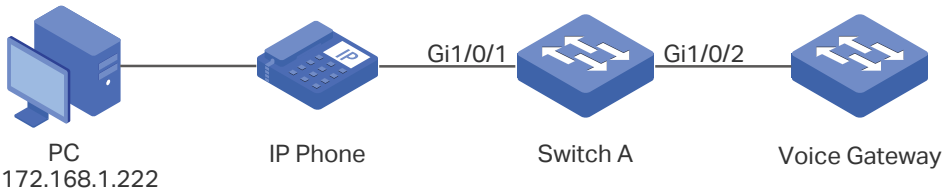
Configure LLDP-MED to work together with Voice VLAN to guarantee the voice quality and reduce the configuration effort. Configure the port which the IP phone is connected with, then IP phone can automatically finish its Voice VLAN configuration using the received LLDP-MED packets and send tagged voice packets to the switch. Voice packets will be transmitted in the Voice VLAN while other traffic will be transmitted in the default VLAN. Please note that the PVID of the port which the IP phone is connected with cannot be the same as the VLAN ID of the Voice VLAN. Refer to *Configuring Voice VLAN* for detailed instructions.

6.2.3 Network Topology

Exampled with the configuration of one IP phone:

One end of the IP phone is connected to the PC, the other end is connect to port Gi1/0/1 on the switch. Port Gi1/0/2 on the switch is connect to the voice gateway.

Figure 6-4 LLDP-MED Network Topology

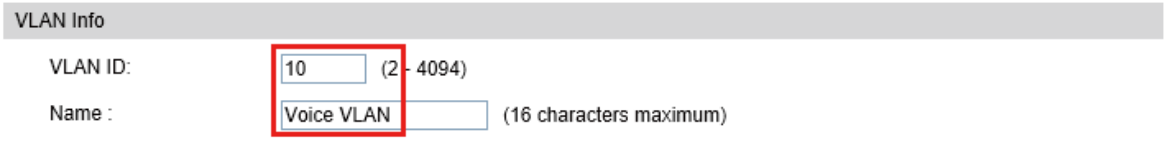


To ensure the voice traffic can be preferentially treated, configure the corresponding settings on each device in the link. Demonstrated with T2600G-28TS, this section provides configuration procedures in two ways: using the GUI and using the CLI.

6.2.4 Using the GUI

1) Choose the menu **VLAN** > **802.1Q VLAN** > **VLAN Config** to load the following page. Create VLAN 10, and name it as Voice VLAN.

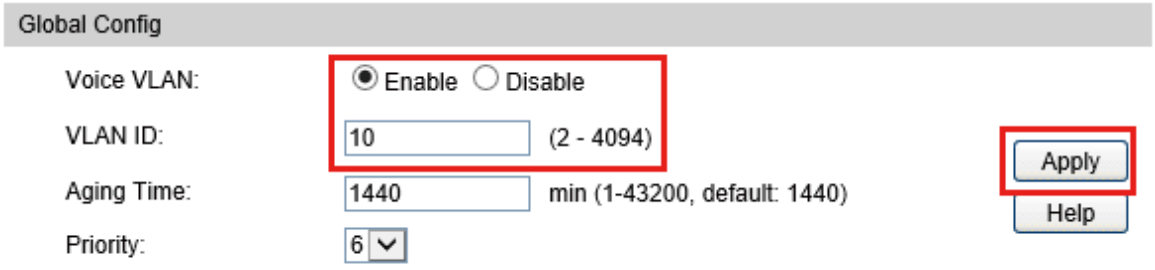
Figure 6-5 Creating a VLAN



2) Enable and configure the Voice VLAN.

Choose the menu **QoS** > **Voice VLAN** > **Global Config**, enable Voice VLAN and set the VLAN ID to 10.

Figure 6-6 Configuring Voice VLAN Globally



Choose the menu **QoS** > **Voice VLAN** > **Port Config**, set the Voice VLAN mode on Gi1/0/1 and Gi1/0/2 as Auto and Manual respectively.

Figure 6-7 Configuring Voice VLAN Mode on Port 1/0/1

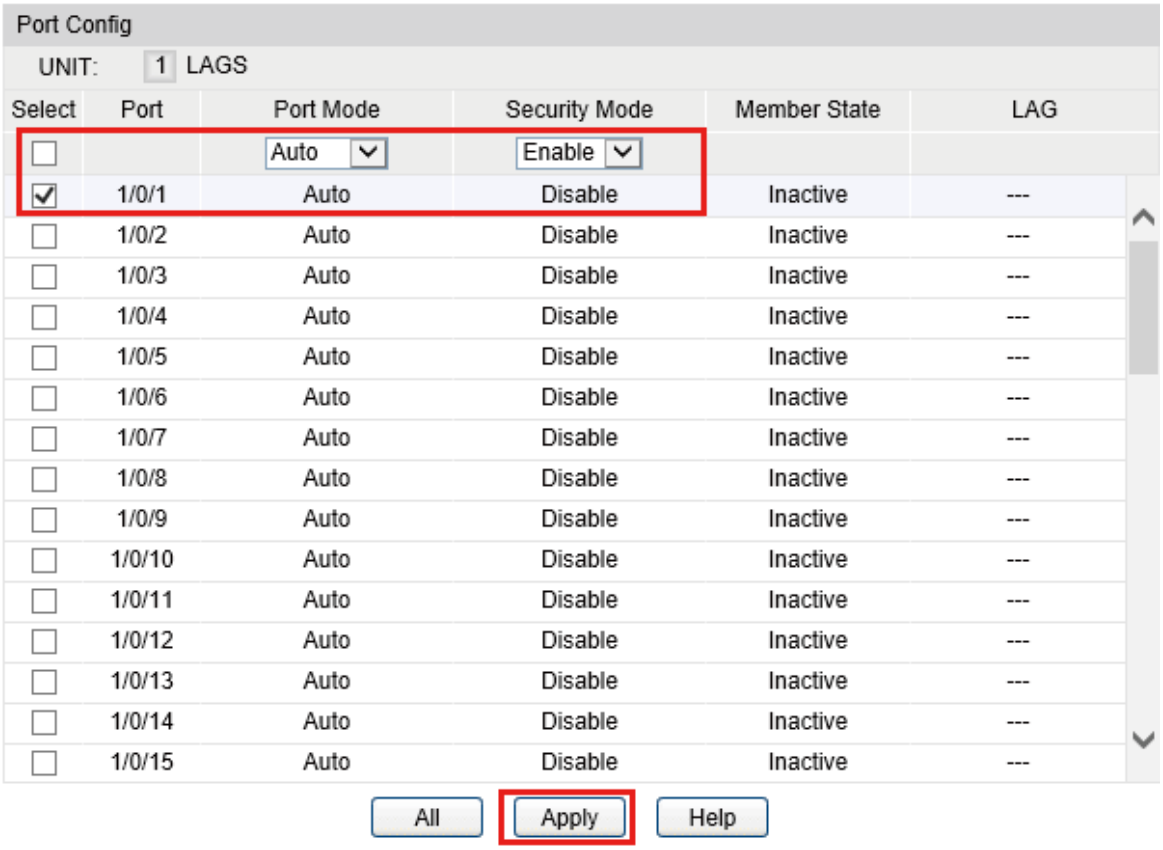
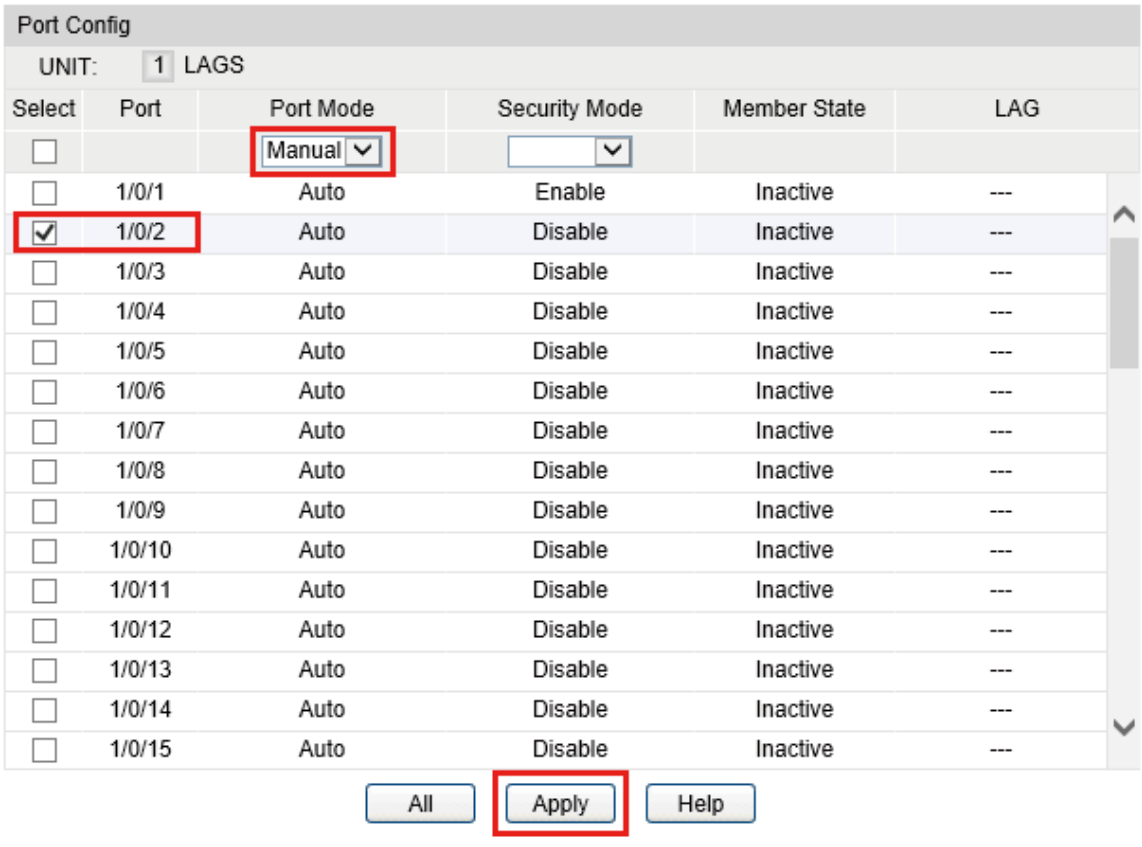
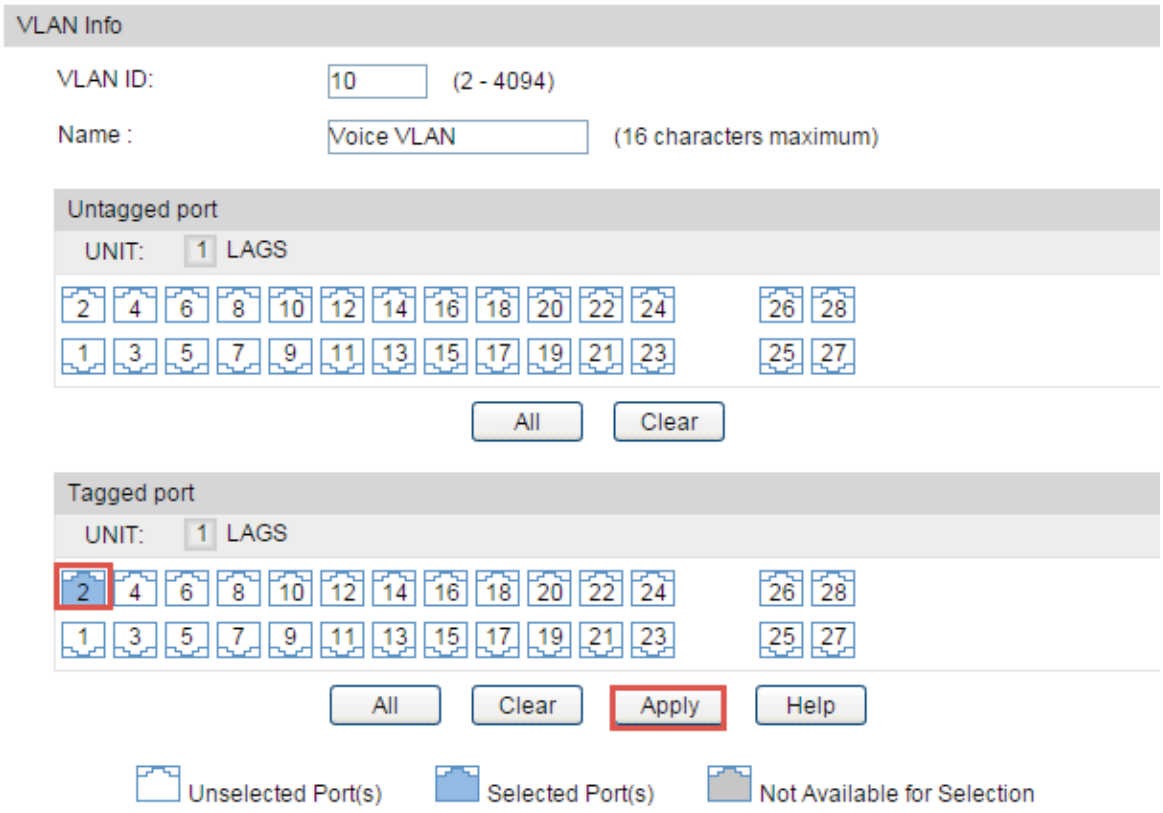


Figure 6-8 Configuring Voice VLAN Mode on Port 1/0/2



Choose the menu **VLAN** > **802.1Q VLAN** > **VLAN Config** to load the following page. Add port 1/0/2 to the Voice VLAN.

Figure 6-9 Adding Port 1/0/2 to the Voice VLAN



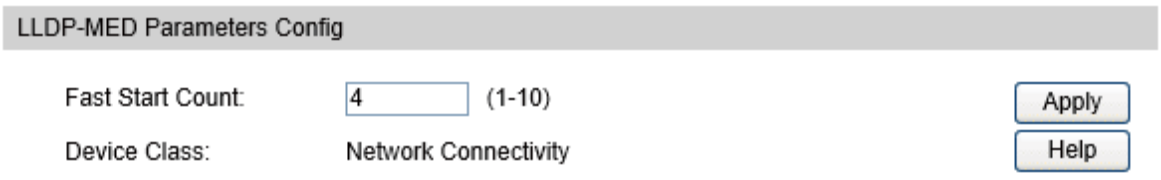
3) Choose the **LLDP** > **Basic Config** > **Global Config** to load the following page and enable LLDP globally.

Figure 6-10 LLDP Global Config



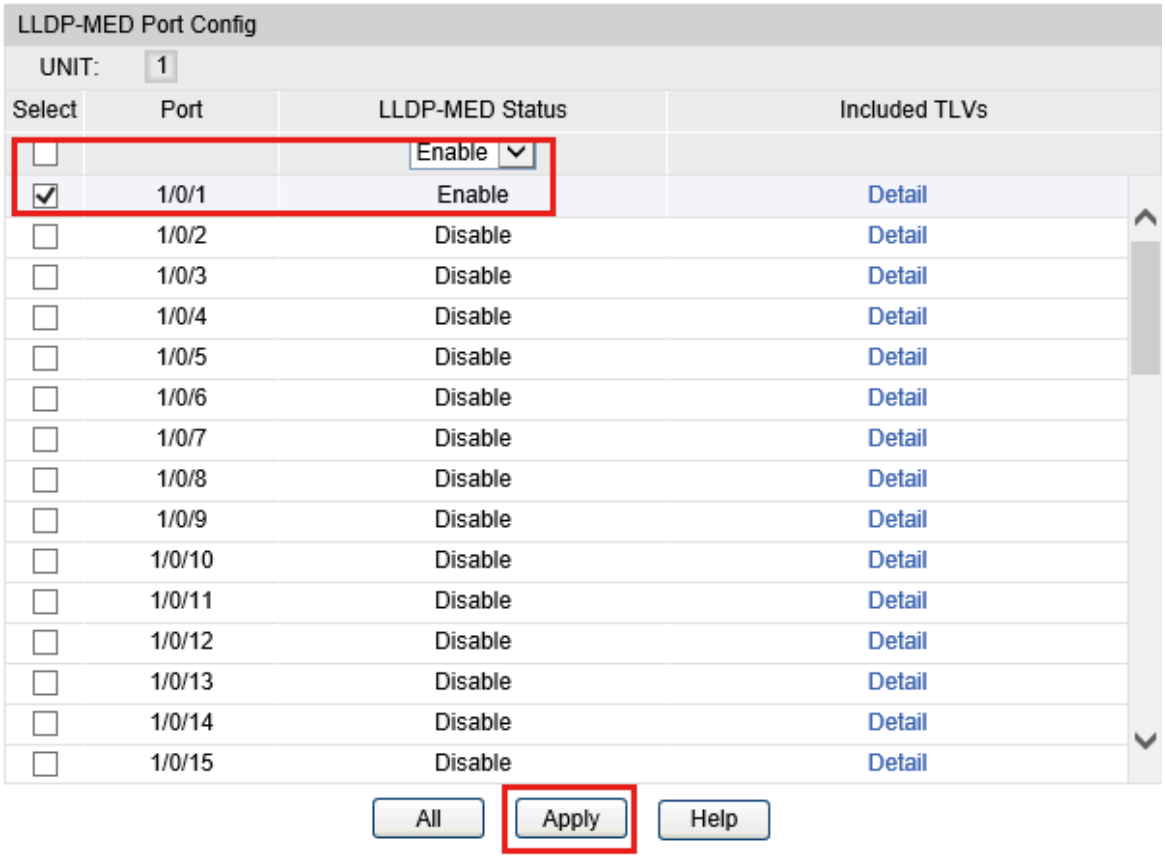
4) Choose the **LLDP** > **LLDP-MED** > **Global Config** to load the following page and configure the fast start count. The default is 4.

Figure 6-11 LLDP-MED Global Config



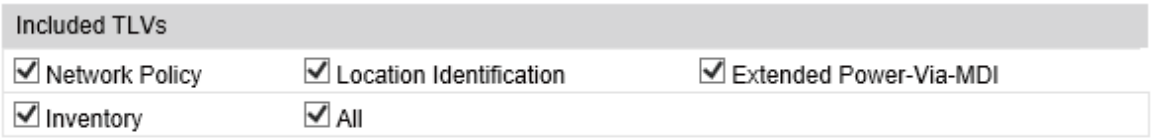
5) Choose th menu **LLDP** > **LLDP-MED** > **Policy Config** to load the following page. Select port 1/0/1 and enable LLDP-MED.

Figure 6-12 LLDP-MED Port Config



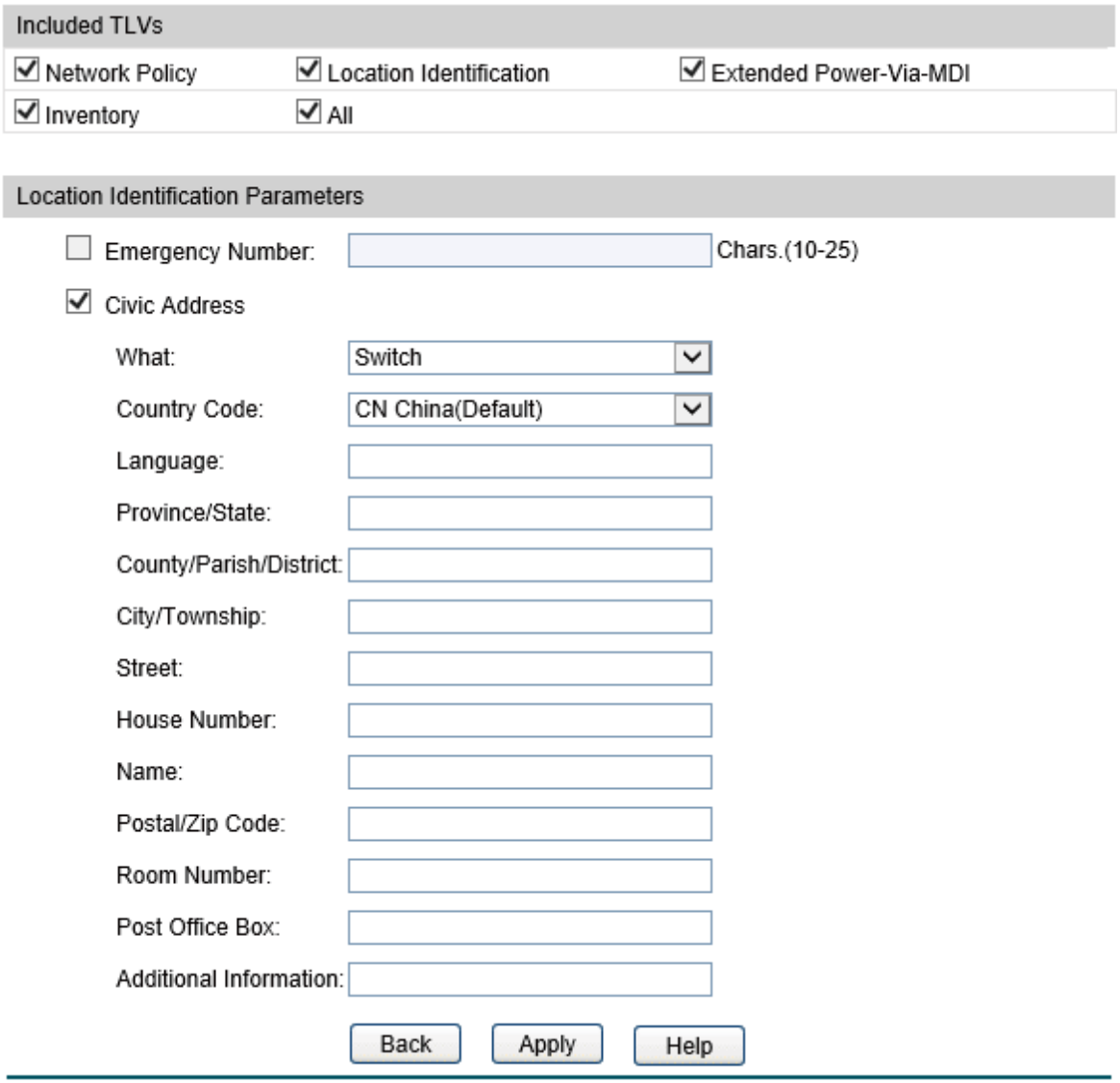
Click **Detail** in the Port 1/0/1 entry to configure TLVs included in the outgoing LLDP-MED packets.

Figure 6-13 LLDP-MED Port Config-Detail



In the Location Identification Parameters section, configure the detailed address of the IP phone. Click **Apply**.

Figure 6-14 Configure the detailed address of the IP phone



6.2.5 Using the CLI

1) Create VLAN 10 and name it as Voice VLAN.

   Switch_A(config)#vlan 10

   Switch_A(config-vlan)#name Voice_VLAN

   Switch_A(config)#voice vlan 10

2) Configure the Voice VLAN mode on port Gi1/0/1 as Auto.

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

   Switch_A(config-if)#switchport voice vlan mode auto

   Switch_A(config-if)#exit

3) Configure the Voice VLAN mode on port Gi1/0/2 as Manual and add port Gi1/0/2 to Voice VLAN.

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

Switch_A(config-if)#switchport voice vlan mode manual

Switch_A(config-if)#switchport general allowed vlan 10 tagged

Switch_A(config-if)#exit

4) Enable LLDP globally.

Switch_A(config)#lldp

5) Configure the fast start count of LLDP-MED. The default is 4.

Switch_A(config)# lldp med-fast-count 4

6) Enable the LLDP-MED on port Gi1/0/1.

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

Switch_A(config-if)#lldp med-status

7) Configure the LLDP-MED TLVs included in the outgoing LLDP packets.

Switch_A(config-if)#lldp med-tlv-select all

8) Configure the detailed address of the IP phone.

Switch_A(config-if)#lldp med-location civic-address language English lci-city Vancouver street X east hastings street postal-zipcode V6A 1P9

Verify the Configurations

View global LLDP-MED settings:

Switch_A#show lldp

LLDP Status:	Enabled
LLDP Forward Message:	Disabled
Tx Interval:	30 seconds
TTL Multiplier:	4
Tx Delay:	2 seconds
Initialization Delay:	2 seconds
Trap Notification Interval:	5 seconds
Fast-packet Count:	3
LLDP-MED Fast Start Repeat Count:	4

View LLDP-MED settings on each port:

Switch_A#show lldp interface gigabitEthernet 1/0/1

LLDP interface config:

gigabitEthernet 1/0/1:

Admin Status:	TxRx
SNMP Trap:	Enabled
TLV	Status
---	------
Port-Description	Yes
System-Capability	Yes
System-Description	Yes
System-Name	Yes
Management-Address	Yes
Port-VLAN-ID	Yes
Protocol-VLAN-ID	Yes
VLAN-Name	Yes
Link-Aggregation	Yes
MAC-Physic	Yes
Max-Frame-Size	Yes
Power	Yes
LLDP-MED Status:	Enabled
TLV	Status
---	------
Network Policy	Yes
Location Identification	Yes
Extended Power Via MDI	Yes
Inventory Management	Yes

View the local information:

Switch_A#show lldp local-information interface gigabitEthernet 1/0/1

LLDP local Information:

gigabitEthernet 1/0/1:

Chassis type:	MAC address
Chassis ID:	00:0A:EB:13:23:97

Port ID type: Interface name

Port ID: GigabitEthernet1/0/1

Port description: GigabitEthernet1/0/1 Interface

TTL: 120

System name: Switch

System description: JetStream 24-Port Gigabit L2 Managed Switch with 4 SFP Slots

System capabilities supported: Bridge Router

System capabilities enabled: Bridge Router

Management address type: ipv4

Management address: 192.168.0.226

Management address interface type: IfIndex

Management address interface ID: 1

Management address OID: 0

Port VLAN ID(PVID): 1

Port and protocol VLAN ID(PPVID): 0

Port and protocol VLAN supported: Yes

Port and protocol VLAN enabled: No

VLAN name of VLAN 1: System-VLAN

Protocol identity:

Auto-negotiation supported: Yes

Auto-negotiation enabled: Yes

OperMau: speed(100)/duplex(Full)

Link aggregation supported: Yes

Link aggregation enabled: Yes

Aggregation port ID: 1

Power port class: PD

PSE power supported: No

PSE power enabled: No

PSE pairs control ability: No

Maximum frame size: 1518

LLDP-MED Capabilities: Capabilities

Network Policy

Location Identification

Inventory

Device Type: Network Connectivity

Application type: Reserved

Unknown policy: Yes

Tagged: No

VLAN ID: 0

Layer 2 Priority: 0

DSCP: 0

Location Data Format: Civic Address LCI

- What: Switch
- Country Code: CN
- Language: chinese
- Province/State: Guangdong
- County/Parish/District: China
- City/Township: Shenzhen
- Street: Keyuan Road
- Name: South Building No.5
- Postal/Zip Code: 518057

Hardware Revision: T2600G-28TS 2.0

Firmware Revision: Reserved

Software Revision: 1.0.1 Build 20151216 Rel.65850(s)

Serial Number: Reserved

Manufacturer Name: TP-Link

Model Name: T2600G-28TS 2.0

Asset ID: unknown

View the neighbor information:

Switch_A#show lldp neighbor-information interface gigabitEthernet 1/0/1

LLDP Neighbor Information:

gigabitEthernet 1/0/1:

Neighbor index 1:

Chassis type: Network address

Chassis ID: 192.168.1.117

Port ID type: Locally assigned

Port ID: 64A0E714DC54:P1

Port description: SW PORT

TTL: 180

System name: SEP64A0E714DC54

System description: Cisco IP Phone 7931G,V4, term default

System capabilities supported: Bridge Telephone

System capabilities enabled: Bridge Telephone

Management address type: ipv4

Management address: 192.168.1.117

Management address interface type: UnKnown

Port VLAN ID(PVID):

Port and protocol VLAN ID(PPVID):

Port and protocol VLAN supported:

Port and protocol VLAN enabled:

Protocol identity:

Auto-negotiation supported: Yes

Auto-negotiation enabled: Yes

OperMau: speed(100)/duplex(Full)

Link aggregation supported:

Link aggregation enabled:

Aggregation port ID:

Power port class:

PSE power supported:	
PSE power enabled:	
PSE pairs control ability:	
Maximum frame size:	
LLDP-MED Capabilities:	Capabilities
	Network Policy
	Extended Power via MDI - PD
	Inventory
Device Type:	Endpoint Class III
Application type:	Voice
Unknown policy:	No
Tagged:	No
VLAN ID:	4095
Layer 2 Priority:	5
DSCP:	46
Application type:	Voice Signaling
Unknown policy:	No
Tagged:	No
VLAN ID:	4095
Layer 2 Priority:	4
DSCP:	32
Power Type:	PD Device
Power Source:	Unknown
Power Priority:	Unknown
Power Value:	7.0w
Hardware Revision:	4
Firmware Revision:	tnp31.3-2-0-11.bin
Software Revision:	term31.default
Serial Number:	FCH1537A2JV
Manufacturer Name:	Cisco Systems, Inc.

7 Appendix: Default Parameters

Default settings of LLDP are listed in the following tables.

Default LLDP Settings

Table 7-1 Default LLDP Settings

Parameter	Default Setting
LLDP	Disable
LLDP Forward Message	Disable
Transmit Interval	30 seconds
Hold Multiplier	4
Transmit Delay	2 seconds
Reinit Delay	2 seconds
Notification Interval	5 seconds
Fast Start Times	3

Table 7-2 Default LLDP Settings on the Port

Parameter	Default Setting
Admin Status	Tx&Rx
Notification Mode	Disable
Included TLVs	All

Default LLDP-MED Settings

Table 7-3 Default LLDP-MED Settings

Parameter	Default Setting
Fast Start Count	4
LLDP-MED Status	Disable
Included TLVs	All

Part 28

Configuring Maintenance

CHAPTERS

1. Maintenance
2. Monitoring the System
3. SFlow Configuration
4. System Log Configurations
5. Diagnosing the Device
6. Diagnosing the Network
6. DLDP Configuration
78. Configuration Examples
89. Appendix: Default Parameters

1 Maintenance

1.1 Overview

The maintenance module assembles various system tools for network troubleshooting.

1.2 Supported Features

The maintenance module includes system monitor, sFlow (sampled Flow), Log, device diagnose, and network diagnose.

System Monitor

You can monitor the memory and the CPU utilizations of the switch.

SFlow

The switch provides a packet-based sFlow, which samples one packet out of a specified number of packets. With the sFlow, you can analyze traffic statistics and monitor the network usage.

Log

You can check system messages for debugging and network management.

Device Diagnose

You can test the cable connection status, cable length and error length for troubleshooting.

Network Diagnose

The network diagnose function includes Ping test and Tracert test. With them, you can test the connectivity between the switch and one node of the network, or the connectivity of the gateways on the path from the source to the destination.

DLDP

DLDP (Device Link Detection Protocol) is a Layer 2 protocol that enables devices connected through fiber or twisted-pair Ethernet cables to detect whether a unidirectional link exists. When a unidirectional link appears, the local device can receive packets from the peer device through the link layer, but the peer device cannot receive packets from the local device. Unidirectional links can cause a variety of problems, such as spanning-tree topology loops. Once detecting a unidirectional link, DLDP can shut down the related port automatically or inform users.

2 Monitoring the System

The system monitor configurations include:

- Monitoring the CPU;
- Monitoring the memory.

Configuration Guidelines

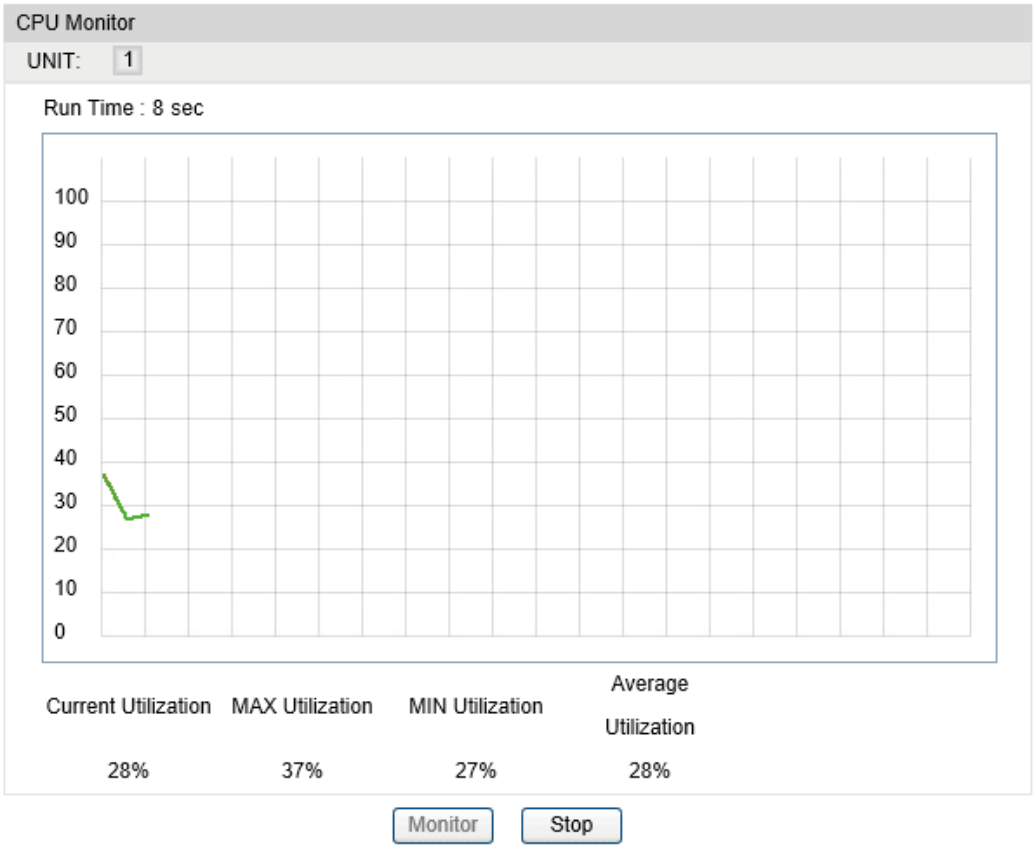
The CPU and memory utilizations should be always under 80%, and excessive use may result in switch malfunctions. For example, the switch fails to respond to management requests. In similar situations, you can monitor the system to verify a CPU or memory utilization problem.

2.1 Using the GUI

2.1.1 Monitoring the CPU

Choose the menu **Maintenance > System Monitor > CPU Monitor** to load the following page.

Figure 2-1 Monitoring the CPU

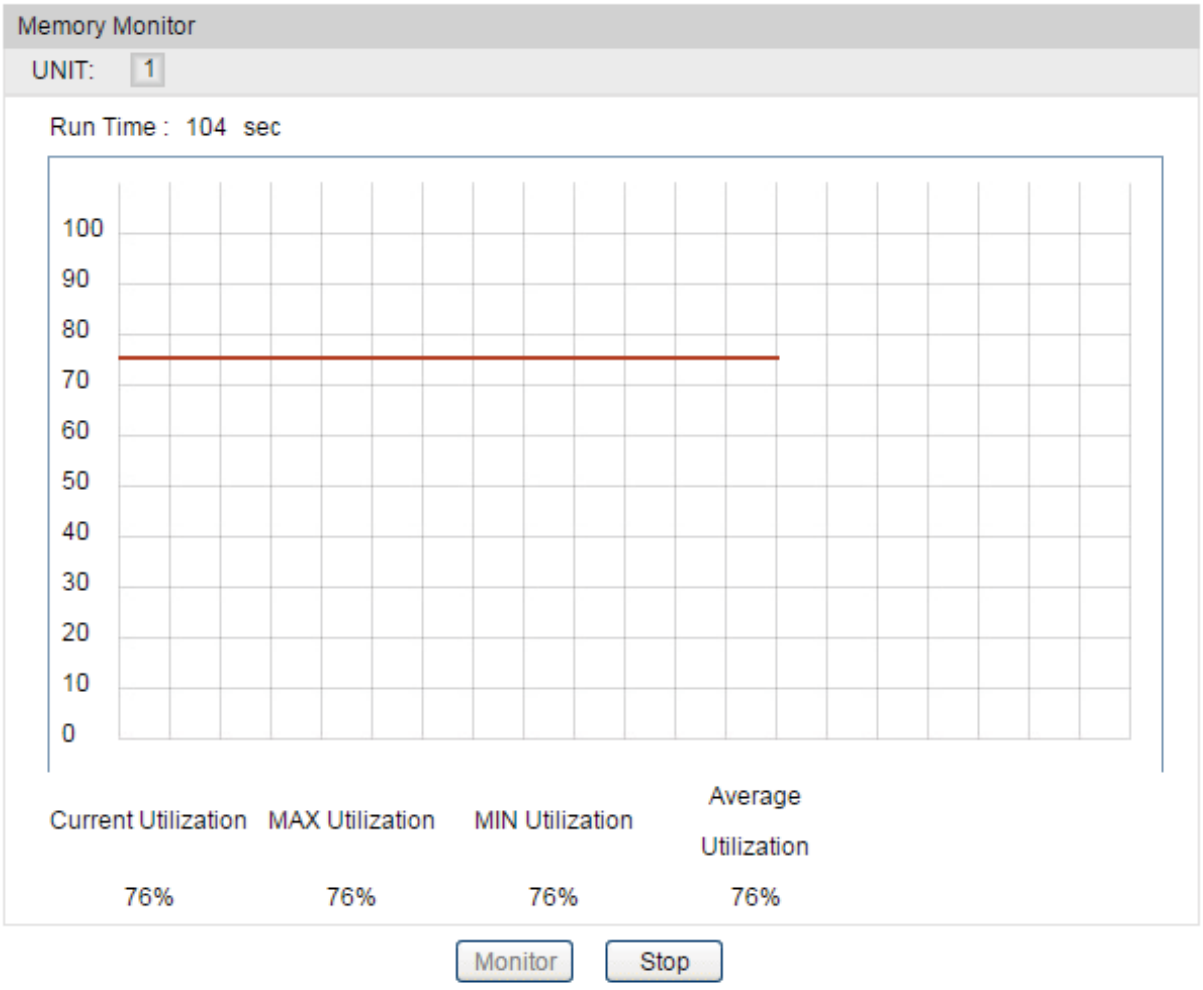


Click **Monitor** to enable the switch to monitor and display its CPU utilization rate every four seconds.

2.1.2 Monitoring the Memory

Choose the menu **Maintenance > System Monitor > Memory Monitor** to load the following page.

Figure 2-2 Monitoing the Memory



Click **Monitor** to enable the switch to monitor and display its memory utilization rate every four seconds.

2.2 Using the CLI

2.2.1 Monitoring the CPU

On privileged EXEC mode or any other configuration mode, you can use the following command to view the CPU utilization:

show cpu-utilization

View the memory utilization of the switch in the last 5 seconds, 1minute and 5minutes.

The following example shows how to monitor the CPU:

Switch#show cpu-utilization

```
Unit   |              CPU Utilization
No.    |  Five-Seconds  One-Minute  Five-Minutes
------+-----------------------------------------------
1      |  13%           13%         13%
```

2.2.2 Monitoring the Memory

On privileged EXEC mode or any other configuration mode, you can use the following command to view the memory utilization:

show memory-utilization

View the memory utilization of the switch in the last 5 seconds, 1minute and 5minutes.

The following example shows how to monitor the memory:

Switch#show memory-utilization

```
Unit   |  Current Memory Utilization
------+---------------------------
1      |  74%
```

3 SFlow Configuration

To complete the configuration, follow these steps:

1) Configure the sFlow collector;
2) Configure the sFlow sampler.

Configuration Guidelines

The sFlow monitoring system consists of an sFlow agent (embedded in a switch or router or in a standalone probe) and an sFlow collector (installed in a host). To get analytic results, you should choose a proper collector.

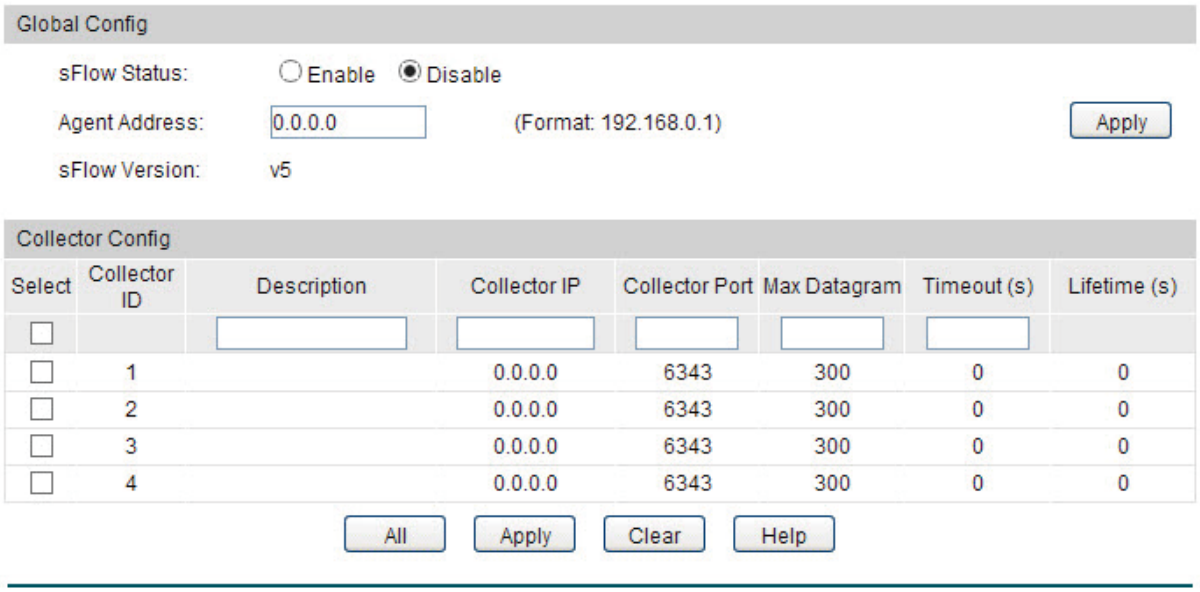
For details on sFlow collectors, refer to https://www.sflow.org.

3.1 Using the GUI

3.1.1 Configuring the SFlow Collector

Choose the menu **Maintenance > sFlow> sFlow collector** to load the following page.

Figure 3-1 Configuring the SFlow Collector



Follow these steps to configure the sFlow collector:

1) In the **Global Config** section, enable the sFlow function, specify the sFlow agent IP address, and then click **Apply**.

sFlow Status	Enable the sFlow function globally on the switch.

Agent Address	Enter the management IP address of the switch to monitor traffic on the switch port.
sFlow Version	The sFlow version is V5.

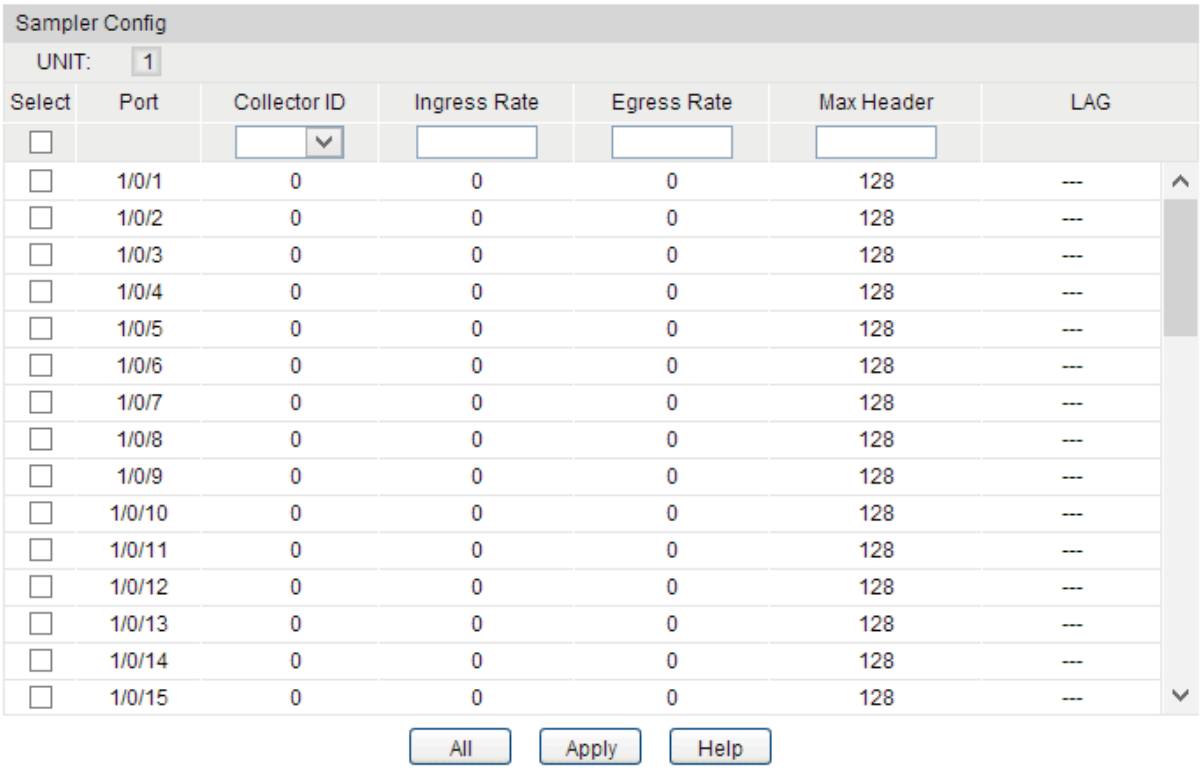
2) In the **Collector Config** section, select a collector to configure relevant parameters, and click **Apply**.

Collector ID	Select a collector for configuration. The switch supports 4 collectors at most.
Description	Give a collector description for identification with 16 characters at most.
Collector IP	Enter the IP address of the host that runs the sFlow collector.
Collector Port	Specify the UDP port number for the sFlow collector. The default is port 6343.
Max Datagram	Specify the maximum number of data bytes that can be sent in a single sample datagram. The values are from 300 to 1400 bytes and the default is 300 bytes.
Timeout (s)	Specify the aging time after which the sFlow collector will become invalid. The values are from 0 to 2000000 seconds; the default is 0, which means the collector is always valid.
Lifetime (s)	Displays the remaining time of the collector. Lifetime counts down from Timeout.

3.1.2 Configuring the SFlow Sampler

Choose the menu **Maintenance > sFlow> sFlow Sampler** to load the following page.

Figure 3-2 Configuring the SFlow Sampler



Follow these steps to configure the sFlow sampler:

1) In the **Sampler Config** section, set one or more ports to be a sampler and configure relevant parameters . One port can be bound to only one collector.

Collector ID	Select a collector for configuration. The switch supports 4 collectors at most.
Ingress Rate	Specify the ingress sampling frequency; then the samplers takes one packet out of the specified number of packets. The values are from 1024 to 65535 and the default is 0 which means no packets will be sampled.
Egress Rate	Specify the egress sampling frequency; then the samplers takes one packet out of the specified number of packets. The values are from 1024 to 65535 and the default is 0 which means no packets will be sampled.
Max Header	Specify the maximum number of bytes that should be copied from a sampled packet. The values are from 18 to 256 bytes; the default is 128 bytes.
LAG	Displays the LAG number which the port belongs to.

2) Click **Apply**.

3.2 Using the CLI

Follow these steps to configure the sFlow:

Step 1	**configure** Enter global configuration mode.
Step 2	**sflow address** { *ipv4-addr* } Configure the IP address of sFlow agent. *ipv4-addr*: Enter the management IP address of the switch to monitor traffic on the switch port.
Step 3	**sflow enable** Enable the sFlow function.
Step 4	**sflow collector collector-ID** *value* { [**descript** *descript*] | [**ip** *ip*] | [**port** *port*] | [**maxData** *maxData*] | [**timeout** *timeout*] } Configure parameters of the sFlow collector. *value*: Enter the ID of the sFlow collector. The values are from 1 to 4. *descript*: Give a collector description for identification with 16 characters at most. *ip*: Enter the IP address of the host that runs the sFlow collector. *port*: Enter the UDP port number for the sFlow collector. The default is port 6343. *maxData*: Specify the maximum number of data bytes that can be sent in a single sample datagram. The values are s from 300 to 1400 bytes; the default is 300 bytes. *timeout*: Specify the aging time after which the sFlow collector will become invalid. The values are from 0 to 2000000 seconds; the default is 0, which means the collector is always valid.

Step 5	**interface** { [**gigabitEthernet** *port*]	[**range gigabitEthernet** *port-list*] } Configure the sampler on the specified ports. *port/port-list:* The number or the list of the Ethernet ports that you want to monitor.
Step 6	**sflow sampler** { [**collector-ID** *value*]	[**ingRate** *ingress-rate*] [**egRate** *egress-rate*]	[**maxHeader** *maxHeader*] } Configure parameters of the sFlow sampler. *value*: Enter the ID of the sFlow collector which the sFlow sampler will send sFlow datagrams to. The values are from 0 to 4. And 0 means no collector is selected. *ingress-rate*: Specify the ingress sampling frequency; then the samplers takes one packet out of the specified number of packets. The values are from 1024 to 65535 and the default is 0 which means no packets will be sampled. *egress-rate*: Specify the egress sampling frequency; then the samplers takes one packet out of the specified number of packets. The values are from 1024 to 65535 and the default 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 values are from 18 to 256 bytes; the default is 128 bytes.
Step 7	**show sflow** { [global]	[collector]	[sampler] } Verify the sFlow configurations. global: View the global configuration of sFlow. collector: View the global configuration of the sFlow collector. sampler: View the global configuration of the sFlow sampler.
Step 8	**end** Return to privileged EXEC mode.
Step 9	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the switch whose IP address is 192.168.0.1 to send sFlow packets to the host whose IP address is 192.168.0.100. Set the sFlow agent IP address as 192.168.0.1, the sFlow collector IP address 1 as 192.168.0.100; configure Gigabit Ethernet port 1 as the sFlow sampler, the Collector-ID as 1, and the ingress rate as 1024:

Switch#configure

Switch(config)#sflow address 192.168.0.1

Switch(config)#sflow enable

Switch(config)#sflow collector collector-ID 1 **ip** 192.168.0.100

Switch(config)# sflow collector collector-ID 1 **port** 6343

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

Switch(config-if)#sflow sampler collector-ID 1

Switch(config-if)#sflow sampler ingRate 1024

Switch(config-if)#show sflow global

sFlow Status: Enable

Agent Address: 192.168.0.1

sFlow Version: v5

Switch(config-if)#show sflow collector

Collector	Col-IP	Col-Port	MaxData	Timeout	Lifetime	Description
1	192.168.0.100	6343	300	0	0	
2	0.0.0.0	6343	300	0	0	
3	0.0.0.0	6343	300	0	0	
4	0.0.0.0	6343	300	0	0	

Switch(config-if)#show sflow sampler

Port	Collector	IngRate	EgRate	MaxHeader	LAG
Gi1/0/1	1	1024	0	128	N/A
Gi1/0/2	0	0	0	128	N/A
Gi1/0/3	0	0	0	128	N/A

...

Switch(config-if)#end

Switch#copy running-config startup-config

4 System Log Configurations

System log configurations include:

- Configuring the local log;
- Configuring the remote log;
- Backing up log files;
- Viewing the log table.

Configuration Guidelines

Logs are classified into the following eight levels. Messages of levels 0 to 4 mean the functionality of the switch is affected. Please take actions according to the log message.

Table 4-1 Levels of Logs

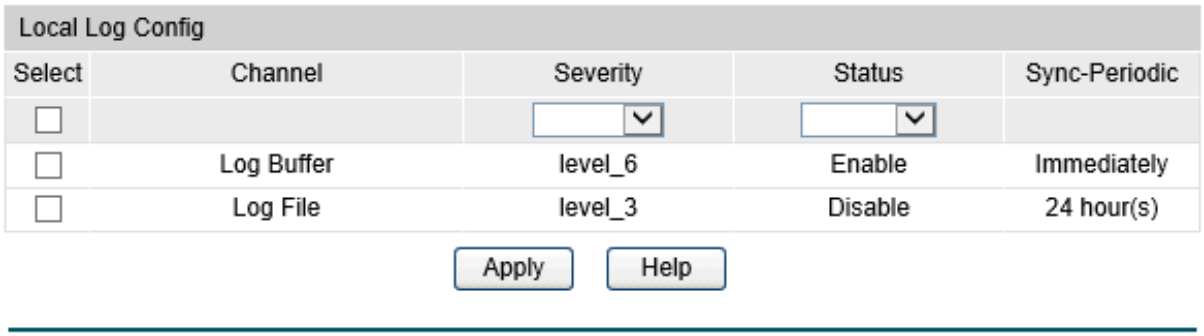
Severity	Level	Description	Example
Emergencies	0	The system is unusable and you have to reboot the switch.	Software malfunctions affect the functionality of the switch.
Alerts	1	Actions must be taken immediately.	The memory utilization reaches the limit.
Critical	2	Cause analysis or actions must be taken immediately.	The memory utilization reaches the warning threshold.
Errors	3	Error operations or unusual processing that will not affect subsequent operations but that should be noted and analyzed.	Wrong command or password is entered.
Warnings	4	Conditions that may cause process failure and that should be noted.	Error protocol packets are detected.
Notifications	5	Normal but significant conditions.	The **shutdown** command is applied to a port.
Informational	6	Normal messages for your information.	The **display** command is used.
Debugging	7	Debug-level messages that you can ignore.	General operational information.

4.1 Using the GUI

4.1.1 Configuring the Local Log

Choose the menu **Maintenance > Log> Local Log** to load the following page.

Figure 4-1 Configuring the Local Log



Follow these steps to configure the local log:

1) Select your desired channel and configure the corresponding severity and status.

Channel	Local log includes 2 channels: log buffer and log file. Log buffer indicates the RAM for saving system log. The channel is enabled by default. The information in the log buffer is displayed on the **Maintenance > Log> Log Table** page. It will be lost when the switch is restarted. Log File indicates the flash sector for saving system log. The information in the log file will not be lost after the switch is restarted and can be exported on the **Maintenance > Log > Backup Log** page.
Severity	Specify the severity level of the log information that is saved to the selected channel. Only the log with the same or smaller severity level value can be saved. There are 8 severity levels marked from 0 to 7. The smaller value means the higher priority.
Status	Enable or disable the channel.
Sync-Periodic	By default, the log information is saved in the log buffer immediately, and synchronized to the log file every 24 hours. If necessary, you can modify the log synchronization frequency using the CLI.

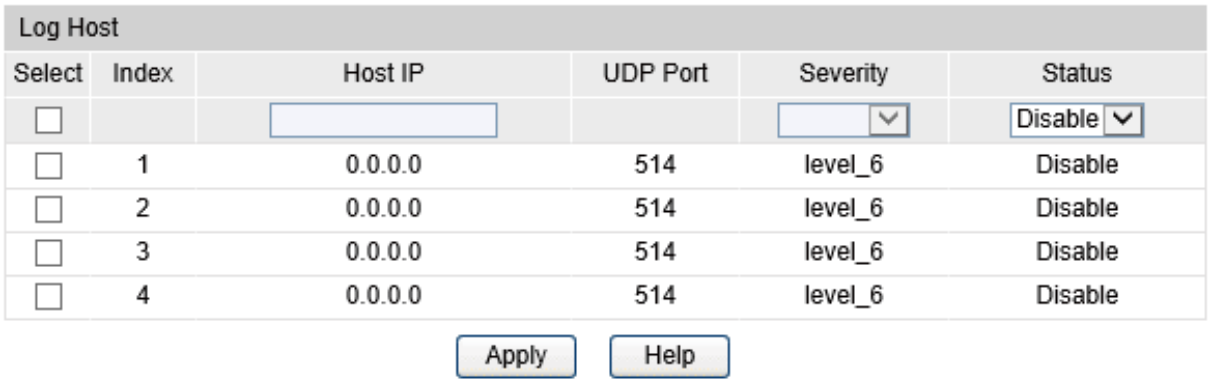
2) Click **Apply**.

4.1.2 Configuring the Remote Log

Remote Log enables the switch to send system logs to a host. To display the logs, the host should run a log server that complies with the syslog standard.

Choose the menu **Maintenance > Log> Remote Log** to load the following page.

Figure 4-2 Configuring the Remote Log



Follow these steps to configure remote log:

1) Select an entry to enable the status, and then set the host IP address and severity.

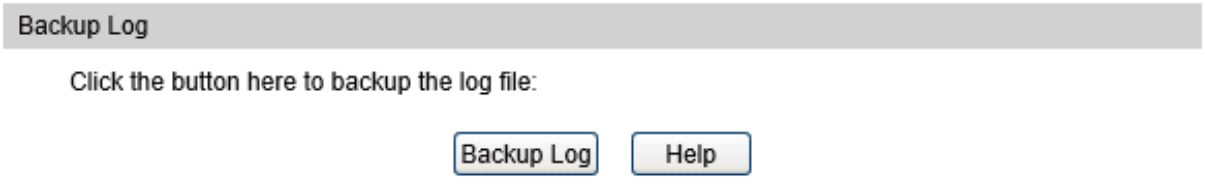
Host IP	Specify an IP address for the log host.
UDP Port	Displays the UDP port that receives and sends the log information. And the switch uses the standard port 514.
Severity	Specify the severity level of the log information sent to the selected log host. Only the log with the same or smaller severity level value will be sent to the corresponding log host.
Status	Enable or disable the log host.

2) Click **Apply**.

4.1.3 Backing up the Log File

Choose the menu **Maintenance > Log > Backup Log** to load the following page.

Figure 4-3 Backup Log

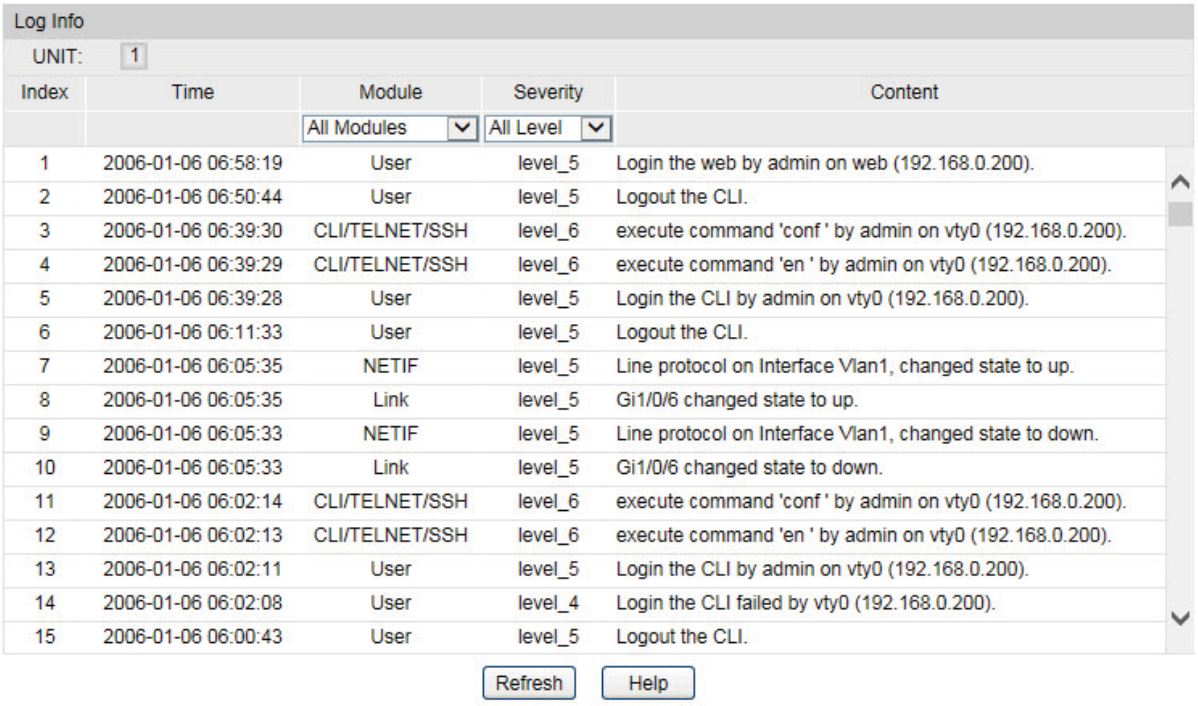


Click **Backup Log** to save the system log as a file on your computer. If the switch system breaks down, you can check the file for troubleshooting.

4.1.4 Viewing the Log Table

Choose the menu **Maintenance > Log> Log Table** to load the following page.

Figure 4-4 Viewing the Log Table



Select a module and a severity to view the corresponding log information.

Time	To get the exact time when the log event occurs, you need to configure the system time on the **System > System Info > System Time** Web management page.
Module	Select a module from the drop-down list to display the corresponding log information.
Severity	Select a severity level to display the log information whose severity level value is the same or smaller.

4.2 Using the CLI

4.2.1 Configuring the Local Log

Follow these steps to configure the local log:

Step 1	**configure** Enter global configuration mode.
Step 2	**logging buffer** The switch stores the system log messages to the RAM. And the information will be lost when the switch is restarted. You can view the logs with **show logging buffer** command.

Step 3	**logging buffer level** */level/* Specify the severity level of the log information that should be saved to the buffer. */level*: Enter the severity level ranging from 0 to 7. The smaller value has the higher priority. Only the log with the same or smaller severity level value can be saved. The default level is 6, indicating that the log information of levels 0 to 6 will be saved in the log buffer.
Step 4	**logging file flash** Store the log messages in the flash sector of the switch. The information in the flash will not be lost after the switch is restarted. You can view the logs with **show logging flash** command.
Step 5	**logging file flash frequency** { **periodic** *periodic* | **immediate** } Specify the frequency to synchronize the system log file in the log buffer to the flash. *periodic*: Specify the frequency 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 means frequent operations on the flash and is not recommended.
Step 6	**logging file flash level** */level/* Specify the severity level of the log information that should be saved to the flash. */level*: Enter the severity level ranging from 0 to 7. The smaller value has the higher priority. Only the log with the same or smaller severity level value can be saved to the flash. The default level is 3, indicating that the log message of levels 0 to 3 will be saved in the log flash.
Step 7	**show logging local-config** View the configuration information of the local log.
Step 8	**end** Return to privileged EXEC mode.
Step 9	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the local log on the switch. Save logs of levels 0 to 5 to the log buffer, and synchronize logs of levels 0 to 2 to the flash every 10 hours:

Switch#configure

Switch(config)#logging buffer

Switch(config)#logging buffer level 5

Switch(config)#logging file flash

Switch(config)#logging file flash frequency periodic 10

Switch(config)#logging file flash level 2

Switch(config)#show logging local-config

Channel	Level	Status	Sync-Periodic
Buffer	5	enable	Immediately
Flash	2	enable	10 hour(s)
Monitor	5	enable	Immediately

Switch(config)#end

Switch#copy running-config startup-config

4.2.2 Configuring the Remote Log

Remote Log enables the switch to send system logs to a host. To display the logs, the host should run a log server that complies with the syslog standard.

Follow these steps to set the remote log:

Step 1	**configure** Enter global configuration mode.
Step 2	**logging host index** *idx host-ip level* Configure the log host which receives the system logs from other devices. You can remotely monitor the settings and operation status of other devices through the log host. *idx*: Enter the index of the log host. The switch supports 4 log hosts at most. *host-ip*: Specify the IP address for the log host. *level*: Enter the severity level of the log information that should be sent to each log host. The range is 0 to 7, and 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. The default is 6, indicating that the log information of levels 0 to 6 will be sent to the log host.
Step 3	**show logging loghost** [*index*] View the configuration information of the log host. *index*: Enter the index of the log host to view the corresponding configuration information. If no value is specified, information of all log hosts will be displayed.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set the remote log on the switch. Enable log host 2, set its IP address as 192.168.0.148, and allow logs of levels 0 to 5 to be sent to the host:

Switch#configure

Switch(config)# logging host index 2 192.168.0.148 5

Switch(config)# show logging loghost

Index	Host-IP	Severity	Status
1	0.0.0.0	6	disable
2	192.168.0.148	5	enable
3	0.0.0.0	6	disable
4	0.0.0.0	6	disable

Switch(config)#end

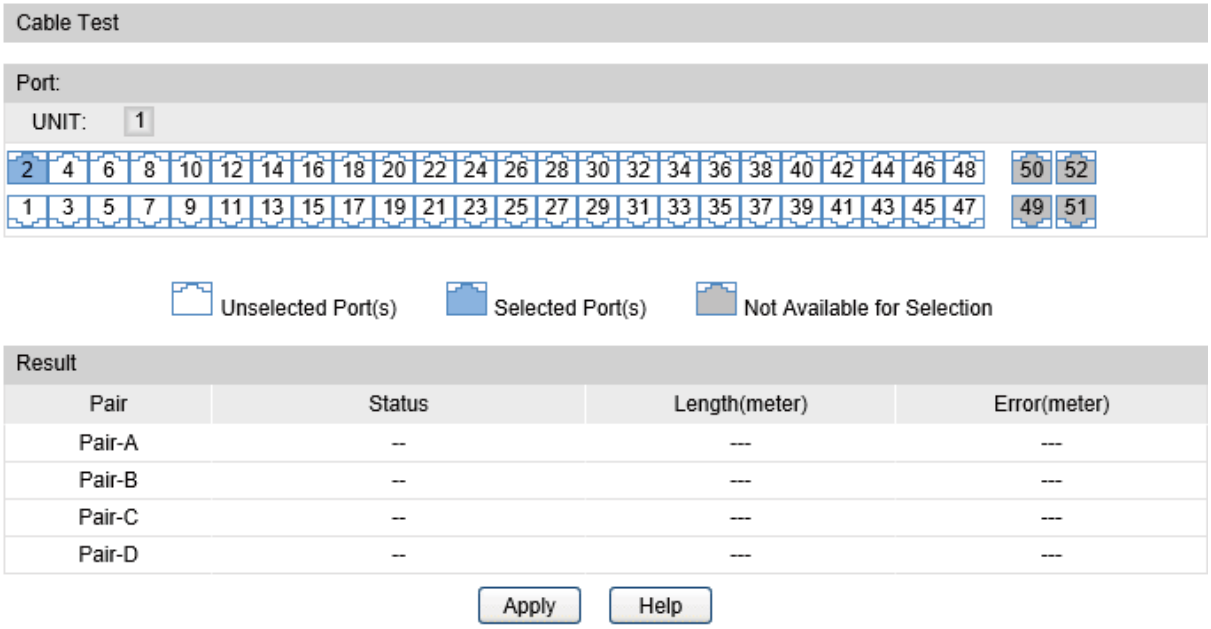
Switch#copy running-config startup-config

5 Diagnosing the Device

5.1 Using the GUI

Choose the menu **Maintenance > Device Diagnose > Cable Test** to load the following page.

Figure 5-1 Diagnosing the Device



1) In the **Port** section, select your desired port for the test.
2) In the **Result** section, click **Apply** and check the test results.

Port	Select the port for cable testing. The interval between two cable tests for one port must be more than 3 seconds.
Pair	Displays the Pair number.
Status	Displays the cable status. Test results include normal, close, open and crosstalk. Normal : The cable is normally connected. Close: A short circuit caused by an abnormal contact of wires in the cable. Open: No device is connected to the other end or the connectivity is broken. Crosstalk: Impedance mismatch caused by the poor quality of the cable.
Length	If the connection status is normal, here displays the length range of the cable. The value makes sense only when the cable is longer than 30m.

Error	If the connection status is short, close or crosstalk, here displays the length from the port to the trouble spot. The value makes sense only when the cable is longer than 30m.

5.2 Using the CLI

On privileged EXEC mode or any other configuration mode, you can use the following command to check the connection status of the cable that is connected to the switch.

show cable-diagnostics interface gigabitEthernet *port*

View the cable diagnostics of the connected Ethernet Port.

port: Enter the port number in 1/0/1 format to check the result of the cable test.

show cable-diagnostics careful interface gigabitEthernet *port*

View the cable diagnostics of the connected Ethernet Port. When taking the careful cable test, the switch will only test the cable for the port which is in the link-down status.

port: Enter the port number in 1/0/1 format to check the result of the cable test.

The following example shows how to check the cable diagnostics of port 1/0/2:

Switch#show cable-diagnostics interface gigabitEhternet 1/0/2

Port	Pair	Status	Length	Error
Gi1/0/2	Pair-A	Normal	2 (+/- 10m)	---
	Pair-B	Normal	2 (+/- 10m)	---
	Pair-C	Normal	0 (+/- 10m)	---
	Pair-D	Normal	2 (+/- 10m)	---

6 Diagnosing the Network

The configuration includes:

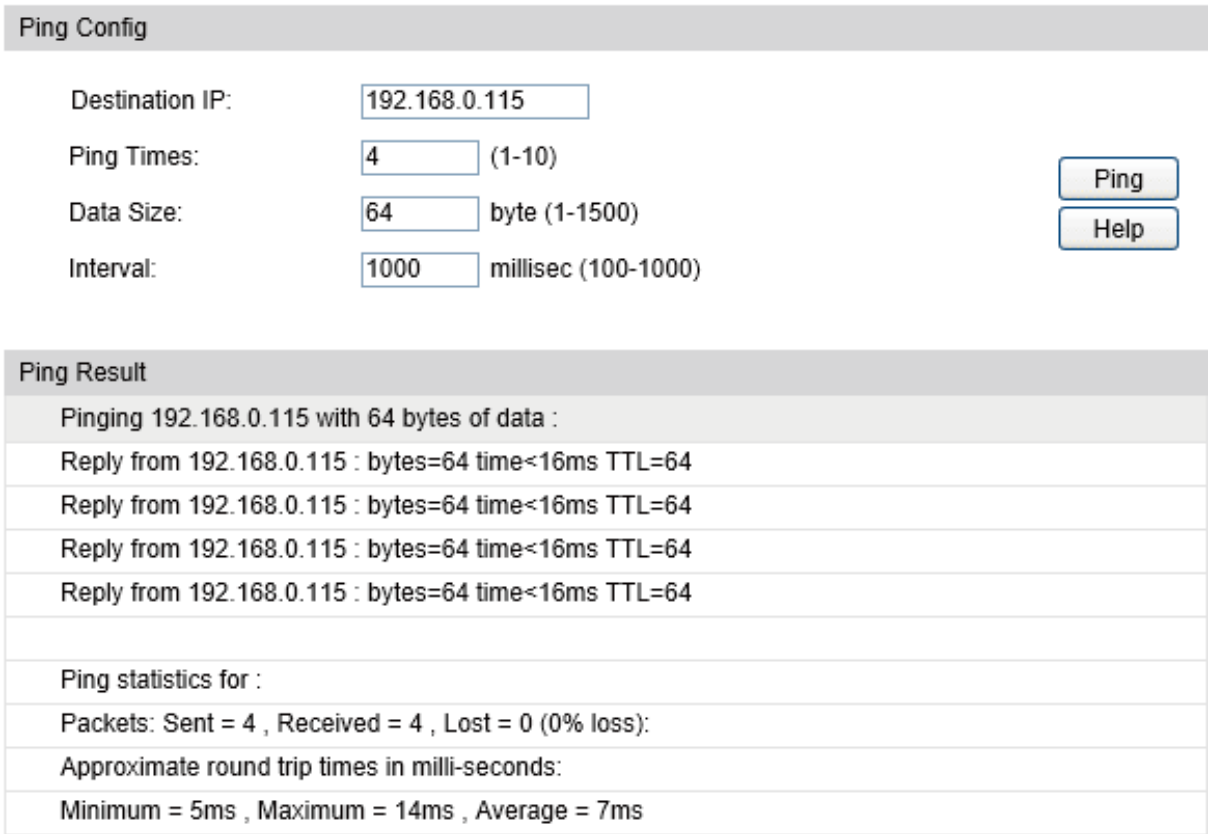
- Configuring the Ping Test;
- Configuring the Tracert Test.

6.1 Using the GUI

6.1.1 Configuring the Ping Test

Choose the menu **Maintenance > Network Diagnose > Ping** to load the following page.

Figure 6-1 Configuring the Ping Test



Follow these steps to test the connectivity between the switch and another device in the network:

1) In the **Ping Config** section, enter the IP address of the destination device for Ping test, set Ping times, data size and interval according to your needs, and then click **Ping** to start the test.

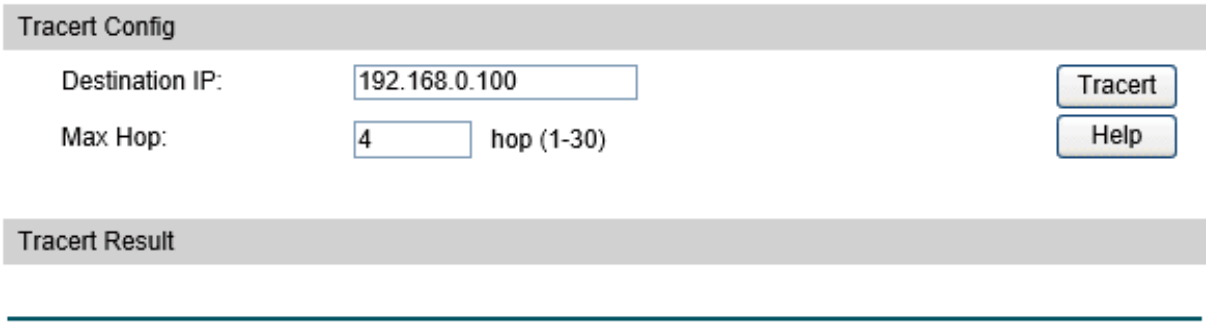
Destination IP	Enter the IP address of the destination node for Ping test. Both IPv4 and IPv6 are supported.
Ping Times	Enter the amount of times to send test data for Ping test. We recommend that you keep the default 4 times.
Data Size	Enter the size of the sending data for Ping test. We recommend that you keep the default 64 bytes.
Interval	Specify the interval to send ICMP request packets. We recommend that you keep the default 1000 milliseconds.

2) In the **Ping Result** section, check the test results.

6.1.2 Configuring the Tracert Test

Choose the menu **Maintenance > Network Diagnose > Tracert** to load the following page.

Figure 6-2 Configuring the Tracert Test



Follow these steps to test connectivity between the switch and routers along the path from the source to the destination:

1) In the **Tracert Config** section, enter the IP address of the destination, set the max hop, and then click **Tracert** to start the test.

Destination IP	Enter the IP address of the destination device. Both IPv4 and IPv6 are supported.
Max Hop	Specify the maximum number of the route hops the test data can pass through.

2) In the **Tracert Result** section, check the test results.

6.2 Using the CLI

6.2.1 Configuring the Ping Test

On privileged EXEC mode or any other configuration mode, you can use the following command to test the connectivity between the switch and one node of the network.

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

Test the connectivity between the switch and destination device.

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, such as 192.168.0.100 or fe80::1234.

-n *count*: Specify the amount of times to send test data for Ping testing. The values are from 1 to 10 times; the default is 4 times.

-l *count*: Specify the size of the sending data for ping testing. The values are from 1 to 1500 bytes; the default is 64 bytes.

-i *count:* Specify the interval to send ICMP request packets. The values are from 100 to 1000 milliseconds; the default is 1000 milliseconds.

The following example shows how to test the connectivity between the switch and the destination device with the IP address 192.168.0.10. Specify the ping times as 3, the data size as 1000 bytes and the interval as 500 milliseconds:

Switch#ping ip 192.168.0.10 **-n** 3 **-l** 1000 **-i** 500

Pinging 192.168.0.10 with 1000 bytes of data :

Reply from 192.168.0.10 : bytes=1000 time<16ms TTL=64

Reply from 192.168.0.10 : bytes=1000 time<16ms TTL=64

Reply from 192.168.0.10 : bytes=1000 time<16ms TTL=64

Ping statistics for 192.168.0.10:

Packets: Sent = 3 , Received = 3 , Lost = 0 (0% loss)

Approximate round trip times in milli-seconds:

Minimum = 0ms , Maximum = 0ms , Average = 0ms

6.2.2 Configuring the Tracert Test

On privileged EXEC mode or any other configuration mode, you can use the following command to test the connectivity between the switch and routers along the path from the source to the destination:

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

Test the connectivity of the gateways along the path from the source to the destination.

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: Enter the IP address of the destination device. If the parameter ip/ipv6 is not selected, both IPv4 and IPv6 addresses are supported, such as 192.168.0.100 or fe80::1234.

maxHops: Specify the maximum number of the route hops the test data can pass though. The range is 1 to 30 hops; the default is 4 hops.

The following example shows how to test the connectivity between the switch and the network device with the IP address 192.168.0.100. Set the maxhops as 2:

Switch#tracert 192.168.0.100 2

Tracing route to 192.168.0.100 over a maximum of 2 hops

1 8 ms 1 ms 2 ms 192.168.1.1

2 2 ms 2 ms 2 ms 192.168.0.100

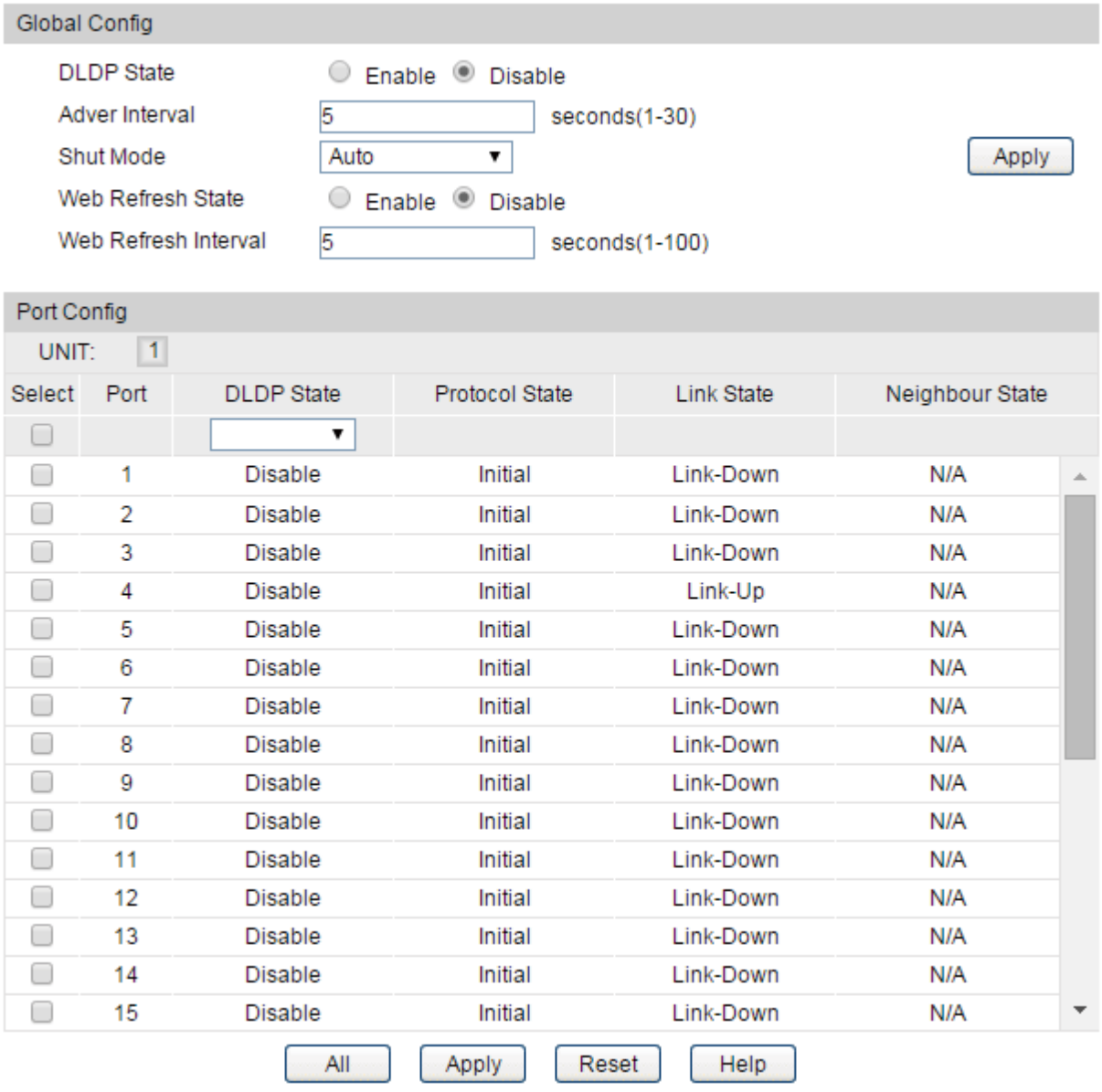
Trace complete.

7 DLDP Configuration

7.1 Using the GUI

Choose the menu **Maintenance > DLDP > DLDP Config** to load the following page.

Figure 7-1 DLDP Config



Follow these steps to configure DLDP:

1) In the **Global Config** section, enable DLDP and configure the relevant parameters. Click **Apply**.

DLDP State	Enable or disable DLDP globally.
Adver Interval	Configure the interval to send advertisement packets. The valid values are from 1 to 30 seconds, and the default value is 5 seconds.
Shut Mode	Choose how to shut down the port when a unidirectional link is detected: **Auto**: When an unidirectional link is detected on a port, DLDP will generate logs and traps and shut down the port, and the DLDP link state will transit to Disable. **Manual**: When an unidirectional link is detected on a port, DLDP will generate logs and traps, and then the users can manually shut down the unidirectional link ports.
Web Refresh State	Enable or disable the web automatic refresh function.
Web Refresh Interval	Configure the interval to refresh the web page. The valid values are from 1 to 100 seconds, and the default value is 5 seconds.
Interval	Specify the interval to send ICMP request packets. We recommend that you keep the default 1000 milliseconds.

2) In the **Port Config** section, select one or more ports, enable DLDP and click **Apply**. Then you can view the relevant DLDP information in the table.

DLDP State	Enable or disable DLDP on the port.
Protocol State	Displays the DLDP protocol state. **Initial**: DLDP is disabled. **Inactive**: DLDP is enabled but the link is down. **Active**: DLDP is enabled and the link is up, or the neighbor entries in this device are empty. **Advertisement**: No unidirectional link is detected: this device establishes bidirectional links with all its neighbors, or DLDP remains in Active state for more than 5 seconds. **Probe**: In this state, the device will send out Probe packets to detect whether the link is unidirectional. The port enters this state from the Active state if it receives a packet from an unknown neighbor. **Disable**: A unidirectional link is detected.
Link State	Displays the link state. **Link-Down**: The link is down. **Link-Up**: The link is up.

Neighbour State	Displays the neighbor state. **Unknown**: Link detecting is in progress. **Unidirectional**: The link between the port and the neighbor is unidirectional. **Bidirectional**: The link between the port and the neighbor is bidirectional.

7.2 Using the CLI

Follow these steps to configure DLDP:

Step 1	**configure** Enter global configuration mode.
Step 2	**dldp** Globally enable DLDP.
Step 3	**dldp interval** *interval-time* Configure the interval of sending advertisement packets on ports that are in the advertisement state. *interval-time*: Specify the interval time. The valid values are from 1 to 30 seconds. By default, it is 5 seconds.
Step 3	**dldp shut-mode** { auto | manual } Configure the DLDP shutdown mode when a unidirectional link is detected. auto: The switch automatically shuts down ports when a unidirectional link is detected. It is the default setting. manual: The switch displays an alert when a unidirectional link is detected. Then the users can manually shut down the unidirectional link ports..
Step 4	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list***}** Enter interface configuration mode.
Step 5	**dldp** Enable DLDP on the specified port.
Step 6	**show dldp** Verify the global DLDP configuration.
Step 7	**show dldp interface** Verify the DLDP configuration of the ports.
Step 8	**end** Return to privileged EXEC mode.

Step 9	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable DLDP globally, configure the DLDP interval as 10 seconds and specify the shutdown mode as auto.

Switch#configure

Switch(config)#dldp

Switch(config)#dldp interval 10

Switch(config)#dldp shut-mode auto

Switch(config)#show dldp

DLDP Global State: Enable

DLDP Message Interval: 10

DLDP Shut Mode: Auto

Switch(config)#end

Switch#copy running-config startup-config

The following example shows how to enable DLDP on port 1/0/1.

Switch#configure

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

Switch(config-if)#dldp

Switch(config-if)#show dldp interface

Port	DLDP State	Protocol State	Link State	Neighbor State
----	----------	-------------	----------	-------------
Gi1/0/1	Enable	Inactive	Link-Down	N/A
Gi1/0/2	Disable	Initial	Link-Down	N/A
Gi1/0/3	Disable	Initial	Link-Down	N/A
Gi1/0/4	Disable	Initial	Link-Down	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

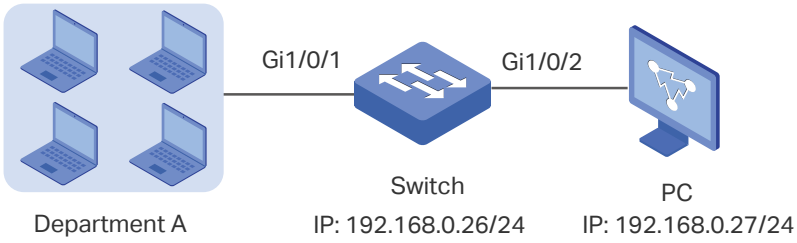
8 Configuration Examples

8.1 Example for Configuring SFlow

8.1.1 Network Requirements

The company network manager needs to monitor and analyze the network usage in department A.

Figure 8-1 Network Topology



8.1.2 Configuration Scheme

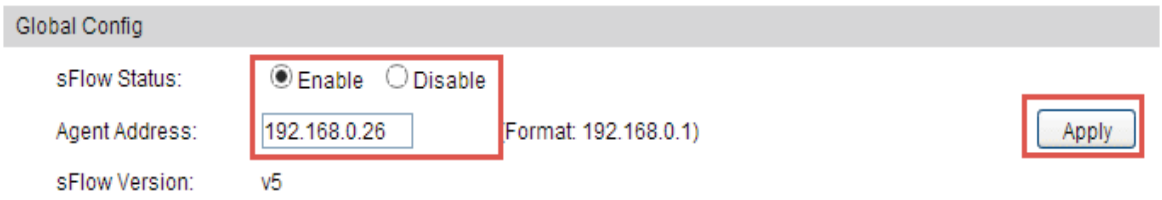
The network manager can configure sFlow to monitor and analyze the network. Set the switch as the sFlow agent that collects traffic data on port 1/0/1, and configure an sFlow collector on the PC to process sFlow packets and display results.

Demonstrated with T2600G-28TS, this chapter provides configuration procedures in two ways: using the GUI and Using the CLI.

8.1.3 Using the GUI

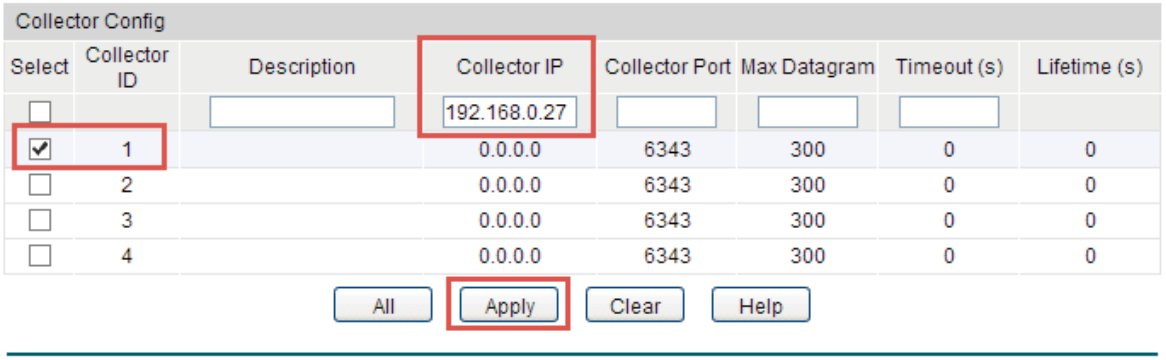
1) Choose the menu **Maintenance > SFlow > SFlow Collector** to load the following page. In the **Global Config** section, enable sFlow, set the switch IP address 192.168.0.26 as the agent address, and click **Apply**.

Figure 8-2 SFlow Collector Global Config



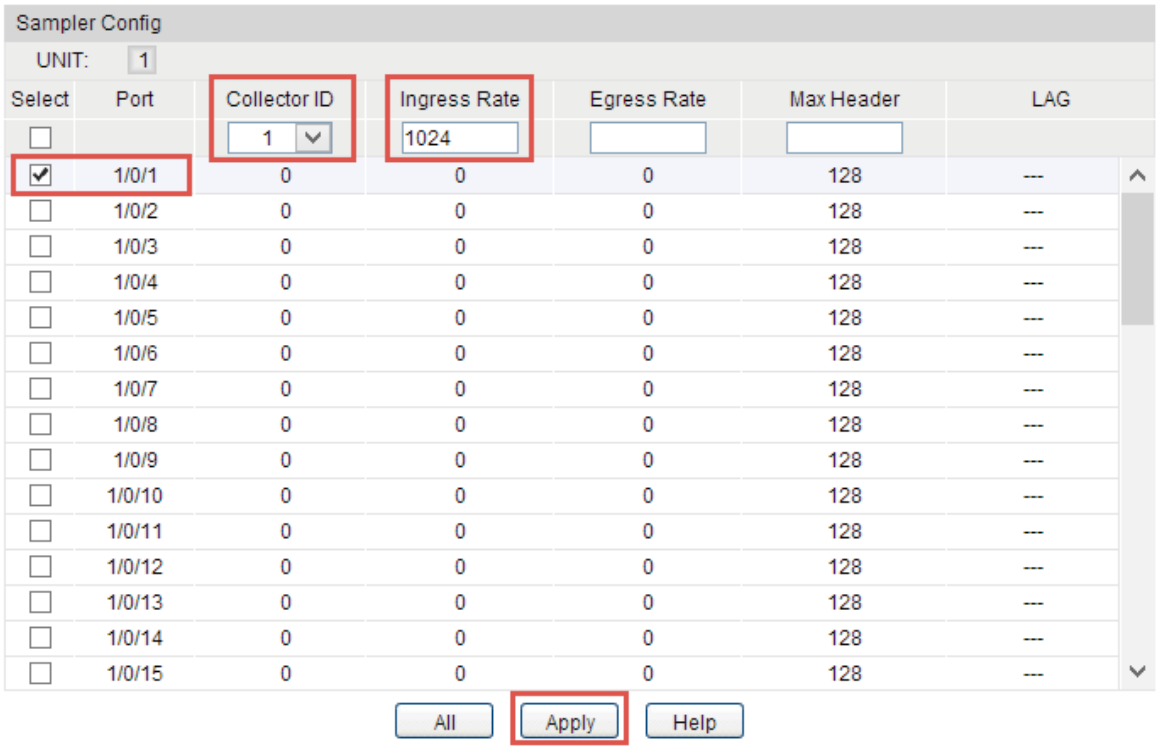
In the **Collector Config** section, select Collector 1, enter the PC IP address 192.168.0.27 as the collector IP address, and click **Apply**.

Figure 8-3 Collector Config



2) Choose the menu **Maintenance > SFlow > SFlow Sampler** to load the following page. Select collector 1 for port 1/0/1, set the ingress rate as 1024, and then click **Apply**.

Figure 8-4 SFlow Sampler Config



8.1.4 Using the CLI

1) Configure the sFlow collector.

Switch#configure

Switch(config)#sflow address 192.168.0.26

Switch(config)#sflow enable

Switch(config)#sflow collector collector-ID 1 ip 192.168.0.27

Switch(config)# sflow collector collector-ID 1 port 6343

2) Configure the sFlow sampler.

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

Switch(config-if)#sflow sampler collector-ID 1

Switch(config-if)#sflow sampler ingRate 1024

Switch(config-if)#end

Switch#copy running-config startup-config

Verify the Configurations

Verify the configuration of global sFlow:

Switch#show sflow global

sFlow Status: Enable

Agent Address: 192.168.0.26

sFlow Version: v5

Verify the configuration of sFlow collector:

Switch#show sflow collector

Collector	Col-IP	Col-Port	MaxData	Timeout	Lifetime	Description
1	192.168.0.27	6343	300	0	0	
2	0.0.0.0	6343	300	0	0	
3	0.0.0.0	6343	300	0	0	
4	0.0.0.0	6343	300	0	0	

Verify the configuration of sFlow sampler:

Switch#show sflow sampler

Port	Collector	IngRate	EgRate	MaxHeader	LAG
Gi1/0/1	1	1024	0	128	N/A
Gi1/0/2	0	0	0	128	N/A

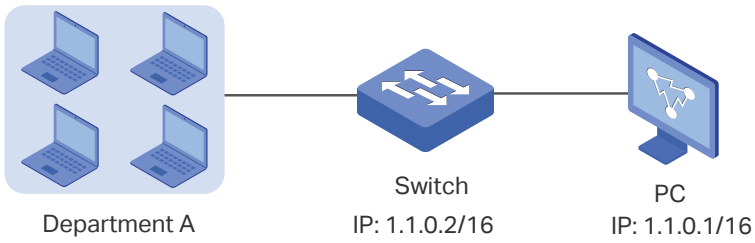
...

8.2 Example for Configuring Remote Log

8.2.1 Network Requirements

The company network manager needs to monitor network of department A for troubleshooting.

Figure 8-1 Network Topology



8.2.2 Configuration Scheme

The network manager can configure the remote log to receive system logs from monitored devices. Make sure the switch and the PC are reachable to each other; configure a log server that complies with the syslog standard on the PC and set the PC as the log host.

Demonstrated with T2600G-28TS, this chapter provides configuration procedures in two ways: using the GUI and Using the CLI.

8.2.3 Using the GUI

1) Choose the menu **Maintenance > Log > Remote Log** to load the following page. Enable host 1, and set the PC IP address 1.1.0.1 as the host IP address, and the severity as level_5; click **Apply**.

Figure 8-2 Remote Log Host

Log Host

Select	Index	Host IP	UDP Port	Severity	Status
☐		1.1.0.1		level_5	Enable
☑	1	0.0.0.0	514	level_6	Disable
☐	2	0.0.0.0	514	level_6	Disable
☐	3	0.0.0.0	514	level_6	Disable
☐	4	0.0.0.0	514	level_6	Disable

Apply Help

8.2.4 Using the CLI

Configure the remote log host.

Switch#configure

```
Switch(config)# logging host index 1 1.1.0.1 5
Switch(config)#end
Switch#copy running-config startup-config
```

Verify the Configurations

```
Switch# show logging loghost
```

Index	Host-IP	Severity	Status
1	1.1.0.1	5	enable
2	0.0.0.0	6	disable
3	0.0.0.0	6	disable
4	0.0.0.0	6	disable

9 Appendix: Default Parameters

Default settings of maintenance are listed in the following tables.

Table 9-1 Default Settings of Local Log

Parameter	Default Setting
Status of Log Buffer	Enabled
Severity of Log Buffer	Level_6
Sync-Periodic of Log Buffer	Immediately
Status of Log File	Disabled
Severity of Log File	Level_3
Sync-Periodic of Log File	24 hours

Table 9-2 Default Settings of Remote Log

Parameter	Default Setting
Host IP	0.0.0.0
UDP Port	514
Severity	Level_6
Status	Disabled

Table 9-3 Default Settings of Ping Config

Parameter	Default Setting
Destination IP	192.168.0.1
Ping Times	4
Data Size	64 bytes
Interval	1000 milliseconds

Table 9-4 Default Settings of Tracert Config

Parameter	Default Setting
Destination IP	192.168.0.100
Max Hop	4 hops

Table 9-5 Default Settings of DLDP

Parameter	Default Setting
Global Config	

Parameter	Default Setting
DLDP State	Disable
Adver Interval	5 seconds
Shut Mode	Auto
Web Refresh State	Disable
Web Refresh Interval	5 seconds
Port Config	
DLDP State	Disable

Part 29

Configuring SNMP & RMON

CHAPTERS

1. SNMP Overview
2. SNMP Configurations
3. Notification Configurations
4. RMON Overview
5. RMON Configurations
6. Configuration Example
7. Appendix: Default Parameters

1 SNMP Overview

SNMP (Simple Network Management Protocol) is a standard network management protocol, widely used on TCP/IP networks. It facilitates device management using NMS (Network Management System) software. With SNMP, network managers can view or modify network device information, and troubleshoot according to notifications sent by those devices in a timely manner.

The device supports three SNMP versions: SNMPv1, SNMPv2c and SNMPv3.*Table 1-1* lists features supported by different SNMP versions, and *Table 1-2* shows corresponding application scenarios.

Table 1-1 Features Supported by Different SNMP Versions

Feature	SNMPv1	SNMPv2c	SNMPv3
Access Control	Based on SNMP Community and MIB View	Based on SNMP Community and MIB View	Based on SNMP User, Group, and MIB View
Authentication and Privacy	Based on Community Name	Based on Community Name	Supported authentication and privacy modes are as follows: Authentication: MD5/SHA Privacy: DES
Trap	Supported	Supported	Supported
Inform	Not supported	Supported	Supported

Table 1-2 Application Scenarios of Different Versions

Version	Application Scenario
SNMPv1	Applicable to small-scale networks with simple networking, low security requirements or good stability (such as campus networks and small enterprise networks).
SNMPv2c	Applicable to medium and large-scale networks with low security requirements and those with good security (such as VPNs), but with busy services in which the traffic congestion may occur. You can configure Inform to ensure that the notifications from managed devices are received by network managers.
SNMPv3	Applicable to networks of various scales, particularly those that have high security requirements and require devices to be managed by authenticated administrators (such as when data needs to be transferred on public networks).

2 SNMP Configurations

To complete the SNMP configuration, choose an SNMP version according to network requirements and supportability of the NMS software, and then follow these steps:

- Choose SNMPv3

1) Enable SNMP.
2) Create an SNMP view for managed objects.
3) Create an SNMP group, and specify the access rights.
4) Create SNMP users, and configure the authentication mode, privacy mode and corresponding passwords.

- Choose SNMPv1 or SNMPv2c

1) Enable SNMP.
2) Create an SNMP view for managed objects.
3) Direct configuration: Create a community, specify the accessible view and the corresponding access rights.

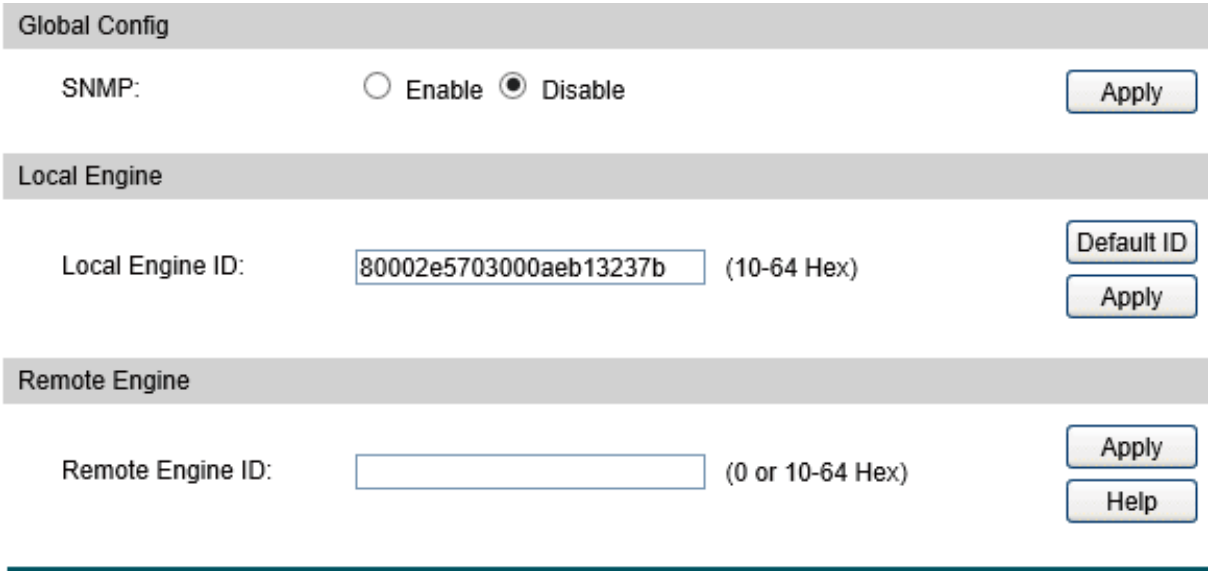
   Indirect configuration: See steps 3) and 4) of *Choose SNMPv3*. In this situation, the user name functions as the community name, and the Read/Write View is the same for the user and the group.

2.1 Using the GUI

2.1.1 Enabling SNMP

Choose the **SNMP > SNMP Config > Global Config** to load the following page.

Figure 2-1 Global Config



Follow these steps to configure SNMP globally:

1) In the **Global Config** section, enable SNMP. Click **Apply**.
2) In the **Local Engine** section, configure the local engine ID. Click **Apply**.

Local Engine ID	Set the ID of the local SNMP Agent with 10 to 64 hexadecimal digits. The local engine ID is a unique alphanumeric string used to identify the SNMP engine on the switch.

3) In the **Remote Engine** section, configure the remote engine ID. Click **Apply**.

Remote Engine ID	Set the ID of the remote SNMP manager with 10 to 64 hexadecimal digits. If no remote SNMP manager is needed, you can leave this field empty. The remote engine ID is a unique alphanumeric string. It is used to identify the SNMP engine on the remote device thats receives inform messages from Switch.

Note:

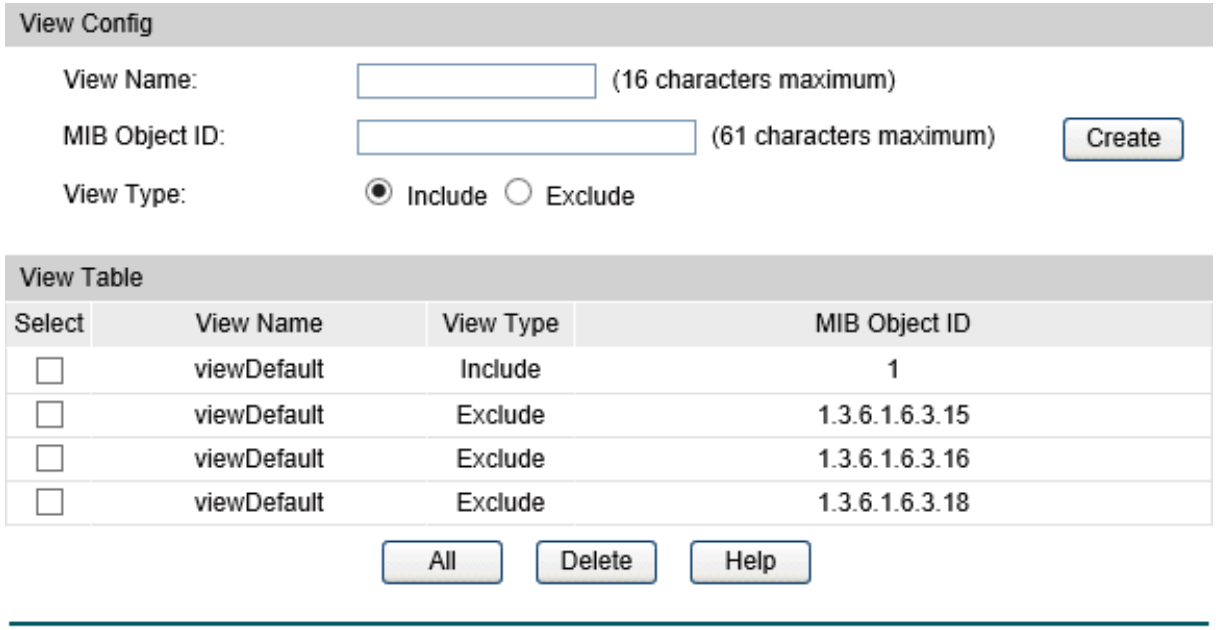
The engine ID must contain an even number of characters.

2.1.2 Creating an SNMP View

Create an SNMP view, and configure the content of the view. NMS (Network Management System) manages MIB (Management Information Base) variables based on the SNMP view.

Choose the menu **SNMP > SNMP Config > SNMP View** to load the following page.

Figure 2-2 SNMP View



Set the view name and one MIB variable that is related to the view. Choose the view type and click **Create** to add the view entry.

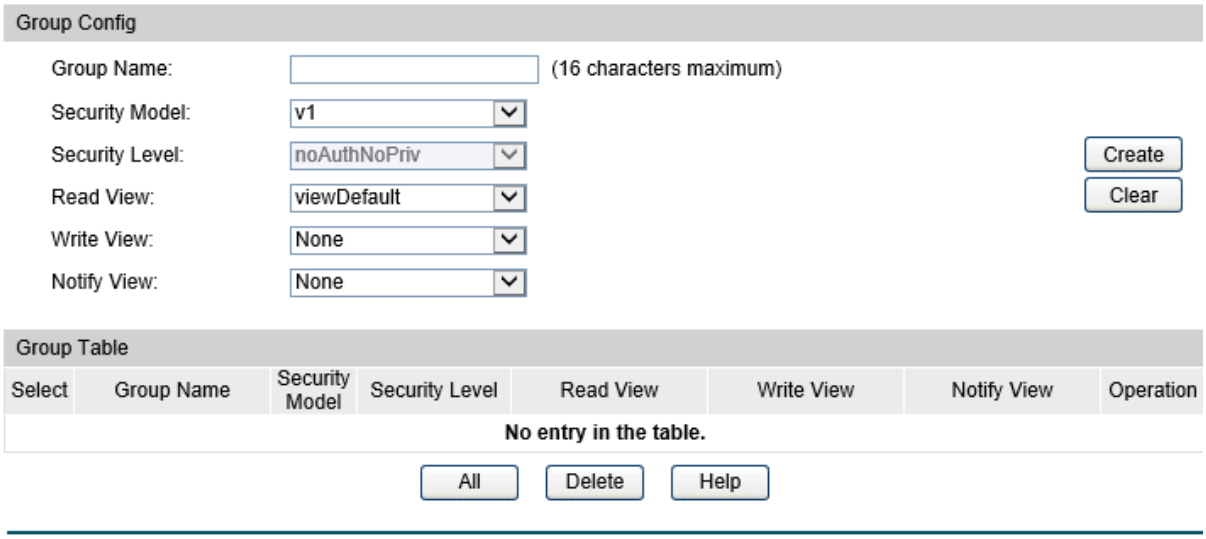
View Name	Set the view name with 1 to 16 characters. A complete view consists of all MIB objects that have the same view name.
MIB Object ID	Enter a MIB Object ID to specify a specific function of the device. For specific ID rules, refer to the device related MIBs.
View Type	Set the view to include or exclude the related MIB object. By default, it is included. **Include:** The NMS can view or manage the function indicated by the object. **Exclude:** The NMS cannot view or manage the function indicated by the object.

2.1.3 Creating an SNMP Group

Create an SNMP group and configure related parameters.

Choose the menu **SNMP > SNMP Config > SNMP Group** to load the following page.

Figure 2-3 SNMP Group



Follow these steps to create an SNMP Group:

1) Set the group name and security model. If you choose SNMPv3 as the security model, you need to further configure security level.

Group Name	Set the SNMP group name. You may enter 1 to 16 characters. The identifier of a group consists of a group name, security model and security level. Groups of the same identifier are recognized as being in the same group.
Security Model	Choose the corresponding SNMP version of the security model. By default, it is SNMPv1. **v1:** The security model of the group is SNMPv1. In this mode, community name match is used for authentication. You can configure the community name on the SNMP community page. **v2c:** The security model of the group is SNMPv2. In this mode, community name match is used for authentication. You can configure the community name on the SNMP community page. **v3:** The security model of the group is SNMPv3. In this mode, USM (User-Based Security Model) is used for authentication.
Security Level	Set the security level which for the SNMPv3 group. The default is noAuthNoPriv. **noAuthNoPriv:** No authentication mode or privacy mode is applied to check or encrypt packets. **authNoPriv:** An authentication mode is applied to check packets, but no privacy mode is applied to encrypt them. **authPriv:** An authentication mode and a privacy mode are applied to check and encrypt packets.

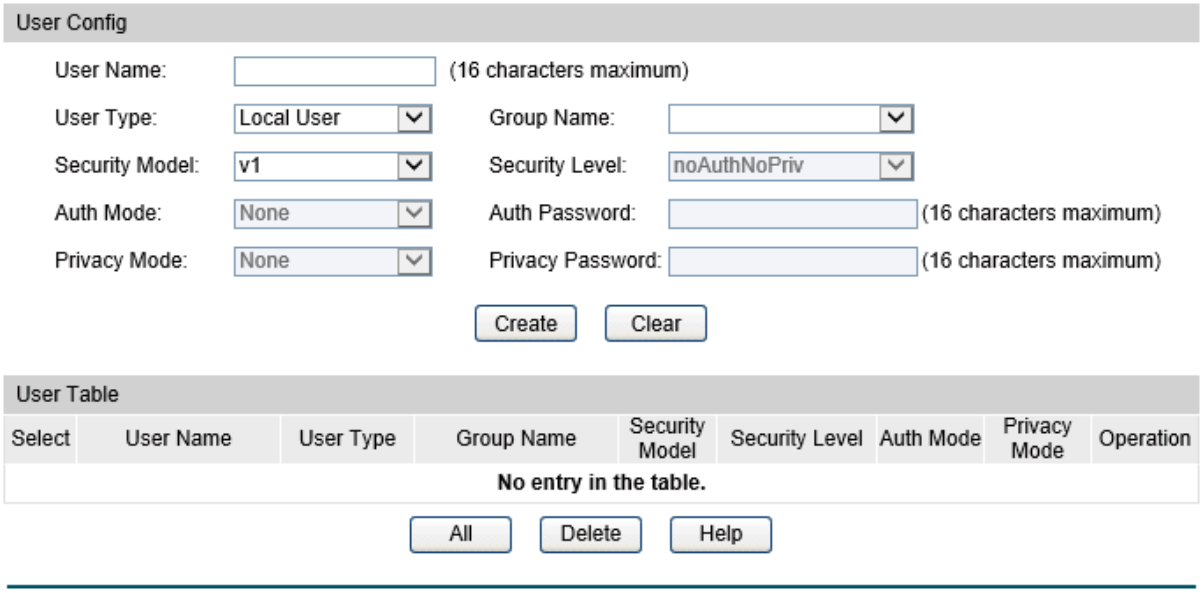
2) Set the read, write and notify view of the SNMP Group. Click **Create**.

Read View	Choose a view to allow parameters to be viewed but not modified by the NMS. The view is necessary for any group. By default, the view is viewDefault. To modify parameters of a view, you need to add it to Write View.
Write View	Choose a view to allow parameters to be modified but not viewed by the NMS. The default is none. The view in Write View should also be added to Read View.
Notify View	Choose a view to allow it to send notifications to the NMS.

2.1.4 Creating SNMP Users

Choose the menu **SNMP > SNMP Config > SNMP User** to load the following page.

Figure 2-4 SNMP User



Follow these steps to create an SNMP user:

1) Specify the user name, user type and the group which the user belongs to. Set the security model according to the related parameters of the specified group. If you choose SNMPv3, you need to configure the security level.

User Name	Set the SNMP user name. You may use 1 to 16 characters. For different entries, user names cannot be the same.
User Type	Choose a user type to indicate the location of the user. The default is Local User. **Local User:** The user resides on the local engine, which is the SNMP Agent of the switch. **Remote User:** The user resides on a remote engine, which is the SNMP Agent of some other device. For this user type, you need to set the remote engine ID first.
Group Name	Choose the group that the user belongs to. Users with the same Group Name, Security Model and Security Level will be in the same group.

Security Model	Choose the SNMP version of the security model. The default is SNMPv1. The setting should be identical with that of the specified group. **v1:** The group's security model is SNMPv1. **v2c:** In this mode, Community Name is used for authentication. You can configure Community Name on the SNMP Community. **v3:** The group's security model is SNMPv3.
Security Level	Set the security level for the SNMPv3 group. The default is noAuthNoPriv. **noAuthNoPriv:** No authentication mode or privacy mode is applied to check or encrypt packets. **authNoPriv:** An authentication mode is applied to check packets, but no privacy mode is applied to encrypt them. **authPriv:** An authentication mode and a privacy mode are applied to check and encrypt packets.

2) If you have chosen **authNoPriv** or **authPriv** as the security level, you need to set corresponding Auth Mode or Privacy Mode. If not, skip the step.

Auth Mode	If you have chosen authNoPriv as the security level, you need to set Auth Mode, which is None by default. **MD5:** Enable the HMAC-MD5 algorithm for authentication. **SHA:** Enable the SHA (Secure Hash Algorithm) algorithm for authentication. SHA algorithm is securer than MD5 algorithm.
Auth Password	Set the password for authentication.
Privacy Mode	If you have chosen authPriv as the security level, you need to set both Auth Mode and Privacy Mode. The privacy mode is None by default. **DES:** Enable the DES (Data Encryption Standard) algorithm for privacy.
Privacy Password	Set the password for encryption.

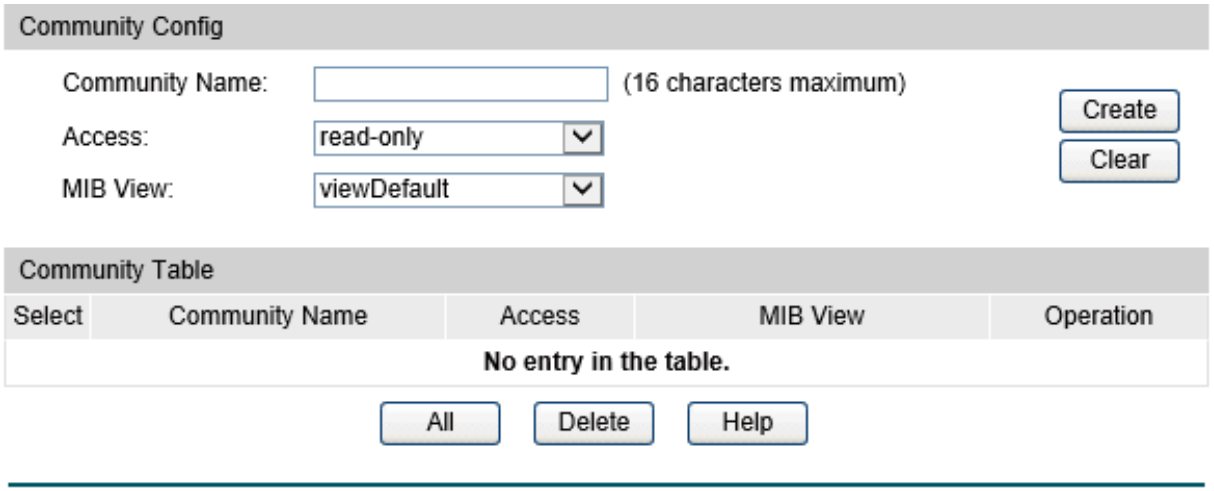
3) Click **Create**.

2.1.5 Creating SNMP Communities

If you want to use SNMPv1 or SNMPv2c as the security model, you can create SNMP communities directly.

Choose the menu **SNMP > SNMP Config > SNMP Community** to load the following page.

Figure 2-5 SNMP Community



Set the community name, access rights and the related view. Click **Create**.

Community Name	Set the community name with 1 to 16 characters. For SNMPv1 and SNMPv2c, the community name match is used for authentication.
Access	Specify the access right to the related view. The default is read-only. **read-only:** The NMS can view but not modify parameters of the specified view. **read-write:** The NMS can view and modify parameters of the specified view.
MIB View	Choose a view to allow it to be accessed by the community. The default is viewDefault.

2.2 Using the CLI

2.2.1 Enabling SNMP

Step 1	**configure** Enter global configuration mode.
Step 2	**snmp-server** Enabling SNMP.

Step 3	**snmp-server engineID** {[**local** *local-engineID*] [**remote** *remote-engineID*]} (Optional) Configure the local engine ID and the remote engine ID. *local-engineID:* Enter the local engine ID with 10 to 64 hexadecimal digits. The ID must contain an even number of characters. It is a unique alphanumeric string, used to identify the SNMP engine on the switch. *remote-engineID:* Enter the remote engine ID with 10 to 64 hexadecimal digits. The ID must contain an even number of characters. The remote engine ID is a unique alphanumeric string. It is used to identify the SNMP engine on the remote device that receives inform messages from Switch. Note that the switch will automatically generate a local engine ID if the ID is not set or is deleted.
Step 4	**show snmp-server** Displays the global settings of SNMP.
Step 5	**show smnp-server engineID** Displays the engine ID of SNMP.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable SNMP and set 123456789a as the remote engine ID:

Switch#configure

Switch(config)#snmp-server

Switch(config)#snmp-server engineID remote 123456789a

Switch(config)#show snmp-server

SNMP agent is enabled.

0 SNMP packets input

0 Bad SNMP version errors

0 Unknown community name

0 Illegal operation for community name supplied

0 Encoding errors

0 Number of requested variables

0 Number of altered variables

0 Get-request PDUs

0 Get-next PDUs

0 Set-request PDUs

0 SNMP packets output

0 Too big errors(Maximum packet size 1500)

0 No such name errors

0 Bad value errors

0 General errors

0 Response PDUs

0 Trap PDUs

Switch(config)#show snmp-server engineID

Local engine ID : 80002e5703000aeb132397

Remote engine ID: 123456789a

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Creating an SNMP View

Specify the OID (Object Identifier) of the view to determine objects to be managed.

Step 1	**configure** Enter global configuration mode.
Step 2	**snmp-server view** *name mib-oid* {include | exclude} Configure the view. *name :* Enter a view name with 1 to 16 characters.You can create multiple entries with each associated to a MIB object. A complete view consists of all MIB objects that have the same view name. *mib-oid :* Enter the MIB object ID with 1 to 61 characters. include|exclude : Specify a view type. Include indicates that objects of the view can be managed by the NMS, while exclude indicates that objects of the view cannot be managed by the NMS.
Step 3	**show snmp-server view** Displays the view table.
Step 4	**end** Return to Privileged EXEC Mode.

Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set a view to allow the NMS to manage all function. Name the view as View:

Switch#configure

Switch(config)#snmp-server view View 1 include

Switch(config)#show snmp-server view

No.	View Name	Type	MOID
---	----------	-------	----
1	viewDefault	include	1
2	viewDefault	exclude	1.3.6.1.6.3.15
3	viewDefault	exclude	1.3.6.1.6.3.16
4	viewDefault	exclude	1.3.6.1.6.3.18
5	View	include	1

Switch(config)#end

Switch#copy running-config startup-config

2.2.3 Creating an SNMP Group

Create an SNMP group and set user access control with read, write and notify views. Meanwhile, set the authentication and privacy modes to secure the communication between the NMS and managed devices.

Step 1	**configure** Enter global configuration mode.

Step 2	**snmp-server group** *name* [**smode** {v1 | v2c | v3}] [**slev** {noAuthNoPriv | authNoPriv | authPriv}] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] Set an SNMP group. *name :* Enter the group name with 1 to 16 characters. The identifier of a group consists of a group name, security model and security level. Groups of the same identifier are recognized as being in the same group. *v1 | v2c | v3 :* Choose a security mode for the SNMP group from the following: SNMPv1, SNMPv2c, SNMPv3. The default is v1. *noAuthNoPriv | authNoPriv | authPriv :* For groups of SNMPv3, choose a security level among noAuthNoPriv (no authorization and no encryption), authNoPriv (authorization and no encryption), authPriv (authorization and encryption). The default is noAuthNoPriv. Please note that if you have chosen v1 or v2c as the security mode, the security level cannot be configured. *read-view :* Set the view as read-only. And then the NMS can view parameters of the specified view. *write-view :* Set the view as write-only. And then the NMS can modify parameters of the specified view. Please note that the view in write-view should also be in read-view. *notify-view :* Set the view as notify-only view. And then the NMS can get notifications of the specified view from the agent.
Step 3	**show snmp-server group** Displays SNMP group entries.
Step 4	**end** Return to Privileged EXEC Mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create an SNMPv3 group. Name the group as nms-monitor, enable Auth Mode and Privacy Mode, and set the view as read View and notify View:

Switch#configure

Switch(config)#snmp-server group nms-monitor **smode** v3 **slev** authPriv **read** View **notify** View

Switch(config)#show snmp-server group

No.	Name	Sec-Mode	Sec-Lev	Read-View	Write-View	Notify-View
1	nms-monitor	v3	authPriv	View		View

Switch(config)#end

Switch#copy running-config startup-config

2.2.4 Creating SNMP Users

Configure users of the SNMP group. Users belong to the group, and use the same security level and access rights as the group.

Step 1	**configure** Enter global configuration mode.
Step 2	**snmp-server user** *name* { local | remote } *group-name* [**smode** { v1 | v2c | v3 }] [**slev** { noAuthNoPriv | authNoPriv | authPriv }] [**cmode** { none | MD5 | SHA }] [**cpwd** *confirm-pwd*] [**emode** { none | DES }] [**epwd** *encrypt-pwd*] Configure users of the SNMP group. *name :* Enter the user name with 1 to 16 characters. *local | remote :* Choose a user type. Local indicates that the user is connected to a local SNMP engine, while remote means that the user is connected to a remote SNMP engine. *group-name :* Enter the name of the group which the user belongs to. The group is determined by the group name, security mode and security level. *v1 | v2c | v3 :* Choose a security mode for the SNMP group from the following: SNMPv1, SNMPv2c, SNMPv3. *noAuthNoPriv | authNoPriv | authPriv :* For SNMPv3 groups, choose a security level from noAuthNoPriv (no authorization and no encryption), authNoPriv (authorization and no encryption), authPriv (authorization and encryption). The defaut is noAuthNoPriv. Please note that if you have chosen v1 or v2c as the security mode, security level cannot be configured. *none | MD5 | SHA :* Choose an authentication algorithm which is only for the user of SNMPv3. SHA authentication mode has a higher security than MD5 mode. By default, the Authentication Mode is none. *confirm-pwd :* Enter an authentication password with 1 to 16 characters excluding question mark and space. This password in the configuration file will be displayed in the symmetric encrypted form. *none | DES :* Choose a privacy mode which is only for the user of SNMPv3. None indicates no privacy method is used, and DES indicates DES encryption method is used. By default, the Privacy Mode is none. Please note that if you have chosen v1 or v2c as the security mode, the privacy mode cannot be configured. *encrypt-pwd :* Enter a privacy password with 1 to 16 characters excluding question mark and space. This password in the configuration file will be displayed in the symmetric encrypted form.
Step 3	**show snmp-server user** Displays the information of SNMP users.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create an SNMP user on the switch. Name the user as admin, and set the user as a remote user, SNMPv3 as the security mode, authPriv as the

security level, SHA as the authentication algorithm, 1234 as the authentication password, DES as the privacy algorithm and 1234 as the privacy password:

Switch#configure

Switch(config)#snmp-server user admin remote nms-monitor **smode** v3 **slev** authPriv **cmode** SHA **cpwd** 1234 **emode** DES **epwd** 1234

Switch(config)#show snmp-server user

No.	U-Name	U-Type	G-Name	S-Mode	S-Lev	A-Mode	P-Mode
1	admin	remote	nms-monitor	v3	authPriv	SHA	DES

Switch(config)#end

Switch#copy running-config startup-config

2.2.5 Creating SNMP Communities

For SNMPv1 and SNMPv2c the Community Name is used for authentication, functioning as the password.

Step 1	**configure** Enter global configuration mode.
Step 2	**snmp-server community** *name* { read-only | read-write } *mib-view* Configure the community. *name:* Enter a group name with 1 to 16 characters. *read-only | read-write:* Choose an access permissions for the community. Read-only indicates that the NMS can view but cannot modify parameters of the view, while read-write indicates that the NMS can both view and modify. *mib-view:* Enter a view to allow it to be accessed by the community. The name contains 1 to 61 characters.
Step 3	**show snmp-server community** Displays community entries.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set an SNMP community. Name the community as the nms-monitor, and allow the NMS to view and modify parameters of View:

Switch#configure

Switch(config)#snmp-server community nms-monitor read-write View

Switch(config)#show snmp-server community

Index	Name	Type	MIB-View
-----	----------	----------	--------
1	nms-monitor	read-write	View

Switch(config)#end

Switch#copy running-config startup-config

3 Notification Configurations

With Notification enabled, the switch can send notifications to the NMS about important events relating to the device's operation. This facilitates the monitoring and management of the NMS.

Configuration Guidelines

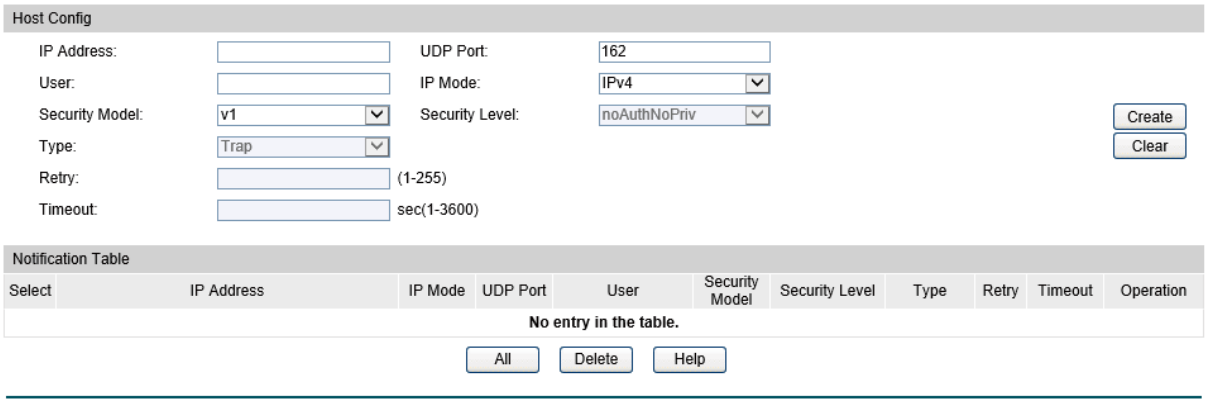
- To guarantee the communication between the switch and the NMS, ensure the switch and the NMS are able to reach one another.

- Some SNMP extended traps can be configured only with CLI. If needed, please refer to *(Optional) Enabling the SNMP Extended trapap*, *(Optional) Enabling the DDM Trap*, and *(Optional) Enabling the Link-status Trap*.

3.1 Using the GUI

Choose the menu **SNMP > Notification > Notification Config** to load the following page.

Figure 3-1 Notification Config



Follow these steps to configure notification:

1) Specify the IP address of the host, the UDP port that sends notifications, and choose the IP mode according to the network environment.

IP Address	If you set the **IP Mode** to IPv4, specify an IPv4 address for the host. If you set the **IP Mode** to IPv6, specify an IPv6 address for the host..
UDP Port	Specify a UDP port on the host to send notifications. The default is port 162. For communication security, we recommend that you change the port number under the condition that communications on other UDP ports are not affected.

IP Mode	Choose an IP mode for the host, which should be coordinated with the IP Address.

2) Specify the user name or community name used by the NMS, and configure the security model and security level based on the settings of the user or community.

User Name	Specify the user name or community name used by the NMS.
Security Model	Choose the corresponding SNMP version for the NMS. The version should be consistent with settings of the user or community. v1: The NMS uses SNMPv1. v2: The NMS uses SNMPv2c. v3: The NMS uses SNMPv3.
Security Level	Choose the security level for the NMS that uses SNMPv3. The setting should be consistent with that of the specified user or community. noAuthNoPriv: No authentication mode or privacy mode is applied to check or encrypt packets. authNoPriv: An authentication mode is applied to check packets, but no privacy mode to encrypt packets. authPriv: An authentication mode and a privacy mode are applied to check and encrypt packets.

3) Choose a notification type based on the SNMP version. If you choose the Inform type, you need to set retry times and timeout interval.

Type	Choose a notification type for the NMS that uses SNMPv2c or SNMPv3; the default type is Trap. Trap: Set the switch to send Trap messages to the NMS. When the NMS receives a trap message, it will not send a response to the switch. Thus the switch cannot determine whether the trap is received or not, and the trap that is not received will not be resent. Inform: Set the switch to send Inform messages to the NMS. When the NMS receives an Inform message, it sends a response to the switch. If the switch does not receive a response within the Timeout interval, it will resend the Inform message. Therefore, Informs are more reliable than Traps.
Retry	Set the retry times for Informs; the default is 3. The switch will resend the Inform message if it does not receive response from the NMS within the timeout interval. It will stop sending Inform messages when the retry time reaches the limit.
Timeout	Set the length of time that the switch waits for a response from the NMS after sending an inform message; the default is 100 seconds. Set the length of time that the switch waits for a response from the NMS after sending an inform message; the default is 100 seconds.

4) Click **Create**.

3.2 Using the CLI

3.2.1 Configuring the Host

Configure parameters of the NMS host and packet handling mechanism.

Step 1	**configure** Enter global configuration mode.
Step 2	**snmp-server host** *ip udp-port user-name* [**smode** { v1 | v2c | v3 }] [**slev** {noAuthNoPriv | authNoPriv | authPriv }] [**type** { trap | inform}] [**retries** *retries*] [**timeout** *timeout*] Configure parameters of the NMS host and packet handling mechanism. *ip:* Specify the IP address of the NMS Host in IPv4 or IPv6. Please make sure the IP addresses of the Host and the switch are able to reach to each other. *udp-port:* Specify a UDP port on the host to send notifications. The default is port 162. For communication security, we recommend that you change the port number under the condition that communications on other UDP ports are not affected. *user-name:* Enter the name used by the NMS. When the NMS uses SNMPv1 or SNMPv2c, enter the Community Name; when the NMS uses SNMPv3, enter the User Name of the SNMP Group. *v1 | v2c | v3 :* Choose a security mode for the SNMP group from the following: SNMPv1, SNMPv2c, SNMPv3. *noAuthNoPriv | authNoPriv | authPriv:* For SNMPv3 groups, choose a security level from noAuthNoPriv (no authorization and no encryption), authNoPriv (authorization and no encryption), authPriv (authorization and encryption). The defaut is noAuthNoPriv. Please note that if you have chosen v1 or v2c as the security mode, security level cannot be configured. *trap | inform:* Choose the information type which is only for SNMPv2c or SNMPv3; the default is trap. When the NMS receives a trap message, it will not send a response to the switch. Thus the switch cannot determine whether the trap is received or not, and the trap that is not received will not be resent. When the NMS receives an Inform message, it will send a response to the switch. If the switch does not receive a response within the Timeout interval, it will resend the Inform message. Therefore, Informs are more reliable than Traps. *retries :* Set the retry times for Inform messages. The range is 1 to 255 and the default is 3. The switch will resend the Inform message if it does not receive response from the NMS within the timeout interval. And it will stop sending Inform message when the retry times reaches the limit. *timeout :* Set the length of time that the switch waits for a response. The range is 1 to 3600 seconds; the default is 100 seconds. The switch will resend the Inform message if it does not receive a response from the NMS within the timeout interval.
Step 3	**show snmp-server host** Displays the information of the host.
Step 4	**end** Return to privileged EXEC mode.

Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set the NMS host IP address as 172.168.1.222, UDP port as port 162, name used by the NMS as admin, security model as SNMPv3, security level as authPriv, notification type as Inform, retry times as 3, and the timeout interval as 100 seconds:

Switch#configure

Switch(config)#snmp-server host 172.168.1.222 162 admin **smode** v3 **slev** authPriv **type** inform **retries** 3 **timeout** 100

Switch(config)#show snmp-server host

No.	Des-IP	UDP	Name	SecMode	SecLev	Type	Retry	Timeout
---	------	-----	----	-------	------	----	-----	-------
1	172.168.1.222	162	admin	v3	authPriv	inform	3	100

Switch(config)#end

Switch#copy running-config startup-config

3.2.2 Enabling SNMP Notification

- Enabling the SNMP Standard Trap

Step 1	**configure** Enter global configuration mode.
Step 2	**snmp-server traps snmp [** linkup | linkdown | warmstart | coldstart | auth-failure **]** Configure parameters of basic traps supported on the switch. *linkup:* When a port status changes from linkdown to linkup, the switch sends a linkup trap. The trap is enabled by default. And the trap can be triggered when you connect a device to a port. *linkdown:* When a port status changes from linkup to linkdown, the switch sends a linkdown trap. The trap is enabled by default and can be triggered when you disconnect the device from the port. *warmstart:* The trap indicates the SNMP feature on the switch is reinitialized with the physical configuration unchanged. The trap is enabled by default and can be triggered if you disable and then enable SNMP after the SNMP is completely configured and enabled. *coldstart:* The trap indicates an SNMP initialization caused by the reinitialization of the switch system. The trap is enabled by default. The trap can be triggered when you reboot the switch. *auth-failure:* The switch will send the trap when the SNMP request fails in authentication. The trap is enabled by default.

Step 3	**end** Return to privileged EXEC mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the switch to send linkup traps:

Switch#configure

Switch(config)#snmp-server traps snmp linkup

Switch(config)#end

Switch#copy running-config startup-config

- (Optional) Enabling the SNMP Extended trap

Step 1	**configure** Enter global configuration mode.

Step 2	**snmp-server traps** { bandwidth-control | cpu | flash | lldp remtableschange | lldp topologychange | loopback-detection | storm-control | spanning-tree | memory } Configure parameters of extended traps supported on the switch. bandwidth-control: The trap is used to monitor whether the bandwidth has reached the limit that you have set. The trap is disabled by default. The trap can be triggered when the feature is enabled and packets are sent to the port with a rate higher than what you have set. cpu: The trap is used to monitor the load status of the switch CPU. And the trap is disabled by default. 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: The trap is used to monitor whether the flash is modified. And the trap is disabled by default. The trap can be triggered when the flash is modified by saving configurations, factory resetting, upgrading and importing configurations. lldp remtableschange: A lldp RemTablesChange notification is sent when the value of lldp StatsRemTableLastChangeTime changes. It can be utilized by an NMS 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%.
Step 3	**end** Return to privileged EXEC mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the switch to enable bandwidth-control traps:

Switch#configure

Switch(config)#snmp-server traps bandwidth-control

Switch(config)#end

Switch#copy running-config startup-config

(Optional) Enabling the DDM Trap

Step 1	**configure** Enter global configuration mode.
Step 2	**snmp-server traps DDM** [create | delete] Enable SNMP extended DDM-related traps. create: Enable DDM-created trap. It is sent when new DDM is created successfully. By default, it is disabled. delete: Enable DDM-deleted trap. It is sent when DDM is deleted successfully. By default, it is disabled.
Step 3	**end** Return to privileged EXEC mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the switch to enable DDM-created trap:

Switch#configure

Switch(config)#snmp-server traps DDM create

Switch(config)#end

Switch#copy running-config startup-config

(Optional) Enabling the DDM Trap

Step 1	**configure** Enter global configuration mode.
Step 2	**snmp-server traps ddm** [temperature | voltage | bias_current | tx_power | rx_power] Enable SNMP DDM traps. DDM function is used to monitor the status of the SFP modules inserted into the SFP ports on the switch. temperature: Enable DDM Temperature trap. It is sent when the DDM temperature value exceeds the alarm threshold or warning threshold. voltage: Enable DDM Voltage trap. It is sent when the DDM voltage value exceeds the alarm threshold or warning threshold. bias_current: Enable DDM Bias Current trap. It is sent when the DDM bias current value exceeds the alarm threshold or warning threshold. tx_power: Enable DDM Tx Power trap. It is sent when the DDM Tx power value exceeds the alarm threshold or warning threshold. rx_power: Enable DDM Rx Power trap. It is sent when the DDM Rx power value exceeds the alarm threshold or warning threshold.

Step 3	**end** Return to privileged EXEC mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the switch to enable all the SNMP DDM trap:

Switch#configure

Switch(config)#snmp-server traps DDM

Switch(config)#end

Switch#copy running-config startup-config

- (Optional) Enabling the Illegal DHCP Server Trap

Step 1	**configure** Enter global configuration mode.
Step 2	**snmp-server traps security dhcp-snoop** Enable illegal DHCP server trap to send SNMP trap message when untrusted port has received DHCP Server packets.
Step 3	**end** Return to privileged EXEC mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the switch to enable illegal DHCP server trap:

Switch#configure

Switch(config)#snmp-server traps security dhcp-snoop

Switch(config)#end

Switch#copy running-config startup-config

- (Optional) Enabling the Link-status Trap

Step 1	**configure** Enter global configuration mode.

Step 2	**interface {fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Configure notification traps on the specified ports. *port/port-list:* The number or the list of the Ethernet ports that you desire to configure notification traps.
Step 3	**snmp-server traps link-status** Enable SNMP extended linkup and linkdown traps. By default, it is disabled.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the switch to enable link-status trap:

Switch#configure

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

Switch(config-if)#snmp-server traps link-status

Switch(config-if)#end

Switch#copy running-config startup-config

4 RMON Overview

RMON (Remote Network Monitoring) together with the SNMP system allows the network manager to monitor remote network devices efficiently. RMON reduces traffic flow between the NMS and managed devices, which is convenient for management in large networks.

RMON includes two parts: the NMS and the Agents running on every network device. The NMS is usually a host that runs the management software to manage Agents of network devices. And the Agent is usually a switch or router that collects traffic statistics (such as total packets on a network segment during a certain time period, or total correct packets that are sent to a host). Based on SNMP protocol, the NMS collects network data through communication with Agents. However, the NMS cannot obtain every datum of RMON MIB because of the limited device resources. Generally, the NMS can only get information of the following four groups: statistics, history, event and alarm.

5 RMON Configurations

With RMON configurations, you can:

- Configuring the statistics group.
- Configuring the history group.
- Configuring the event group.
- Configuring the alarm group.

Configuration Guidelines

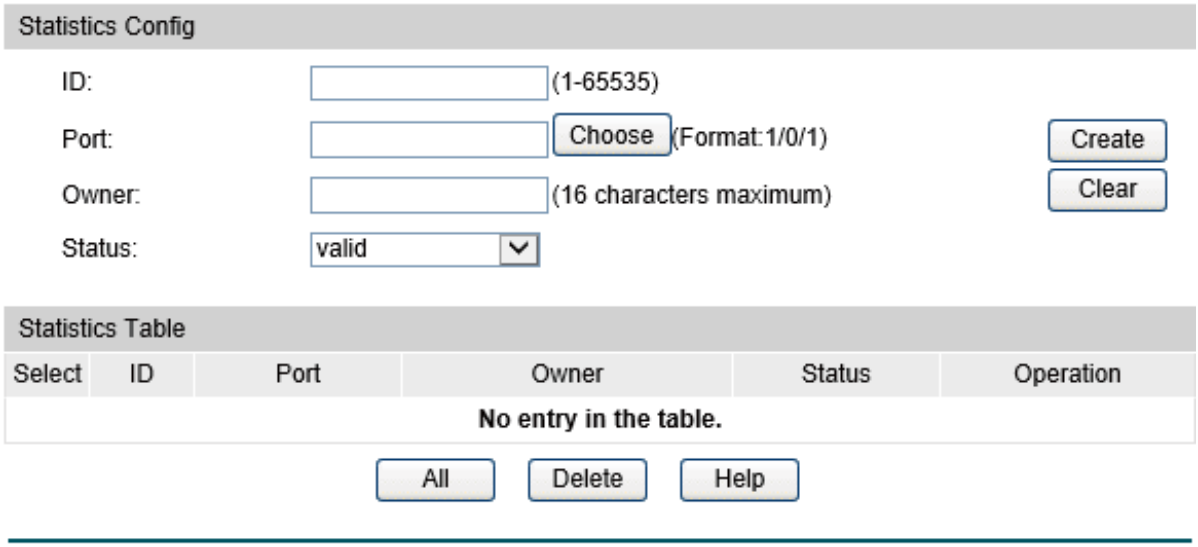
To ensure that the NMS receives notifications normally, please complete configurations of SNMP and SNMP Notification before RMON configurations.

5.1 Using the GUI

5.1.1 Configuring Statistics

Choose the menu **SNMP > RMON > Statistics** to load the following page.

Figure 5-1 Statistics Config



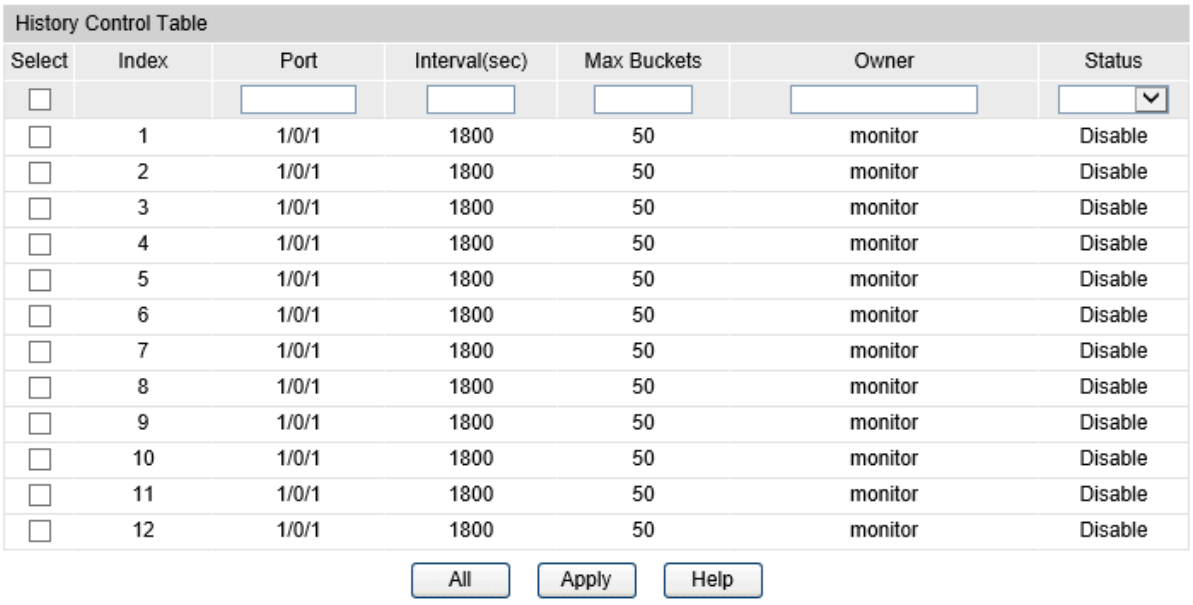
Specify the entry ID, the port to be monitored, and the owner name of the entry. Set the entry as valid or underCreation, and click **Create**.

ID	Enter the ID of the entry.
Port	Click **Choose** to specify an Ethernet port to be monitored in the entry, or enter the port number in the format of 1/0/1.
Owner	Enter the owner name of the entry with1 to 16 characters.
Status	Set the entry as valid or underCreation. By default, it is valid. Valid: The entry is created and valid. underCreation: The entry is created but invalid.

5.1.2 Configuring History

Choose the menu **SNMP > RMON > History** to load the following page.

Figure 5-2 History Control Table



Follow these steps to configure history:

1) Select a history entry, and specify a port to be monitored.

Index	Displays the index of history entries. There are 12 history entries all together.
Port	Specify a port in 1/0/1 format to be monitored. To change the port, please enable the entry first.

2) Set the sample interval and the maximum buckets of history entries.

Interval	Set the sample interval from 10 to 3600 seconds; the default is 1800 seconds. Every history entry has its own timer. For the monitored port, the switch collects packet information and generates a record in every interval.
Max Buckets	Set the maximum number of records for the history entry. When the number of records exceeds the limit, the earliest record will be overwritten. The ranges are from 10 to 130; the default is 50.

3) Enter the owner name, and set the status of the entry. Click **Apply**.

Owner	Enter the owner name of the entry with 1 to 16 characters. By default, it is monitor.
Status	Enable or disable the entry. By default, it is disabled. Enable: The entry is enabled. Disable: The entry is disabled.

5.1.3 Configuring Event

Choose the menu **SNMP > RMON > Event** to load the following page.

Figure 5-3 Event Table

Event Table

Select	Index	User	Description	Type	Owner	Status
☐						
☐	1	public		None	monitor	Disable
☐	2	public		None	monitor	Disable
☐	3	public		None	monitor	Disable
☐	4	public		None	monitor	Disable
☐	5	public		None	monitor	Disable
☐	6	public		None	monitor	Disable
☐	7	public		None	monitor	Disable
☐	8	public		None	monitor	Disable
☐	9	public		None	monitor	Disable
☐	10	public		None	monitor	Disable
☐	11	public		None	monitor	Disable
☐	12	public		None	monitor	Disable

All Apply Help

Follow these steps to configure event:

1) Choose an event entry, and set the SNMP User of the entry.

Index	Displays the index of event entries. There are 12 event entries all together.
User	Enter the SNMP user name or community name of the entry. The name should be what you have set in SNMP previously. By default, it is public.

2) Set the description and type of the event.

Description	Give a description to the event.
Type	Specify the action type of the event; then the switch will take the specified action to deal with the event. By default, the type is None. None: No action. Log: The switch records the event in the log, and the NMS should initiate requests to get notifications. Notify: The switch initiates notifications to the NMS. Log&Notify: The switch records the event in the log and sends notifications to the NMS.

3) Enter the owner name, and set the status of the entry. Click **Apply**.

Owner	Enter the owner name of the entry with 1 to 16 characters. By default, it is monitor.
Status	Enable or disable the entry. By default, it is disabled. Enable: The entry is enabled. Disable: The entry is disabled.

5.1.4 Configuring Alarm

Before you begin, please complete configurations of Statistics entries and Event entries, because the Alarm entries must be associated with Statistics and Event entries.

Choose the menu **SNMP > RMON > Alarm** to load the following page.

Figure 5-4 Alarm Config



Follow these steps to configure alarm:

1) Select an alarm entry, choose a variable to be monitored, and associate the entry with a statistics entry.

Index	Displays the index of alarm entries. There are 12 alarm entries all together.

Variable	Set the alarm variable to be monitored. The switch will monitor the specified variable in sample intervals and act in the set way when the alarm is triggered. The default variable is RecBytes. RecBytes: Total received bytes. RecPackets: Total received packets. BPackets: Total broadcast packets. MPackets: Total multicast packets. CRC&Align ERR: Packets that range from 64 to 1518 bytes and contain FCS Error or Alignment Error. Undersize: Packets that are smaller than 64 bytes. Oversize: Packets that are larger than 1518 bytes. Jabbers: Packets that are sent when port collisions occur. Collisions: Collision times in the network segment. 64, 65-127, 128-255, 256-511, 512-1023, 1024-10240: Total packets of the specified size.
Statistics	Associate the alarm entry with a statistics entry. Then the switch monitors the specified variable of the statistics entry.

2) Set the sample type, the rising and falling threshold, the corresponding event action, and the alarm type of the entry.

Sample Type	Set the sampling method of the specified variable; the default is absolute. Absolute: Compare the sampling value against the preset threshold. Delta: The switch obtains the difference between the sampling values of the current interval and the previous interval, and then compares the difference against the preset threshold.
Rising Threshold	Set the rising threshold of the variable. When the sampled value exceeds the threshold, the system will trigger the corresponding **Rising Event**. The ranges are from 1 to 2147483647; the default is 100.
Rising Event	Specify the index of the event that will be triggered when the sampled value exceeds the preset threshold.
Falling Threshold	Set the falling threshold of the variable. When the sampled value is below the threshold, the system will trigger the corresponding **Falling Event**. The ranges are from 1 to 2147483647; the default is 100.
Falling Event	Specify the index of the event that will be triggered when the sampled value is below the preset threshold.

Alarm Type	Specify the alarm type for the entry. By default, the alarm type is all. Rising: The alarm is triggered only when the sampled value exceeds the rising threshold. Falling: The alarm is triggered only when the sampled value is below the falling threshold. All: The alarm is triggered when the sampled value exceeds the rising threshold or is below the falling threshold.

3) Enter the owner name, and set the status of the entry. Click **Apply**.

Owner	Enter the owner name of the entry with 1 to 16 characters. By default, it is monitor.
Status	Enable or disable the entry. By default, it is disabled. Enable: The entry is enabled. Disable: The entry is disabled.

5.2 Using the CLI

5.2.1 Configuring Statistics

Step 1	**configure** Enter global configuration mode.
Step 2	**rmon statistics** *index* **interface** {[**gigabitEthernet** *port*] [**ten-gigabitEthernet** *port*]} [**owner** *owner-name*] [**status** { underCreation | valid }] Configure RMON statistic entries. *index:* Enter the ID of the statistics entry from 1 to 65535 in the format of 1-3 or 5. *port:* Enter the port number in 1/0/1 format to bind it to the entry. *owner-name:* Enter the owner name of the entry with 1 to 16 characters. The default name is monitor. underCreation | valid: Enter the status of the entry. UnderCreation indicates that the entry is created but invalid, while valid indicates the entry is created and valid. By default, it is valid.
Step 3	**show rmon statistics** [*index*] Displays the statistics entries and their configurations. *index:* Enter the index of statistics entries that you want to view. The ranges are from 1 to 65535.
Step 4	**end** Return to privileged EXEC mode.

Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create two statistics entries on the switch to monitor port 1/0/1 and 1/0/2 respectively. The owner of the entry is monitor and the entry is valid:

Switch#configure

Switch(config)#rmon statistics 1 **interface gigabitEthernet** 1/0/1 **owner** monitor **status** valid

Switch(config)#rmon statistics 2 **interface gigabitEthernet** 1/0/2 **owner** monitor **status** valid

Switch(config)#show rmon statistics

Index	Port	Owner	State
-----	----	-----	-----
1	Gi1/0/1	monitor	valid
2	Gi1/0/2	monitor	valid

Switch(config)#end

Switch#copy running-config startup-config

5.2.2 Configuring History

Step 1	**configure** Enter global configuration mode.
Step 2	**rmon history** *index* **interface** { **fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* } [**interval** *seconds*] [**owner** *owner-name*] [**buckets** *number*] Configuring RMON history entries. *index:* Enter the index of the history entry from 1 to 12 in the format of 1-3 or 5. *port:* Enter the port number in 1/0/1 format to bind it to the entry. *seconds:* Set the sample interval. The values are from 10 to 3600 seconds; the default is 1800 seconds. *owner-name:* Enter the owner name of the entry with 1 to 16 characters. The default name is monitor. *number:* Set the maximum number of records for the history entry. When the number of records exceeds the limit, the earliest record will be overwritten. The values are from 10 to 130; the default is 50.

Step 3	**show rmon history** [*index*] Displays the specified history entry and related configurations. *index:* Enter the index of history entries that you want to view. The range is 1 to 12, and the format is 1-3 or 5.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create a history entry on the switch to monitor port 1/0/1. Set the sample interval as 100 seconds, max buckets as 50, and the owner as monitor:

Switch#configure

Switch(config)#rmon history 1 **interface gigabitEthernet** 1/0/1 **interval** 100 **owner** monitor **buckets** 50

Switch(config)#show rmon history

Index	Port	Interval	Buckets	Owner	State
1	Gi1/0/1	100	50	monitor	Enable

Switch(config)#end

Switch#copy running-config startup-config

5.2.3 Configuring Event

Step 1	**configure** Enter global configuration mode.

Step 2	**rmon event** *index* [**user** *user-name*] [**description** *description*] [**type** { none | log | notify | log-notify }] [**owner** *owner-name*] Configuring RMON event entries. *index:* Enter the index of the event entry from 1 to12 in the format of 1-3 or 5. *user-name:* Enter the SNMP user name or community name of the entry. The name should be what you have set in SNMP previously. The default name is public. *description:* Give a description to the entry with 1 to 16 characters. By default, the description is empty. none | log | notify | log-notify: Specify the action type of the event; then the switch will take the specified action to deal with the event. By default, the type is none. None indicates the switch takes no action, log indicates the switch records the event, notify indicates the switch sends notifications to the NMS, and log-notify indicates the switch records the event and sends notifications to the NMS. *owner-name:* Enter the owner name of the entry with 1 to 16 characters. The default name is monitor.
Step 3	**show rmon event** [*index*] Displays the specified event entry and related configurations. *index:* Enter the index of event entries that you want to view. The range is 1 to 12, and the format is 1-3 or 5.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to create an event entry on the switch. Set the user name as admin, the event type as Notify (set the switch to initiate notifications to the NMS), and the owner as monitor:

Switch#configure

Switch(config)#rmon event 1 **user** admin **description** rising-notify **type** notify **owner** monitor

Switch(config)#show rmon event

Index	User	Description	Type	Owner	State
1	admin	rising-notify	Notify	monitor	Enable

Switch(config)#end

Switch#copy running-config startup-config

5.2.4 Configuring Alarm

Step 1	**configure** Enter global configuration mode.
Step 2	**rmon alarm** *index* { **stats-index** *sindex* } [**alarm-variable** { revbyte | revpkt | bpkt | mpkt | crc-align | undersize | oversize | jabber | collision | 64 | 65-127 | 128-255 | 256-511 | 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*] Configuring RMON alarm entries. *index:* Enter the index of the alarm entry from 1 to12 in the format of 1-3 or 5. *sindex:* Set the index of the related statistics entry from 1 to 65535. *revbyte | revpkt | bpkt | mpkt | crc-align | undersize | oversize | jabber | collision | 64 | 65- 127 | 128-255 | 256-511 | 512-1023 | 1024-10240:* Choose an alarm variable to monitor. The switch will monitor the specified variable in sample intervals and act in the set way when the alarm is triggered. The default variable is revbyte. revbyte means total received bytes; revpkt means total received packets; bpkt means total broadcast packets. mpkt means total multicast packets; crc-align means packets that range from 64 to 1518 bytes and contain FCS Error or Alignment Error; undersize means packets that are smaller than 64 bytes; oversize means packets that are larger than 1518 bytes; jabber means packets that are sent when port collisions occur; collision means the collision times in the network segment; 64 | 65-127 | 128-255 | 256-511 | 512-1023 | 1024-10240 means total packets of the specified size. absolute | delta: Choose the sampling mode. The default is absolute. In the absolute mode, the switch compares the sampling value against the preset threshold; in the delta mode, the switch obtains the difference between the sampling values of the current interval and the previous interval, and then compares the difference against the preset threshold. *r-hold:* Enter the rising threshold from 1 to 2147483647; the default is 100. *r-event:* Enter the event entry index from 1 to 12 to bind it to the rising threshold. The event entry will be triggered when the sampling value exceeds the preset threshold. *f-hold:* Enter a falling threshold from 1 to 2147483647; the default is 100. *f-event:* Enter the event entry index from 1 to 12 to bind it to the falling threshold. The event entry will be triggered when the sampling value goes below the preset threshold. rise | fall | all: Choose an alarm type; the default is all. Rise indicates that the alarm is triggered only when the sampled value exceeds the rising threshold. Fall indicates that the alarm is triggered only when the sampled value is below the falling threshold. All indicates that the alarm is triggered when the sampled value exceeds the rising threshold or is below the falling threshold. *owner-name:* Enter the owner name of the entry using 1 to 16 characters. The default name is monitor. *interval:* Set the sampling interval. The value ranges from 10 to 3600 seconds; the default is 1800 seconds.

Step 3	**show rmon alarm** [*index*] Displays the specified alarm entry and related configurations. *index:* Enter the index of alarm entries that you want to view. The range is 1 to 12, and the format is 1-3 or 5.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set an alarm entry to monitor BPackets on the switch. Set the related Statistics entry ID as 1, the sample type as Absolute, the rising threshold as 3000, the related rising event entry index as 1, the falling threshold as 2000, the related falling event index as 2, the alarm type as all, the notification interval as 10 seconds, and the owner of the entry as monitor:

Switch#configure

Switch(config)#rmon alarm 1 **stats-index** 1 **alarm-variable** bpkt **s-type** absolute **rising-threshold** 3000 **rising-event-index** 1 **falling-threshold** 2000 **falling-event-index** 2 **a-type all interval** 10 **owner** monitor

Switch(config)#show rmon alarm

Index-State: 1-Enabled

Statistics index: 1

Alarm variable: BPkt

Sample Type: Absolute

RHold-REvent: 3000-1

FHold-FEvent: 2000-2

Alarm startup: All

Interval: 10

Owner: monitor

Switch(config)#end

Switch#copy running-config startup-config

6 Configuration Example

6.1 Network Requirements

A company that deploys NMS to monitor the operation status of TP-Link switches has requirements as follows:

1) Monitor traffic flow of specified ports, and send notifications to the NMS when the actual rate of transmitting and receiving packets exceeds the preset threshold.
2) Monitor the sending status of specified ports, and regularly collect and save data for follow-up checks. Specifically, during the sample interval, the switch should notify the NMS when the number of packets transmitted and received on the port exceeds the preset threshold; the switch should record but not notify the NMS when the number of packets transmitted and received is below the threshold.

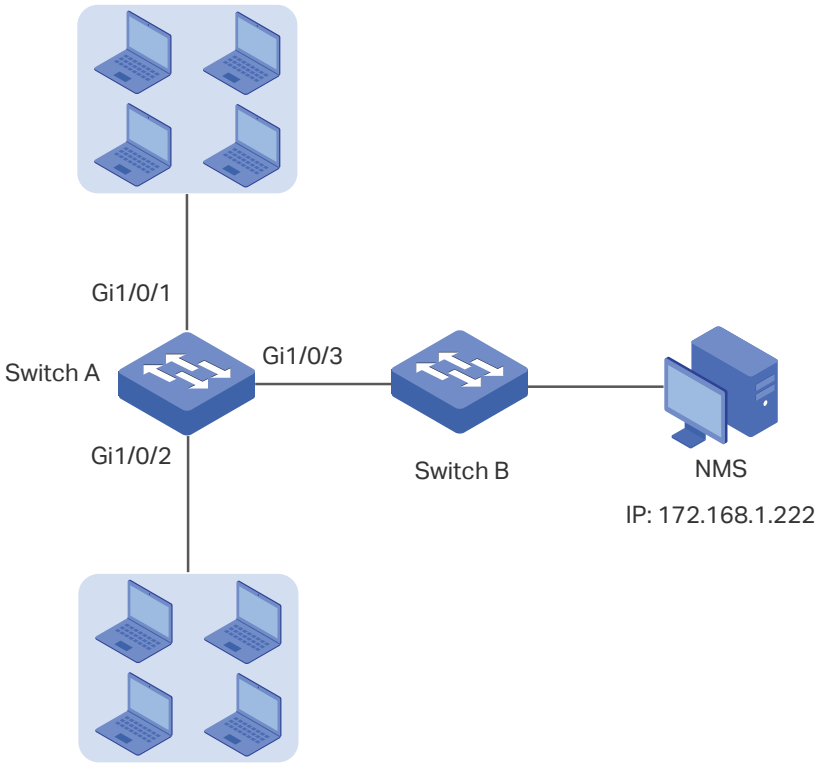
6.2 Configuration Scheme

1) Set a limit on the rate of the specified ports, and then enable SNMP on Switch A. Configure SNMP and Notification, and enable Trap notifications on the ports. Switch A can then send notifications to the NMS when the actual rate exceeds the preset threshold.
2) After SNMP and Notification configurations, you need to create statistic entries on the ports to monitor the real-time transmitting and receiving of packets and create history entries to regularly collect and save related data. Create two event entries: one is the notify type used to notify the NMS, the other is the log type used to record related events. In addition, create an alarm entry to monitor BPackets (Broadcast Packets), set the rising threshold and falling threshold, and bind the rising event to the notify event entry, and the falling event to the log event entry.

6.3 Network Topology

As shown in the following figure, the NMS host with IP address 172.168.1.222 is connected to the core switch, Switch B. On Switch A, ports 1/0/1 and 1/0/2 are monitored by the NMS; port 1/0/3 is connected to Switch B. And port 1/0/3 and the NMS are able to reach one another.

Figure 6-1 Network Topology



Demonstrated with T2600G-28TS, this chapter provides configuration procedures in two ways: using the GUI and using the CLI.

6.4 Using the GUI

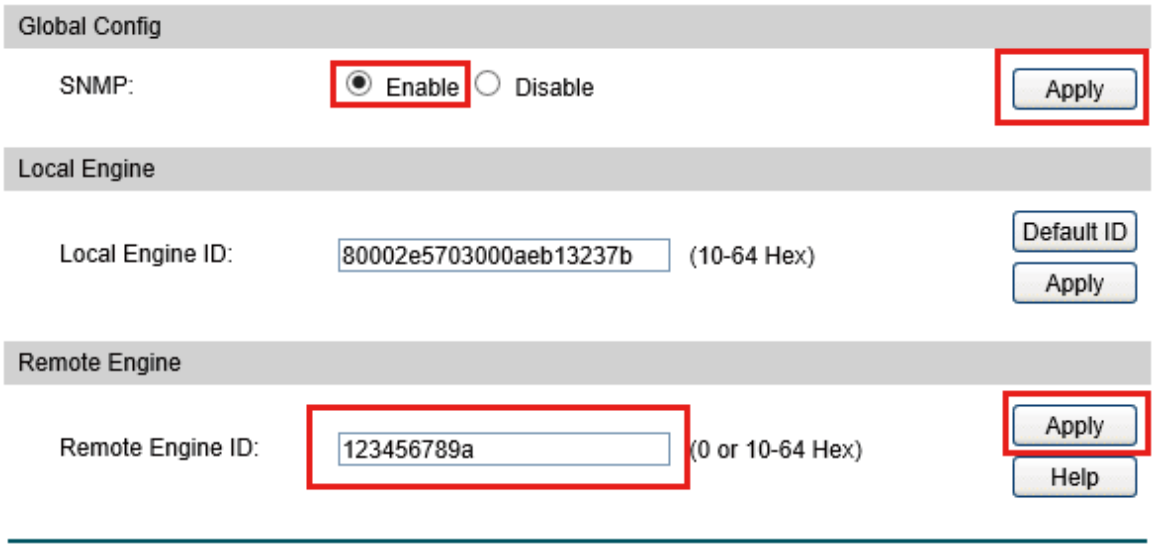
- Configuring Rate Limit on ports

  Configure the rate limit on required ports. For detailed configuration, please refer to *Configuring QoS*.

- Configuring SNMP

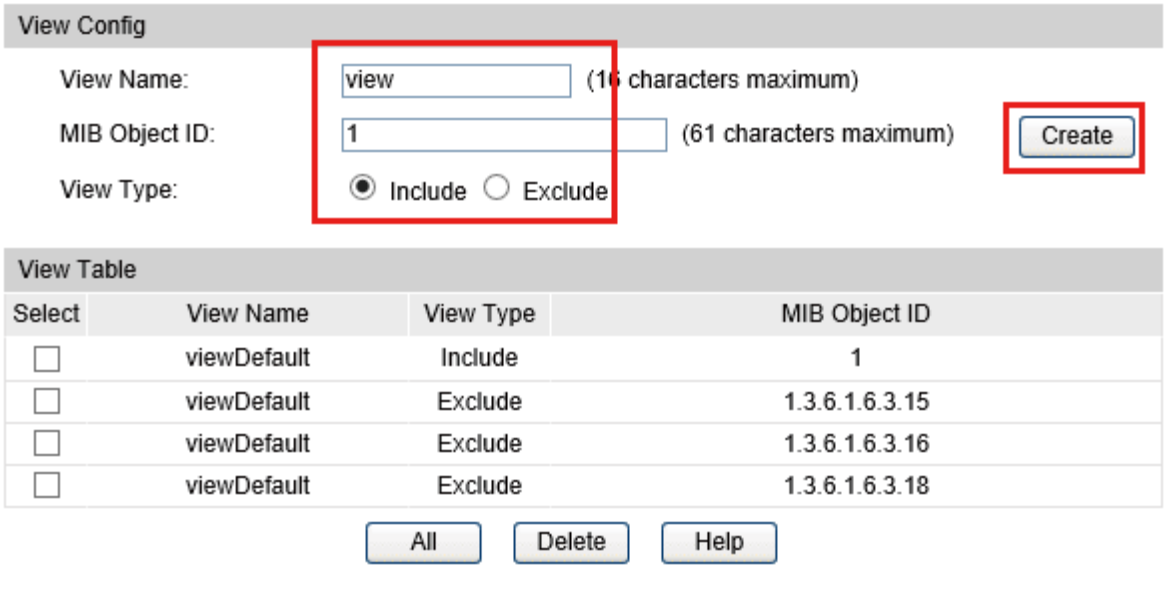
1) Choose **SNMP > SNMP Config > Global Confi**g to load the following page. Enable SNMP, and set the Remote Engine ID as 123456789a. Click **Apply**.

Figure 6-2 Enabling SNMP



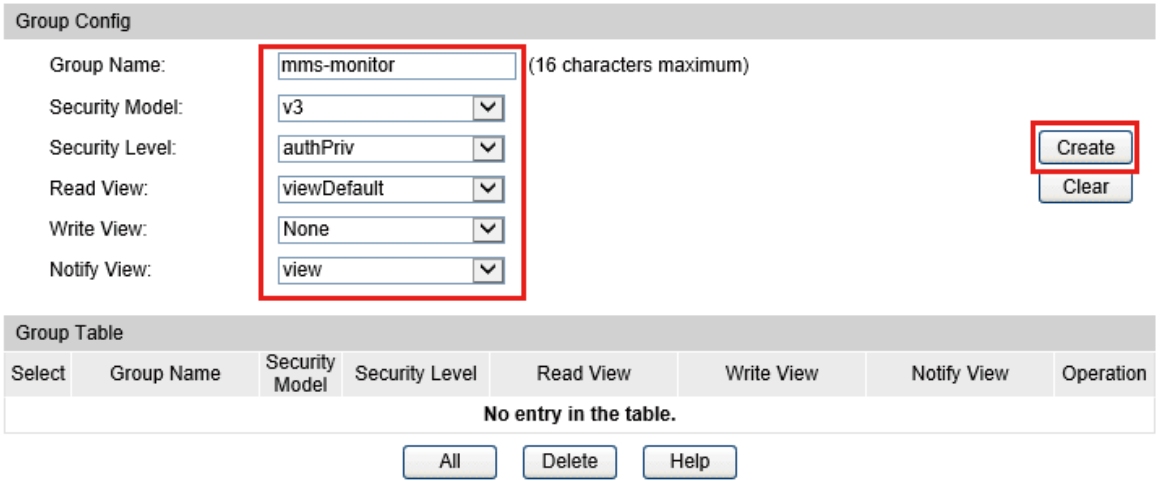
2) Choose **SNMP > SNMP Config > SNMP View** to load the following page. Name the SNMP view as View, set MIB Object ID as 1 (which means all functions), and set the view type as Include. Click **Create**.

Figure 6-3 SNMP View Configuration



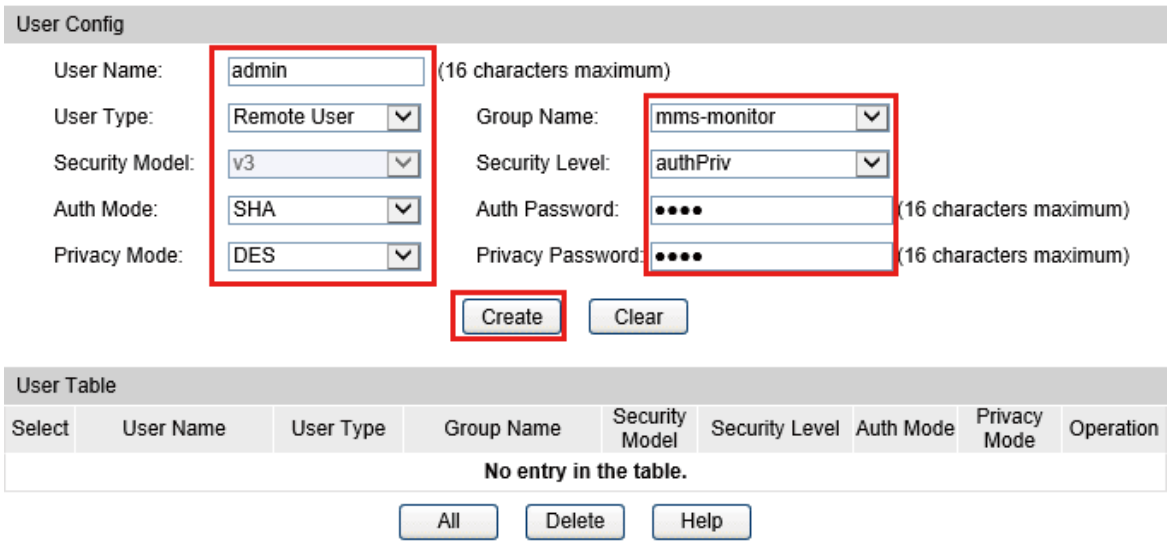
3) Choose **SNMP > SNMP Config > SNMP Group** to load the following page. Create a group with the name of nms-monitor, choose SNMPv3 and enable authentication and privacy, and add View to Read View and Notify View. Click **Create**.

Figure 6-4 SNMP Group Configuration



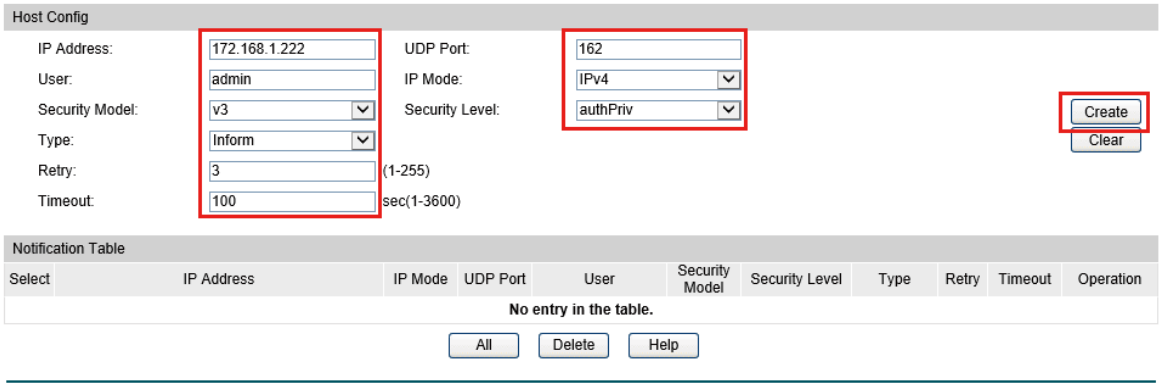
4) Choose **SNMP > SNMP Config > SNMP User** to load the following page. Create a user named admin for the NMS, set the user type as Remote User and specify the group name. Set the Security Model and Security Level in accordance with those of the group nms-monitor. Choose SHA authentication algorithm and DES privacy algorithm, and set corresponding passwords. Click **Create**.

Figure 6-5 User Config



5) Choose **SNMP > Notification > Notification Config** to load the following page. Specify the IP address of the NMS host and the port of the host for transmitting notifications. Set the User, Security Model and Security Level according to configurations of the SNMP User. Choose the type as Inform, and set the retry times as 3, with the timeout period as 100 seconds. Click **Create**.

Figure 6-6 Notification Configuration



6) Click **Save Config** to save the settings.

Enabling Bandwith-control Trap

The feature can be configured only with the CLI. You can enter the following commands under the CLI configuration mode:

Switch>enable	Enter Privileged EXEC Mode.
Switch#config	Enter global configuration mode.
Switch(config)#snmp-server traps bandwidth-control	Enable Bandwitch-control trap.

Configuring RMON

1) Choose **SNMP > RMON > Statistics** to load the following page. Create two entries and bind them to ports 1/0/1 and 1/0/2 respectively. Set the owner of the entries as monitor and the status as valid.

Figure 6-7 Configuring Entry 1

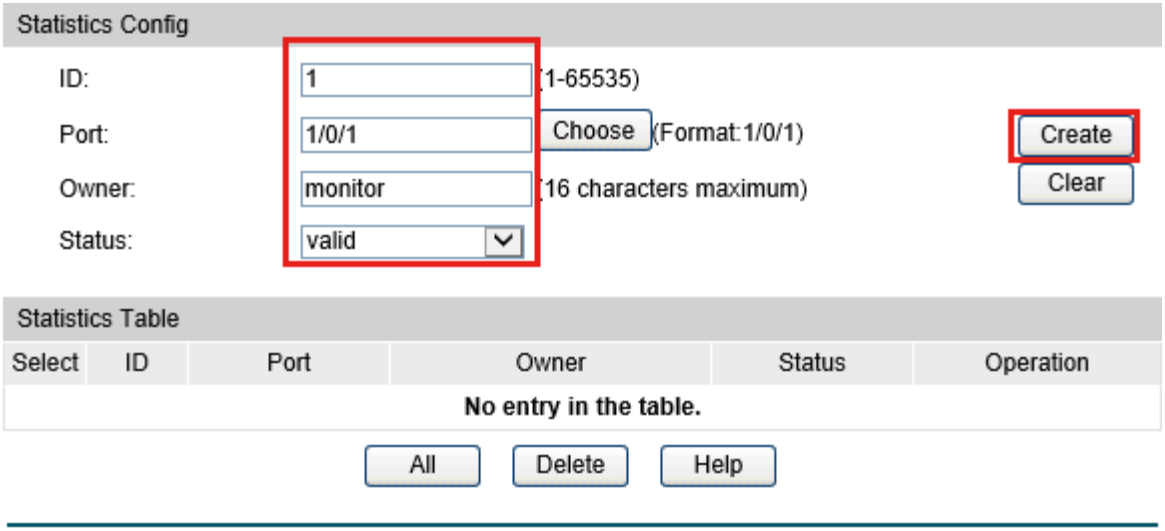
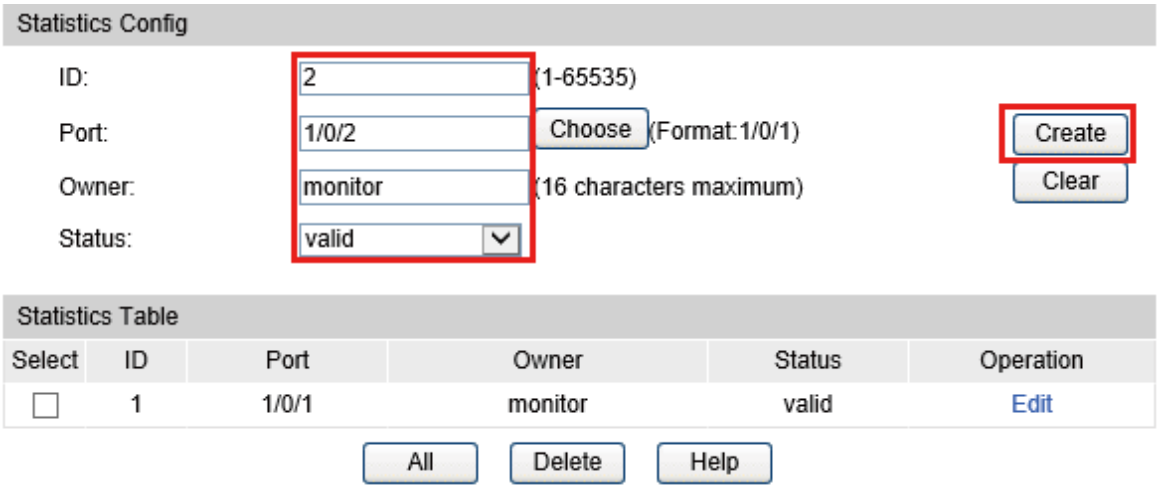
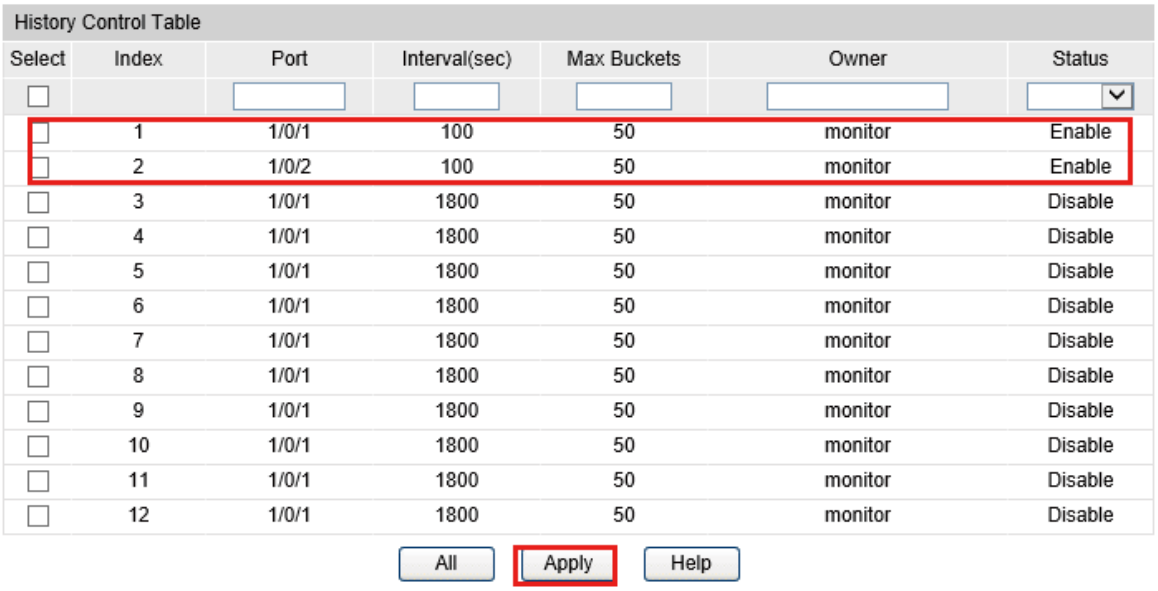


Figure 6-8 Configuring Entry 2



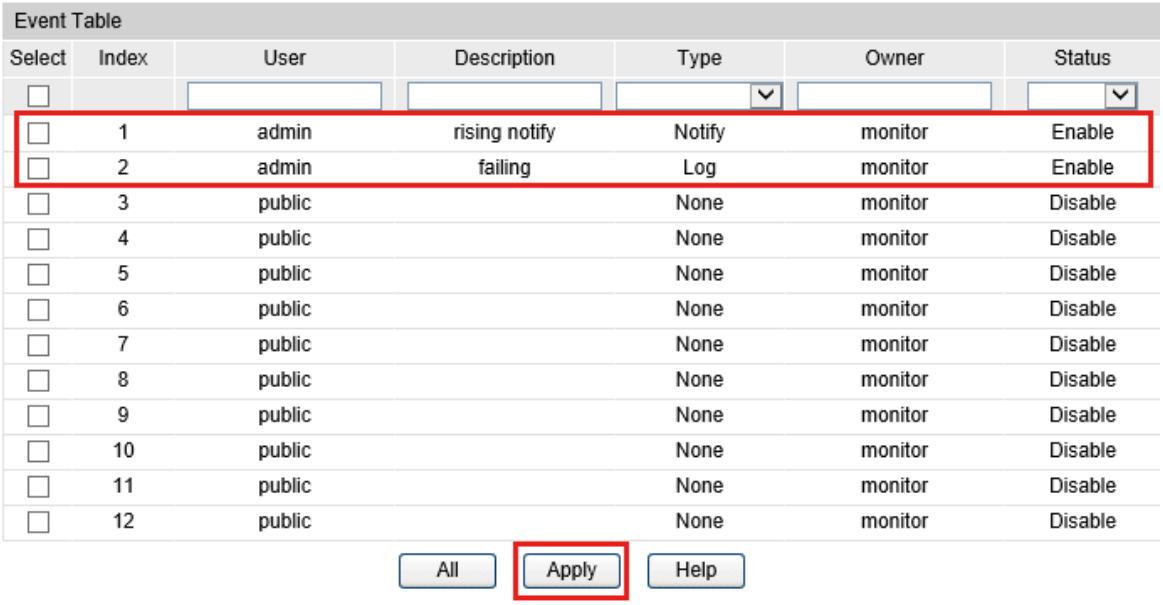
2) Choose the menu **SNMP > RMON > History** to load the following page. Configure entries 1 and 2. Bind entries 1 and 2 to ports 1/0/1 and 1/0/2 respectively, and set the Interval as 100 seconds, Max Buckets as 50, the owner of the entries as monitor, and the status as Enable.

Figure 6-9 History Configuration



3) Choose the menu **SNMP > RMON > Event** to load the following page. Configure entries 1 and 2. For entry 1, set the SNMP user name as admin, type as Notify, description as “rising notify”, owner as monitor, and status as enable. For entry 2, set the SNMP user name as admin, type as Log, description as “falling log”, owner as monitor, and status as enable.

Figure 6-10 Event Configuration



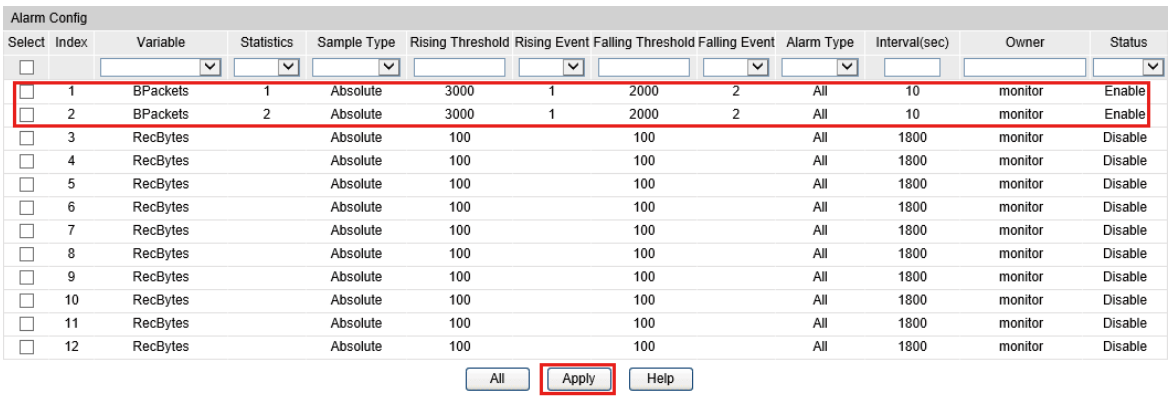
Event Table

Select	Index	User	Description	Type	Owner	Status
	1	admin	rising notify	Notify	monitor	Enable
	2	admin	failing	Log	monitor	Enable
	3	public		None	monitor	Disable
	4	public		None	monitor	Disable
	5	public		None	monitor	Disable
	6	public		None	monitor	Disable
	7	public		None	monitor	Disable
	8	public		None	monitor	Disable
	9	public		None	monitor	Disable
	10	public		None	monitor	Disable
	11	public		None	monitor	Disable
	12	public		None	monitor	Disable

All Apply Help

4) Choose **SNMP > RMON > Alarm** to load the following page. Configure entries 1 and 2. For entry 1, set the alarm variable as BPackets, related statistics entry ID as 1 (bound to port 1/0/1), the sample type as Absolute, the rising threshold as 3000, associated rising event entry ID as 1 (which is the notify type), the falling threshold as 2000, the associated falling event entry ID as 2 (which is the log type), the alarm type as all, the interval as 10 seconds, the owner name as monitor. For entry 2, set the associated statistics entry ID as 2 (bound to port 1/0/2). Other configurations are the same as those of entry 1.

Figure 6-11 Alarm Configuration



Alarm Config

Select	Index	Variable	Statistics	Sample Type	Rising Threshold	Rising Event	Falling Threshold	Falling Event	Alarm Type	Interval(sec)	Owner	Status
	1	BPackets	1	Absolute	3000	1	2000	2	All	10	monitor	Enable
	2	BPackets	2	Absolute	3000	1	2000	2	All	10	monitor	Enable
	3	RecBytes		Absolute	100		100		All	1800	monitor	Disable
	4	RecBytes		Absolute	100		100		All	1800	monitor	Disable
	5	RecBytes		Absolute	100		100		All	1800	monitor	Disable
	6	RecBytes		Absolute	100		100		All	1800	monitor	Disable
	7	RecBytes		Absolute	100		100		All	1800	monitor	Disable
	8	RecBytes		Absolute	100		100		All	1800	monitor	Disable
	9	RecBytes		Absolute	100		100		All	1800	monitor	Disable
	10	RecBytes		Absolute	100		100		All	1800	monitor	Disable
	11	RecBytes		Absolute	100		100		All	1800	monitor	Disable
	12	RecBytes		Absolute	100		100		All	1800	monitor	Disable

All Apply Help

5) Click **Save Config** to save settings.

6.5 Using the CLI

- Configuring Rate Limit on ports

  Configure the rate limit on required ports. For detailed configuration, please refer to *Configuring QoS*.

- Configuring SNMP

1) Enable SNMP and specify the remote engine ID.

   Switch#configure

   Switch(config)#snmp-server

   Switch(config)#snmp-server engineID remote 123456789a

2) Create a view with the name View; set the MIB Object ID as 1 (which represents all functions), and the view type as Include.

   Switch(config)#snmp-server view View 1 include

3) Create a group of SNMPv3 with the name of nms-monitor. Enable Auth Mode and Privacy Mode, and set the view as read View and notify view.

   Switch(config)#snmp-server group nms-monitor smode v3 slev authPriv read View notify View

4) Create an SNMP user with the name admin. Set the user as a remote user and configure the security mode and security level based on the group. Set the Auth Mode as SHA algorithm, password as 1234, the Privacy Mode as DES, and password as 1234.

   Switch(config)#snmp-server user admin remote nms-monitor smode v3 slev authPriv cmode SHA cpwd 1234 emode DES epwd 1234

5) To configure Notification, specify the IP address of the NMS host and UDP port. Set the User, Security Model and Security Level according to configurations of the SNMP User. Choose the type as Inform, and set the retry times as 3, and the timeout period as 100 seconds.

   Switch(config)#snmp-server host 172.168.1.222 162 admin smode v3 slev authPriv type inform retries 3 timeout 100

- Enable Bandwith-control Trap

  Switch(config)#snmp-server traps bandwidth-control

- Configuring RMON

1) Create two Statistics entries to monitor ports 1/0/1 and 1/0/2 respectively. The owner of the entries is set as monitor, and the status is set as valid.

   Switch(config)#rmon statistics 1 interface gigabitEthernet 1/0/1 owner monitor status valid

   Switch(config)#rmon statistics 2 interface gigabitEthernet 1/0/2 owner monitor status valid

2) Create two history entries and bind them to ports 1/0/1 and 1/0/2 respectively. Set the sample interval as 100 seconds, max buckets as 50, and the owner as monitor.

   Switch(config)#rmon history 1 interface gigabitEthernet 1/0/1 interval 100 owner monitor buckets 50

Switch(config)#rmon history 2 interface gigabitEthernet 1/0/2 interval 100 owner monitor buckets 50

3) Create two event entries named admin, which is the SNMP user name. Set entry 1 as the Notify type and its description as "rising notify". Set entry 2 as the Log type and its description as "falling log". Set the owner of them as monitor.

   Switch(config)#rmon event 1 user admin description rising-notify type notify owner monitor

   Switch(config)#rmon event 2 user admin description falling-log type log owner monitor

4) Create two alarm entries. For entry 1, set the alarm variable as BPackets, associated statistics entry ID as 1 (bound to port 1/0/1), the sample type as Absolute, the rising threshold as 3000, the associated rising event entry ID as 1 (Notify type), the falling threshold as 2000, the associated falling event entry ID as 2 (the log type), the alarm type as all, the interval as 10 seconds, and the owner name as monitor. For entry 2, set the associated statistics entry ID as 2 (bound to port 1/0/2), while all other configurations are the same as those of entry 1.

   Switch(config)#rmon alarm 1 stats-index 1 alarm-variable bpkt s-type absolute rising-threshold 3000 rising-event-index 1 falling-threshold 2000 falling-event-index 2 a-type all interval 10 owner monitor

   Switch(config)#rmon alarm 2 stats-index 2 alarm-variable bpkt s-type absolute rising-threshold 3000 rising-event-index 1 falling-threshold 2000 falling-event-index 2 a-type all interval 10 owner monitor

Verify the Configurations

Verify global SNMP configurations:

Switch(config)#show snmp-server

SNMP agent is enabled.

0 SNMP packets input

0 Bad SNMP version errors

0 Unknown community name

0 Illegal operation for community name supplied

0 Encoding errors

0 Number of requested variables

0 Number of altered variables

0 Get-request PDUs

0 Get-next PDUs

0 Set-request PDUs

0 SNMP packets output

0 Too big errors(Maximum packet size 1500)

0 No such name errors

0 Bad value errors

0 General errors

0 Response PDUs

0 Trap PDUs

Verify SNMP engine ID:

Switch(config)#show snmp-server engineID

Local engine ID : 80002e5703000aeb132397

Remote engine ID: 123456789a

Verify SNMP view configurations:

Switch(config)#show snmp-server view

No.	View Name	Type	MOID
1	viewDefault	include	1
2	viewDefault	exclude	1.3.6.1.6.3.15
3	viewDefault	exclude	1.3.6.1.6.3.16
4	viewDefault	exclude	1.3.6.1.6.3.18
5	View	include	1

Verify SNMP group configurations:

Switch(config)#show snmp-server group

No.	Name	Sec-Mode	Sec-Lev	Read-View	Write-View	Notify-View
1	nms-monitor	v3	authPriv	View		View

Verify SNMP user configurations:

Switch(config)#show snmp-server user

```
No. U-Name     U-Type    G-Name        S-Mode    S-Lev       A-Mode   P-Mode
--- ---------- ------    ------        ------    -----       ------   ------
1    admin      remote    nms-monitor   v3        authPriv    SHA      DES
```

Verify SNMP host configurations:

Switch(config)#show snmp-server host

```
No. Des-IP           UDP   Name    SecMode   SecLev     Type    Retry  Timeout
--- ---------------- ----- ------- --------- ---------- ------- -----  --------
1   172.168.1.222    162   admin    v3        authPriv   inform  3      100
```

Verify RMON statistics configurations:

Switch(config)#show rmon statistics

```
Index  Port       Owner      State
-----  ---------- ---------  -------
1      Gi1/0/1    monitor    valid
2      Gi1/0/2    monitor    valid
```

Verify RMON history configurations:

Switch(config)#show rmon history

```
Index  Port       Interval  Buckets   Owner      State
-----  ---------  --------  --------- ---------- ---------
1      Gi1/0/1    100       50        monitor    Enable
2      Gi1/0/2    100       50        monitor    Enable
```

Verify RMON event configurations:

Switch(config)#show rmon event

```
Index  User       Description       Type       Owner      State
-----  ------     -----------       --------   ---------- ----------
1      admin      rising-notify     Notify     monitor    Enable
2      admin      falling-log       Log        monitor    Enable
```

Verify RMON alarm configurations:

```
Switch(config)#show rmon alarm
  Index-State:        1-Enabled
  Statistics index:   1
  Alarm variable:     BPkt
  Sample Type:        Absolute
  RHold-REvent:       3000-1
  FHold-FEvent:       2000-2
  Alarm startup:      All
  Interval:           10
  Owner:              monitor
  Index-State:        2-Enabled
  Statistics index:   2
  Alarm variable:     BPkt
  Sample Type:        Absolute
  RHold-REvent:       3000-1
  FHold-FEvent:       2000-2
  Alarm startup:      All
  Interval:           10
  Owner:              monitor
```

7 Appendix: Default Parameters

Default settings of SNMP are listed in the following table.

Table 7-1 Default Global Config Settings

Parameter	Default Setting
SNMP	Disable
Local Engine ID	Automatically
Remote Engine ID	None

Table 7-2 Default SNMP View Settings

Parameter	Default Setting
View Name	None
MIB Object ID	None
View Type	Include

Table 7-3 Default SNMP View Table Settings

View Name	View Type	MIB Object ID
viewDefault	Include	1
viewDefault	Exclude	1.3.6.1.6.3.15
viewDefault	Exclude	1.3.6.1.6.3.16
viewDefault	Exclude	1.3.6.1.6.3.18

Table 7-4 Default Group Settings

Parameter	Default Setting
Group Name	None
Security Model	v1
Security Level	noAuthNoPriv
Read View	viewDefault
Write View	None
Notify View	None

Table 7-5 Default User Settings

Parameter	Default Setting
User Name	None
User Type	Local User
Group Name	None
Security Model	v1
Security Level	noAuthNoPriv
Auth Mode	None
Auth Password	None
Privacy Mode	None
Privacy Password	None

Table 7-6 Default Community Settings

Parameter	Default Setting
Community Name	None
Access	read-only
MIB View	viewDefault

Default settings of Notification are listed in the following table.

Table 7-7 Default Host Config Settings

Parameter	Default Setting
IP Address	None
UDP Port	162
User	None
IP Mode	IPv4
Security Model	v1
Security Level	noAuthNoPriv
Type	Trap
Retry	None in trap mode; 3 times in Inform mode.
Timeout	None in trap mode; 100 seconds in Inform mode.

Table 7-8 Default Statistics Config Settings

Parameter	Default Setting
ID	None
Port	None
Owner	None
IP Mode	valid

Table 7-9 Default Settings for History Entries

Parameter	Default Setting
Port	1/0/1
Interval	1800 seconds
Max Buckets	50
Owner	monitor
Status	Disable

Table 7-10 Default Settings for Event Entries

Parameter	Default Setting
User	public
Description	None
Type	None
Owner	monitor
Status	Disable

Table 7-11 Default Settings for Alarm Entries

Parameter	Default Setting
Variable	RecBytes
Statistics	None
Sample Type	Absolute
Rising Threshold	100
Rising Event	None
Falling Threshold	100
Falling Event	None
Alarm Type	All
Interval	1800 seconds
Owner	monitor

Parameter	Default Setting
Status	Disable