Configuration Guide

T1600G Series Switches

T1600G-52TS (TL-SG2452) / T1600G-52PS (TL-SG2452P)

1910012333 REV3.0.0

January 2018

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 10
- Console Login (only for switch with console port) 10
- Telnet Login 12
- SSH Login 13
- Disable Telnet login 17
- Disable SSH login 18
- Copy running-config startup-config 18
- Change the Switch's IP Address and Default Gateway 19

Managing System

System 21
- Overview 21
- Supported Features 21

System Info Configurations 23
- Using the GUI 23
  - Viewing the System Summary 23
  - Configuring the Device Description 26
  - Configuring the System Time 27
  - Configuring the Daylight Saving Time 28
- Using the CLI 29
  - Viewing the System Summary 29
  - Configuring the Device Description 30

Configuring the System Time 31
Configuring the Daylight Saving Time 34
User Management Configurations 36
Using the GUI 36
Creating Accounts 36
Configuring Enable Password 37
Using the CLI 38
Creating Accounts 38
Configuring Enable Password 40
System Tools Configurations 43
Using the GUI 43
Configuring the Boot File 43
Restoring the Configuration of the Switch 44
Backing up the Configuration File 45
Upgrading the Firmware 46
Rebooting the switch 47
Reseting the Switch 48
Using the CLI 48
Configuring the Boot File 48
Restoring the Configuration of the Switch 49
Backing up the Configuration File 50
Upgrading the Firmware 50
Rebooting the Switch 51
Reseting the Switch 53
EEE Configuration 54
Using the CLI 54
PoE Configurations 56
Using the GUI 57
Configuring the PoE Parameters Manually 57
Configuring the PoE Parameters Using the Profile 60
Using the CLI 63
Configuring the PoE Parameters Manually 63
Configuring the PoE Parameters Using the Profile 65
SDM Template Configuration 68
Using the GUI 68
Using the CLI 69
Time Range Configuration 71
Using the GUI 71

Adding Time Range Entries 71
Configuring Holiday 73
Using the CLI 74
Adding Time Range Entries 74
Configuring Holiday 75
Example for PoE Configurations 77
Network Requirements 77
Configuring Scheme 77
Using the GUI 77
Using the CLI 80
Appendix: Default Parameters 82

Managing Physical Interfaces

Physical Interface 86
Overview 86
Supported Features 86
Basic Parameters Configurations 87
Using the GUI 87
Using the CLI 88
Port Isolation Configurations 91
Using the GUI 91
Using the CLI 92
Loopback Detection Configuration 94
Using the GUI 94
Using the CLI 96
Configuration Examples 98
Example for Port Isolation 98
Network Requirements 98
Configuration Scheme 98
Using the GUI 98
Using the CLI 100
Example for Loopback Detection 101
Network Requirements 101
Configuration Scheme 101
Using the GUI 102
Using the CLI 103
Appendix: Default Parameters 104

Configuring LAG

LAG 106
Overview 106
Supported Features 106
LAG Configuration 107
Using the GUI 108
Configuring Load-balancing Algorithm 108
Configuring Static LAG or LACP 109
Using the CLI 111
Configuring Load-balancing Algorithm 111
Configuring Static LAG or LACP 112
Configuration Example 116
Network Requirements 116
Configuration Scheme 116
Using the GUI 117
Using the CLI 118
Appendix: Default Parameters 120

Managing MAC Address Table

MAC Address Table 122
Overview 122
Supported Features 122
MAC Address Configurations 123
Using the GUI 123
Adding Static MAC Address Entries 123
Modifying the Aging Time of Dynamic Address Entries 125
Adding MAC Filtering Address Entries 126
Viewing Address Table Entries 126
Using the CLI 127
Adding Static MAC Address Entries 127
Modifying the Aging Time of Dynamic Address Entries 128
Adding MAC Filtering Address Entries 129
Appendix: Default Parameters 131

Configuring 802.1Q VLAN

Overview 133
802.1Q VLAN Configuration 134

Using the GUI 134
Configuring the PVID of the Port 134
Configuring the VLAN 135
Using the CLI 136
Creating a VLAN 136
Configuring the Port 137
Adding the Port to the Specified VLAN 138
Configuration Example 140
Network Requirements 140
Configuration Scheme 140
Network Topology 141
Using the GUI 141
Using the CLI 144
Appendix: Default Parameters 146

Configuring MAC VLAN

Overview 148
MAC VLAN Configuration 149
Using the GUI 149
Configuring 802.1Q VLAN 149
Binding the MAC Address to the VLAN 149
Enabling MAC VLAN for the Port 150
Using the CLI 151
Configuring 802.1Q VLAN 151
Binding the MAC Address to the VLAN 151
Enabling MAC VLAN for the Port 152
Configuration Example 153
Network Requirements 153
Configuration Scheme 153
Using the GUI 154
Using the CLI 158
Appendix: Default Parameters 161

Configuring Protocol VLAN

Overview 163
Protocol VLAN Configuration 164
Using the GUI 164

Configuring 802.1Q VLAN 164
Creating Protocol Template 165
Configuring Protocol VLAN 166
Using the CLI 167
Configuring 802.1Q VLAN 167
Creating a Protocol Template 167
Configuring Protocol VLAN 168
Configuration Example 171
Network Requirements 171
Configuration Scheme 171
Using the GUI 172
Using the CLI 177
Appendix: Default Parameters 182

Configuring GVRP

Overview 184
GVRP Configuration 185
Using the GUI 186
Using the CLI 187
Configuration Example 190
Network Requirements 190
Configuration Scheme 190
Using the GUI 191
Using the CLI 195
Appendix: Default Parameters 199

Configuring Layer 2 Multicast

Layer 2 Multicast 201
Overview 201
Supported Features 203
IGMP Snooping Configuration 204
Using the GUI 204
Configuring IGMP Snooping Globally 204
Configuring IGMP Snooping for VLANs 205
Configuring IGMP Snooping for Ports 209
Configuring Hosts to Statically Join a Group 209
Using the CLI 210

Configuring IGMP Snooping Globally 210
Configuring IGMP Snooping for VLANs 212
Configuring IGMP Snooping for Ports 217
Configuring Hosts to Statically Join a Group 218
MLD Snooping Configuration 220
Using the GUI 220
Configuring MLD Snooping Globally 220
Configuring MLD Snooping for VLANs 221
Configuring MLD Snooping for Ports 224
Configuring Hosts to Statically Join a Group 224
Using the CLI 225
Configuring MLD Snooping Globally 225
Configuring MLD Snooping for VLANs 226
Configuring MLD Snooping for Ports 231
Configuring Hosts to Statically Join a Group 232
MVR Configuration 234
Using the GUI 234
Configuring 802.1Q VLANs 234
Configuring MVR Globally 235
Adding Multicast Groups to MVR 236
Configuring MVR for the Port 237
(Optional) Adding Ports to MVR Groups Statically 238
Using the CLI 239
Configuring 802.1Q VLANs 239
Configuring MVR Globally 239
Configuring MVR for the Ports 241
Multicast Filtering Configuration 244
Using the GUI 244
Creating the Multicast Profile 244
Configure Multicast Filtering for Ports 246
Using the CLI 247
Creating the Multicast Profile 247
Binding the Profile to Ports 250
Viewing Multicast Snooping Information 254
Using the GUI 254
Viewing IPv4 Multicast Table 254
Viewing IPv4 Multicast Statistics on Each Port 255
Viewing IPv6 Multicast Table 256

Viewing IPv6 Multicast Statistics on Each Port....257
Using the CLI....258
Viewing IPv4 Multicast Snooping Information....258
Viewing IPv6 Multicast Snooping Configurations....258
Configuration Examples....259
Example for Configuring Basic IGMP Snooping....259
Network Requirements....259
Configuration Scheme....259
Using the GUI....260
Using the CLI....262
Example for Configuring MVR....264
Network Requirements....264
Network Topology....264
Configuration Scheme....265
Using the GUI....265
Using the CLI....269
Example for Configuring Unknown Multicast and Fast Leave....272
Network Requirement....272
Configuration Scheme....272
Using the GUI....273
Using the CLI....274
Example for Configuring Multicast Filtering....276
Network Requirements....276
Configuration Scheme....276
Network Topology....276
Using the GUI....277
Using the CLI....280
Appendix: Default Parameters....283
Default Parameters for IGMP Snooping....283
Default Parameters for MLD Snooping....284
Default Parameters for MVR....285
Default Parameters for Multicast Filtering....285

Configuring Spanning Tree

Spanning Tree....287
Overview....287
Basic Concepts....287

STP/RSTP Concepts....287
MSTP Concepts....291
STP Security....292
STP/RSTP Configurations....295
Using the GUI....295
Configuring STP/RSTP Parameters on Ports....295
Configuring STP/RSTP Globally....297
Verifying the STP/RSTP Configurations....299
Using the CLI....301
Configuring STP/RSTP Parameters on Ports....301
Configuring Global STP/RSTP Parameters....303
Enabling STP/RSTP Globally....305
MSTP Configurations....307
Using the GUI....307
Configuring Parameters on Ports in CIST....307
Configuring the MSTP Region....310
Configuring MSTP Globally....314
Verifying the MSTP Configurations....316
Using the CLI....317
Configuring Parameters on Ports in CIST....317
Configuring the MSTP Region....319
Configuring Global MSTP Parameters....322
Enabling Spanning Tree Globally....324
STP Security Configurations....327
Using the GUI....327
Using the CLI....328
Configuring the STP Security....328
Configuration Example for MSTP....331
Network Requirements....331
Configuration Scheme....331
Using the GUI....332
Using the CLI....338
Appendix: Default Parameters....345

Configuring LLDP

LLDP....348
Overview....348

Supported Features 348
LLDP Configurations 349
Using the GUI 349
Configuring LLDP Globally 349
Configuring LLDP For the Port 351
Using the CLI 352
Global Config 352
Port Config 354
LLDP-MED Configurations 357
Using the GUI 357
Configuring LLDP Globally 357
Configuring LLDP-MED Globally 357
Configuring LLDP-MED for Ports 358
Using the CLI 360
Global Config 360
Port Config 361
Viewing LLDP Settings 364
Using GUI 364
Viewing LLDP Device Info 364
Viewing LLDP Statistics 367
Using CLI 368
Viewing LLDP-MED Settings 369
Using GUI 369
Using CLI 371
Configuration Example 372
Network Requirements 372
Network Topology 372
Configuration Scheme 372
Using the GUI 372
Using CLI 373
Appendix: Default Parameters 379

Configuring Layer 3 Interfaces

Overview 381
Layer 3 Interface Configurations 382
Using the GUI 382
Creating an Layer 3 Interface 382

Configuring IPv4 Parameters of the Interface 384
Configuring IPv6 Parameters of the Interface 385
Viewing Detail Information of the Interface 388
Using the CLI 389
Creating an Layer 3 Interface 389
Configuring IPv4 Parameters of the Interface 391
Configuring IPv6 Parameters of the Interface 392
Appendix: Default Parameters 395

Configuring Routing

Overview 397
IPv4 Static Routing Configuration 398
Using the GUI 398
Using the CLI 399
IPv6 Static Routing Configuration 400
Using the GUI 400
Using the CLI 400
Viewing Routing Table 402
Using the GUI 402
Viewing IPv4 Routing Table 402
Viewing IPv6 Routing Table 403
Using the CLI 403
Viewing IPv4 Routing Table 403
Viewing IPv6 Routing Table 404
Example for Static Routing 405
Network Requirements 405
Configuration Scheme 405
Using the GUI 405
Using the CLI 407

Configuring DHCP Service

DHCP 411
Overview 411
Supported Features 411
DHCP Server Configuration 414
Using the GUI 414
Enabling DHCP Server 414

Configuring DHCP Server Pool 416
Configuring Manual Binding 417
Using the CLI 418
Enabling DHCP Server 418
Configuring DHCP Server Pool 421
Configuring Manual Binding 423
DHCP Relay Configuration 425
Using the GUI 425
Enabling DHCP Relay and Configuring Option 82 425
Configuring DHCP Interface Relay 427
Configuring DHCP VLAN Relay 427
Using the CLI 429
Enabling DHCP Relay 429
(Optional) Configuring Option 82 430
Configuring DHCP Interface Relay 432
Configuring DHCP VLAN Relay 433
DHCP L2 Relay Configuration 435
Using the GUI 435
Enabling DHCP L2 Relay 435
Configuring Option 82 for Ports 436
Using the CLI 437
Enabling DHCP Relay 437
Configuring Option 82 for Ports 438
Configuration Examples 440
Example for DHCP Server 440
Network Requirements 440
Configuration Scheme 440
Using the GUI 440
Using the CLI 442
Example for DHCP Interface Relay 443
Network Requirements 443
Configuration Scheme 443
Using the GUI 444
Using the CLI 445
Appendix: Default Parameters 446

Configuring ARP

Overview 450
Supported Features 450
ARP Configurations 452
Using the GUI 452
Viewing the ARP Entries 452
Adding Static ARP Entries Manually 453
Configuring Gratuitous ARP 453
Configuring Proxy ARP 454
Configuring Local Proxy ARP 455
Using the CLI 456
Configuring the ARP Entry 456
Configuring the Gratuitous ARP 458
Configuring Proxy ARP 460
Appendix: Default Parameters 463

Configuring QoS

QoS 465
Overview 465
Supported Features 465
Class of Service Configuration 467
Using the GUI 468
Configuring Port Priority 468
Configuring 802.1p Priority 470
Configuring DSCP Priority 472
Specifying the Scheduler Settings 475
Using CLI 476
Configuring Port Priority 476
Configuring 802.1p Priority 478
Configuring DSCP Priority 481
Specifying the Scheduler Settings 486
Bandwidth Control Configuration 488
Using the GUI 488
Configuring Rate Limit 488
Configuring Storm Control 489
Using the CLI 490
Configuring Rate Limit 490

Configuring Storm Control 491
Voice VLAN Configuration 494
Using the GUI 494
Configuring OUI Addresses 494
Configuring Voice VLAN Globally 495
Adding Ports to Voice VLAN 496
Using the CLI 497
Auto VoIP Configuration 500
Using the GUI 500
Using the CLI 501
Configuration Examples 505
Example for Class of Service 505
Network Requirements 505
Configuration Scheme 505
Using the GUI 506
Using the CLI 508
Example for Voice VLAN 510
Network Requirements 510
Configuration Scheme 511
Using the GUI 511
Using the CLI 515
Example for Auto VoIP 518
Network Requirements 518
Configuration Scheme 518
Using the GUI 519
Using the CLI 526
Appendix: Default Parameters 531

Configuring Access Security

Access Security 536
Overview 536
Supported Features 536
Access Security Configurations 537
Using the GUI 537
Configuring the Access Control Feature 537
Configuring the HTTP Function 540
Configuring the HTTPS Function 542

Configuring the SSH Feature 545
Configuring the Telnet Function 546
Using the CLI 547
Configuring the Access Control 547
Configuring the HTTP Function 548
Configuring the HTTPS Function 550
Configuring the SSH Feature 552
Configuring the Telnet Function 555
Appendix: Default Parameters 556

Configuring AAA

Overview 559
AAA Configuration 560
Using the GUI 561
Adding Servers 561
Configuring Server Groups 563
Configuring the Method List 564
Configuring the AAA Application List 565
Configuring Login Account and Enable Password 566
Using the CLI 567
Adding Servers 567
Configuring Server Groups 569
Configuring the Method List 570
Configuring the AAA Application List 572
Configuring Login Account and Enable Password 575
Configuration Example 577
Network Requirements 577
Configuration Scheme 577
Using the GUI 578
Using the CLI 580
Appendix: Default Parameters 583

Configuring 802.1x

Overview 586
802.1x Configuration 588
Using the GUI 588
Configuring the RADIUS Server 588

Configuring 802.1x Globally....591
Configuring 802.1x on Ports....592
View the Authenticator State....594
Using the CLI....595
Configuring the RADIUS Server....595
Configuring 802.1x Globally....597
Configuring 802.1x on Ports....599
Viewing Authenticator State....601
Configuration Example....603
Network Requirements....603
Configuration Scheme....603
Network Topology....603
Using the GUI....604
Using the CLI....606
Appendix: Default Parameters....609

Configuring Port Security

Overview....611
Port Security Configuration....612
Using the GUI....612
Using the CLI....613
Appendix: Default Parameters....616

Configuring ACL

Overview....618
ACL Configuration....619
Using the GUI....619
Configuring Time Range....619
Creating an ACL....619
Configuring ACL Rules....620
Configuring MAC ACL Rule....620
Configuring IP ACL Rule....624
Configuring the IPv6 ACL Rule....628
Configuring ACL Binding....632
Using the CLI....634
Configuring Time Range....634
Configuring ACL....634

Configuring Policy....640
Configuring ACL Binding....642
Viewing ACL Counting....643
Configuration Example for ACL....644
Network Requirements....644
Configuration Scheme....644
Using the GUI....645
Using the CLI....649
Appendix: Default Parameters....652

Configuring IPv4 IMPB

IPv4 IMPB....655
Overview....655
Supported Features....655
IP-MAC Binding Configuration....656
Using the GUI....656
Binding Entries Manually....656
Binding Entries via ARP Scanning....658
Binding Entries via DHCP Snooping....659
Viewing the Binding Entries....661
Using the CLI....662
Binding Entries Manually....662
Binding Entries via DHCP Snooping....664
Viewing Binding Entries....665
ARP Detection Configuration....666
Using the GUI....666
Adding IP-MAC Binding Entries....666
Enabling ARP Detection....666
Configuring ARP Detection on Ports....667
Viewing ARP Statistics....668
Using the CLI....669
Adding IP-MAC Binding Entries....669
Enabling ARP Detection....669
Configuring ARP Detection on Ports....670
Viewing ARP Statistics....672
IPv4 Source Guard Configuration....673
Using the GUI....673

Adding IP-MAC Binding Entries 673
Configuring IPv4 Source Guard 673
Using the CLI 674
Adding IP-MAC Binding Entries 674
Configuring IPv4 Source Guard 674
Configuration Examples 676
Example for ARP Detection 676
Network Requirements 676
Configuration Scheme 676
Using the GUI 677
Using the CLI 679
Example for IP Source Guard 681
Network Requirements 681
Configuration Scheme 681
Using the GUI 681
Using the CLI 683
Appendix: Default Parameters 685

Configuring IPv6 IMPB

IPv6 IMPB 688
Overview 688
Supported Features 688
IPv6-MAC Binding Configuration 690
Using the GUI 690
Binding Entries Manually 690
Binding Entries via ND Snooping 692
Binding Entries via DHCPv6 Snooping 693
Viewing the Binding Entries 695
Using the CLI 696
Binding Entries Manually 696
Binding Entries via ND Snooping 698
Binding Entries via DHCPv6 Snooping 699
Viewing Binding Entries 700
ND Detection Configuration 701
Using the GUI 701
Adding IPv6-MAC Binding Entries 701
Enabling ND Detection 701

Configuring ND Detection on Ports....702
Viewing ND Statistics....703
Using the CLI....703
Adding IPv6-MAC Binding Entries....703
Enabling ND Detection....703
Configuring ND Detection on Ports....705
Viewing ND Statistics....705
IPv6 Source Guard Configuration....707
Using the GUI....707
Adding IPv6-MAC Binding Entries....707
Configuring IPv6 Source Guard....707
Using the CLI....708
Adding IPv6-MAC Binding Entries....708
Configuring IPv6 Source Guard....708
Configuration Examples....710
Example for ND Detection....710
Network Requirements....710
Configuration Scheme....710
Using the GUI....711
Using the CLI....713
Example for IPv6 Source Guard....715
Network Requirements....715
Configuration Scheme....715
Using the GUI....715
Using the CLI....717
Appendix: Default Parameters....718

Configuring DHCP Filter

DHCP Filter....721
Overview....721
Supported Features....721
DHCPv4 Filter Configuration....723
Using the GUI....723
Configuring the Basic DHCPv4 Filter Parameters....723
Configuring Legal DHCPv4 Servers....725
Using the CLI....725
Configuring the Basic DHCPv4 Filter Parameters....725

Configuring Legal DHCPv4 Servers 727
DHCPv6 Filter Configuration 729
Using the GUI 729
Configuring the Basic DHCPv6 Filter Parameters 729
Configuring Legal DHCPv6 Servers 730
Using the CLI 731
Configuring the Basic DHCPv6 Filter Parameters 731
Configuring Legal DHCPv6 Servers 732
Configuration Examples 734
Example for DHCPv4 Filter 734
Network Requirements 734
Configuration Scheme 734
Using the GUI 735
Using the CLI 736
Example for DHCPv6 Filter 737
Network Requirements 737
Configuration Scheme 738
Using the GUI 738
Using the CLI 740
Appendix: Default Parameters 742

Configuring DoS Defend

Overview 744
DoS Defend Configuration 745
Using the GUI 745
Using the CLI 746
Appendix: Default Parameters 749

Monitoring the System

Overview 751
Monitoring the CPU 752
Using the GUI 752
Using the CLI 752
Monitoring the Memory 754
Using the GUI 754
Using the CLI 754

Monitoring Traffic

Traffic Monitor 757
Using the GUI 757
Using the CLI 761
Appendix: Default Parameters 762

Mirroring Traffic

Mirroring 764
Using the GUI 764
Using the CLI 766
Configuration Examples 768
Network Requirements 768
Configuration Scheme 768
Using the GUI 768
Using the CLI 769
Appendix: Default Parameters 771

Configuring DLDP

Overview 773
DLDP Configuration 774
Using the GUI 774
Using the CLI 776
Appendix: Default Parameters 778

Configuring SNMP & RMON

SNMP 780
Overview 780
Basic Concepts 780
SNMP Configurations 784
Using the GUI 784
Enabling SNMP 784
Creating an SNMP View 785
Creating SNMP Communities (For SNMP v1/v2c) 786
Creating an SNMP Group (For SNMP v3) 787
Creating SNMP Users (For SNMP v3) 788
Using the CLI 789
Enabling SNMP 789

Creating an SNMP View....791
Creating SNMP Communities (For SNMP v1/v2c)....792
Creating an SNMP Group (For SNMPv3)....793
Creating SNMP Users (For SNMPv3)....795
Notification Configurations....797
Using the GUI....797
Configuring the Information of NMS Hosts....797
Enabling SNMP Traps....799
Using the CLI....801
Configuring the NMS Host....801
Enabling SNMP Traps....802
RMON....809
RMON Configurations....810
Using the GUI....810
Configuring Statistics Group....810
Configuring History Group....811
Configuring Event Group....812
Configuring Alarm Group....813
Using the CLI....815
Configuring Statistics....815
Configuring History....817
Configuring Event....818
Configuring Alarm....819
Configuration Example....822
Network Requirements....822
Configuration Scheme....823
Using the GUI....823
Using the CLI....828
Appendix: Default Parameters....834

Diagnosing the Device & Network

Diagnosing the Device....839
Using the GUI....839
Using the CLI....840
Diagnosing the Network....841
Using the GUI....841
Troubleshooting with Ping Testing....841

Troubleshooting with Tracert Testing....842
Using the CLI....843
Configuring the Ping Test....843
Configuring the Tracert Test....844
Appendix: Default Parameters....845

Configuring System Logs

Overview....847
System Logs Configurations....848
Using the GUI....849
Configuring the Local Logs....849
Configuring the Remote Logs....849
Backing up the Logs....850
Viewing the Log Table....851
Using the CLI....852
Configuring the Local Logs....852
Configuring the Remote Logs....853
Configuration Example....855
Network Requirements....855
Configuration Scheme....855
Using the GUI....855
Using the CLI....856
Appendix: Default Parameters....857

About This Guide

This Configuration Guide provides information for managing T1600G 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 http://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 http://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 http://www.tp-link.com.
- A Technical Support Forum is provided for you to discuss our products at http://forum.tp-link.com.
- Our Technical Support contact information can be found at the Contact Technical Support page at http://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.

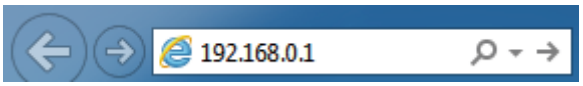
The following example shows how to login via the HTTP server.

2.1 Login

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

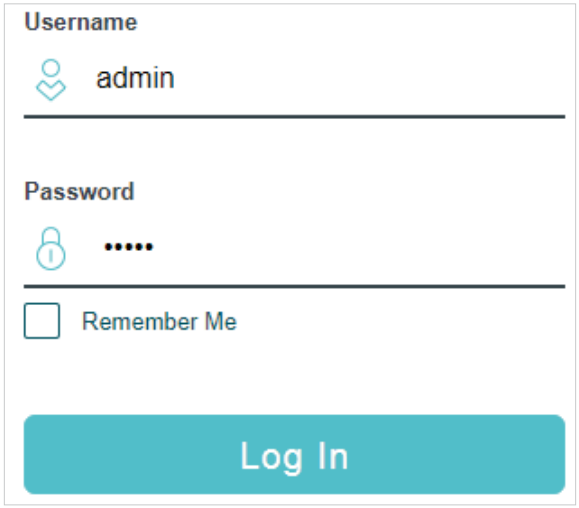
1) Make sure that the route between the host PC and the switch is available.
2) Launch a web browser. The supported web browsers include, but are not limited to, the following types:
   - IE 8.0, 9.0, 10.0, 11.0
   - Firefox 26.0, 27.0
   - Chrome 32.0, 33.0
3) Enter the switch's IP address in the web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



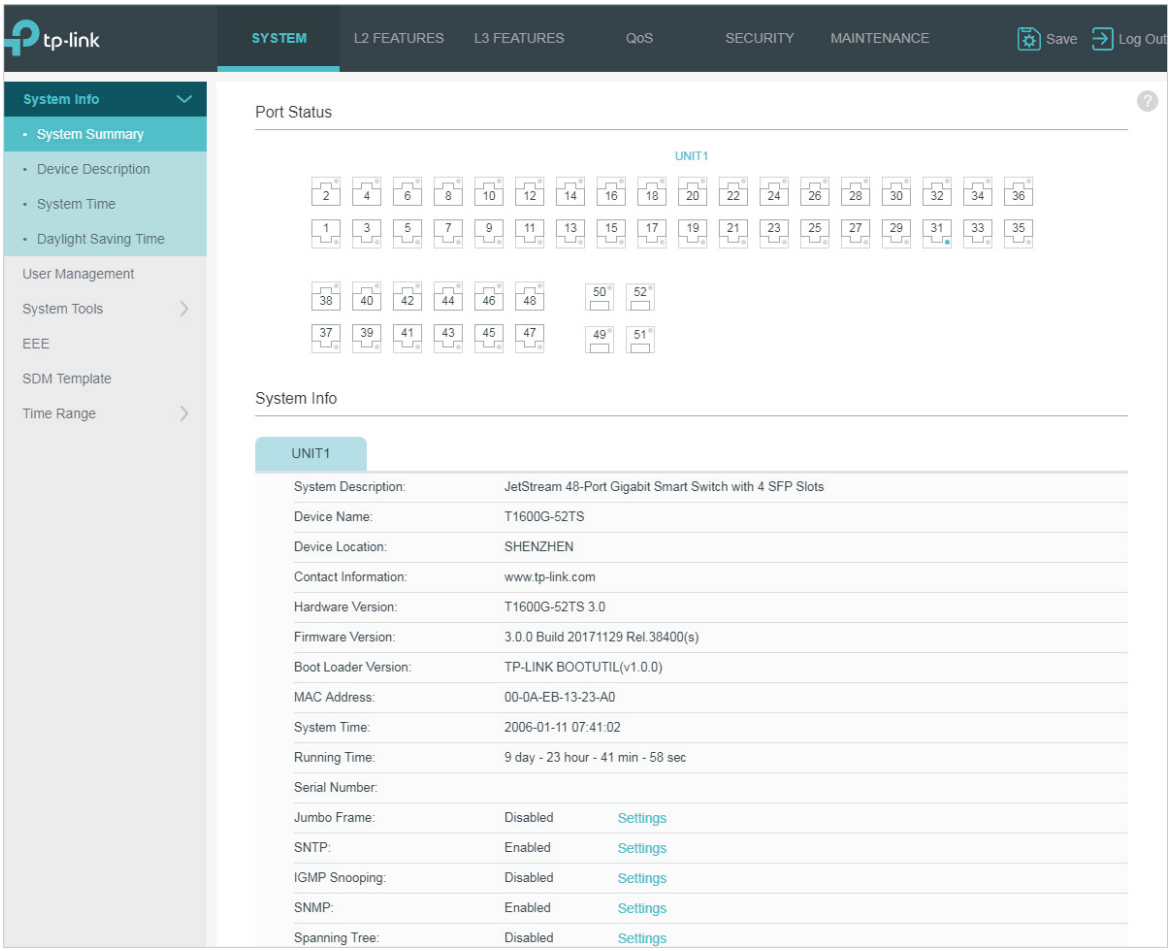
4) Enter the username and password in the pop-up login window. Use **admin** for both username and password in lower case letters.

   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



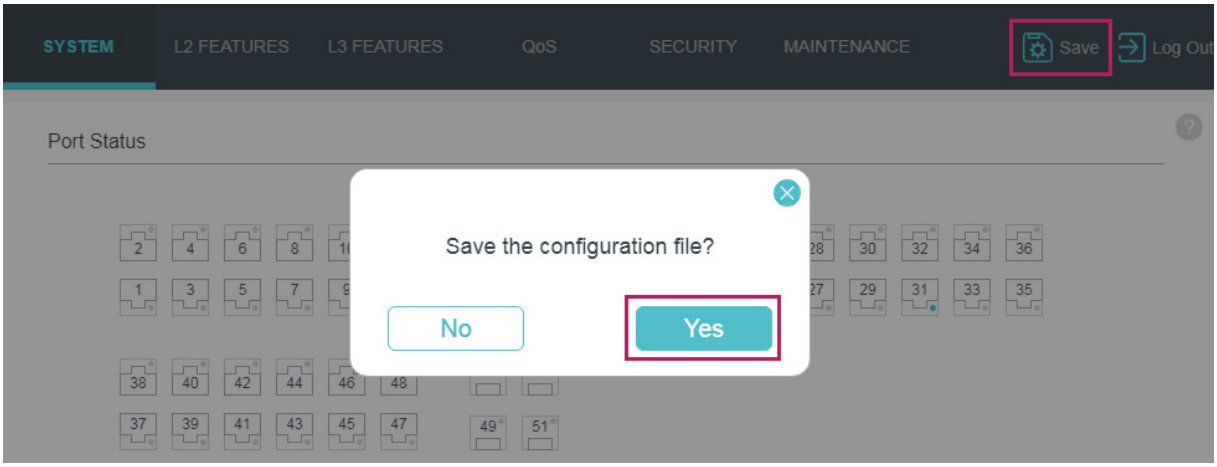
2.2 Save Config Function

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** function on the main interface to save the configurations in the start-up configuration file.

Figure 2-4 Save the Configuration

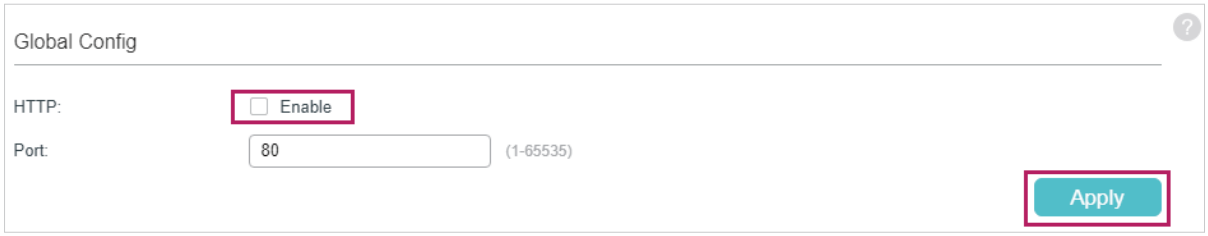


2.3 Disable the Web Server

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

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

Figure 2-5 Shut down HTTP server



Go to **SECURITY > 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

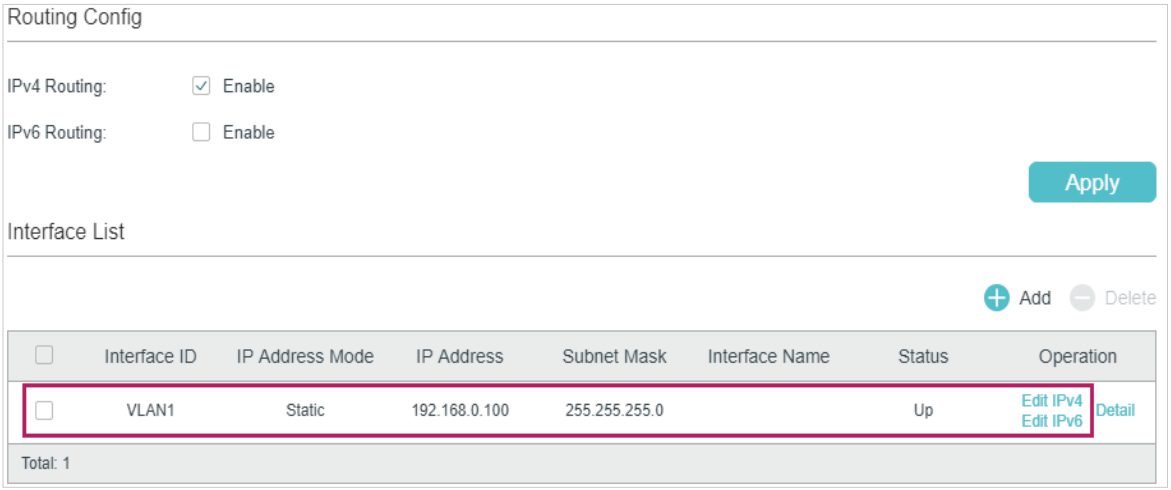
If you want to access the switch via a specified port (hereafter referred to as the access port), you can configure the port as a routed port and specify its IP address, or configure the IP address of the VLAN which the access port belongs to.

- 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.

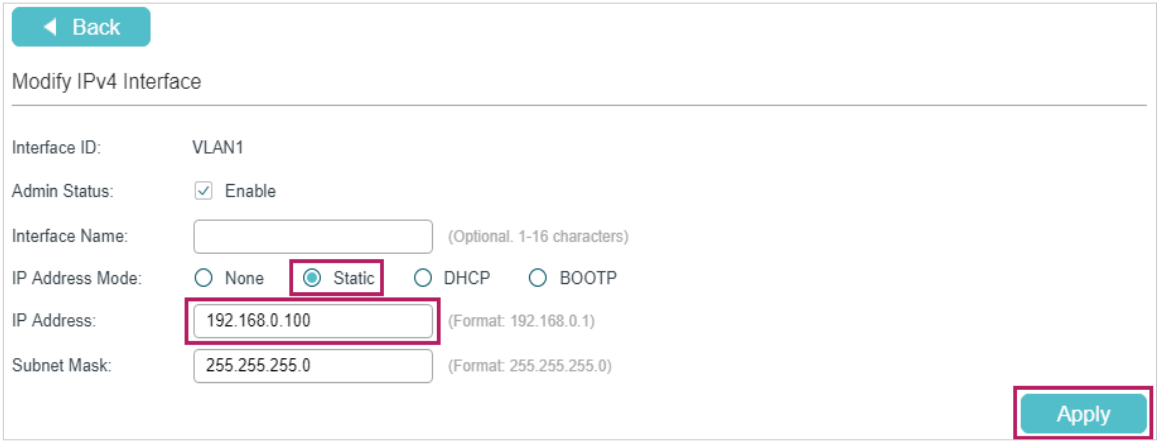
1) Go to **L3 FEATURES > Interface**. The default access IP address in VLAN 1 in the Interface List. Click **Edit IPv4** to modify VLAN1's IP address.

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.

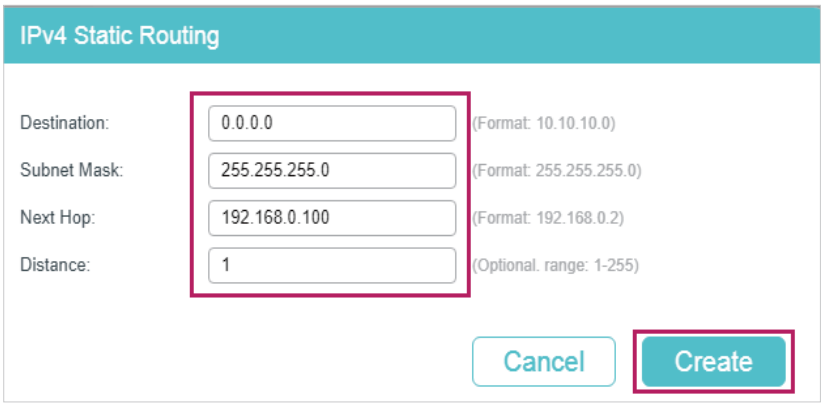
4) Click Save to save the settings.

- 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 **L3 FEATURES > Static Routing > IPv4 Static Routing**. Click Add to load the following page and configure the parameters related to the switch's gateway. Then click **Create**.

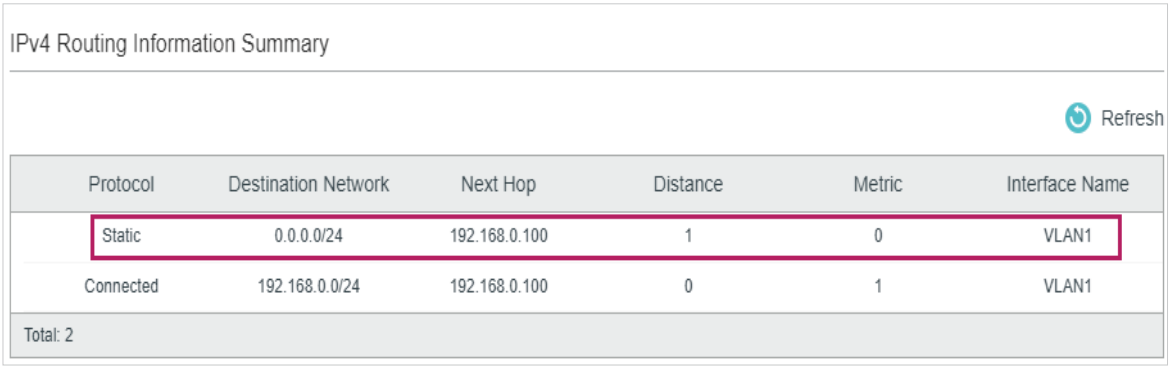
Figure 2-9 Configure the default gateway



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 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



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

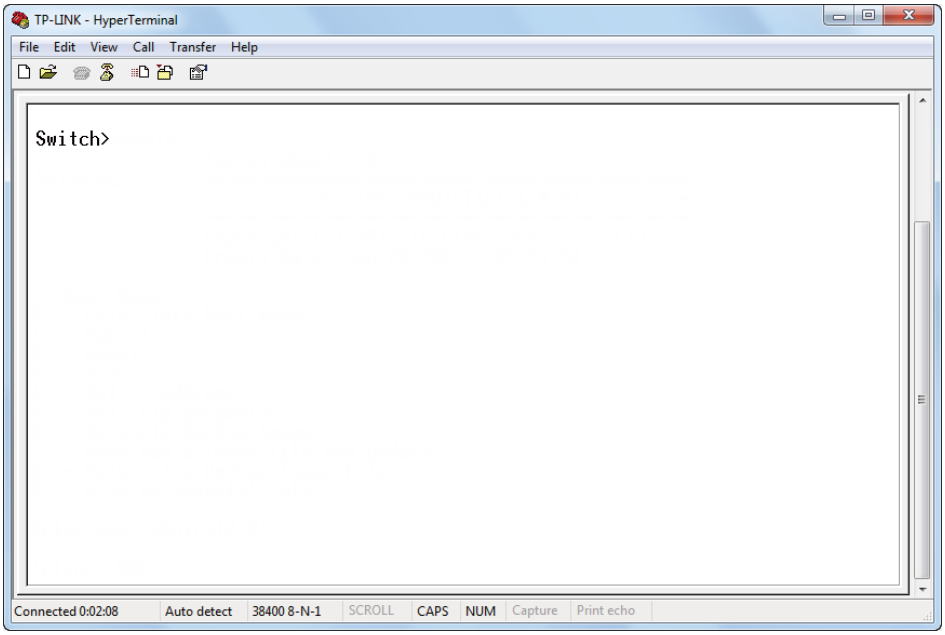
Method	Using Port	Typical Applications
Console	Console port (connected directly)	Hyper Terminal
Telnet	RJ-45 port	CMD
SSH	RJ-45 port	Putty

3.1 Console Login (only for switch with console port)

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

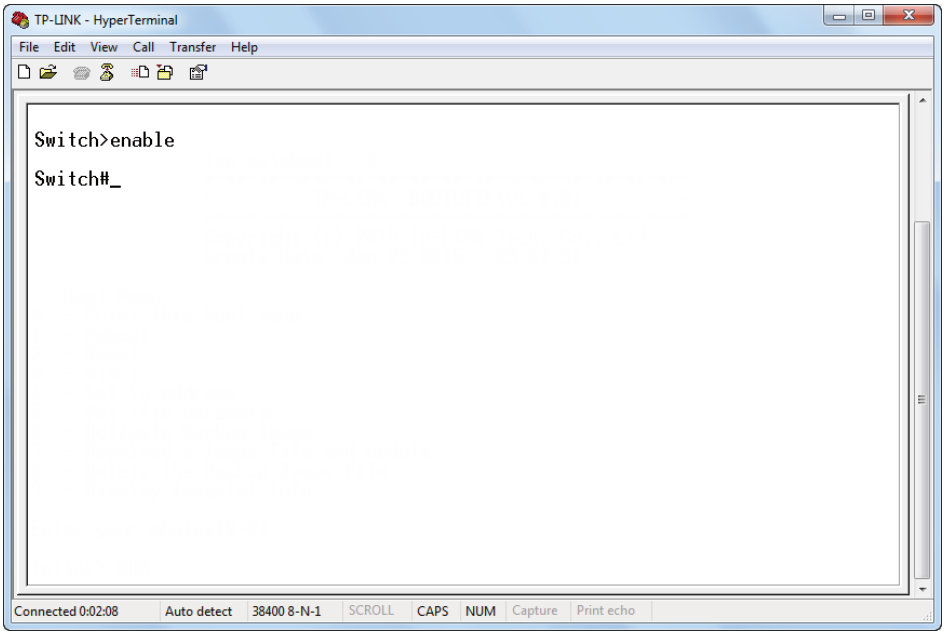
1) Connect the PC or terminal to the Console port on the switch with the serial cable.
2) Start the terminal emulation program (such as the Hyper Terminal) on the PC and configure the terminal emulation program as follows:
   - Baud Rate: 38400bps
   - Data Bits: 8
   - Parity: None
   - Stop Bits: 1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

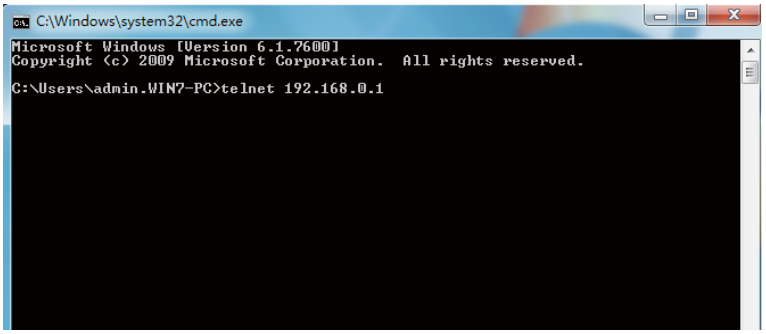
1) Make sure the switch and the PC are in the same LAN (Local Area Network). Click **Start** and type in **cmd** in the Search bar and press **Enter**.

Figure 3-3 Open the cmd Window



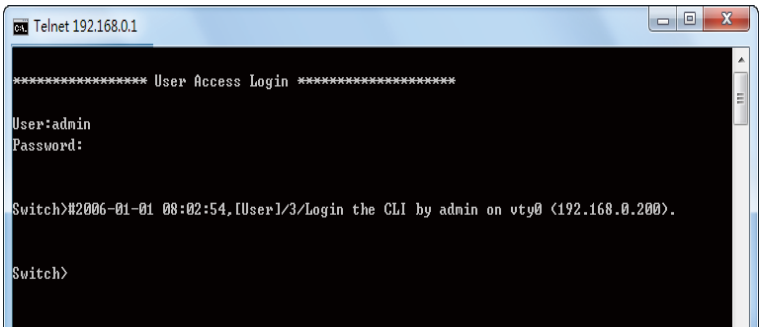
2) Type in **telnet 192.168.0.1** in the cmd window and press **Enter**.

Figure 3-4 Log In to the Switch



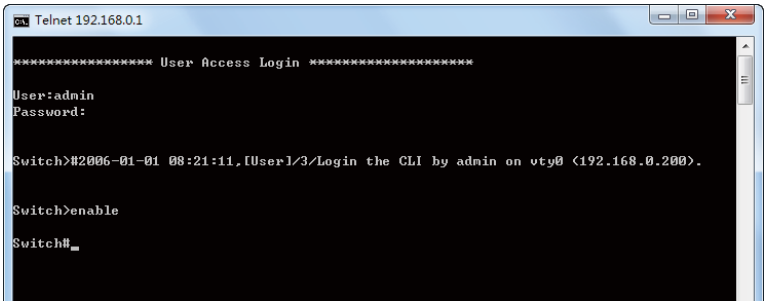
3) Type in the login username and password (both **admin** by default). Press **Enter** and you will enter User EXEC Mode.

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.

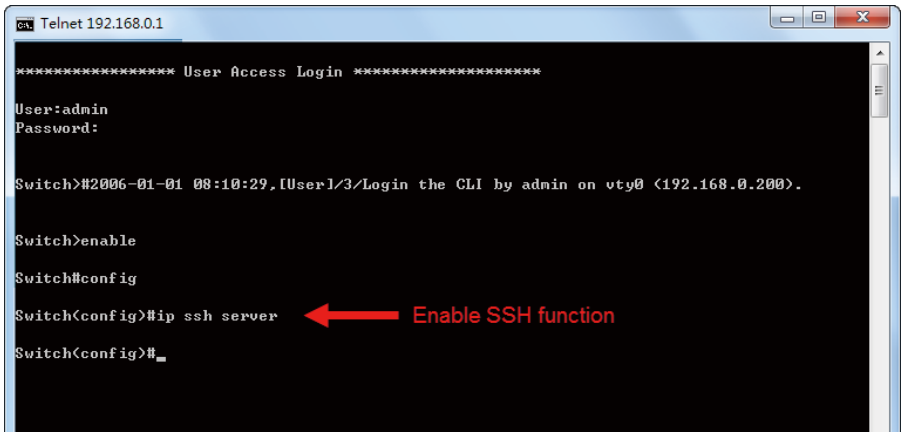
3.3 SSH Login

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:

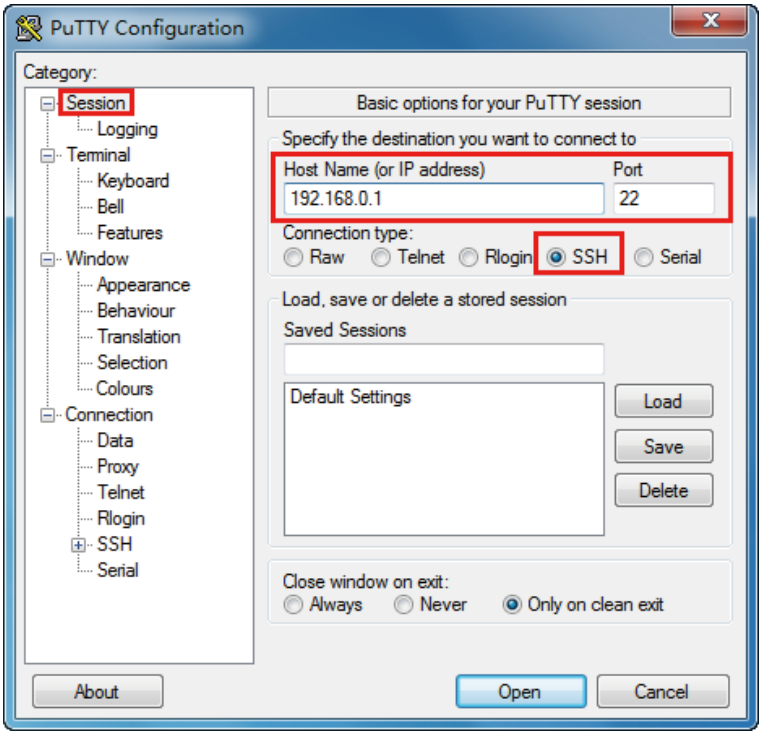
Figure 3-7 Enable SSH



Password Authentication Mode

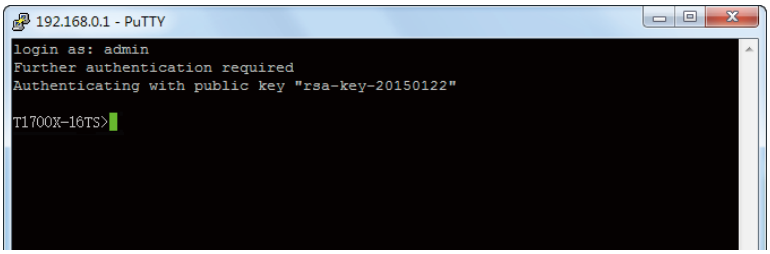
1) Open PuTTY and go to the Session page. Enter the IP address of the switch in the **Host Name** field and keep the default value 22 in the **Port** field; select **SSH** as the Connection type. Click **Open**.

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.

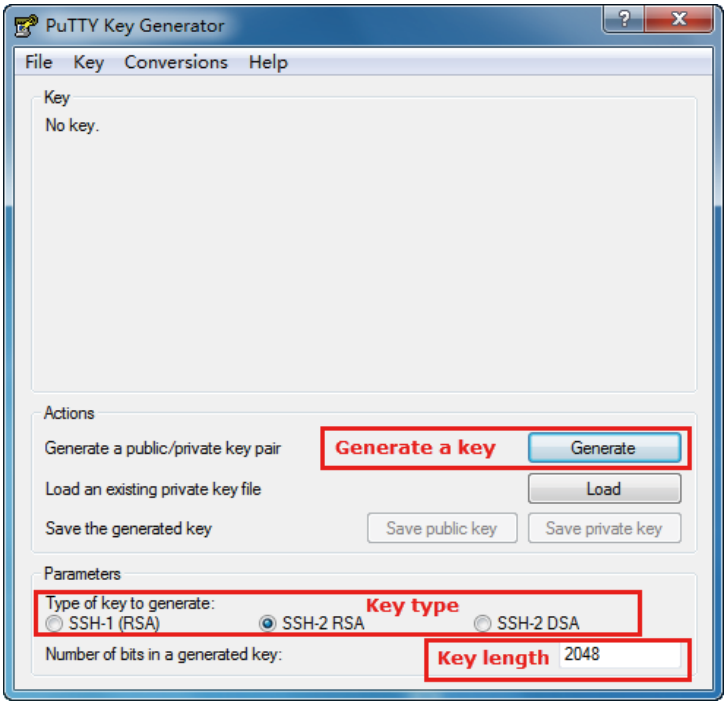
Figure 3-9 Log In to the Switch



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

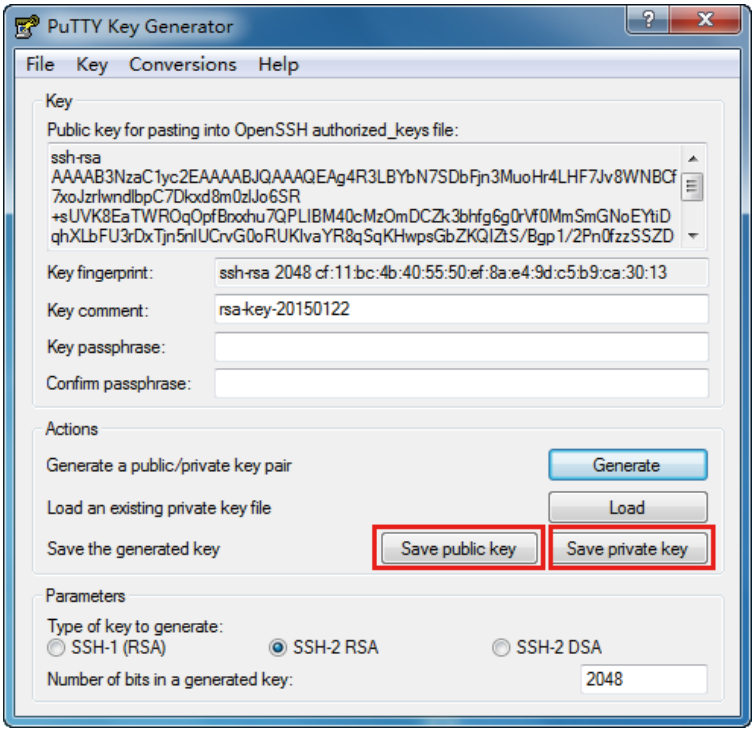


Note:

- 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.

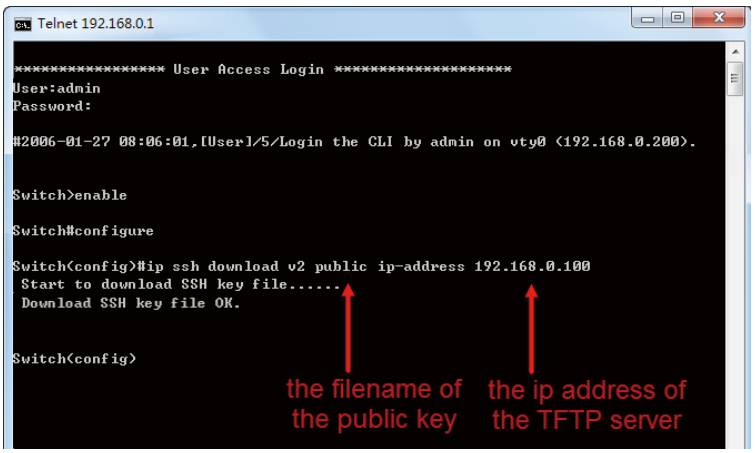
2) After the keys are successfully generated, click **Save public key** to save the public key to a TFTP server; click **Save private key** to save the private key to the host PC.

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

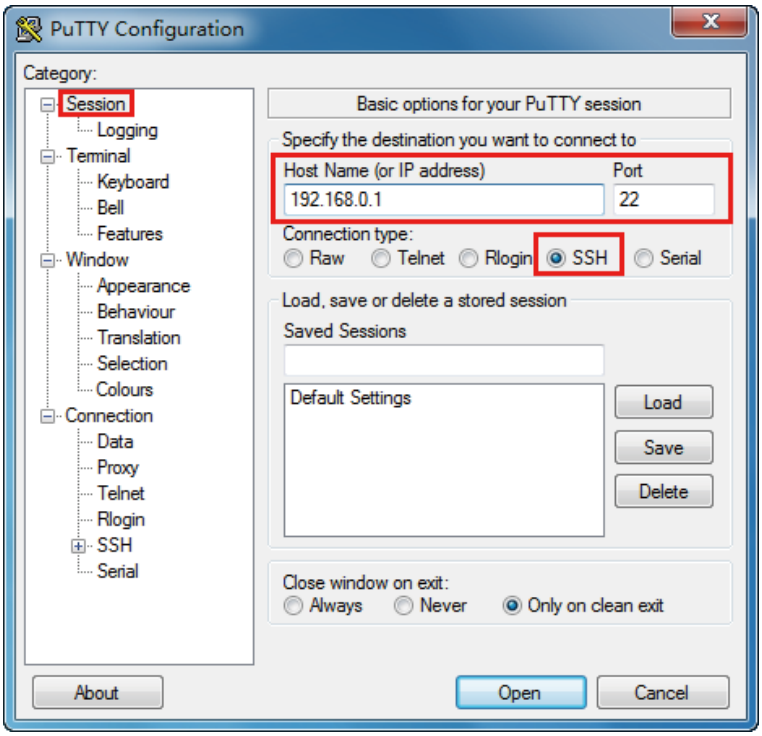


Note:

- 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.

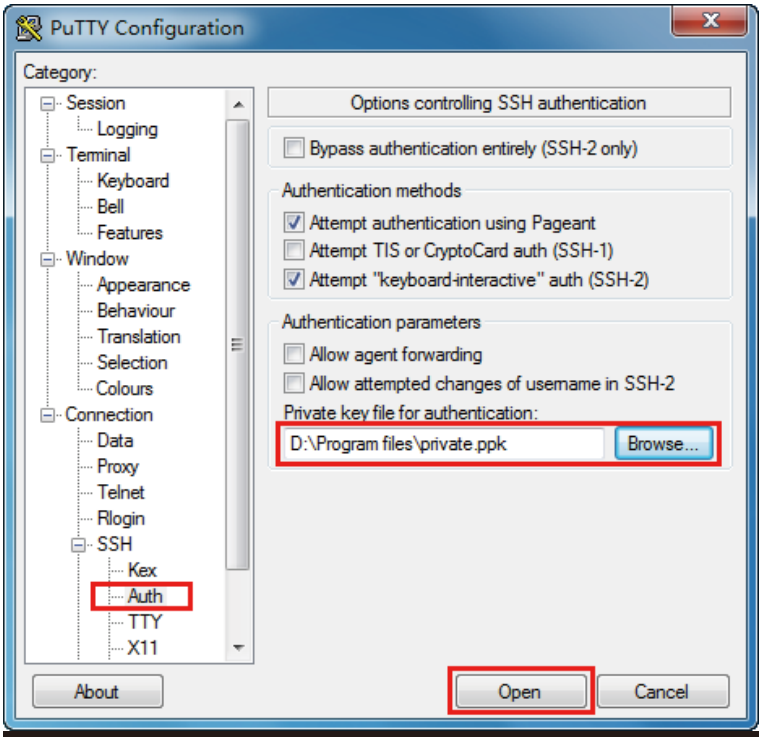
4) After the public key is downloaded, open PuTTY and go to the **Session** page. Enter the IP address of the switch and select **SSH** as the Connection type (keep the default value in the Port field).

Figure 3-13 Configure the Host Name and Connection Type



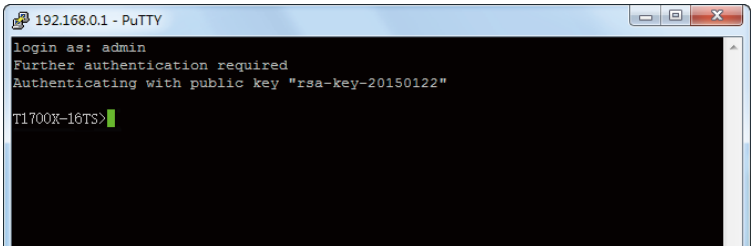
5) Go to **Connection > SSH > Auth**. Click **Browse** to download the private key file to PuTTY. Click **Open** to start the connection and negotiation.

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



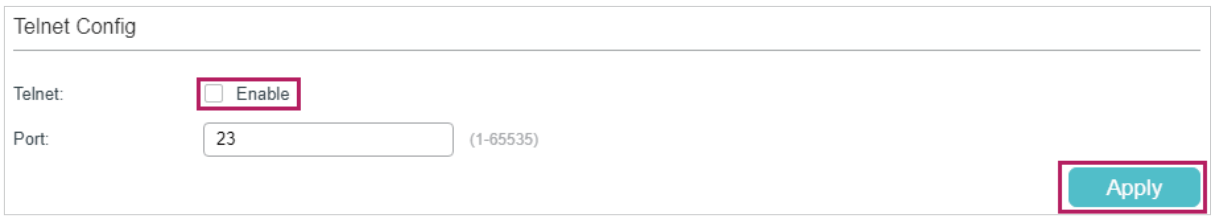
3.4 Disable Telnet login

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

- Using the GUI:

Go to **SECURITY > 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 **SECURITY > 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. EEE Configuration
6. PoE Configurations
7. SDM Template Configuration
8. Time Range Configuration
9. Example for PoE Configurations
10. Appendix: Default Parameters

1 System

1.1 Overview

In System module, you can view the system information and configure the system parameters and features of the switch.

1.2 Supported Features

System Info

You can view the switch's port status and system information, and configure the device description, system time, and daylight saving time.

User Management

You can manage the user accounts for login to the switch. There are multiple user types which have different access levels, and you can create different user accounts according to your need.

System Tools

You can configure the boot file of the switch, backup and restore the configurations, update the firmware, reset the switch, and reboot the switch.

EEE

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

PoE

Note:

Only T1600G-52PS supports PoE feature.

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.

SDM Template

SDM (Switch Database Management) Template is used to prioritize hardware resources for certain features. The switch provides three templates which allocate different hardware resources for different usage, and you can choose one according to your need.

Time Range

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

2 System Info Configurations

With system information configurations, you can:

- View the System Summary
- Configure the Device Description
- Configure the System Time
- Configure the Daylight Saving Time

2.1 Using the GUI

2.1.1 Viewing the System Summary

Choose the menu **SYSTEM** > **System Info** > **System Summary** to load the System Summary page. You can view the port status and system information of the switch.

Viewing the Port Status

In the **Port Status** section, you can view the status and bandwidth utilization of each port.

Figure 2-1 Viewing the System Summary

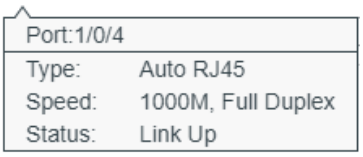


The following table introduces the meaning of each port status:

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.
	Indicates the SFP port is at the speed of 100Mbps.

You can move your cursor to a port to view the detailed information of the port.

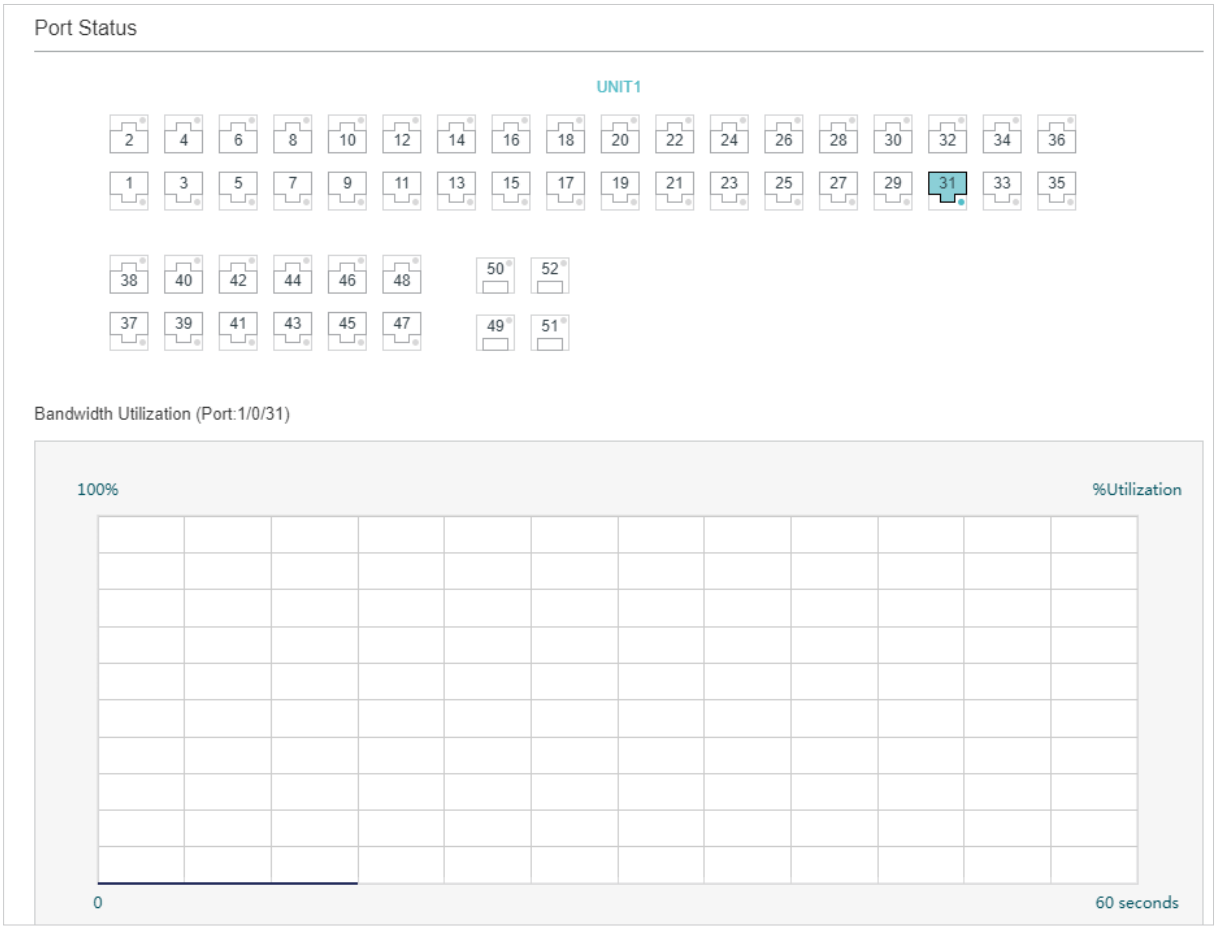
Figure 2-2 Port Information



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

You can click a port to view the bandwidth utilization on this port.

Figure 2-3 Bnadwidth Utilization

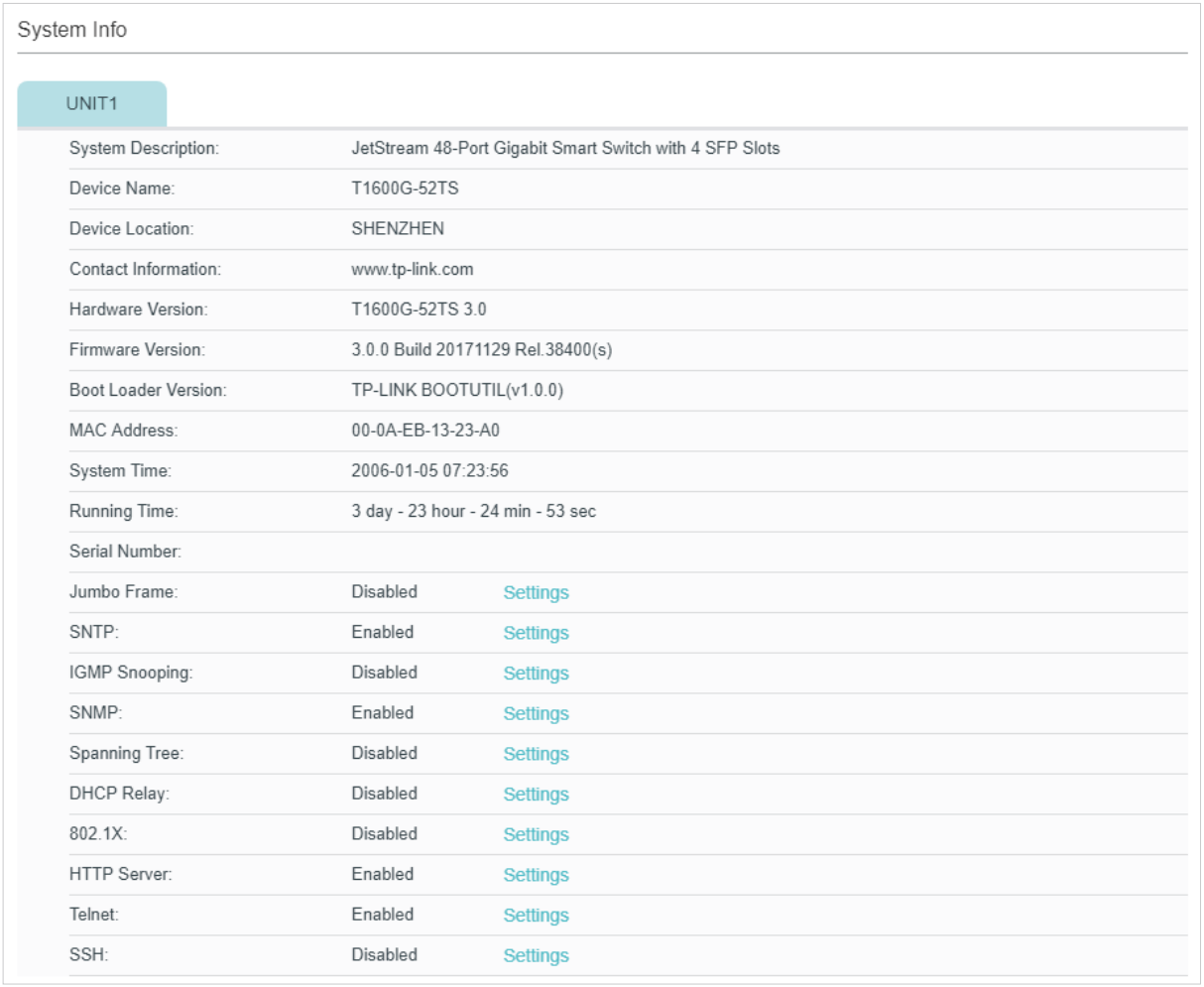


RX	Displays the bandwidth utilization of receiving packets on this port.
TX	Displays the bandwidth utilization of sending packets on this port.

Viewing the System Information

In the **System Info** section, you can view the system information of the switch.

Figure 2-4 System Information



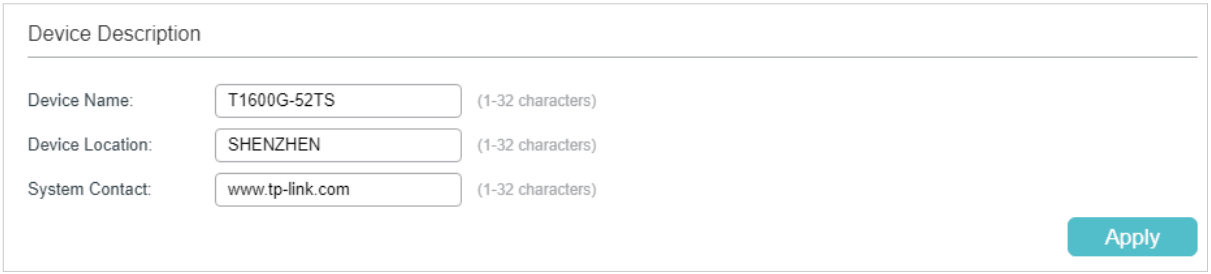
System Description	Displays the system description of the switch.
Device Name	Displays the name of the switch. You can edit it on the Device Description page.
Device Location	Displays the location of the switch. You can edit it on the Device Description page.
Contact Information	Displays the contact information of the switch. You can edit it on the Device Description page.
Hardware Version	Displays the hardware version of the switch.
Firmware Version	Displays the firmware version of the switch.
Boot Loader Version	Displays the boot loader version of the switch.

MAC Address	Displays the MAC address of the switch.
System Time	Displays the system time of the switch.
Running Time	Displays the running time of the switch.
Serial Number	Displays the serial number of the switch.
Jumbo Frame	Displays whether Jumbo Frame is enabled. You can click **Settings** to jump to the Jumbo Frame configuration page.
SNTP	Displays whether the switch gets system time from NTP Server. You can click **Settings** to jump to the System Time configuration page.
IGMP Snooping	Displays whether IGMP Snooping is enabled. You can click **Settings** to jump to the IGMP Snooping configuration page.
SNMP	Displays whether SNMP is enabled. You can click **Settings** to jump to the SNMP configuration page.
Spanning Tree	Displays whether Spanning Tree is enabled. You can click **Settings** to jump to the Spanning Tree configuration page.
DHCP Relay	Displays whether DHCP Relay is enabled. You can click **Settings** to jump to the DHCP Relay configuration page.
802.1x	Displays whether Jumbo Frame is enabled. You can click **Settings** to jump to the Jumbo Frame configuration page.
HTTP Server	Displays whether HTTP server is enabled. You can click **Settings** to jump to the HTTP configuration page.
Telnet	Displays whether Telnet is enabled. You can click **Settings** to jump to the Telnet configuration page.
SSH	Displays whether SSH is enabled. You can click **Settings** to jump to the SSH configuration page.

2.1.2 Configuring the Device Description

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

Figure 2-5 Configuring the Device Description



1) In the **Device Description** section, configure the following parameters.

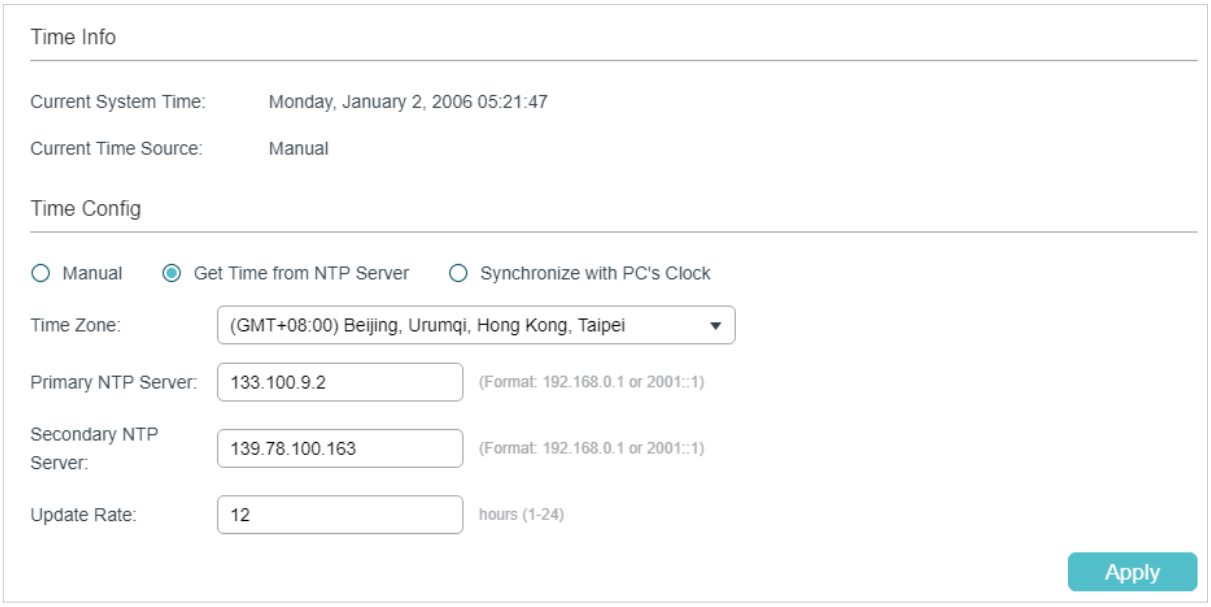
Device Name	Specify a name for the switch.
Device Location	Enter the location of the switch.
System Contact	Enter the contact information.

2) Click **Apply**.

2.1.3 Configuring the System Time

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

Figure 2-6 Configuring the System Time



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

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

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 related parameters.

Manual	Set the system time manually. **Date**: Specify the date of the system. **Time**: Specify the time of the system.

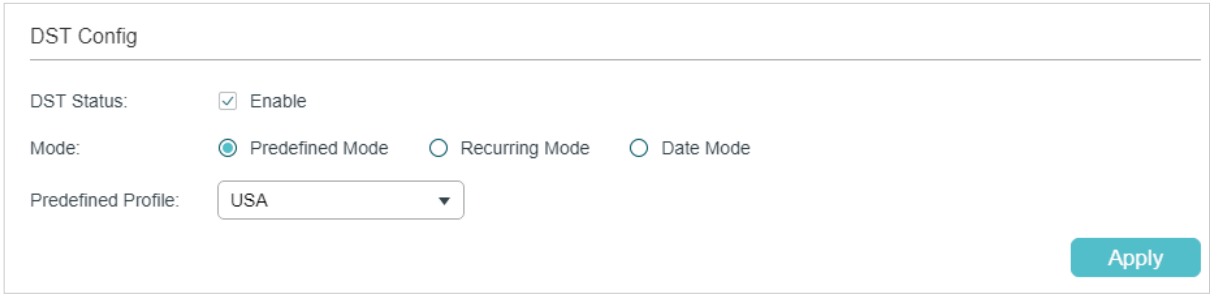
Get Time from NTP Server	Get the system time from an NTP server. Make sure the NTP server is accessible on your network. If the NTP server is on the internet, connect the switch to the internet first. **Time Zone**: Select your local time zone. **Primary Server**: Enter the IP Address of the primary NTP server. **Secondary Server**: Enter the IP Address of the secondary NTP server. Once the primary NTP server is down, the switch can get the system time from the secondary NTP server. **Update Rate**: Specify the interval the switch fetching time from NTP server, which ranges from 1 to 24 hours.
Synchronize with PC's Clock	Synchronize the system time with the clock of your currently logged-in host.

2) Click **Apply**.

2.1.4 Configuring the Daylight Saving Time

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

Figure 2-7 Configuring the Daylight Saving Time



Follow these steps to configure Daylight Saving Time:

1) In the **DST Config** section, enable the Daylight Saving Time function.
2) Choose one method to set the Daylight Saving Time and specify the related parameters.

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**.

2.2 Using the CLI

2.2.1 Viewing the System Summary

On privileged EXEC mode or any other configuration mode, you can use the following commands 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

...

Switch#show system-info

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

System Name - T1600G-52TS

System Location - SHENZHEN

Contact Information - www.tp-link.com

Hardware Version - T1600G-52TS 3.0

Software Version - 3.0.0 Build 20171029 Rel.38400(s)

Bootloader Version - TP-LINK BOOTUTIL(v1.0.0)

Mac Address - 00-0A-EB-13-23-A0

Serial Number -

System Time - 2017-10-27 11:23:32

Running Time - 1 day - 2 hour - 33 min - 42 sec

2.2.2 Configuring the Device Description

Follow these steps to configure the device description:

Step 1	**configure** Enter global configuration mode.
Step 2	**hostname [** *hostname* **]** Specify the system name of the switch. *hostname*: Enter the device 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 http://www.tp-link.com.

Switch#configure

Switch(config)#hostname Switch_A

Switch(config)#location BEIJING

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

Switch(config)#show system-info

System Description - JetStream 24-Port Gigabit L2 Managed Switch with 4 SFP Slots

System Name - Switch_A

System Location - BEIJING

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

...

Switch(config)#end

Switch#copy running-config startup-config

2.2.3 Configuring the System Time

Follow these steps to configure the system time:

Note:

The mode of Synchronize with PC's Clock does not support CLI command.

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. Ensure the NTP server is accessible. If the NTP server is on the internet, connect the switch to the internet first.

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

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 Configuring the Daylight Saving Time

Follow these steps to configure 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, 2017, set the end time as 01:00 September 1st,2017 and set the offset as 50.

Switch#configure

Switch(config)#system-time dst date Aug 1 01:00 2017 Sep 1 01:00 2017 50

Switch(config)#show system-time dst

DST starts at 01:00:00 on Aug 1 2017

DST ends at 01:00:00 on Sep 1 2017

DST offset is 50 minutes

DST configuration is one-off

Switch(config)#end

Switch#copy running-config startup-config

3 User Management Configurations

With User Management, you can create and manage the user accounts for login to the switch.

3.1 Using the GUI

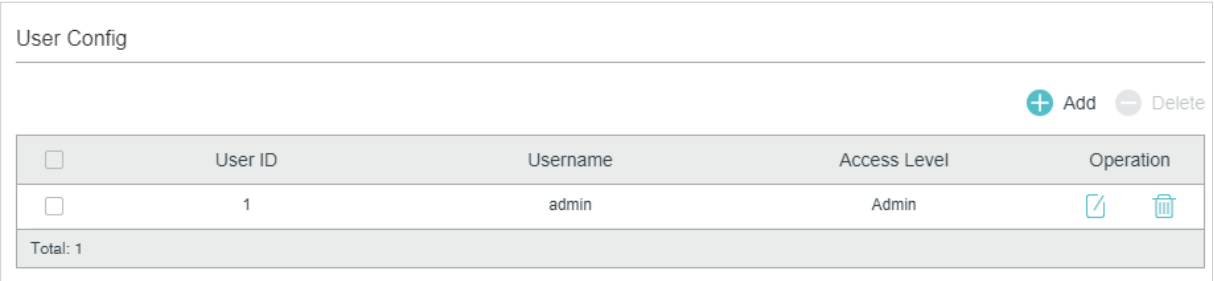
There are four types of user accounts with different access levels: Admin, Operator, Power User and User.

- There is a default Admin account which cannot be deleted. The default username and password of this account are both admin. You can also create more Admin accounts.
- If you create Operator, Power User or User accounts, you need go to the AAA section to create an Enable Password. If needed, these types of users can use the Enable Password to change their access level to Admin.

3.1.1 Creating Accounts

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

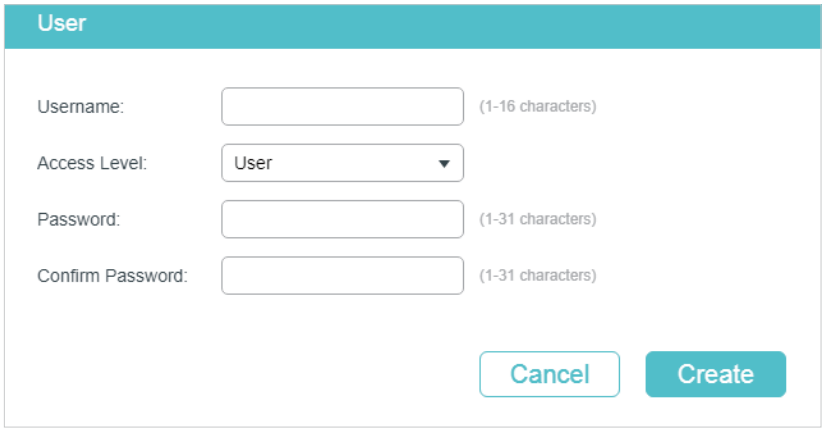
Figure 3-1 User Config Page



By default, there is a default Admin account in the table. You can click to edit this Admin account but you cannot delete it.

You can create new user accounts. Click Add and the following window will pop up.

Figure 3-2 Adding Account



Follow these steps to create a new user account.

1) Configure the following parameters:

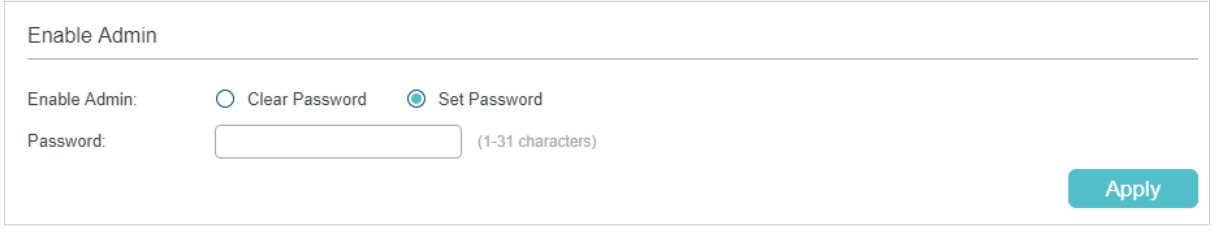
Username	Specify a username for the account. It contains 16 characters at most, composed of digits, English letters and underscore only.
Access Level	Select the access level. There are four options provided: **Admin**: Admin can edit, modify and view all the settings of different functions. **Operator**: 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	Specify a password for the account. It contains 1-31 alphanumeric characters or symbols, composed of digits, English letters (case sensitive), underscore and sixteen special characters only.
Confirm Password	Retype the password.

2) Click **Create**.

3.1.2 Configuring Enable Password

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

Figure 3-3 Configure Enable Password



Follow these steps to configure Enable Password:

1) Select **Set Password** and specify the Enable Password in the **Password** field.
2) Click **Apply**.

Tips:

The logged-in users can enter the Enable Password on this page to get the administrative privileges.

3.2 Using the CLI

There are four types of user accounts with different access levels: Admin, Operator, Power User and User.

- There is a default Admin account which cannot be deleted. The default username and password of this account are both admin. You can also create more Admin accounts.
- If you create Operator, Power User or User accounts, you need go to the AAA section to create an Enable Password. If needed, these types of users can use the Enable Password to change their access level to Admin.

3.2.1 Creating Accounts

Follow these steps to create an 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 | operator | power_user | user **} password {** [0] *password* **|** 7 *encrypted-password* **}**

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

admin | operator | power_user | user: Specify the access level for the user. Admin can edit, modify and view all the settings of different functions. 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.: 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 32 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 | operator | power_user | user **} 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 | operator | power_user | user: Specify the access level for the user. Admin can edit, modify and view all the settings of different functions. 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.: 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 32 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 Configuring Enable Password

Follow these steps to create an account of other type:

Step 1	**configure** Enter global configuration mode.
Step 2	**aaa enable** Globally enable the AAA function.

Step 3	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 32 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 32 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 4	**show user account-list** Verify the information of the current users.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

Tips:

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 username as user1 and 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, you can:

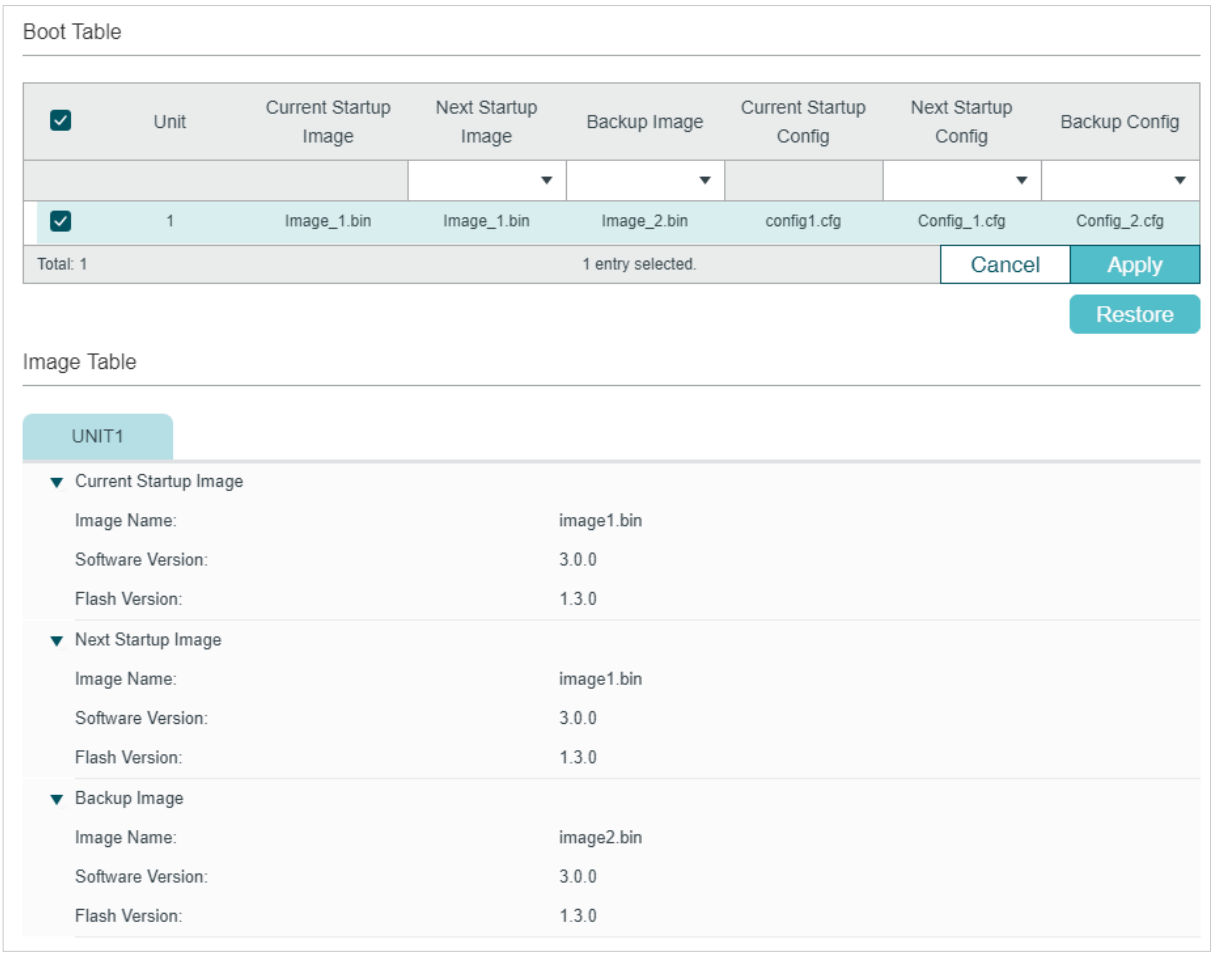
- Configure the boot file
- Restore the configuration of the switch
- Back up the configuration file
- Upgrade the firmware
- Reboot the switch
- Reset the switch

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.

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 image 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.
Current Startup Config	Displays the current startup configuration.
Next Startup Config	Specify the next startup configuration. When the switch is powered on, it will try to start up with the next startup configuration. The next startup configuration and backup configuration should not be the same.
Backup Config	Specify the backup configuration. When the switch fails to start up with the next startup configuration, it will try to start up with the backup configuration. The next startup and backup configuration should not be the same.

2) Click **Apply**.

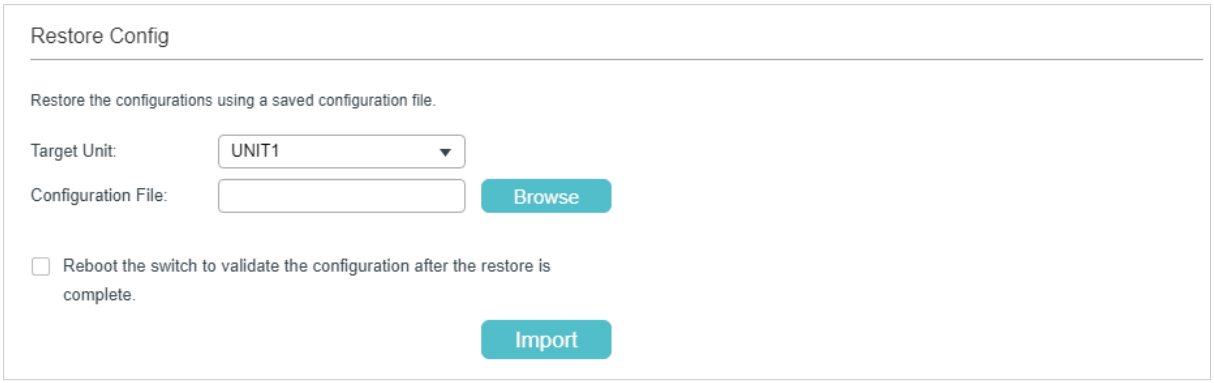
In the **Image Table**, you can view the information of the current startup image, next startup image and backup image. The displayed information is as follows:

Image Name	Displays the name of the image.
Software Version	Displays the software version of the image.
Flash Version	Displays the flash version of the image.

4.1.2 Restoring the Configuration of the Switch

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

Figure 4-2 Restoring the Configuration of the Switch



Follow these steps to restore the current configuration of the switch:

1) In the **Restore Config** section, select the unit to be restored.
2) Click **Browse** and select the desired configuration file to be imported.
3) Choose whether to reboot the switch after restoring is completed. Only after the switch is rebooted will the imported configuration take effect.
4) Click **Import** to import the configuration file.

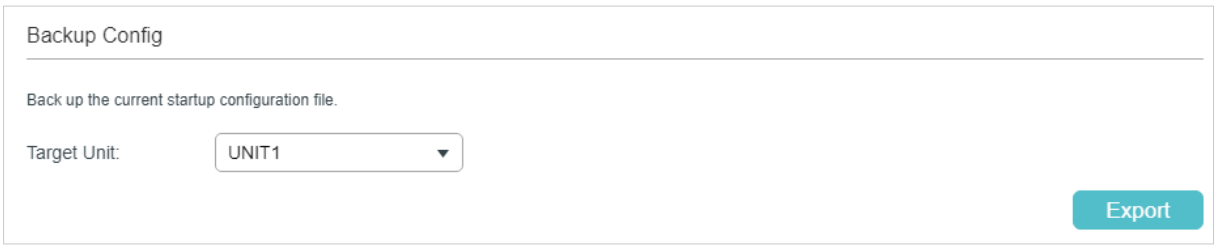
Note:

It will take some time to restore the configuration. Please wait without any operation.

4.1.3 Backing up the Configuration File

Choose the menu **SYSTEM** > **System Tools** > **Backup Config** 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.

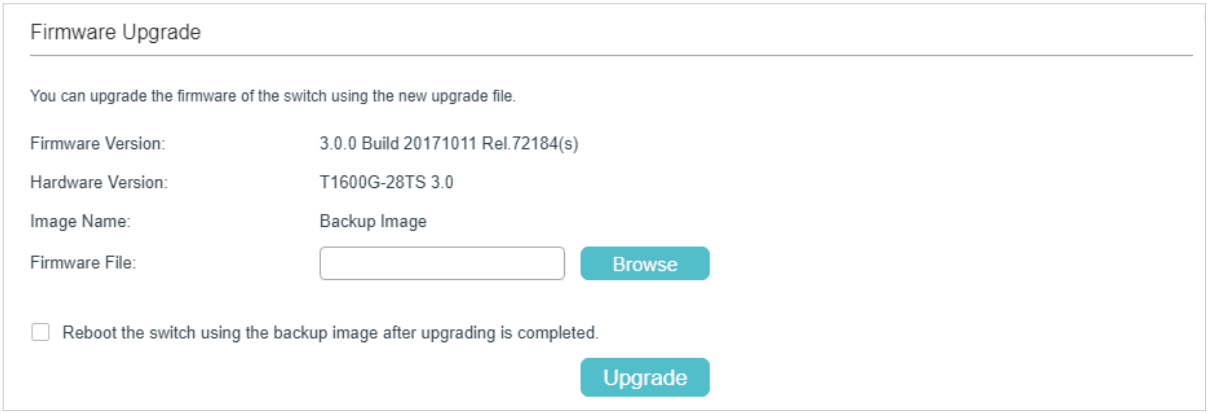
Note:

It will take some time to export the configuration. Please wait without any operation.

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



You can view the current firmware information on this page:

Firmware Version	Displays the current firmware version of the system.
Hardware Version	Displays the current hardware version of the system.
Image Name	Displays the image to upgrade. The operation will only affect the image displayed here.

Follow these steps to upgrade the firmware of the switch:

1) Click **Browse** and select the proper firmware upgrade file.
2) Choose whether to reboot the switch after upgrading is completed. Only after the switch is rebooted will the new firmware take effect.
3) Click **Upgrade** to upgrade the system.

Note:

- It will take some time to upgrade the switch. Please wait without any operation.
- It is recommended to backup your configuration before upgrading.

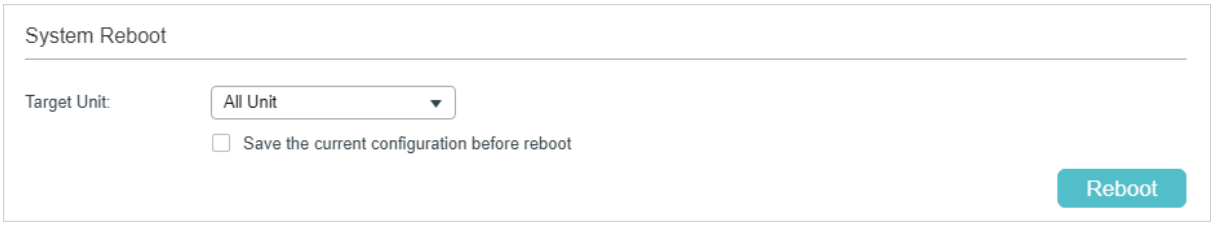
4.1.5 Rebooting the switch

There are two methods to reboot the switch: manually reboot the switch and configure reboot schedule to automatically reboot the switch.

Manually Rebooting the Switch

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

Figure 4-5 Manually Rebooting the Switch



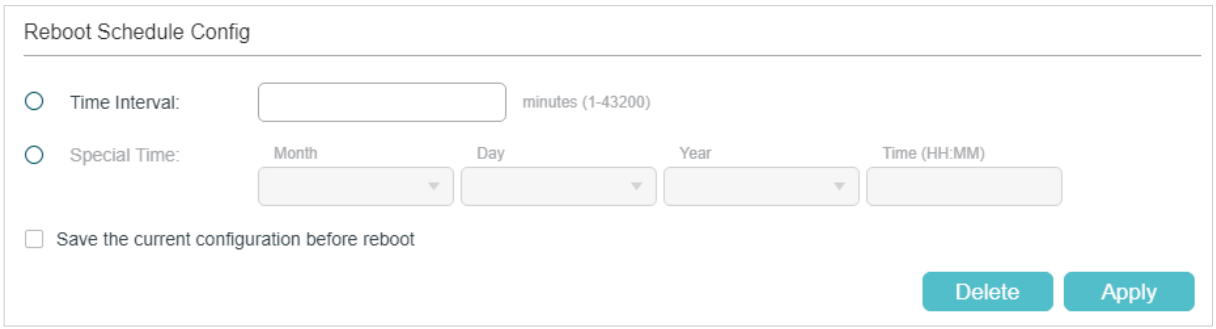
Follow these steps to reboot the switch:

1) In the **System Reboot** section, select the desired unit.
2) Choose whether to save the current configuration before reboot.
3) Click **Reboot**.

Configuring Reboot Schedule

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

Figure 4-6 Configuring the Reboot Schedule



Follow these steps to configure the reboot schedule:

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

Time Interval	Specify a period of time. The switch will reboot after this period. Valid values are from 1 to 43200 minutes. To make this schedule recur, you need to click Save to save current configuration or enable the option **Save the current configuration before reboot**.

Special Time	Specify the date and time for the switch to reboot. **Month/Day/Year:** Specify the date for the switch to reboot. **Time (HH:MM)**: Specify the time for the switch to reboot, in the format of HH:MM.

2) Choose whether to save the current configuration before the reboot.
3) Click **Apply**.

4.1.6 Reseting the Switch

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

Figure 4-7 Reseting the Switch



In the **System Reset** section, select the desired unit and click **Reset**. After reset, all configurations of the switch will be reset to the factory defaults.

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, image1.bin is the startup image and 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	**boot config filename {** config1 | config2 **} {** startup | backup **}** Specify the configuration of the boot file. By default, config1.cfg is the startup configuration file and config2.cfg is the backup configuration file. config1 | config2: Select the configuration file to be configured. startup | backup: Specify the property of the configuration file.
Step 4	**show boot** Verify the boot configuration of the system.

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 next startup image as image1, the backup image as image2, the next startup configuration file as config1 and the backup configuration file as config2.

Switch#configure

Switch(config)#boot application filename image1 startup

Switch(config)#boot application filename image2 backup

Switch(config)#boot config filename config1 startup

Switch(config)#boot config filename config2 backup

Switch(config)#show boot

Boot config:

Current Startup Image - image2.bin

Next Startup Image - image1.bin

Backup Image - image2.bin

Current Startup Config - config2.cfg

Next Startup Config - config1.cfg

Backup Config - config2.cfg

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 some time to restore the configuration. Please wait without any operation.

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.cfg

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 to 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 and then enter Y to reboot the switch with the backup image.

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 Rebooting the Switch

Manually Rebooting the Switch

Follow these steps to reboot the switch:

Step 1	**enable** Enter privileged mode.
Step 2	**reboot** Reboot the switch.

Configuring Reboot Schedule

Follow these steps to configure the reboot schedule:

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

Step 2	Use the following command to set the interval of 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. To make this schedule recur, you can add this part to the command. Use the following command to set the special time of 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 will reboot 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 15/08/2017.

Switch#configure

Switch(config)#reboot-schedule at 12:00 15/08/2017 save_before_reboot

Reboot system at 15/08/2017 12:00. Continue? (Y/N): Y

Reboot Schedule Settings

Reboot schedule at 2017-08-15 12:00 (in 25582 minutes)

Save before reboot: Yes

Switch(config)#end

Switch#copy running-config startup-config

4.2.6 Reseting the Switch

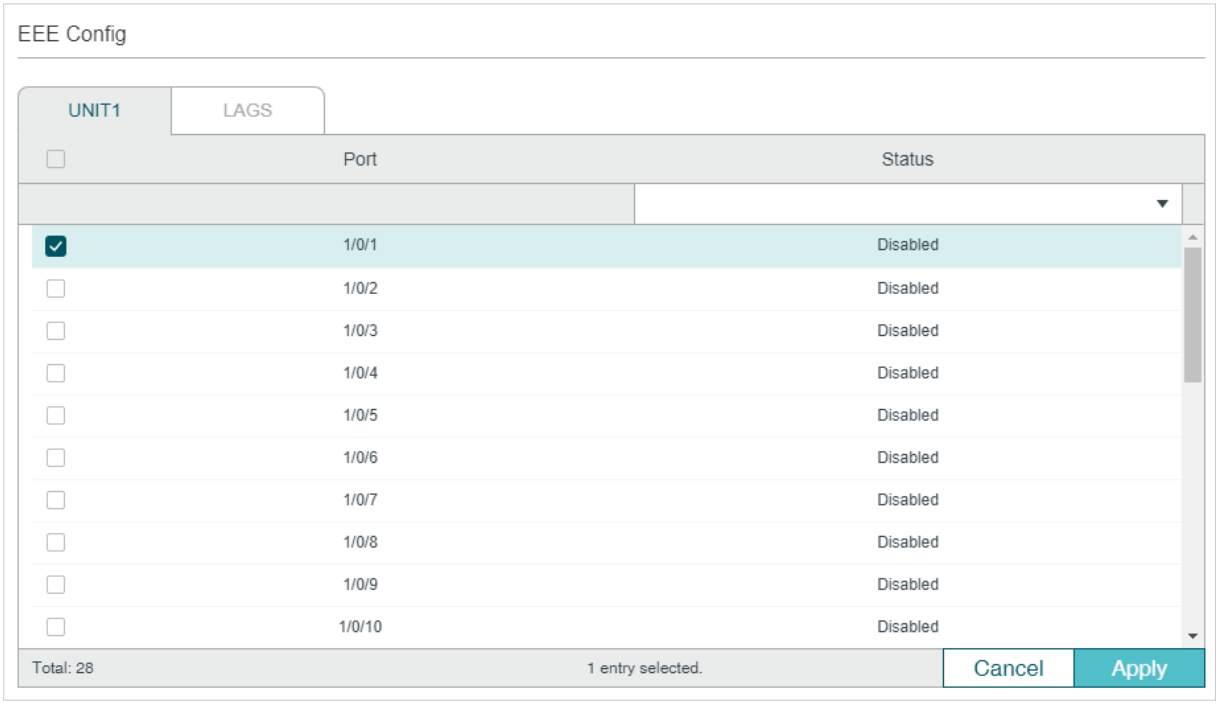
Follow these steps to reset the switch:

Step 1	**enable** Enter privileged mode.
Step 2	**reset** Reset the switch, and all configurations of the switch will be reset to the factory defaults.

5 EEE Configuration

Choose the menu **SYSTEM** > **EEE** to load the following page.

Figure 5-1 Configuring EEE



Follow these steps to configure EEE:

1) In the **EEE Config** section, select one or more ports to be configured.
2) Enable or disable EEE on the selected port(s).
3) Click **Apply**.

5.1 Using the CLI

Follow these steps to configure EEE:

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	**eee** Enable EEE on the port.

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 the EEE feature on port 1/0/1.

Switch#config

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

Switch(config-if)#eee

Switch(config-if)#show interface eee

Port EEE status

Gi1/0/1 Enable

Gi1/0/2 Disable

...

Switch(config-if)#end

Switch#copy running-config startup-config

6 PoE Configurations

Note:

Only T1600G-52PS supports PoE feature.

With the PoE feature, you can:

- Configure the PoE parameters manually
- Configure the PoE parameters using the profile

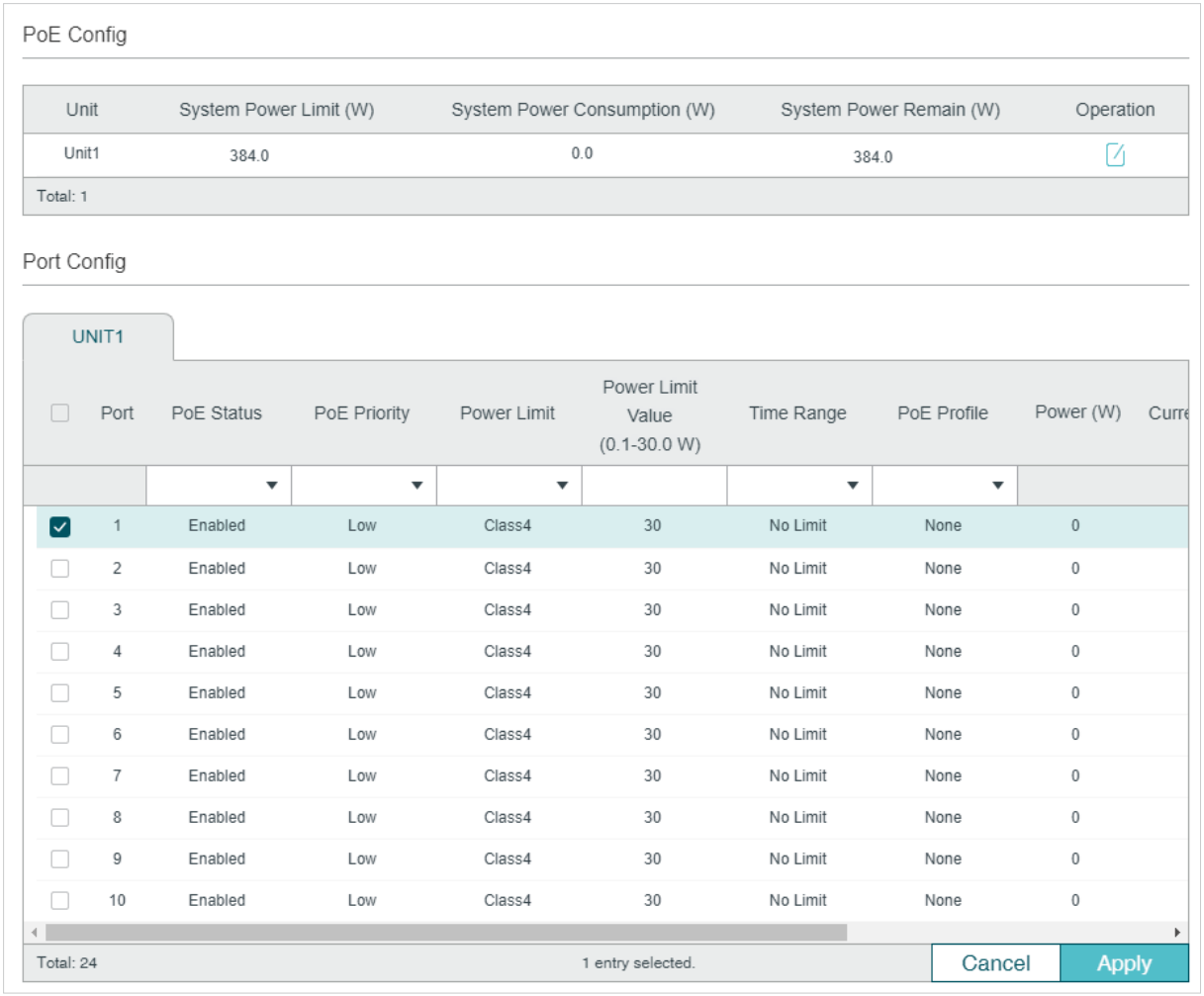
You can configure the PoE parameters one by one via configuring the PoE parameters manually. You can also set a profile with the desired parameters and bind the profile to the corresponding ports to quickly configure the PoE parameters.

6.1 Using the GUI

6.1.1 Configuring the PoE Parameters Manually

Choose the menu **SYSTEM > PoE** > **PoE Config** to load the following page.

Figure 6-1 Configuring PoE Parameters Manually



Follow these steps to configure the basic PoE parameters:

1) In the **PoE Config** section, you can view the current PoE parameters.

System Power Limit (w)	Displays the maximum power the PoE switch can supply.
System Power Consumption (w)	Displays the real-time system power consumption of the PoE switch.
System Power Remain (w)	Displays the real-time system remaining power of the PoE switch.

In addition, you can click and configure the System Power Limit. Click **Apply**.

Figure 6-2 Configuring System Power Limit



Unit	Displays the unit number.
System Power Limit	Specify the maximum power the PoE switch can supply.

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	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**: You can enter a value manually.
Power Limit Value (0.1w-30w)	If you select **Manual** as Power Limit mode, specify a maximum power supply value in this field. If you select **Class1** to **Class4** as Power Limit mode, you can view the maximum power supply value in this field.
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 Configuration*.

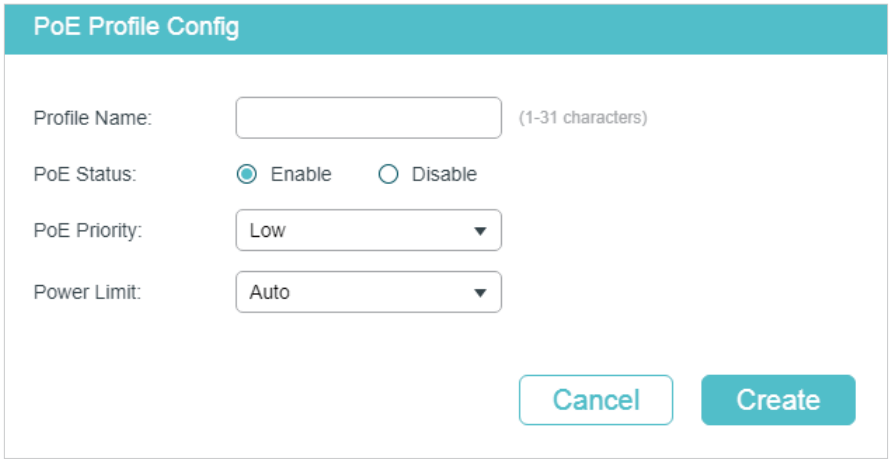
PoE Profile	A quick configuration method for the corresponding ports. If one profile is selected, you will not be able to modify PoE status, PoE priority or power limit manually. For how to create a profile, refer to *Configuring the PoE Parameters Using the Profile*.
Power (w)	Displays the port's real-time 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.

6.1.2 Configuring the PoE Parameters Using the Profile

■ Creating a PoE Profile

Choose the menu **SYSTEM > PoE > PoE Profile** and click Add to load the following page.

Figure 6-3 Creating 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.

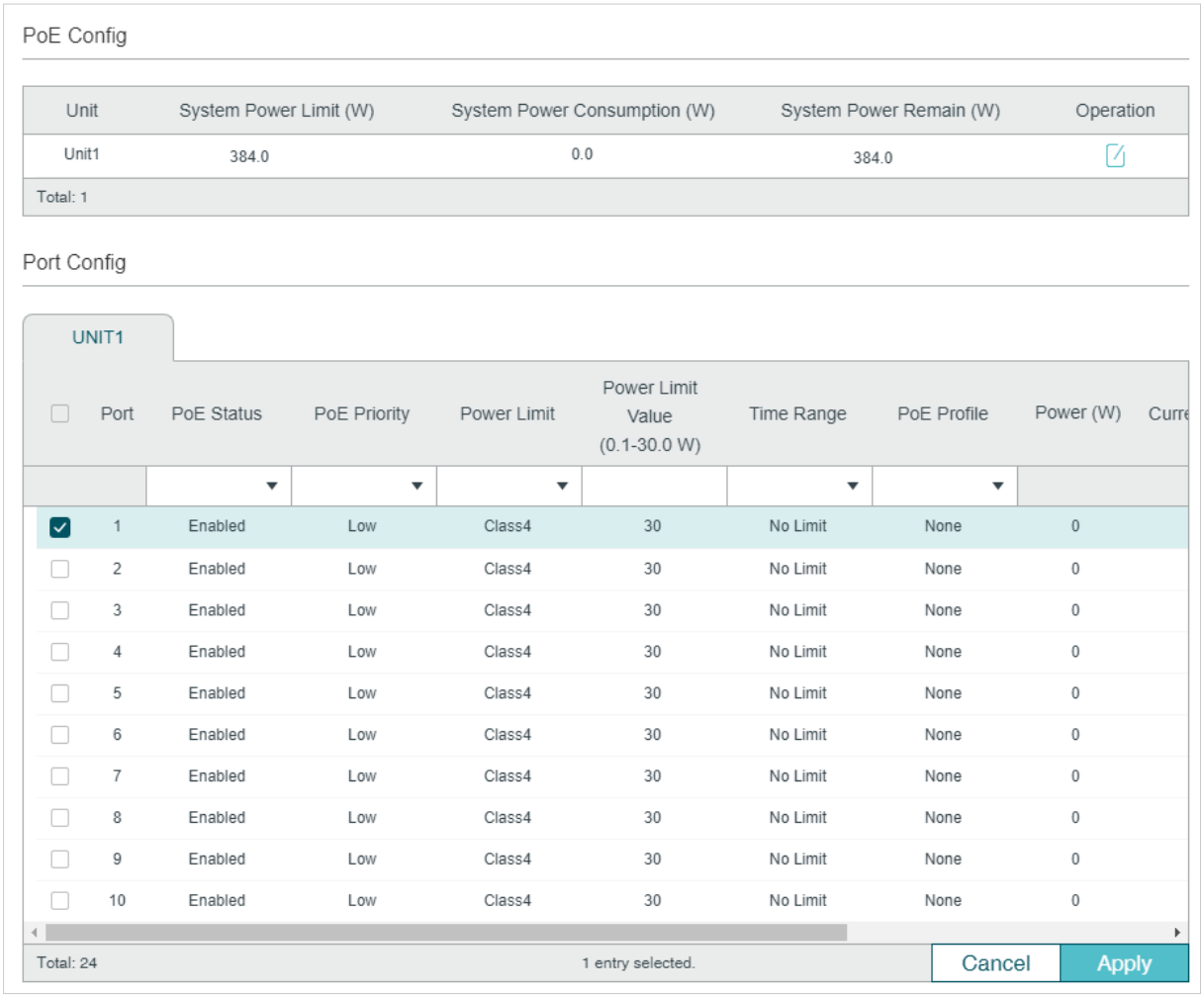
Profile Name	Specify a name for the PoE profile.
PoE Status	Specify the PoE status for the PoE profile.
PoE Priority	Specify the priority level for the PoE profile. The following options are provided: **High**, **Middle** and **Low**. When the supply power exceeds the system power limit, the switch will 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 (4w)**: The maximum power that the port can supply is 4W. **Class2 (7w)**: The maximum power that the port can supply is 7W. **Class3 (15.4w)**: The maximum power that the port can supply is 15.4W. **Class4 (30w)**: The maximum power that the port can supply is 30W. **Manual**: Enter a value manually.

2) Click **Create**.

Binding the Profile to the Corresponding Ports

Choose the menu **SYSTEM > PoE** > **PoE Config** to load the following page.

Figure 6-4 Binding the Profile to the Corresponding Ports



Follow these steps to bind the profile to the corresponding ports:

1) In the **PoE Config** section, you can view the current PoE parameters.

System Power Limit (w)	Displays the maximum power the PoE switch can supply.
System Power Consumption (w)	Displays the real-time system power consumption of the PoE switch.
System Power Remain (w)	Displays the real-time system remaining power of the PoE switch.

In addition, you can click and configure the System Power Limit. Click **Apply**.

Figure 6-5 Configuring System Power Limit



Unit	Displays the unit number.
System Power Limit	Specify the maximum power the PoE switch can supply.

2) In the **Port Config** section, select one or more ports and configure the following two parameters: Time Range and PoE Profile. Click **Apply** and the PoE parameters of the selected PoE Profile, such as PoE Status and PoE Priority, will be displayed in the table.

PoE Status	Displays the PoE function for on corresponding port. The port can supply power to the PD when its status is enable.
PoE Priority	Displays 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	Displays the maximum power the corresponding port can supply.
Power Limit Value (0.1W-30.0W)	Displays the power limit value.
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 Configuration*.
PoE Profile	Select the PoE profile 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.

6.2 Using the CLI

6.2.1 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 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* **| 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.
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	**time-range** *name* Specify a time range for the port. Then the port will supply power only during the time range. For how to create a time range, refer to *Time Range Configuration*. *name:* Specify the name of the time range.
Step 8	**show power inline** Verify the global PoE information of the system.

Step 9	**show power inline configuration interface [fastEthernet { *port* | *port-list* } | gigabitEthernet { *port* | *port-list* } | ten-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 10	**show power inline information interface [fastEthernet { *port* | *port-list* } | gigabitEthernet { *port* | *port-list* } | ten-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 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 set the system power limit as 160W. Set the priority as middle and set the power limit as class3 for 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-if)#end

Switch#copy running-config startup-config

6.2.2 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 inline consumption** *power-limit* Specify 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	**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 4	**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.

Step 5	**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 6	**time-range** *name* Specify a time range for the port. Then the port will supply power only during the time range. For how to create a time range, refer to *Time Range Configuration*. *name:* Specify the name of the time range.
Step 7	**show power profile** Verify the defined PoE profile.
Step 8	**show power inline configuration interface [fastEthernet {** *port* **|** *port-list* **} | gigabitEthernet {** *port* **|** *port-list* **} | ten-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* **} | ten-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 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

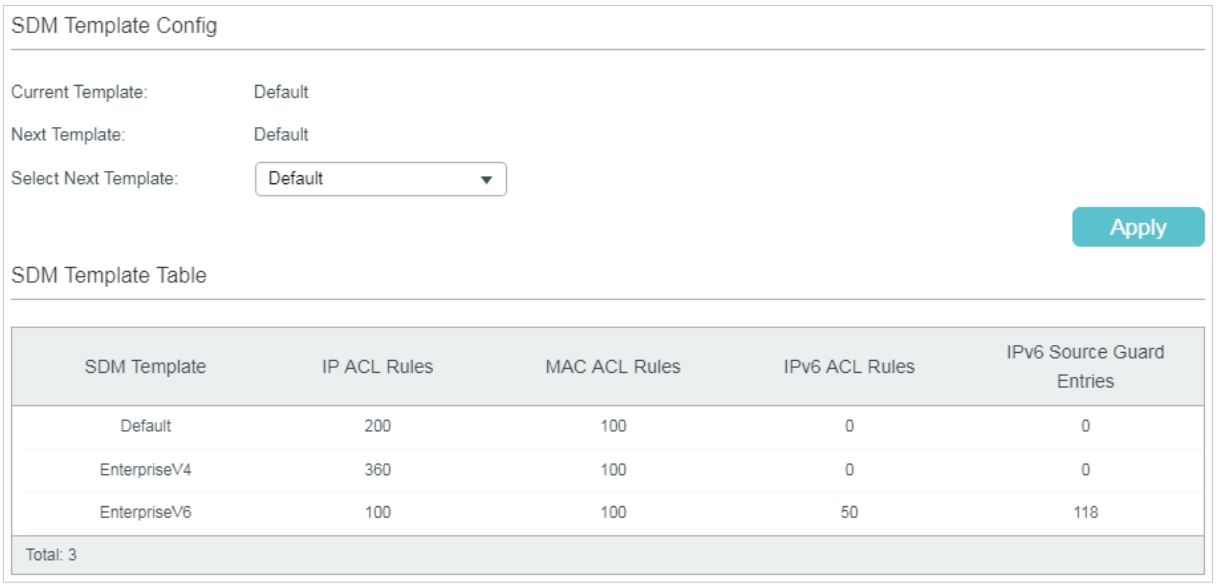
Switch#copy running-config startup-config

7 SDM Template Configuration

7.1 Using the GUI

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

Figure 7-1 Configuring SDM Template



In **SDM Template Config** section, select one template and click **Apply**. The setting will be effective after the switch is rebooted.

Current Template	Displays the template currently in effect.
Next Template	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 Layer 3 ACL Rules and Layer 4 ACL Rules.

MAC ACL Rules	Displays the number of Layer 2 ACL Rules.
IPv6 ACL Rules	Displays the number of IPv6 ACL rules.
IPv6 Source Guard Entries	Displays the number of IPv6 source guard entries.

7.2 Using the CLI

Follow these steps to configure the SDM template:

Step 1	**configure** Enter global configuration mode.
Step 2	**show sdm prefer {** used | default | enterpriseV4 | enterpriseV6 **}** View the template table. It will help you determine which template is suitable for your network. 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 switch is rebooted. 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 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 : 100

number of IPV6 ACL Rules : 0

number of IPV6 Source Guard Entries : 0

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

8 Time Range Configuration

To complete Time Range configuration, follow these steps:

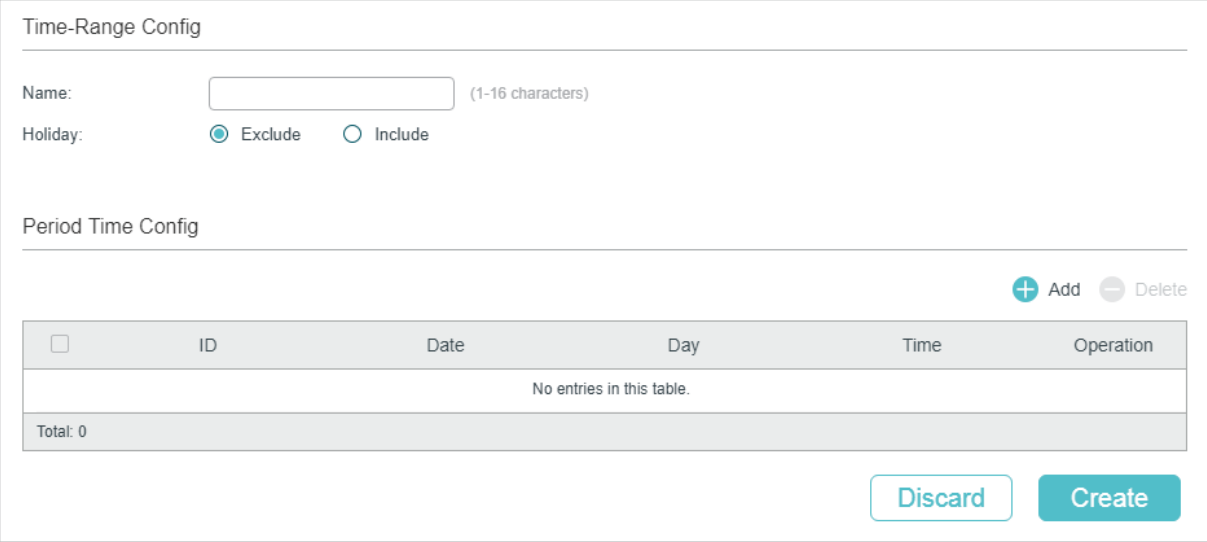
1) Add time range entries.
2) Configure Holiday time range.

8.1 Using the GUI

8.1.1 Adding Time Range Entries

Choose the menu **SYSTEM** > **Time Range > Time Range Config** and click Add to load the following page.

Figure 8-1 Configuring Time Range



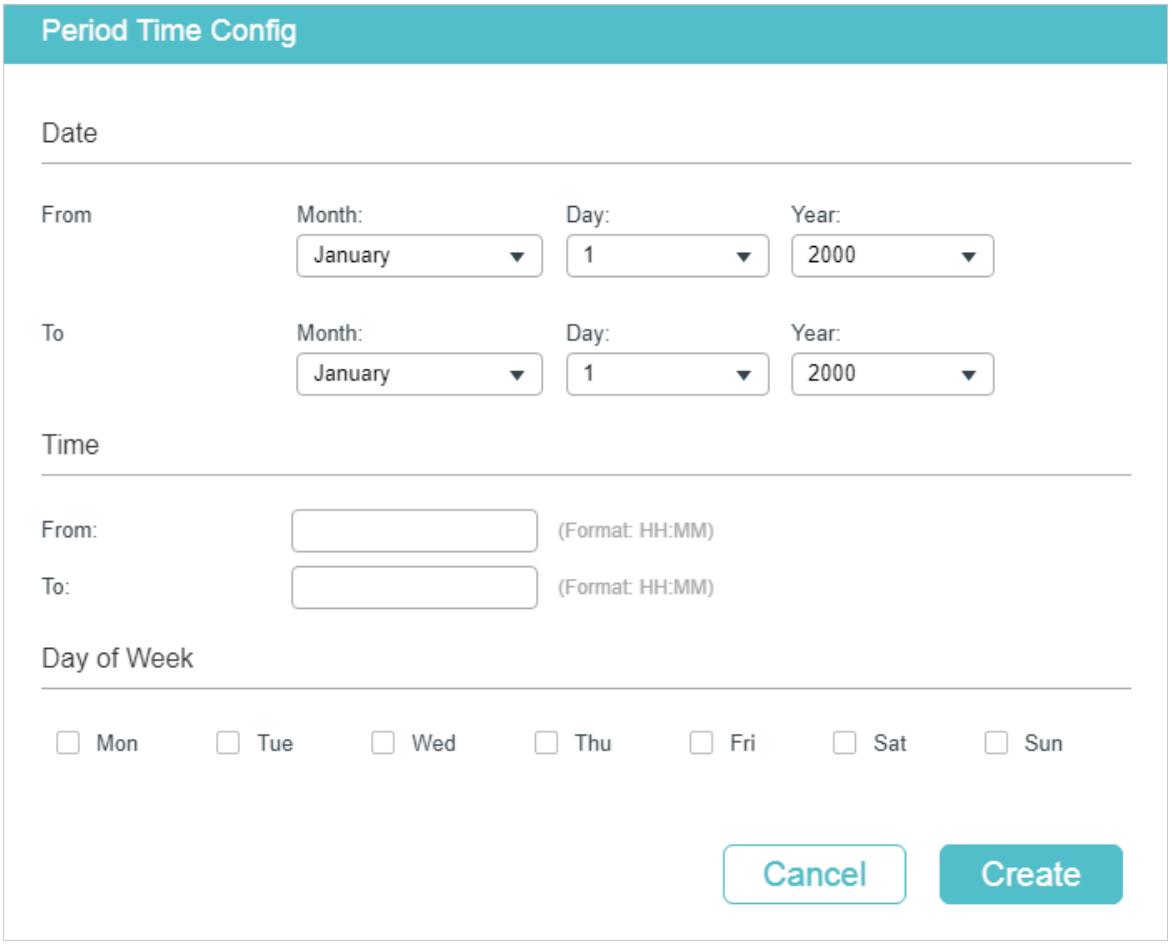
Follow these steps to add time range entries:

1) In the **Time-Range Config** section, specify a name for the entry and select the Holiday mode.

Name	Specify a name for the entry.
Holiday	Select to include or exclude the holiday in the time range. **Exclude:** The time range will not take effect on holiday. **Include:** The time range will not be affected by holiday. To configure Holiday, refer to *Configuring Holiday*.

2) In the **Period Time Config** section, click Add and the following window will pop up.

Figure 8-2 Adding Period Time

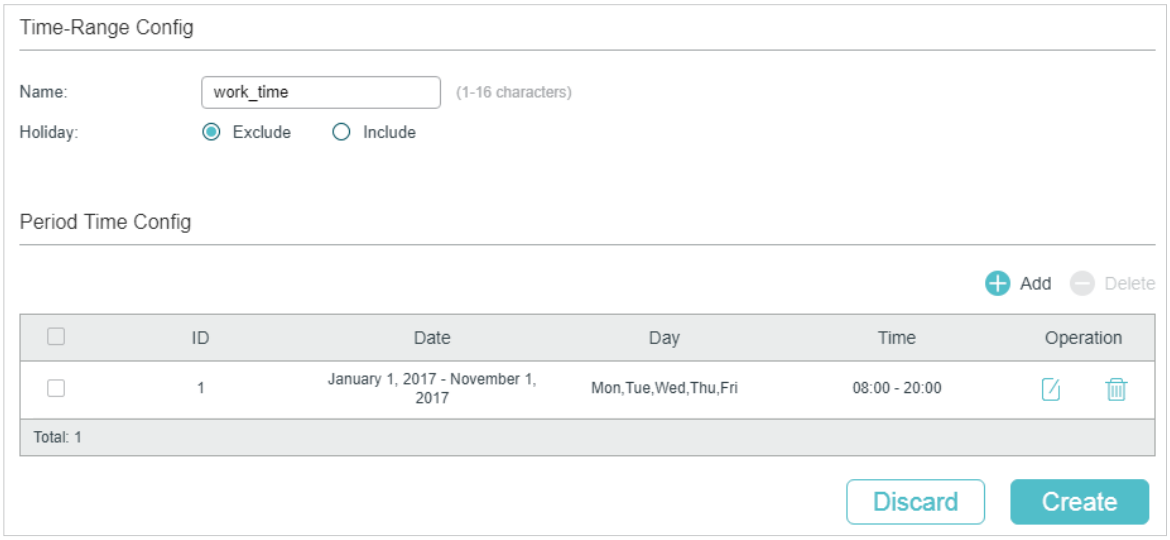


Configure the following parameters and click **Create**:

Date	Specify the start date and end date of this time range.
Time	Specify the start time and end time of a day.
Day of Week	Select days of a week as the period of this time range.

3) Similarly, you can add more entries of period time according to your needs. The final period time is the sum of all the periods in the table. Click **Create**.

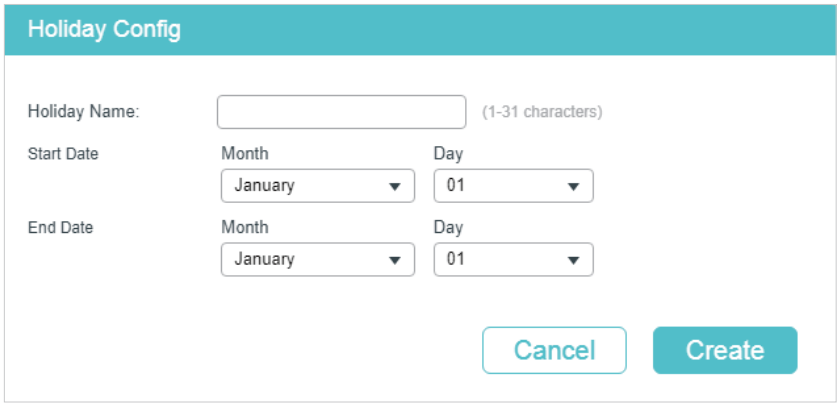
Figure 8-3 View Configruation Result



8.1.2 Configuring Holiday

Choose the menu **SYSTEM** > **Time Range** > **Holiday Config** and click Add to load the following page.

Figure 8-1 Configuring Holiday



Configure the following parameters and click **Create** to add a Holiday entry.

Holiday Name	Specify a name for the entry.
Start Date	Specify the start date of the Holiday time range.
End Date	Specify the end date of the Holiday time range.

Similarly, you can add more Holiday entries. The final Holiday time range is the sum of all the entries.

8.2 Using the CLI

8.2.1 Adding Time Range Entries

Follow these steps to add time range entries:

Step 1	**configure** Enter global configuration mode.
Step 2	**time-range** *name* Create a time-range entry. *name*: Specify a name for the entry.
Step 3	**holiday {** exclude | include **}** Include or exclude the holiday in the time range. exclude: The time range will not take effect on holiday. include: The time range will not be affected by holiday. To configure Holiday, refer to *Configuring Holiday*.
Step 4	**absolute from** *start-date* **to** *end-date* Specify the start date and end date of this time range. *start-date*: Specify the start date in the format MM/DD/YYYY. *end-date*: Specify the end date in the format MM/DD/YYYY.
Step 5	**periodic { [start** *start-time* **] [end** *end-time* **] [day-of-the-week** *week-day* **] }** Specify days of a week as the period of this time range. *start-time*: Specify the start end time of a day in the format HH:MM. *end-time*: Specify the end time and end time of a day in the format HH:MM. *week-day*: Specify the days of week in the format of 1-3, 7. The numbers 1-7 respectively represent Monday, Tuesday, Wednesday, Thursday, Friday, Saturday and Sunday.
Step 6	**show time-range** View the configuration of Time Range.
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 create a time range entry and set the name as time1, holiday mode as exclude, absolute time as 10/01/2017 to 10/31/2017 and periodic time as 8:00 to 20:00 on every Monday and Tuesday:

Switch#config

Switch(config)#time-range time1

Switch(config-time-range)#holiday exclude

Switch(config-time-range)#absolute from 10/01/2017 **to** 10/31/2017

Switch(config-time-range)#periodic start 08:00 **end** 20:00 **day-of-the-week** 1,2

Switch(config-time-range)#show time-range

Time-range entry: 12 (Inactive)

Time-range entry: time1 (Inactive)

holiday: exclude

number of time slice: 1

01 - 10/01/2017 to 10/31/2017

- 08:00 to 20:00 on 1,2

Switch(config-time-range)#end

Switch#copy running-config startup-config

8.2.2 Configuring Holiday

Follow these steps to configure Holiday time range:

Step 1	**configure** Enter global configuration mode.
Step 2	**holiday** *name* **start-date** *start-date* **end-date** *end-date* Create a holiday entry. *name*: Specify a name for the entry. *start-date* : Specify the start date in the format MM/DD. *end-date*: Specify the end date in the format MM/DD.
Step 3	**show holiday** View the configuration of Holiday.
Step 4	**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 create a holiday entry and set the entry name as holiday1 and set start date and end date as 07/01 and 09/01:

Switch#config

Switch(config)#holiday holiday1 **start-date** 07/01 **end-date** 09/01

Switch(config)#show holiday

Index Holiday Name Start-End

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

1 holiday1 07.01-09.01

Switch(config)#end

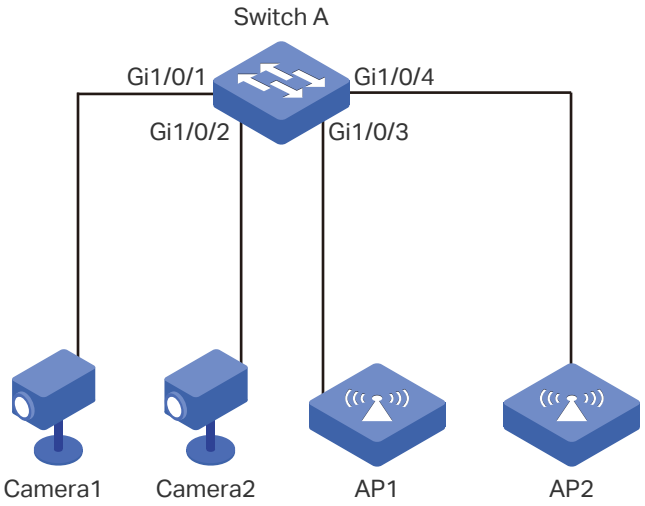
Switch#copy running-config startup-config

9 Example for PoE Configurations

9.1 Network Requirements

The network topology of a company is shown as below. Camera1 and Camera2 work for the security of the company and cannot be power off all the time. AP1 and AP2 provide the internet service and only work in the office time.

Figure 9-1 Network Topology



9.2 Configuring Scheme

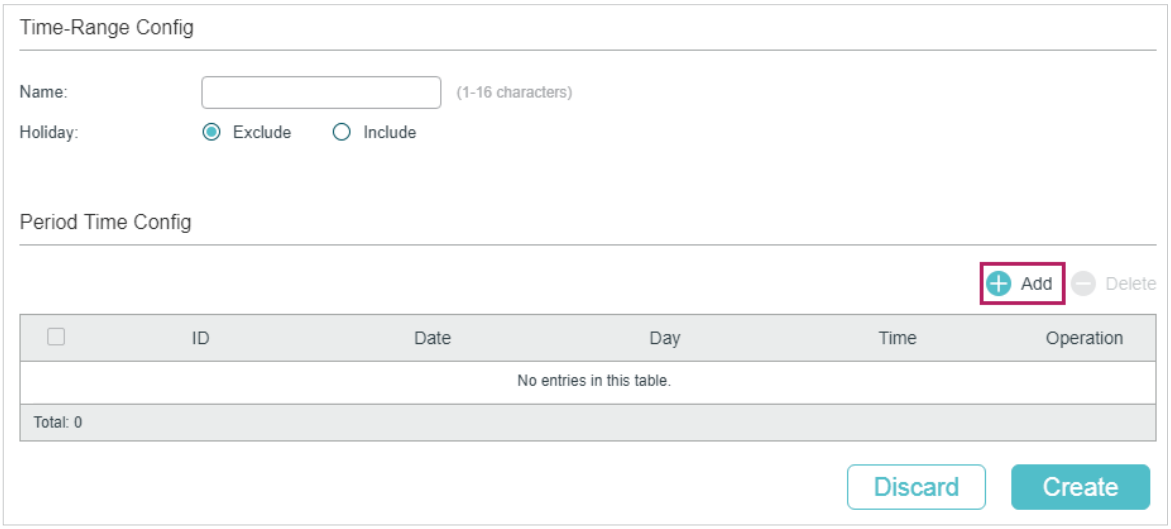
To implement this requirement, you can set a PoE time-range as the office time, for example, from 08:30 to 18:00 on work days. Then apply the settings to port 1/0/3 and 1/0/4. Port 1/0/1 and port1/0/2 need to supply power all the time, so the time range configurations can be left as the default settings here.

9.3 Using the GUI

The configurations of port 1/0/4 is similar with the configurations of port 1/0/3. Here we take port 1/0/3 for example.

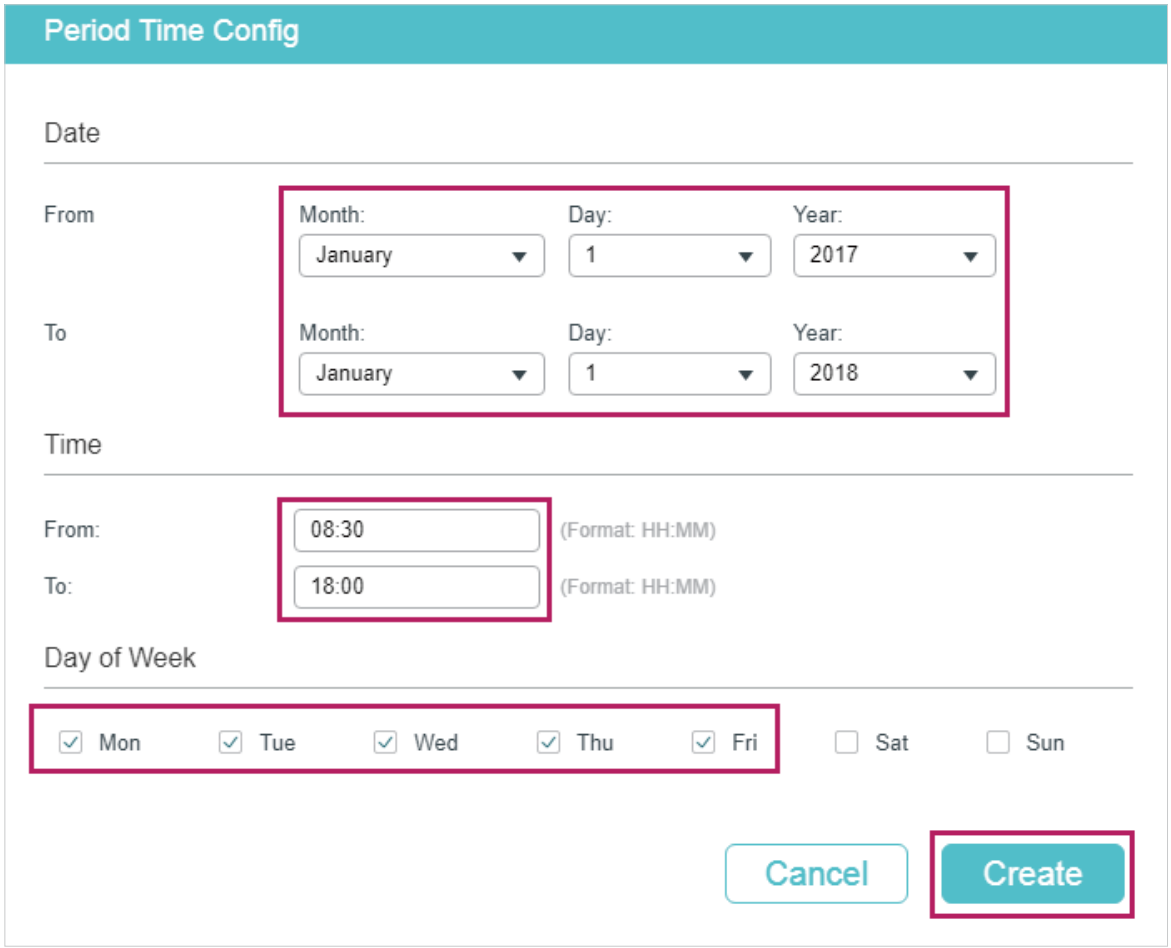
1) Choose the menu **SYSTEM** > **Time Range** > **Time Range Create** and click Add to load the following page.

Figure 9-2 Creating Time Range



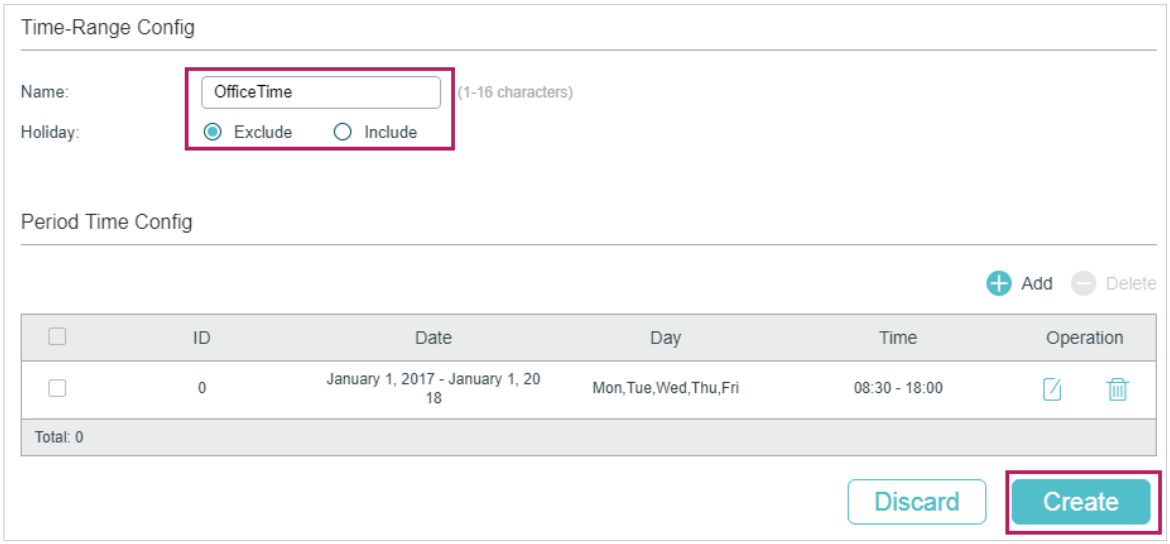
2) Click Add and the following window will pop up. Set **Date, Time** and **Day** of Week as the following figure shows. Click **Create**.

Figure 9-3 Creating a Periodic Time



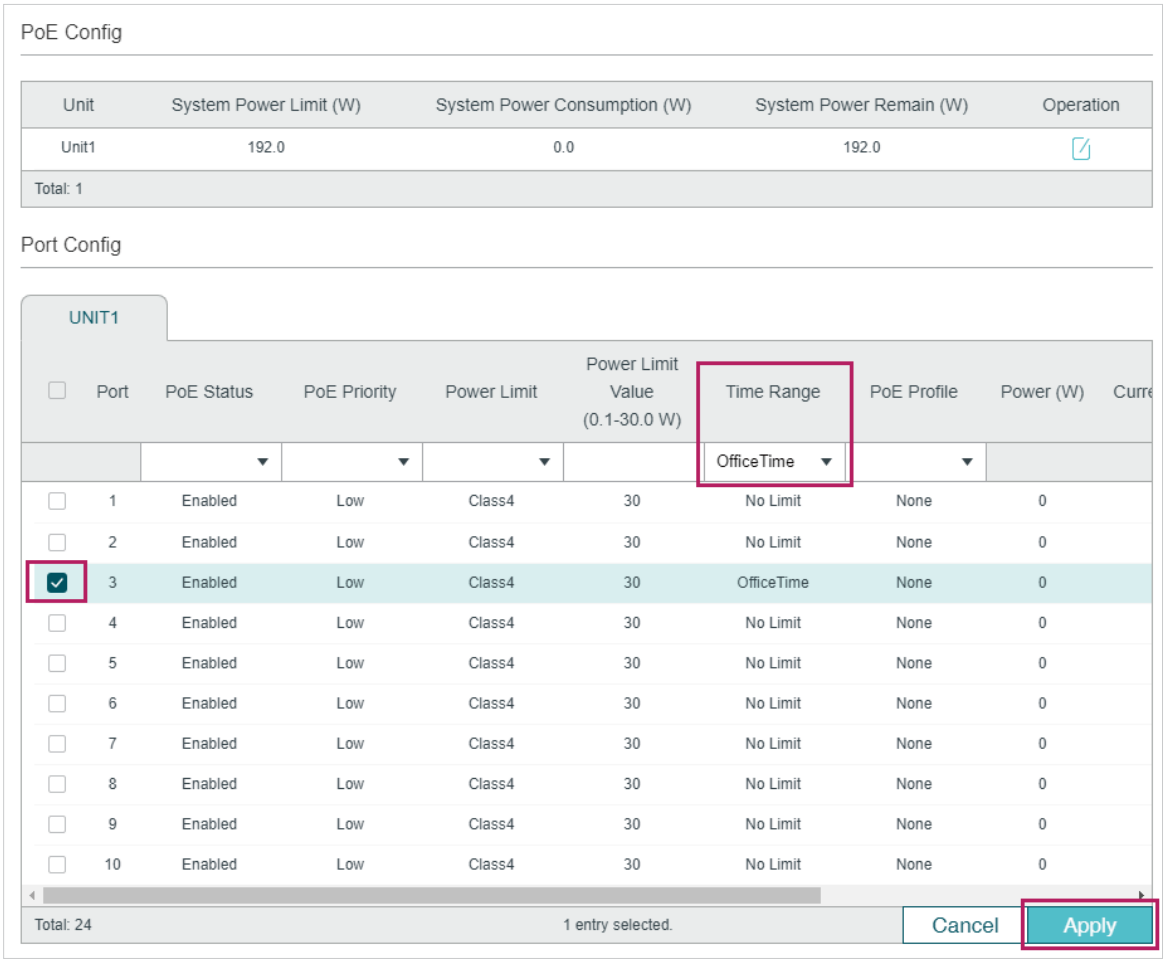
3) Specify a name for the time range and select **Exclude** to make the time-range settings not be affected on holiday. Click **Create**.

Figure 9-4 Configuring Time Range



4) Choose the menu **SYSTEM** > **PoE** > **PoE Config** to load the following page. Select port 1/0/3 and set the **Time Range** as OfficeTime. Click **Apply**.

Figure 9-5 Configure the Port



5) Click Save to save the settings.

9.4 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)#time-range office-time

   Switch_A(config-time-range)#holiday exclude

   Switch_A(config-time-range)#absolute from 01/01/2017 to 01/01/2018

   Switch_A(config-time-range)#periodic start 08:30 end 18:00 day-of-the-week 1-5

   Switch_A(config-time-range)#exit

2) 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)#end

   Switch_A#copy running-config startup-config

Verify the Configuration

Verify the configuration of the time-range:

Switch_A#show power time-range

Time-range entry: office-time (Active)

holiday: exclude

number of time slice: 1

01 - 01/01/2017 to 01/01/2018

- 08:00 to 18:00 on 1,2,3,4,5

Verify the configuration of the PoE basic parameters:

Switch_A#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

10 Appendix: Default Parameters

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

Table 10-1 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 10-2 Default Settings of System Time Configuration

Parameter	Default Setting
Time Source	Manual

Table 10-3 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 10-4 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 10-5 Default Settings of Boot Configuration

Parameter	Default Setting
Current Startup Image	image1.bin
Next Startup Image	image1.bin
Backup Image	image2.bin
Current Startup Config	config1.cfg
Next Startup Config	config1.cfg

Parameter	Default Setting
Backup Config	config2.cfg

Default setting of EEE is listed in the following table.

Table 10-6 Default Settings of EEE Configuration

Parameter	Default Setting
Status	Disabled

Default settings of PoE is listed in the following table.

Table 10-7 Default Settings of PoE Configuration

Parameter	Default Setting
PoE Config	
System Power Limit	384.0W
Port Config	
PoE Status	Enable
PoE Priority	Low
Power Limit (0.1w-30.0w)	Class 4
Time Range	No Limit
PoE Profile	None
Profile Config	
Profile Name	None
PoE Status	Enable
PoE Priority	Low
Power Limit	Auto

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

Table 10-8 Default Settings of SDM Template Configuration

Parameter	Default Setting
Current Template ID	Default
Next Template ID	Default

Default settings of Time Range are listed in the following table.

Table 10-9 Default Settings of Time Range Configuration

Parameter	Default Setting
Holiday	Exclude

Part 3

Managing Physical Interfaces

CHAPTERS

1. Physical Interface
2. Basic Parameters Configurations
3. Port Isolation Configurations
4. Loopback Detection Configuration
5. Configuration Examples
6. Appendix: Default Parameters

1 Physical Interface

1.1 Overview

Interfaces are used to exchange data and interact with interfaces of other network devices. Interfaces are classified into physical interfaces and layer 3 interfaces.

- Physical interfaces are the ports on the switch panel. They forward packets based on MAC address table.
- Layer 3 interfaces are used to forward IPv4 and IPv6 packets using static or dynamic routing protocols. You can use Layer 3 interfaces for IP routing and inter-VLAN routing.

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 Isolation

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

Loopback Detection

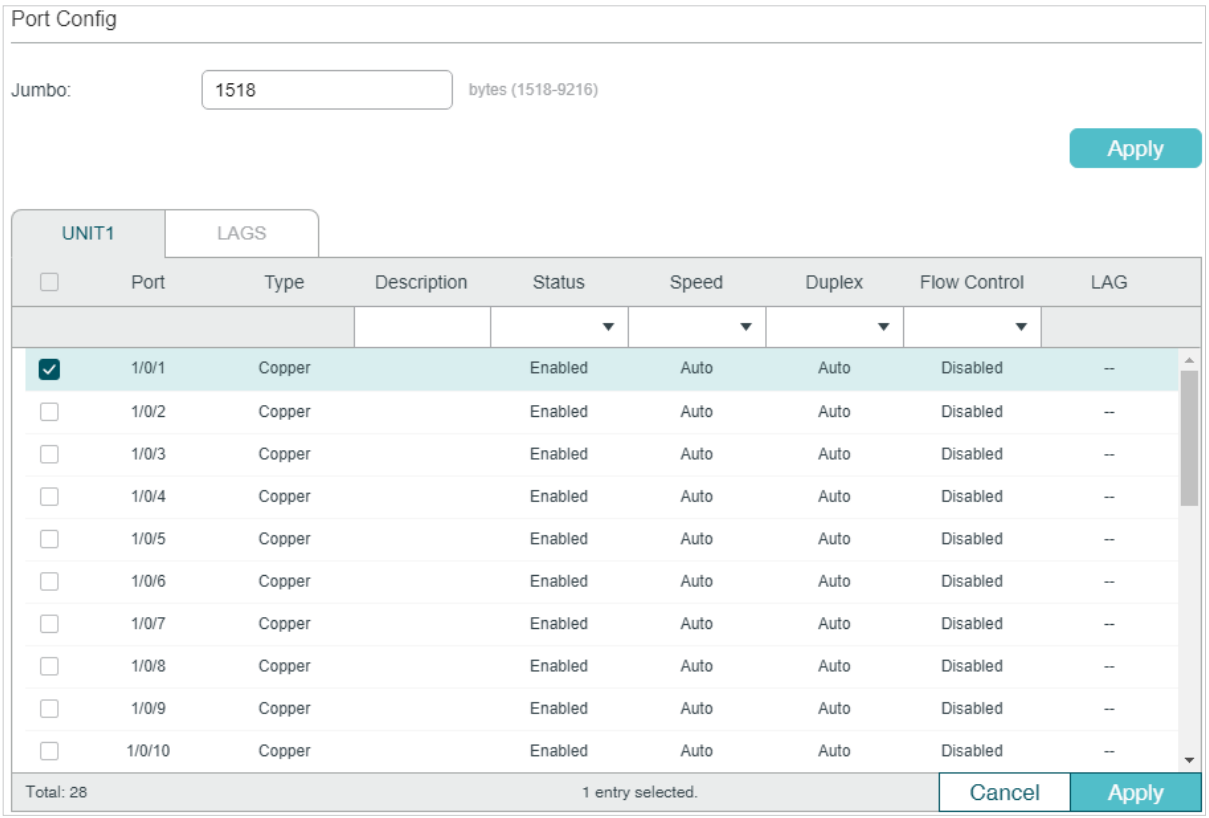
This function allows the switch to detect loops in the network. When a loop is detected on a port or VLAN, the switch will display an alert on the management interface and block the corresponding port or VLAN according to your configurations.

2 Basic Parameters Configurations

2.1 Using the GUI

Choose the menu **L2 FEATURES > Switching > Port > Port Config** to load the following page.

Figure 2-1 Configuring Basic Parameters



Follow these steps to configure basic parameters for the ports:

1) Configure the MTU size of jumbo frames for all the ports, then click **Apply**.

Jumbo	Configure the size of jumbo frames. By default, it is 1518 bytes. Generally, the MTU (Maximum Transmission Unit) size of a normal frame is 1518 bytes. If you want the switch supports to transmit frames of which the MTU size is greater than 1518 bytes, you can configure the MTU size manually here.

2) Select one or more ports to configure the basic parameters. Then click **Apply**.

UNIT/LAGS	Click the **UNIT** number to configure physical ports. Click **LAGS** to configure LAGs.
Type	Displays the port type. **Copper** indicates an Ethernet port, and **Fiber** indicates an SFP port.

Description	(Optional) Enter a description for the port.
Status	With this option enabled, the port forwards packets normally. Otherwise, the port cannot work. By default, it is enabled.
Speed	Select the appropriate speed mode for the port. When **Auto** is selected, the port automatically negotiates speed mode with the neighbor device. The default setting is **Auto**. It is recommended to select **Auto** if both ends of the link support auto-negotiation.
Duplex	Select the appropriate duplex mode for the port. There are three options: **Half**, **Full** and **Auto**. The default setting is **Auto**. **Half**: The port can send and receive packets, but only one-way at a time. **Full**: The port can send and receive packets simultaneously. **Auto**: The port automatically negotiates duplex mode with the peer device.
Flow Control	With this option enabled, when a device gets overloaded it will send a PAUSE frame to notify the peer device to stop sending data for a specified period of time, thus avoiding the packet loss caused by congestion. 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	**jumbo-size** *size* Change the MTU (Maximum Transmission Unit) size to support jumbo frames. The default MTU size for frames received and sent on all ports is 1518 bytes. To transmit jumbo frames, you can manually configure MTU size of frames up to 9216 bytes. *size*: Configure the MTU size of jumbo frames. The value ranges from 1518 to 9216bytes.
Step 3	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| ten-range gigabitEthernet** *port-list* **| port-channel** *port-channel* **| range port-channel** *port-channel-list* **|}** Enter interface configuration mode.

Step 4	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 | 10000 | auto **}** Set the appropriate speed mode for the port. 10 | 100 | 1000 | 10000 | 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, it is disabled.
Step 5	**show interface configuration [fastEthernet** *port* **| gigabitEthernet** *port* **| | ten-gigabitEthernet** *port* **| port-channel** *port-channel-id* **]** Verify the configuration of the port or LAG.
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 implement the basic configurations of port1/0/1, including setting a description for the port, configuring the jumbo frame, making the port automatically negotiate speed and duplex with the neighboring port, and enabling the flow-control:

Switch#configure

Switch#jumbo-size 9216

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)#show interface configuration gigabitEthernet 1/0/1

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

Switch(config-if)#show jumbo-size

Global jumbo size : 9216

Switch(config-if)#end

Switch#copy running-config startup-config

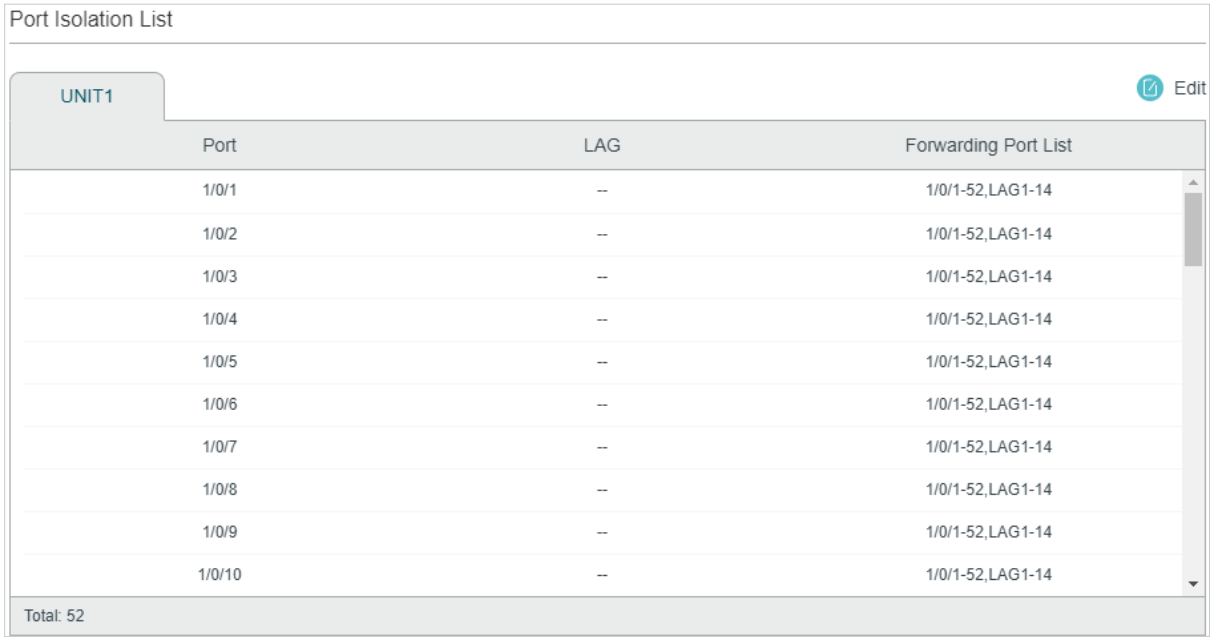
3 Port Isolation Configurations

3.1 Using the GUI

Port Isolation is used to limit the data transmitted by a port. The isolated port can only send packets to the ports specified in its Forwarding Port List.

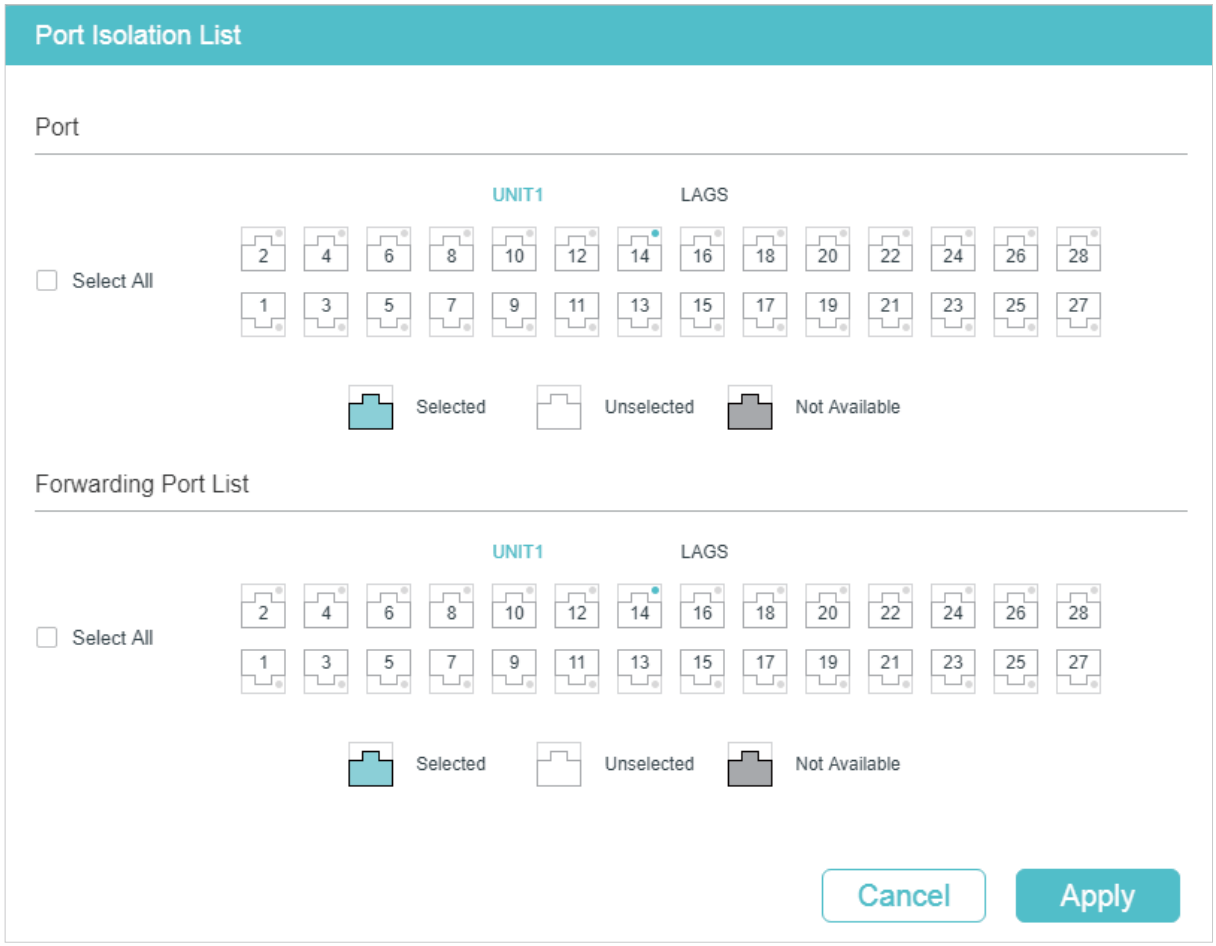
Choose the menu **L2 FEATURES > Switching > Port > Port Isolation** to load the following page.

Figure 3-1 Port Isolation List



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

Figure 3-2 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 **Forwarding Port List** section, select the forwarding ports or LAGs which the isolated ports can only communicate with. It is multi-optional.
3) Click **Apply**.

3.2 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* **| ten-gigabitEthernet** *port* **| ten-range gigabitEthernet** *port-list* **| port-channel** *port-channel* **| range port-channel** *port-channel-list* **|}** Specify the port to be isolated and enter interface configuration mode.

Step 3	**port isolation { [fa-forward-list** *fa-forward-list*] **[gi-forward-list** *gi-forward-list*] **[te-forward-list** *te-forward-list*] **[po-forward-list** *po-forward-list* **] }** Add ports or LAGs to the forwarding port list of the isolated port. It is multi-optional. *fa-forward-list / gi-forward-list / te-forward-list*: Specify the forwarding Ethernet ports. *po-forward-list:* Specify the forwarding LAGs.
Step 4	**show port isolation interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel* **}** 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 forwarding 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

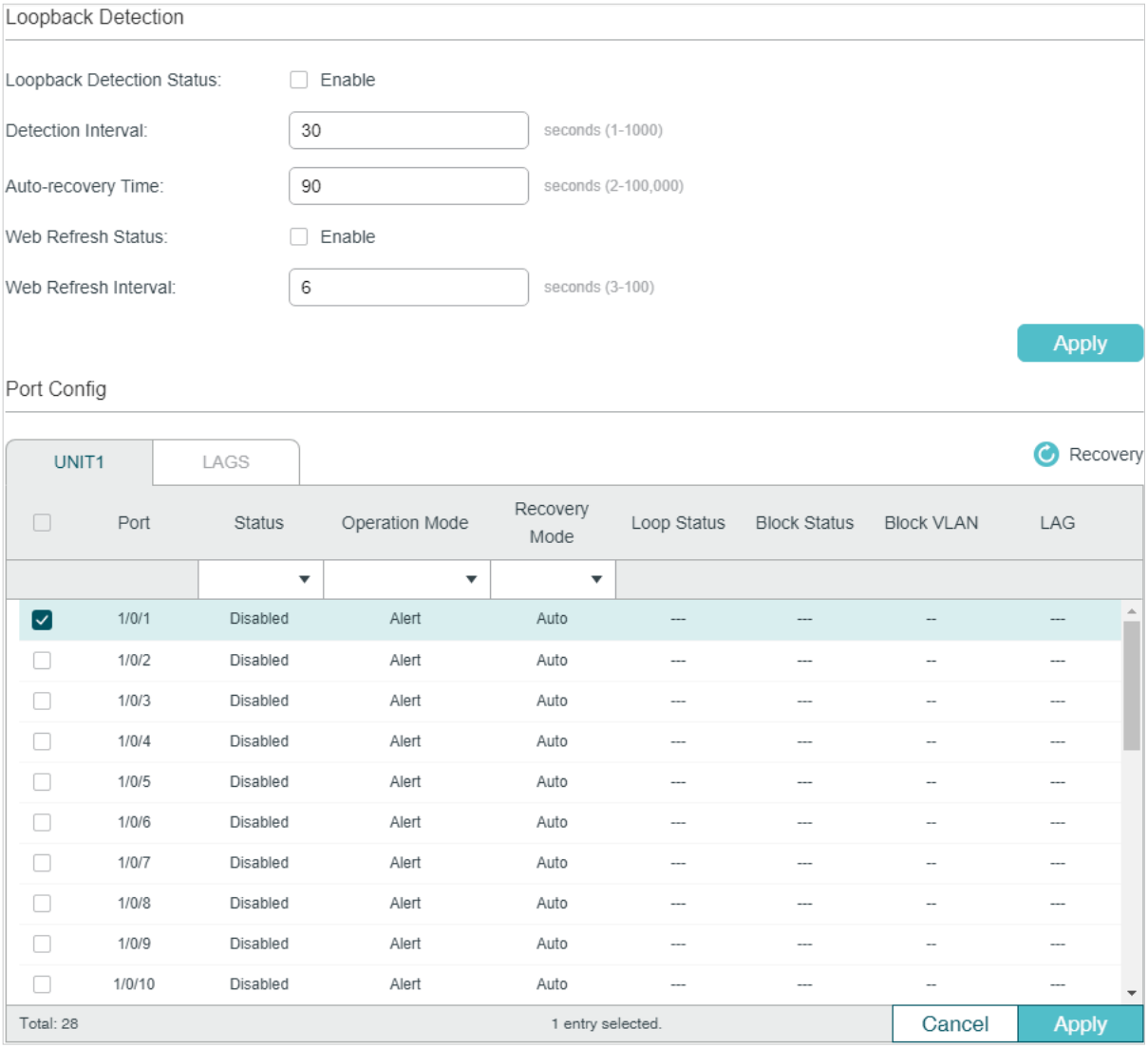
4 Loopback Detection Configuration

4.1 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 **L2 FEATURES > Switching > Port > Loopback Detection** to load the following page.

Figure 4-1 Configuring Loopback Detection



Follow these steps to configure loopback detection:

1) In the **Loopback Detection** 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 in seconds. The valid value ranges from 1 to 1000 and the default value is 30.
Auto-recovery Time	Set the recovery time globally. The blocked port in Auto Recovery mode will automatically be recovered to normal status after the Auto-recovery Time expires. The value ranges from 2 to 100,000 in seconds, and the default value is 90.
Web Refresh Status	With this option enabled, the switch will refresh the web timely. By default, it is disabled.
Web Refresh Interval	If you enabled web refresh status, set the refresh interval in seconds between 3 and 100. The default value is 6.

2) In the **Port Config** section, select one or more ports to configure the loopback detection parameters. Then click **Apply**.

Status	Enable loopback detection for the port.
Operation Mode	Select the operation mode when a loopback is detected on the port: **Alert**: The Loop Status will display whether there is a loop detected on the corresponding port. It is the default setting. **Port Based**: In addition to displaying alerts, the switch will block the port on which the loop is detected. **VLAN-Based**: If a loop is detected in a VLAN on that port, in addition to displaying alerts, the switch will block that VLAN. The traffic of the other VLANs can still be normally forwarded by 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: **Auto**: The blocked port will automatically be recovered to normal status after the automatic recovery time expires. It is the default setting. **Manual**: You need to manually release the blocked port. Click **Recovery** to release the selected port.

3) (Optional) View the loopback detection information.

Loop Status	Displays whether a loop is detected on the port.
Block Status	Displays whether the port is blocked.
Block VLAN	Displays the blocked VLANs.

4.2 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 auto-recovery time, after which the blocked port in Auto Recovery mode can automatically be recovered to normal status. *recovery-time*: Specify the detection interval, ranging from 2 to 100,000 seconds. The default value is 90.
Step 5	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| ten-range gigabitEthernet** *port-list* **| port-channel** *port-channel* **| range port-channel** *port-channel-list* **|}** Enter interface configuration mode.
Step 6	**loopback-detection** Enable loopback detection for 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: The switch will only display alerts when a loopback is detected. It is the default setting. port-based: In addition to displaying alerts, the switch will block the port on which the loop is detected. vlan-based: In addition to displaying alerts, the switch will block the VLAN of the port in which the loop is detected. Set the recovery mode for the blocked port. There are two modes: auto: After the recovery time expires, the blocked port will automatically recover to normal status and restart to detect loops in the network. manual: The blocked port can only be released manually. You can use the command 'loopback-detection recover' to recover the blocked port 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* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel* **}** 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 (keep the default parameters):

Switch#configure

Switch(config)#loopback-detection

Switch(config)#show loopback-detection global

Loopback detection global status : enable

Loopback detection interval : 30s

Loopback detection recovery time : 3 intervals

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

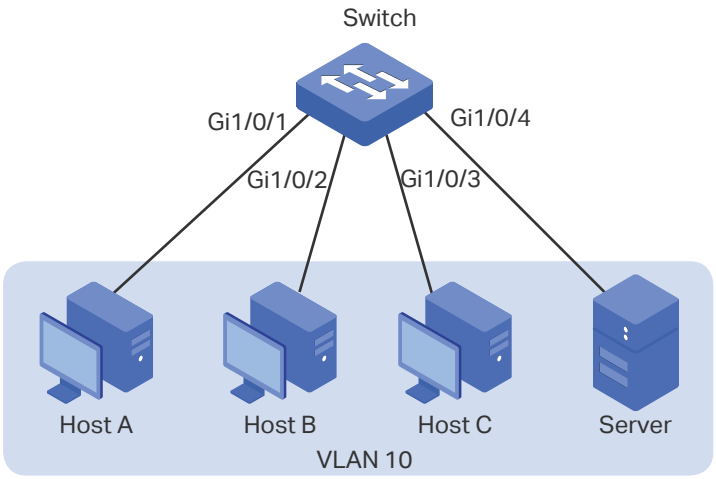
5 Configuration Examples

5.1 Example for Port Isolation

5.1.1 Network Requirements

As shown below, three hosts and a server are connected to the switch and all belong to VLAN 10. Without changing the VLAN configuration, 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 5-1 Network Topology



5.1.2 Configuration Scheme

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

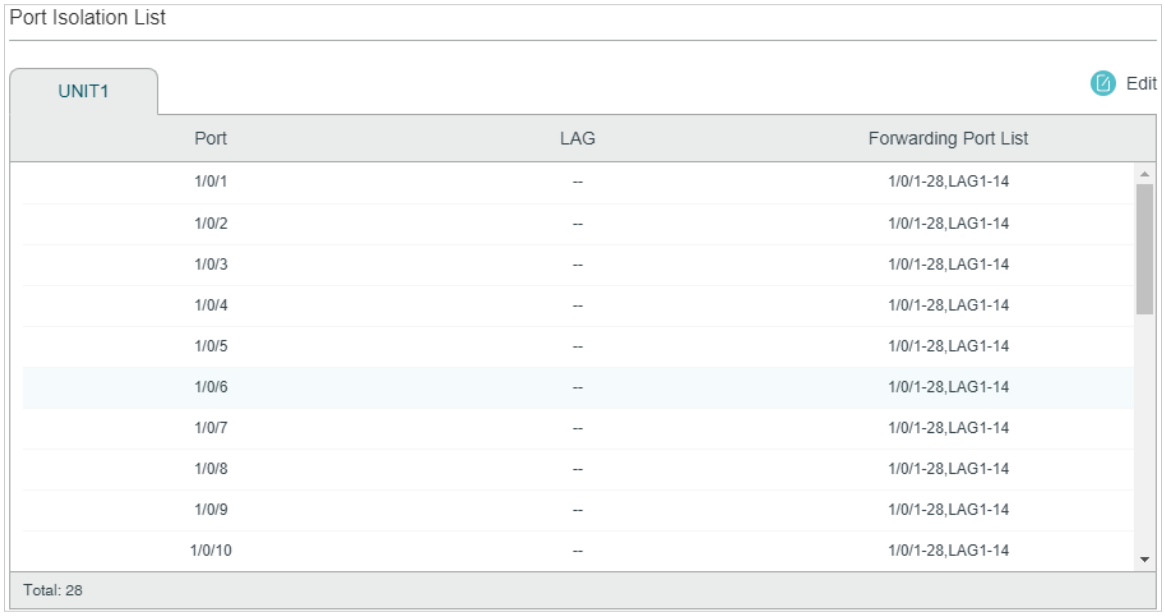
Since communications are bidirectional, if you want Host A and the server to communicate normally, you also need to add port 1/0/1 as the forwarding port for port 1/0/4.

Demonstrated with T1600G-52TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

5.1.3 Using the GUI

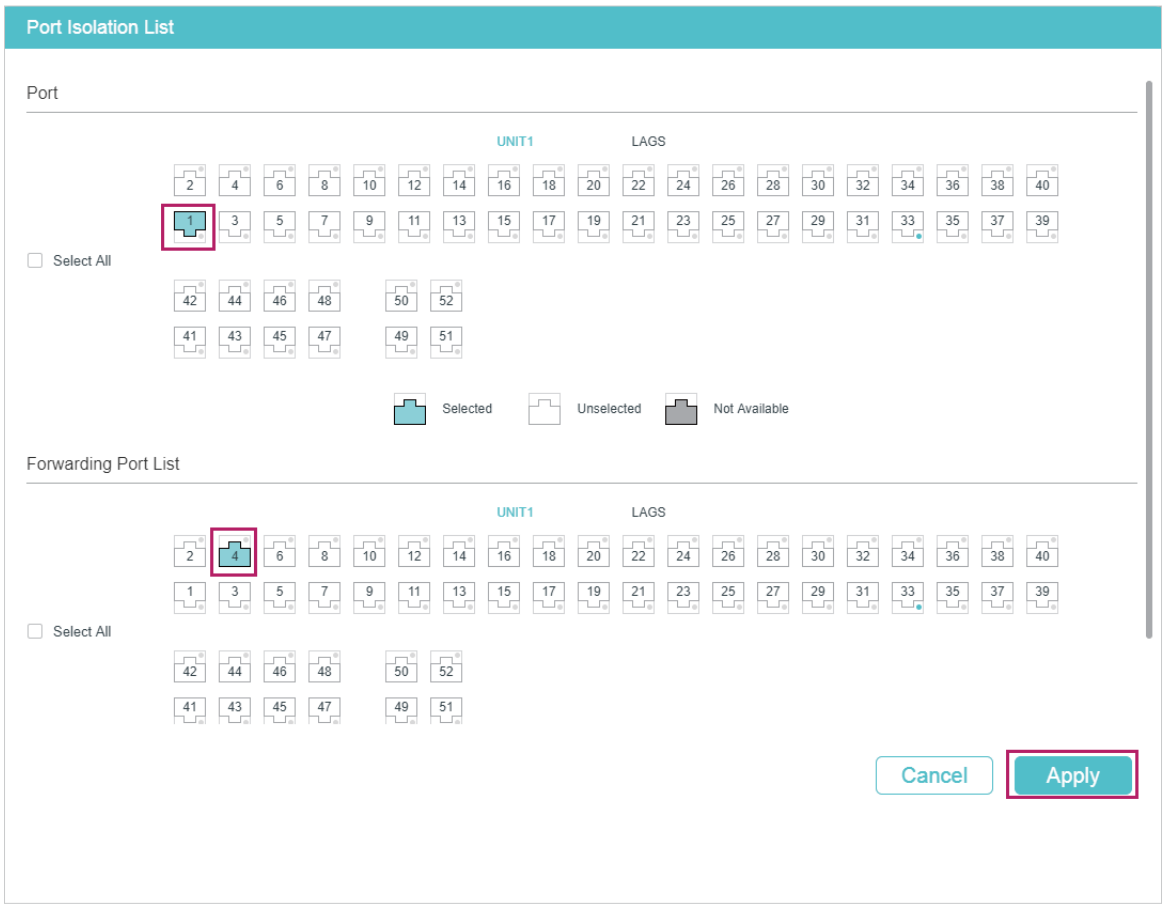
1) Choose the menu **L2 FEATURES > Switching > Port > Port Isolation** to load the following page. It displays the port isolation list.

Figure 5-2 Port Isolation List



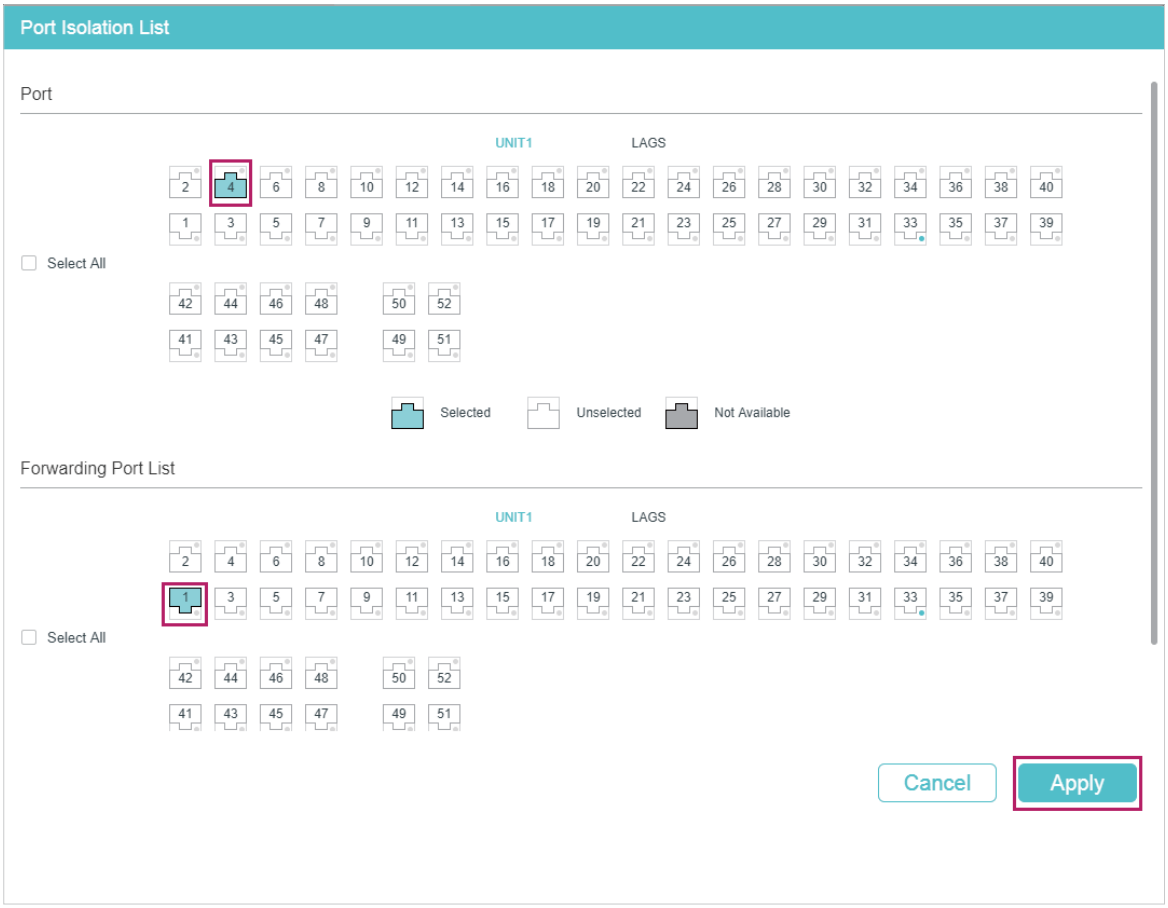
2) Click **Edit** on the above page to load the following page. Select port 1/0/1 as the port to be isolated, and select port 1/0/4 as the forwarding port. Click **Apply**.

Figure 5-3 Port Isolation Configuration



3) Select port 1/0/4 as the port to be isolated, and select port 1/0/1 as the forwarding port. Click **Apply**.

Figure 5-4 Port Isolation Configuration



4) Click Save to save the settings.

5.1.4 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)#exit

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

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

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 Gi1/0/1-28,Po1-14

Gi1/0/3 N/A Gi1/0/1-28,Po1-14

Gi1/0/4 N/A Gi1/0/1

.....

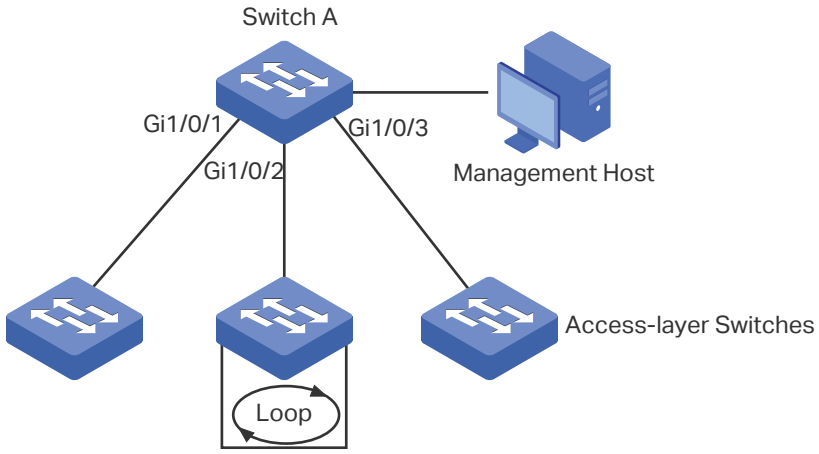
5.2 Example for Loopback Detection

5.2.1 Network Requirements

As shown below, Switch A is a convergence-layer switch connecting to 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 5-5 Network Topology



5.2.2 Configuration Scheme

Enable loopback detection on ports 1/0/1-3 and configure SNMP to receive the trap 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.

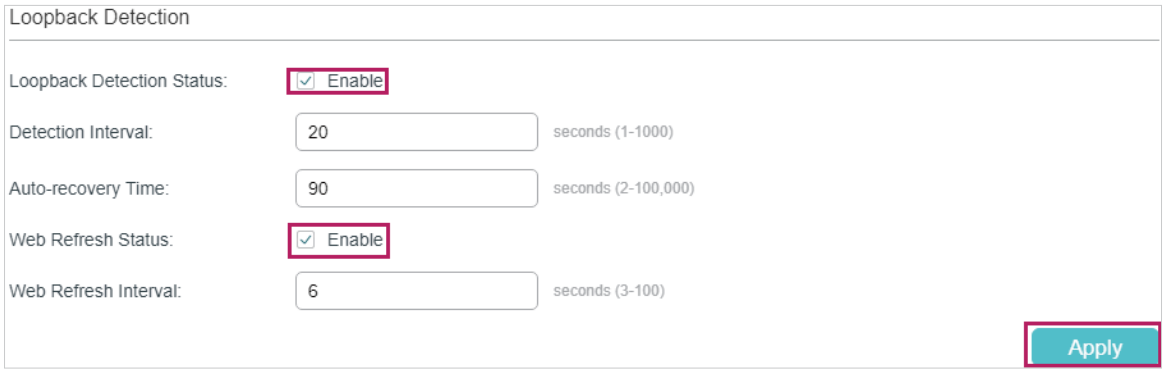
Demonstrated with T1600G-52TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

5.2.3 Using the GUI

1) Choose the menu **L2 FEATURES > Switching > Port > Loopback Detection** to load the configuration page.

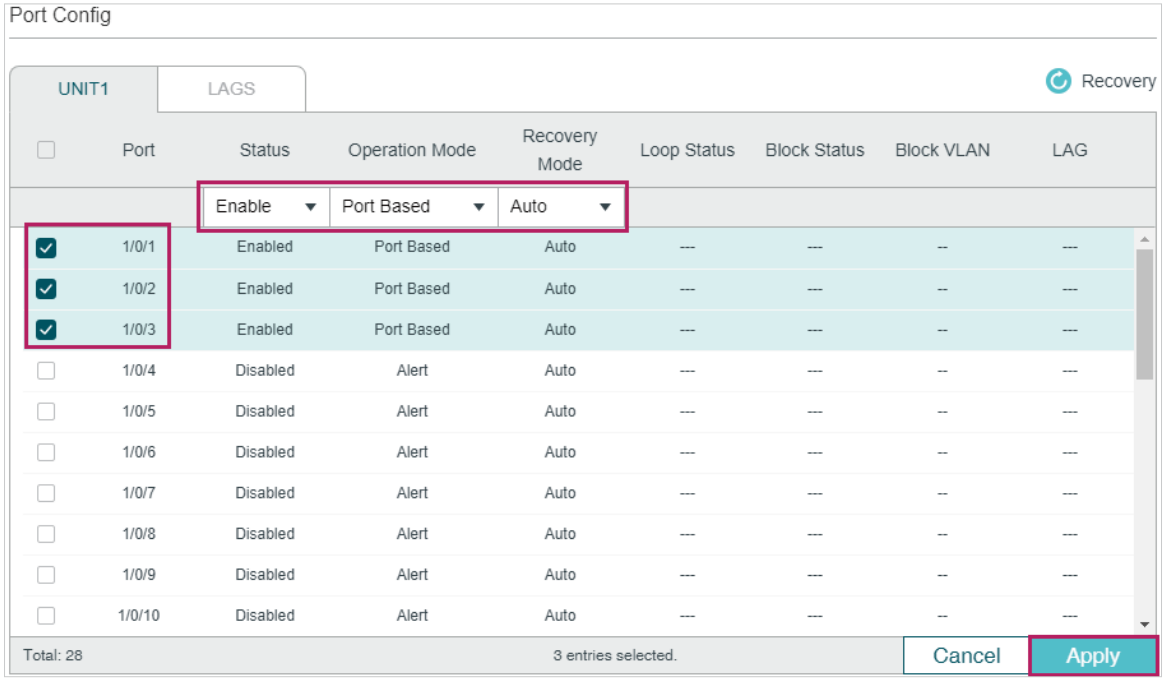
2) In the **Loopback Detection** section, enable loopback detection and web refresh globally. Keep the other parameters as default values and click **Apply**.

Figure 5-6 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 automatically be recovered to normal status after the auto-recovery time. Click **Apply**.

Figure 5-7 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.

5.2.4 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 3

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-range)#loopback-detection

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

   Switch(config-if-range)#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

6 Appendix: Default Parameters

Default settings of Switching are listed in th following tables.

Table 6-1 Configurations for Ports

Parameter	Default Setting
Port Config	
Jumbo	1518 bytes
Type	Copper (For RJ45 Ports) Fiber (For SFP Ports)
Status	Enabled
Speed	Auto (For RJ45 Ports) 1000M (For SFP Ports)
Duplex	Auto (For RJ45 Ports) Full (For SFP Ports)
Flow Control	Disabled
Loopback Detection	
Loopback Detection Status	Disabled
Detection Interval	30 seconds
Auto-recovery Time	90 seconds
Web Refresh Status	Disabled
Web Refresh Interval	6 seconds
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, increasing link bandwidth and providing 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 peer device. 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

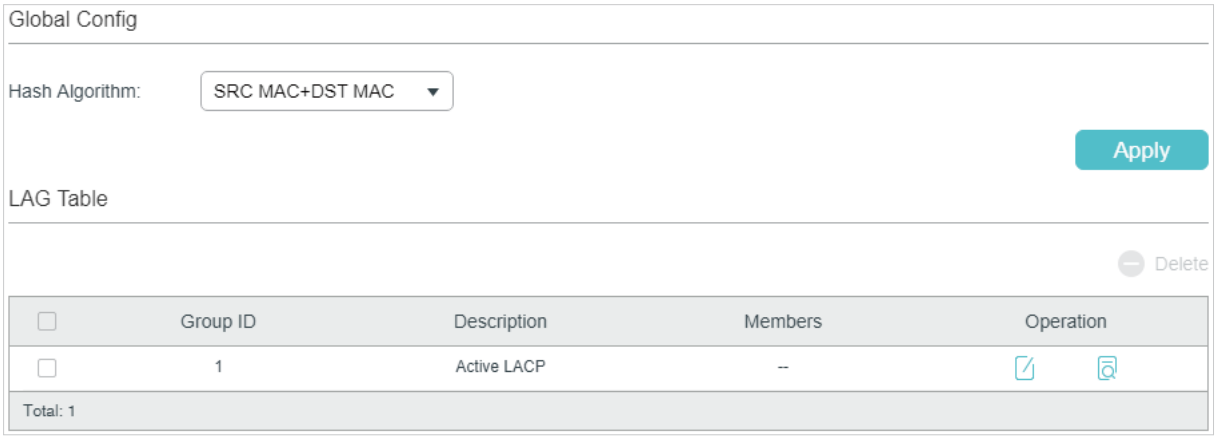
- Ensure that both ends of the aggregation link work in the same LAG mode. For example, if the local end works in LACP mode, the peer end should also be set as LACP mode.
- Ensure that devices on both ends of the aggregation link use the same number of physical ports with the same speed, duplex, jumbo 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 bandwidth evenly. If an active link fails, the other active links share the bandwidth evenly.
- One LACP LAG supports multiple member ports, but at most eight of them can work simultaneously, and the other member ports are backups. Using LACP protocol, the switches negotiate parameters and determine the working ports. When a working port fails, the backup port with the highest priority will replace the faulty port 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 enabled with Port Security, Port Mirror, MAC Address Filtering or 802.1X cannot be added to an 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 **L2 FEATURES > Switching > LAG > LAG Table** to load the following page.

Figure 2-1 Global Config



In the **Global Config** section, select the load-balancing algorithm (Hash Algorithm), then click **Apply**.

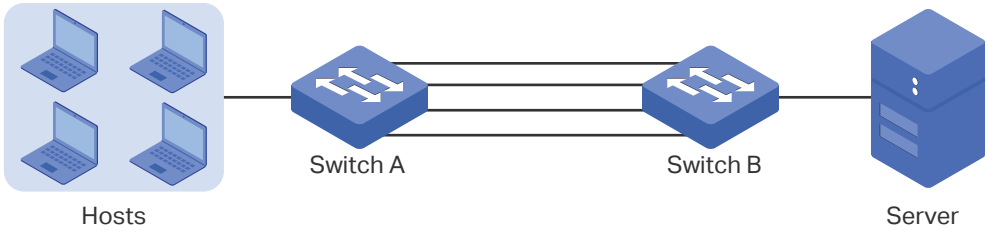
Hash Algorithm	Select the Hash Algorithm, based on which the switch can choose the port to forward the received packets. In this way, different data flows are forwarded on different physical links to implement load balancing. There are six options: **SRC MAC**: The computation is based on the source 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, you can set the algorithm

as "SRC MAC" to allow Switch A to determine the forwarding port based on the source MAC addresses of the received packets.

Figure 2-2 Hash Algorithm Configuration



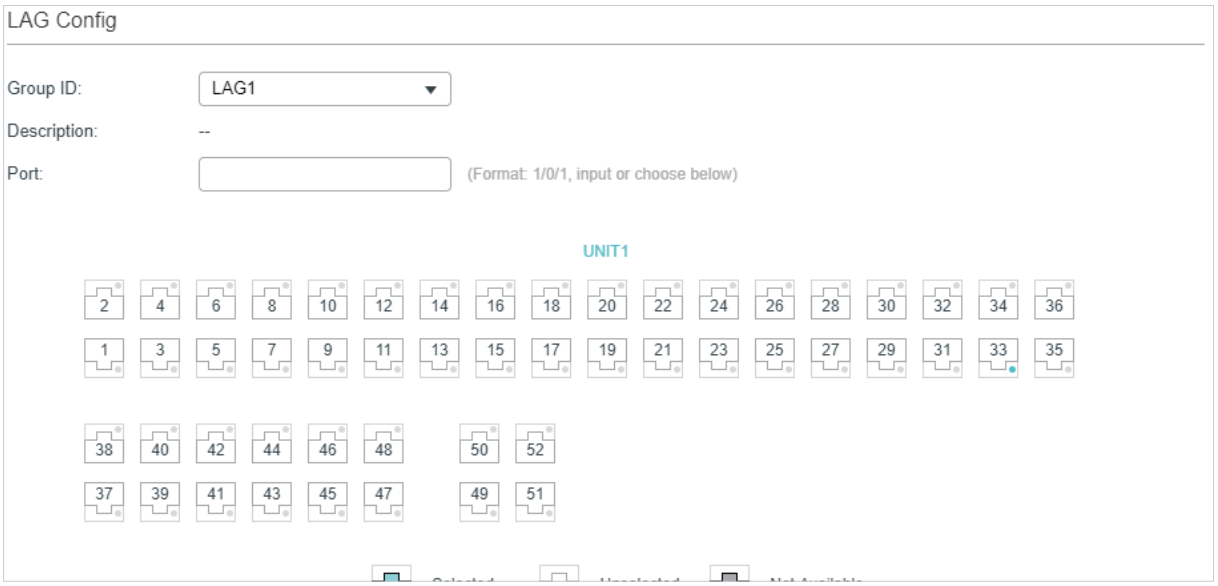
2.1.2 Configuring Static LAG or LACP

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 **L2 FEATURES > Switching > LAG > Static LAG** to load the following page.

Figure 2-3 Static LAG



Follow these steps to configure the static LAG:

1) Select an LAG for configuration.

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

2) Select the member ports for the LAG. It is multi-optional.

3) Click **Apply**.

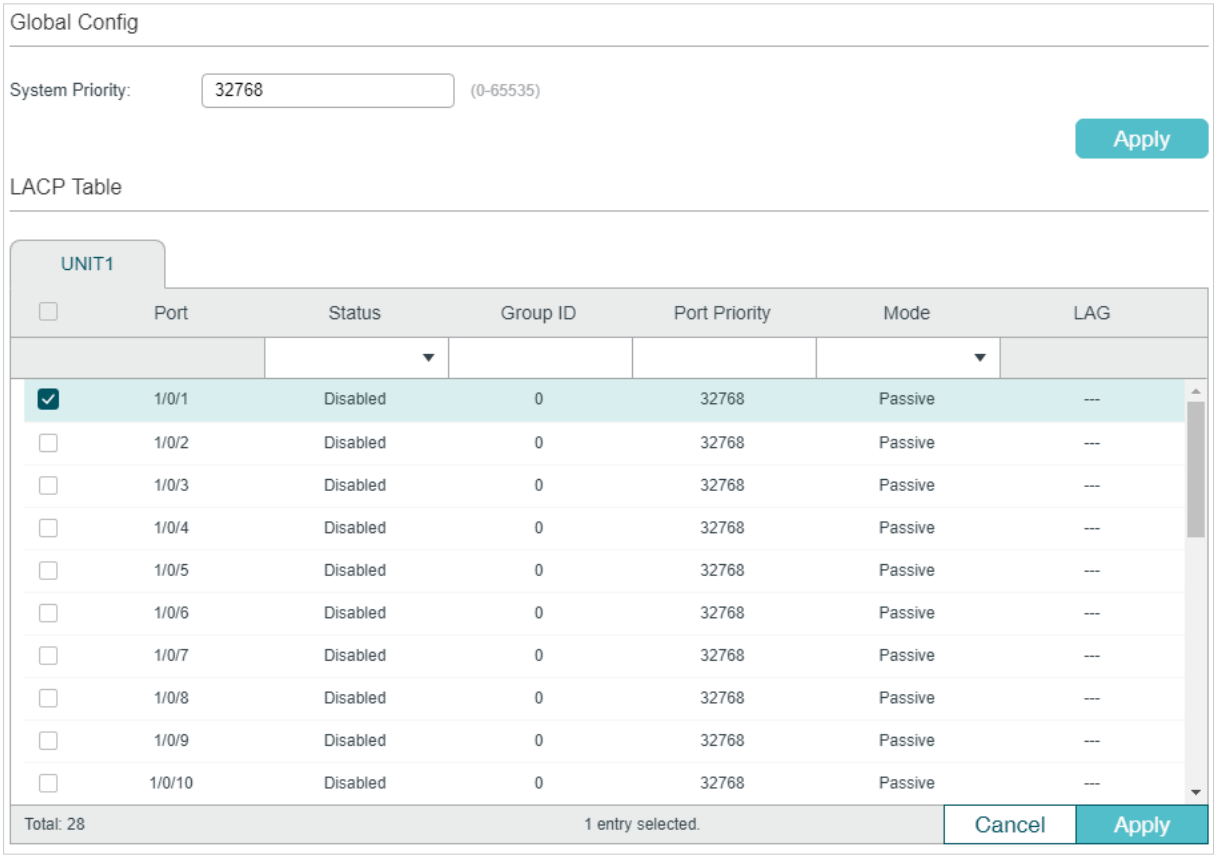
Note:

Clearing all member ports will delete the LAG.

Configuring LACP

Choose the menu **L2 FEATURES > 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 system 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 device with a smaller MAC address has the higher priority.

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

Group ID	Specify the group ID of the LAG. Note that the group ID of other static LAGs cannot be set as this value. The valid value of the Group ID is determined by the maximum number of LAGs supported by your switch. For example, if your switch supports up to 14 LAGs, the valid value ranges 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 working port to forward data, and at most eight ports can work simultaneously. 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* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Enter interface configuration mode.
Step 3	**channel-group** *num* **mode on** Add the port to a static LAG. *num*: The group ID of the LAG.
Step 4	**show etherchannel** *num* **summary** Verify the configuration of the static LAG. *num*: The group 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.

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* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Enter interface configuration mode.
Step 4	**channel-group** *num* **mode {** active | passive **}** Add the port to an LAG and set the mode as LACP. *num*: The group ID 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. 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 working 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

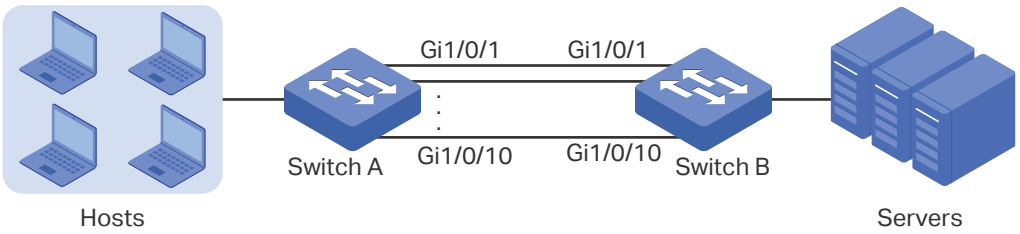
As shown below, hosts and servers are connected to Switch A and Switch B, and heavy traffic is transmitted between the two switches. To achieve high speed and reliability of data transmission, users need to improve the bandwidth and redundancy of the link between the two switches.

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 between 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 lower port priority for ports 1/0/9-10 to set them as the backup ports. When any of ports 1/0/1-8 is down, the backup ports will automatically be enabled to transmit data.

Demonstrated with T1600G-52TS, 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.

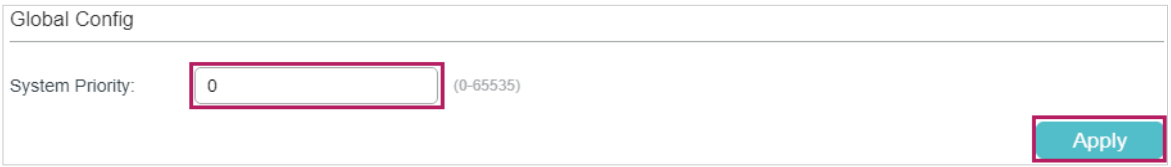
1) Choose the menu **L2 FEATURES > Switching > LAG > LAG Table** to load the following page. Select the hash algorithm as 'SRC MAC+DST MAC'.

Figure 3-2 Global Configuration



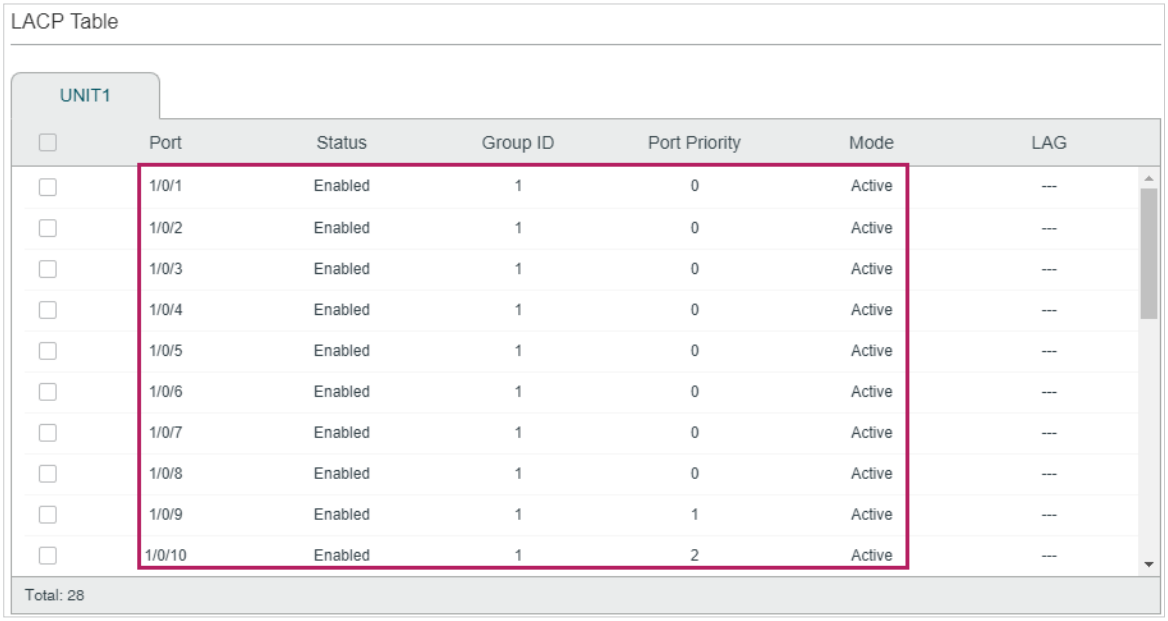
2) Choose the menu **L2 FEATURES > Switching > LAG > LACP Config** to load the following page. In the **Global Config** section, specify the system priority of Switch A as **0** and Click **Apply**. Remember to ensure that the system priority value of Switch B is bigger than 0.

Figure 3-3 System Priority Configuration



3) In the **LACP Table** section, select ports 1/0/1-10, and respectively set the status, group ID, port priority and mode for each port as follows.

Figure 3-4 LACP Configuration



4) Click Save 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

Managing MAC Address Table

CHAPTERS

1. MAC Address Table
2. MAC Address Configurations
3. Appendix: Default Parameters

1 MAC Address Table

1.1 Overview

The MAC address table contains address information that the switch uses to forward packets. As shown below, the table lists map entries of MAC addresses, VLAN IDs and ports. These entries can be manually added or automatically learned by the switch. Based on the MAC-address-to-port mapping in the table, the switch can forward packets 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 according to your needs.

Address Configurations

- Dynamic address

Dynamic addresses are addresses learned by the switch automatically, and 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 specify the aging time if needed.

- Static address

Static addresses are manually added to the address table 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 and determine the packets with specific source or destination MAC addresses that will be dropped by the switch.

2 MAC Address Configurations

With MAC address table, you can:

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

2.1 Using the GUI

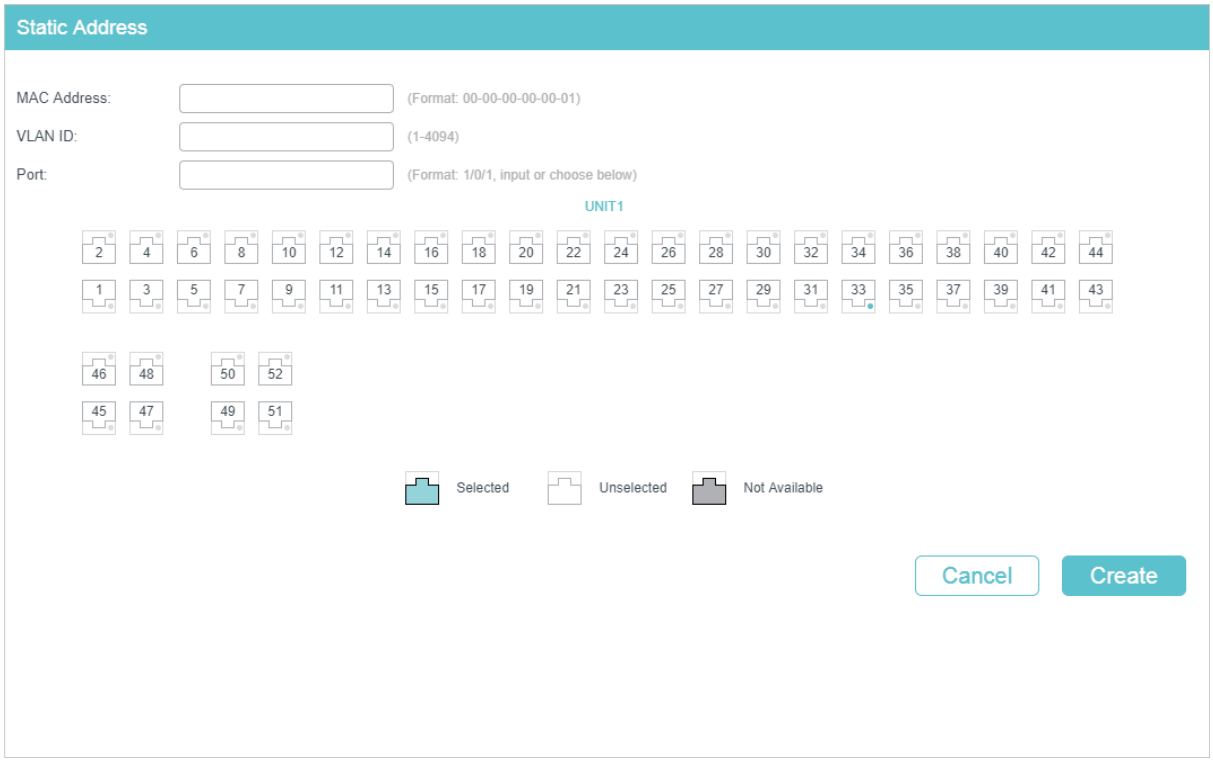
2.1.1 Adding Static MAC Address Entries

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 **L2 FEATURES > Switching > MAC Address > Static Address** and click Add 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 as an address entry.

MAC Address	Enter the static MAC address to be added to the static MAC address entry.
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.

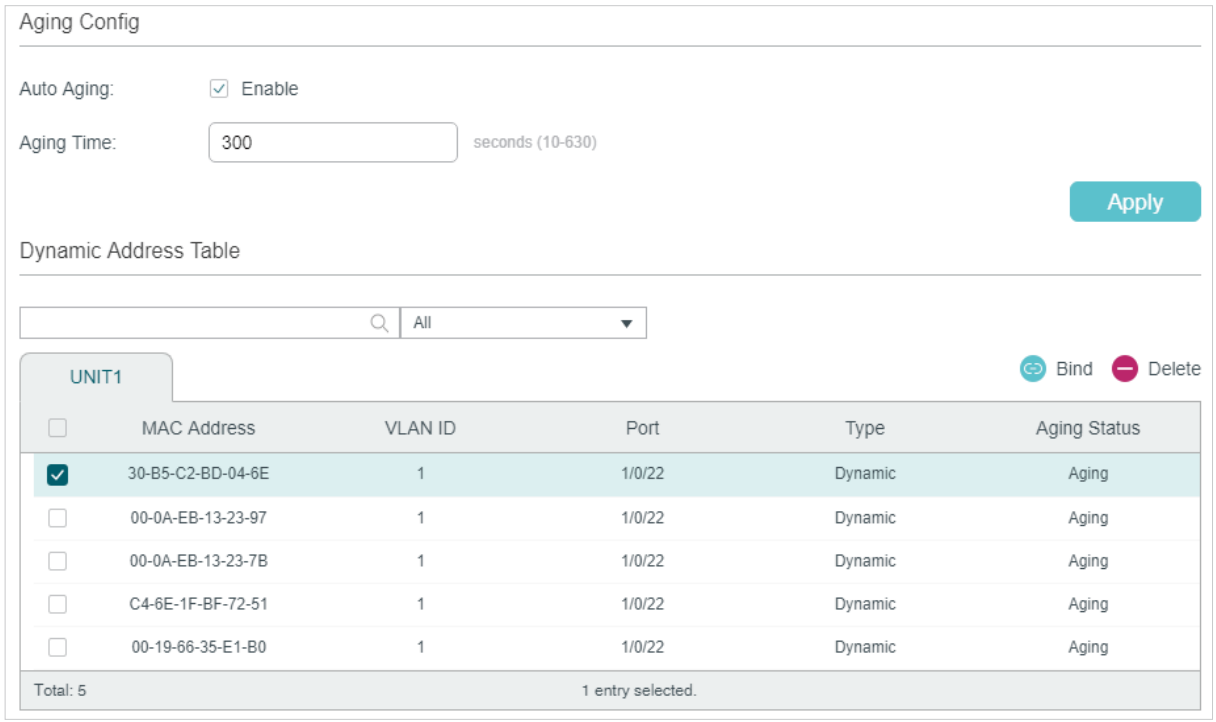
2) Click **Create**.

■ Binding Dynamic Address Entries

If some dynamic address entries are frequently used, you can bind these entries as static entries.

Choose the menu **L2 FEATURES > 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) In the **Dynamic Address Table**section, Select your desired MAC address entries.
2) Click **Bind**, and then the selected entries will become static MAC address entries.

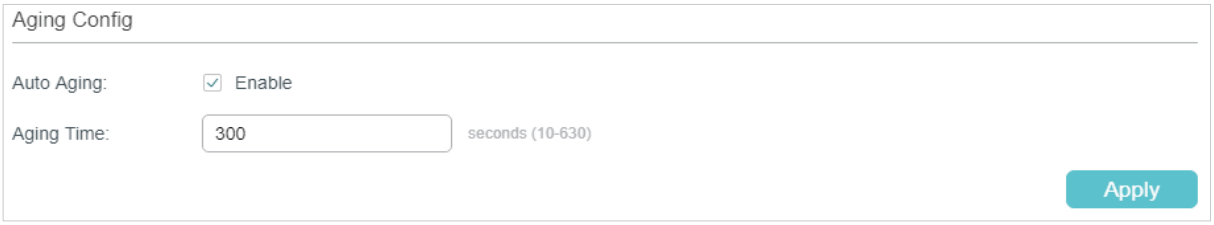
Note:

- 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 **L2 FEATURES > 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.

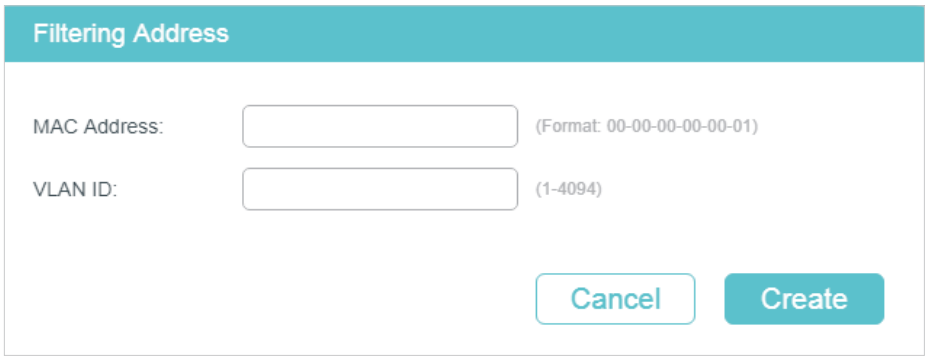
Auto Aging	Enable Auto Aging, then the switch automatically updates the dynamic address table with the aging mechanism. By default, it is enabled.
Aging Time	Set the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated. The valid values are from 10 to 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 **L2 FEATURES > Switching > MAC Address > Filtering Address** and click Add to load the following page.

Figure 2-4 Adding MAC Filtering Address Entries



Follow these steps to add MAC filtering address entries:

1) Enter the MAC Address and VLAN ID.

MAC Address	Specify the MAC address to be used by the switch to filter the received packets.
VLAN ID	Specify an existing VLAN in which packets with the specific MAC address are dropped.

2) Click **Create**.

Note:

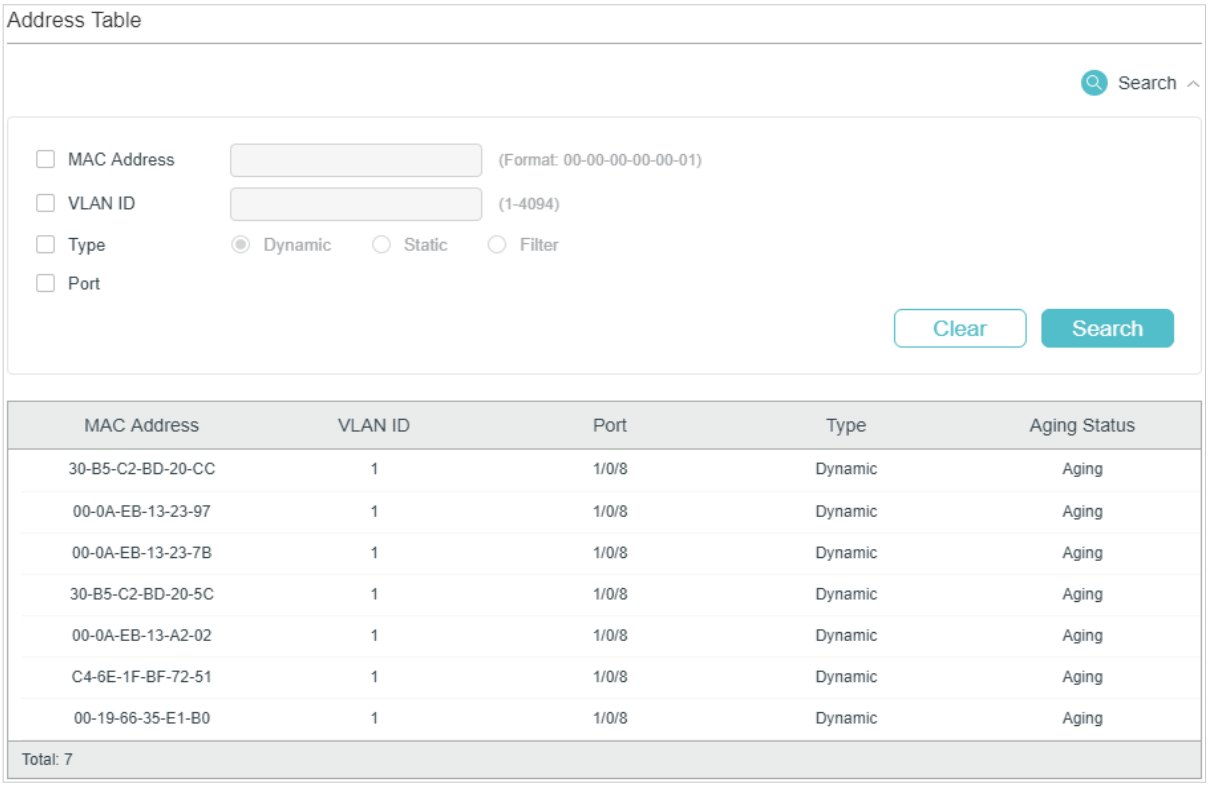
- In the same VLAN, once an address is configured as a filtering address, it cannot be set as a static address, and vice versa.
- Multicast or broadcast addresses cannot be set as filtering addresses .

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 **L2 FEATURES > Switching > MAC Address > Address Table** and click Search to load the following page.

Figure 2-5 Viewing Address Table Entries



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 { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-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 1/0/1.

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. Value 0 means the Auto Aging function is disabled. The default value is 300 and we recommend you keep the default value if you are unsure.
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 be used by the switch to filter the received packets. The switch will drop packets of which the source address or destination address is the specified MAC 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 will be 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 Appendix: Default Parameters

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

Table 3-1 Entries in the MAC Address Table

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

Table 3-2 Default Settings of Dynamic Address Table

Parameter	Default Setting
Auto Aging	Enable
Aging Time	300 seconds

Part 6

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:

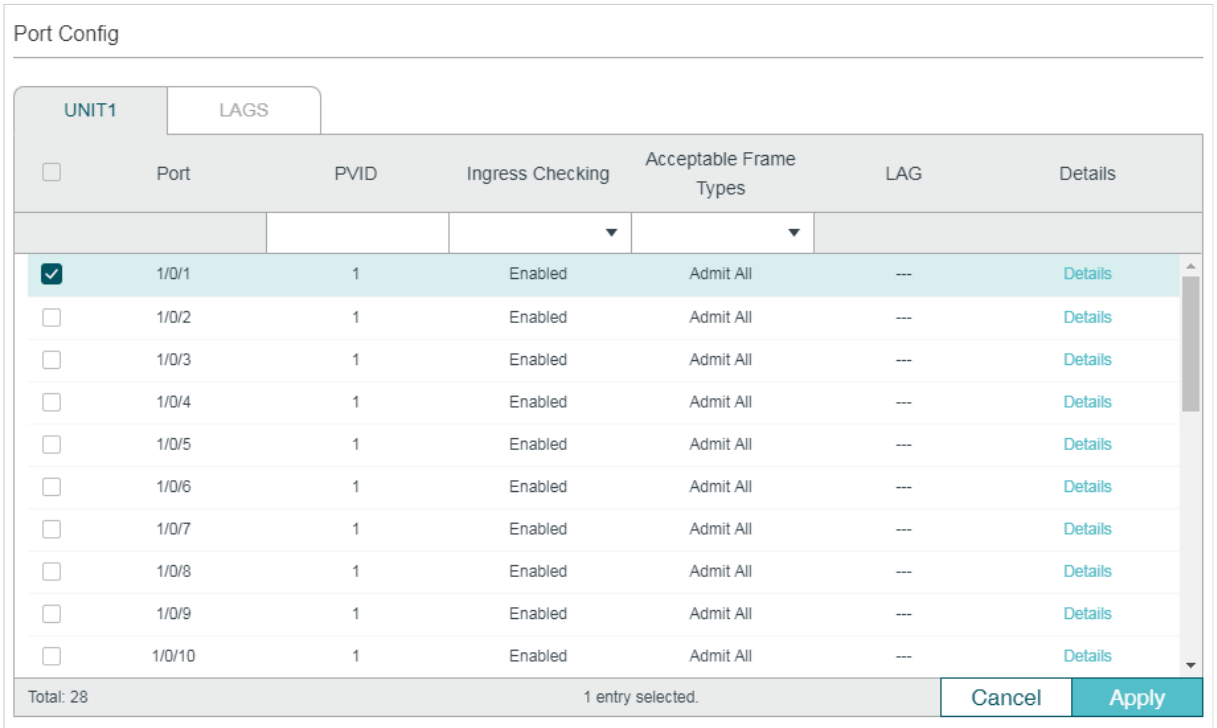
1) Configure the port parameters;
2) Configure the VLAN, including creating a VLAN and adding the configured port to the VLAN.

2.1 Using the GUI

2.1.1 Configuring the PVID of the Port

Choose the menu **L2 FEATURES > VLAN > 802.1Q VLAN > Port Config** to load the following page.

Figure 2-1 Configuring the Port



Select a port and configure the parameters. Click **Apply**.

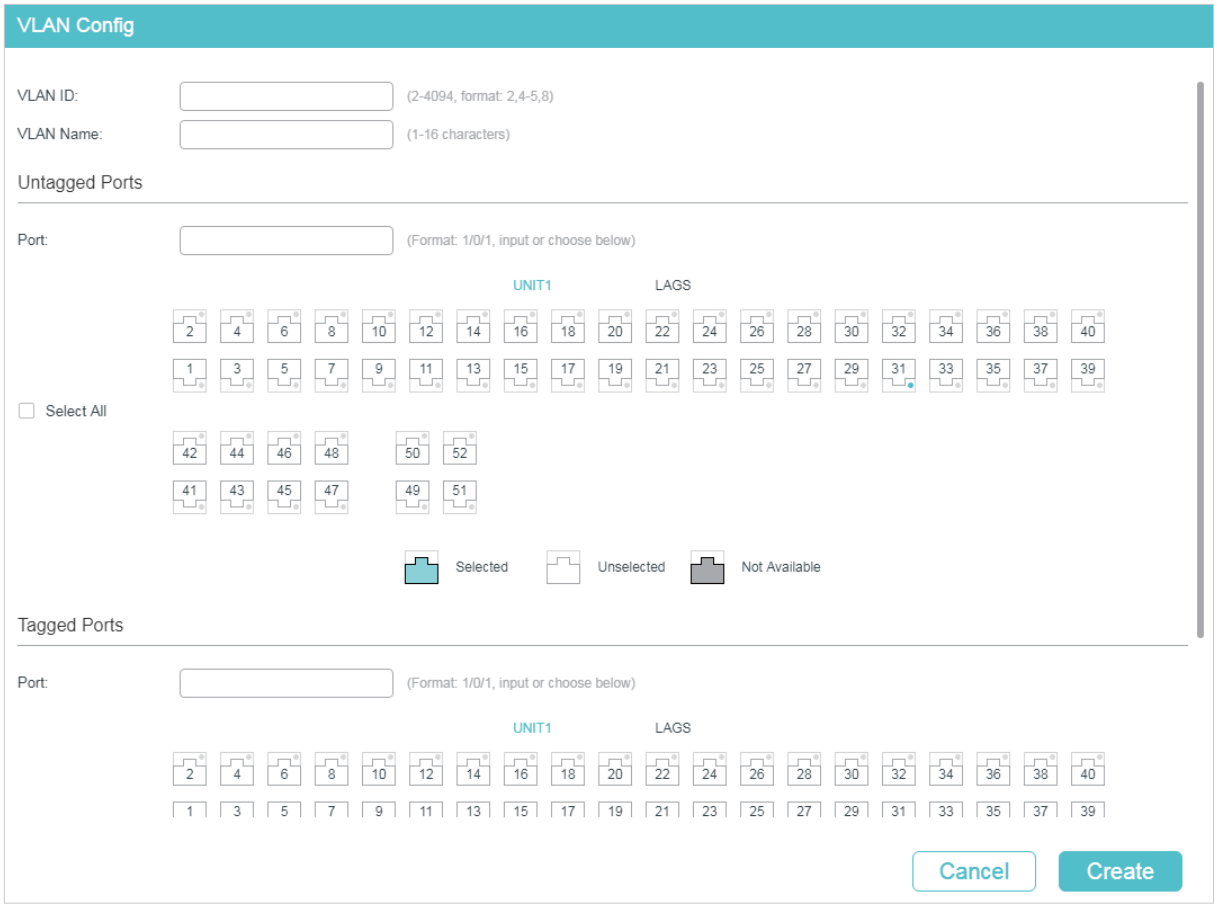
PVID	Set the default VLAN ID of the port. Valid values are from 1 to 4094. It is used mainly in the following two ways: When the port receives an untagged packet, the switch inserts a VLAN tag to the packet based on the PVID.

Ingress Checking	Enable or disable Ingress Checking. With this function enabled, the port will accept the packet of which the VLAN ID is in the port's VLAN list and discard others. With this function disabled, the port will forward the packet directly.
Acceptable Frame Types	Select the acceptable frame type for the port and the port will perform this operation before Ingress Checking. **Admit All:** The port will accept both the tagged packets and the untagged packets. **Tagged Only:** The port will accept the tagged packets only.
LAG	Displays the LAG (Link Aggregation Group) which the port belongs to.
Details	Click the Details button to view the VLANs to which the port belongs.

2.1.2 Configuring the VLAN

Choose the menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** and click Add 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.
VLAN 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. 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. 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* **| 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	**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 4	**switchport check ingress** Enable or disable Ingress Checking. With this function enabled, the port will accept the packet of which the VLAN ID is in the port's VLAN list and discard others. With this function disabled, the port will forward the packet directly.
Step 5	**switchport acceptable frame {**all **|** tagged**}** Select the acceptable frame type for the port and the port will perform this operation before Ingress Checking. all: The port will accept both the tagged packets and the untagged packets. tagged: The port will accept the tagged packets only.
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 PVID of port 1/0/5 as 2, enable the ingress checking and set the acceptable frame type as all:

Switch#configure

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

Switch(config-if)#switchport pvid 2

Switch(config-if)#switchport check ingress

Switch(config-if)#switchport acceptable frame all

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

Port Gi1/0/5:

PVID: 2

Acceptable frame type: All

Ingress Checking: Enable

Member in LAG: N/A

Link Type: General

Member in VLAN:

Vlan	Name	Egress-rule
----	----------	----------
1	System-VLAN	Untagged

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* **| 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	**switchport general allowed vlan** *vlan-list* **{** tagged **|** untagged **}** Add ports to the specified VLAN. *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: Select the egress rule for the port.
Step 4	**show interface switchport [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *lag-id***]** Verify the information 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 add the 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

Acceptable frame type: All

Ingress Checking: Enable

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 Department A and Department B in the company are located in different places, and some computers in different offices connect to the same switch.
- It is required that computers can communicate with each other in the same department but not with computers in the other department.

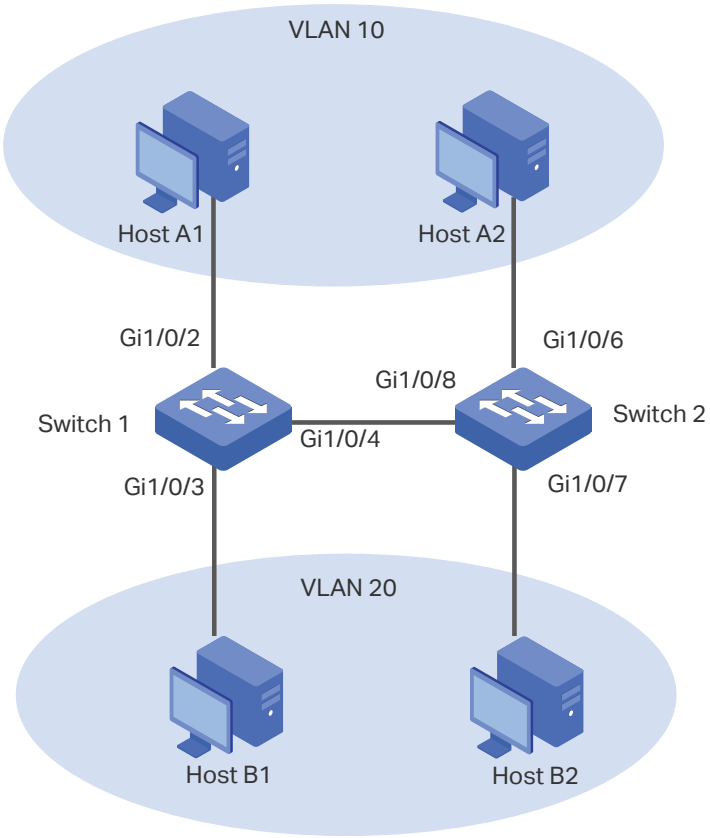
3.2 Configuration Scheme

- 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. Add untagged ports to the corresponding VLANs and specify the PVID.
- The intermediate link between two switches carries traffic from two VLANs simultaneously. Add the tagged ports to both VLANs.

3.3 Network Topology

The figure below shows the network topology. Host A1 and Host A2 are in Department A, while Host B1 and Host B2 are 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



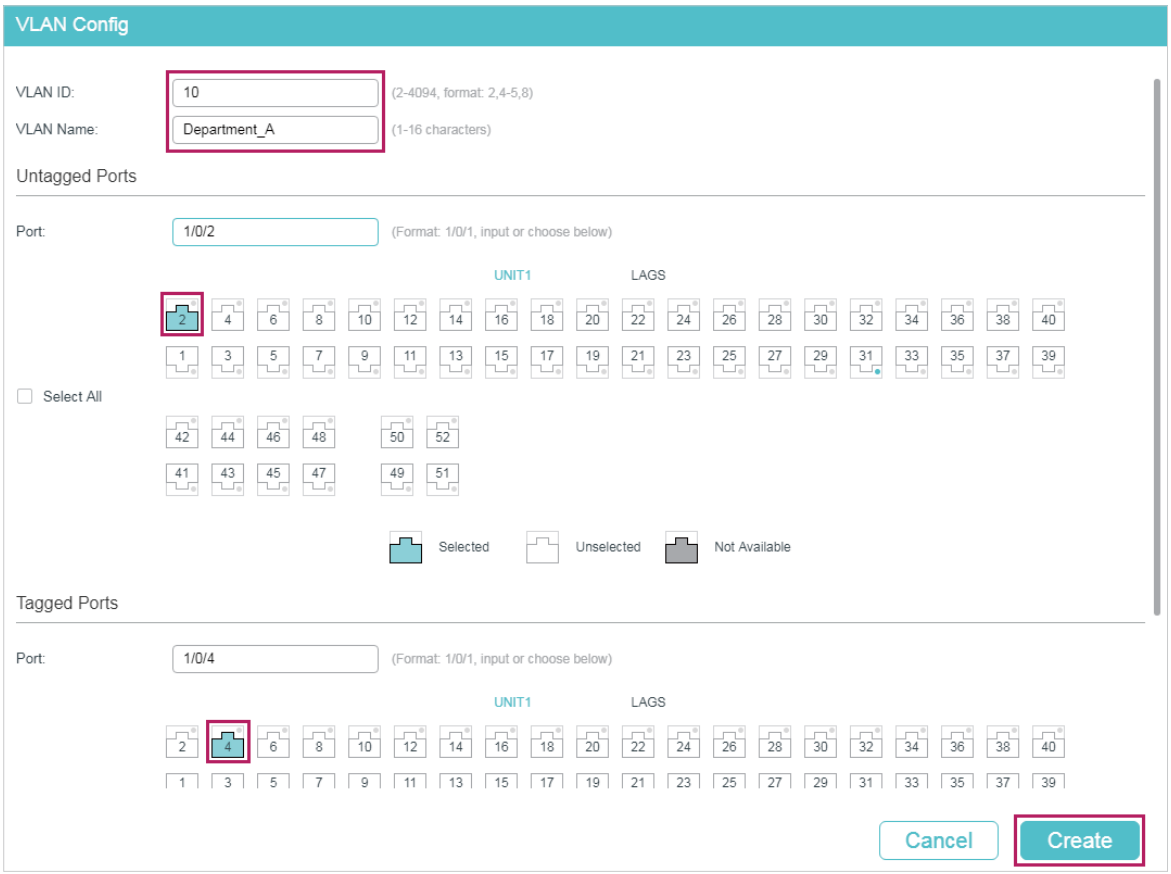
Demonstrated with T1600G-52TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

3.4 Using the GUI

The configurations of Switch 1 and Switch 2 are similar. The following introductions take Switch 1 as an example.

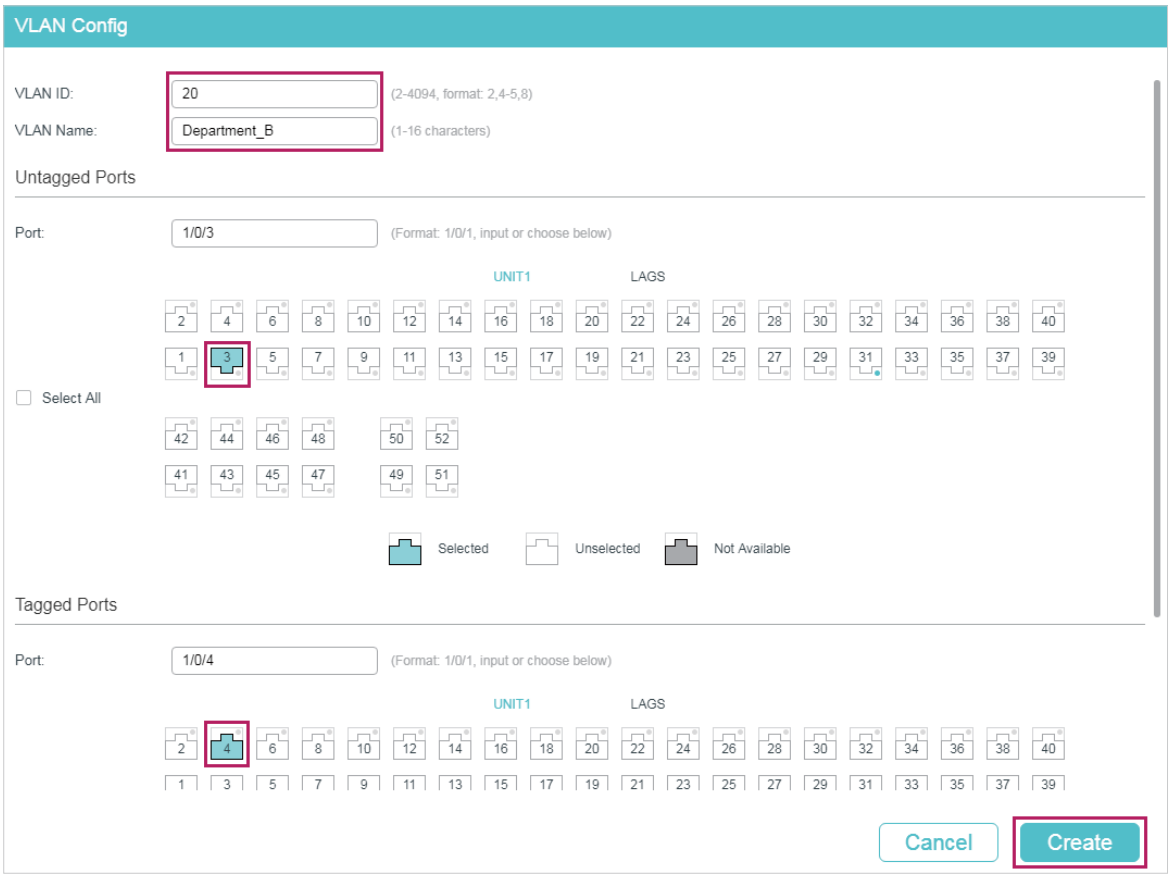
1) Choose the menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** and click Add to load the following page. Create VLAN 10 with the description of Department_A. Add port 1/0/2 as an untagged port and port 1/0/4 as a tagged port to VLAN 10. Click **Create**.

Figure 3-2 Creating VLAN 10 for Department A



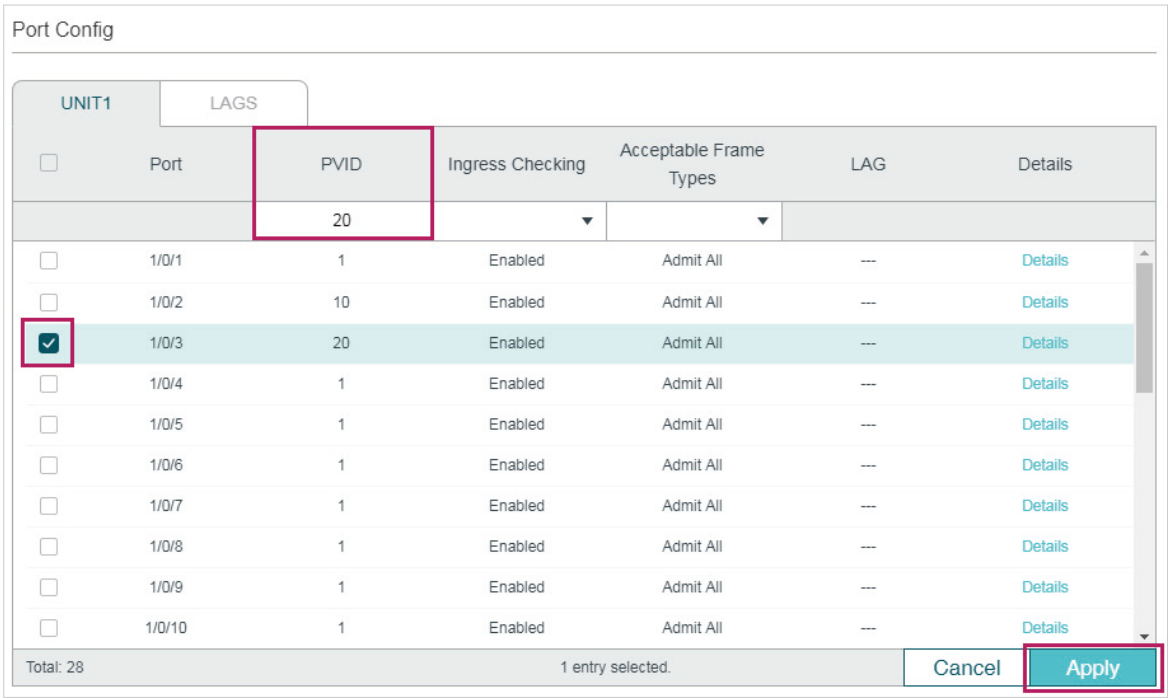
2) Choose the menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** and click Add to load the following page. Create VLAN 20 with the description of Department_B. Add port 1/0/3 as an untagged port and port 1/0/4 as a tagged port to VLAN 20. Click **Create**.

Figure 3-3 Creating VLAN 20 for Department B



3) Choose the menu **L2 FEATURES > VLAN > 802.1Q VLAN > Port Config** to load the following page. Set the PVID of port 1/0/2 as 10 and click **Apply**. Set the PVID of port 1/0/3 as 20 and click **Apply**.

Figure 3-4 Specifying the PVID for the ports



4) Click Save 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) Add untagged port 1/0/2 and tagged port 1/0/4 to VLAN 10. Add untagged port 1/0/3 and tagged port 1/0/4 to VLAN 20.

```
Switch_1(config)#interface gigabitEthernet 1/0/2
Switch_1(config-if)#switchport general allowed vlan 10 untagged
Switch_1(config-if)#exit
Switch_1(config)#interface gigabitEthernet 1/0/3
Switch_1(config-if)#switchport general allowed vlan 20 untagged
Switch_1(config-if)#exit
Switch_1(config)#interface gigabitEthernet 1/0/4
Switch_1(config-if)#switchport general allowed vlan 10 tagged
Switch_1(config-if)#switchport general allowed vlan 20 tagged
Switch_1(config-if)#exit
```

3) Set the PVID of port 1/0/2 as 10, and set the PVID of port 1/0/3 as 20.

```
Switch_1(config)#interface gigabitEthernet 1/0/2
Switch_1(config-if)#switchport pvid 10
Switch_1(config-if)#exit
Switch_1(config)#interface gigabitEthernet 1/0/3
```

```
Switch_1(config-if)#switchport pvid 20
Switch_1(config-if)#end
Switch_1#copy running-config startup-config
```

Verify the Configurations

Verify the 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,
                                       Gi1/0/5, Gi1/0/6, Gi1/0/7, Gi1/0/8,
                                       ...
                                       Gi1/0/49, Gi1/0/50, Gi1/0/51, Gi1/0/52
10     Department-A         active     Gi1/0/2, Gi1/0/4
20     Department-B         active     Gi1/0/3, Gi1/0/4
Primary  Secondary  Type        Ports
-------  ---------  ----------  ---------------------
```

Verify the VLAN configuration:

```
Switch_1(config)#show interface switchport
Port      LAG   Type      PVID  Acceptable frame type   Ingress Checking
-------   ---   ----      ----  ---------------------   ----------------
Gi1/0/1   N/A   General   1     All                     Enable
Gi1/0/2   N/A   General   10    All                     Enable
Gi1/0/3   N/A   General   20    All                     Enable
Gi1/0/4   N/A   General   1     All                     Enable
Gi1/0/5   N/A   General   1     All                     Enable
.....
```

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
Ingress Checking	Enabled
Acceptable Frame Types	Admit All

Part 7

Configuring MAC VLAN

CHAPTERS

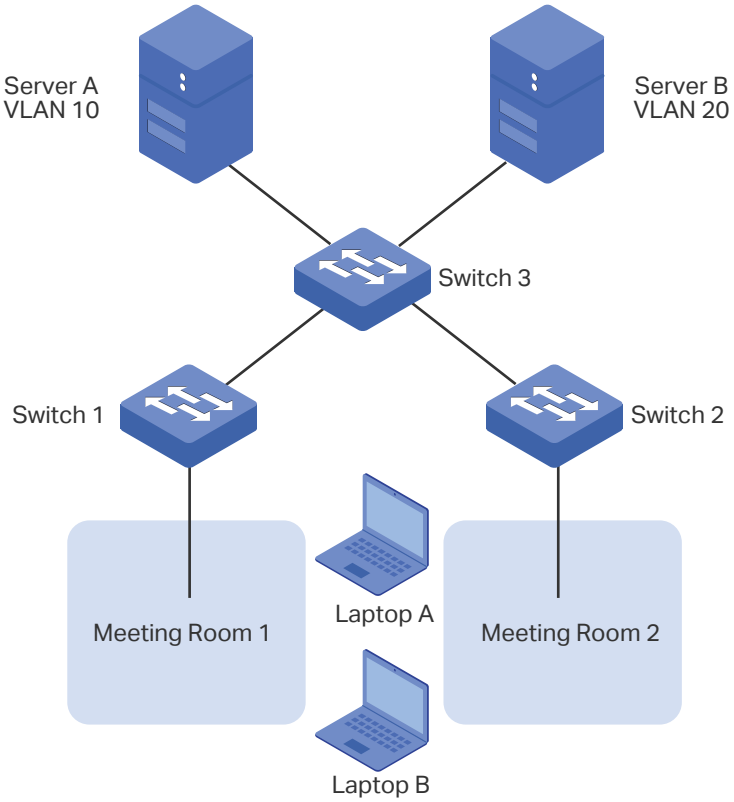
1. Overview
2. MAC VLAN Configuration
3. Configuration Example
4. Appendix: Default Parameters

1 Overview

VLAN is generally divided by ports. It is a common way of division but isn't suitable for those networks that require frequent topology changes. With the popularity of mobile office, at different times a terminal device may access the network 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 MAC 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 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

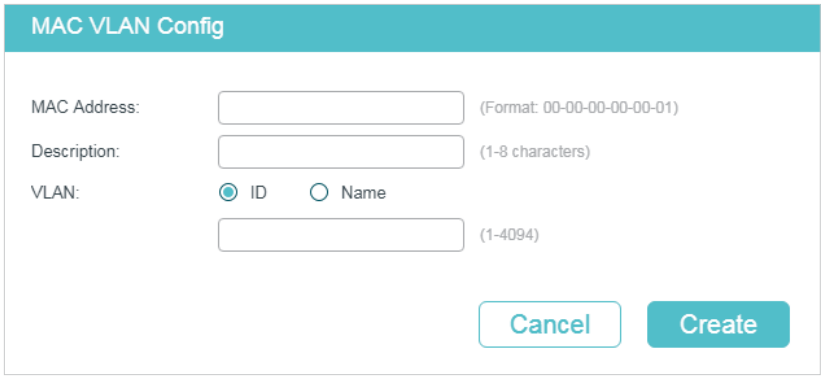
2.1.1 Configuring 802.1Q VLAN

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 **L2 FEATURES > VLAN > MAC VLAN** and click Add to load the following page.

Figure 2-1 Creating MAC VLAN



Follow these steps to bind the MAC address to the 802.1Q 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 in the format of 00-00-00-00-00-01.
Description	Give a MAC address description for identification with up to 8 characters.
VLAN ID/Name	Enter the ID number or name of the 802.1Q VLAN that will be bound to the MAC VLAN..

2) Click **Create**.

Note:

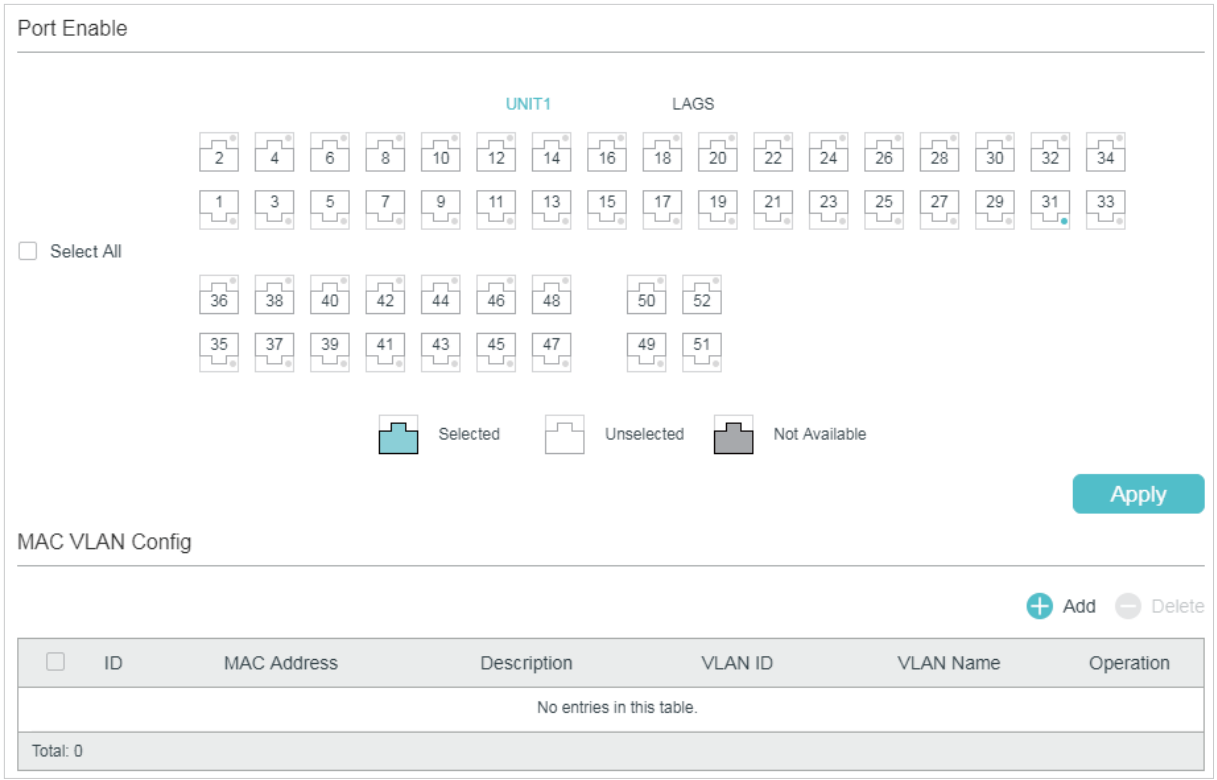
One MAC address can be bound to only one VLAN.

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 **L2 FEATURES > VLAN > MAC VLAN** to load the following page.

Figure 2-2 Enabling MAC VLAN for the Port



In the **Port Enable** section, select the 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 and 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*: Specify the MAC address of the device in the format of xx:xx:xx:xx:xx:xx. *vlan-id*: Enter the ID number of the 802.1Q VLAN that will be bound to the MAC VLAN. *descript*: Specify the MAC address description for identification, with up to 8 characters.
Step 3	**show mac-vlan { all | mac-address** *mac-addr* **| vlan** *vlan-id* **}** 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* **| 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	**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

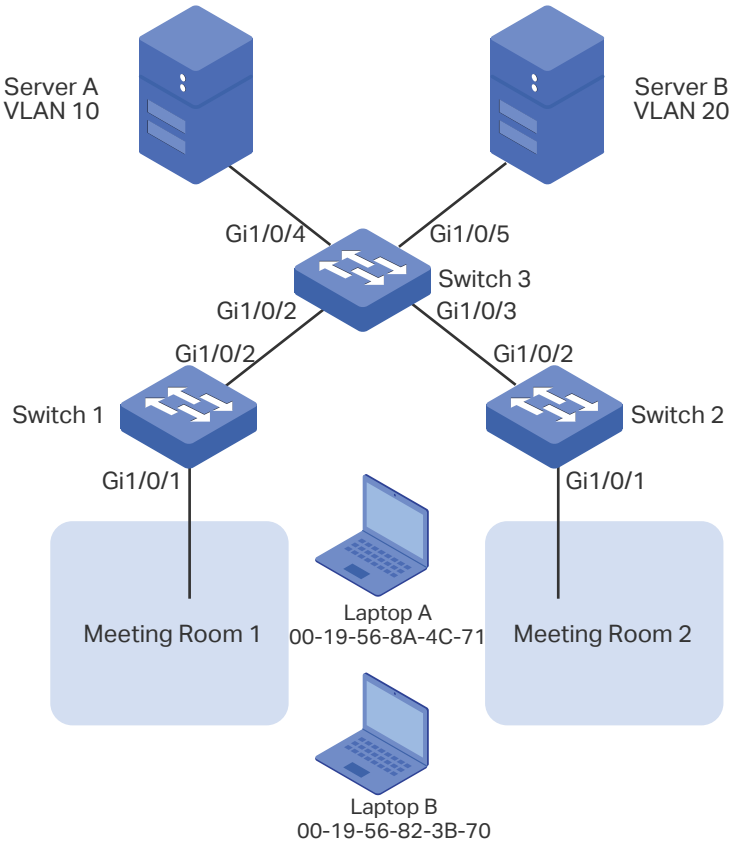
Switch#copy running-config startup-config

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 and add the ports to the VLANs based on the network topology. For the ports connecting the laptops, set the

egress rule as Untagged; for the ports connecting to other switch, 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 T1600G-52TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

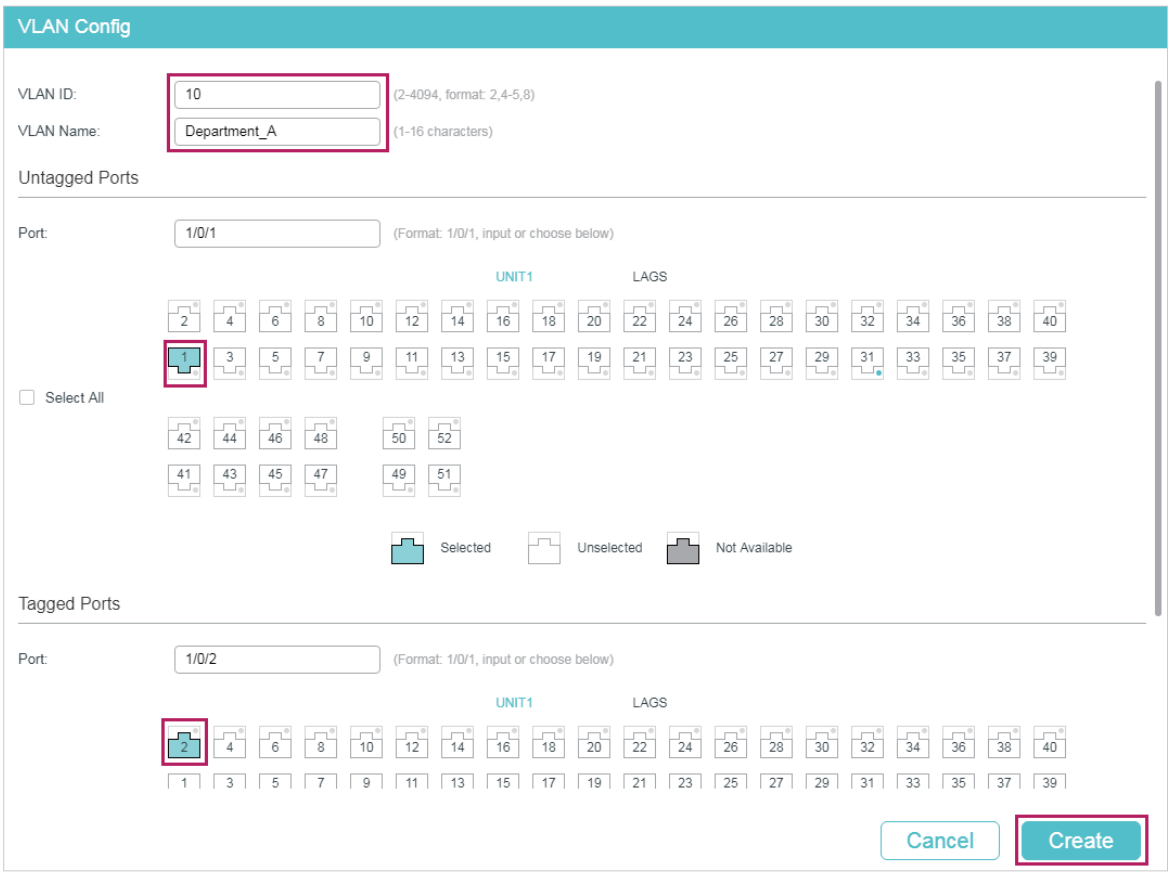
3.3 Using the GUI

■ 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.

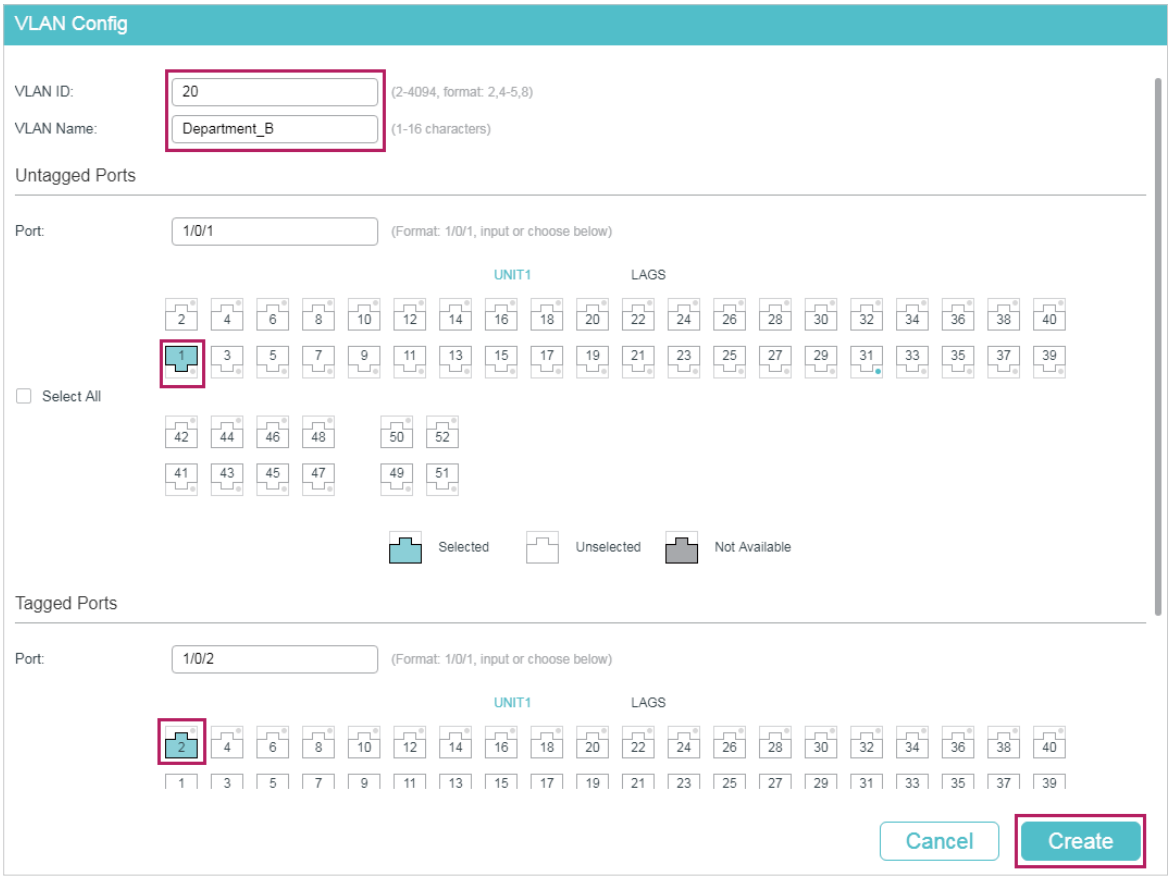
1) Choose the menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** and click Add to load the following page. Create VLAN 10, and add untagged port 1/0/1 and tagged port 1/0/2 to VLAN 10. Click **Create**.

Figure 3-2 Creating VLAN 10



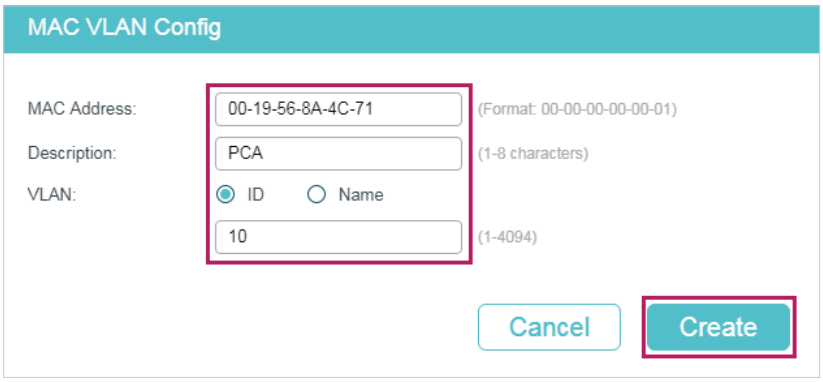
2) Choose the menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** and click Add to load the following page. Create VLAN 20, and add untagged port 1/0/1 and tagged port 1/0/2 to VLAN 20. Click **Create**.

Figure 3-3 Creating VLAN 20



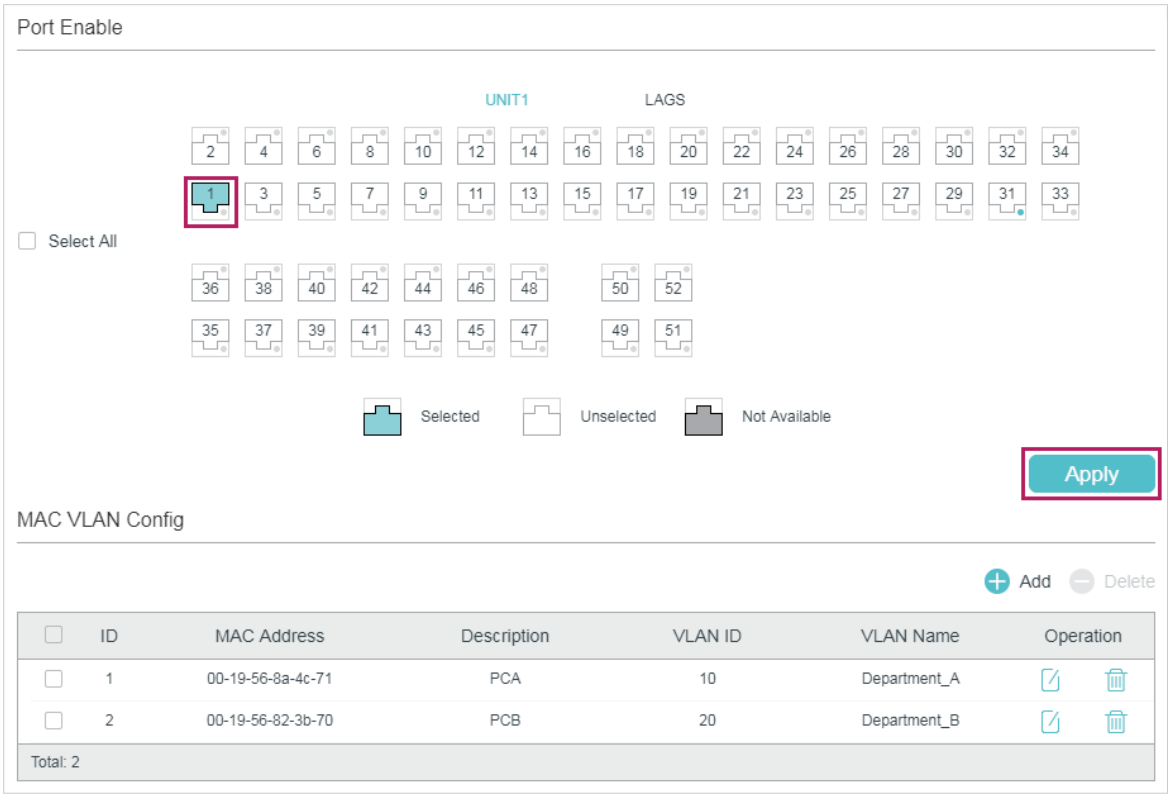
3) Choose the menu **L2 FEATURES > VLAN > MAC VLAN** and click Add to load the following page. Specify the corresponding parameters and click **Create** to bind the MAC address of Laptop A to VLAN 10 and bind the MAC address of Laptop B to VLAN 20.

Figure 3-4 Creating MAC VLAN



4) Choose the menu **L2 FEATURES > VLAN > MAC VLAN** to load the following page. In the **Port Enable** section select port 1/0/1 and click **Apply** to enable MAC VLAN.

Figure 3-5 Enabing MAC VLAN for the Port

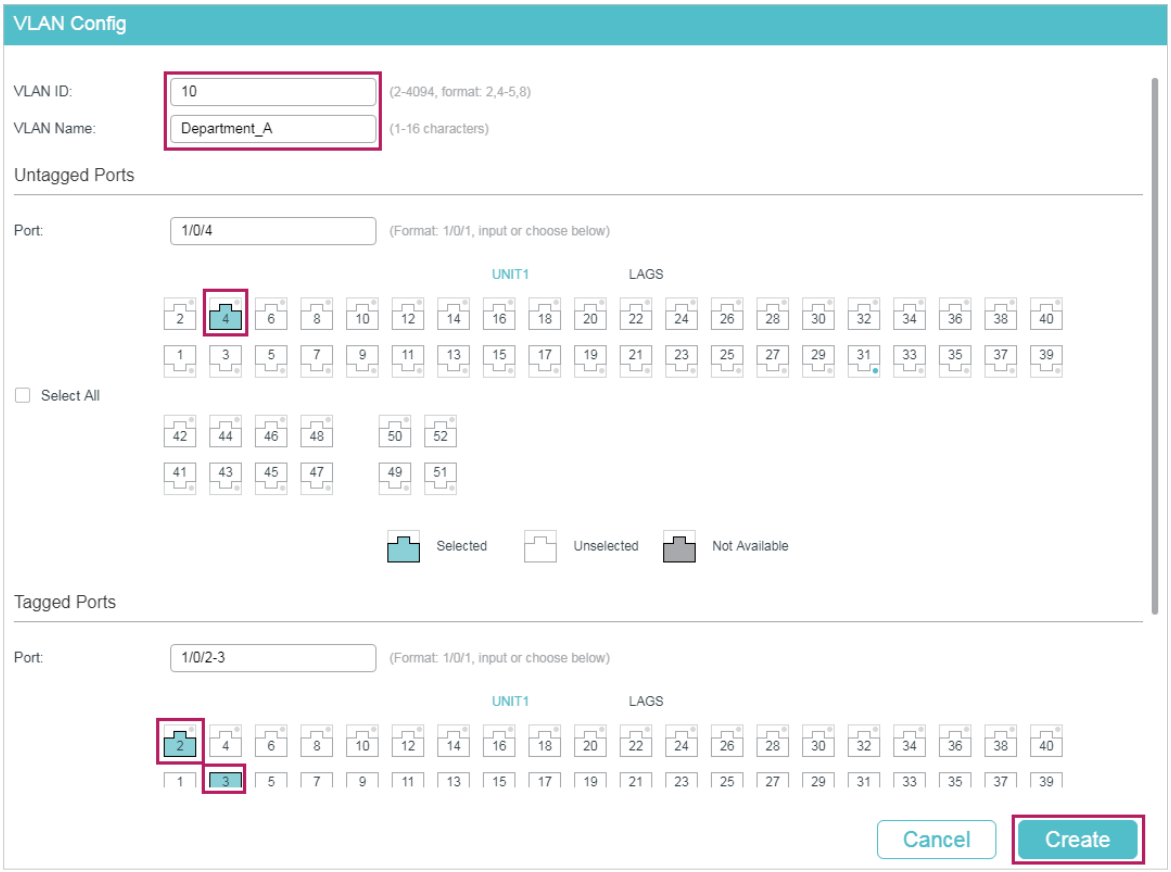


5) Click Save to save the settings.

Configurations for Switch 3

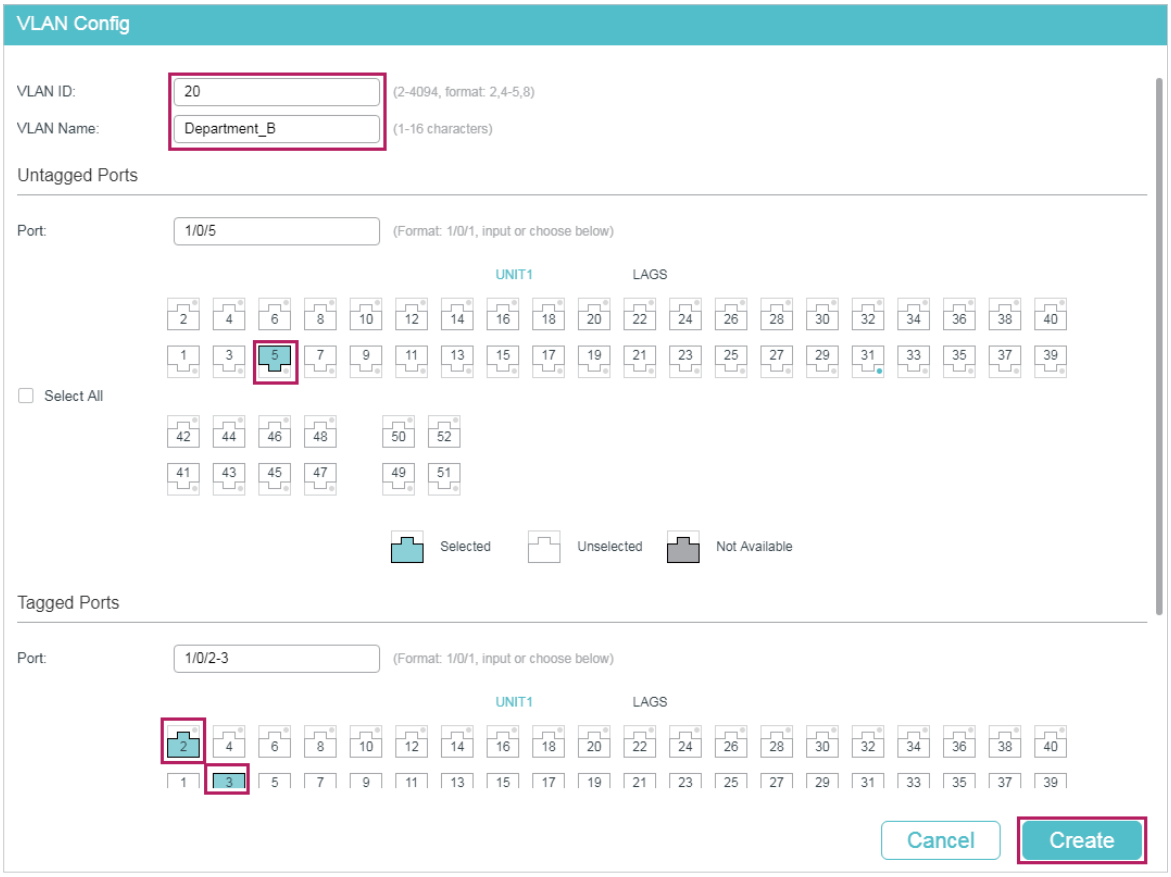
1) Choose the menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** and click Add to load the following page. Create VLAN 10, and add untagged port 1/0/4 and tagged ports 1/0/2-3 to VLAN 10. Click **Create**.

Figure 3-6 Creating VLAN 10



2) Click **Create** to load the following page. Create VLAN 20, and add untagged port 1/0/5 and tagged ports 1/0/2-3 to VLAN 20. Click **Create**.

Figure 3-7 Creating VLAN 20



3) Click Save 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) Add tagged port 1/0/2 and untagged port 1/0/1 to both VLAN 10 and VLAN 20. Then enable MAC VLAN on port 1/0/1.

Switch_1(config)#interface gigabitEthernet 1/0/2

Switch_1(config-if)#switchport general allowed vlan 10,20 tagged

Switch_1(config-if)#exit

Switch_1(config)#interface gigabitEthernet 1/0/1

Switch_1(config-if)#switchport general allowed vlan 10,20 untagged

Switch_1(config-if)#mac-vlan

Switch_1(config-if)#exit

3) 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) Add tagged port 1/0/2 and port 1/0/3 to both VLAN 10 and VLAN 20.

Switch_3(config)#interface gigabitEthernet 1/0/2

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) Add untagged port 1/0/4 to VLAN 10 and untagged port 1/0/5 to VLAN 20.

Switch_3(config)#interface gigabitEthernet 1/0/4

```
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 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 Add              Name              VLAN-ID
-------------------  ----------------  ----------
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       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      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	Disabled

Part 8

Configuring Protocol VLAN

CHAPTERS

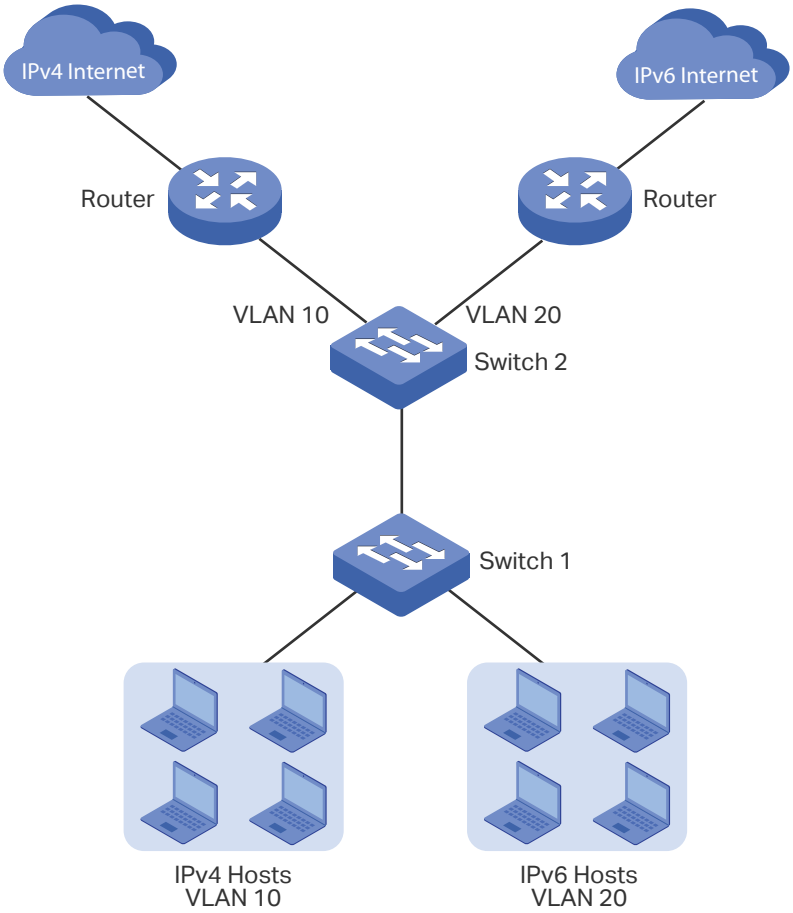
1. Overview
2. Protocol VLAN Configuration
3. Configuration Example
4. Appendix: Default Parameters

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 specific fields of received packets, encapsulate the packets in specific formats, and forward the packets with 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.

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.
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 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. (If MAC VLAN is also configured, the switch will first process Protocol VLAN, then MAC 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

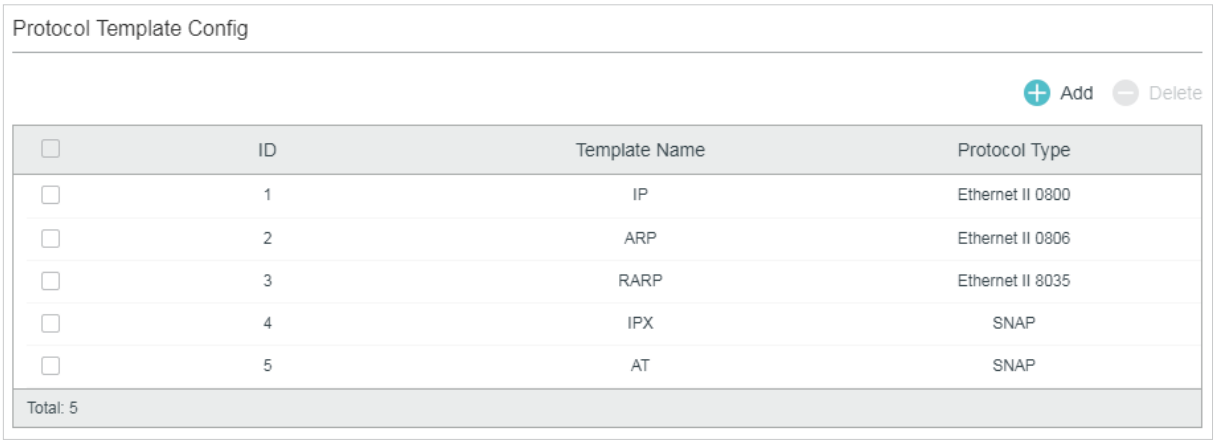
2.1.1 Configuring 802.1Q VLAN

Before configuring 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 **L2 FEATURES > VLAN > Protocol VLAN > Protocol Template** to load the following page.

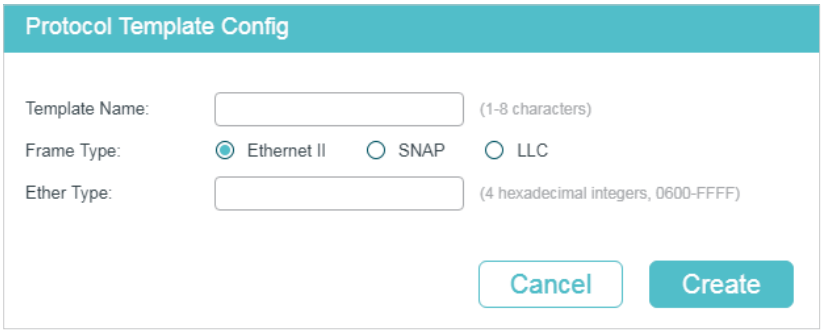
Figure 2-1 Check the Protocol Template



Follow these steps to create a protocol template:

1) Check whether your desired template already exists in the **Protocol Template Config** section. If not, click Add to create a new template.

Figure 2-2 Creating a Protocol Template



Template Name	Give a protocol name to identify the protocol template.
Frame Type	Select the frame type of the new protocol template. **Ethernet II:** A common Ethernet frame format. Select to specify the Frame Type by entering the Ether Type. **SNAP:** An Ethernet 802.3 frame format based on IEEE 802.3 and IEEE 802.2 SNAP. Select to specify the Frame Type by entering the Ether Type. **LLC:** An Ethernet 802.3 frame format based on IEEE 802.3 and IEEE 802.2 LLC. Select to specify the Frame Type by entering the DSAP and SSAP.
Ether Type	Enter the Ethernet protocol type value for the protocol template. It is available when **Ethernet II** and **SNAP** is selected. It is the Ether Type field in the frame and is used to identify the data type of the frame.

DSAP	Enter the DSAP value for the protocol template. It is available when **LLC** is selected. It is the DSAP field in the frame and is used to identify the data type of the frame.
SSAP	Enter the SSAP value for the protocol template. It is available when **LLC** is selected. It is the SSAP field in the frame and is used to identify the data type of the frame.

2) Click **Create**.

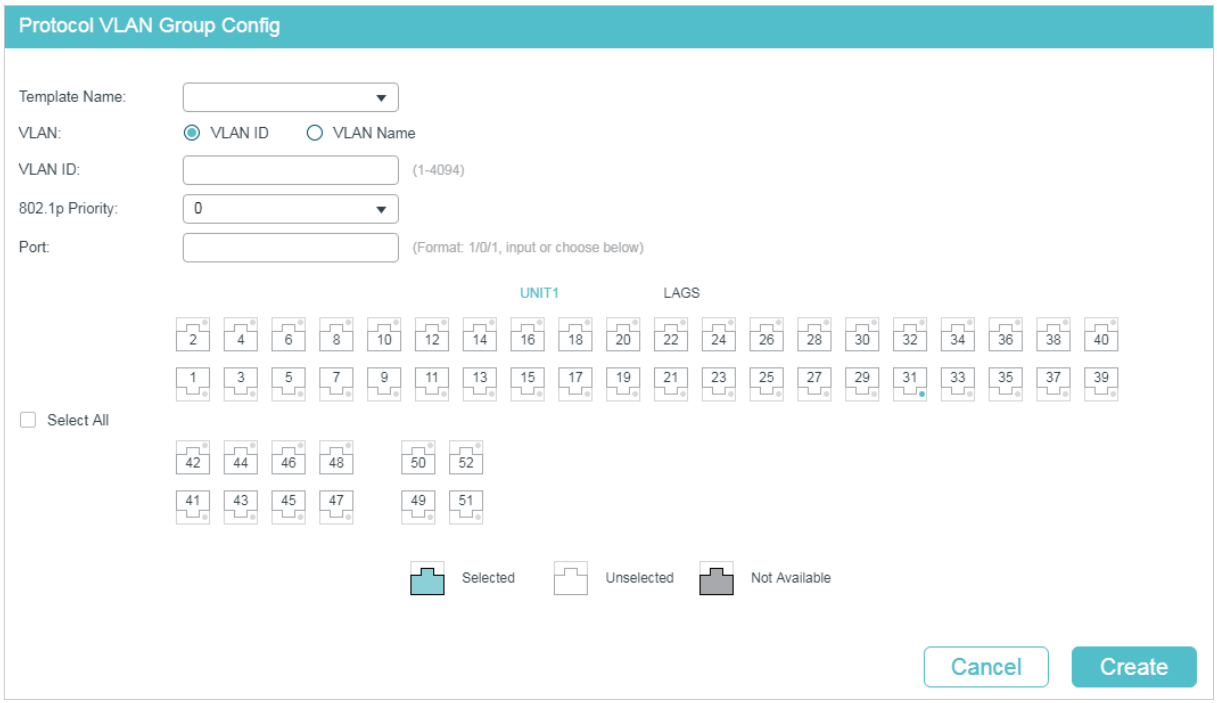
Note:

A protocol template that is bound to a VLAN cannot be deleted.

2.1.3 Configuring Protocol VLAN

Choose the menu **L2 FEATURES > VLAN > Protocol VLAN > Protocol VLAN Group** and click Add to load the following page.

Figure 2-3 Configure the Protocol VLAN Group



Follow these steps to configure the protocol group:

1) In the **Protocol Group Config** section, specify the following parameters.

Template Name	Select the previously defined protocol template.
VLAN ID/Name	Enter the ID number or name of the 802.1Q VLAN that will be bound to the Protocol VLAN..
802.1p Priority	Specify the 802.1p priority for the packets that belong to the protocol VLAN. The switch will determine the forwarding sequence according this value. The packets with larger value of 802.1p priority have the higher priority.

2) Select the desired ports. Click **Create**.

Note:

The member port of an LAG (Link Aggregation Group) follows the configuration of the LAG and 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*: Enter4 hexadecimal numbers as the Ethernet protocol type for the protocol template. It is the Ether Type field in the frame and is used to identify the data type of the frame. *dsap_type*: Enter 2 hexadecimal numbers as the DSAP value for the protocol template. It is the DSAP field in the frame and is used to identify the data type of the frame. *ssap_type*: Enter 2 hexadecimal numbers as the SSAP value for the protocol template. It is the SSAP field in the frame and is used to identify the data type of the frame.
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* **priority** *priority* **template** *index* Bind the protocol template to the VLAN. *vid* : Enter the ID number of the 802.1Q VLAN that will be bound to the Protocol VLAN. *priority* : Specify the 802.1p priority for the packets that belong to the protocol VLAN. The switch will determine the forwarding sequence according this value. The packets with larger value of 802.1p priority have the higher priority. *index* : Specify the protocol template index.
Step 4	**show protocol-vlan vlan** Check the protocol VLAN index (entry-id) of each protocol group.
Step 5	**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 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 and add port 1/0/2 to protocol VLAN:

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 **priority** 5 **template** 6

Switch(config)#show protocol-vlan vlan

Index	Protocol-Name	VID	Priority	Member
1	IPv6	10	0	

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

Switch(config-if)#protocol-vlan group 1

Switch(config-if)#show protocol-vlan vlan

Index	Protocol-Name	VID	Priority	Member
1	IPv6	10	5	Gi1/0/2

Switch(config-if)#end

Switch#copy running-config startup-config

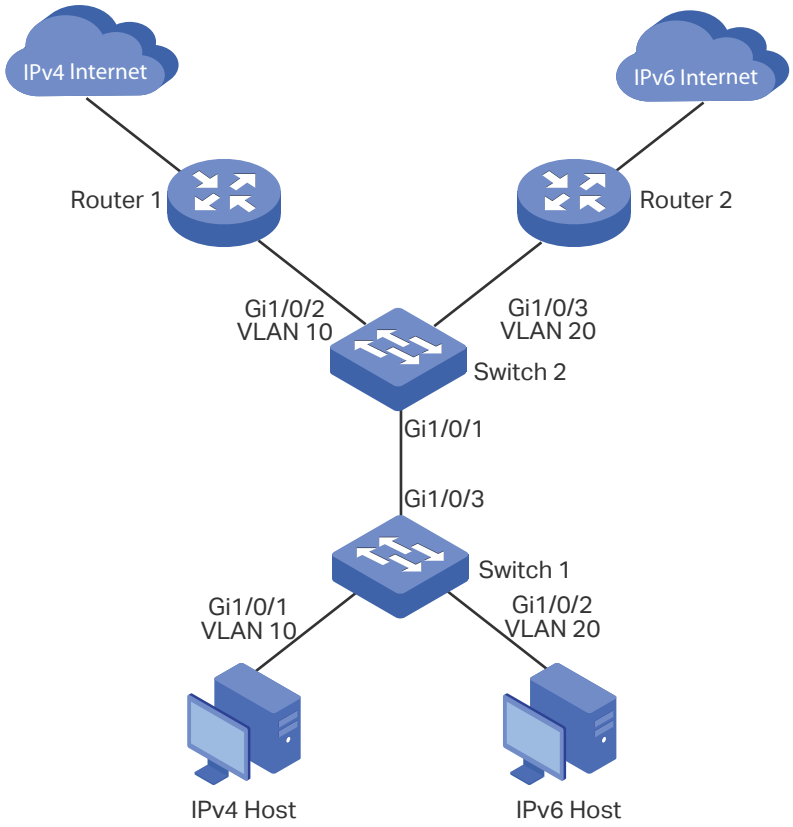
3 Configuration Example

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 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.

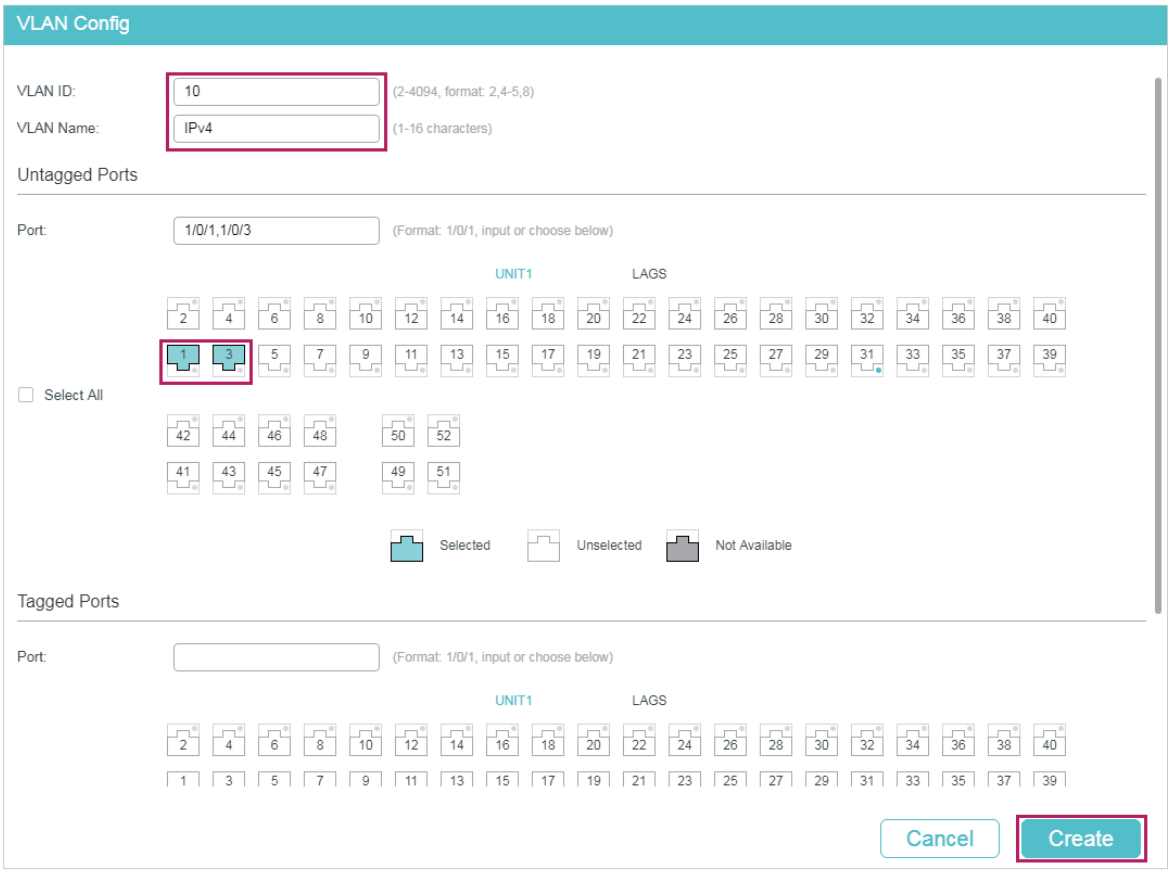
Demonstrated with T1600G-52TS, this chapter provides configuration procedures in two ways: using the GUI and using the CLI.

3.3 Using the GUI

- Configurations for Switch 1

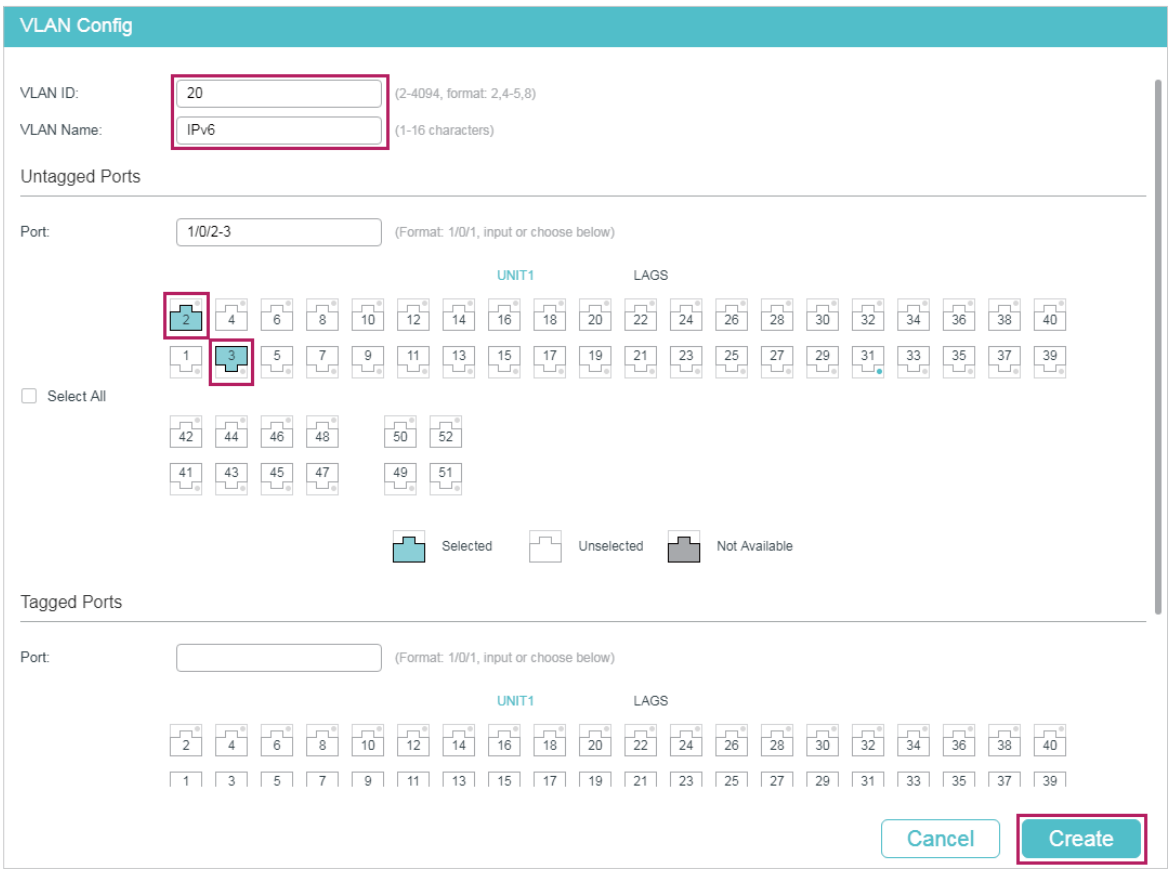
1) Choose the menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** and click Add to load the following page. Create VLAN 10, and add untagged port 1/0/1 and untagged port 1/0/3 to VLAN 10. Click **Create**.

Figure 3-2 Create VLAN 10



2) Click Add to load the following page. Create VLAN 20, and add untagged ports 1/0/2-3 to VLAN 20. Click **Create**.

Figure 3-3 Create VLAN 20

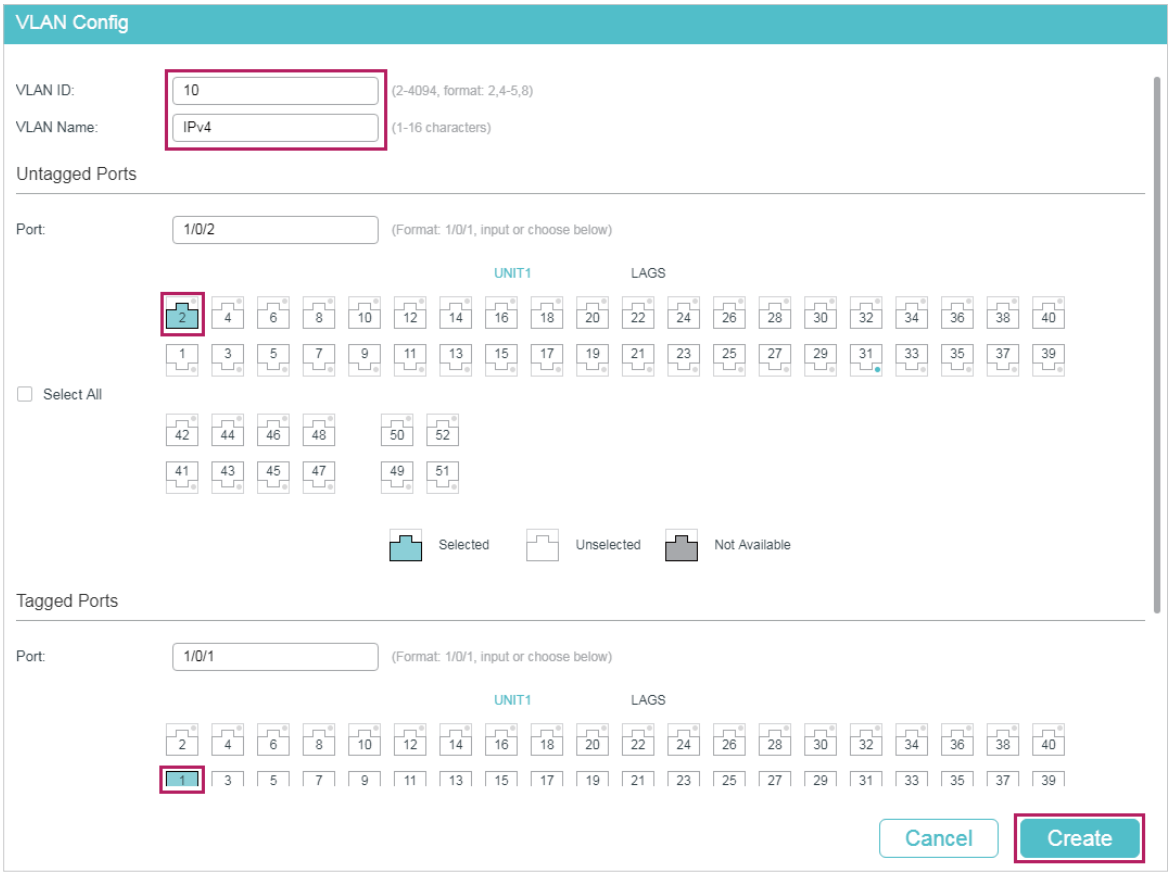


3) Click Save to save the settings.

Configurations for Switch 2

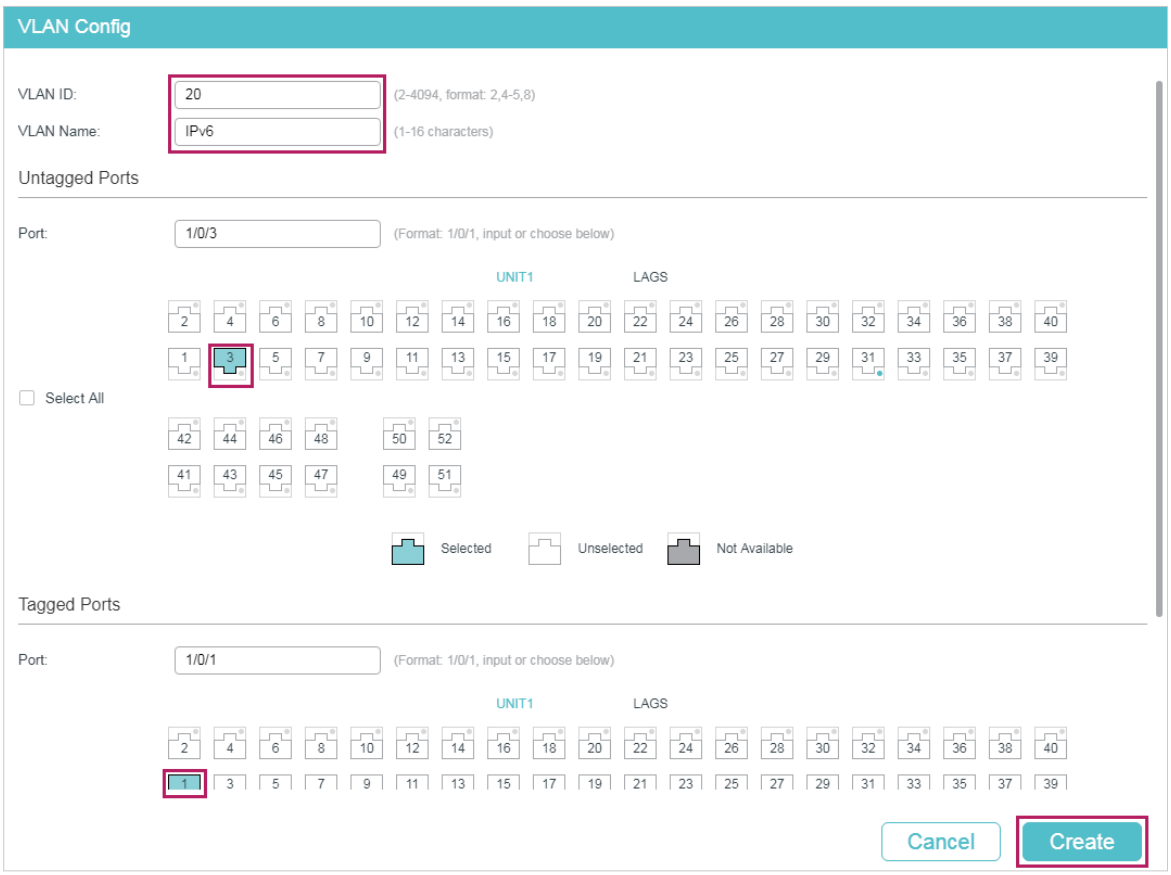
1) Choose the menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** and click Add to load the following page. Create VLAN 10, and add tagged port 1/0/1 and untagged port 1/0/2 to VLAN 10. Click **Create**.

Figure 3-4 Create VLAN 10



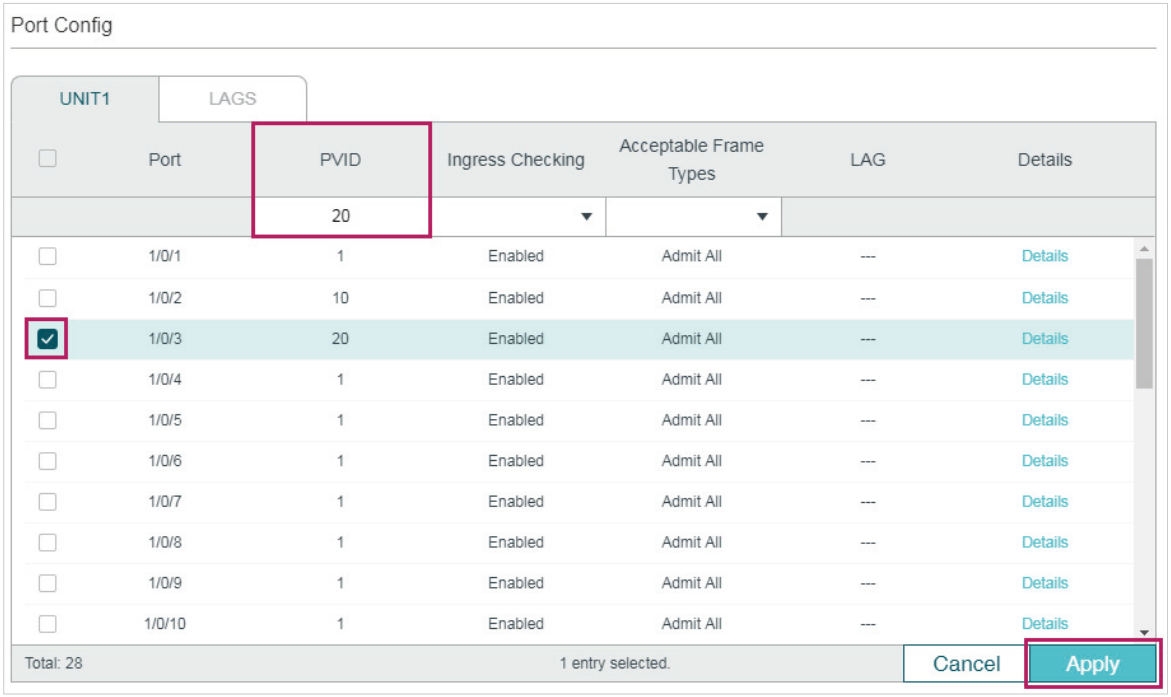
2) Click Add to load the following page. Create VLAN 20, and add tagged port 1/0/1 and untagged port 1/0/3 to VLAN 20. Click **Create**.

Figure 3-5 Create VLAN 20



3) Choose the menu **L2 FEATURES > VLAN > 802.1Q VLAN > Port Config** to load the following page. Set the PVID of port 1/0/2 and port 1/0/3 as 10 and 20 respectively . Click **Apply**.

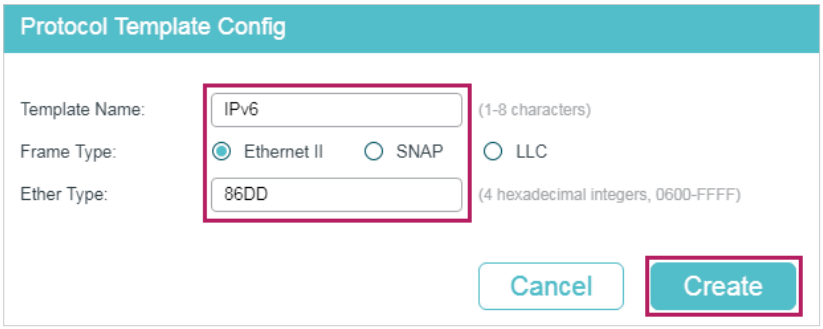
Figure 3-6 Port Configuration



4) Choose the menu **L2 FEATURES > VLAN > Protocol VLAN > Protocol Template** and click Add 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 3-7 Create the IPv6 Protocol Template



5) Choose the menu **L2 FEATURES > VLAN > Protocol VLAN > Protocol VLAN Group** and click Add 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 **Create**. Select the IPv6 protocol name, enter VLAN ID 20, select port 1, and click **Create**.

Figure 3-8 Configure the IPv4 Protocol Group

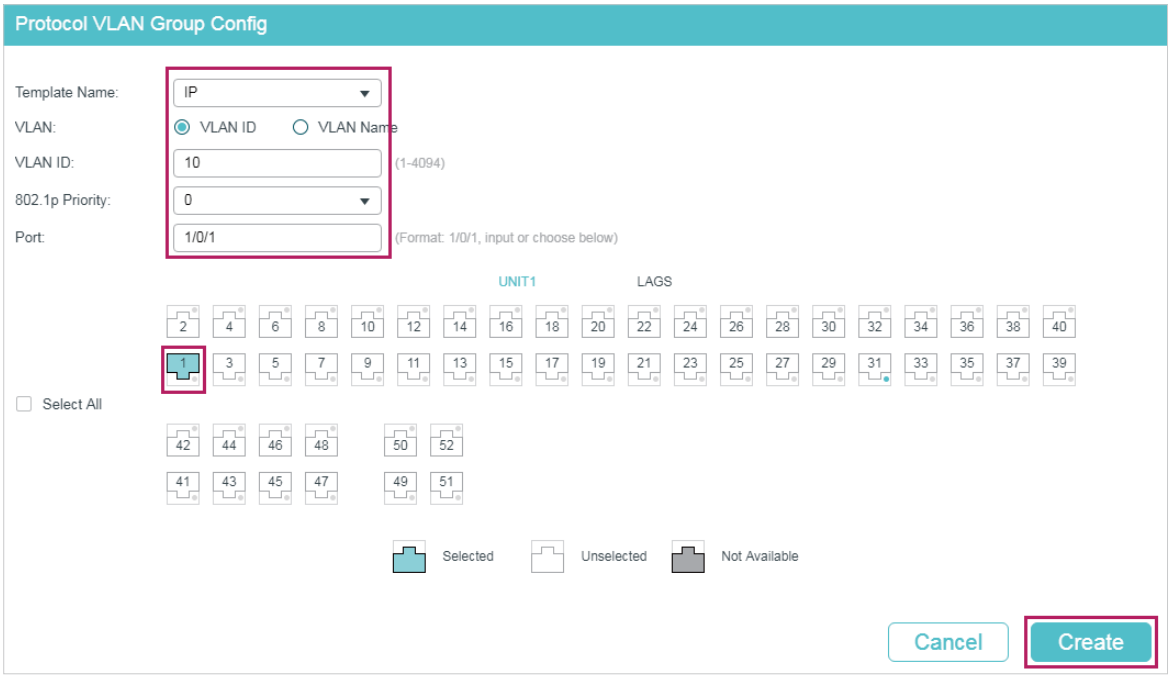
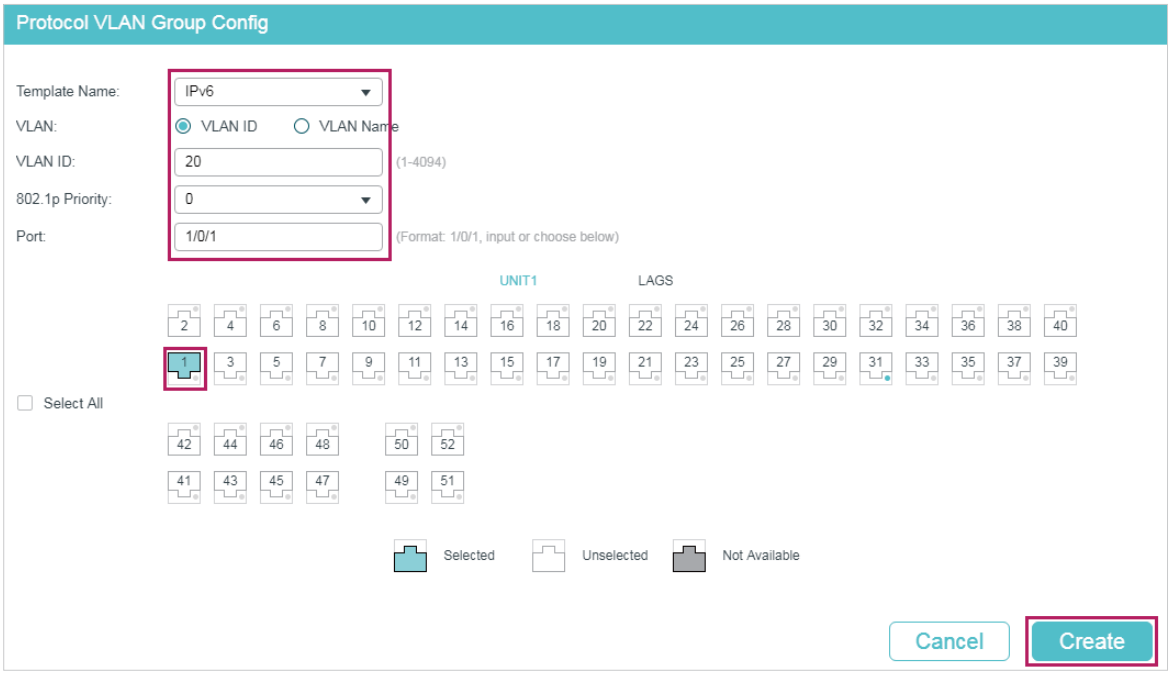


Figure 3-9 Configure the IPv6 Protocol Group



6) Click Save 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) Add untagged port 1/0/1 to VLAN 10. Add untagged port 1/0/2 to VLAN 20. Add untagged port 1/0/3 to both VLAN10 and VLAN 20.

Switch_1(config)#interface gigabitEthernet 1/0/1

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 general allowed vlan 20 untagged

Switch_1(config-if)#exit

Switch_1(config)#interface gigabitEthernet 1/0/3

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) Add tagged port 1/0/1 to both VLAN 10 and VLAN 20. Specify the PVID of untagged port 1/0/2 as 10 and add it to VLAN 10. Specify the PVID of untagged port 1/0/3 as 20 and add it to VLAN 20.

Switch_2(config)#interface gigabitEthernet 1/0/1

```
Switch_2(config-if)#switchport general allowed vlan 10,20 tagged
Switch_2(config-if)#exit
Switch_2(config)#interface gigabitEthernet 1/0/2
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
```

3) 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
```

4) Configure the protocol groups.

```
Switch_2(config)#protocol-vlan vlan 10 priority 0 template 1
Switch_2(config)#protocol-vlan vlan 20 priority 0 template 6
```

5) 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
                                   ......
                                   Gi1/0/49, Gi1/0/50, Gi1/0/51, Gi1/0/52
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
                                   ......
                                   Gi1/0/49, Gi1/0/50, Gi1/0/51, Gi1/0/52
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     Priority    Member
--------  --------------------  ------  ------    -----------
 1       IP                   10      0           Gi1/0/1
 2       IPv6                 20      0           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 9

Configuring GVRP

CHAPTERS

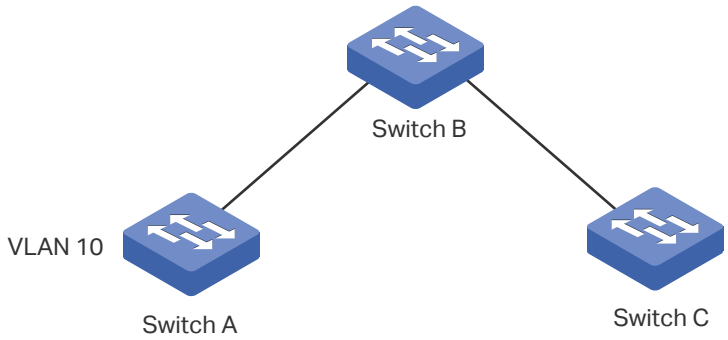
1. Overview
2. GVRP Configuration
3. Configuration Example
4. Appendix: Default Parameters

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.

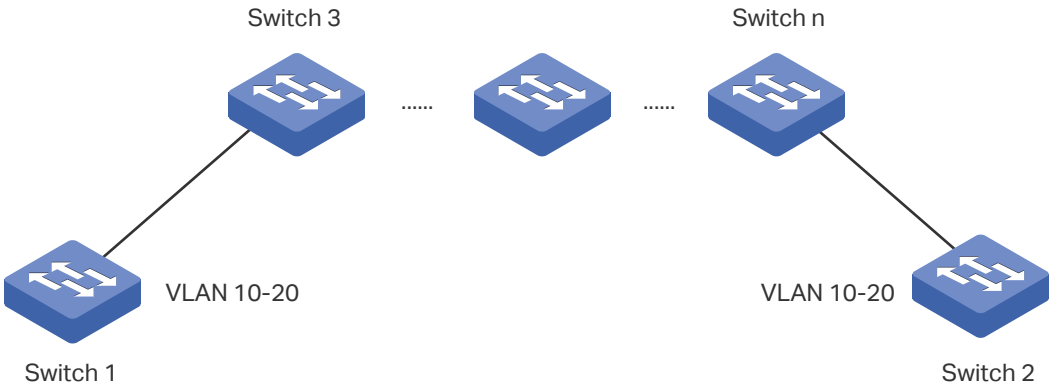
Without GVRP operating, configuring the same VLAN on a network would require manual configuration on each device. As shown in Figure 1-1, Switch A, B and C are connected through trunk ports. VLAN 10 is configured on Switch A, and VLAN 1 is configured on Switch B and Switch C. Switch C can receive messages 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 used 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.
2) Enable GVRP globally.
3) Enable GVRP on each port and configure the corresponding parameters.

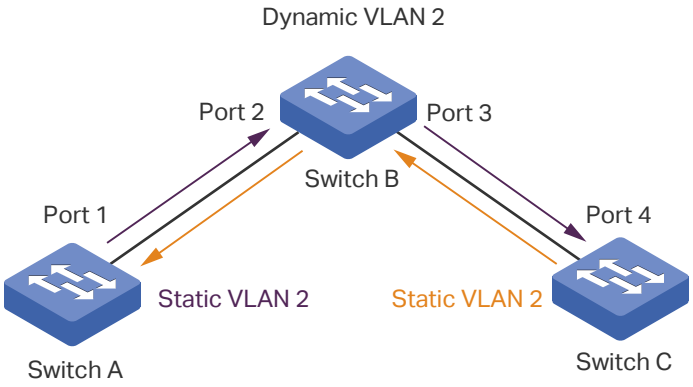
Configuration Guidelines

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

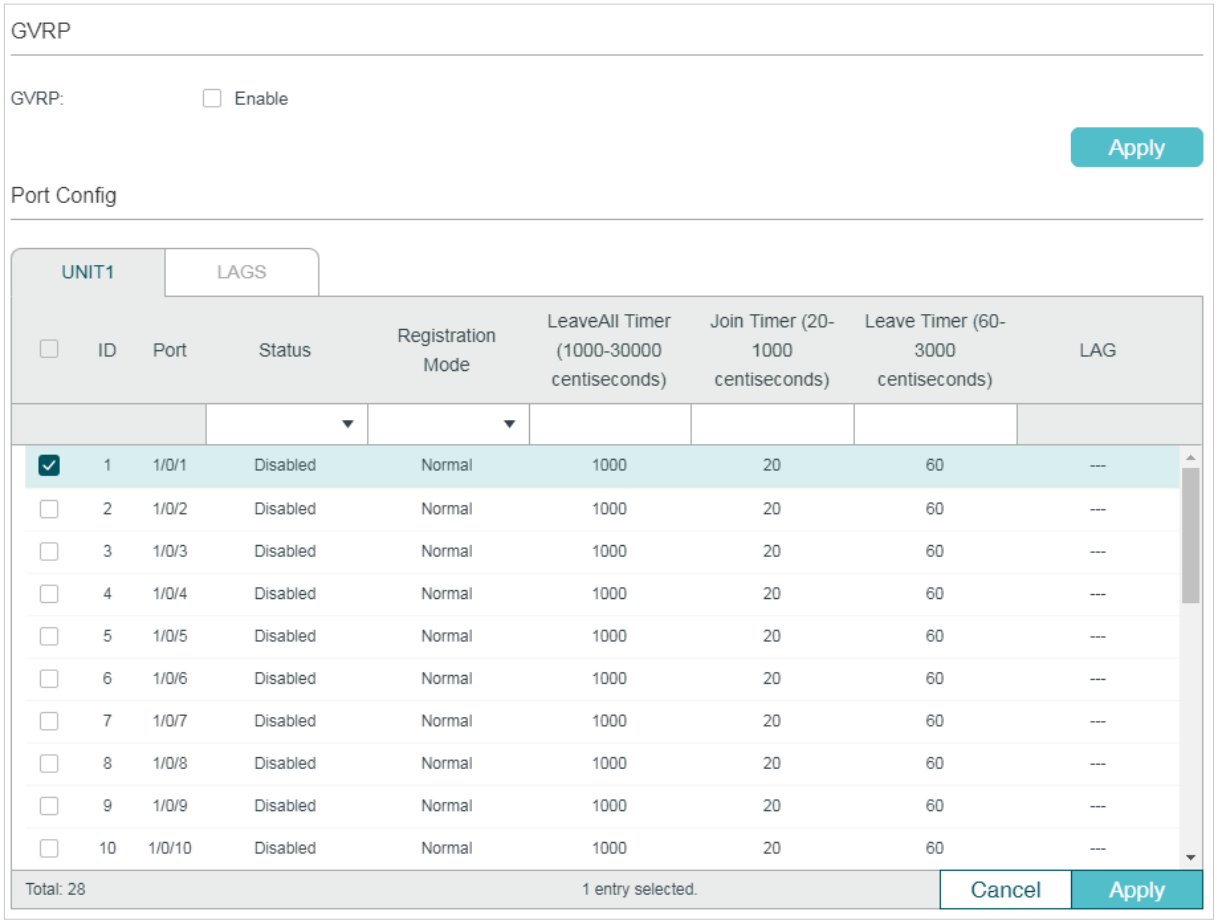


Similarly, if you want to delete a VLAN from the link, two-way deregistration is required. And you need to manually delete the static VALN on both ends of the link.

2.1 Using the GUI

Choose the menu **L2 FEATURES > VLAN > GVRP > GVRP Config** to load the following page.

Figure 2-1 GVRP Config



Follow these steps to configure GVRP:

1) In the **GVRP** 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.
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 will be started. When the LeaveAll timer expires, the GARP participant will send 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 and should be an integral multiple of 5. The default value is 1000 centiseconds.
Join Timer (centisecond)	Join timer controls the sending of Join messages. A GVRP participant starts the Join timer after sending the first Join message. If the participant does not receive any response, it will send the second Join message when the Join timer expires to ensures that the Join message can be sent to other participants. The timer ranges from 20 to 1000 centiseconds and should be an integral multiple of 5. The default value is 20 centiseconds.
Leave Timer (centisecond)	The Leave timer controls attribute deregistration. A participant will send a Leave message if it wants other participants to deregister some of its attributes. 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 timer ranges from 60 to 3000 centiseconds and should be an integral multiple of 5. The default value 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 and not its own. The configurations of the port can take effect only after it leaves the LAG.
- The egress rule of the ports dynamically added to the VLAN is tagged.
- The egress rule of the fixed port should be tagged.
- 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

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* **| 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	**gvrp** Enable GVRP on the port.
Step 5	**gvrp registration** { normal | fixed | forbidden } Configure the GVRP registration mode for the port. By default, it is normal. normal: In this mode, the port can dynamically register and deregister VLANs, and transmit both dynamic and static VLAN registration information. fixed: n 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.
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 will be started. When the LeaveAll timer expires, the GARP participant will send LeaveAll messages to request other GARP participants to re-register all its attributes. After that, the participant restarts the LeaveAll timer. join: Join timer controls the sending of Join messages. A GVRP participant starts the Join timer after sending the first Join message. If the participant does not receive any response, it will send the second Join message when the Join timer expires to ensures that the Join message can be sent to other participants. leave: The Leave timer controls attribute deregistration. A participant will send a Leave message if it wants other participants to deregister some of its attributes. 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. It should be an integral multiple of 5. For LeaveAll timer, the valid values are from 1000 to 30000 centiseconds and the default value is 1000 centiseconds. For Join timer, the valid values are from 20 to 1000 centiseconds and the default value is 20 centiseconds. For Leave timer, the valid values are from 60 to 3000 centiseconds and the default value is 60 centiseconds.
Step 7	**show gvrp global** Verify the global configurations of GVRP.
Step 8	**show gvrp interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-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 and not its own. The configurations of the port can take effect only after it leaves the LAG.
- The egress rule of the ports dynamically added to the VLAN is tagged.
- The egress rule of the fixed port should be tagged.
- 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 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

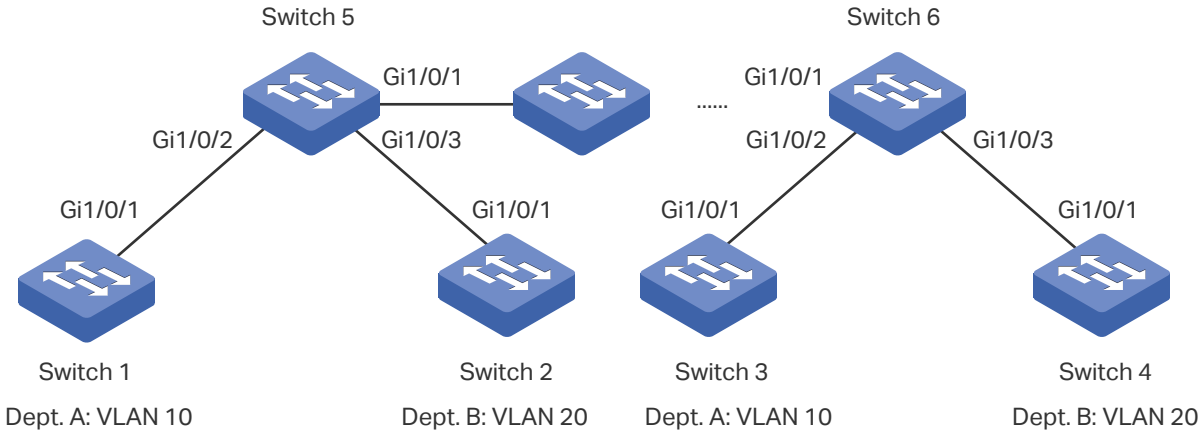
Switch#copy running-config startup-config

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:

- 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 deregistration of VLANs.

Demonstrated with T1600G-52TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

3.3 Using the GUI

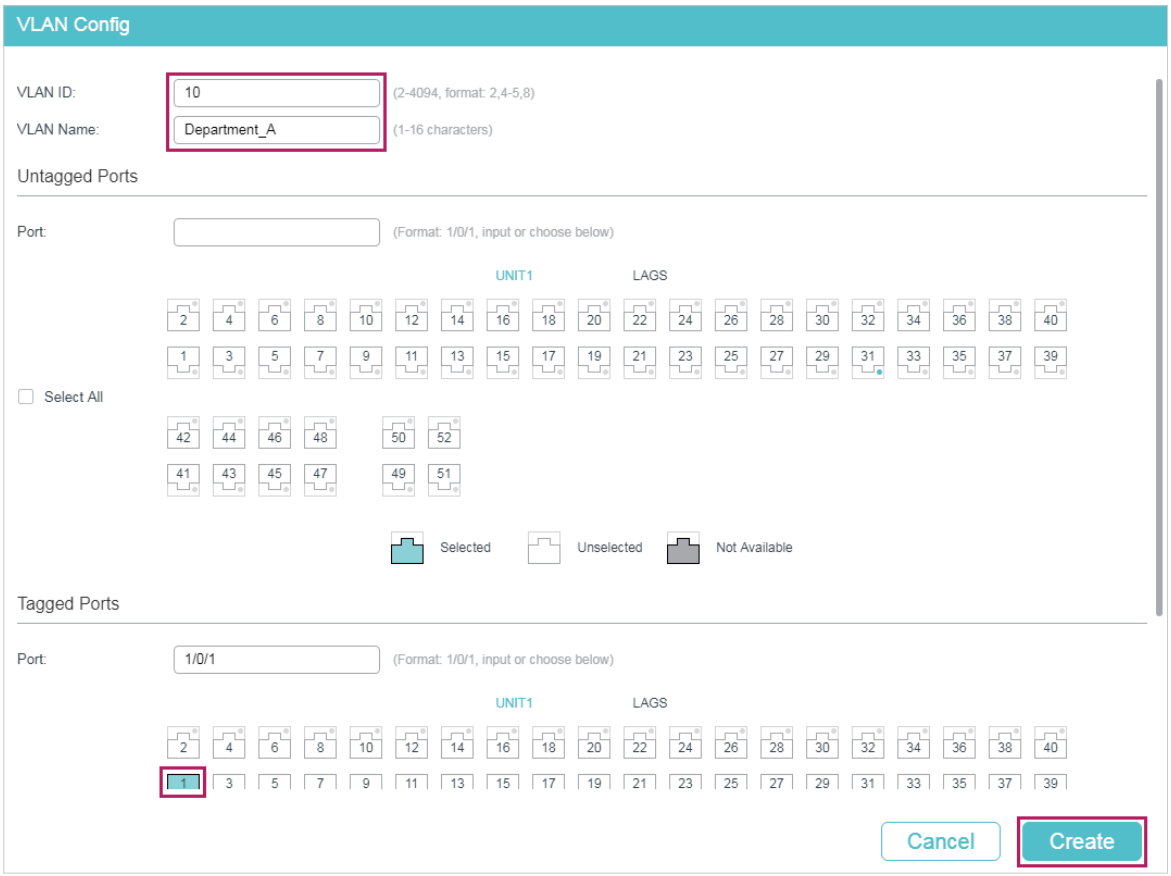
GVRP configuration for Switch 3 is the same as Switch 1, and Switch 4 the same as Switch 2. Other switches share similar configurations.

The following configuration procedures take Switch 1, Switch 2 and Switch 5 as example.

- Configurations for Switch 1

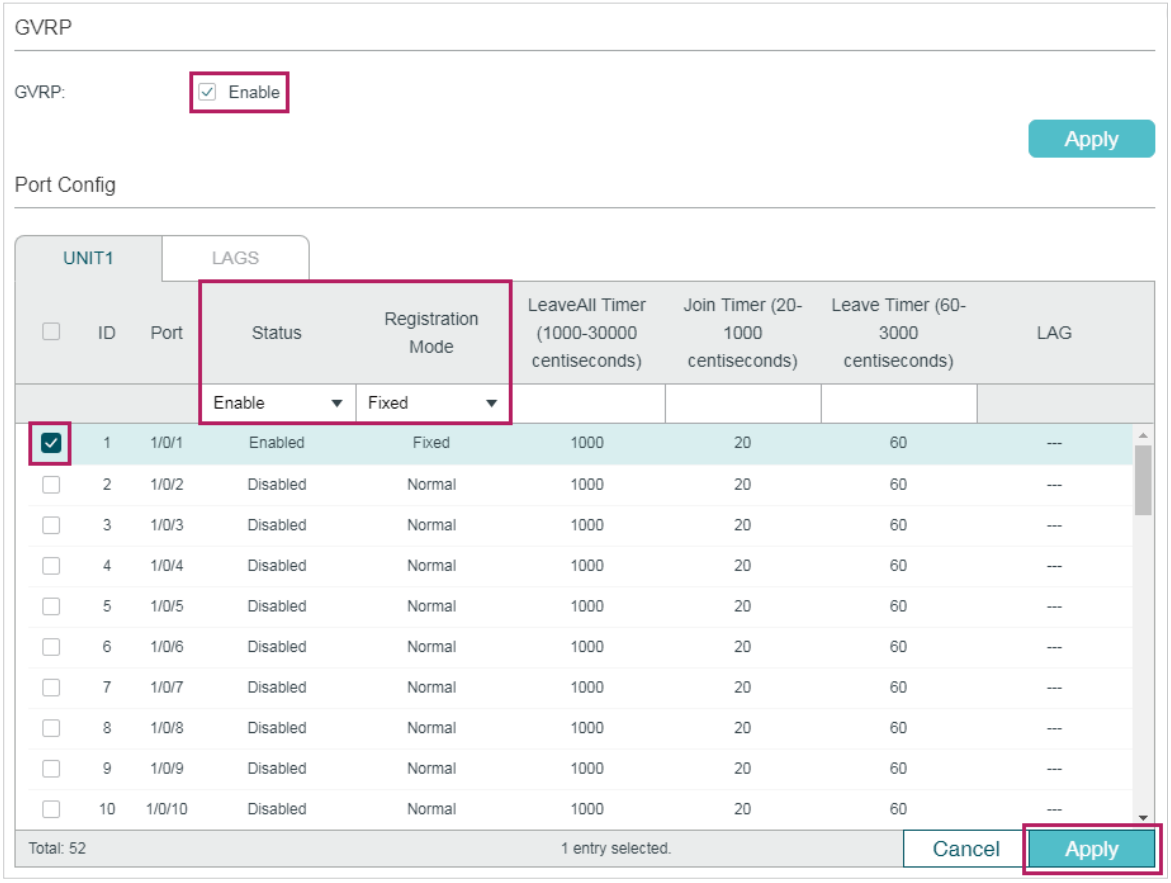
1) Choose the menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** and click Add to load the following page. Create VLAN 10 and add tagged port 1/0/1 to it. Click **Create**.

Figure 3-2 Create VLAN 10



2) Choose the menu **L2 FEATURES > VLAN > GVRP** 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 3-3 GVRP Configuration

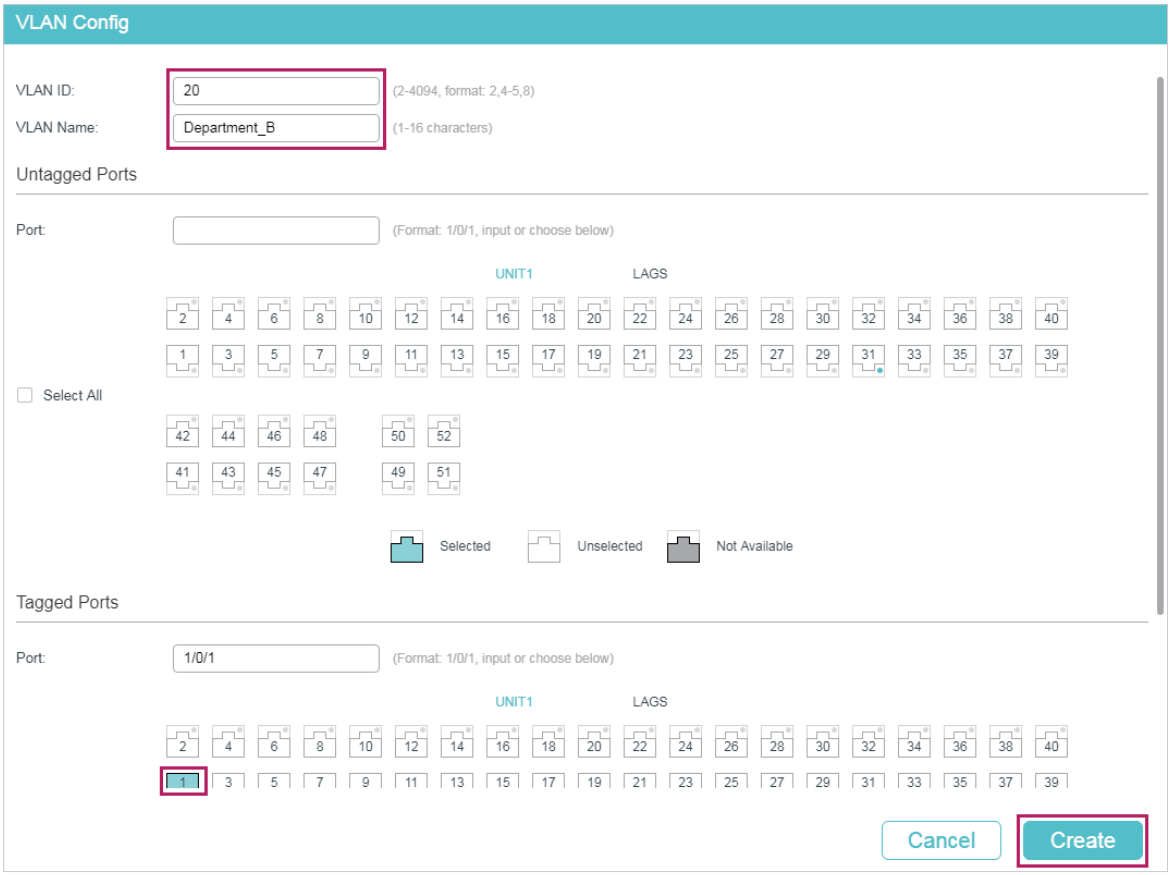


3) Click Save to save the settings.

Configurations for Switch 2

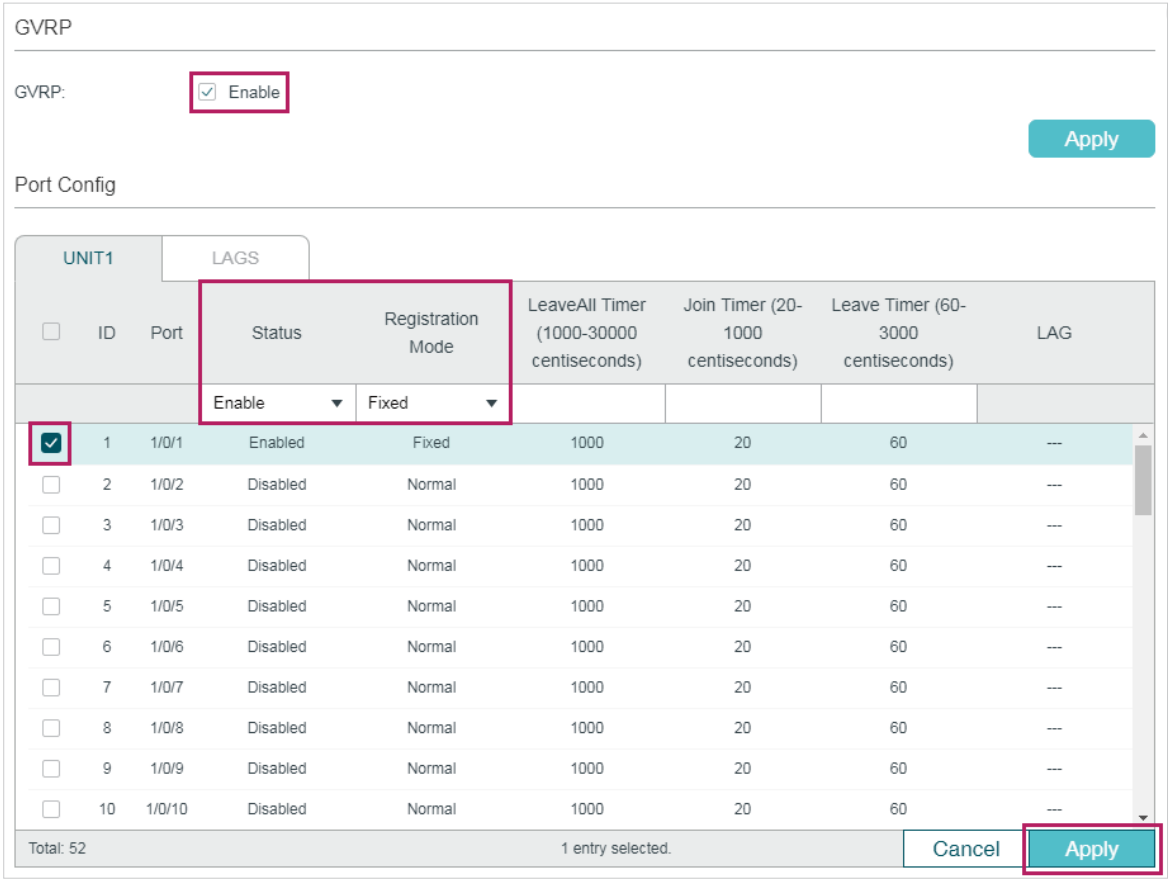
1) Choose the menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** and click Add to load the following page. Create VLAN 20 and add tagged port 1/0/1 to it. Click **Create**.

Figure 3-4 Create VLAN 20



2) Choose the menu **L2 FEATURES > VLAN > GVRP** 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 3-5 GVRP Configuration

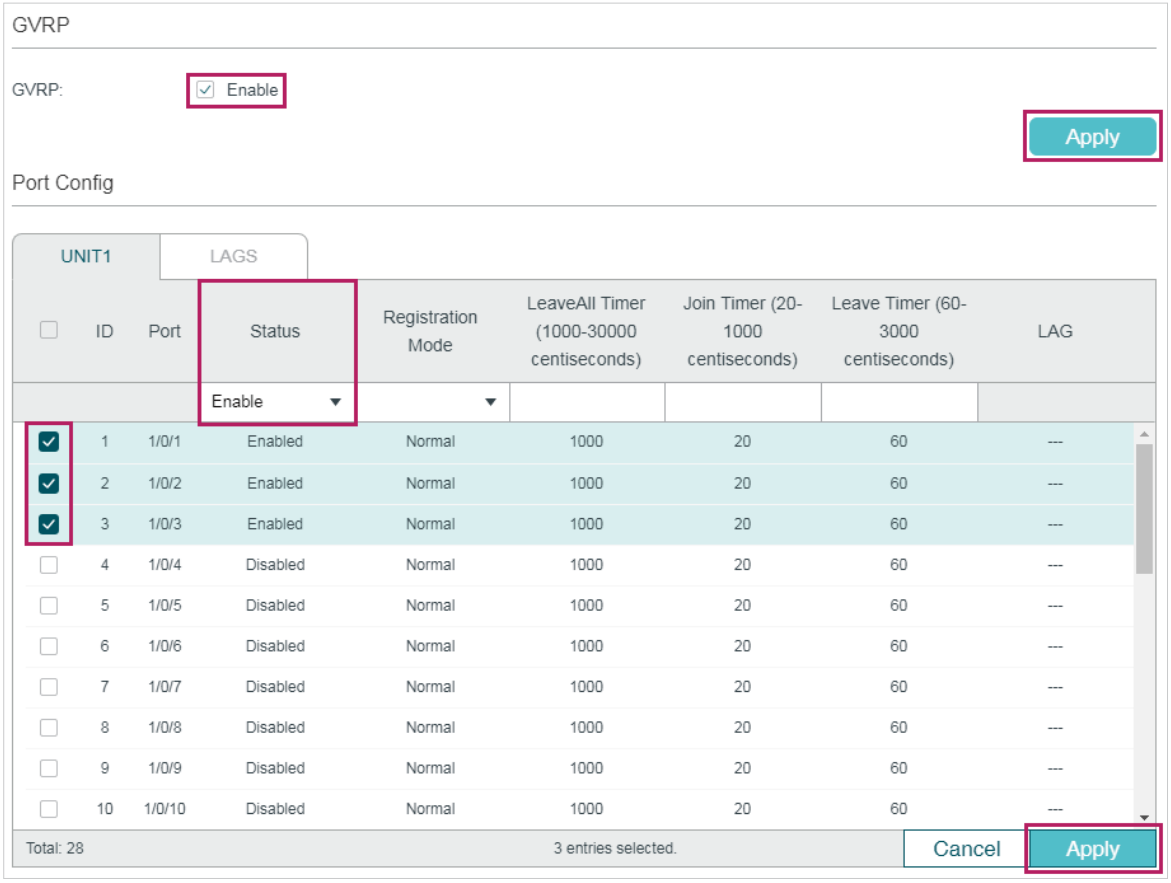


3) Click Save to save the settings.

Configurations for Switch 5

1) Choose the menu **L2 FEATURES > VLAN > GVRP** 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 3-6 GVRP Configuration



2) Click Save 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) Add tagged port 1/0/1 to VLAN 10. Enable GVRP on port and set the registration mode as Fixed.

Switch_1(config)#interface gigabitEthernet 1/0/1

Switch_1(config-if)#switchport general allowed vlan 10 tagged

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) Add tagged port 1/0/1 to VLAN 20. Enable GVRP on the port and set the registration mode as Fixed.

Switch_2(config)#interface gigabitEthernet 1/0/1

Switch_2(config-if)#switchport general allowed vlan 20 tagged

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) Enable GVRP on ports 1/0/1-3.

Switch_5(config)#interface range gigabitEthernet 1/0/1-3

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	Disabled
Port Config	
Status	Disabled
Registration Mode	Normal
LeaveAll Timer	1000 centiseconds
Join Timer	20 centiseconds
Leave Timer	60 centiseconds

Part 10

Configuring Layer 2 Multicast

CHAPTERS

1. Layer 2 Multicast
2. IGMP Snooping Configuration
3. MLD Snooping Configuration
4. MVR Configuration
5. Multicast Filtering Configuration
6. Viewing Multicast Snooping Information
7. Configuration Examples
8. 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.

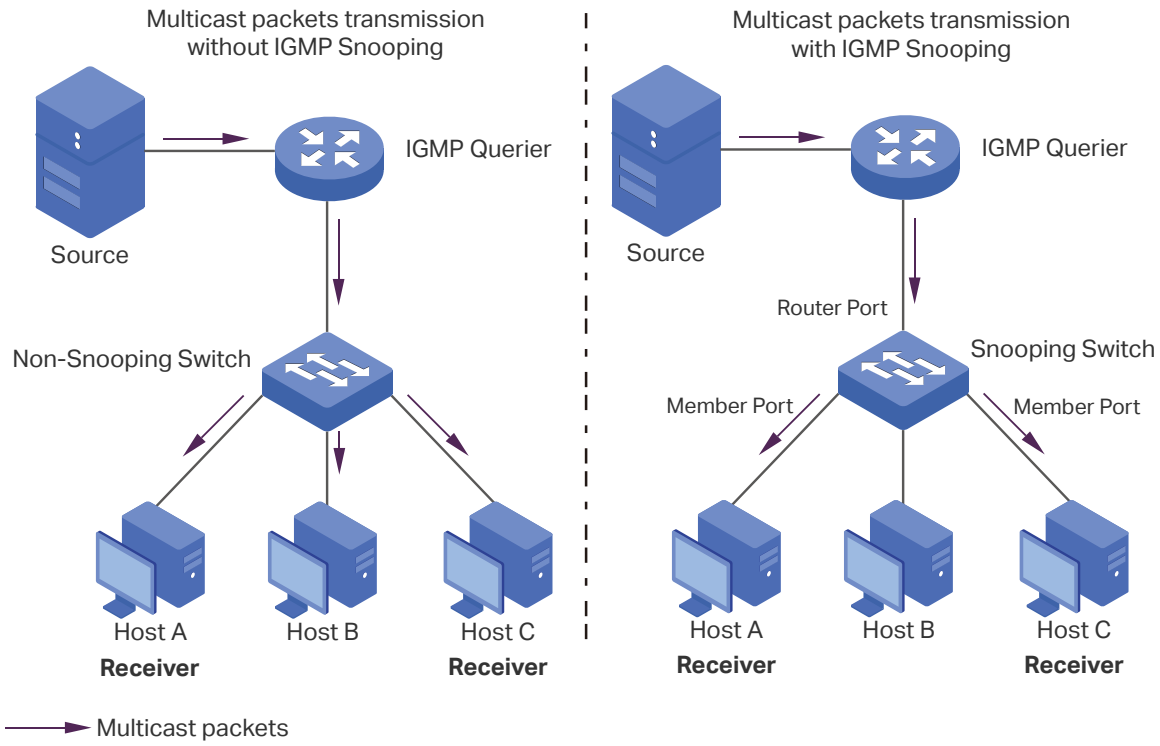
In practical applications, Internet information provider can provide value-added services such as Online Live, IPTV, Distance Education, Telemedicine, Internet Radio and Real-time Video Conferences more conveniently using multicast.

Layer 2 Multicast allows Layer 2 switches to listen for IGMP (Internet Group Management Protocol) packets between IGMP Querier 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 Layer 2 network.

Demonstrated as below:

Figure 1-1 IGMP Snooping



The following basic concepts of IGMP Snooping will be introduced: IGMP querier, snooping switch, router port and member port.

IGMP Querier

An IGMP querier is a multicast router (a router or a Layer 3 switch) that sends query messages to maintain a list of multicast group memberships for each attached network, and a timer for each membership.

Normally only one device acts as querier per physical network. If there are more than one multicast router in the network, a querier election process will be implemented to determine which one acts as the querier.

Snooping Switch

A snooping switch indicates a switch with IGMP Snooping enabled. The switch maintains a multicast forwarding table by snooping on the IGMP transmissions between the host and the querier. With the multicast forwarding table, the switch can forward multicast data only to the ports that are in the corresponding multicast group, so as to constrain the flooding of multicast data in the Layer 2 network.

Router Port

A router port is a port on snooping switch that is connecting to the IGMP querier.

Member Port

A member port is a port on snooping switch that is connecting to the host.

1.2 Supported Features

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 the IGMP querier and the 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 MLD packets between the MLD querier and the users, to build and maintain Layer 2 multicast forwarding table.

Multicast VLAN Registration (MVR)

MVR allows a single multicast VLAN to be shared for multicast member ports in different VLANs in IPv4 network. In IGMP Snooping, if member ports are in different VLANs, a copy of the multicast streams is sent to each VLAN that has member ports. While MVR provides a dedicated multicast VLAN to forward multicast traffic over the Layer 2 network, to avoid duplication of multicast streams for clients in different VLANs. Clients can dynamically join or leave the multicast VLAN without interfering with their relationships in other VLANs.

There are two types of MVR modes:

- Compatible Mode

In compatible mode, the MVR switch does not forward report or leave messages from the hosts to the IGMP querier. So the IGMP querier cannot learn the multicast groups membership information from the MVR switch. You have to statically configure the IGMP querier to transmit all the required multicast streams to the MVR switch via the multicast VLAN.

- Dynamic Mode

In dynamic mode, after receiving report or leave messages from the hosts, the MVR switch will forward them to the IGMP querier via the multicast VLAN (with appropriate translation of the VLAN ID). So the IGMP querier can learn the multicast groups membership information through the report and leave messages, and transmit the multicast streams to the MVR switch via the multicast VLAN according to the multicast forwarding table.

Multicast Filtering

Multicast Filtering allows you to control the set of multicast groups to which a host can belong. You can filter multicast joins on a per-port basis by configuring IP multicast profiles (IGMP profiles or MLD profiles) and associating them with individual switch ports.

2 IGMP Snooping Configuration

To complete IGMP Snooping configuration, follow these steps:

1) Enable IGMP Snooping globally and configure the global parameters.
2) Configure IGMP Snooping for VLANs.
3) Configure IGMP Snooping for ports.
4) (Optional) Configure hosts to statically join a group.

Note:

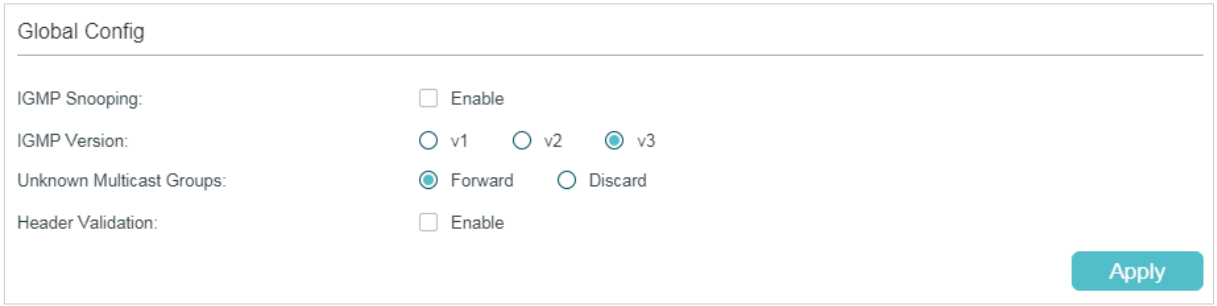
IGMP Snooping takes effect only when it is enabled globally, in the corresponding VLAN and port at the same time.

2.1 Using the GUI

2.1.1 Configuring IGMP Snooping Globally

Choose the menu **L2 FEATURES > Multicast > IGMP Snooping > Global Config** to load the following page.

Figure 2-1 Configure IGMP Snooping Globally



Follow these steps to configure IGMP Snooping globally:

1) In the **Global Config** section, enable IGMP Snooping globally and configure the global parameters.

IGMP Snooping	Enable or disable IGMP Snooping globally.

IGMP Version	Specify the IGMP version. **v1**: The switch works as an IGMPv1 Snooping switch. It can only process IGMPv1 messages from the host. Messages of other versions are ignored. **v2**: The switch works as an IGMPv2 Snooping switch. It can process both IGMPv1 and IGMPv2 messages from the host. IGMPv3 messages are ignored. **v3**: The switch works as an IGMPv3 Snooping switch. It can process IGMPv1, IGMPv2 and IGMPv3 messages from the host.
Unknown Multicast Groups	Set the way in which the switch processes data that are sent to unknown multicast groups as Forward or Discard. By default, it is Forward. Unknown multicast groups are multicast groups that do not match any of the groups announced in earlier IGMP membership reports, and thus cannot be found in the multicast forwarding table of the switch. *Note:* IGMP Snooping and MLD Snooping share the setting of Unknown Multicast Groups, so you have to enable MLD Snooping globally on the **L2 FEATURES > Multicast > MLD Snooping > Global Config** page at the same time.
Header Validation	Enable or disable Header Validation. By default, it is disabled. Generally, for IGMP packets, the TTL value should be 1, ToS field should be 0xC0, and Router Alert option should be 0x94040000. The fields to be validated depend on the IGMP version being used. IGMPv1 only checks the TTL field. IGMPv2 checks the TTL field and the Router Alert option. IGMPv3 checks TTL field, ToS field and Router Alert option. Packets that fail the validation process will be dropped.

2) Click **Apply**.

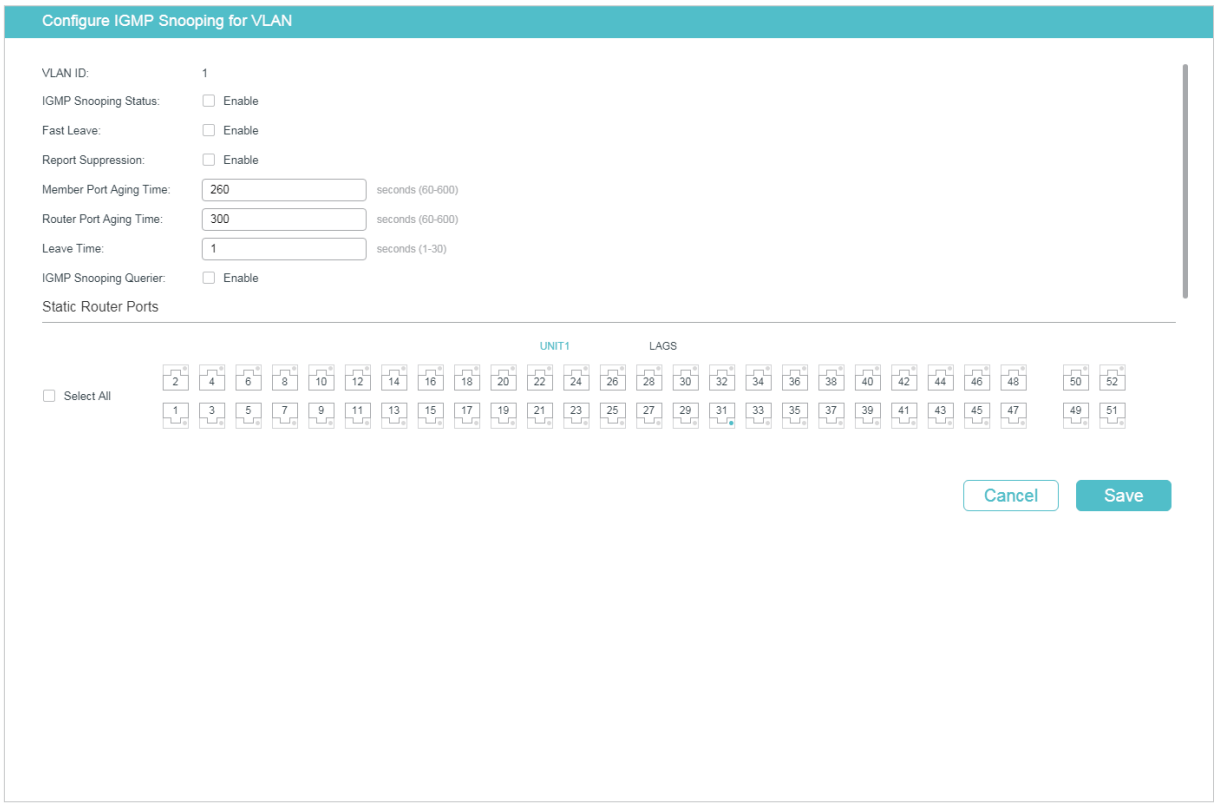
2.1.2 Configuring IGMP Snooping for VLANs

Before configuring IGMP Snooping for VLANs, set up the VLANs that the router ports and the member ports are in. For details, please refer to *Configuring 802.1Q VLAN*.

The switch supports configuring IGMP Snooping on a per-VLAN basis. After IGMP Snooping is enabled globally, you also need to enable IGMP Snooping and configure the corresponding parameters for the VLANs that the router ports and the member ports are in.

Choose the menu **L2 FEATURES > Multicast > IGMP Snooping > Global Config,** and click in your desired VLAN entry in the **IGMP VLAN Config** section to load the following page.

Figure 2-2 Configure IGMP Snooping for VLAN



Follow these steps to configure IGMP Snooping for a specific VLAN:

1) Enable IGMP Snooping for the VLAN, and configure the corresponding parameters.

VLAN ID	Displays the VLAN ID.
IGMP Snooping	Enable or disable IGMP Snooping for the VLAN.

Fast Leave	Enable or disable Fast Leave for the VLAN. IGMPv1 does not support Fast Leave. Without Fast Leave, after a receiver sends an IGMP leave message to leave a multicast group, the switch will forward the leave message to the Layer 3 device (the querier). From the point of view of the querier, the port connecting to the switch is a member port of the corresponding multicast group. After receiving the leave message from the switch, the querier will send out a configured number (Last Member Query Count) of group-specific queries on that port with a configured interval (Last Member Query Interval), and wait for IGMP group membership reports. If there are other receivers connecting to the switch, they will response to the queries before the Last Member Query Interval expires. If no reports are received after the response time of the last query expires, the querier will remove the port from the forwarding list of the corresponding multicast group. That is, if there are other receivers connecting to the switch, the one sent leave message have to wait until the port ages out from the switch's forwarding list of the corresponding multicast group (the maximum waiting time is decided by the Member Port Aging Time). With Fast Leave enabled on a VLAN, the switch will remove the (Multicast Group, Port, VLAN) entry from the multicast forwarding table before forwarding the leave message to the querier. This helps to reduce bandwidth waste since the switch no longer sends the corresponding multicast streams to the VLAN of the port as soon as the port receives a leave message from the VLAN.
Report Suppression	Enable or disable Report Suppression for the VLAN. When enabled, the switch will only forward the first IGMP report message for each multicast group to the IGMP querier and suppress subsequent IGMP report messages for the same multicast group during one query interval. This feature prevents duplicate report messages from being sent to the IGMP querier.
Member Port Aging Time	Specify the aging time of the member ports in the VLAN. Once the switch receives an IGMP membership report message from a port, the switch adds this port to the member port list of the corresponding multicast group. Member ports that are learned in this way are called dynamic member ports. If the switch does not receive any IGMP membership report messages for a specific multicast group from a dynamic member port, it will no longer consider this port as a member port of this multicast group and delete it from the multicast forwarding table.
Router Port Aging Time	Specify the aging time of the router ports in the VLAN. Once the switch receives an IGMP general query message from a port, the switch adds this port to the router port list. Router ports that are learned in this way are called dynamic router ports. If the switch does not receive any IGMP general query message from a dynamic router port within the router port aging time, the switch will no longer consider this port as a router port and delete it from the router port list.

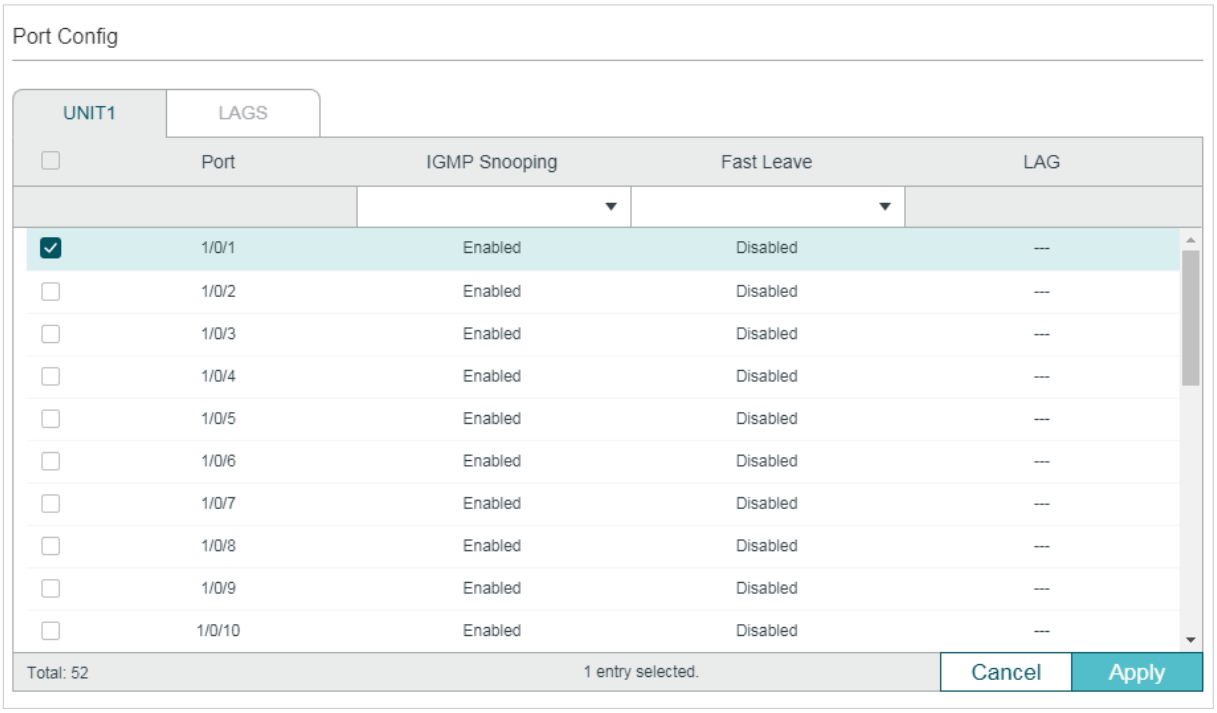
Leave Time	Specify the leave time for the VLAN. When the switch receives a leave message from a port to leave a multicast group, it will wait for a leave time before removing the port from the multicast group. During the period, if the switch receives any report messages from the port, the port will not be removed from the multicast group. Exceptions are as follows: • If the member port ages out before the Leave Time ends and no report messages are received, the port will be removed from the multicast group once its Member Port Aging Time ends. • The Leave Time mechanism will not take effect when Fast Leave takes effect. A proper leave time value can avoid other hosts connecting to the same port of the switch being mistakenly removed from the multicast group when only some of them want to leave.
IGMP Snooping Querier	Enable or disable the IGMP Snooping Querier for the VLAN. When enabled, the switch acts as an IGMP Snooping Querier for the hosts in this VLAN. A querier periodically sends a general query on the network to solicit membership information, and sends group-specific queries when it receives leave messages from hosts.
Query Interval	With IGMP Snooping Querier enabled, specify the interval between general query messages sent by the switch.
Maximum Response Time	With IGMP Snooping Querier enabled, specify the host's maximum response time to general query messages.
Last Member Query Interval	With IGMP Snooping Querier enabled, when the switch receives an IGMP leave message, it obtains the address of the multicast group that the host wants to leave from the message. Then the switch sends out group-specific queries to this multicast group through the port receiving the leave message. This parameter determines the interval between group-specific queries.
Last Member Query Count	With IGMP Snooping Querier enabled, specify the number of group-specific queries to be sent. If specified count of group-specific queries are sent and no report message is received, the switch will delete the multicast address from the multicast forwarding table.
General Query Source IP	With IGMP Snooping Querier enabled, specify the source IP address of the general query messages sent by the switch. It should be a unicast address.
Static Router Ports	Select one or more ports to be the static router ports in the VLAN. Static router ports do not age. Multicast streams and IGMP packets to all groups in this VLAN will be forwarded through the static router ports. Multicast streams and IGMP packets to the groups that have dynamic router ports will be also forwarded through the corresponding dynamic router ports.
Forbidden Router Ports	Select ports to forbid them from being router ports in the VLAN.

2) Click **Save**.

2.1.3 Configuring IGMP Snooping for Ports

Choose the menu **L2 FEATURES > Multicast > IGMP Snooping > Port Config** to load the following page.

Figure 2-3 Configure IGMP Snooping for Ports



Follow these steps to configure IGMP Snooping for ports:

1) Enable IGMP Snooping for the port and enable Fast Leave if there is only one receiver connected to the port.

IGMP Snooping	Enable or disable IGMP Snooping for the port.
Fast Leave	Enable or disable Fast Leave for the port. IGMPv1 does not support fast leave. Fast Leave can be enabled on a per-port basis or per-VLAN basis. When enabled on a per-port basis, the switch will remove the port from the corresponding multicast group of all VLANs before forwarding the leave message to the querier. You should only use Fast Leave for a port when there is a single receiver connected to the port. For more details about Fast Leave, see *2.1.2 Configuring IGMP Snooping for VLANs*.
LAG	Displays the LAG the port belongs to.

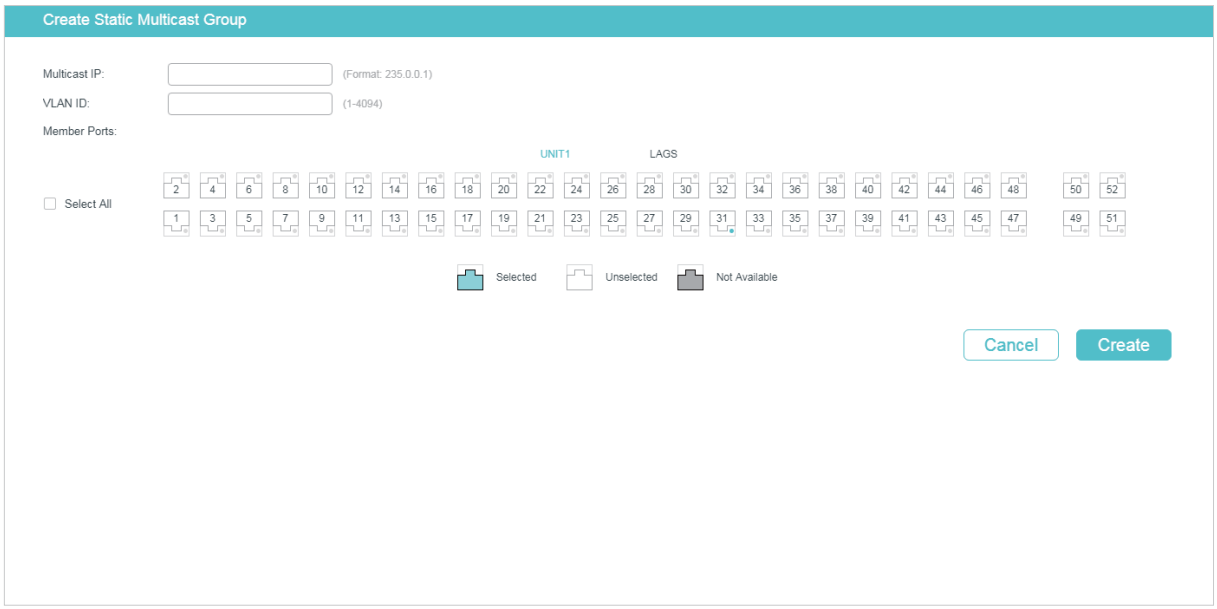
2) Click **Apply**.

2.1.4 Configuring Hosts to Statically Join a Group

Hosts or Layer 2 ports normally join multicast groups dynamically, but you can also configure hosts to statically join a group.

Choose the menu **L2 FEATURES > Multicast > IGMP Snooping > Static Group Config** and click Add to load the following page.

Figure 2-4 Configure Hosts to Statically Join a Group



Follow these steps to configure hosts to statically join a group:

1) Specify the multicast IP address, VLAN ID. Select the ports to be the static member ports of the multicast group.

Multicast IP	Specify the address of the multicast group that the hosts need to join.
VLAN ID	Specify the VLAN that the hosts are in.
Member Ports	Select the ports that the hosts are connected to. These ports will become the static member ports of the multicast group and will never age.

2) Click **Create**.

2.2 Using the CLI

2.2.1 Configuring IGMP Snooping Globally

Follow these steps to configure IGMP Snooping globally:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip igmp snooping** Enable IGMP Snooping Globally.

Step 3	**ip igmp snooping version {**v1 | v2 | v3**}** Configure the IGMP version. v1:The switch works as an IGMPv1 Snooping switch. It can only process IGMPv1 report messages from the host. Report messages of other versions are ignored. v2: The switch works as an IGMPv2 Snooping switch. It can process both IGMPv1 and IGMPv2 report messages from the host. IGMPv3 report messages are ignored. v3: The switch works as an IGMPv3 Snooping switch. It can process IGMPv1, IGMPv2 and IGMPv3 report messages from the host.
Step 4	**ip igmp snooping drop-unknown** (Optional) Configure the way how the switch processes multicast streams that are sent to unknown multicast groups as Discard. By default, it is Forward. Unknown multicast groups are multicast groups that do not match any of the groups announced in earlier IGMP membership reports, and thus cannot be found in the multicast forwarding table of the switch. *Note:* IGMP Snooping and MLD Snooping share the setting of Unknown Multicast Groups, you need to ensure MLD Snooping is enabled globally. To enable MLD Snooping globally, use the **ipv6 mld snooping** command in global configuration mode.
Step 5	**ip igmp snooping header-validation** (Optional) Enable header validation. Generally, for IGMP packets, the TTL value should be 1, ToS field should be 0xC0, and Router Alert option should be 0x94040000. The fields validated depend on the IGMP version being used. IGMPv1 only checks the TTL field. IGMPv2 checks the TTL field and the Router Alert option. IGMPv3 checks TTL field, ToS field and Router Alert option. Packets that fail the validation process will be dropped.
Step 6	**show ip igmp snooping** Show the basic IGMP Snooping configuration.
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 IGMP Snooping and header validation globally, and specify the IGMP Snooping version as IGMPv3, the way how the switch processes multicast streams that are sent to unknown multicast groups as discard.

Switch#configure

Switch(config)#ip igmp snooping

Switch(config)#ip igmp snooping version v3

Switch(config)#ipv6 mld snooping

Switch(config)#ip igmp snooping drop-unknown

Switch(config)#ip igmp snooping header-validation

Switch(config)#show ip igmp snooping

IGMP Snooping :Enable

IGMP Version :V3

Unknown Multicast :Discard

Header Validation :Enable

...

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Configuring IGMP Snooping for VLANs

Before configuring IGMP Snooping for VLANs, set up the VLANs that the router ports and the member ports are in. For details, please refer to *Configuring 802.1Q VLAN*.

The switch supports configuring IGMP Snooping on a per-VLAN basis. After IGMP Snooping is enabled globally, you also need to enable IGMP Snooping and configure the corresponding parameters for the VLANs that the router ports and the member ports are in.

Follow these steps to configure IGMP Snooping for VLANs:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip igmp snooping vlan-config** *vlan-id-list* **mtime** *member-time* Enable IGMP Snooping for the specified VLANs, and specify the member port aging time for the VLANs. *vlan-id-list:* Specify the ID or the ID list of the VLAN(s). *member-time:* Specify the aging time of the member ports in the specified VLANs. Valid values are from 60 to 600 seconds. By default, it is 260 seconds. Once the switch receives an IGMP membership report message from a port, the switch adds this port to the member port list of the corresponding multicast group. Member ports that are learned in this way are called dynamic member ports. If the switch does not receive any IGMP membership report message for a specific multicast group from a dynamic member port, it will no longer consider this port as a member port of this multicast group and delete it from the multicast forwarding table.

Step 3 **ip igmp snooping vlan-config** *vlan-id-list* **rtime** *router-time*

Specify the router port aging time for the VLANs.

vlan-id-list: Specify the ID or the ID list of the VLAN(s).

router-time: Specify the aging time of the router ports in the specified VLANs. Valid values are from 60 to 600 seconds. By default, it is 300 seconds.

Once the switch receives an IGMP general query message from a port, the switch adds this port to the router port list. Router ports that are learned in this way are called dynamic router ports.

If the switch does not receive any IGMP general query message from a dynamic router port within the router port aging time, the switch will no longer consider this port as a router port and delete it from the router port list.

Step 4 **ip igmp snooping vlan-config** *vlan-id-list* **ltime** *leave-time*

Specify the router port aging time for the VLANs.

vlan-id-list: Specify the ID or the ID list of the VLAN(s).

leave-time: Specify the leave time for the VLAN(s). Valid values are from 1 to 30 in seconds, and the default value is 1 second.

When the switch receives a leave message from a port to leave a multicast group, it will wait for a leave time before removing the port from the multicast group. During the period, if the switch receives any report messages from the port, the port will not be removed from the multicast group. Exceptions are as follows:

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

A proper leave time value can avoid other hosts connecting to the same port of the switch being mistakenly removed from the multicast group when only some of them want to leave.

Step 5 **ip igmp snooping vlan-config** *vlan-id-list* **report-suppression**

(Optional) Enable the Report Suppression for the VLANs. By default, it is disabled.

When enabled, the switch will only forward the first IGMP report message for each multicast group to the IGMP querier and suppress subsequent IGMP report messages for the same multicast group during one query interval. This feature prevents duplicate report messages from being sent to the IGMP querier.

vlan-id-list: Specify the ID or the ID list of the VLAN(s).

Step 6 **ip igmp snooping vlan-config** *vlan-id-list* **immediate-leave**

(Optional) Enable the Fast Leave for the VLANs. By default, it is disabled. IGMPv1 does not support fast leave.

Without Fast Leave, after a receiver sends an IGMP leave message to leave a multicast group, the switch will forward the leave message to the Layer 3 device (the querier).

From the point of view of the querier, the port connecting to the switch is a member port of the corresponding multicast group. After receiving the leave message from the switch, the querier will send out a configured number (Last Member Query Count) of group-specific queries on that port with a configured interval (Last Member Query Interval), and wait for IGMP group membership reports. If there are other receivers connecting to the switch, they will response to the queries before the Last Member Query Interval expires. If no reports are received after the response time of the last query expires, the querier will remove the port from the forwarding list of the corresponding multicast group.

That is, if there are other receivers connecting to the switch, the one sent leave message have to wait until the port ages out from the switch's forwarding list of the corresponding multicast group (the maximum waiting time is decided by the Member Port Aging Time).

With Fast Leave enabled on a VLAN, the switch will remove the (Multicast Group, Port, VLAN) entry from the multicast forwarding table before forwarding the leave message to the querier. This helps to reduce bandwidth waste since the switch no longer sends the corresponding multicast streams to the VLAN of the port as soon as the port receives a leave message from the VLAN.

You should only enable Fast Leave for a VLAN when there is a single receiver belongs to this VLAN on every port of the VLAN.

vlan-id-list: Specify the ID or the ID list of the VLAN(s).

Step 7 **ip igmp snooping vlan-config** *vlan-id-list* **rport interface { fastEthernet** *port-list* **| gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port-list*| **port-channel** *lag-list* **}**

(Optional) Specify the static router ports for the VLANs. Static router ports do not age.

vlan-id-list: Specify the ID or the ID list of the VLAN(s).

port-list: The number or the list of the Ethernet port that need to be configured as static router ports.

lag-list: The ID or the list of the LAG that need to be configured as static router ports.

Step 8 **ip igmp snooping vlan-config** *vlan-id-list* **router-ports-forbidden interface { fastEthernet** *port-list* **| gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port-list*| **port-channel** *lag-list* **}**

(Optional) Specify the ports to forbid them from being router ports in the VLANs.

vlan-id-list: Specify the ID or the ID list of the VLAN(s).

port-list: The number or the list of the Ethernet port that need to be forbidden from being router ports.

lag-list: The ID or the list of the LAG that need to be forbidden from being router ports.

Step 9	**ip igmp snooping vlan-config** *vlan-id-list* **querier** (Optional) Enable the IGMP Snooping Querier for the VLAN. By default, it is disabled. When enabled, the switch acts as an IGMP Snooping Querier for the hosts in this VLAN. A querier periodically sends a general query on the network to solicit membership information, and sends group-specific queries when it receives leave messages from hosts. *vlan-id-list:* Specify the ID or the ID list of the VLAN(s). After enabling IGMP Snooping Querier feature, you need to specify the corresponding parameters including the Last Member Query Count, Last Member Query Interval, Maximum Response Time, Query Interval and General Query Source IP. Use the command below in global configuration mode to configure the parameters: **ip igmp snooping vlan-config** *vlan-id-list* **querier { max-response-time** *response-time* **| query-interval** *interval* **| general-query source-ip** *ip-addr* **| last-member-query-count** *num* **| last-member-query-interval** *interval* **}** *vlan-id-list:* Specify the ID or the ID list of the VLAN(s). *response-time:* Specify the host's maximum response time to general query messages. Valid values are from 1 to 25 seconds, and the default value is 10 seconds. **query-interval** *interval:* Specify the interval between general query messages sent by the switch. Valid values are from 10 to 300 seconds, and the default value is 60 seconds. *ip-addr:* Specify the source IP address of the general query messages sent by the switch. It should be a unicast address. By default, it is 0.0.0.0. *num:* Specify the number of group-specific queries to be sent. With IGMP Snooping Querier enabled, when the switch receives an IGMP leave message, it obtains the address of the multicast group that the host wants to leave from the message. Then the switch sends out group-specific queries to this multicast group through the port receiving the leave message. If specified count of group-specific queries are sent and no report message is received, the switch will delete the multicast address from the multicast forwarding table. Valid values are from 1 to 5, and the default value is 2. **last-member-query-interval** *interval:* Specify the interval between group-specific queries. Valid values are from 1 to 5 seconds, and the default value is 1 second.
Step 10	**show ip igmp snooping vlan** *vlan-id* Show the basic IGMP Snooping configuration in the specified 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 enable IGMP Snooping for VLAN 1, and configure the member port aging time as 300 seconds, the router port aging time as 320 seconds, and then enable Fast Leave and Report Suppression for the VLAN:

Switch#configure

Switch(config)#ip igmp snooping vlan-config 1 **mtime** 300

Switch(config)#ip igmp snooping vlan-config 1 **rtime** 320

Switch(config)#ip igmp snooping vlan-config 1 **immediate-leave**

Switch(config)#ip igmp snooping vlan-config 1 **report-suppression**

Switch(config)#show ip igmp snooping vlan 1

Vlan Id: 1

Vlan IGMP Snooping Status: Enable

Fast Leave: Enable

Report Suppression: Enable

Router Time:320

Member Time: 300

Querier: Disable

...

Switch(config)#end

Switch#copy running-config startup-config

The following example shows how to enable IGMP Snooping querier for VLAN 1, and configure the query interval as 100 seconds, the maximum response time as 15 seconds, the last member query interval as 2 seconds, the last member query count as 3, and the general query source IP as 192.168.0.5:

Switch#configure

Switch(config)#ip igmp snooping vlan-config 1 **querier**

Switch(config)#ip igmp snooping vlan-config 1 **querier query-interval** 100

Switch(config)#ip igmp snooping vlan-config 1 **querier max-response-time** 15

Switch(config)#ip igmp snooping vlan-config 1 **querier last-member-query-interval** 2

Switch(config)#ip igmp snooping vlan-config 1 **querier last-member-query-count** 3

Switch(config)#ip igmp snooping vlan-config 1 **querier general-query source-ip**192.168.0.5

Switch(config)#show ip igmp snooping vlan 1

Vlan Id: 1

...

Querier:

Maximum Response Time: 15

Query Interval: 100

Last Member Query Interval: 2

Last Member Query Count: 3

General Query Source IP: 192.168.0.5

...

Switch(config)#end

Switch#copy running-config startup-config

2.2.3 Configuring IGMP Snooping for Ports

Follow these steps to configure IGMP Snooping 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***| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Enter interface configuration mode**.**
Step 3	**ip igmp snooping** Enable IGMP Snooping for the port. By default, it is enabled.
Step 4	**ip igmp snooping immediate-leave** (Optional) Enable Fast Leave on the specified port. Fast Leave can be enabled on a per-port basis or per-VLAN basis. When enabled on a per-port basis, the switch will remove the port from the corresponding multicast group of all VLANs before forwarding the leave message to the querier. You should only use Fast Leave for a port when there is a single receiver connected to the port. For more details about Fast Leave, see *2.2.2 Configuring IGMP Snooping for VLANs*.
Step 5	**show ip igmp snooping interface [fastEthernet** [*port-list*] | **gigabitEthernet** [*port-list*] **| ten-gigabitEthernet** [*port-list*] **| port-channel** [*port-channel-list*] **] basic-config** Show the basic IGMP Snooping configuration 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 enable IGMP Snooping and fast leave for port 1/0/1-3:

Switch#configure

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

Switch(config-if-range)#ip igmp snooping

Switch(config-if-range)#ip igmp snooping immediate-leave

Switch(config-if-range)#show ip igmp snooping interface gigabitEthernet 1/0/1-3

Port	IGMP-Snooping	Fast-Leave
Gi1/0/1	enable	enable
Gi1/0/2	enable	enable
Gi1/0/3	enable	enable

Switch(config-if-range)#end

Switch#copy running-config startup-config

2.2.4 Configuring Hosts to Statically Join a Group

Hosts or Layer 2 ports normally join multicast groups dynamically, but you can also configure hosts to statically join a group.

Follow these steps to configure hosts to statically join a group:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip igmp snooping vlan-config** *vlan-id-list* **static** *ip* **interface { fastEthernet** *port-list* **| gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port-list*| **port-channel** *lag-list* **}** *vlan-id-list:* Specify the ID or the ID list of the VLAN(s). *ip:* Specify the IP address of the multicast group that the hosts want to join. *port-list* / *lag-list:* Specify the ports that is connected to the hosts. These ports will become static member ports of the group.
Step 3	**show ip igmp 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 port 1/0/1-3 in VLAN 2 to statically join the multicast group 239.1.2.3:

Switch#configure

Switch(config)#ip igmp snooping vlan-config 2 **static** 239.1.2.3 **interface gigabitEthernet** 1/0/1-3

Switch(config)#show ip igmp snooping groups static

Multicast-ip	VLAN-id	Addr-type	Switch-port
----------	-------	---------	----------
239.1.2.3	2	static	Gi1/0/1-3

Switch(config)#end

Switch#copy running-config startup-config

3 MLD Snooping Configuration

To complete MLD Snooping configuration, follow these steps:

1) Enable MLD Snooping globally and configure the global parameters.
2) Configure MLD Snooping for VLANs.
3) Configure MLD Snooping for ports.
4) (Optional) Configure hosts to statically join a group.

Note:

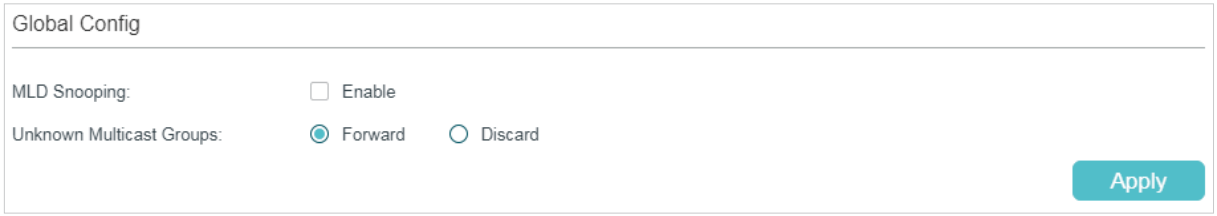
MLD Snooping takes effect only when it is enabled globally, in the corresponding VLAN and port at the same time.

3.1 Using the GUI

3.1.1 Configuring MLD Snooping Globally

Choose the menu **L2 FEATURES > Multicast > MLD Snooping > Global Config** to load the following page.

Figure 3-1 Configure MLD Snooping Globally



Follow these steps to configure MLD Snooping globally:

1) In the **Global Config** section, enable MLD Snooping and configure the Unknown Multicast Groups feature globally.

MLD Snooping	Enable or disable MLD Snooping globally.
Unknown Multicast Groups	Configure the way in which the switch processes data that are sent to unknown multicast groups as Forward or Discard. By default, it is Forward. Unknown multicast groups are multicast groups that do not match any of the groups announced in earlier IGMP membership reports, and thus cannot be found in the multicast forwarding table of the switch. *Note:* IGMP Snooping and MLD Snooping share the setting of Unknown Multicast Groups, so you have to enable IGMP Snooping globally on the **L2 FEATURES > Multicast > IGMP Snooping > Global Config** page at the same time.

2) Click **Apply**.

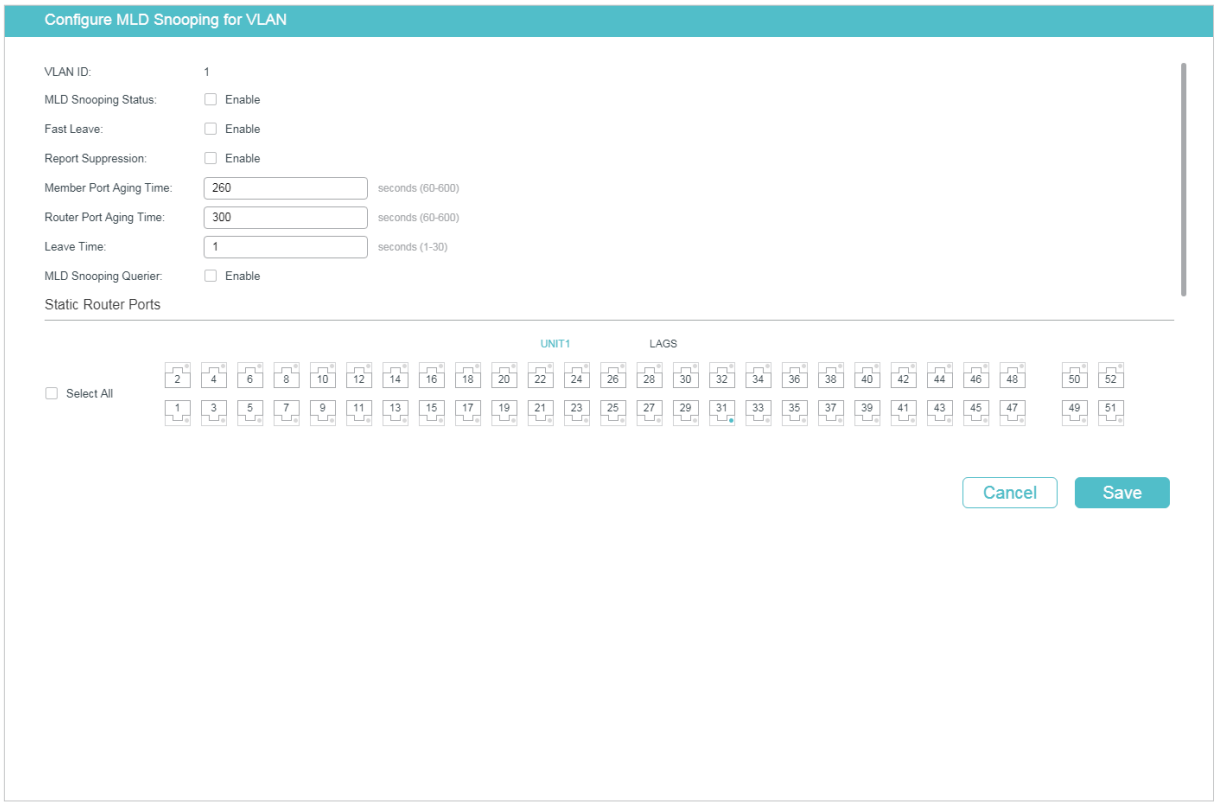
3.1.2 Configuring MLD Snooping for VLANs

Before configuring MLD Snooping for VLANs, set up the VLANs that the router ports and the member ports are in. For details, please refer to *Configuring 802.1Q VLAN*.

The switch supports configuring MLD Snooping on a per-VLAN basis. After MLD Snooping is enabled globally, you also need to enable MLD Snooping and configure the corresponding parameters for the VLANs that the router ports and the member ports are in.

Choose the menu **L2 FEATURES > Multicast > MLD Snooping > Global Config,** and click in your desired VLAN entry in the **MLD VLAN Config** section to load the following page.

Figure 3-2 Configure MLD Snooping for VLAN



Follow these steps to configure MLD Snooping for a specific VLAN:

1) Enable MLD Snooping for the VLAN, and configure the corresponding parameters.

VLAN ID	Displays the VLAN ID.
MLD Snooping	Enable or disable MLD Snooping for the VLAN.

Fast Leave	Enable or disable Fast Leave for the VLAN. Without Fast Leave, after a receiver sends an MLD done message (equivalent to an IGMP leave message) to leave a multicast group, the switch will forward the done message to the Layer 3 device (the querier). From the point of view of the querier, the port connecting to the switch is a member port of the corresponding multicast group. After receiving the done message from the switch, the querier will send out a configured number (Last Listener Query Count) of Multicast-Address-Specific Queries (MASQs) on that port with a configured interval (Last Listener Query Interval), and wait for MLD reports. If there are other receivers connecting to the switch, they will response to the MASQs before the Last Listener Query Interval expires. If no reports are received after the response time of the last query expires, the querier will remove the port from the forwarding list of the corresponding multicast group. That is, if there are other receivers connecting to the switch, the one sent done message have to wait until the port ages out from the switch's forwarding list of the corresponding multicast group (the maximum waiting time is decided by the Member Port Aging Time). With Fast Leave enabled on a VLAN, the switch will remove the (Multicast Group, Port, VLAN) entry from the multicast forwarding table before forwarding the done message to the querier. This helps to reduce bandwidth waste since the switch no longer sends the corresponding multicast streams to the VLAN of the port as soon as the port receives a done message from the VLAN.
Report Suppression	Enable or disable Report Suppression for the VLAN. When enabled, the switch will only forward the first MLD report message for each multicast group to the MLD querier and suppress subsequent MLD report messages for the same multicast group during one query interval. This feature prevents duplicate report messages from being sent to the MLD querier.
Member Port Aging Time	Specify the aging time of the member ports in the VLAN. Once the switch receives an MLD report message from a port, the switch adds this port to the member port list of the corresponding multicast group. Member ports that are learned in this way are called dynamic member ports. If the switch does not receive any MLD report messages for a specific multicast group from a dynamic member port, it will no longer consider this port as a member port of this multicast group and delete it from the multicast forwarding table.
Router Port Aging Time	Specify the aging time of the router ports in the VLAN. Once the switch receives an MLD general query message from a port, the switch adds this port to the router port list. Router ports that are learned in this way are called dynamic router ports. If the switch does not receive any MLD general query messages from a dynamic router port within the router port aging time, the switch will no longer consider this port as a router port and delete it from the router port list.

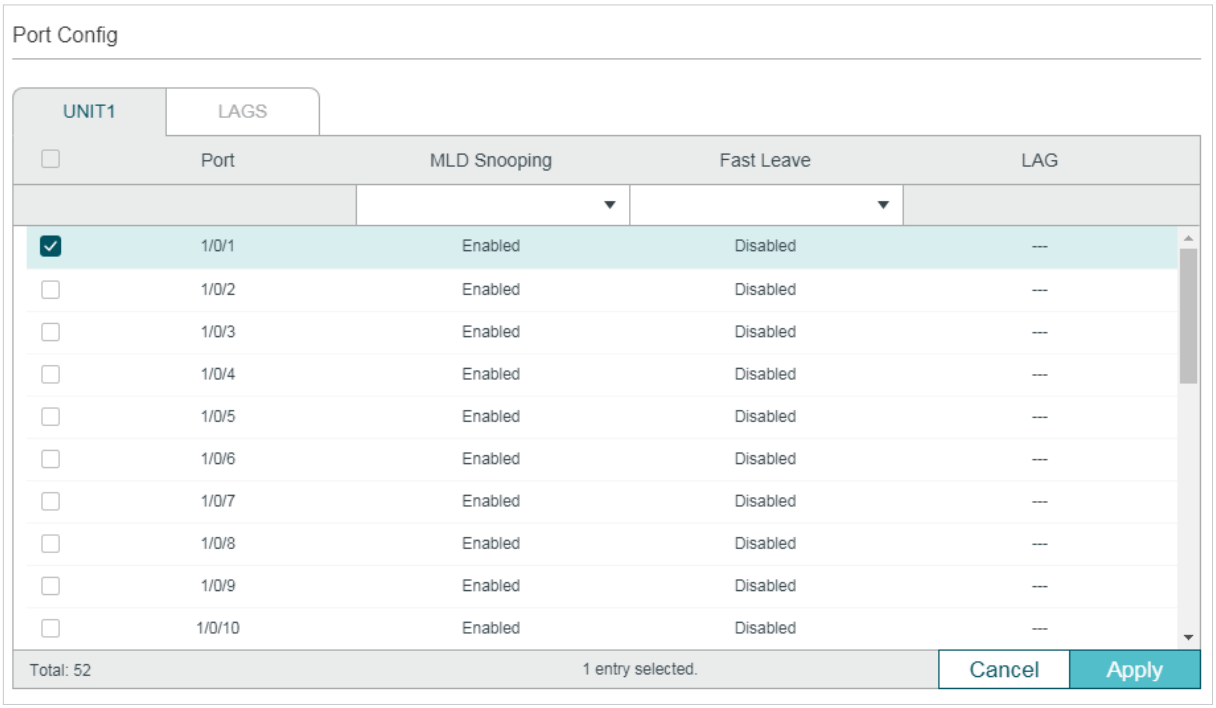
Leave Time	Specify the leave time for the VLAN. When the switch receives a leave message from a port to leave a multicast group, it will wait for a leave time before removing the port from the multicast group. During the period, if the switch receives any report messages from the port, the port will not be removed from the multicast group. Exceptions are as follows: • If the member port ages out before the Leave Time ends and no report messages are received, the port will be removed from the multicast group once its Member Port Aging Time ends. • The Leave Time mechanism will not take effect when Fast Leave takes effect. A proper leave time value can avoid other hosts connecting to the same port of the switch being mistakenly removed from the multicast group when only some of them want to leave.
MLD Snooping Querier	Enable or disable the MLD Snooping Querier for the VLAN. When enabled, the switch acts as an MLD Snooping Querier for the hosts in this VLAN. A querier periodically sends a general query on the network to solicit membership information, and sends MASQs when it receives done messages from hosts.
Query Interval	With MLD Snooping Querier enabled, specify the interval between general query messages sent by the switch.
Maximum Response Time	With MLD Snooping Querier enabled, specify the host's maximum response time to general query messages.
Last Listener Query Interval	With MLD Snooping Querier enabled, when the switch receives a done message, it 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 done message. This parameter determines the interval between MASQs.
Last Listener Query Count	With MLD Snooping Querier enabled, specify the number of MASQs to be sent. If specified count of MASQs are sent and no report message is received, the switch will delete the multicast address from the multicast forwarding table.
General Query Source IP	With MLD Snooping Querier enabled, specify the source IPv6 address of the general query messages sent by the switch. It should be a unicast address.
Static Router Ports	Select one or more ports to be the static router ports in the VLAN. Static router ports do not age. Multicast streams and MLD packets to all groups in this VLAN will be forwarded through the static router ports. Multicast streams and MLD packets to the groups that have dynamic router ports will be also forwarded through the corresponding dynamic router ports.
Forbidden Router Ports	Select the ports to forbid them from being router ports in the VLAN.

2) Click **Save**.

3.1.3 Configuring MLD Snooping for Ports

Choose the menu **L2 FEATURES > Multicast > MLD Snooping > Port Config** to load the following page.

Figure 3-3 Configure MLD Snooping for Ports



Follow these steps to configure MLD Snooping for ports:

1) Enable MLD Snooping for the port and enable Fast Leave if there is only one receiver connected to the port.

MLD Snooping	Enable or disable MLD Snooping for the port.
Fast Leave	Enable or disable Fast Leave for the port. Fast Leave can be enabled on a per-port basis or per-VLAN basis. When enabled on a per-port basis, the switch will remove the port from the corresponding multicast group of all VLANs before forwarding the done message to the querier. You should only use Fast Leave for a port when there is a single receiver connected to the port. For more details about Fast Leave, see *3.1.2 Configuring MLD Snooping for VLANs*.
LAG	Displays the LAG the port belongs to.

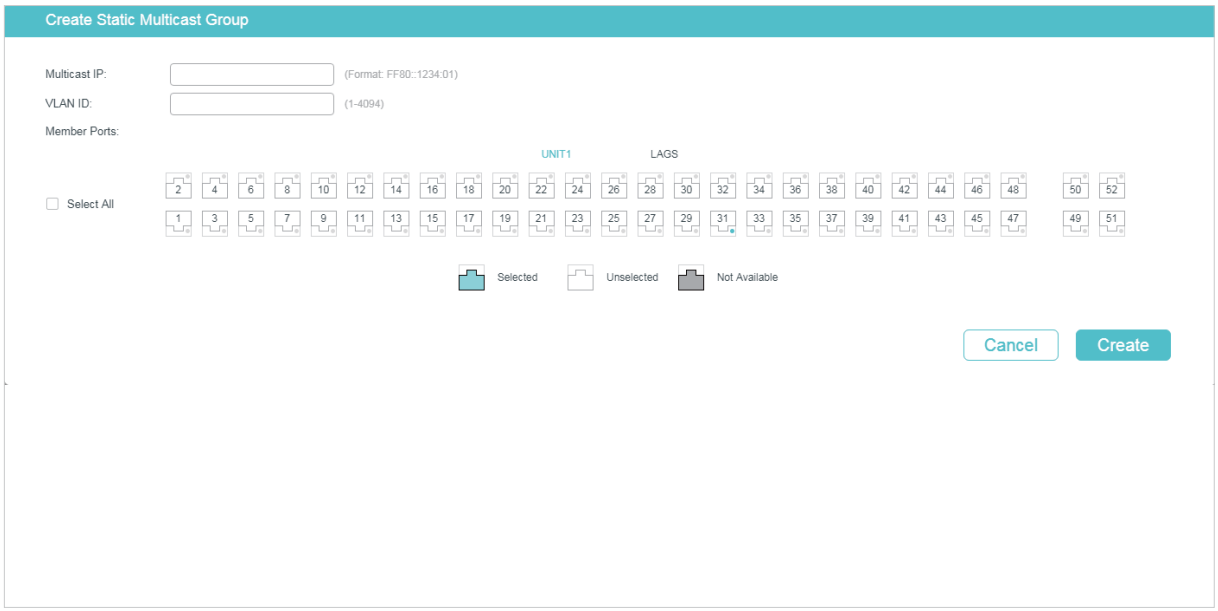
2) Click **Apply**.

3.1.4 Configuring Hosts to Statically Join a Group

Hosts or Layer 2 ports normally join multicast groups dynamically, but you can also configure hosts to statically join a group.

Choose the menu **L2 FEATURES > Multicast > MLD Snooping > Static Group Config** and click Add to load the following page.

Figure 3-4 Configure Hosts to Statically Join a Group



Follow these steps to configure hosts to statically join a group:

1) Specify the multicast IP address, VLAN ID. Select the ports to be the static member ports of the multicast group.

Multicast IP	Specify the IPv6 address of the multicast group that the hosts need to join.
VLAN ID	Specify the VLAN that the hosts are in.
Member Ports	Select the ports that the hosts are connected to. These ports will become the static member ports of the multicast group and will never age.

2) Click **Create**.

3.2 Using the CLI

3.2.1 Configuring MLD Snooping Globally

Follow these steps to configure MLD Snooping globally:

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 mld snooping** Enable MLD Snooping Globally.

Step 3	**ipv6 mld snooping drop-unknown** (Optional) Configure the way how the switch processes multicast streams that are sent to unknown multicast groups as Discard. By default, it is Forward. Unknown multicast groups are multicast groups that do not match any of the groups announced in earlier IGMP membership reports, and thus cannot be found in the multicast forwarding table of the switch. *Note:* IGMP Snooping and MLD Snooping share the setting of Unknown Multicast Groups, you need to ensure IGMP Snooping is enabled globally. To enable IGMP Snooping globally, use the **ip igmp snooping** command in global configuration mode.
Step 4	**show ipv6 mld 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 enable MLD Snooping globally, and the way how the switch processes multicast streams that are sent to unknown multicast groups as discard.

Switch#configure

Switch(config)#ipv6 mld snooping

Switch(config)#ipv6 mld snooping

Switch(config)#ipv6 mld snooping drop-unknown

Switch(config)#show ipv6 mld snooping

MLD Snooping :Enable

Unknown Multicast :Discard

...

Switch(config)#end

Switch#copy running-config startup-config

3.2.2 Configuring MLD Snooping for VLANs

Before configuring MLD Snooping for VLANs, set up the VLANs that the router ports and the member ports are in. For details, please refer to *Configuring 802.1Q VLAN*.

The switch supports configuring MLD Snooping on a per-VLAN basis. After MLD Snooping is enabled globally, you also need to enable MLD Snooping and configure the corresponding parameters for the VLANs that the router ports and the member ports are in.

Follow these steps to configure MLD Snooping for VLANs:

Step 1 **configure**

Enter global configuration mode.

Step 2 **ipv6 mld snooping vlan-config** *vlan-id-list* **mtime** *member-time*

Enable MLD Snooping for the specified VLANs, and specify the member port aging time for the VLANs.

vlan-id-list: Specify the ID or the ID list of the VLAN(s).

member-time: Specify the aging time of the member ports in the specified VLANs. Valid values are from 60 to 600 seconds. By default, it is 260 seconds.

Once the switch receives an MLD report message from a port, the switch adds this port to the member port list of the corresponding multicast group. Member ports that are learned in this way are called dynamic member ports.

If the switch does not receive any MLD report message for a specific multicast group from a dynamic member port, it will no longer consider this port as a member port of this multicast group and delete it from the multicast forwarding table.

Step 3 **ipv6 mld snooping vlan-config** *vlan-id-list* **rtime** *router-time*

Specify the router port aging time for the VLANs.

vlan-id-list: Specify the ID or the ID list of the VLAN(s).

router-time: Specify the aging time of the router ports in the specified VLANs. Valid values are from 60 to 600 seconds. By default, it is 300 seconds.

Once the switch receives an MLD general query message from a port, the switch adds this port to the router port list. Router ports that are learned in this way are called dynamic router ports.

If the switch does not receive any MLD general query message from a dynamic router port within the router port aging time, the switch will no longer consider this port as a router port and delete it from the router port list.

Step 4 **ipv6 mld snooping vlan-config** *vlan-id-list* **ltime** *leave-time*

Specify the router port aging time for the VLANs.

vlan-id-list: Specify the ID or the ID list of the VLAN(s).

leave-time: Specify the leave time for the VLAN(s). Valid values are from 1 to 30 in seconds, and the default value is 1 second.

When the switch receives a leave message from a port to leave a multicast group, it will wait for a leave time before removing the port from the multicast group. During the period, if the switch receives any report messages from the port, the port will not be removed from the multicast group. Exceptions are as follows:

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

A proper leave time value can avoid other hosts connecting to the same port of the switch being mistakenly removed from the multicast group when only some of them want to leave.

Step 5 **ipv6 mld snooping vlan-config** *vlan-id-list* **report-suppression**

(Optional) Enable Report Suppression for the VLANs. By default, it is disabled.

When enabled, the switch will only forward the first MLD report message for each multicast group to the MLD querier and suppress subsequent MLD report messages for the same multicast group during one query interval. This feature prevents duplicate report messages from being sent to the MLD querier.

vlan-id-list: Specify the ID or the ID list of the VLAN(s).

Step 6 **ipv6 mld snooping vlan-config** *vlan-id-list* **immediate-leave**

(Optional) Enable Fast Leave for the VLANs. By default, it is disabled.

Without Fast Leave, after a receiver sends an MLD done message (equivalent to an IGMP leave message) to leave a multicast group, the switch will forward the done message to the Layer 3 device (the querier).

From the point of view of the querier, the port connecting to the switch is a member port of the corresponding multicast group. After receiving the done message from the switch, the querier will send out a configured number (Last Listener Query Count) of Multicast-Address-Specific Queries (MASQs) on that port with a configured interval (Last Listener Query Interval), and wait for MLD reports. If there are other receivers connecting to the switch, they will response to the MASQs before the Last Listener Query Interval expires. If no reports are received after the response time of the last query expires, the querier will remove the port from the forwarding list of the corresponding multicast group.

That is, if there are other receivers connecting to the switch, the one sent done message have to wait until the port ages out from the switch's forwarding list of the corresponding multicast group (the maximum waiting time is decided by the Member Port Aging Time).

With Fast Leave enabled on a VLAN, the switch will remove the (Multicast Group, Port, VLAN) entry from the multicast forwarding table before forwarding the done message to the querier. This helps to reduce bandwidth waste since the switch no longer sends the corresponding multicast streams to the VLAN of the port as soon as the port receives a done message from the VLAN.

vlan-id-list: Specify the ID or the ID list of the VLAN(s).

Step 7 **ipv6 mld snooping vlan-config** *vlan-id-list* **rport interface { fastEthernet** *port-list* **| gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port-list*| **port-channel** *lag-list* **}**

(Optional) Specify the static router ports for the VLANs. Static router ports do not age.

vlan-id-list: Specify the ID or the ID list of the VLAN(s).

port-list: The number or the list of the Ethernet port that need to be configured as static router ports.

lag-list: The ID or the list of the LAG that need to be configured as static router ports.

Step 8 **ipv6 mld snooping vlan-config** *vlan-id-list* **router-ports-forbidden interface { fastEthernet** *port-list* **| gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port-list* **| port-channel** *lag-list* **}**

(Optional) Specify the ports to forbid them from being router ports in the VLANs.

vlan-id-list: Specify the ID or the ID list of the VLAN(s).

port-list: The number or the list of the Ethernet port that need to be forbidden from being router ports.

lag-list: The ID or the list of the LAG that need to be forbidden from being router ports.

Step 9	**ipv6 mld snooping vlan-config** *vlan-id-list* **querier** (Optional) Enable MLD Snooping Querier for the VLAN. By default, it is disabled. When enabled, the switch acts as an MLD Snooping Querier for the hosts in this VLAN. A querier periodically sends a general query on the network to solicit membership information, and sends group-specific queries when it receives done messages from hosts. *vlan-id-list:* Specify the ID or the ID list of the VLAN(s). After enabling MLD Snooping Querier feature, you need to specify the corresponding parameters including the Last Member Query Count, Last Member Query Interval, Maximum Response Time, Query Interval and General Query Source IP. Use the command below in global configuration mode to configure the parameters: **ipv6 mld snooping vlan-config** *vlan-id-list* **querier { max-response-time** *response-time* **| query-interval** *interval* **| general-query source-ip** *ip-addr* **| last-listener-query-count** *num* **| last-listener-query-interval** *interval* **}** *vlan-id-list:* Specify the ID or the ID list of the VLAN(s). *response-time:* Specify the host's maximum response time to general query messages. **query-interval** *interval:* Specify the interval between general query messages sent by the switch. *ip-addr:* Specify the source IP address of the general query messages sent by the switch. It should be a unicast address. *num:* Specify the number of group-specific queries to be sent. With MLD Snooping Querier enabled, when the switch receives a done message, it 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 done message. If specified count of MASQs are sent and no report message is received, the switch will delete the multicast address from the multicast forwarding table. **last-listener-query-interval** *interval:* Specify the interval between MASQs.
Step 10	**show ipv6 mld snooping vlan** *vlan-id* Show the basic MLD snooping configuration in the specified 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 enable MLD Snooping for VLAN 1, and configure the member port aging time as 300 seconds, the router port aging time as 320 seconds, and then enable Fast Leave and Report Suppression for the VLAN:

Switch#configure

Switch(config)#ipv6 mld snooping vlan-config 1 **mtime** 300

Switch(config)#ipv6 mld snooping vlan-config 1 **rtime** 320

Switch(config)#ipv6 mld snooping vlan-config 1 **immediate-leave**

Switch(config)#ipv6 mld snooping vlan-config 1 **report-suppression**

Switch(config)#show ipv6 mld snooping vlan 1

Vlan Id: 1

Vlan MLD Snooping Status: Enable

Fast Leave: Enable

Report Suppression: Enable

Router Time: Enable

Member Time: Enable

Querier: Disable

...

Switch(config)#end

Switch#copy running-config startup-config

The following example shows how to enable MLD Snooping querier for VLAN 1, and configure the query interval as 100 seconds, the maximum response time as 15 seconds, the last listener query interval as 2 seconds, the last listener query count as 3, and the general query source IP as 2000::1:2345:6789:ABCD:

Switch#configure

Switch(config)#ipv6 mld snooping vlan-config 1 **querier**

Switch(config)#ipv6 mld snooping vlan-config 1 **querier query-interval** 100

Switch(config)#ipv6 mld snooping vlan-config 1 **querier max-response-time** 15

Switch(config)#ipv6 mld snooping vlan-config 1 **querier last-listener-query-interval** 2

Switch(config)#ipv6 mld snooping vlan-config 1 **querier last-listener-query-count** 3

Switch(config)#ipv6 mld snooping vlan-config 1 **querier general-query source-ip** 2000::1:2345:6789:ABCD

Switch(config)#show ipv6 mld snooping vlan 1

Vlan Id: 1

...

Querier:	Enable
Maximum Response Time:	15
Query Interval:	100
Last Member Query Interval:	2
Last Member Query Count:	3
General Query Source IP:	2000::1:2345:6789:abcd

...

Switch(config)#end

Switch#copy running-config startup-config

3.2.3 Configuring MLD Snooping for Ports

Follow these steps to configure MLD Snooping 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***| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Enter interface configuration mode**.**
Step 3	**ipv6 mld snooping** Enable MLD Snooping for the port. By default, it is enabled.
Step 4	**ipv6 mld snooping immediate-leave** (Optional) Enable Fast Leave on the specified port. Fast Leave can be enabled on a per-port basis or per-VLAN basis. When enabled on a per-port basis, the switch will remove the port from the corresponding multicast group of all VLANs before forwarding the done message to the querier. You should only use Fast Leave for a port when there is a single receiver connected to the port. For more details about Fast Leave, see *3.2.2 Configuring MLD Snooping for VLANs*.
Step 5	**show ipv6 mld snooping interface [fastEthernet** [*port-list*] **| gigabitEthernet** [*port-list*] **| ten-gigabitEthernet** [*port-list*] **| port-channel** [*port-channel-list*]**] basic-config** Show the basic MLD Snooping configuration 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 enable MLD Snooping and fast leave for port 1/0/1-3:

Switch#configure

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

Switch(config-if-range)#ipv6 mld snooping

Switch(config-if-range)#ipv6 mld snooping immediate-leave

Switch(config-if-range)#show ipv6 mld snooping interface gigabitEthernet 1/0/1-3

Port	MLD-Snooping	Fast-Leave
Gi1/0/1	enable	enable
Gi1/0/2	enable	enable
Gi1/0/3	enable	enable

Switch(config-if-range)#end

Switch#copy running-config startup-config

3.2.4 Configuring Hosts to Statically Join a Group

Hosts or Layer 2 ports normally join multicast groups dynamically, but you can also configure hosts to statically join a group.

Follow these steps to configure hosts to statically join a group:

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 mld snooping vlan-config** *vlan-id-list* **static** *ip* **interface {fastEthernet** *port-list* **| gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port-list* **| port-channel** *lag-list***}** *vlan-id-list:* Specify the ID or the ID list of the VLAN(s). *ip:* Specify the IP address of the multicast group that the hosts want to join. *port-list* / *lag-list:* Specify the ports that is connected to the hosts. These ports will become static member ports of the group.
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 port 1/0/1-3 in VLAN 2 to statically join the multicast group 239.1.2.3:

Switch#configure

Switch(config)#ipv6 mld snooping vlan-config 2 **static** 239.1.2.3 **interface gigabitEthernet** 1/0/1-3

Switch(config)#show ipv6 mld snooping groups static

Multicast-ip	VLAN-id	Addr-type	Switch-port
239.1.2.3	2	static	Gi1/0/1-3

Switch(config)#end

Switch#copy running-config startup-config

4 MVR Configuration

To complete MVR configuration, follow these steps:

1) Configure 802.1Q VLANs.
2) Configure MVR globally.
3) Add multicast groups to MVR.
4) Configure MVR for the ports.
5) (Optional) Statically add ports to MVR groups.

Configuration Guidelines

- MVR does not support IGMPv3 messages.
- Do not configure MVR on private VLAN ports, otherwise MVR cannot take effect.
- MVR operates on the underlying mechanism of IGMP Snooping, but the two features operate independently of each other. Both protocols can be enabled on a port at the same time. When both are enabled, MVR listens to the report and leave messages only for the multicast groups configured in MVR. All other multicast groups are managed by IGMP Snooping.

4.1 Using the GUI

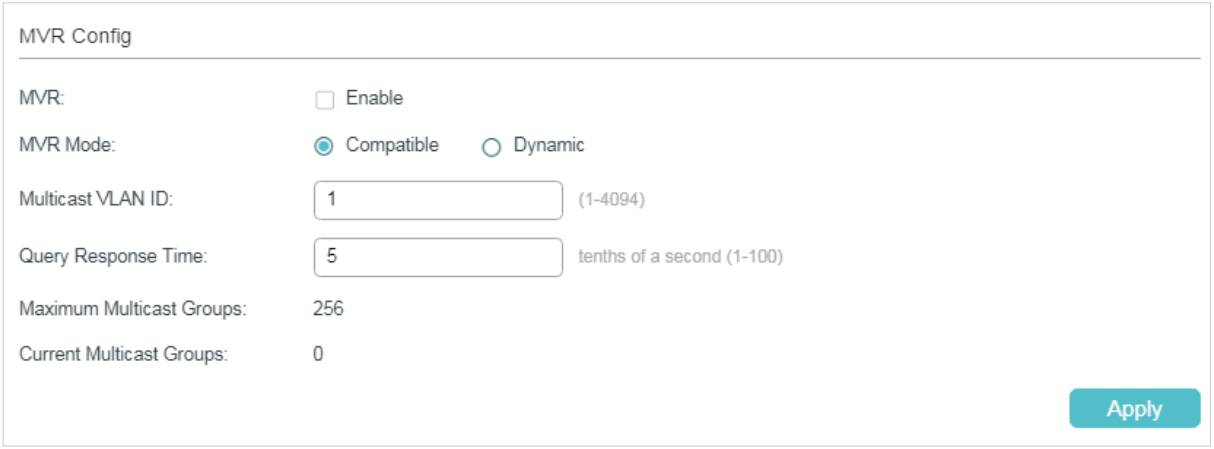
4.1.1 Configuring 802.1Q VLANs

Before configuring MVR, create an 802.1Q VLAN as the multicast VLAN. Add all source ports (uplink ports that receive multicast data from the router) to the multicast VLAN as tagged ports. Configure 802.1Q VLANs for the receiver ports (ports that are connecting to the hosts) according to network requirements. Note that receiver ports can only belong to one VLAN and cannot be added to the multicast VLAN. For details, refer to *Configuring 802.1Q VLAN*.

4.1.2 Configuring MVR Globally

Choose the menu **L2 FEATURES > Multicast > MVR > MVR Config** to load the following page.

Figure 4-1 Configure MVR Globally



Follow these steps to configure MVR globally:

1) Enable MVR globally and configure the global parameters.

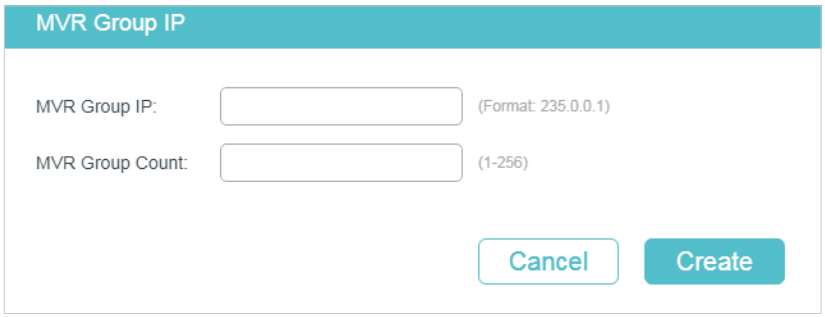
MVR	Enable or disable MVR globally.
MVR Mode	Specify the MVR mode as compatible or dynamic. **Compatible:** In this mode, the switch does not forward report or leave messages from the hosts to the IGMP querier. This means IGMP querier cannot learn the multicast groups' membership information from the switch. The IGMP querier must be statically configured to transmit all the required multicast streams to the switch via the multicast VLAN. **Dynamic:** In this mode, after receiving report or leave messages from the hosts, the switch will forward them to the IGMP querier via the multicast VLAN (with appropriate translation of the VLAN ID). The IGMP querier can learn the multicast groups' membership information through the report and leave messages, and transmit the multicast streams to the switch via the multicast VLAN according to the multicast forwarding table.
Multicast VLAN ID	Specify an existing 802.1Q VLAN as the multicast VLAN.
Query Response Time	Specify the maximum time to wait for IGMP report on a receiver port before removing the port from multicast group membership.
Maximum Multicast Groups	Displays the maximum number of multicast groups that can be configured on the switch.
Current Multicast Groups	Displays the current number of multicast groups that have been configured on the switch.

2) Click **Apply**.

4.1.3 Adding Multicast Groups to MVR

You need to manually add multicast groups to the MVR. Choose the menu **L2 FEATURES > Multicast > MVR > MVR Group Config** and click Add to load the following page.

Figure 4-2 Add Multicast Groups to MVR



Follow these steps to add multicast groups to MVR:

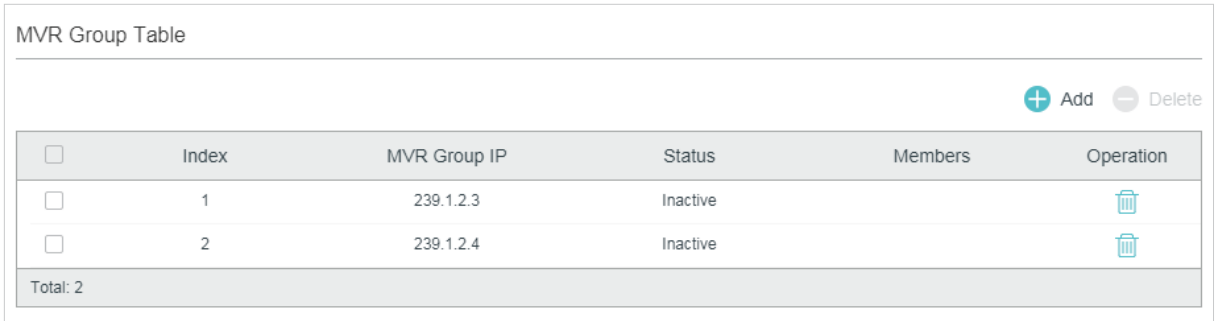
1) Specify the IP address of the multicast groups.

MVR Group IP / MVR Group Count	Specify the start IP address and the number of contiguous series of multicast groups. Multicast data sent to the address specified here will be sent to all source ports on the switch and all receiver ports that have requested to receive data from that multicast address.

2) Click **Create**.

Then the added multicast groups will appear in the MVR group table, as the following figure shows:

Figure 4-3 MVR Group Table



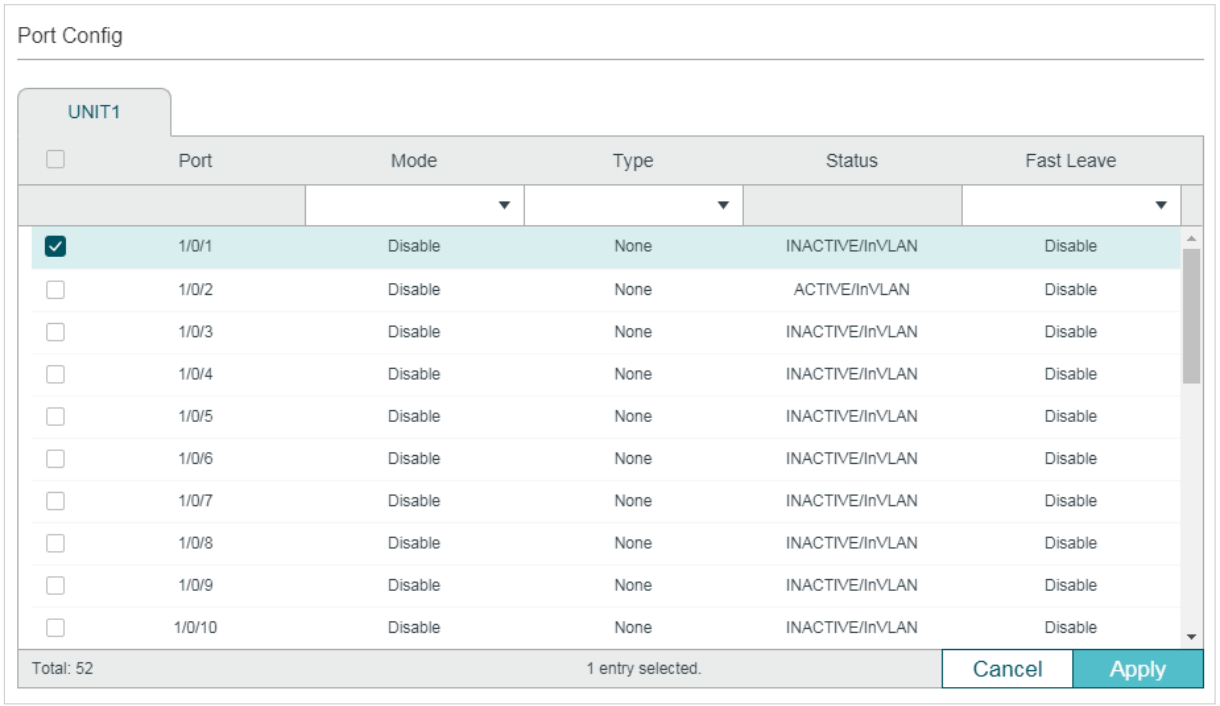
MVR Group IP	Displays the IP address of multicast group.

Status	Displays the status of the MVR group. In compatible mode, all the MVR groups are added manually, so the status is always active. In dynamic mode, there are two status: **Inactive**: The MVR group is added successfully, but the source port has not received any query messages from this multicast group. **Active**: The MVR group is added successfully and the source port has received query messages from this multicast group.
Member	Displays the member ports in this MVR group.

4.1.4 Configuring MVR for the Port

Choose the menu **L2 FEATURES > Multicast > MVR > Port Config** to load the following page.

Figure 4-4 Configure MVR for the Port



Follow these steps to add multicast groups to MVR:

1) Select one or more ports to configure.
2) Enable MVR, and configure the port type and Fast Leave feature for the port.

Mode	Enable or disable MVR for the selected ports.

Type	Configure the port type. **None**: The port is a non-MVR port. If you attempt to configure a non-MVR port with MVR characteristics, the operation will be unsuccessful. **Source**: Configure the uplink ports that receive and send multicast data on the multicast VLAN as source ports. Source ports should belong to the multicast VLAN. In compatible mode, source ports will be automatically added to all multicast groups, while in dynamic mode, you need to manually add them to the corresponding multicast groups. **Receiver**: Configure the ports that are connecting to the hosts as receiver ports. A receiver port can only belong to one VLAN, and cannot belong to the multicast VLAN. In both modes, the switch will add or remove the receiver ports to the corresponding multicast groups by snooping the report and leave messages from the hosts.
Status	Displays the port's status. **Active/InVLAN**: The port is physically up and in one or more VLANs. **Active/NotInVLAN**: The port is physically up and not in any VLAN. **Inactive/InVLAN**: The port is physically down and in one or more VLANs. **Inactive/NotInVLAN**: The port is physically down and not in any VLAN.
Fast Leave	Enable or disable Fast Leave for the selected ports. Only receiver ports support Fast Leave. Before enabling Fast Leave for a port, make sure there is only a single receiver device connecting to the port.

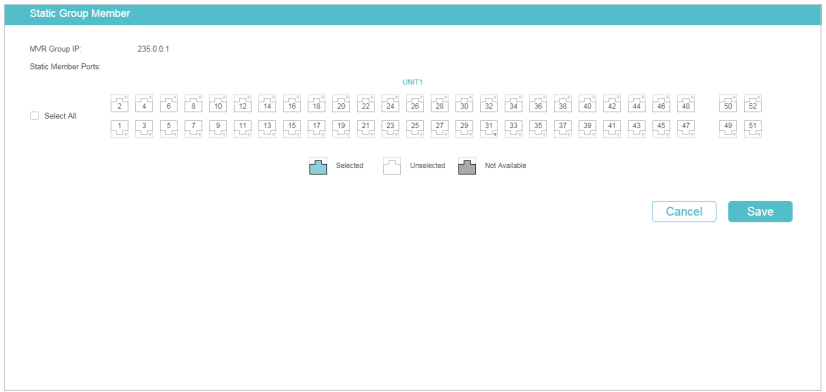
3) Click **Apply**.

4.1.5 (Optional) Adding Ports to MVR Groups Statically

You can add only receiver ports to MVR groups statically. The switch adds or removes receiver ports to the corresponding multicast groups by snooping the report and leave messages from the hosts. You can also statically add a receiver port to an MVR group.

Choose the menu **L2 FEATURES > Multicast > MVR > Static Group Members,** and click in your desired MVR group entry to load the following page.

Figure 4-5 Configure Hosts to Statically Join an MVR group



Follow these steps to statically add ports to an MVR group:

1) Select the ports to add them to the MVR group.
2) Click **Save**.

4.2 Using the CLI

4.2.1 Configuring 802.1Q VLANs

Before configuring MVR, create an 802.1Q VLAN as the multicast VLAN. Add the all source ports to the multicast VLAN as tagged ports. Configure 802.1Q VLANs for the receiver ports according to network requirements. Note that receiver ports can only belong to one VLAN and cannot be added to the multicast VLAN. For details, refer to *Configuring 802.1Q VLAN*.

4.2.2 Configuring MVR Globally

Follow these steps to configure MVR globally:

Step 1	**configure** Enter global configuration mode.
Step 2	**mvr** Enable MVR Globally.
Step 3	**mvr mode {** compatible | dynamic **}** Configure the MVR mode as compatible or dynamic. compatible: In this mode, the switch does not forward report or leave messages from the hosts to the IGMP querier. So the IGMP querier cannot learn the multicast groups membership information from the switch. You have to statically configure the IGMP querier to transmit all the required multicast streams to the switch via the multicast VLAN. dynamic: In this mode, after receiving report or leave messages from the hosts, the switch will forward them to the IGMP querier via the multicast VLAN (with appropriate translation of the VLAN ID). So the IGMP querier can learn the multicast groups membership information through the report and leave messages, and transmit the multicast streams to the switch via the multicast VLAN according to the multicast forwarding table.
Step 4	**mvr vlan** *vlan-id* Specify the multicast VLAN. *vlan-id:* Specify the ID of the multicast VLAN. Valid values are from 1 to 4094.
Step 5	**mvr querytime** *time* Specify the maximum time to wait for IGMP report on a receiver port before removing the port from multicast group membership. *time:* Specify the maximum response time. Valid values are from 1 to100 tenths of a second, and the default value is 5 tenths of a second.

Step 6	**mvr group** *ip-addr count* Add multicast groups to the MVR. *ip-addr:* Specify the start IP address of the contiguous series of multicast groups. *count:* Specify the number of the multicast groups to be added to the MVR. The range is 1 to 256.
Step 7	**show mvr** Show the global MVR configuration. **show mvr members** Show the existing MVR groups.
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 MVR globally, and configure the MVR mode as compatible, the multicast VLAN as VLAN 2 and the query response time as 5 tenths of a second. Then add 239.1.2.3-239.1.2.5 to MVR group.

Switch#configure

Switch(config)#mvr mode compatible

Switch(config)#mvr vlan 2

Switch(config)#mvr querytime 5

Switch(config)#mvr group 239.1.2.3 3

Switch(config)#show mvr

MVR	:Enable
MVR Multicast Vlan	:2
MVR Max Multicast Groups	:256
MVR Current Multicast Groups	:3
MVR Global Query Response Time	:5 (tenths of sec)
MVR Mode Type	:Compatible

Switch(config)#show mvr members

MVR Group IP	status	Members
---	---	---
239.1.2.3	active	
239.1.2.4	active	
239.1.2.5	active	

Switch(config)#end

Switch#copy running-config startup-config

4.2.3 Configuring MVR for the Ports

Follow these steps to configure MVR 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* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Enter interface configuration mode**.**
Step 3	**mvr** Enable MVR for the port.
Step 4	**mvr type {** source | receiver **}** Configure the MVR port type as receiver or source. By default, the port is a non-MVR port. If you attempt to configure a non-MVR port with MVR characteristics, the operation fails. source: Configure the uplink ports that receive and send multicast data on the multicast VLAN as source ports. Source ports should belong to the multicast VLAN. receiver: Configure the ports that are connecting to the hosts as receiver ports. A receiver port can only belong to one VLAN, and cannot belong to the multicast VLAN.
Step 5	**mvr immediate** (Optional) Enable the Fast Leave feature of MVR for the port. Only receiver ports support Fast Leave. Before enabling Fast Leave for a port, make sure there is only a single receiver device connecting to the port.
Step 6	**mvr vlan** *vlan-id* **group** *ip-addr* (Optional) Statically add the port to an MVR group. Then the port can receive multicast traffic sent to the IP multicast address via the multicast VLAN. This command applies to only receiver ports. The switch adds or removes the receiver ports to the corresponding multicast groups by snooping the report and leave messages from the hosts. You can also statically add a receiver port to an MVR group. *vlan-id*: Enter the multicast VLAN ID. *ip-addr*: Specify the IP address of the multicast group.

Step 7	**show mvr interface {fastEthernet [*port-list*] | gigabitEthernet [*port-list*] | ten-gigabitEthernet [*port-list*] }** Show the MVR configuration of the specified interface(s). **show mvr members** Show the membership information of all MVR groups.
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 port 1/0/7 as source port, and port 1/0/1-3 as receiver ports. Then statically add port 1/0/1-3 to group 239.1.2.3 and enable MVR Fast Leave for these ports. The multicast VLAN is VLAN 2.

Switch#configure

Switch(config)#interface gigabitEthernet 1/0/7

Switch(config-if)#mvr

Switch(config-if)#mvr type source

Switch(config-if)#exit

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

Switch(config-if-range)#mvr

Switch(config-if-range)#mvr type receiver

Switch(config-if-range)#mvr immediate

Switch(config-if-range)#mvr vlan 2 **group** 239.1.2.3

Switch(config-if-range)#show mvr interface gigabitEtnernet 1/0/1-3,1/0/7

Port	Mode	Type	Status	Immediate Leave
Gi1/0/1	Enable	Receiver	INACTIVE/InVLAN	Enable
Gi1/0/2	Enable	Receiver	INACTIVE/InVLAN	Enable
Gi1/0/3	Enable	Receiver	INACTIVE/InVLAN	Enable
Gi1/0/7	Enable	Source	INACTIVE/InVLAN	Disable

Switch(config-if-range)#show mvr members

MVR Group IP	status	Members
239.1.2.3	active	Gi1/0/1-3, 1/0/7

Switch(config)#end

Switch#copy running-config startup-config

5 Multicast Filtering Configuration

To complete multicast filtering configuration, follow these steps:

1) Create the IGMP profile or MLD profile.
2) Configure multicast groups a port can join and the overflow action.

5.1 Using the GUI

5.1.1 Creating the Multicast Profile

You can create multicast profiles for both IPv4 and IPv6 network. With multicast profile, the switch can define a blacklist or whitelist of multicast groups so as to filter multicast sources.

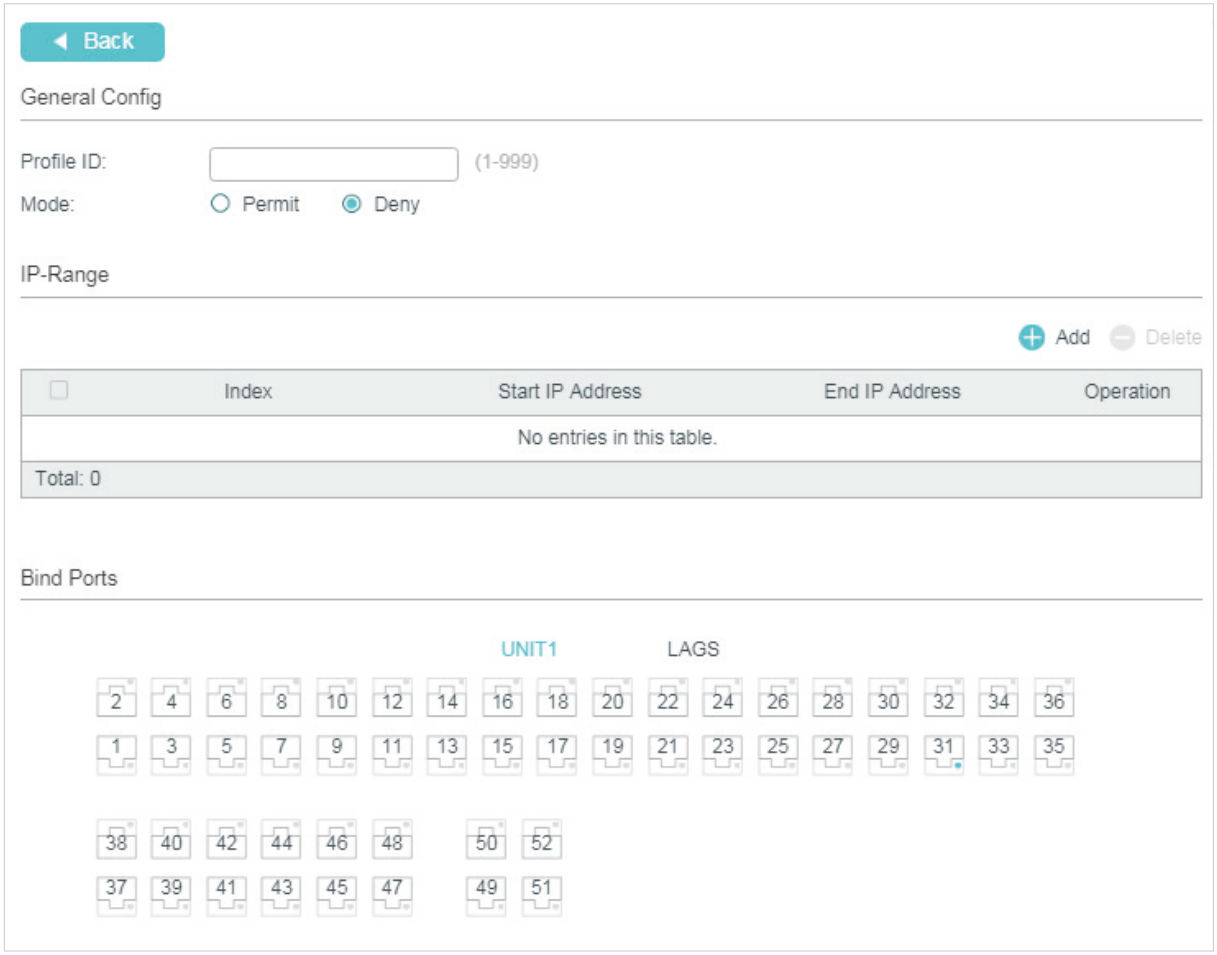
The process for creating multicast profiles for IPv4 and IPv6 are similar. The following introductions take creating an IPv4 profile as an example.

Choose the menu **L2 FEATURES > Multicast > Multicast Filtering > IPv4 Profile**, and click Add to load the following page.

Note:

To create a multicast profile for IPv6, choose the menu **L2 FEATURES > Multicast > Multicast Filtering > IPv6 Profile**.

Figure 5-1 Create IPv4 Profile



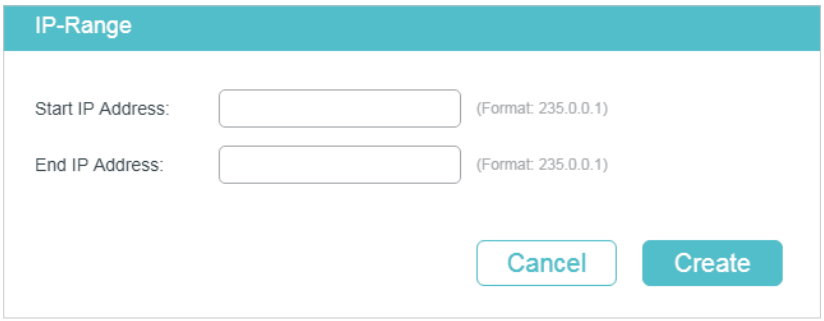
Follow these steps to create a profile.

1) In the **General Config** section, specify the Profile ID and Mode.

Profile ID	Enter a profile ID between 1 and 999.
Mode	Select **Permit** or **Deny** as the filtering mode. **Permit**: Acts as a whitelist and only allows specific member ports to join specified multicast groups. **Deny**: Acts as a blacklist and prevents specific member ports from joining specific multicast groups.

2) In the **IP-Range** section, click Add to load the following page. Configure the start IP address and end IP address of the multicast groups to be filtered, and click **Create**.

Figure 5-2 Configure Multicast Groups to Be Filtered



3) In the **Bind Ports** section, select your desired ports to be bound with the profile.

4) Click **Save**.

5.1.2 Configure Multicast Filtering for Ports

You can modify the mapping relation between ports and profiles in batches, and configure the number of multicast groups a port can join and the overflow action.

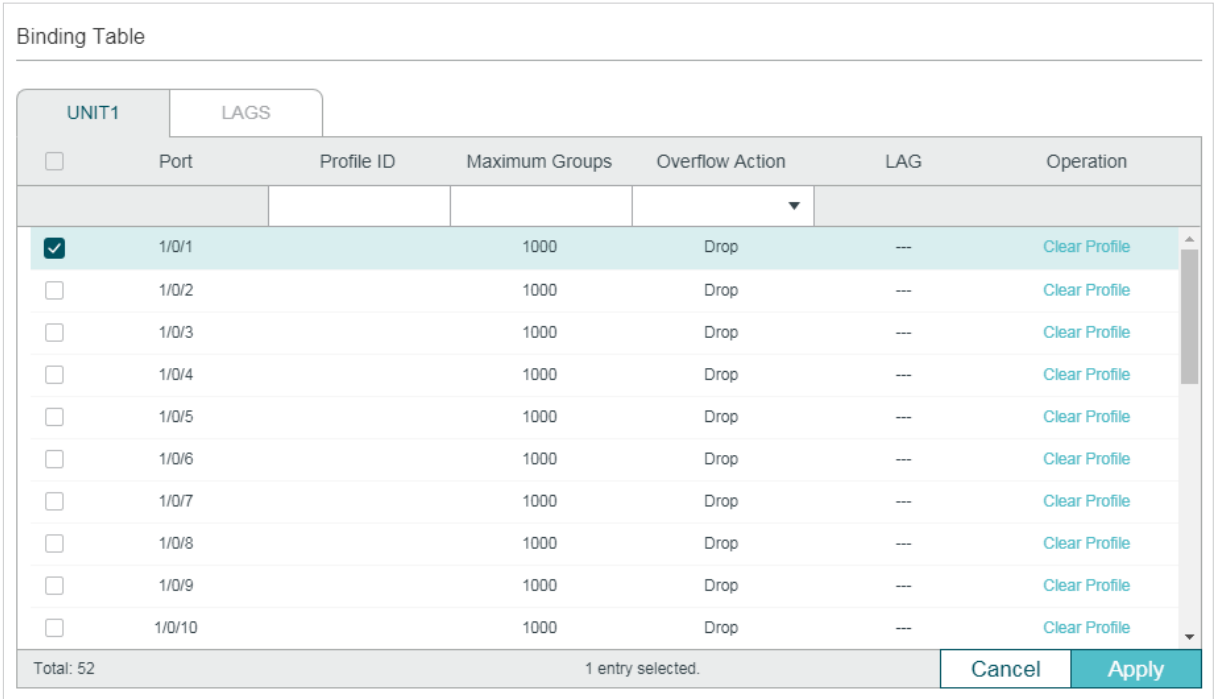
The process for configuring multicast filtering for ports in IPv4 and IPv6 are similar. The following introductions take configuring multicast filtering for ports in IPv4 as an example.

Choose the menu **L2 FEATURES > Multicast > Multicast Filtering > IPv4 Ports Binding** to load the following page.

Note:

For IPv6, choose the menu **L2 FEATURES > Multicast > Multicast Filtering > IPv6 Ports Binding**.

Figure 5-3 Configure Multicast Filtering for Ports



Follow these steps to bind the profile to ports and configure the corresponding parameters for the ports:

1) Select one or more ports to configure.
2) Specify the profile to be bound, and configure the maximum groups the port can join and the overflow action.

Profile ID	Specify the ID of an existing profile to bind the profile to the selected ports. One port can only be bound to one profile.
Maximum Groups	Enter the number of multicast groups the port can join. Valid values are from 0 to 1000.
Overflow Action	Select the action the switch will take with the new multicast member groups when the number of multicast groups the port has joined exceeds the maximum. **Drop**: Drop all subsequent membership report messages to prevent the port joining a new multicast groups. **Replace**: Replace the existing multicast group that has the lowest multicast MAC address with the new multicast group.
LAG	Displays the LAG the port belongs to.
Operation	Click **Clear Profile** to clear the binding between the profile and the port.

3) Click **Apply**.

5.2 Using the CLI

5.2.1 Creating the Multicast Profile

You can create multicast profiles for both IPv4 and IPv6 network. With multicast profile, the switch can define a blacklist or whitelist of multicast groups so as to filter multicast sources.

Creating IGMP Profile (Multicast Profile for IPv4)

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** Configure the profile's filtering mode as permit. Then the profile acts as a whitelist and only allows specific member ports to join specified multicast groups. **deny** Configure the profile's filtering mode as deny. Then the profile acts as a blacklist and prevents specific member ports from joining specific multicast groups.
Step 4	**range** *start-ip end-ip* Configure the range of multicast IP addresses to be filtered. *start-ip* / *end-ip:* Specify the start IP address and end IP address of the IP range.
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 streams 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

Creating MLD Profile (Multicast Profile for IPv6)

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

Step 2	**ipv6 mld profile** *id* Create a new profile and enter profile configuration mode.
Step 3	**Permit** Configure the profile's filtering mode as permit. It is similar to a whitelist, indicating that the switch only allow specific member ports to join specific multicast groups. **deny** Configure the profile's filtering mode as deny. It 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 addresses to be filtered. *start-ip* / *end-ip:* Specify the start IP address and end IP address of the IP range.
Step 5	**show ipv6 mld profile** [*id*] Show the detailed MLD 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 streams 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

5.2.2 Binding the Profile to Ports

You can bind the created IGMP profile or MLD profile to ports, and configure the number of multicast groups a port can join and the overflow action.

Binding the IGMP Profile to 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* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Enter interface configuration mode.
Step 3	**ip igmp filter** *profile-id* Bind the IGMP profile to the specified ports. *profile-id*: Specify the ID of the profile to be bound. It should be an existing profile.
Step 4	**ip igmp snooping max-groups** *maxgroup* Configure the maximum number of multicast groups the port can join. *maxgroup*: Specify the maximum number of multicast groups the port can join. The range is 0 to 1000.
Step 5	**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 the limit. drop: Drop all subsequent membership report messages, and the port join no more new multicast groups. replace: Replace the existing multicast group owning the lowest multicast MAC address with the new multicast group.
Step 6	**show ip igmp profile** [*id*] Show the detailed IGMP profile configurations. **show ip igmp snooping interface [fastEthernet** [*port-list*] **| gigabitEthernet** [*port-list*] **| ten-gigabitEthernet** [*port-list*] **| port-channel** [*port-channel-list*] **] max-groups** Show the multicast group limitation on the specified port(s) or of all 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 bind the existing Profile 1 to port 1/0/2, and specify the maximum number of multicast groups that port 1/0/2 can join as 50 and the Overflow Action as Drop:

Switch#configure

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

Switch(config-if)#ip igmp snooping

Switch(config-if)#ip igmp filter 1

Switch(config-if)#ip igmp snooping max-groups 50

Switch(config-if)#ip igmp snooping max-groups action drop

Switch(config-if)#show ip igmp profile

IGMP Profile 1

...

Binding Port(s)

Gi1/0/2

Switch(config-if)#show ip igmp snooping interface gigabitEthernet 1/0/2 **max-groups**

Port	Max-Groups	Overflow-Action
Gi1/0/2	50	Drops

Switch(config)#end

Switch#copy running-config startup-config

Binding the MLD Profile to 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* **| port-channel** *port-channel-id* **| range port-channel** *port-channel-list***}** Enter interface configuration mode.
Step 3	**ipv6 mld filter** *profile-id* Bind the MLD profile to the specified ports. *profile-id*: Specify the ID of the profile to be bound. It should be an existing profile.

Step 4	**ipv6 mld snooping max-groups** *maxgroup* Configure the maximum number of multicast groups the port can join. *maxgroup*: Specify the maximum number of multicast groups the port can join. The range is 0 to 1000.
Step 5	**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 owning the lowest multicast MAC address with the new multicast group.
Step 6	**show ipv6 mld profile** [*id*] Show the detailed MLD profile configuration. **show ipv6 mld snooping interface [fastEthernet** [*port-list*] **| gigabitEthernet** [*port-list*] **| ten-gigabitEthernet** [*port-list*] **| port-channel** [*port-channel-list*] **] max-groups** Show the multicast group limitation on the specified port(s) or of all 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 bind the existing Profile 1 to port 1/0/2, and specify the maximum number of multicast groups that port 1/0/2 can join as 50 and the Overflow Action as Drop:

Switch#configure

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

Switch(config-if)#ipv6 mld snooping

Switch(config-if)#ipv6 mld filter 1

Switch(config-if)#ipv6 mld snooping max-groups 50

Switch(config-if)#ipv6 mld snooping max-groups action drop

Switch(config-if)#show ipv6 mld profile

MLD Profile 1

...

Binding Port(s)

Gi1/0/2

Switch(config-if)#show ipv6 mld snooping interface gigabitEthernet 1/0/2 **max-groups**

Port	Max-Groups	Overflow-Action
Gi1/0/2	50	Drops

Switch(config)#end

Switch#copy running-config startup-config

6 Viewing Multicast Snooping Information

You can view the following multicast snooping information:

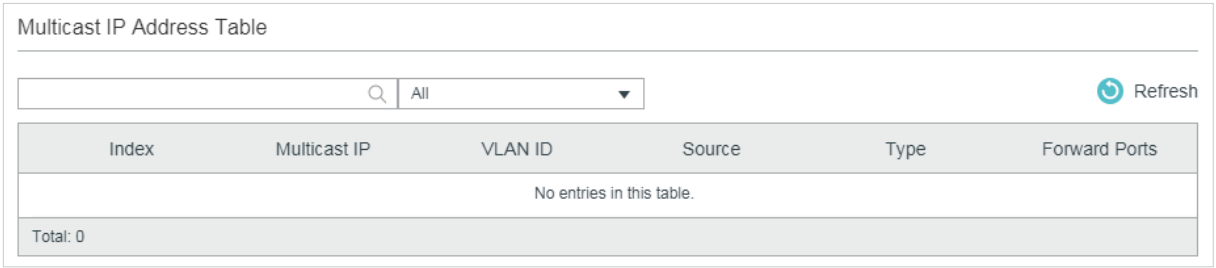
- View IPv4 multicast table.
- View IPv4 multicast statistics on each port.
- View IPv6 multicast table.
- View IPv6 multicast statistics on each port.

6.1 Using the GUI

6.1.1 Viewing IPv4 Multicast Table

Choose the menu **L2 FEATURES > Multicast > Multicast Info > IPv4 Multicast Table** to load the following page:

Figure 6-1 IPv4 Multicast Table



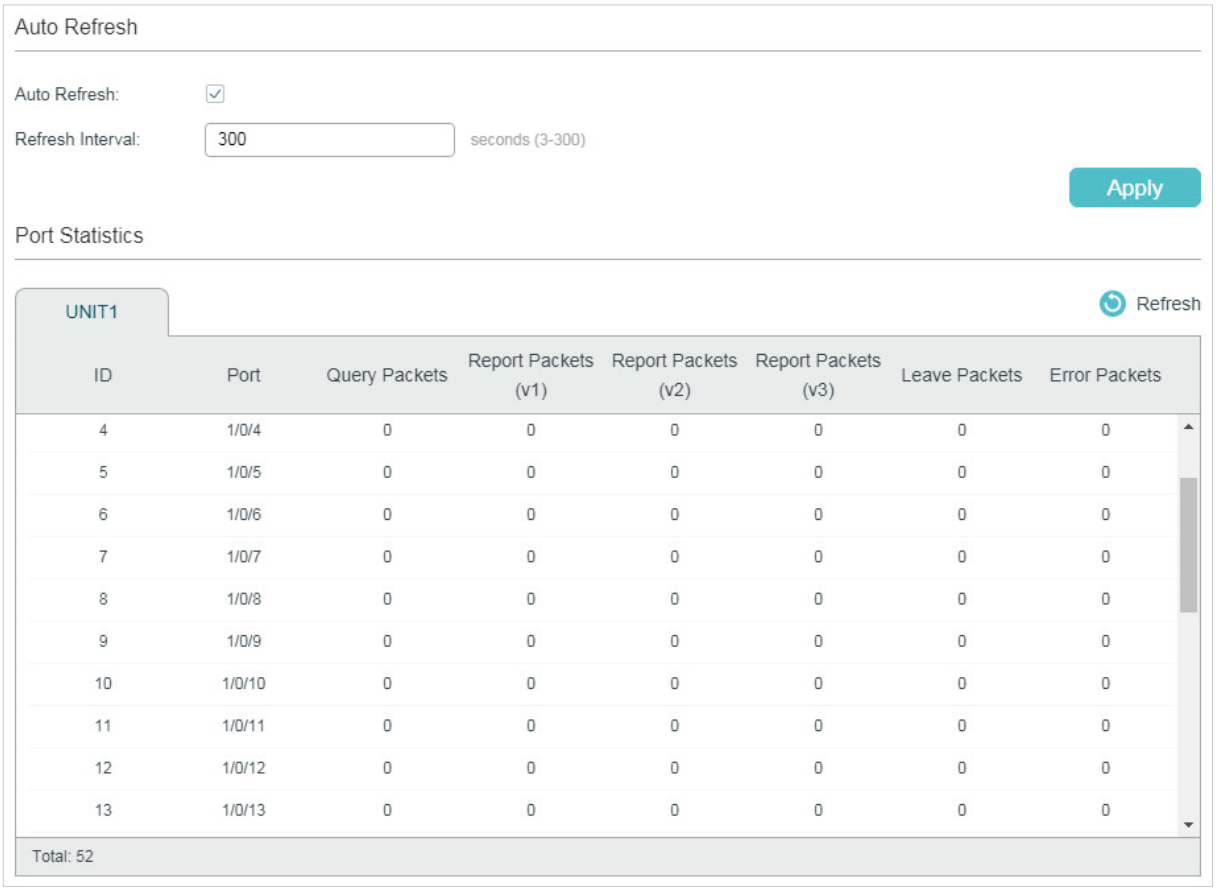
The multicast IP address table shows all valid Multicast IP-VLAN-Port entries:

Multicast IP	Displays the multicast source IP address.
VLAN ID	Displays the ID of the VLAN the multicast group belongs to.
Source	Displays whether the multicast group is learned dynamically or added manually.
Type	Displays whether the multicast group is managed by IGMP Snooping or MVR.
Forward Ports	All ports in the multicast group, including router ports and member ports.

6.1.2 Viewing IPv4 Multicast Statistics on Each Port

Choose the menu **L2 FEATURES > Multicast > Multicast Info > IPv4 Multicast Statistics** to load the following page:

Figure 6-2 IPv4 Multicast Statistics



Follow these steps to view IPv4 multicast statistics on each port:

1) To get the real-time multicast statistics, enable **Auto Refresh**, or click **Refresh**.

Auto Refresh	Enable or disable Auto Refresh. When enabled, the switch will automatically refresh the multicast statistics.
Refresh Interval	After **Auto Refresh** is enabled, specify the time interval for the switch to refresh the multicast statistics.

2) In the **Port Statistics** section, view IPv4 multicast statistics on each port.

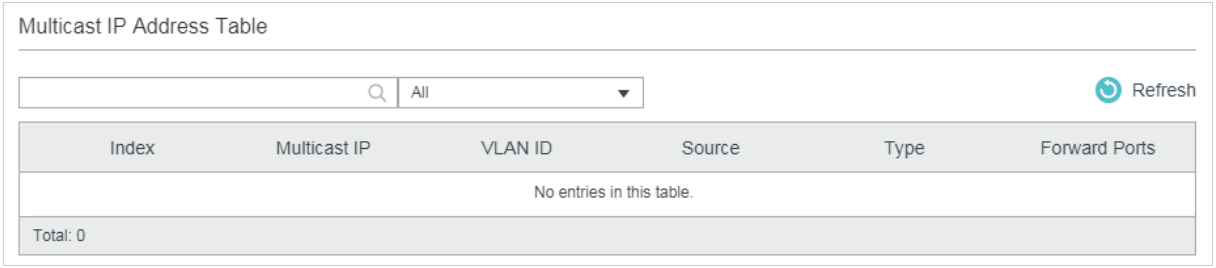
Query Packets	Displays the number of query packets received by the port.
Report Packets (v1)	Displays the number of IGMPv1 report packets received by the port.
Report Packets (v2)	Displays the number of IGMPv2 report packets received by the port.

Report Packets (v3)	Displays the number of IGMPv3 report packets received by the port.
Leave Packets	Displays the number of leave packets received by the port.
Error Packets	Displays the number of error packets received by the port.

6.1.3 Viewing IPv6 Multicast Table

Choose the menu **L2 FEATURES > Multicast > Multicast Info > IPv6 Multicast Table** to load the following page:

Figure 6-3 IPv6 Multicast Table



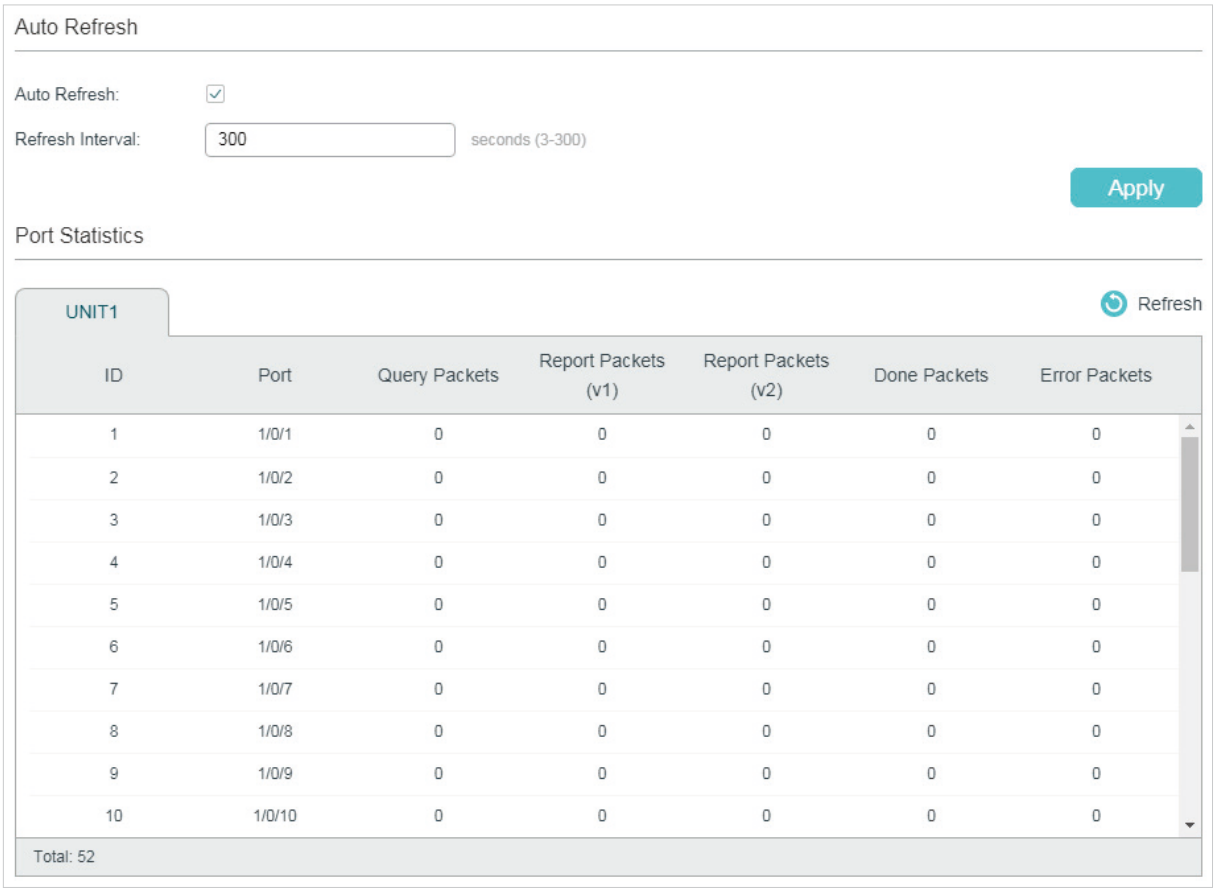
The multicast IP address table shows all valid Multicast IP-VLAN-Port entries:

Multicast IP	Displays the multicast source IP address.
VLAN ID	Displays the ID of the VLAN the multicast group belongs to.
Source	Displays whether the multicast group is learned dynamically or added manually.
Type	Displays whether the multicast group is managed by IGMP Snooping or MVR. All the IPv6 multicast groups are managed by MLD Snooping.
Forward Port	All ports in the multicast group, including router ports and member ports.

6.1.4 Viewing IPv6 Multicast Statistics on Each Port

Choose the menu **L2 FEATURES > Multicast > Multicast Info > IPv6 Multicast Statistics** to load the following page:

Figure 6-4 IPv6 Multicast Statistics



Follow these steps to view IPv6 multicast statistics on each port:

1) To get the real-time IPv6 multicast statistics, enable **Auto Refresh**, or click **Refresh**.

Auto Refresh	Enable or disable Auto Refresh. When enabled, the switch will automatically refresh the multicast statistics.
Refresh Interval	After **Auto Refresh** is enabled, specify the time interval for the switch to refresh the multicast statistics.

2) In the **Port Statistics** section, view IPv6 multicast statistics on each port.

Query Packets	Displays the number of query packets received by the port.
Report Packets (v1)	Displays the number of MLDv1 packets received by the port.
Report Packets (v2)	Displays the number of MLDv2 packets received by the port.

Done Packets	Displays the number of done packets received by the port.
Error Packets	Displays the number of error packets received by the port.

6.2 Using the CLI

6.2.1 Viewing IPv4 Multicast Snooping Information

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 multicast groups.

static: Displays information of all static multicast groups.

static count: Displays the number of static multicast groups.

show ip igmp snooping interface [fastEthernet [*port-list*] **| gigabitEthernet** [*port-list*] **| ten-gigabitEthernet** [*port-list*] **] packet-stat**

Displays the packet statistics on specified ports or all ports.

clear ip igmp snooping statistics

Clear all statistics of all IGMP packets.

6.2.2 Viewing IPv6 Multicast Snooping Configurations

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 interface [fastEthernet [*port-list*] **| gigabitEthernet** [*port-list*] **| ten-gigabitEthernet** [*port-list*] **] packet-stat**

Displays the packet statistics on specified ports or all ports.

clear ipv6 mld snooping statistics

Clear all statistics of all MLD packets.

7 Configuration Examples

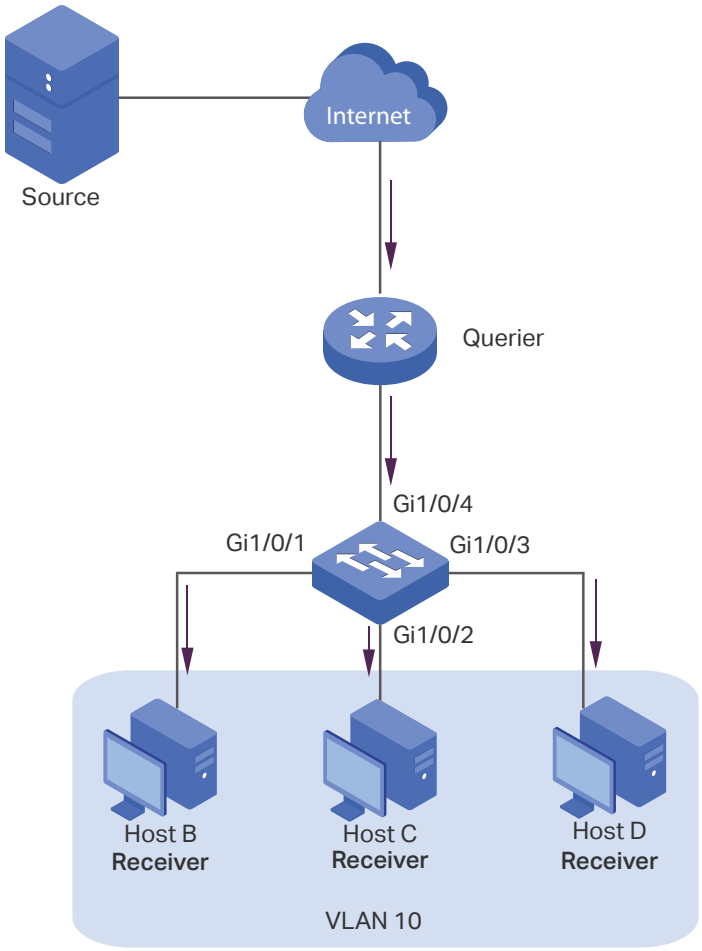
7.1 Example for Configuring Basic IGMP Snooping

7.1.1 Network Requirements

Host B, Host C and Host D are in the same VLAN of the switch. All of them want to receive multicast streams 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 7-1 Network Topology for Basic IGMP Snooping



7.1.2 Configuration Scheme

- Add the three member ports and the router port to a VLAN and configure their PVIDs.
- Enable IGMP Snooping globally and in the VLAN.

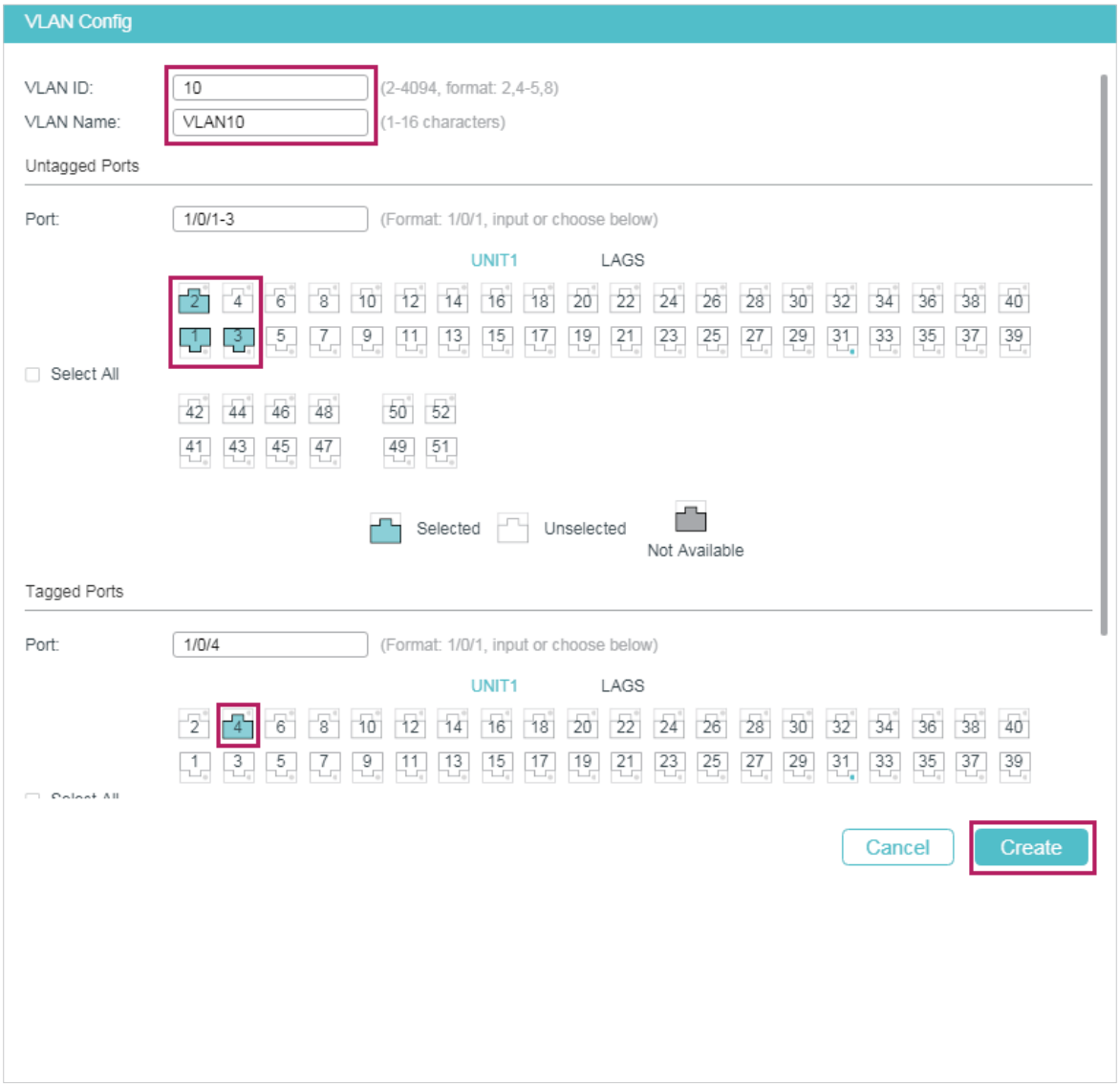
- Enable IGMP Snooping on the ports.

Demonstrated with T1600G-52TS, this section provides configuration procedures in two ways: using the GUI and using the CLI.

7.1.3 Using the GUI

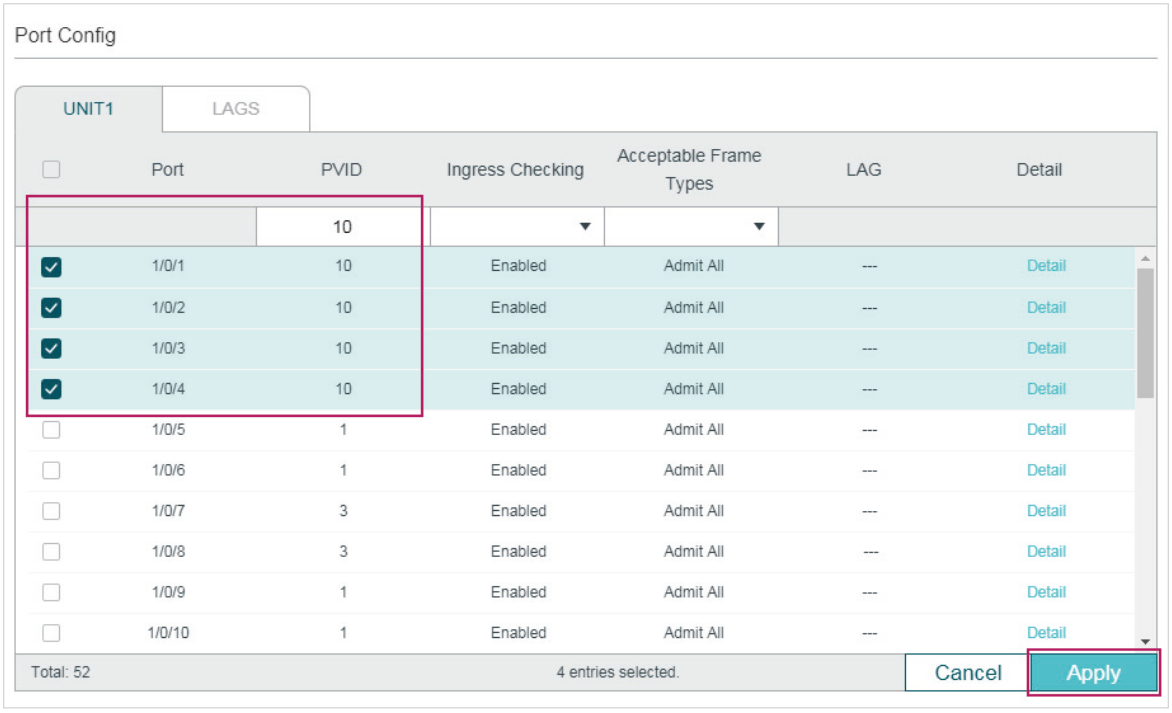
1) Choose the menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** and click Add to load the following page. Create VLAN 10 and add Untagged port 1/0/1-3 and Tagged port 1/0/4 to VLAN 10.

Figure 7-2 Create VLAN 10



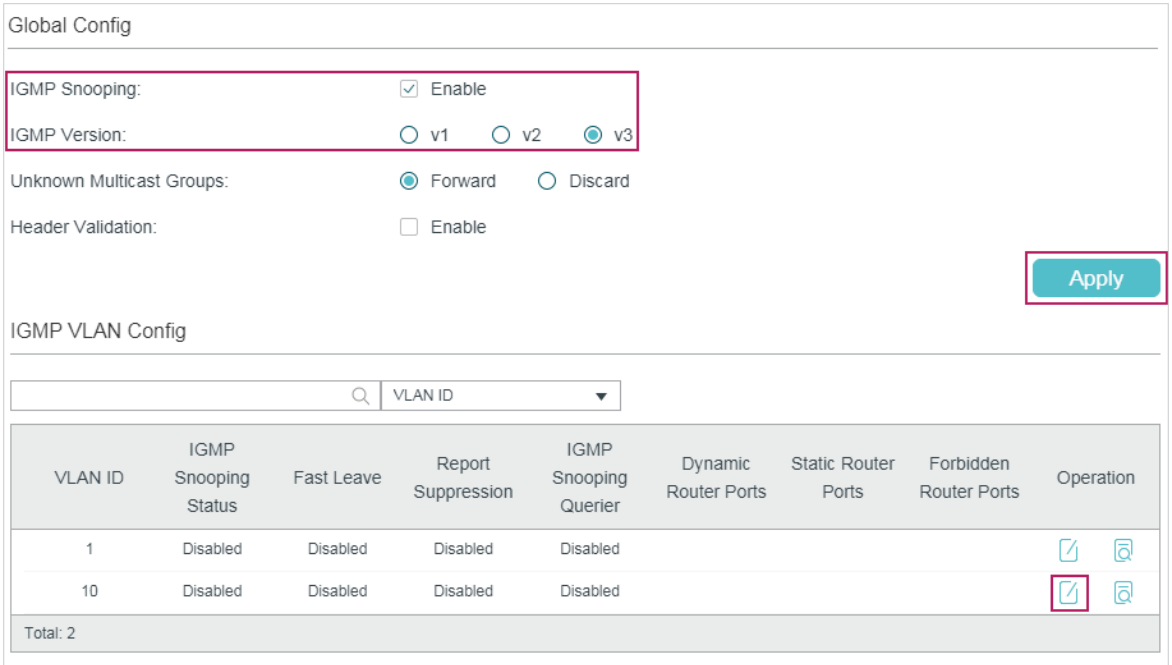
2) Choose the menu **L2 FEATURES > VLAN > 802.1Q VLAN > Port Config** to load the following page. Configure the PVID of port 1/0/1-4 as 10.

Figure 7-3 Configure PVID for the Ports



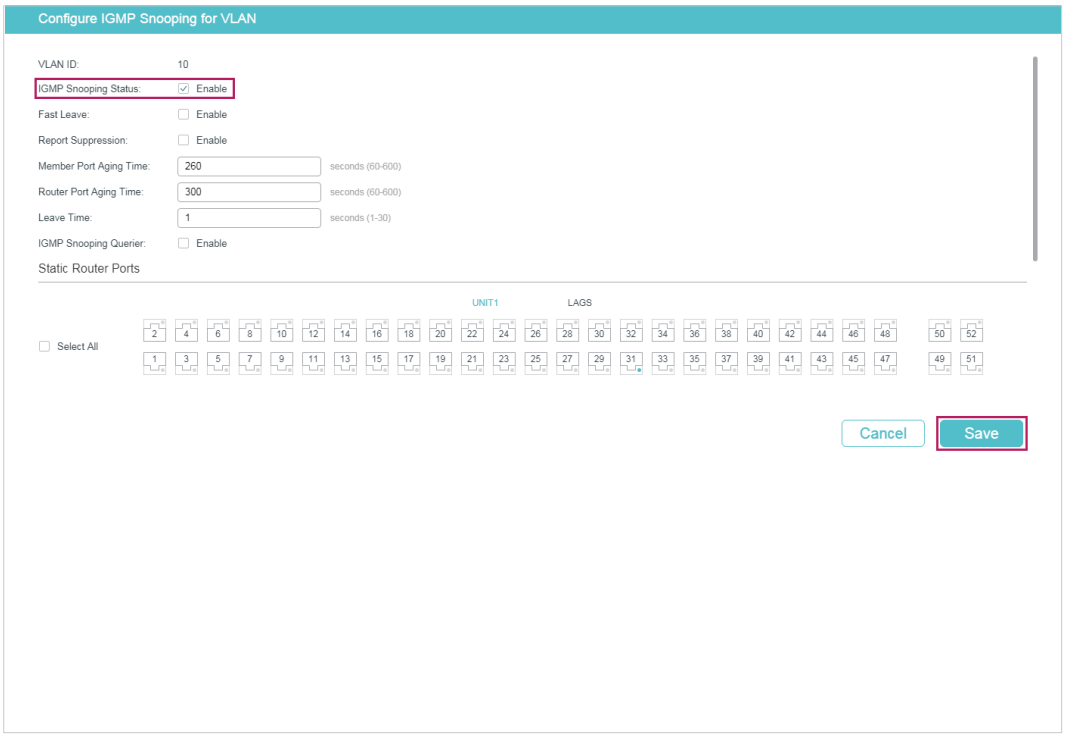
3) Choose the menu **L2 FEATURES > Multicast > IGMP Snooping > Global Config** to load the following page. In the **Global Config** section, enable IGMP Snooping globally. Configure the IGMP version as v3 so that the switch can process IGMP messages of all versions. Then click **Apply**.

Figure 7-4 Configure IGMP Snooping Globally



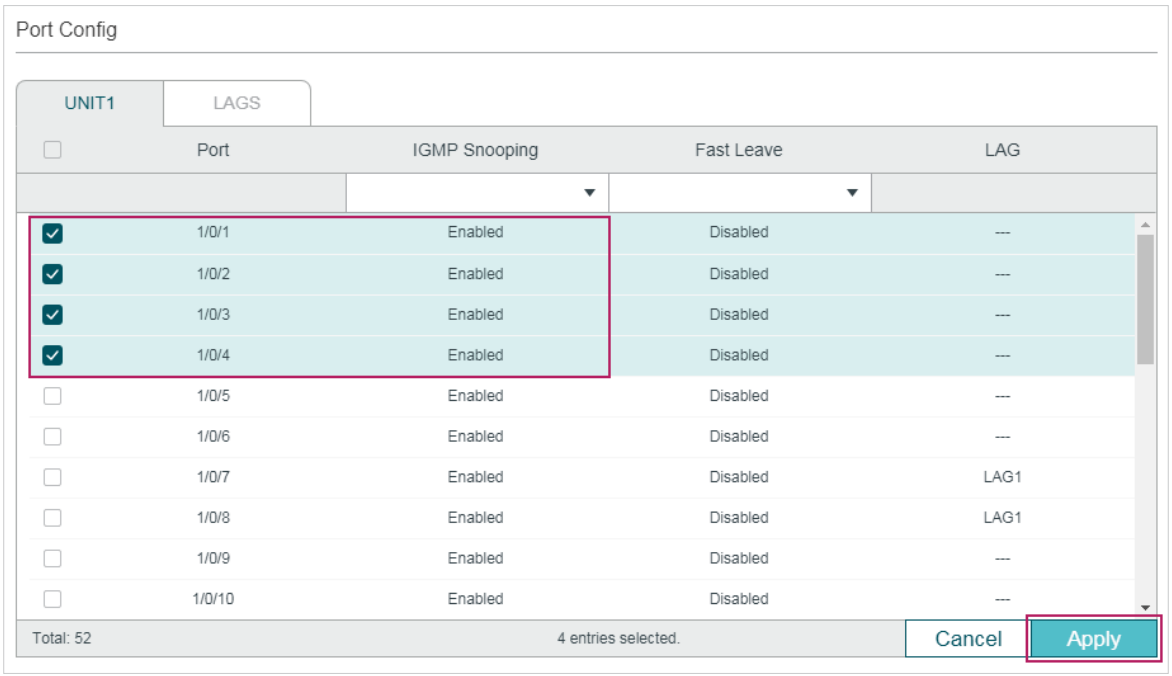
4) In the **IGMP VLAN Config** section, click in VLAN 10 to load the following page. Enable IGMP Snooping for VLAN 10.

Figure 7-5 Enable IGMP Snooping on the Ports



5) Choose the menu **L2 FEATURES > Multicast > IGMP Snooping > Port Config** to load the following page. Enable IGMP Snooping for ports 1/0/1-4.

Figure 7-6 Enable IGMP Snooping in the VLAN



6) Click Save to save the settings.

7.1.4 Using the CLI

1) Create VLAN 10.

Switch#configure

Switch(config)#vlan 10

Switch(config-vlan)#name vlan10

Switch(config-vlan)#exit

2) 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

3) 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

4) Enable IGMP Snooping globally.

Switch(config)#ip igmp snooping

5) Enable IGMP Snooping in VLAN 10.

Switch(config)#ip igmp snooping vlan-config 10

6) 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

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

IGMP Version :V3

Header Validation :Disable

Global Authentication Accounting :Disable

Enable Port : Gi1/0/1-4

Enable VLAN:10

7.2 Example for Configuring MVR

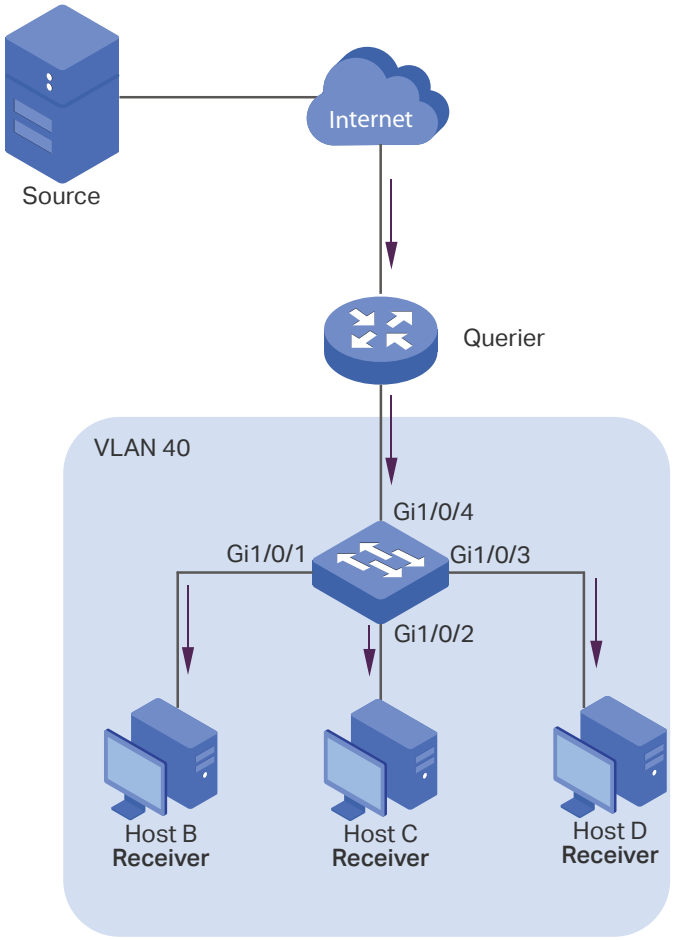
7.2.1 Network Requirements

Host B, Host C and Host D are in three different VLANs of the switch. All of them want to receive multicast streams sent to multicast group 225.1.1.1.

7.2.2 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.

Figure 7-7 Network Topoloy for Multicast VLAN



7.2.3 Configuration Scheme

As the hosts are in different VLANs, in IGMP Snooping, the Querier need to duplicate multicast streams for hosts in each VLAN. To avoid duplication of multicast streams being sent between Querier and the switch, you can configure MVR on the switch.

The switch can work in either MVR compatible mode or MVR dynamic mode. When in compatible mode, remember to statically configure the Querier to transmit the streams of multicast group 225.1.1.1 to the switch via the multicast VLAN. Here we take the MVR dynamic mode as an example.

Demonstrated with T1600G-52TS, this section provides configuration procedures in two ways: using the GUI and using the CLI.

7.2.4 Using the GUI

1) Add port 1/0/1-3 to VLAN 10, VLAN 20 and VLAN 30 as Untagged ports respectively, and configure the PVID of port 1/0/1 as 10, port 1/0/2 as 20, port 1/0/3 as 30. Make sure port1/0/1-3 only belong to VLAN 10, VLAN 20 and VLAN 30 respectively. For details, refer to *Configuring 802.1Q VLAN*.

Figure 7-8 VLAN Configurations for Port 1/0/1-3

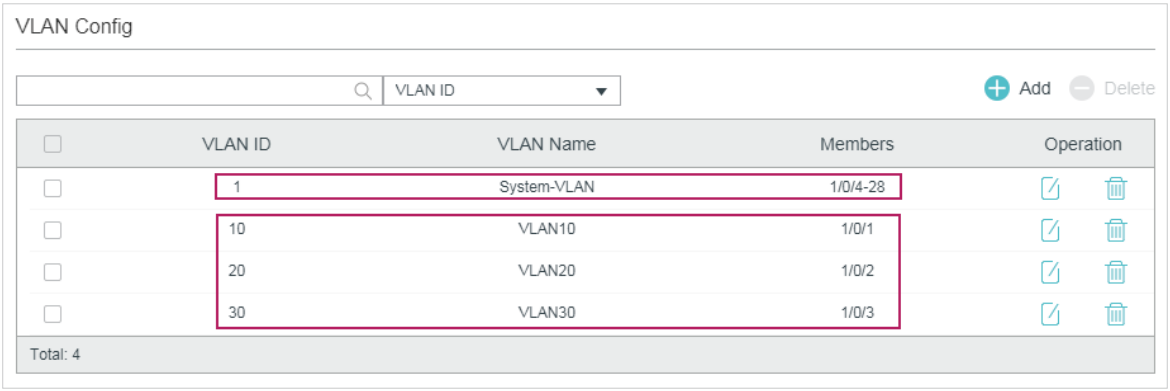
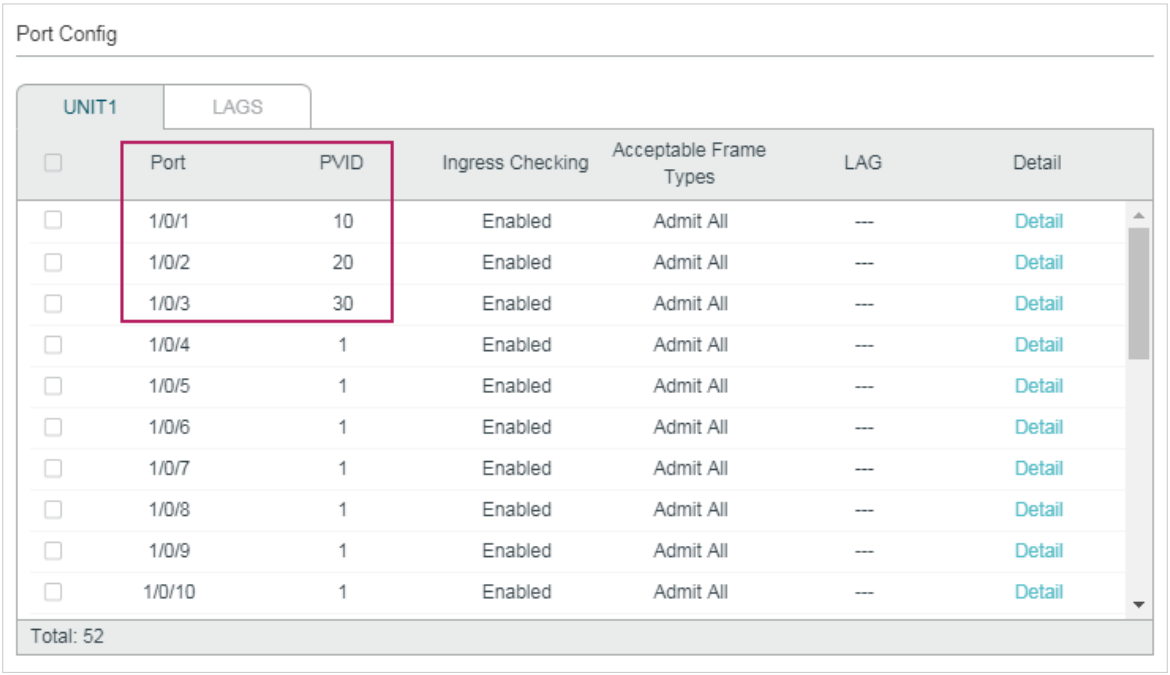
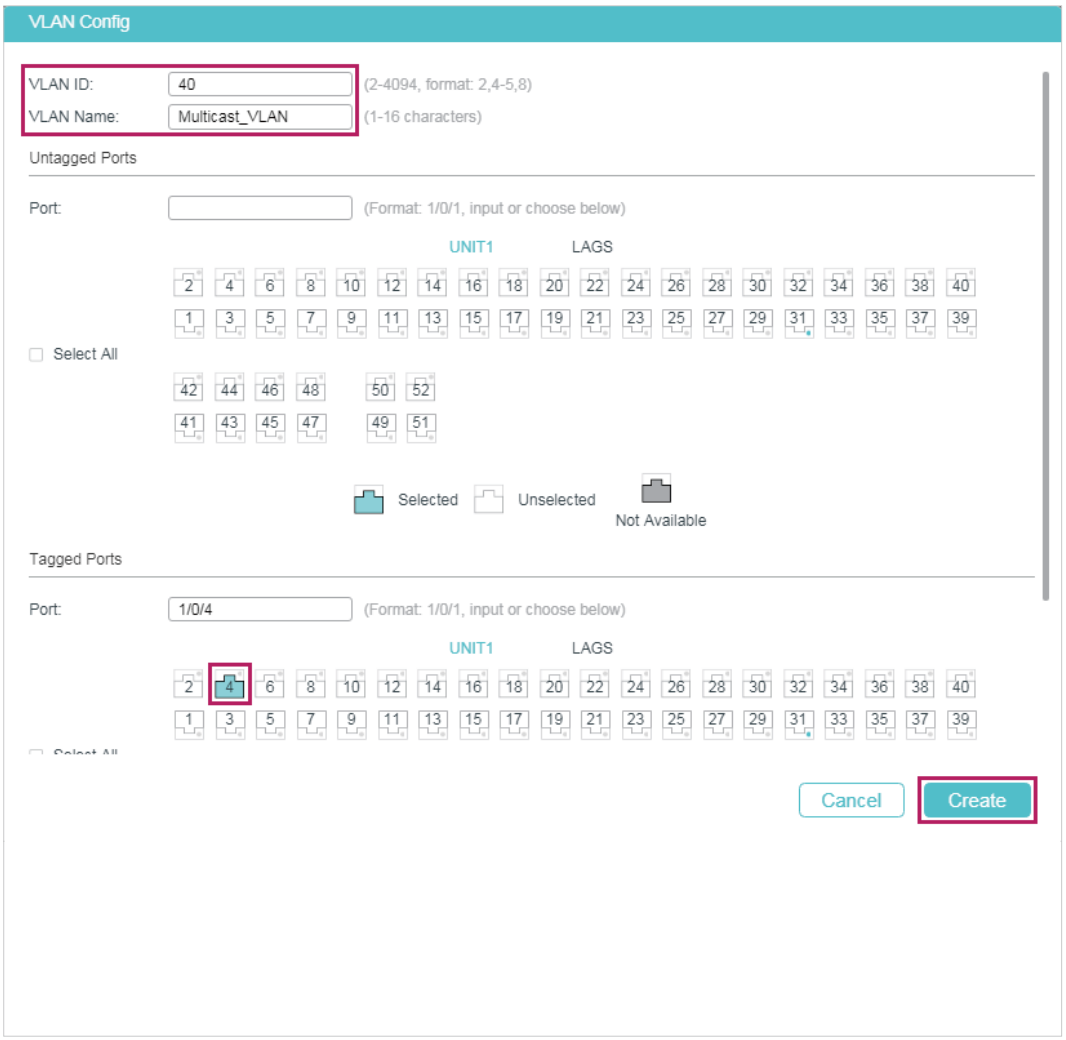


Figure 7-9 PVID for Port 1/0/1-3



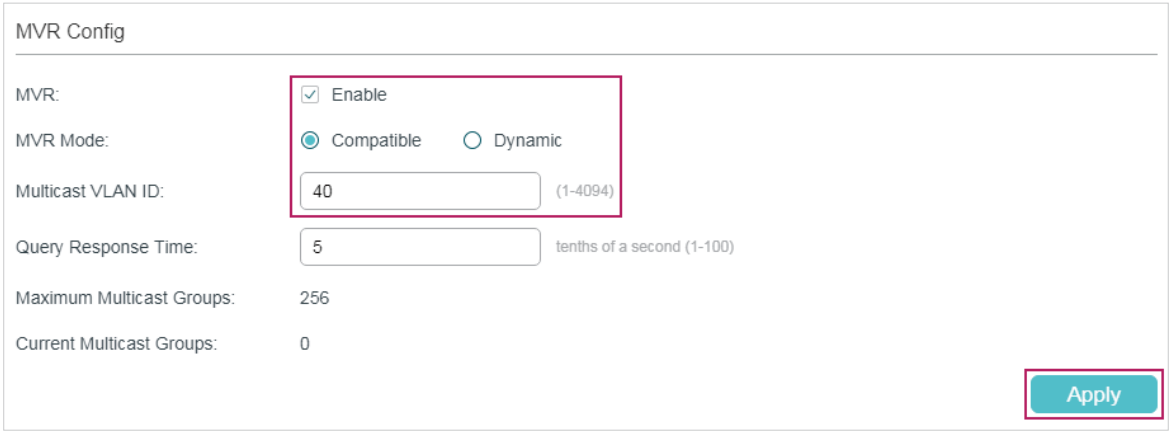
2) Choose the menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** and click Add to load the following page. Create VLAN 40 and add port 1/0/4 to the VLAN as Tagged port.

Figure 7-10 Create Multicast VLAN



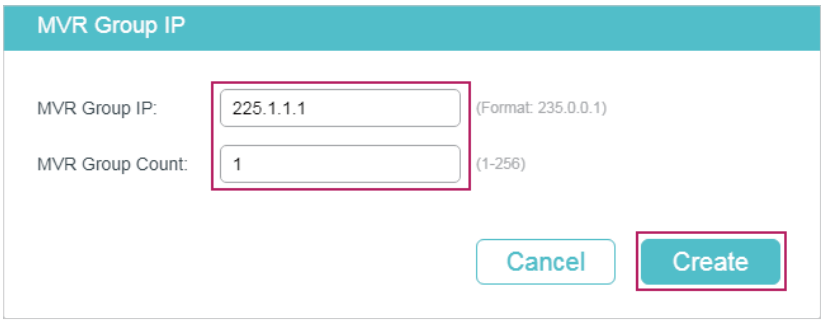
3) Choose the menu **L2 FEATURES > Multicast > MVR > MVR Config** to load the following page. Enable MVR globally, and configure the MVR mode as **Dynamic**, multicast VLAN ID as **40**.

Figure 7-11 Configure MVR Globally



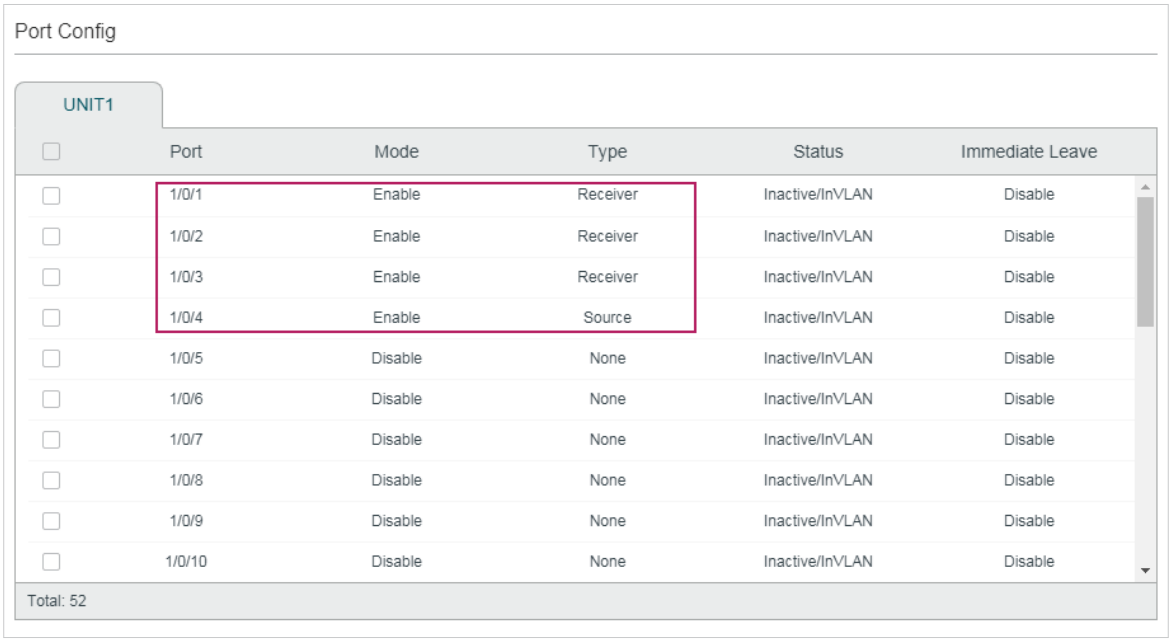
4) Choose the menu **L2 FEATURES > Multicast > MVR > MVR Group Config** and click Add to load the following page. Add multicast group 225.1.1.1 to MVR.

Figure 7-12 Add Multicast Group to MVR



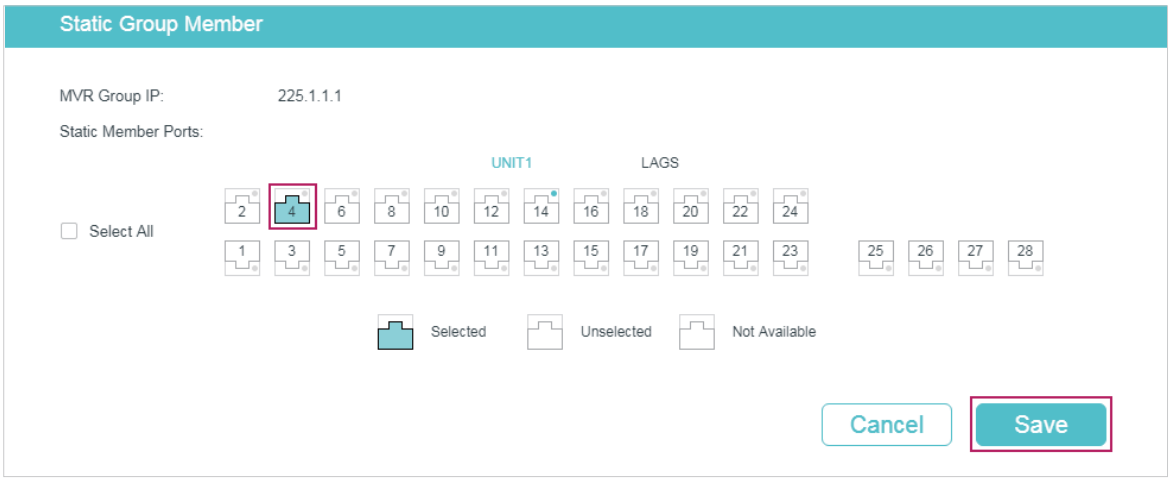
5) Choose the menu **L2 FEATURES > Multicast > MVR > Port Config** to load the following page. Enable MVR for port 1/0/1-4. Configure port 1/0/1-3 as **Receiver** ports and port 1/0/4 as **Source** port.

Figure 7-13 Configure MVR for the Ports



6) Choose the menu **L2 FEATURES > Multicast > MVR > Static Group Members** and click in the group 225.1.1.1 entry to load the following page. Select port 1/0/4 to statically add it to the group and click **Save**.

Figure 7-14 Statically Add Port 1/0/4 to the Group



7) Click Save to save the settings.

7.2.5 Using the CLI

1) Create VLAN 10, VLAN 20, VLAN 30 and VLAN 40.

Switch#configure

Switch(config)#vlan 10,20,30,40

Switch(config-vlan)#exit

2) Add port 1/0/1-3 to VLAN 10, VLAN 20 and VLAN 30 as untagged ports respectively, and configure the PVID of port 1/0/1 as 10, port 1/0/2 as 20, port 1/0/3 as 30. Add port 1/0/4 to VLAN 40 as tagged port and configure the PVID as of port 1/0/4 as 40.

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

Switch(config-if)#switchport general allowed vlan 10 untagged

Switch(config-if)#switchport pvid 10

Switch(config-if)#exit

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

Switch(config-if)#switchport general allowed vlan 20 untagged

Switch(config-if)#switchport pvid 20

Switch(config-if)#exit

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

Switch(config-if)#switchport general allowed vlan 30 untagged

Switch(config-if)#switchport pvid 30

Switch(config-if)#exit

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

Switch(config-if)#switchport general allowed vlan 40 tagged

Switch(config-if)#switchport pvid 40

Switch(config-if)#exit

3) Check whether port1/0/1-3 only belong to VLAN 10, VLAN 20 and VLAN 30 respectively. If not, delete them from the other VLANs. By default, all ports are in VLAN 1, so you need to delete them from VLAN 1.

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
20	VLAN20	active	Gi1/0/2
30	VLAN30	active	Gi1/0/3
40	VLAN40	active	Gi1/0/4

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

Switch(config-if-range)#no switchport general allowed vlan 1

Switch(config-if-range)#exit

4) Enable MVR globally, and configure the MVR mode as **Dynamic**, multicast VLAN ID as **40**. Add multicast group 225.1.1.1 to MVR.

Switch(config)#mvr

Switch(config)#mvr mode dynamic

Switch(config)#mvr vlan 40

Switch(config)#mvr group 225.1.1.1 1

5) Enable MVR for port 1/0/1-4. Configure port 1/0/1-3 as **Receiver** ports and port 1/0/4 as **Source** port. Then statically add port 1/0/4 to group 225.1.1.1.

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

Switch(config-if-range)#mvr

Switch(config-if-range)#mvr type receiver

Switch(config-if-range)#exit

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

Switch(config-if)#mvr

Switch(config-if)#mvr type source

Switch(config-if)#mvr vlan 40 group 225.1.1.1

Switch(config-if)#exit

6) Save the settings.

Switch(config)#end

Switch#copy running-config startup-config

Verify the Configurations

Show the brief information of all VLANs:

Switch(config)#show vlan brief

VLAN	Name	Status	Ports
1	System-VLAN	active	Gi1/0/4, Gi1/0/5, Gi1/0/6, Gi1/0/7, ...
10	VLAN10	active	Gi1/0/1
20	VLAN20	active	Gi1/0/2
30	VLAN30	active	Gi1/0/3
40	VLAN40	active	Gi1/0/4

Show the brief information of MVR:

Switch(config)#show mvr

MVR	:Enable
MVR Multicast Vlan	:40
MVR Max Multicast Groups	:256
MVR Current Multicast Groups	:1
MVR Global Query Response Time	:5 (tenths of sec)
MVR Mode Type	:Dynamic

Show the membership of MVR groups:

Switch(config)#show mvr members

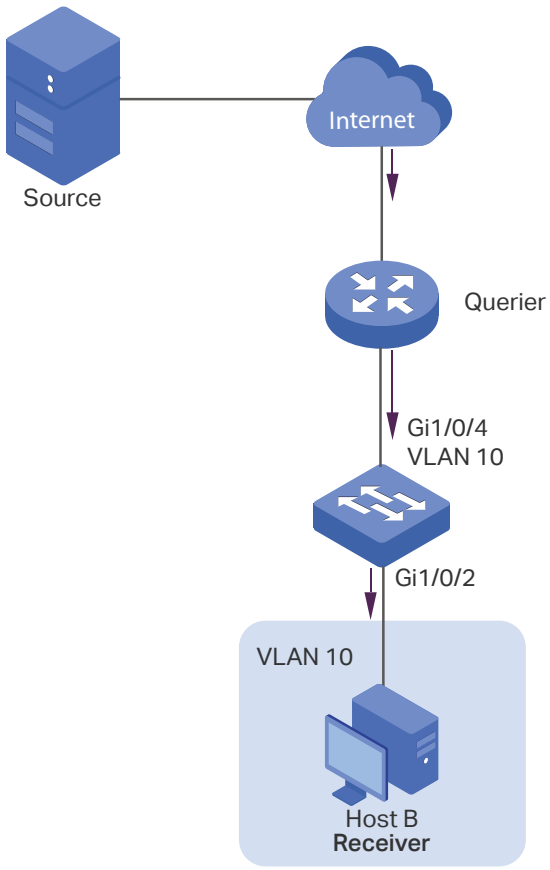
MVR Group IP	Status	Members
225.1.1.1	active	Gi1/0/4

7.3 Example for Configuring Unknown Multicast and Fast Leave

7.3.1 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 7-15 Network Topology for Unknow Multicast and Fast Leave



7.3.2 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.

To avoid Host B from receiving irrelevant multicast data, you can enable Fast Leave on port 1/0/2 and configure the switch to discard unknown multicast data. To change channel, Host B sends a leave message about leaving the previous channel. With Fast Leave

enabled on port 1/0/2, the switch will then drop multicast data from the previous channel, which ensures that Host B only receives multicast data from the new channel and that the multicast network is unimpeded.

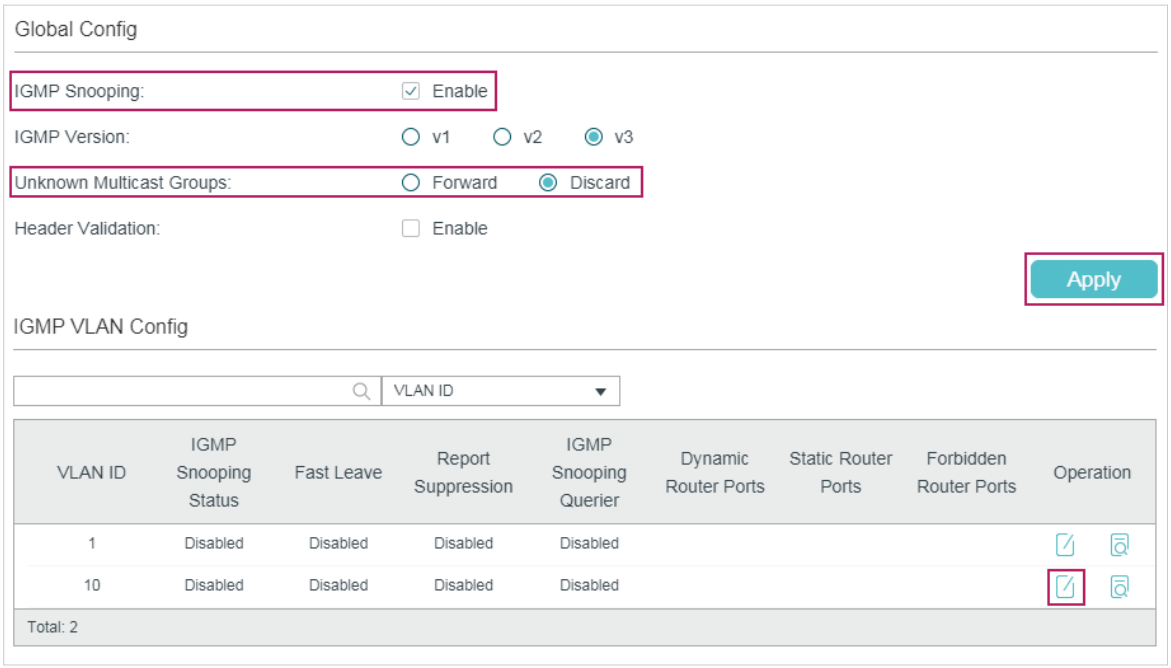
Demonstrated with T1600G-52TS, this section provides configuration procedures in two ways: using the GUI and using the CLI.

7.3.3 Using the GUI

1) Create VLAN 10. Add port 1/0/2 to the VLAN as untagged port and port 1/0/4 as tagged port. Configure the PVID of the two ports as 10. For details, refer to *Configuring 802.1Q VLAN*.

2) Choose the menu **L2 FEATURES > Multicast > IGMP Snooping > Global Config** to load the following page. In the **Global Config** section, enable IGMP Snooping globally and configure Unknown Multicast Groups as **Discard**.

Figure 7-16 Configure IGMP Snooping Globally

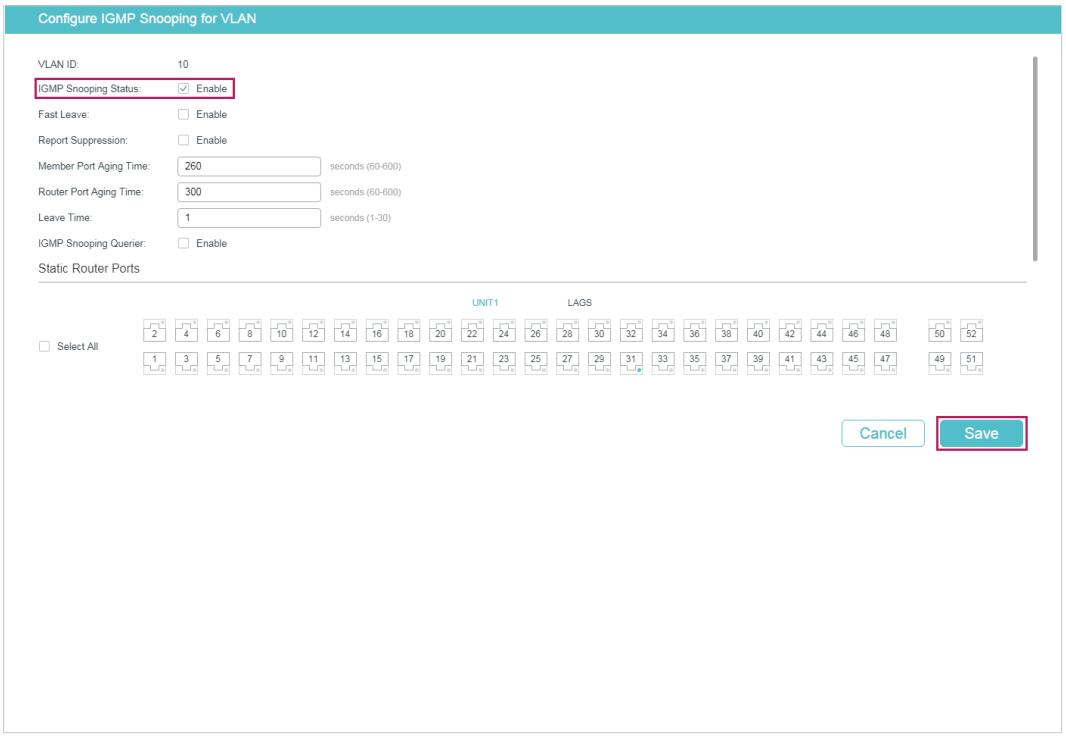


Note:

IGMP Snooping and MLD Snooping share the setting of Unknown Multicast, so you have to enable MLD Snooping globally on the **L2 FEATURES > Multicast > MLD Snooping > Global Config** page at the same time.

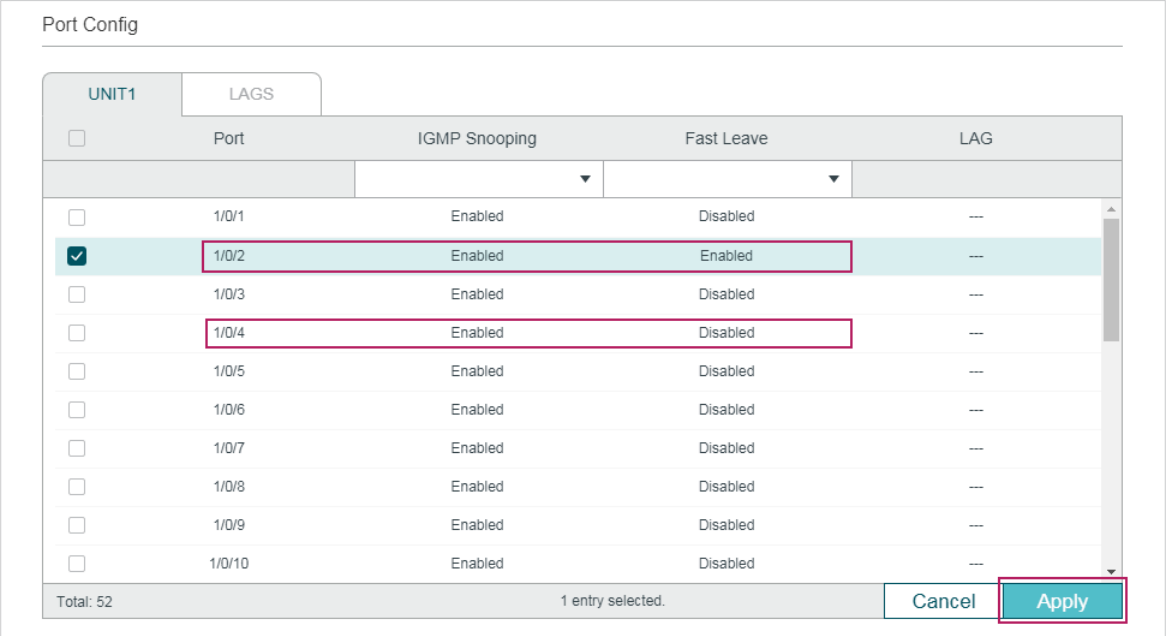
3) In the **IGMP VLAN Config** section, click in VLAN 10 to load the following page. Enable IGMP Snooping for VLAN 10.

Figure 7-17 Enable IGMP Snooping for VLAN 10



4) Choose the menu **L2 FEATURES > 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 7-18 Configure IGMP Snooping on Ports



5) Click Save to save the settings.

7.3.4 Using the CLI

1) Enable IGMP Snooping and MLD Snooping globally.

Switch#configure

Switch(config)#ip igmp snooping

Switch(config)#ipv6 mld snooping

2) Configure Unknown Multicast Groups 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

IGMP Version :V3

Unknown Multicast :Discard

...

Enable Port: Gi1/0/1-28

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

7.4 Example for Configuring Multicast Filtering

7.4.1 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.

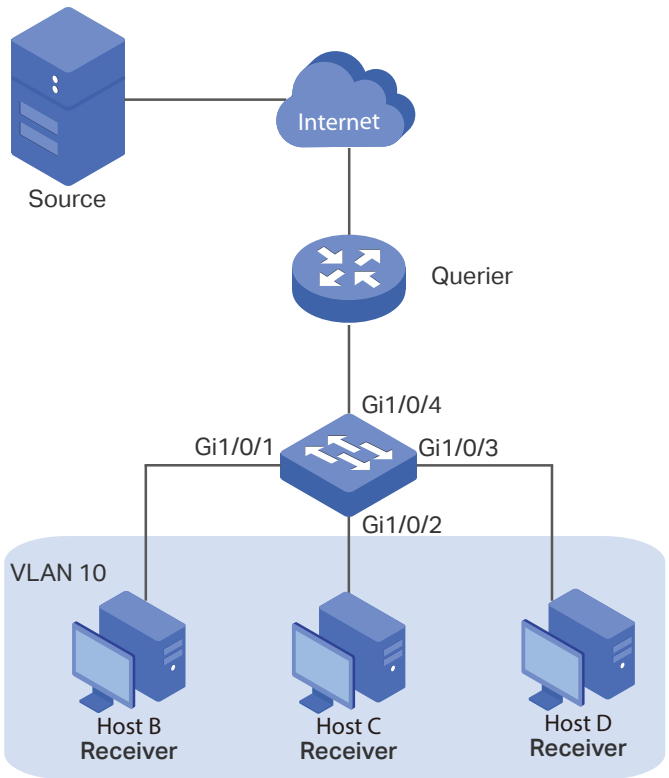
7.4.2 Configuration Scheme

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.

7.4.3 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 7-19 Network Topology for Multicast Filtering



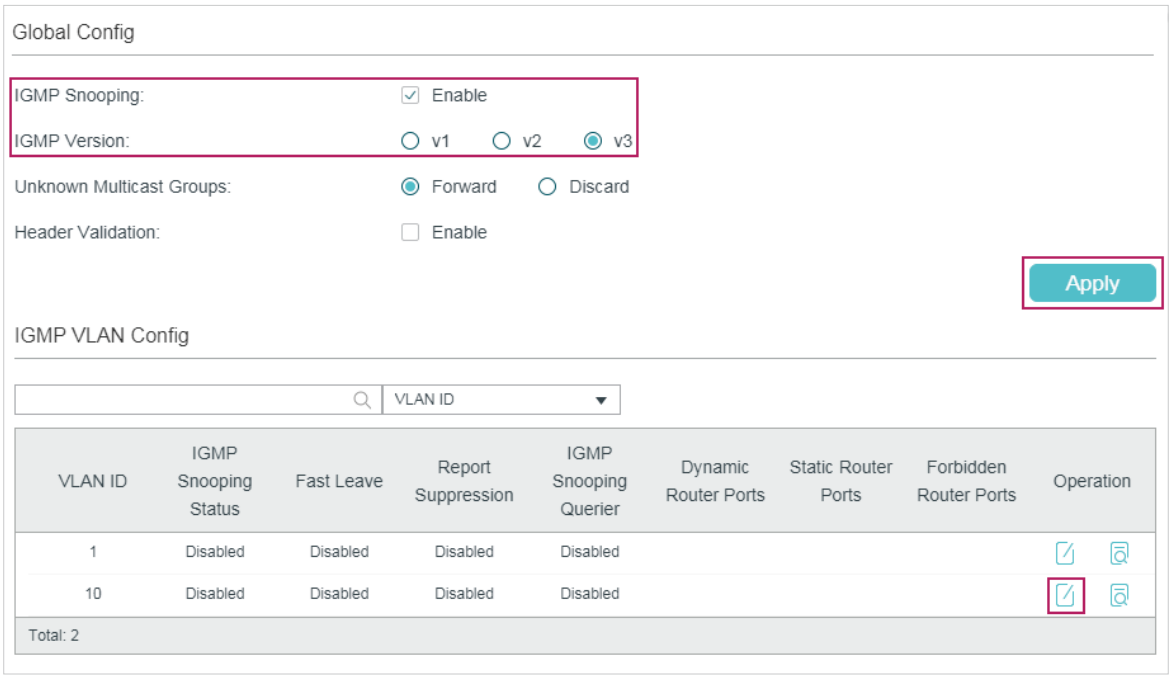
Demonstrated with T1600G-52TS, this section provides configuration procedures in two ways: using the GUI and using the CLI.

7.4.4 Using the GUI

1) Create VLAN 10. Add port 1/0/1-3 to the VLAN as untagged port and port 1/0/4 as tagged port. Configure the PVID of the four ports as 10. For details, refer to *Configuring 802.1Q VLAN*.

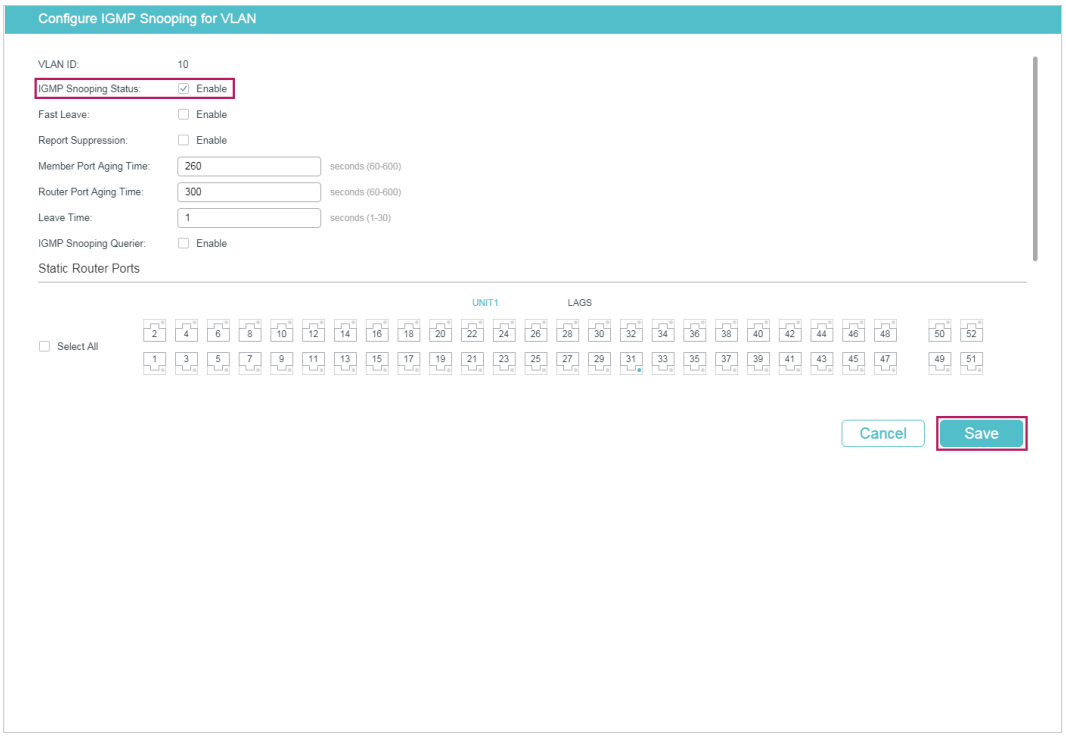
2) Choose the menu **L2 FEATURES > Multicast > IGMP Snooping > Global Config** to load the following page. In the **Global Config** section, enable IGMP Snooping globally.

Figure 7-20 Enable IGMP Snooping Globally



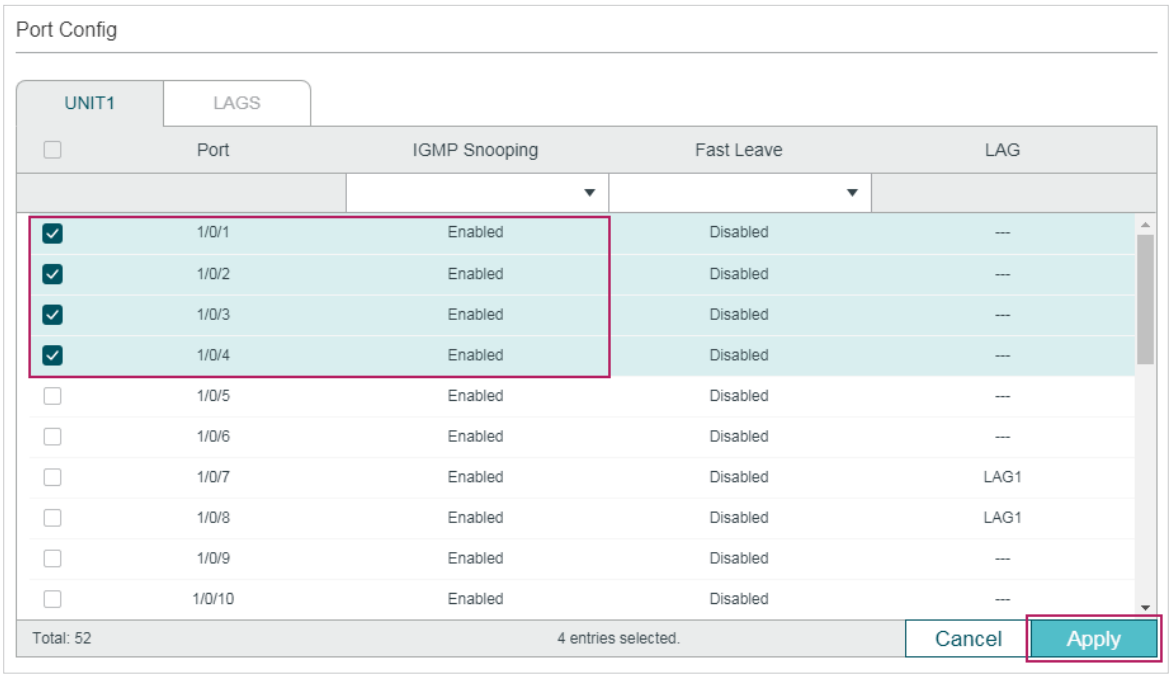
3) In the **IGMP VLAN Config** section, click in VLAN 10 to load the following page. Enable IGMP Snooping for VLAN 10.

Figure 7-21 Enable IGMP Snooping for VLAN 10



4) Choose the menu **L2 FEATURES > Multicast > IGMP Snooping > Port Config** to load the following page.

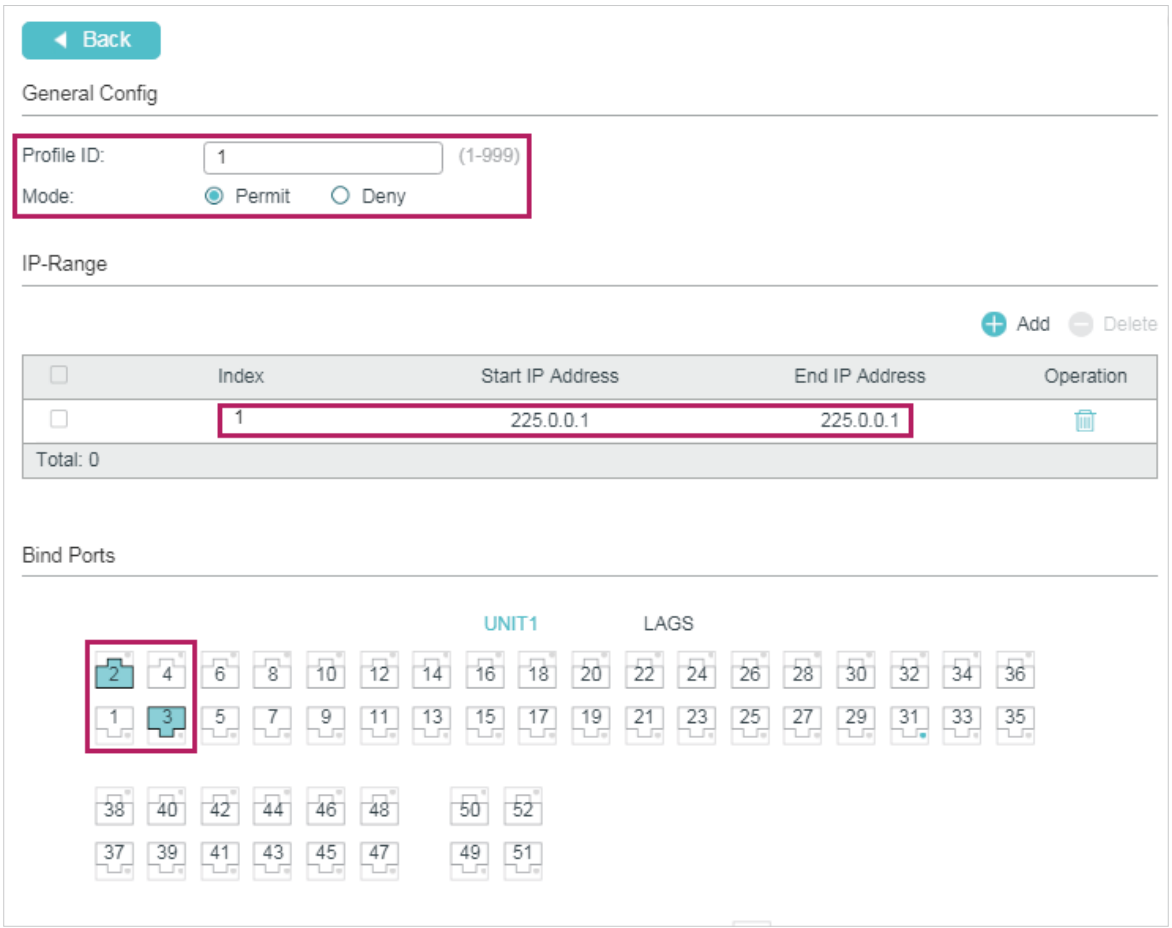
Figure 7-22 Enable IGMP Snooping on the Port



5) Choose the menu **L2 FEATURES > Multicast > Multicast Filtering > IPv4 Profile** and click Add to load the following page. Create Profile 1, specify the mode as

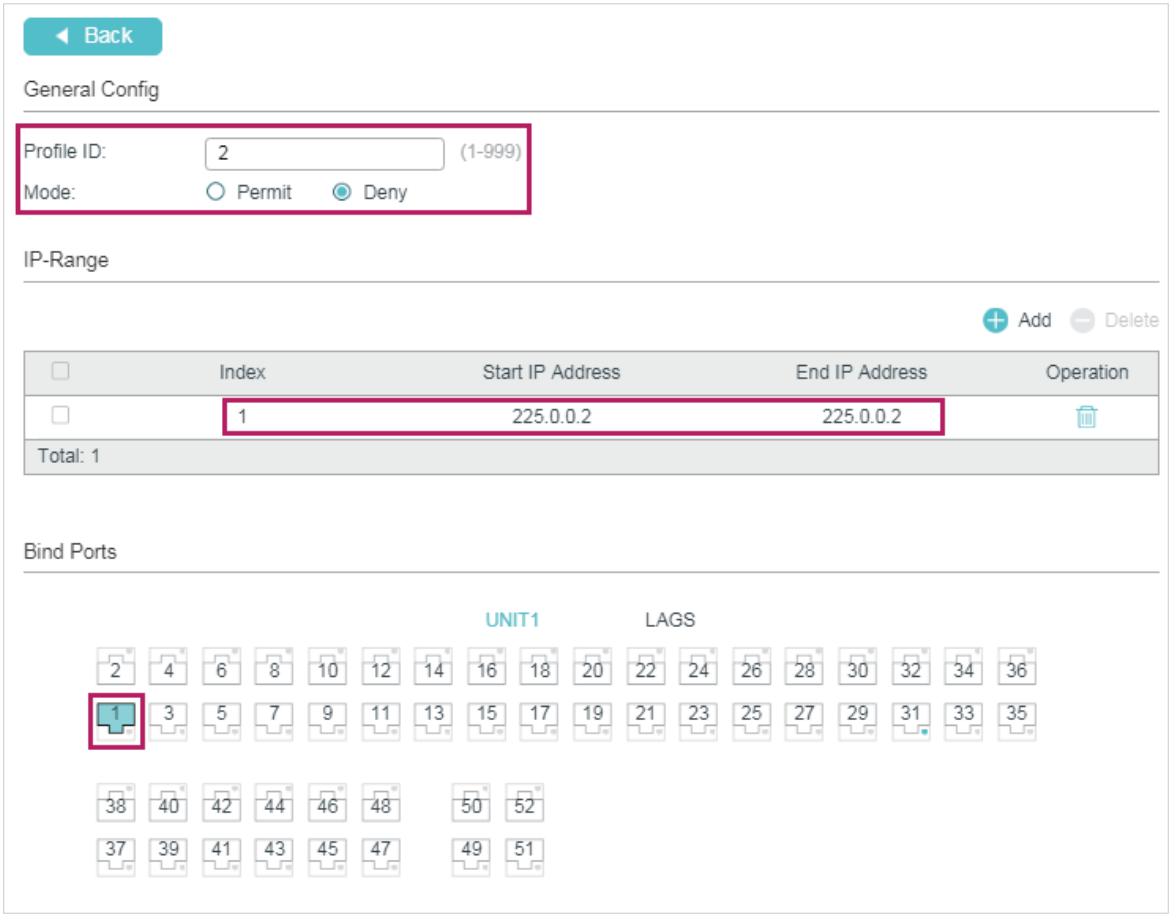
Permit, bind the profile to port 1/0/2-3, and specify the filtering multicast IP address as 225.0.0.1. Then click **Back** to return to the **IPv4 Profile Table** page.

Figure 7-23 Configure Filtering Profile for Host C and Host D



6) Click Add again to load the following page. Create Profile 2, specify the mode as **Deny,** bind the profile to port 1/0/1, and specify the filtering multicast IP address as 225.0.0.2.

Figure 7-24 Configure Filtering Profile for Host B



7) Click Save to save the settings.

7.4.5 Using the CLI

1) Create VLAN 10.

Switch#configure

Switch(config)#vlan 10

Switch(config-vlan)#name vlan10

Switch(config-vlan)#exit

2) 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

3) 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

4) Enable IGMP Snooping Globally.

Switch(config)#ip igmp snooping

5) Enable IGMP Snooping in VLAN 10.

Switch(config)#ip igmp snooping vlan-config 10

6) 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

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

IGMP Version :V3

...

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

8 Appendix: Default Parameters

8.1 Default Parameters for IGMP Snooping

Table 8-1 Default Parameters of IGMP Snooping

Function	Parameter	Default Setting
Global Settings of IGMP Snooping	IGMP Snooping	Disabled
	IGMP Version	v3
	Unknown Multicast Groups	Forward
	Header Validation	Disabled
IGMP Snooping Settings in the VLAN	IGMP Snooping	Disabled
	Fast Leave	Disabled
	Report Suppression	Disabled
	Member Port Aging Time	260 seconds
	Router Port Aging Time	300 seconds
	Leave Time	1 second
	IGMP Snooping Querier	Disabled
	Query Interval	60 seconds
	Maximum Response Time	10 seconds
	Last Member Query Interval	1 second
	Last Member Query Count	2
	General Query Source IP	0.0.0.0
	Static Router Ports	None
	Forbidden Router Ports	None
IGMP Snooping Settings on the Port and LAG	IGMP Snooping	Enabled
	Fast Leave	Disabled
Static Multicast Group Settings	Static Multicast Group Entries	None

8.2 Default Parameters for MLD Snooping

Table 8-2 Default Parameters of MLD Snooping

Function	Parameter	Default Setting
Global Settings of IGMP Snooping	MLD Snooping	Disabled
	Unknown Multicast Groups	Forward
MLD Snooping Settings in the VLAN	MLD Snooping	Disabled
	Fast Leave	Disabled
	Report Suppression	Disabled
	Member Port Aging Time	260 seconds
	Router Port Aging Time	300 seconds
	Leave Time	1 second
	MLD Snooping Querier	Disabled
	Query Interval	60 seconds
	Maximum Response Time	10 seconds
	Last Listener Query Interval	1 second
	Last Listener Query Count	2
	General Query Source IP	::
	Static Router Ports	None
	Forbidden Router Ports	None
MLD Snooping Settings on the Port and LAG	MLD Snooping	Enabled
	Fast Leave	Disabled
Static Multicast Group Settings	Static Multicast Group Entries	None

8.3 Default Parameters for MVR

Table 8-3 Default Parameters of MVR

Function	Parameter	Default Setting
Global Settings of MVR	MVR	Disabled
	MVR Mode	Compatible
	Multicast VLAN ID	1
	Query Response Time	5 tenths of a second
	Maximum Multicast Groups	256
MVR Group Settings	MVR Group Entries	None
MVR Settings on the Port	MVR Mode	Disabled
	MVR Port Type	None
	Fast Leave	Disabled
MVR Static Group Members	MVR Static Group Member Entries	None

8.4 Default Parameters for Multicast Filtering

Table 8-4 Default Parameters of Multicast Filtering

Function	Parameter	Default Setting
Profile Settings	IPv4 Profile and IPv6 Profile Entries	None
Multicast Filtering Settings on the Port and LAG	Bound Profile	None
	Maximum Groups	1000
	Overflow Action	Drop

Part 11

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

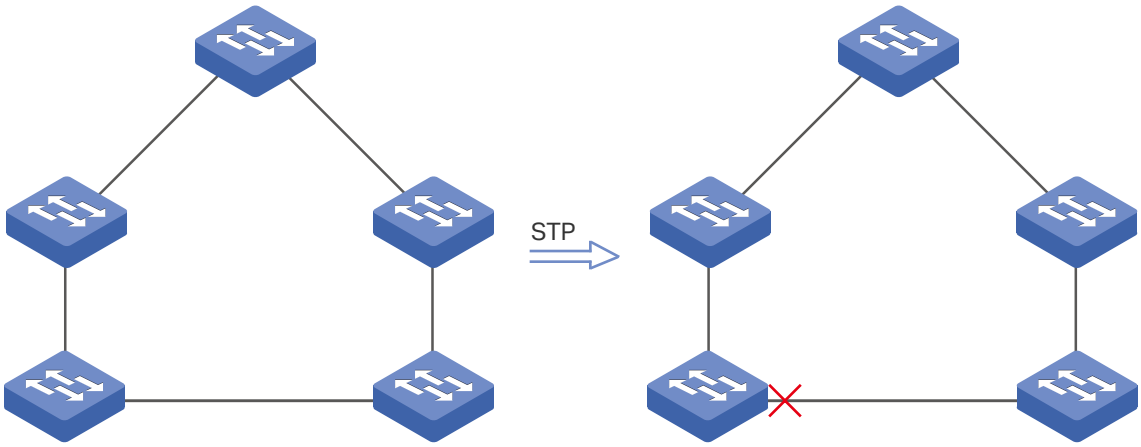
1.1 Overview

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 specific ports of the switches to build a loop-free topology.
- Detect topology changes and automatically generate a new loop-free topology.

Figure 1-1 STP Function



RSTP

RSTP (Rapid Spanning Tree Protocol) provides the same features as STP. Besides, RSTP can provide much faster spanning tree convergence.

MSTP

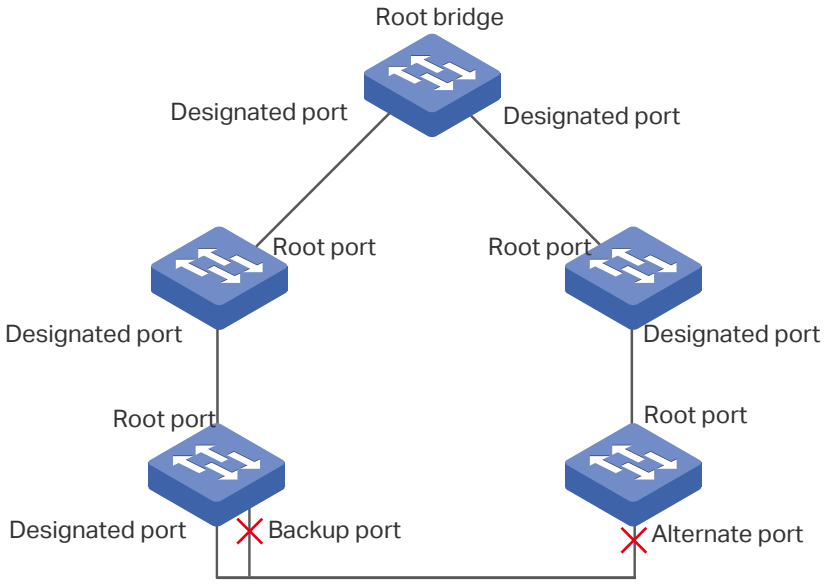
MSTP (Multiple Spanning Tree Protocol) also provides the fast spanning tree convergence as RSTP. In addition, MSTP enables VLANs to be mapped to different spanning trees (MST instances), and traffic in different VLANs will be transmitted along their respective paths, implementing load balancing.

1.2 Basic Concepts

1.2.1 STP/RSTP Concepts

Based on the networking topology below, 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. The switch with te lowest bridge ID will be the root bridge, and there is only one root bridge in a spanning tree.

Bridge ID

Bridge ID is used to select the root bridge. It 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 the switches are the same, the switch with the smallest MAC address will be selected as the root bridge.

Port Role

- Root Port

The root port is selected on non-root bridge that can provide the lowest root path cost. There is only one root port in each non-root bridge.

- Designated Port

The designated port is selected in each LAN segment that can 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 switch receives this BPDU, the root path cost wll be increased according to the path cost of the receive port. Then it create a new BPDU with the new root file cost and forwards it to the

downstream switch. The value of the accumulated root path cost increases as the BPDU spreads further.

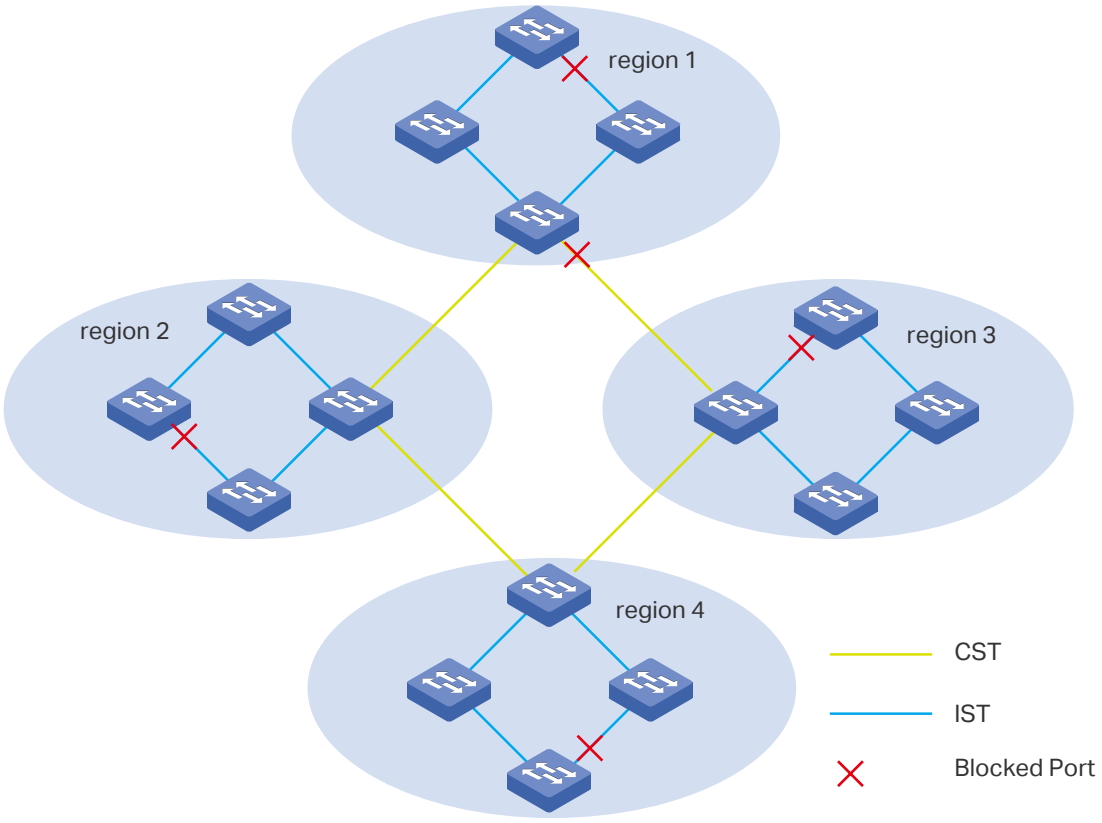
BPDU

BPDU is a kind of packet that is used to generate and maintain 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 spanning 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 used in MSTP.

Figure 1-3 MSTP Topology



MST Region

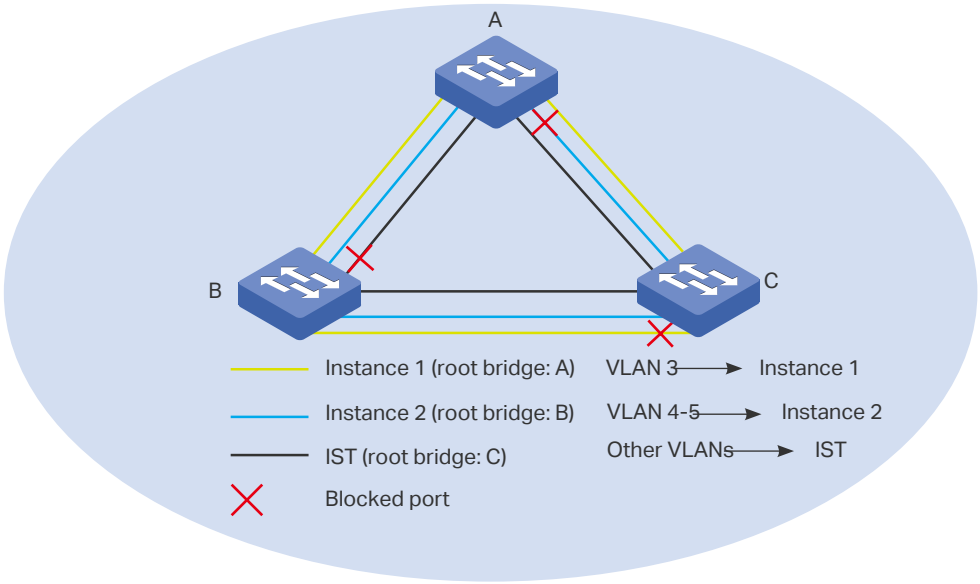
An MST region consists of multiple interconnected switches. The switches with the same following characteristics are considered as in the same region:

- 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 (IST), which is a special MST instance with an instance ID 0. By default, all the VLANs are mapped to IST.

CST

The Common Spanning Tree (CST), that is the spanning tree connecting 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 (CIST), comprising IST and CST. CIST 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

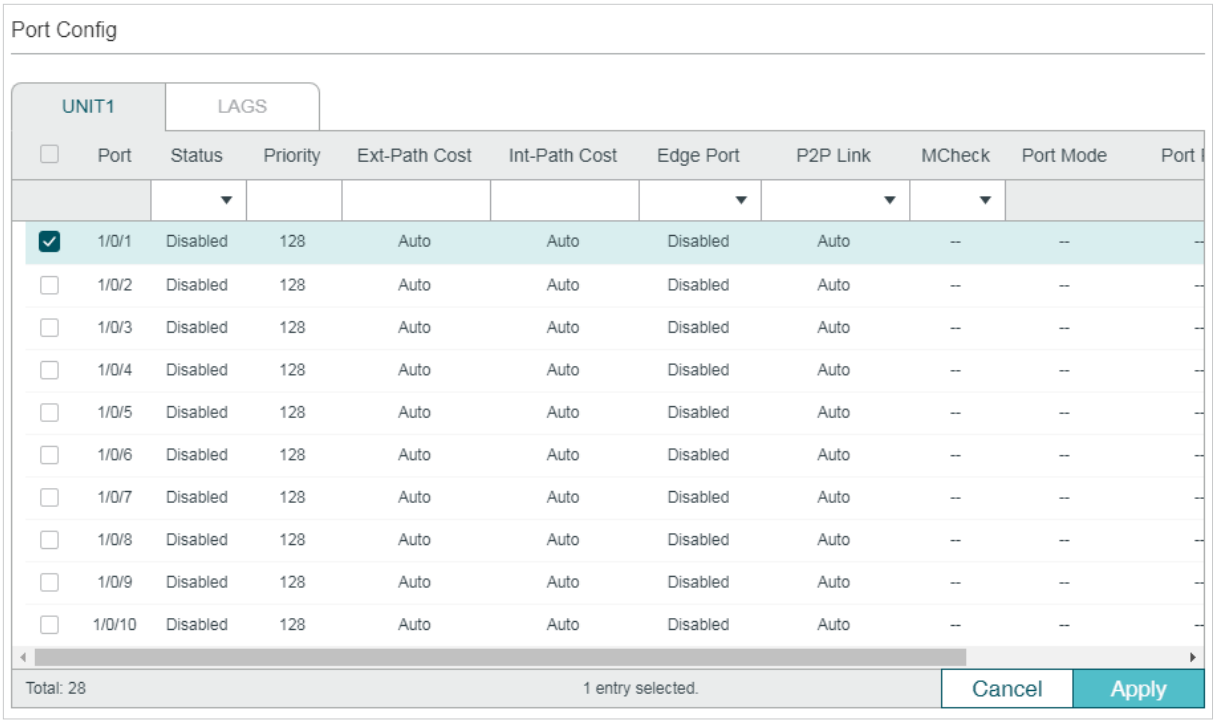
- Before configuring the spanning tree, it's necessary to make clear the role that each switch plays in a spanning tree.
- To avoid any possible network flapping caused by STP/RSTP parameter changes, it is recommended to enable STP/RSTP function globally after configuring the relevant parameters.

2.1 Using the GUI

2.1.1 Configuring STP/RSTP Parameters on Ports

Choose the menu **L2 FEATURES > Spanning Tree > 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	Specify the Priority for the desired port. The value should be an integral multiple of 16, ranging from 0 to 240. The port with lower value has the higher priority. When the root path of the port is the same as other ports', the switch will compare the port priorities between these port and select a root port with the highest priority.
Ext-Path Cost	Enter the value of the external path cost. The valid values are from 0 to 2000000. The default setting is Auto, which means the port calculates the external path cost automatically according to the port's link speed. For STP/RSTP, external path cost indicates the path cost of the port in spanning tree. The port with the lowest root path cost will be elected as the root port of the switch. For MSTP, external path cost indicates the path cost of the port in CST.
Int-Path Cost	Enter the value of the internal path cost. The default setting is Auto, which means the port calculates the internal path cost automatically according to the port's link speed. This parameter is only used in MSTP and you need not to configure it if the spanning tree mode is STP/RSTP. For MSTP, internal path cost is used to calculate the path cost in IST. The port with the lowest root path cost will be elected as the root port of the switch in IST.
Edge Port	Select Enable to set the port as an edge port. When the topology is changed, the edge port can transit its state from blocking to forwarding directly. For the quick generation of the spanning tree, it is recommended to set the ports that are connected to the end devices as edge ports.
P2P Link	Select the status of the P2P (Point-to-Point) link to which the ports are connected. During the regeneration of the spanning tree, if the port of P2P link is elected as the root port or the designated port, it can transit its state to forwarding directly. Three options are supported: Auto, Open(Force) and Closed(Force). By default, it is Auto. **Auto**: The switch automatically checks if the port is connected to a P2P link, then sets the status as Open or Closed. **Open(Force)**: A port is set as the one that is connected to a P2P link. You should check the link first. **Close(Force)**: A port is set as the one that is not connected to a P2P link. You should check the link first.

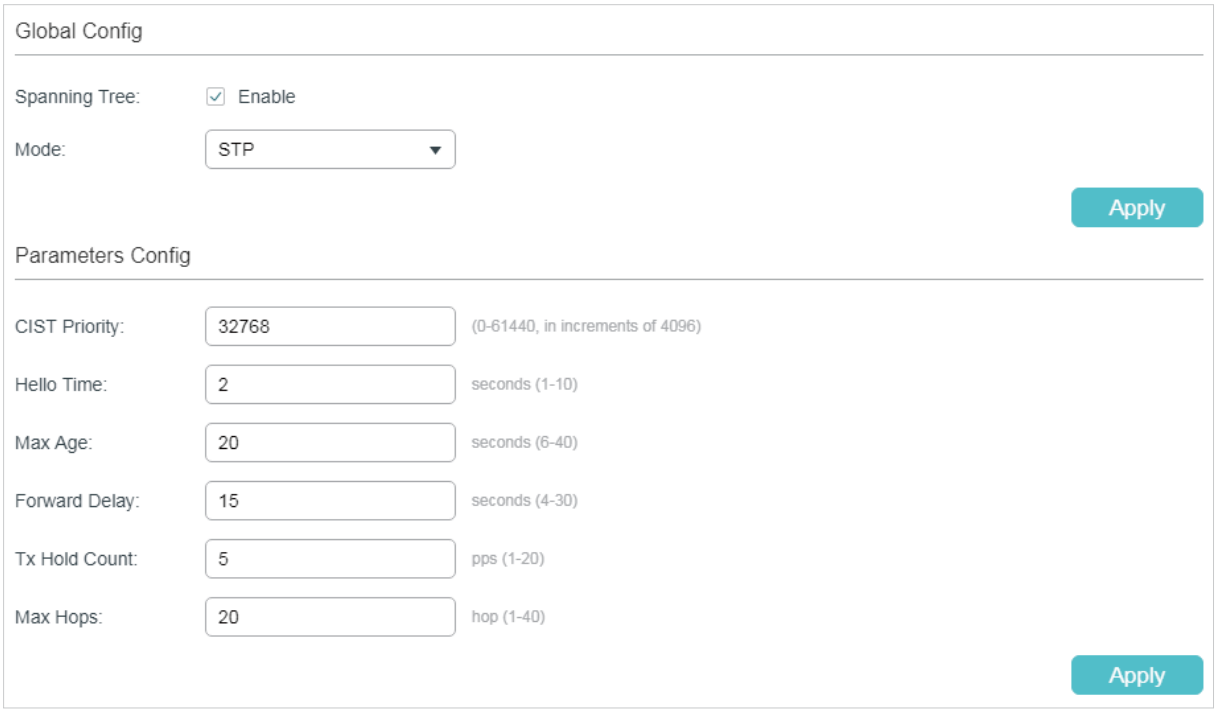
MCheck	Select whether to perform MCheck operations on the port. If a port on an RSTP-enabled/MSTP-enabled device is connected to an STP-enabled device, the port will switch to STP compatible mode and send packets in STP format. MCheck is used to switch the mode of the port back to RSTP/MSTP after the port is disconnected from the STP-enabled device. The MCheck configuration can take effect only once, after that the MCheck status of the port will switch to Disabled.
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 that the port is the root port in the spanning tree. It has the lowest path cost from the root bridge to this switch and is used to communicate with the root bridge. **Designated Port**: Indicates that the port is the designated port in the spanning tree. It has the lowest path cost from the root bridge to this physical network segment and is used to forward data for the corresponding network segment. **Alternate Port**: Indicates that the port is the alternate port in the spanning tree. It is the backup of the root port or master port. **Backup Port**: Indicates that the port is the backup port in the spanning tree. It is the backup of the designated port. **Disabled**: Indicates that 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. It also receives user traffic, but doesn't forward the traffic. **Blocking**: The port only receives and sends BPDUs. **Disconnected**: The port has the spanning tree function enabled but is 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 **L2 FEATURES > 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 for the switch. CIST priority is a parameter used to determine the root bridge for spanning tree. The switch with the lower value has the higher priority. In STP/RSTP, CIST priority is the priority of the switch in spanning tree. The switch with the highest priority will be elected as the root bridge. In MSTP, CISP priority is the priority of the switch in CIST. The switch with the higher priority will be elected as the root bridge in CIST.
Hello Time	Specify the interval between BPDUs' sending. The default value is 2.The root bridge sends configuration BPDUs at an interval of Hello Time. It works with the MAX Age to test the link failures and maintain the spanning tree.
Max Age	Specify the maximum time that the switch can wait without receiving a BPDU before attempting to regenerate a new spanning tree. The default value is 2.
Forward Delay	Specify the interval between the port state transition from listening to learning. The default value is 15. It is used to prevent the network from causing temporary loops during the regeneration of spanning tree. The interval between the port state transition from learning to forwarding is also the Forward Delay.
Tx Hold Count	Specify the maximum number of BPDU that can be sent in a second. The default value is 5.

Max Hops	Specify the maximum BPDU counts that can be forwarded in a MST region. The default value is 20. A switch receives BPDU, then decrements the hop count by one and generates BPDUs with the new value. When the hop reaches zero, the switch will discard the BPDU. This value can control the scale of the spanning tree in the 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**.

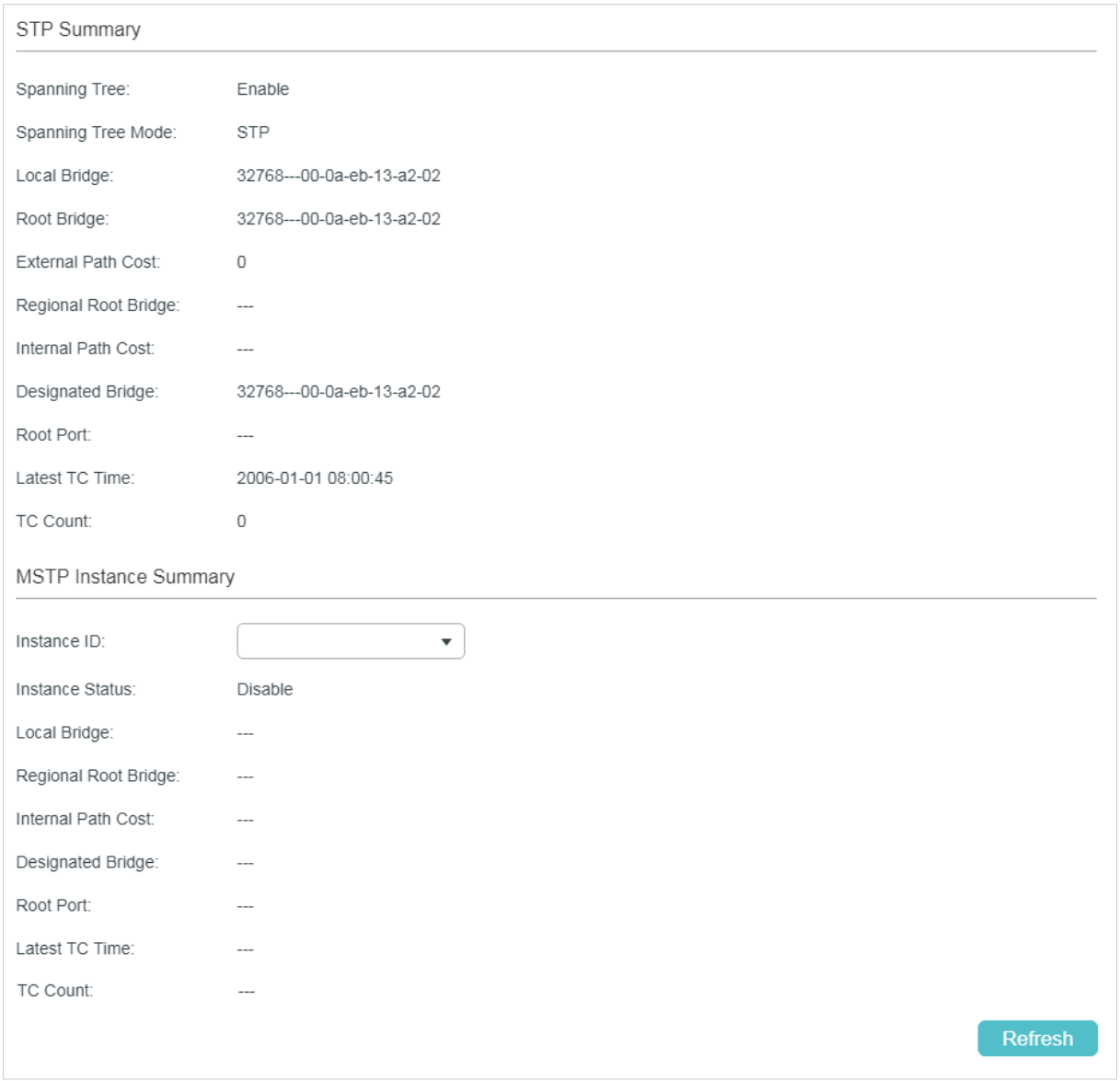
Spanning Tree	Check the box to enable the spanning tree function globally.
Mode	Select the desired spanning tree mode as STP/RSTP on the switch. By default, it's STP. **STP**: Specify the spanning tree mode as STP. **RSTP**: Specify the spanning tree mode as RSTP. **MSTP**: Specify the spanning tree 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 **L2 FEATURES > 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 {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	**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 Priority for the desired port. The value should be an integral multiple of 16, ranging from 0 to 240. The default value is 128. Ports with lower values have higher priority. When the root path of the port is the same as other ports', the switch will compare the port priorities and select a root port with the highest priority.

ext-cost: Specify the value of the external path cost. The valid values are from 0 to 2000000 and the default setting is Auto, which means the port calculates the external path cost automatically according to the port's link speed.

For STP/RSTP, external path cost indicates the path cost of the port in spanning tree. The Port with the lowest root path cost will be elected as the root port of the switch.

For MSTP, external path cost indicates the path cost of the port in CST.

portfast { enable | disable }: Enable to set the port as an edge port. By default, it is disabled. When the topology is changed, the edge port can transit its state from blocking to forwarding directly. For the quick generation of the spanning tree, it is recommended to set the ports that are connected to the end devices as edge ports.

point-to-point { auto | open | close }: Select the status of the P2P (Point-to-Point) link to which the ports are connected. During the regeneration of the spanning tree, if the port of P2P link is elected as the root port or the designated port, it can transit its state to forwarding directly. Auto indicates that the switch automatically checks if the port is connected to a P2P link, then sets the status as Open or Closed. Open is used to set the port as the one that is connected to a P2P link. Close is used to set the port as the one that is not connected to a P2P link.

Step 5 **spanning-tree mcheck**

(Optional) Perform MCheck operations on the port.

If a port on an RSTP-enabled/MSTP-enabled device is connected to an STP-enabled device, the port will switch to STP compatible mode and send packets in STP format. MCheck is used to switch the mode of the port back to RSTP/MSTP after the port is disconnected from the STP-enabled device. The MCheck configuration can take effect only once, after that the MCheck status of the port will switch to Disabled.

Step 6 **show spanning-tree interface** [**fastEthernet** *port* **| gigabitEthernet** *port* | **ten- 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.

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
Gi1/0/3	Enable	32	Auto	Auto	No	No(auto)	N/A

Role	Status	LAG
N/A	LnkDwn	N/A

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 priority for the switch. The valid value is from 0 to 61440, which are divisible by 4096. The priority is a parameter used to determine the root bridge for spanning tree. The switch with the lower value has the higher priority. In STP/RSTP, the value is the priority of the switch in spanning tree. The switch with the highest priority will be elected as the root bridge. In MSTP, the value is the priority of the switch in CIST. The switch with the higher 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. It is the interval between the port state transition from listening to learning. The valid values are from 4 to 30 in seconds, and the default value is 15. Forward Delay is used to prevent the network from causing temporary loops during the regeneration of spanning tree. The interval between the port state transition from learning to forwarding is also the Forward Delay. *hello-time:* Specify the value of Hello Time. It is the interval between BPDUs' sending. 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. It works with the MAX Age to test the link failures and maintain the spanning tree. *max-age:* Specify the value of Max Age. It is the maximum time that the switch can wait without receiving a BPDU before attempting to regenerate a new spanning tree. The valid values are from 6 to 40 in seconds, and the default value is 20.
Step 4	**spanning-tree hold-count** *value* Specify the maximum number of BPDU that can be sent in a second. *value:* Specify the maximum number of BPDU packets that can be sent in a second. 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
Gi1/0/16	Enable	128	200000	200000	No	Yes(auto)	Rstp
Gi1/0/18	Enable	128	200000	200000	No	Yes(auto)	Rstp
Gi1/0/20	Enable	128	200000	200000	No	Yes(auto)	Rstp

Role	Status	LAG
Desg	Fwd	N/A
Desg	Fwd	N/A
Desg	Fwd	N/A

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

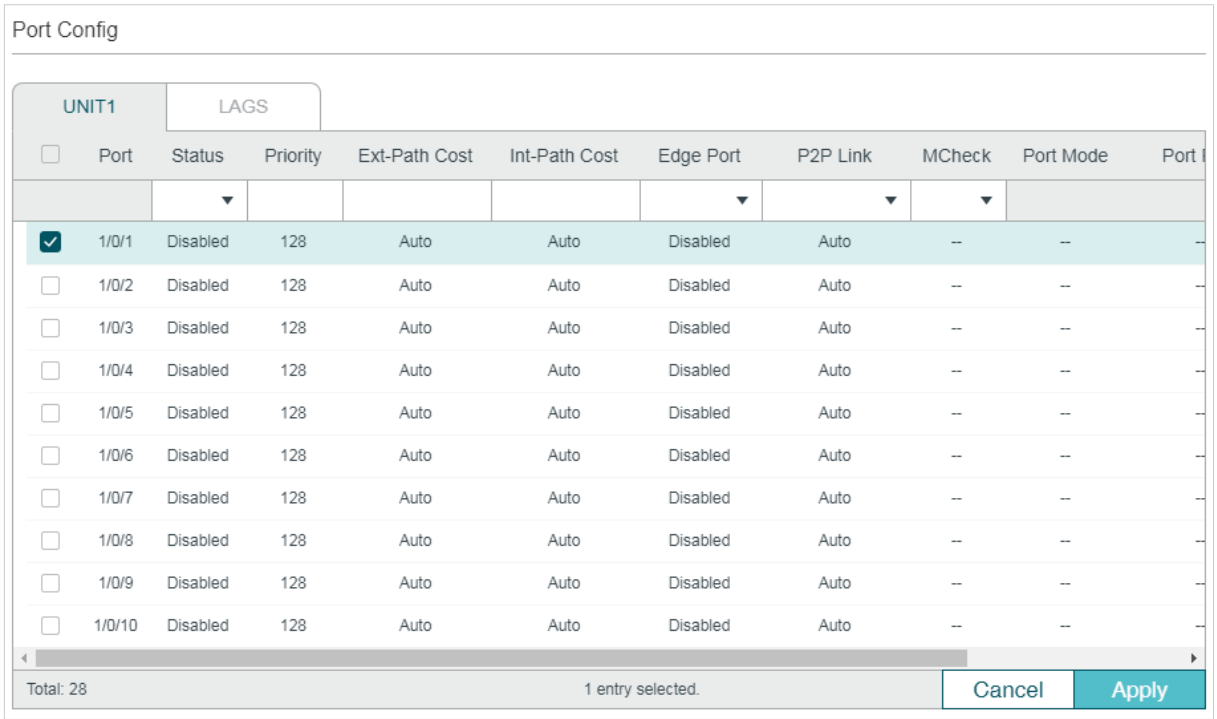
- Before configuring the spanning tree, it's necessary to make clear the role that each switch plays in a spanning tree.
- To avoid any possible network flapping caused by MSTP parameter changes, it is recommended to enable MSTP function globally after configuring the relevant parameter.

3.1 Using the GUI

3.1.1 Configuring Parameters on Ports in CIST

Choose the menu **L2 FEATURES > Spanning Tree > 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	Specify the Priority for the desired port. The value should be an integral multiple of 16, ranging from 0 to 240. The port with lower value has the higher priority. When the root path of the port is the same as other ports', the switch will compare the port priorities between these port and select a root port with the highest priority.
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. For STP/RSTP, external path cost indicates the path cost of the port in spanning tree. The port with the lowest root path cost will be elected as the root port of the switch. For MSTP, external path cost indicates the path cost of the port in CST.
Int-Path Cost	Enter the value of the internal path cost. The valid values are from 0 to 2000000. The default setting is Auto, which means the port calculates the internal path cost automatically according to the port's link speed. This parameter is only used in MSTP and you need not to configure it if the spanning tree mode is STP/RSTP. For MSTP, internal path cost is used to calculate the path cost in IST. The port with the lowest root path cost will be elected as the root port of the switch in IST.
Edge Port	Select Enable to set the port as an edge port. When the topology is changed, the edge port can transit its state from blocking to forwarding directly. For the quick generation of the spanning tree, it is recommended to set the ports that are connected to the end devices as edge ports.

P2P Link	Select the status of the P2P (Point-to-Point) link to which the ports are connected. During the regeneration of the spanning tree, if the port of P2P link is elected as the root port or the designated port, it can transit its state to forwarding directly. Three options are supported: Auto, Open(Force) and Closed(Force). By default, it is Auto. **Auto**: The switch automatically checks if the port is connected to a P2P link, then sets the status as Open or Closed. **Open(Force)**: A port is set as the one that is connected to a P2P link. You should check the link first. **Close(Force)**: A port is set as the one that is not connected to a P2P link. You should check the link first.
MCheck	Select whether to perform MCheck operations on the port. If a port on an RSTP-enabled/MSTP-enabled device is connected to an STP-enabled device, the port will switch to STP compatible mode and send packets in STP format. MCheck is used to switch the mode of the port back to RSTP/MSTP after the port is disconnected from the STP-enabled device. The MCheck configuration can take effect only once, after that the MCheck status of the port will switch to Disabled.
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 that the port is the root port in the spanning tree. It has the lowest path cost from the root bridge to this switch and is used to communicate with the root bridge. **Designated Port**: Indicates that the port is the designated port in the spanning tree. It has the lowest path cost from the root bridge to this physical network segment and is used to forward data for the corresponding network segment. **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 the corresponding region. **Alternate Port**: Indicates that the port is the alternate port in the spanning tree. It is the backup of the root port or master port. **Backup Port**: Indicates that the port is the backup port in the spanning tree. It is the backup of the designated port. **Disabled**: Indicates that 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. It also receives user traffic, but doesn't forward the traffic. **Blocking**: The port only receives and sends BPDUs. **Disconnected**: The port has the spanning tree function enabled but is not connected to any device.
LAG	Displays the LAG the port belongs to.

2) Click **Apply**.

3.1.2 Configuring the MSTP Region

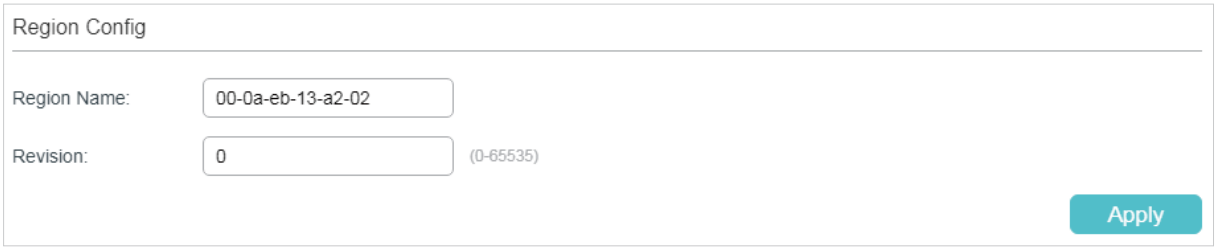
Configure the region name, revision level, VLAN-Instance mapping of the switch. The switches with the same region name, the same revision level and the same VLAN-Instance mapping are considered as in the same region.

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 **L2 FEATURES > 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.

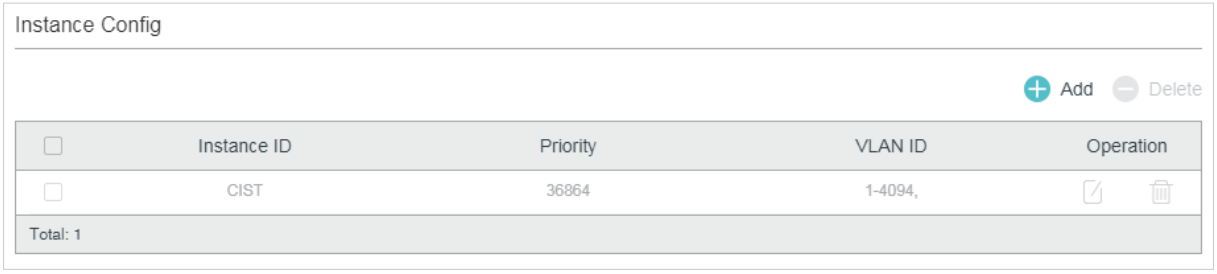
Region Name	Configure the name for an MST region using up to 32 characters. By default, it is the MAC address of the switch.
Revision	Enter the revision level. By default, it is 0.

2) Click **Apply**.

Configuring the VLAN-Instance Mapping and Switch Priority

Choose the menu **L2 FEATURES > Spanning Tree > MSTP Instance > Instance Config** to load the following page.

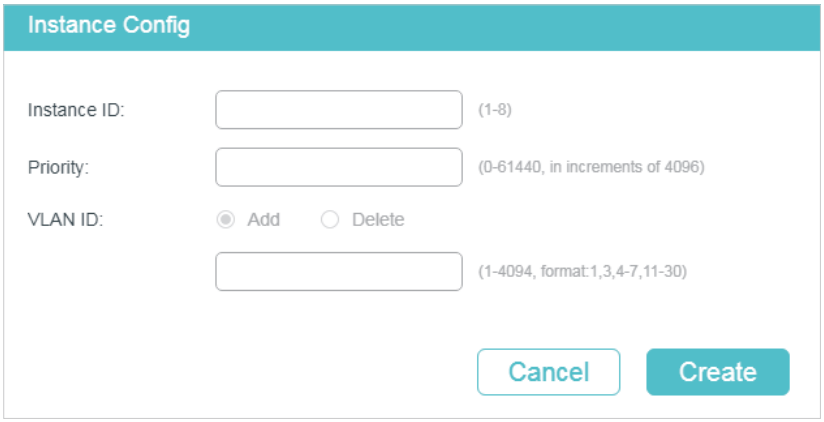
Figure 3-3 Configuring the VLAN-Instance Mapping



Follow these steps to map VLANs to the corresponding instance, and configure the priority of the switch in the desired instance:

1) In the **Instance Config** section, click **Add** and enter the instance ID, Priority and corresponding VLAN ID.

Figure 3-4 Configuring the Instance



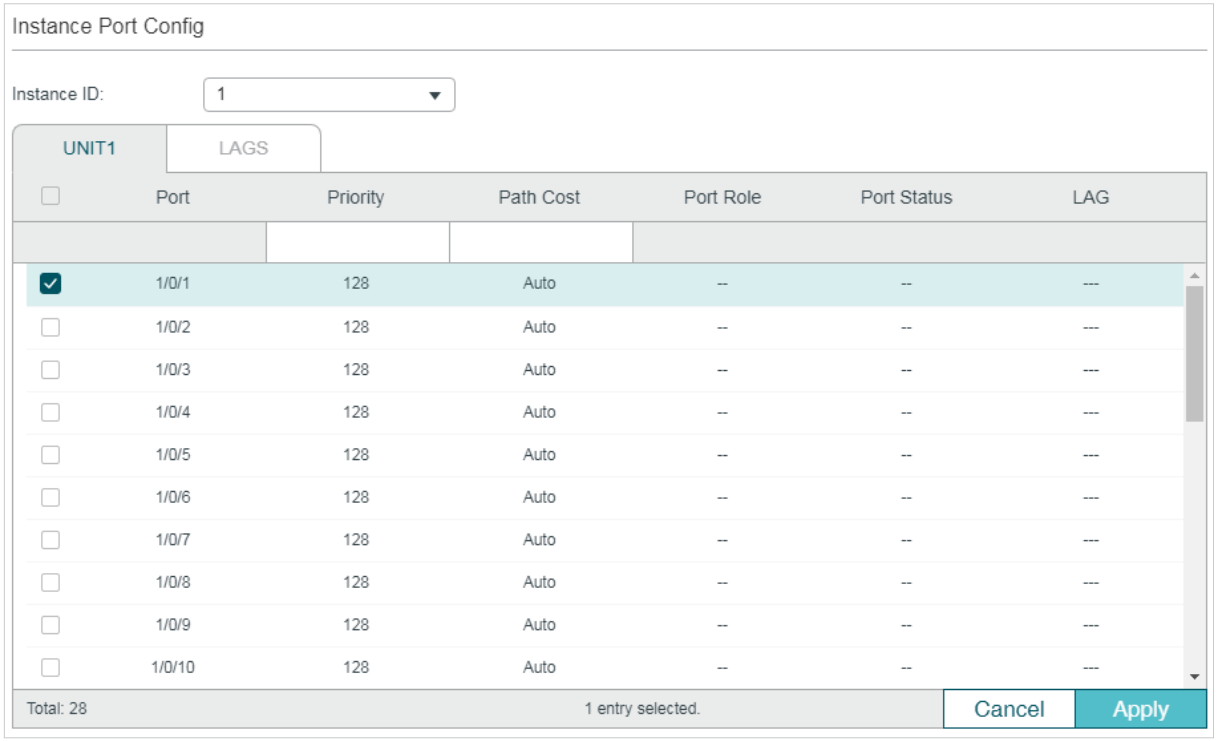
Instance ID	Enter the corresponding instance ID.
Priority	Specify the priority for the switch in the corresponding instance. The value should be an integral multiple of 4096, ranging from 0 to 61440. It is used to determine the root bridge for the instance. Switches with a lower value have higher priority, and the switch with the highest priority will be elected as the root bridge in the corresponding instance.
VLAN ID	Enter the VLAN ID to map the VLAN to the desired instance or unbind the VLAN-instance mapping.

2) Click **Create**.

Configuring Parameters on Ports in the Instance

Choose the menu **L2 FEATURES > Spanning Tree > MSTP Instance > Instance Port Config** to load the following page.

Figure 3-5 Configuring Port Parameters in the Instance



Follow these steps to configure port parameters in the instance:

1) In the **Instance Port Config** section, select the desired instance ID.

Instance ID	Select the ID number of the instance that you want to configure.

2) Configure port parameters in the desired instance.

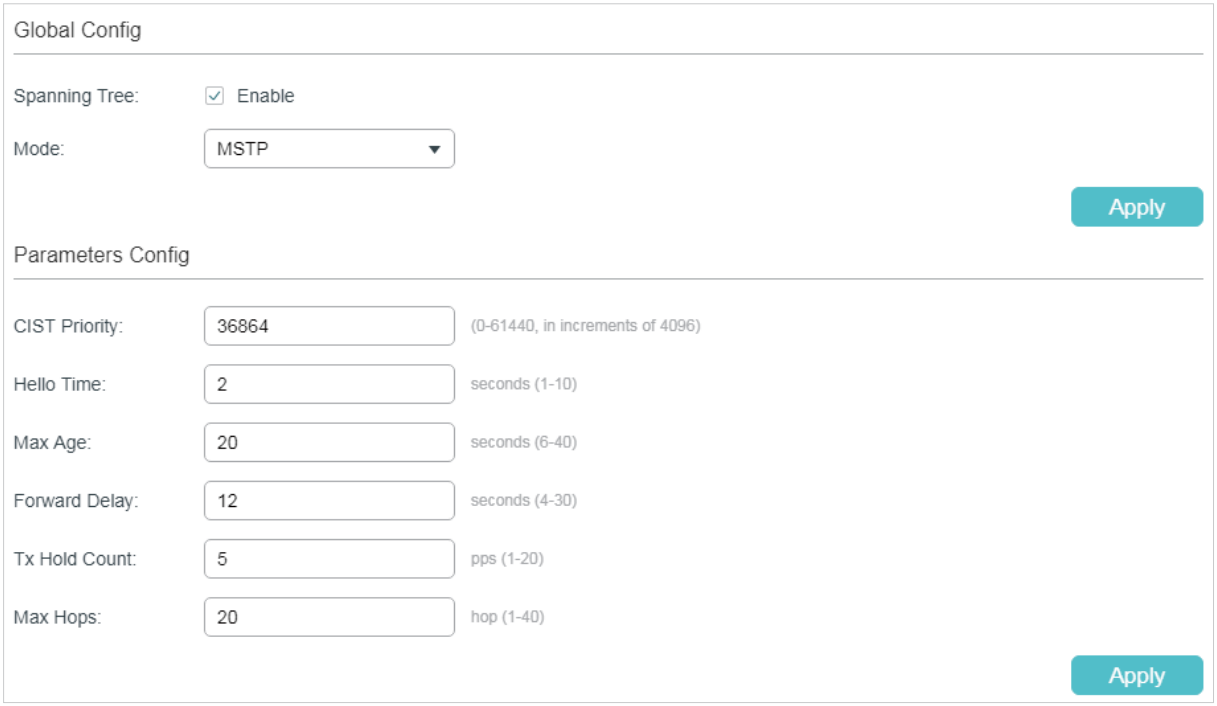
UNIT	Select the desired unit or LAGs for configuration.
Priority	Specify the Priority for the port in the corresponding instance. The value should be an integral multiple of 16, ranging from 0 to 240. The port with lower value has the higher priority. When the root path of the port is the same as other ports', the switch will compare the port priorities between these ports and select a root port with the highest priority.
Path Cost	Enter the value of the path cost in the corresponding instance. The valid values are from 0 to 2000000. The default setting is Auto, which means the port calculates the path cost automatically according to the port's link speed. The port with the lowest root path cost will be elected as the root port of the switch in desired instance.

Port Role	Displays the role that the port plays in the desired instance. **Root Port**: Indicates that the port is the root port in the desired instance. It has the lowest path cost from the root bridge to this switch and is used to communicate with the root bridge. **Designated Port**: Indicates that the port is the designated port in the desired instance. It has the lowest path cost from the root bridge to this physical network segment and is used to forward data for the corresponding network segment. **Alternate Port**: Indicates that the port is the alternate port in the desired instance. It is the backup of the root port or master port. **Backup Port**: Indicates that the port is the backup port in the desired instance. It is the backup of the designated port. **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 the corresponding region. **Disabled**: Indicates that 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 traffic. **Learning**: The port receives and sends BPDUs. It also receives user traffic, but doesn't forward the traffic. **Blocking**: The port only receives and sends BPDUs. **Disconnected**: The port has the spanning tree function enabled but is not connected to any device.
LAG	Displays the LAG which the port belongs to.

3.1.3 Configuring MSTP Globally

Choose the menu **L2 FEATURES > Spanning Tree > STP Config > STP Config** to load the following page.

Figure 3-6 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	Specify the CIST priority for the switch. CIST priority is a parameter used to determine the root bridge for spanning tree. The switch with the lower value has the higher priority. In STP/RSTP, CIST priority is the priority of the switch in spanning tree. The switch with the highest priority will be elected as the root bridge. In MSTP, CISP priority is the priority of the switch in CIST. The switch with the higher priority will be elected as the root bridge in CIST.
Hello Time	Specify the interval between BPDUs' sending. The default value is 2. The root bridge sends configuration BPDUs at an interval of Hello Time. It works with the MAX Age to test the link failures and maintain the spanning tree.
Max Age	Specify the maximum time that the switch can wait without receiving a BPDU before attempting to regenerate a new spanning tree. The default calue is 20.

Forward Delay	Specify the interval between the port state transition from listening to learning. The default value is 15. It is used to prevent the network from causing temporary loops during the regeneration of spanning tree. The interval between the port state transition from learning to forwarding is also the Forward Delay.
Tx Hold Count	Specify the maximum number of BPDU that can be sent in a second. The default value is 5.
Max Hops	Specify the maximum BPDU hop counts that can be forwarded in a MST region. The default value is 20. A switch receives BPDU, then decrements the hop count by one and generates BPDUs with the new value. When the hop reaches zero, the switch will discard the BPDU. This value can control the scale of the spanning tree in the 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

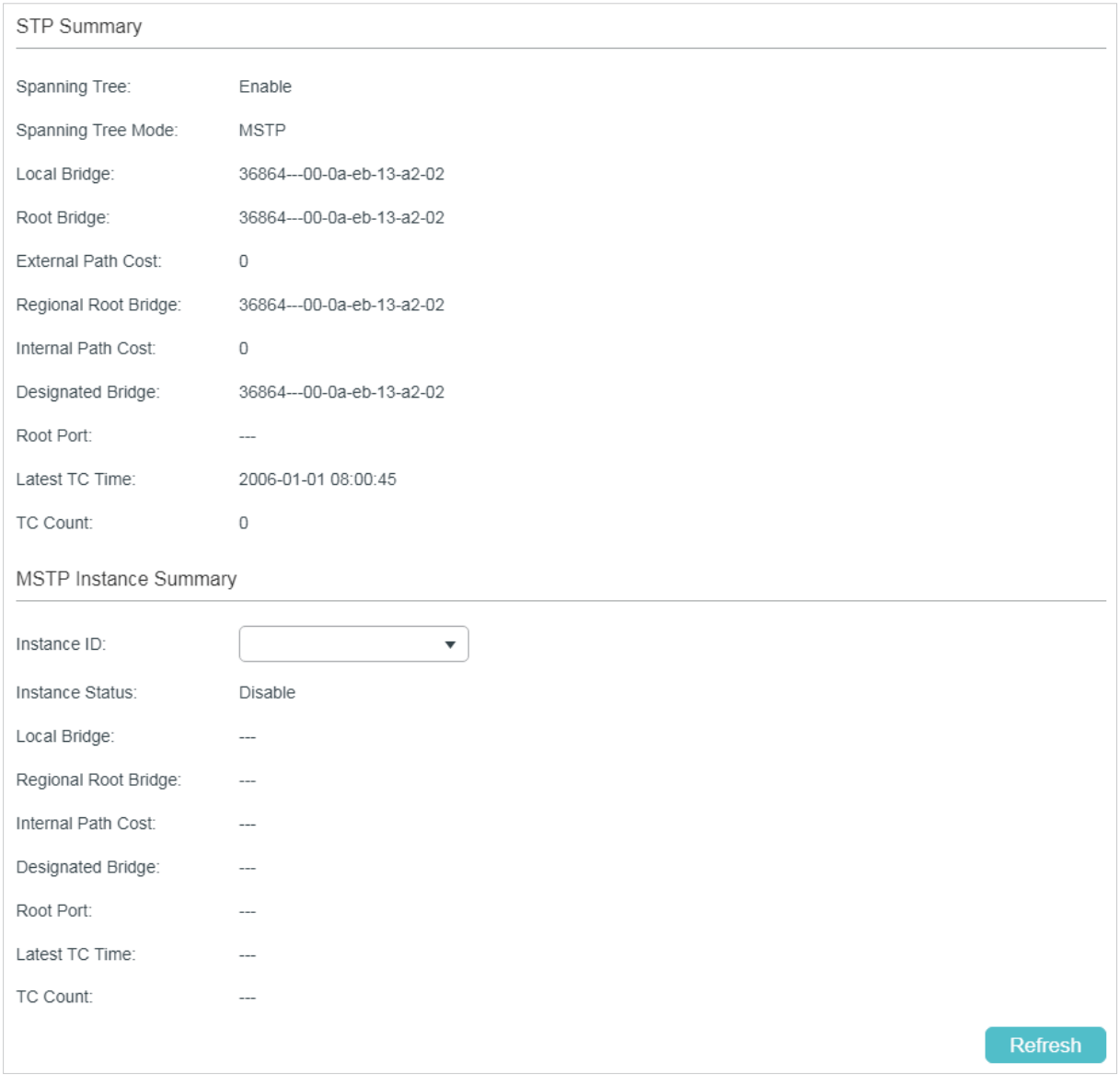
2) In the **Global Config** section, enable Spanning-Tree function and choose the STP mode as MSTP and click **Apply**.

Spanning-Tree	Check the box to enable the spanning tree function globally.
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.

3.1.4 Verifying the MSTP Configurations

Choose the menu **Spanning Tree > STP Config > STP Summary** to load the following page.

Figure 3-7 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 Instance 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 {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 **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 Priority for the desired port. The value should be an integral multiple of 16, ranging from 0 to 240. The default value is 128. Ports with lower values have higher priority. When the root path of the port is the same as other ports', the switch will compare the port priorities and select a root port with the highest priority.

ext-cost: Specify the value of the external path cost. The valid values are from 0 to 2000000 and the default setting is Auto, which means the port calculates the external path cost automatically according to the port's link speed.

For STP/RSTP, external path cost indicates the path cost of the port in spanning tree. The Port with the lowest root path cost will be elected as the root port of the switch.

For MSTP, external path cost indicates the path cost of the port in CST.

int-cost: Specify the value of the internal path cost. The valid values are from 0 to 2000000. The default setting is Auto, which means the port calculates the internal path cost automatically according to the port's link speed. This parameter is only used in MSTP.

For MSTP, internal path cost is used to calculate the path cost in IST. The port with the lowest root path cost will be elected as the root port of the switch in IST.

portfast { enable | disable }*:* Enable to set the port as an edge port. By default, it is disabled. When the topology is changed, the edge port can transit its state from blocking to forwarding directly. For the quick generation of the spanning tree, it is recommended to set the ports that are connected to the end devices as edge ports.

point-to-point { auto | open | close }*:* Select the status of the P2P (Point-to-Point) link to which the ports are connected. During the regeneration of the spanning tree, if the port of P2P link is elected as the root port or the designated port, it can transit its state to forwarding directly. Auto indicates that the switch automatically checks if the port is connected to a P2P link, then sets the status as Open or Closed. Open is used to set the port as the one that is connected to a P2P link. Close is used to set the port as the one that is not connected to a P2P link.

Step 5 **spanning-tree mcheck**

(Optional) Perform MCheck operations on the port.

If a port on an RSTP-enabled/MSTP-enabled device is connected to an STP-enabled device, the port will switch to STP compatible mode and send packets in STP format. MCheck is used to switch the mode of the port back to RSTP/MSTP after the port is disconnected from the STP-enabled device. The MCheck configuration can take effect only once, after that the MCheck status of the port will switch to Disabled.

Step 6 **show spanning-tree interface** [**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-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 for the switch in the corresponding instance. The value should be an integral multiple of 4096, ranging from 0 to 61440. The default value is 32768. It is used to determine the root bridge for the instance. Switches with a lower value have higher priority, and the switch with the highest priority will be elected as the root bridge in the corresponding 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* | **ten-gigabitEthernet** *port*]] } (Optional) View the related information of MSTP Instance. *digest*: Specify to display the 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 {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	**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 for the port in the corresponding instance. The value should be an integral multiple of 16, ranging from 0 to 240. The default valueis 128. The port with lower value has the higher priority. When the root path of the port is the same as other ports', the switch will compare the port priorities between these ports and select a root port with the highest priority. *cost:* Enter the value of the path cost in the corresponding instance. The valid values are from 0 to 2000000. The default setting is Auto, which means the port calculates the path cost automatically according to the port's link speed. The port with the lowest root path cost will be elected as the root port of the switch in desired instance.

Step 4	**show spanning-tree mst** { **configuration** [digest] | **instance** *instance-id* [**interface** [**fastEthernet** *port* | **gigabitEthernet** *port* | **port-channel** *lagid* | **ten-gigabitEthernet** *port*]] } (Optional) View the related information of MSTP Instance. *digest:* Specify to display the 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	LAG
Gi1/0/3	Enable	32	Auto	Auto	No	No(auto)	N/A	N/A	LnkDwn	N/A

MST-Instance 5

Interface	Prio	Cost	Role	Status	LAG
Gi1/0/3	144	200	N/A	LnkDwn	N/A

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 priority for the switch. The valid value is from 0 to 61440, which are divisible by 4096. The priority is a parameter used to determine the root bridge for spanning tree. The switch with the lower value has the higher priority.

In STP/RSTP, the value is the priority of the switch in spanning tree. The switch with the highest priority will be elected as the root bridge.

In MSTP, the value is the priority of the switch in CIST. The switch with the higher 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. It is the interval between the port state transition from listening to learning. The valid values are from 4 to 30 in seconds, and the default value is 15. Forward Delay is used to prevent the network from causing temporary loops during the regeneration of spanning tree. The interval between the port state transition from learning to forwarding is also the Forward Delay.

hello-time: Specify the value of Hello Time. It is the interval between BPDUs' sending. 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. It works with the MAX Age to test the link failures and maintain the spanning tree.

max-age: Specify the value of Max Age. It is the maximum time that the switch can wait without receiving a BPDU before attempting to regenerate a new spanning tree. The valid values are from 6 to 40 in seconds, and the default value is 20.

Step 4 **spanning-tree hold-count** *value*

(Optional) Specify the maximum number of BPDU that can be sent in a second.

value: Specify the maximum number of BPDU packets that can be sent in a second. The valid values are from 1 to 20 pps, and the default value is 5.

Step 5 **spanning-tree max-hops** *value*

(Optional) Specify the maximum BPDU hop counts that can be forwarded in a MST region. A switch receives BPDU, then decrements the hop count by one and generates BPDUs with the new value. When the hop reaches zero, the switch will discard the BPDU. This value can control the scale of the spanning tree in the MST region.

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

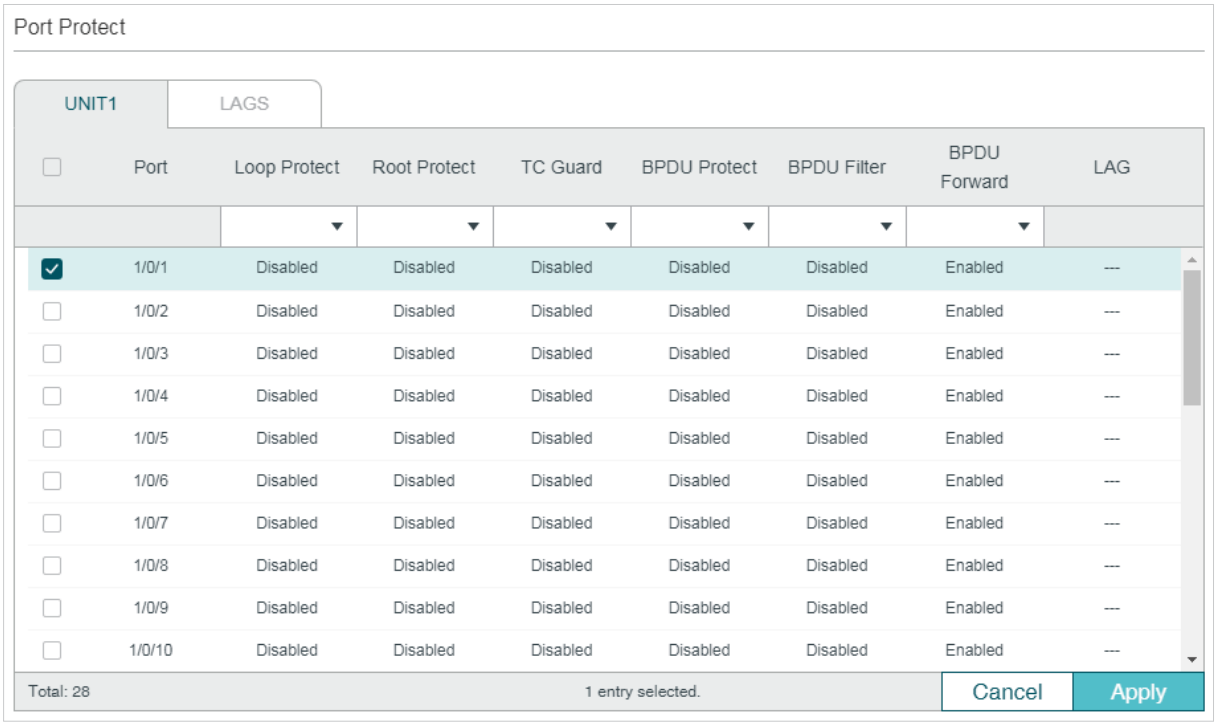
Switch#copy running-config startup-config

4 STP Security Configurations

4.1 Using the GUI

Choose the menu **L2 FEATURES > Spanning Tree > STP Security** 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 Loop Protect. It is recommended to enable this function on root ports and alternate ports. When there are link congestions or link failures in the network, the switch will not receive BPDUs from the upstream device in time. Loop Protect is used to avoid loop caused by the recalculation in this situation. With Loop Protect function enabled, the port will temporarily transit to a blocking state after it does not receive BPDUs in time.

Root Protect	Enable or disable Root Protect. It is recommended to enable this function on the designated ports of the root bridge. Switches with faulty configurations may produce a higher-priority BPDUs than the root bridge's, and this situation will cause recalculation of the spanning tree. Root Protect is used to ensure that the desired root bridge will not lose its position in the scenario above. With root protect enabled, the port will temporarily transit to blocking state when it receives higher-priority BDPUs. After two forward delays, if the port does not receive any other higher-priority BDPUs, it will transit to its normal state.
TC Guard	Enable or disable the TC Guard function. It is recommended to enable this function on the ports of non-root switches. TC Guard function is used to prevent the switch from frequently changing the MAC address table. With TC Guard function enabled, when the switch receives TC-BPDUs, it will not process the TC-BPDUs at once. The switch will wait for a fixed time and process the TC-BPDUs together after receiving the first TC-BPDU, then it will restart timing.
BPDU Protect	Enable or disable the BPDU Protect function. It is recommended to enable this function on edge ports. Edge ports in spanning tree are used to connect to the end devices and it doesn't receive BPDUs in the normal situation. If edge ports receive BPDUs, it may be an attack. BPDU Protect is used to protect the switch from the attack talked above. With BPDU protect function enabled, the edge ports will be shutdown when they receives BPDUs, and will report these cases to the administrator. Only the administrator can restore the state of the ports.
BPDU Filter	Enable or disable BPDU Filter. It is recommended to enable this function on edge ports. With BPDU filter function enabled, the port does not receive or forward BPDUs, but it sends out its own BPDUs. BPDU Filter can prevent the switch from being attacked as with BPDU Protect.
BPDU Forward	Enable or disable BPDU Forward. This function only takes effect when the spanning tree function is disabled globally. With BPDU forward enabled, the port can still forward spanning tree BPDUs when the spanning tree function is disabled.

4.2 Using the CLI

4.2.1 Configuring the STP Security

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 {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	**spanning-tree guard loop** (Optional) Enable Loop Protect. It is recommended to enable this function on root ports and alternate ports. When there are link congestions or link failures in the network, the switch will not receive BPDUs from the upstream device in time. Loop Protect is used to avoid loop caused by the recalculation in this situation. With Loop Protect function enabled, the port will temporarily transit to a blocking state after it does not receive BPDUs in time.
Step 4	**spanning-tree guard root** (Optional) Enable Root Protect. It is recommended to enable this function on the designated ports of the root bridge. Switches with faulty configurations may produce a higher-priority BPDUs than the root bridge's, and this situation will cause recalculation of the spanning tree. Root Protect is used to ensure that the desired root bridge will not lose its position in the scenario above. With root protect enabled, the port will temporarily transit to blocking state when it receives higher-priority BDPUs. After two forward delays, if the port does not receive any other higher-priority BDPUs, it will transit to its normal state.
Step 5	**spanning-tree guard tc** (Optional) Enable the TC Guard function. It is recommended to enable this function on the ports of non-root switches. TC Guard function is used to prevent the switch from frequently changing the MAC address table. With TC Guard function enabled, when the switch receives TC-BPDUs, it will not process the TC-BPDUs at once. The switch will wait for a fixed time and process the TC-BPDUs together after receiving the first TC-BPDU, then it will restart timing.
Step 6	**spanning-tree bpduguard** (Optional) Enable the BPDU Protect function. It is recommended to enable this function on edge ports. Edge ports in spanning tree are used to connect to the end devices and it doesn't receive BPDUs in the normal situation. If edge ports receive BPDUs, it may be an attack. BPDU Protect is used to protect the switch from the attack talked above. With BPDU protect function enabled, the edge ports will be shutdown when they receives BPDUs, and will report these cases to the administrator. Only the administrator can restore the state of the ports.
Step 7	**spanning-tree bpdufilter** (Optional) Enable or disable BPDU Filter. It is recommended to enable this function on edge ports. With BPDU filter function enabled, the port does not receive or forward BPDUs, but it sends out its own BPDUs. BPDU Filter can prevent the switch from being attacked as with BPDU Protect.

Step 8	**spanning-tree bpduflood** (Optional) Enable BPDU Forward. This function only takes effect when the spanning tree function is disabled globally. By default, it is enabled. With BPDU forward enabled, the port can still forward spanning tree BPDUs when the spanning tree function is disabled.
Step 9	**show spanning-tree interface-security** [**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **port-channel** *port-channel-id*] [bpdufilter | bpduguard | bpduflood | loop | root | tc] (Optional) View the protect inforamtion of ports. *port*: Specify the port number. *lagid*: Specify the ID of the 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 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	BPDU-Flood
Gi1/0/3	Enable	Enable	Enable	Enable	Disable	Enable

Switch(config-if)#end

Switch#copy running-config startup-config

5 Configuration Example for MSTP

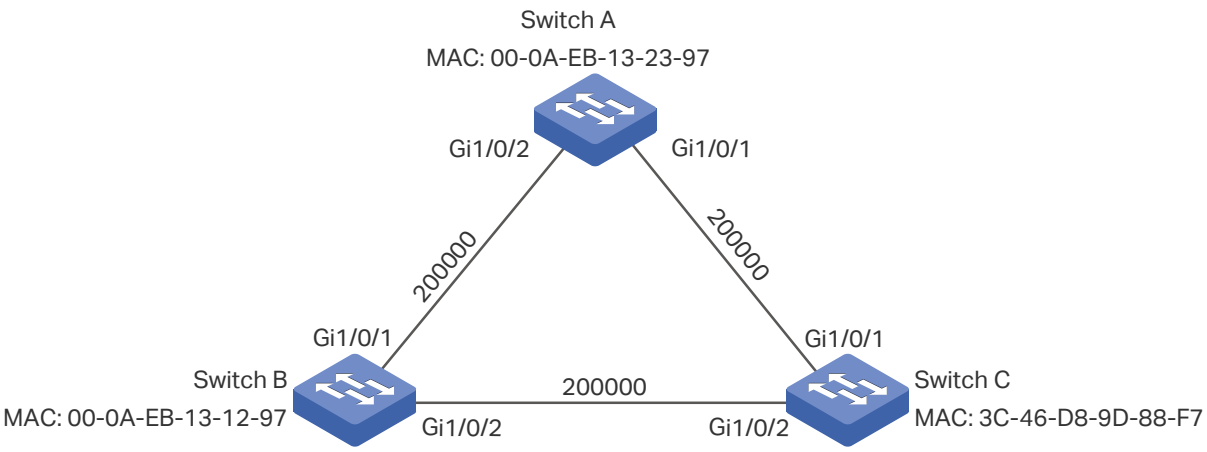
MSTP, backwards-compatible with STP and RSTP, can map VLANs to instances to implement load-balancing, thus providing a more flexible method in network management. Here we take the MSTP configuration as an example.

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

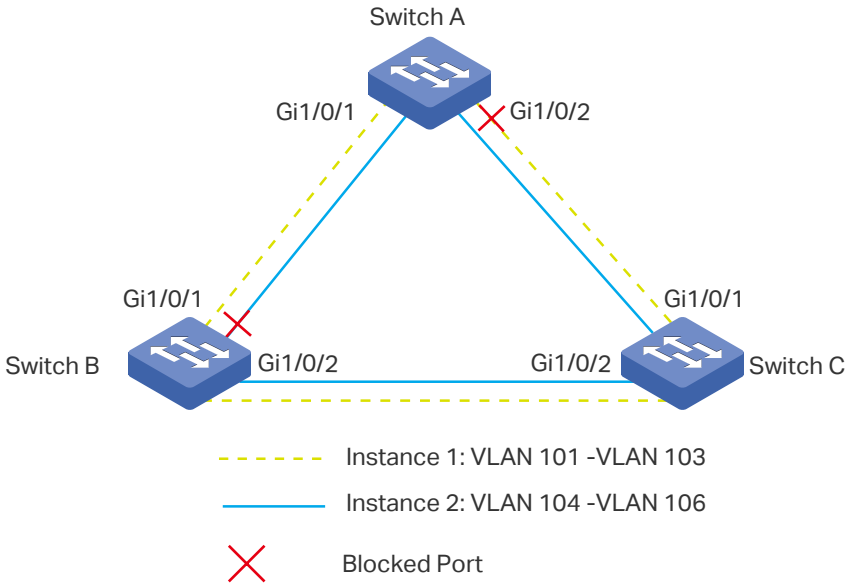


5.2 Configuration Scheme

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:

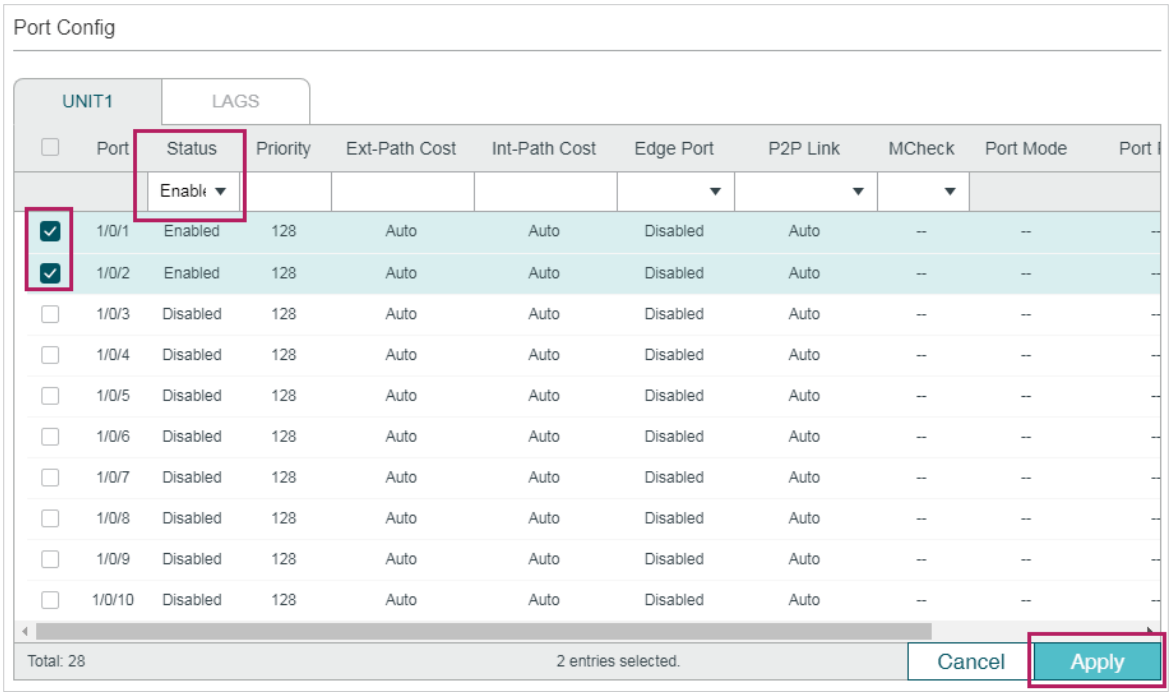
1) Enable the Spanning Tree function on the ports in each switch.
2) Configure Switch A, Switch B and Switch C in the same region. Configure the region name as 1, and the revision level as 100. Map VLAN 101 - VLAN 103 to instance 1 and VLAN 104 - VLAN 106 to instance 2.
3) Configure the priority of Switch 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.

5.3 Using the GUI

- Configurations for Switch A

1) Choose the menu **L2 FEATURES > 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. Click **Apply**.

Figure 5-3 Enable Spanning Tree Function on Ports



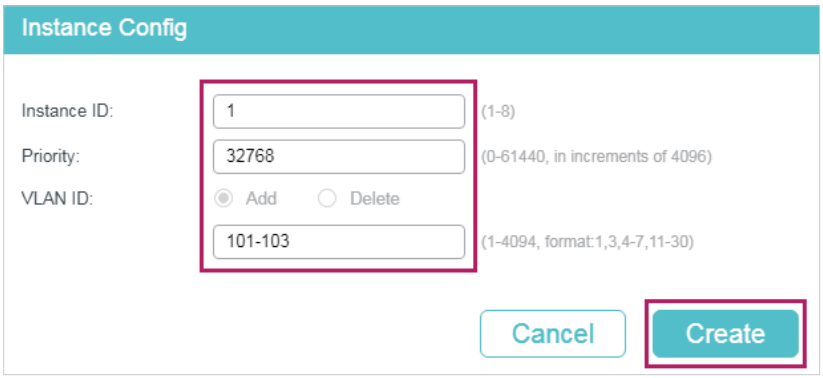
2) Choose the menu **L2 FEATURES > Spanning Tree > MSTP Instance > Region Config** to load the following page. Set the region name as 1 and the revision level as 100. Click **Apply**.

Figure 5-4 Configuring the MST Region



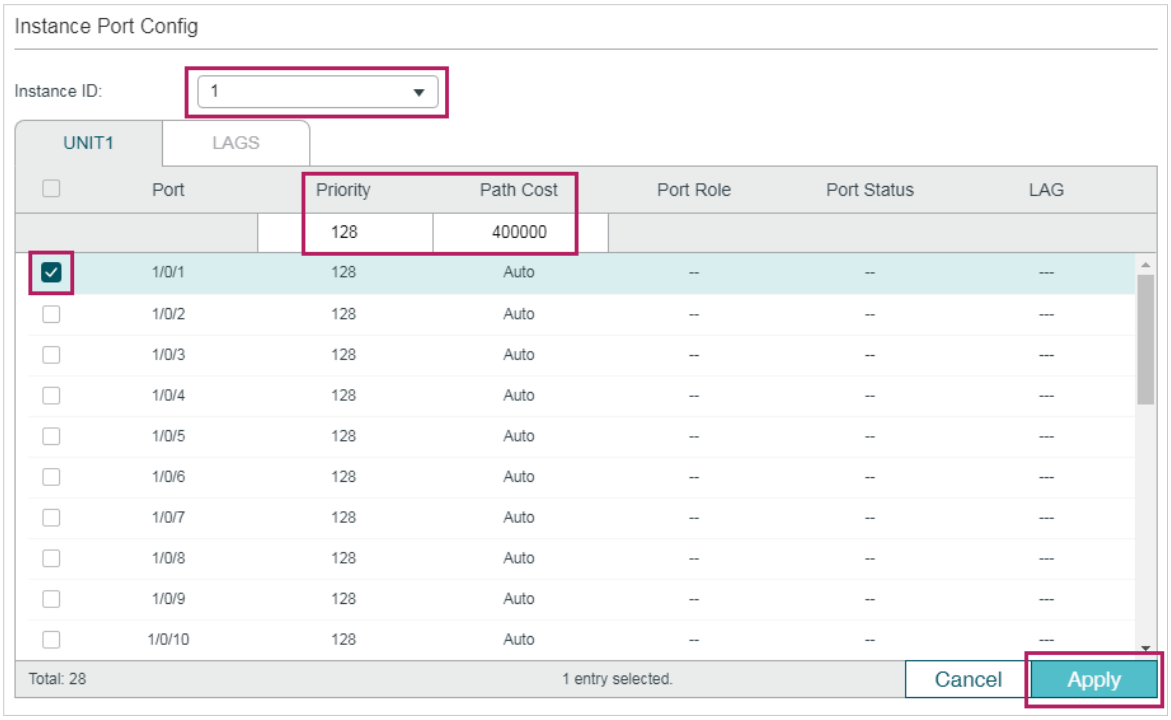
3) Choose the menu **L2 FEATURES > Spanning Tree > MSTP Instance > Instance Config**. Click Add, map VLAN101-VLAN103 to instance 1 and set the priority as 32768; map VLAN104-VLAN106 to instance 2 and set the priority as 32768. Click **Create**.

Figure 5-5 Configuring the VLAN-Instance Mapping



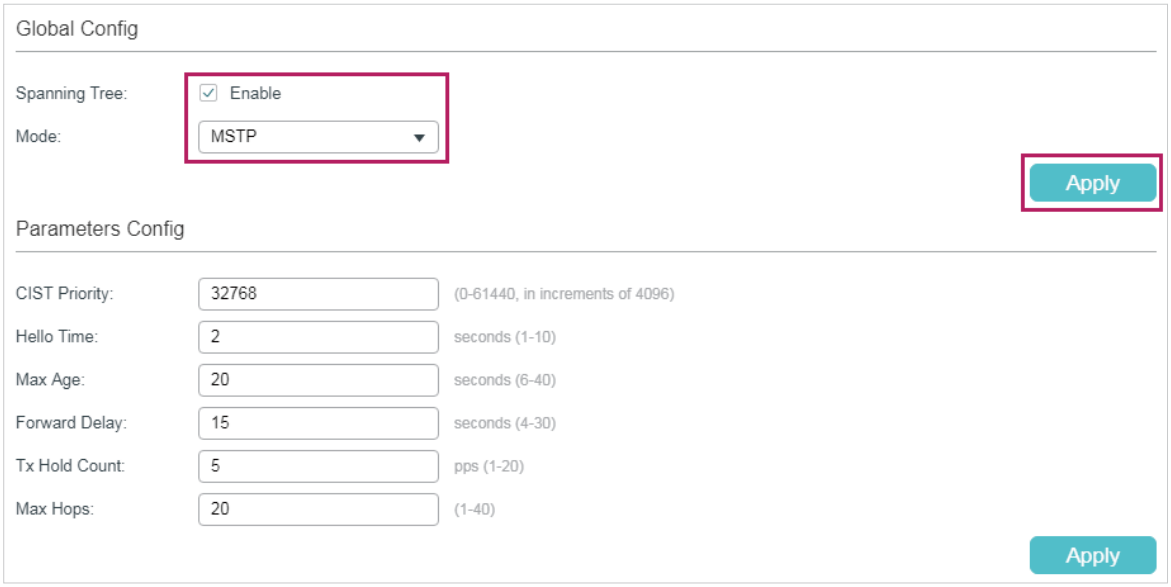
4) Choose the menu **L2 FEATURES > Spanning Tree > MSTP Instance > Instance Port Config** to load the following page. Set the path cost of port 1/0/1 in instance 1 as 400000. Click **Apply**.

Figure 5-6 Configure the Path Cost of Port 1/0/1 In Instance 1



5) Choose the menu **L2 FEATURES > 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. **Click Apply**.

Figure 5-7 Configure the Global MSTP Parameters of the Switch

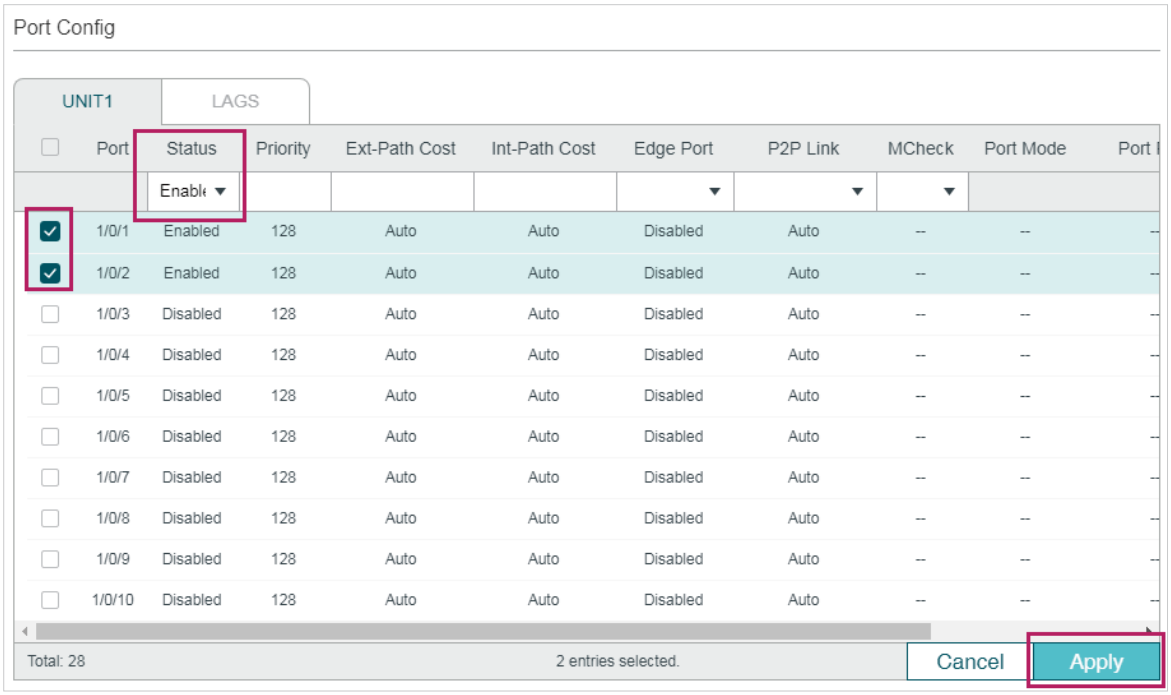


6) Click Save to save the settings.

Configurations for Switch B

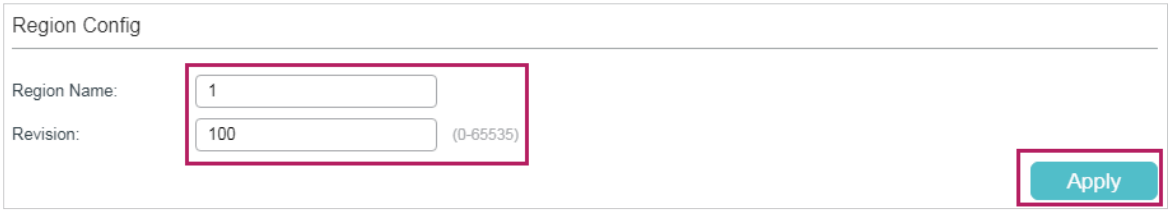
1) Choose the menu **L2 FEATURES > Spanning Tree > STP Config > Port Config** to load the following page. Enable the spanning tree function on port 1/0/1 and port 1/0/2. Here we leave the values of the other parameters as default settings. Click **Apply**.

Figure 5-8 Enable Spanning Tree Function on Ports



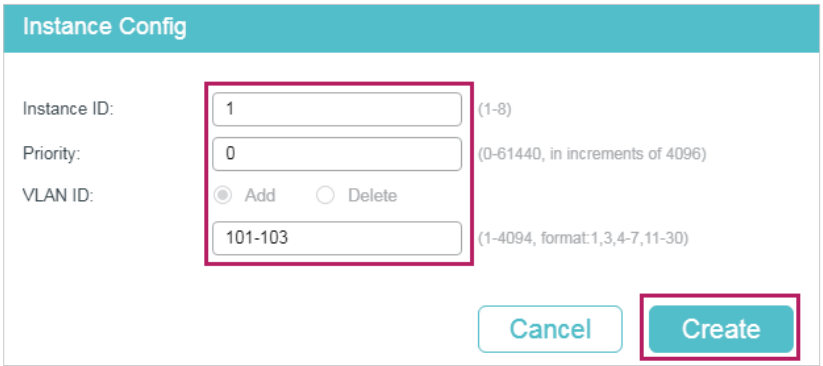
2) Choose the menu **L2 FEATURES > Spanning Tree > MSTP Instance > Region Config** to load the following page. Set the region name as 1 and the revision level as 100. Click **Apply**.

Figure 5-9 Configuring the Region



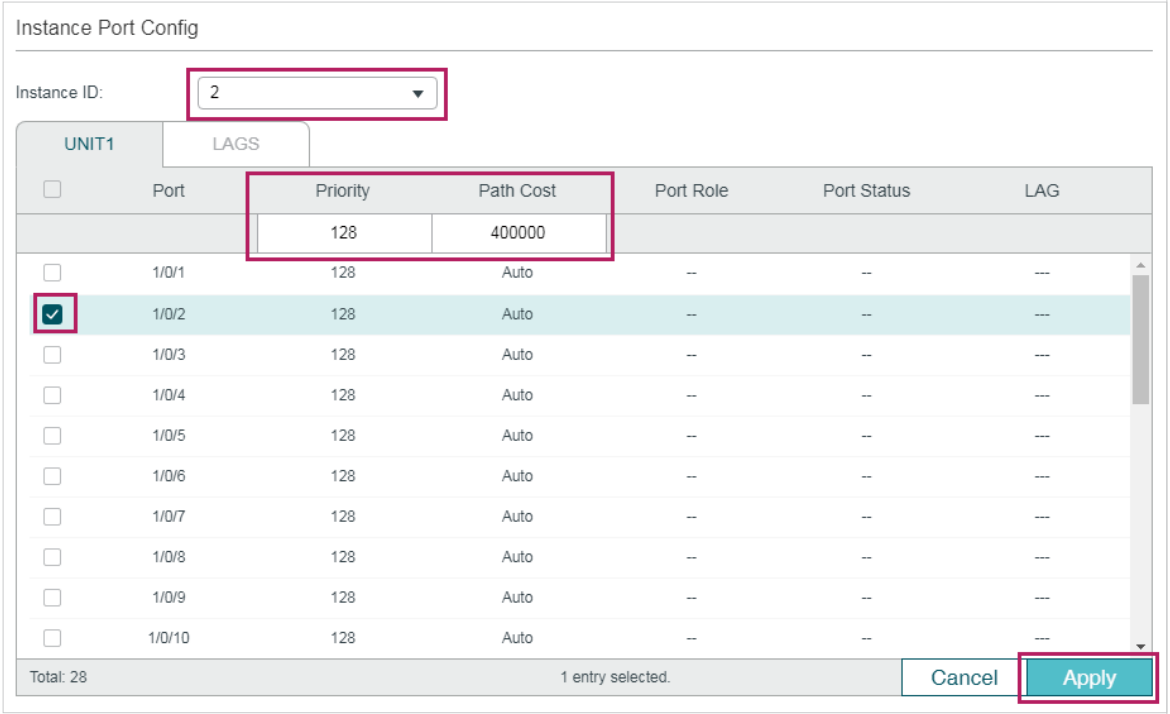
3) Choose the menu **L2 FEATURES > Spanning Tree > MSTP Instance > Instance Config**. Click Add. map VLAN101-VLAN103 to instance 1 and set the Priority as 0; map VLAN104-VLAN106 to instance 2 and set the priority as 32768. Click **Create**.

Figure 5-10 Configuring the VLAN-Instance Mapping



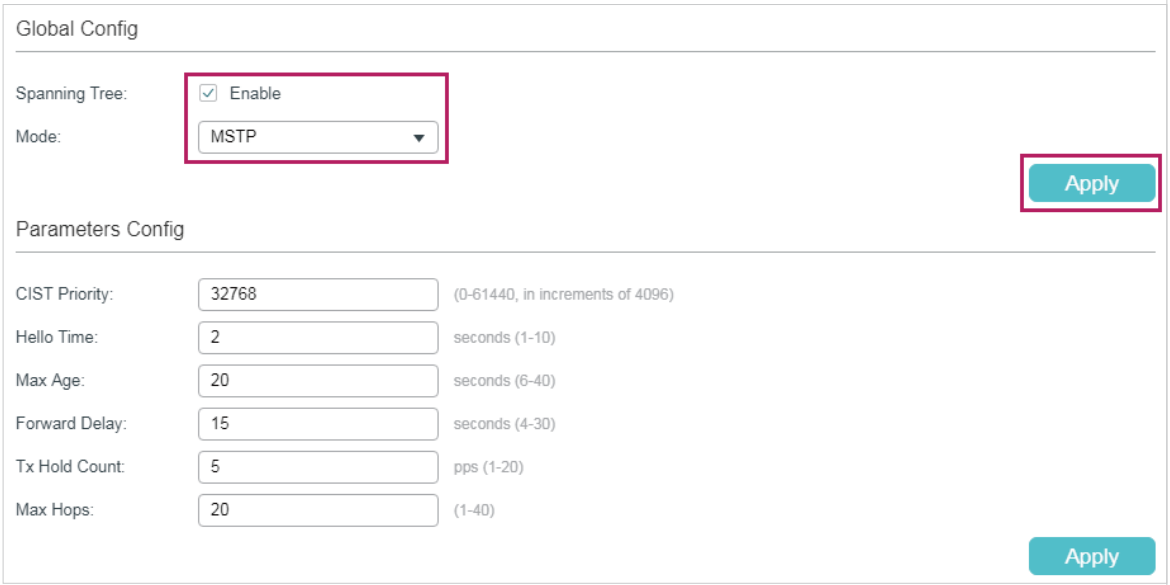
4) Choose the menu **L2 FEATURES > Spanning Tree > MSTP Instance > Instance Port Config** to load the following page. Set the path cost of port 1/0/2 in instance 2 as 400000. Click **Apply**.

Figure 5-11 Configure the Path Cost of Port 1/0/2 in Instance 2



5) Choose the menu **L2 FEATURES > 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. Click **Apply**.

Figure 5-12 Configuring the MSTP Globally

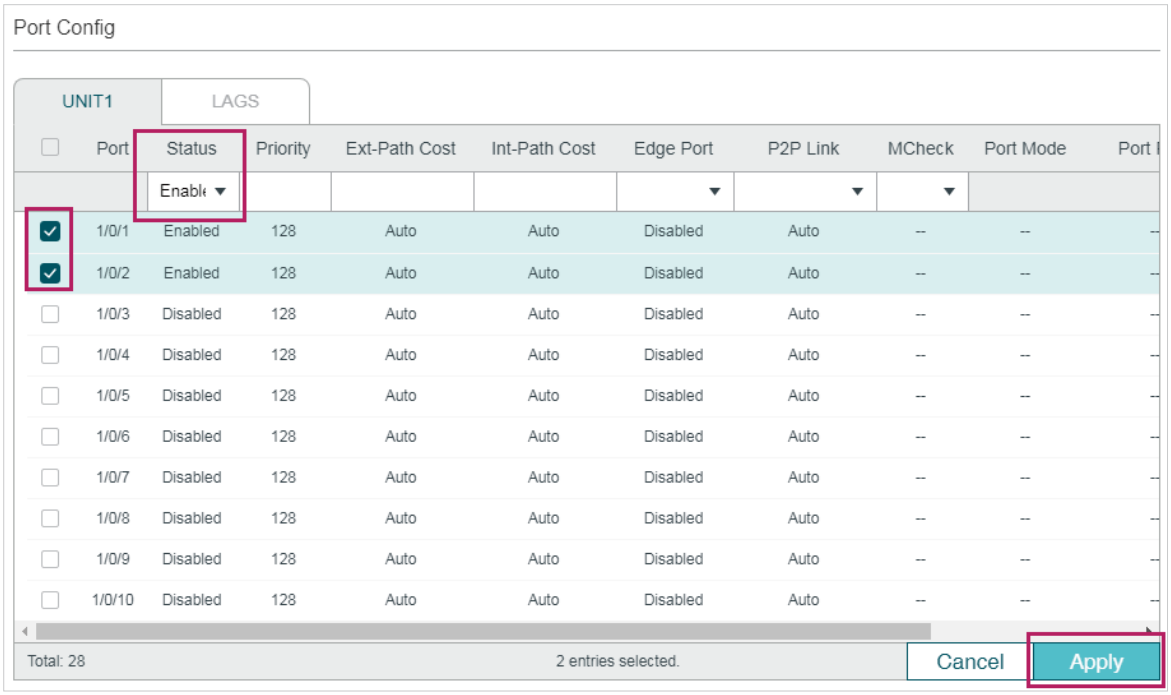


6) Click Save to save the settings.

Configurations for Switch C

1) Choose the menu **L2 FEATURES > 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. Click **Apply**.

Figure 5-13 Enable Spanning Tree Function on Ports



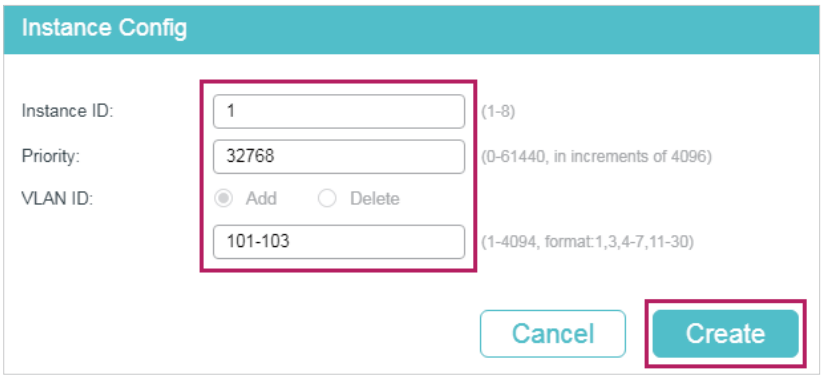
2) Choose the menu **Spanning Tree > MSTP Instance > Region Config** to load the following page. Set the region name as 1 and the revision level as 100. Click **Apply**.

Figure 5-14 Configuring the Region



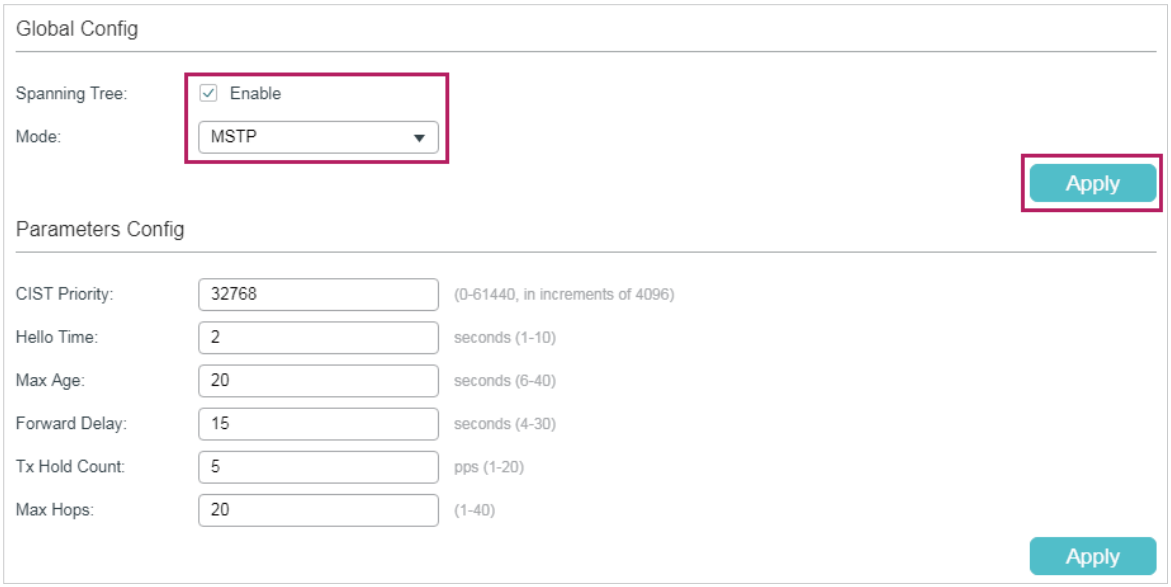
3) Choose the menu **L2 FEATURES > Spanning Tree > MSTP Instance > Instance Config**. Click Add, map VLAN101-VLAN103 to instance 1 and set the priority as 32768; map VLAN104-VLAN106 to instance 2 and set the priority as 0. Click **Create**.

Figure 5-15 Configuring the VLAN-Instance Mapping



4) Choose the menu **L2 FEATURES > 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. Click **Apply**.

Figure 5-16 Configuring the MSTP Globally



5) Click Save 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	Disabled
Mode	STP
CIST Priority	32768
Hello Time	2 seconds
Max Age	20 seconds
Forward Delay	15 seconds
Tx Hold Count	5 pps
Max Hops	20 hops

Table 6-2 Default Settings of the Port Parameters

Parameter	Default Setting
Status	Disabled
Priority	128
Ext-Path Cost	Auto
In-Path Cost	Auto
Edge Port	Disabled
P2P Link	Auto
MCheck	------

Table 6-3 Default Settings of the MSTP Instance

Parameter	Default Setting
Status	Disabled
Revision Level	0

Parameter	Default Setting
Priority	32768
Port Priority	128
Path Cost	Auto

Table 6-4 Default Settings of the STP Security

Parameter	Default Setting
Loop Protect	Disabled
Root Protect	Disabled
TC Guard	Disabled
BPDU Protect	Disabled
BPDU Filter	Disabled
BPDU Forward	Enabled

Part 12

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 LLDP enabled, the switch can get its neighbors' information, and network administrators can use the NMS (Network Management System) to gather these information, helping them to know about the network topology, examine the network connectivity and troubleshoot the network faults.

LLDP-MED (LLDP for Media Endpoint Discovery) is an extension of LLDP and is used to advertise information between network devices and media endpoints. It is specially used together with Auto VoIP (Voice over Internet Protocol) to allow VoIP 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. The neighbors store the received LLDPDU in a standard MIB (Management Information Base), making it possible for the information to be accessed by a NMS (Network Management System) using a management protocol such as the SNMP (Simple Network Management Protocol).

LLDP-MED allows the network device to send its information including Auto VoIP information, PoE (Power over Ethernet) capacity and more to the media endpoint devices (for example, IP phones) for auto-configuration. The media endpoint devices receive the Auto VoIP information and finish the auto-configuration, then send the voice traffic with the desired configuration, which can provide preferential treatment to the voice traffic.

2 LLDP Configurations

T configure LLDP function, follow the steps:

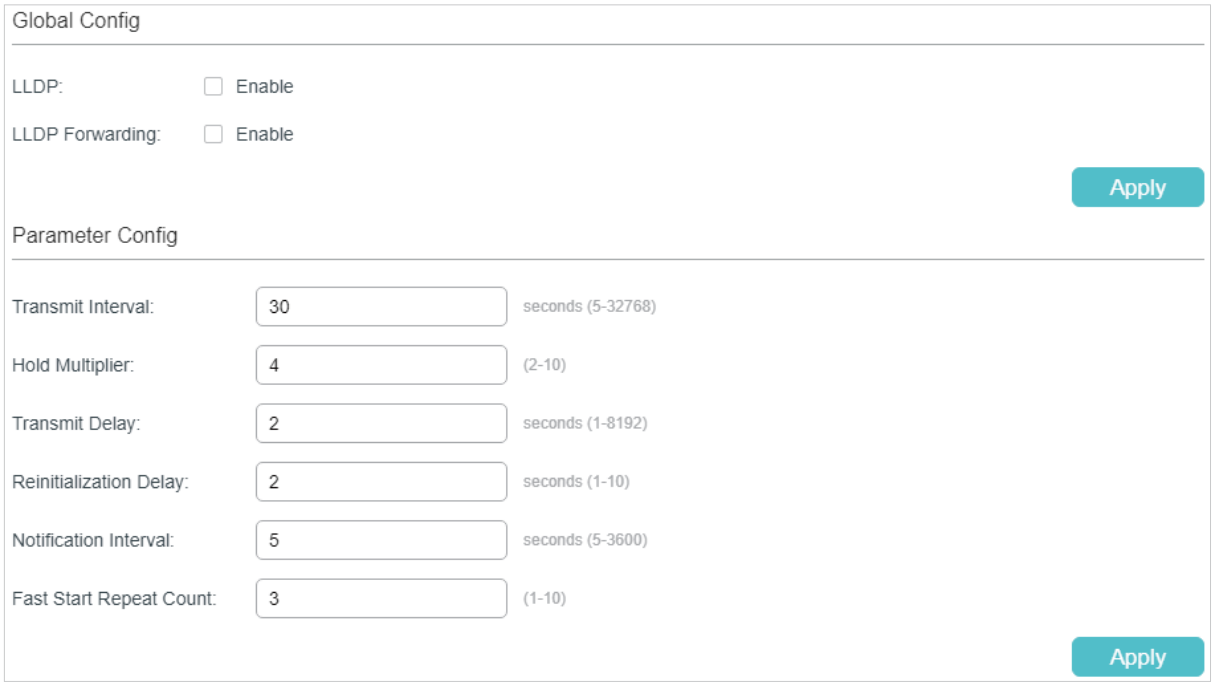
1) Configure the LLDP feature globally.
2) Configure the LLDP feature for the port.

2.1 Using the GUI

2.1.1 Configuring LLDP Globally

Choose the **L2 FEATURES > LLDP** > **LLDP Config** > **Global Config** to load the following page.

Figure 2-1 Global Config



Follow these steps to 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 LLDP function globally.
LLDP Forwarding	(Optional) Enable the switch to forward LLDP messages when LLDP function is disabled.

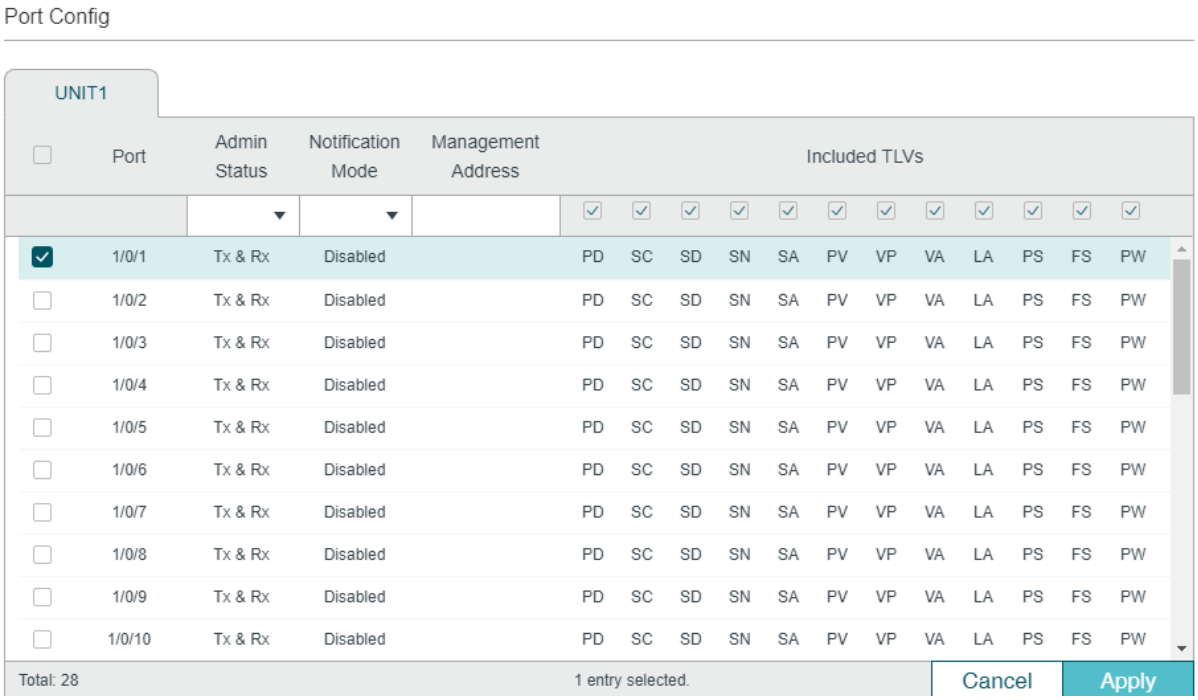
3) In the **Parameter Config** section, configure the LLDP parameters. Click **Apply**.

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	This parameter is a multiplier on the Transmit Interval that determines the actual TTL (Time To Live) value used in an LLDP packet. TTL is the duration that the neighbor device should hold the received LLDP packet before discarding it. The default value is 4. TTL= Hold Multiplier * Transmit Interval.
Transmit Delay	Specify the amount of delay from when Admin Status of ports becomes “Disable“ until reinitialization will be attempted. The default value is 2 seconds.
Reinitialization Delay	Specify the amount of delay from when Admin Status of ports becomes “Disable’ until reinitialization will be attempted. The default value is 2 seconds.
Notification Interval	Enter the interval between successive in seconds Trap messages that are periodically sent from the local device to the NMS. The default value is 5.
Fast Start Repeat Count	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 value 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 Configuring LLDP For the Port

Choose th menu **L2 FEATURES > LLDP** > **LLDP Config** > **Port Config** to load the following page.

Figure 2-2 Port Config



Follow these steps to configure the LLDP feature for the interface.

1) Select one or more ports to configure.
2) Configure the Admin Status and Notification Mode for the port.

Admin Status	Set Admin Status for the port to deal with LLDP packets. Tx&Rx: The port transmits LLDP packets and receives LLDP packets. Rx_Only: The port only receives LLDP packets. Tx_Only: The port only transmits LLDP packets. Disable: The port will not transmit LLDP packets or drop the received LLDP packets.
Notification Mode	(Optional) Enable the switch to send trap messages to the NMS when the information of the neighbor device connected to this port changes.
Management Address	Specify the Management IP address of the port to be notified to the neighbor. Value 0.0.0.0 means the port will notify its default management address to the neighbor.

3) 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. The switch 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.

4) Click **Apply**.

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** *multiplier* (Optional) Specify the amount of time the neighbor device should hold the received information before discarding it. This parameter is a multiplier on the Transmit Interval that determines the actual TTL (Time To Live) value used in an LLDP packet. TTL is the duration that the neighbor device should hold the received LLDP packet before discarding it. TTL= Hold Multiplier * Transmit Interval. *multiplier:* Specify the hold-multiplier. The valid value ranges from 2 to 10, and the default value is 4.
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 the NMS when neighbor information changed. 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	**show lldp interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}** Display LLDP configuration of the corresponding 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 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

To configure LLDP-MED function, follow the steps:

1) Enable LLDP feature globally and configure the LLDP parametres for the ports.
2) Configuring LLDP-MED fast repeat count globally.
3) Enable and configure the LLDP-MED feature on the port.

Configuration Guidelines

LLDP-MED is used together with Auto VoIP to implement VoIP access. Besides the configuration of LLDP-MED feature, you also need configure the Auto VoIP feature. Refer to *Configuring QoS* for detailed instructions.

3.1 Using the GUI

3.1.1 Configuring LLDP Globally

Enable LLDP globally and configure the LLDP parametres for the ports. For the details of LLDP configuration, refer to *LLDP Configuration*.

3.1.1 Configuring LLDP-MED Globally

Choose the menu **L2 FEATURES > LLDP Config** > **LLDP-MED Config** > **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**.

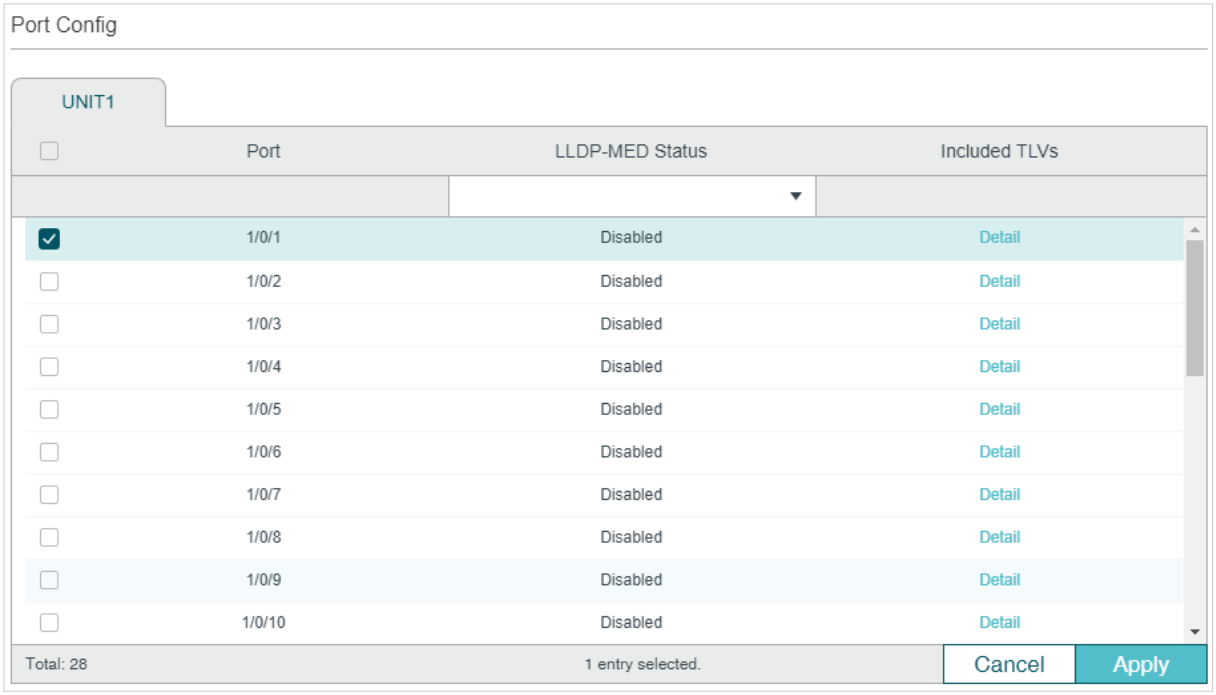
Fast Start Repeat Count	Specify the number of successive LLDP-MED packets that the switch sends when it receives the LLDP-MED packets from the neighbor endpoints. The default is 4. If the switch receives LLDP-MED packets from the neighbor endpoints for the first time, it will send the specified number of LLDP-MED 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 Configuring LLDP-MED for Ports

Choose the menu **L2 FEATURES > LLDP** > **LLDP-MED Config** > **Port Config** to load the following page.

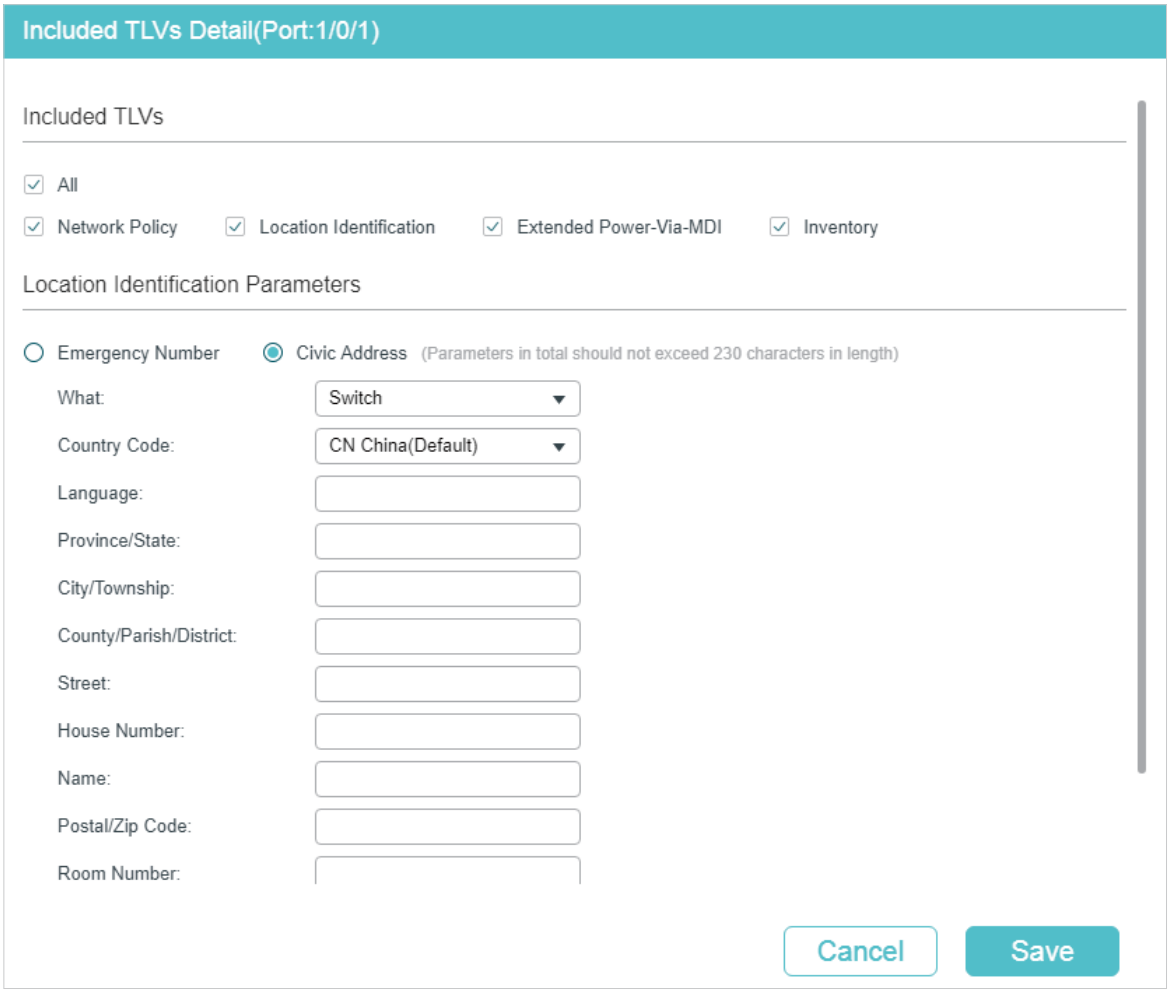
Figure 3-2 LLDP-MED Port Config



Follow these steps to enable LLDP-MED:

1) Select the desired port and enable 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 and 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.

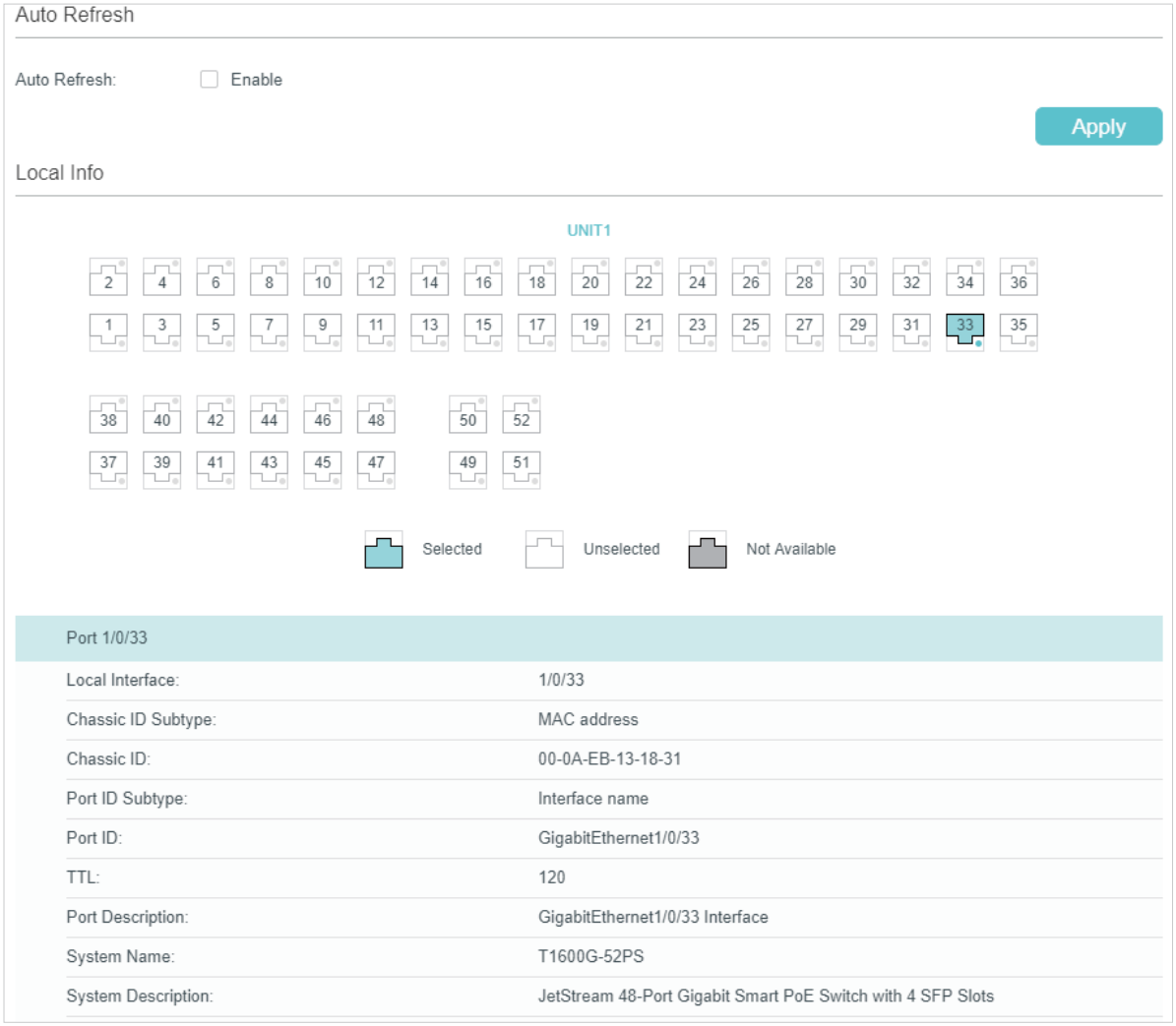
4.1 Using GUI

4.1.1 Viewing LLDP Device Info

- Viewing the Local Info

Choose the menu **L2 FEATURES** > **LLDP** > **LLDP Config** > **Local Info** to load the following page.

Figure 4-1 Local Info



Follow these steps to view the local information:

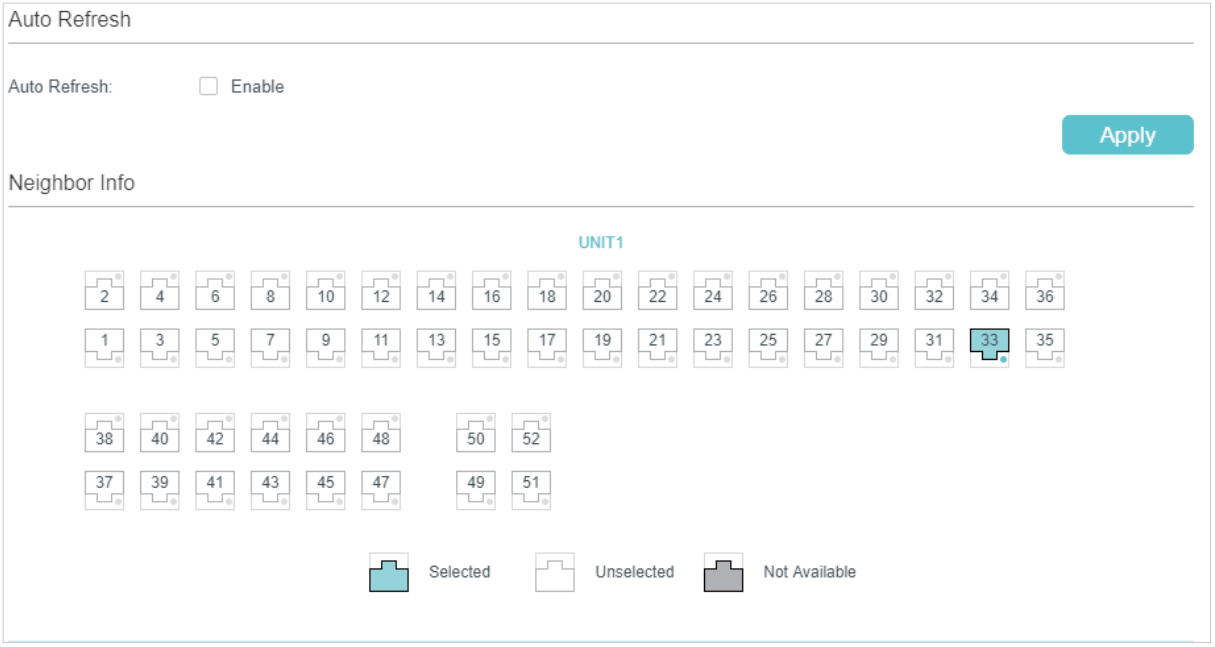
1) In the **Auto Refresh** section, enable the Auto Refresh feature and set the Refresh Rate according to your needs. Click **Apply**.
2) In the **Local Info** section, select the desired port and view its associated local device information.

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 in seconds 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 IP address of the local device.

Viewing the Neighbor Info

Choose the menu **L2 FEATURES** > **LLDP** > **LLDP Config** > **Neighbor Info** to load the following page.

Figure 4-2 Neighbor Info



Follow these steps to view the neighbor information:

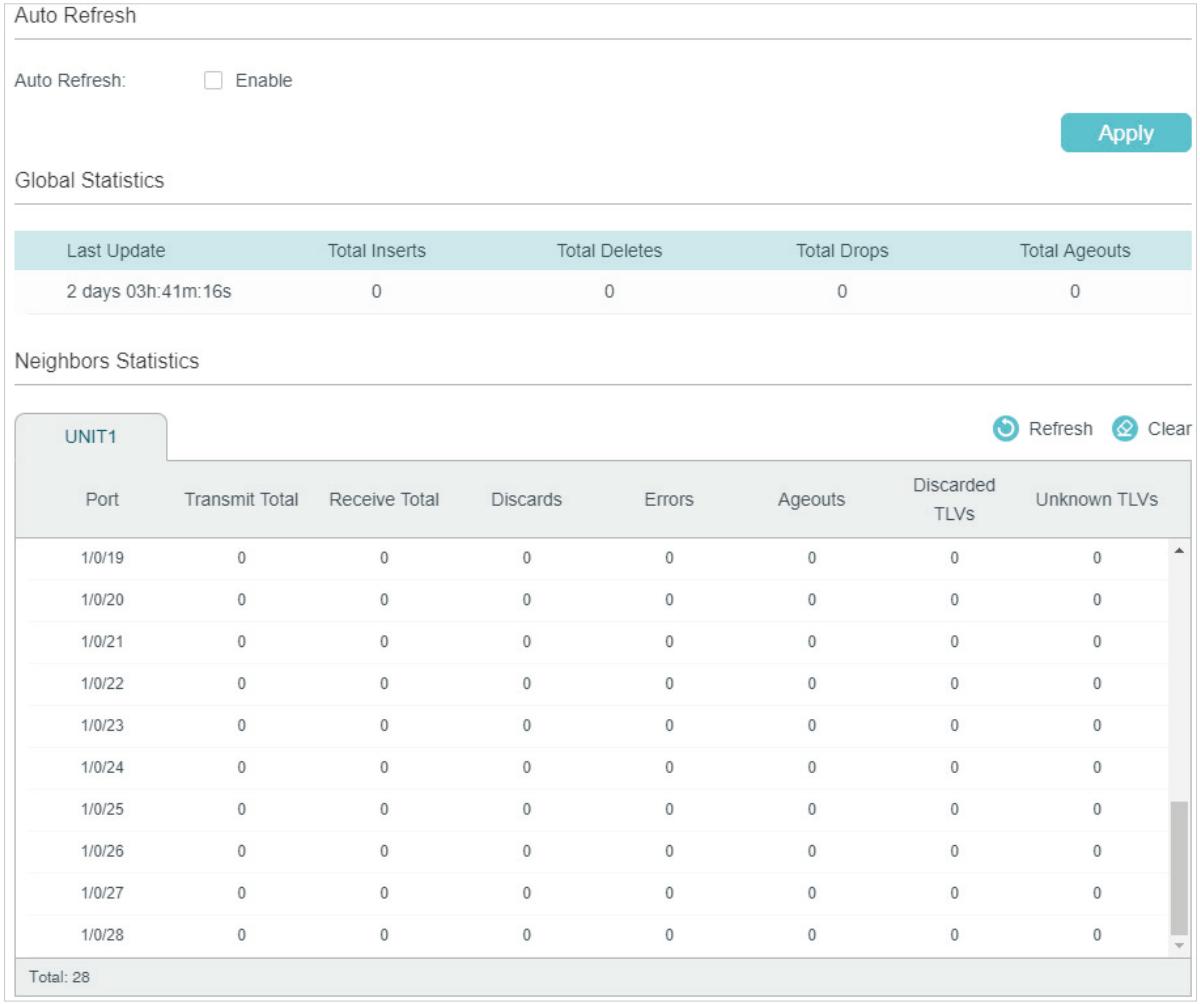
1) In the **Auto Refresh** section, enable the Auto Refresh feature and set the Refresh Rate according to your needs. Click **Apply**.
2) In the **Neighbor Info** section, select the desired port and view its associated neighbor device information.

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 **L2 FEATURES** > **LLDP** > **LLDP Config** > **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 total number of neighbors during latest update time.
Total Deletes	Displays the number of neighbors deleted by the local device. The port will delet neighbors when the port is disabled or the TTL of the LLDP packets sent by the neighbor is 0.
Total Drops	Displays the number of neighbors dropped by the local device. Each port can learn a maximum of 80 neighbor device, and the subsquent neighbors will be dropped when the limit is exceeded.

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* **| ten-gigabitEthernet** *port* **}**

View the statistics of the corresponding port on the local device.

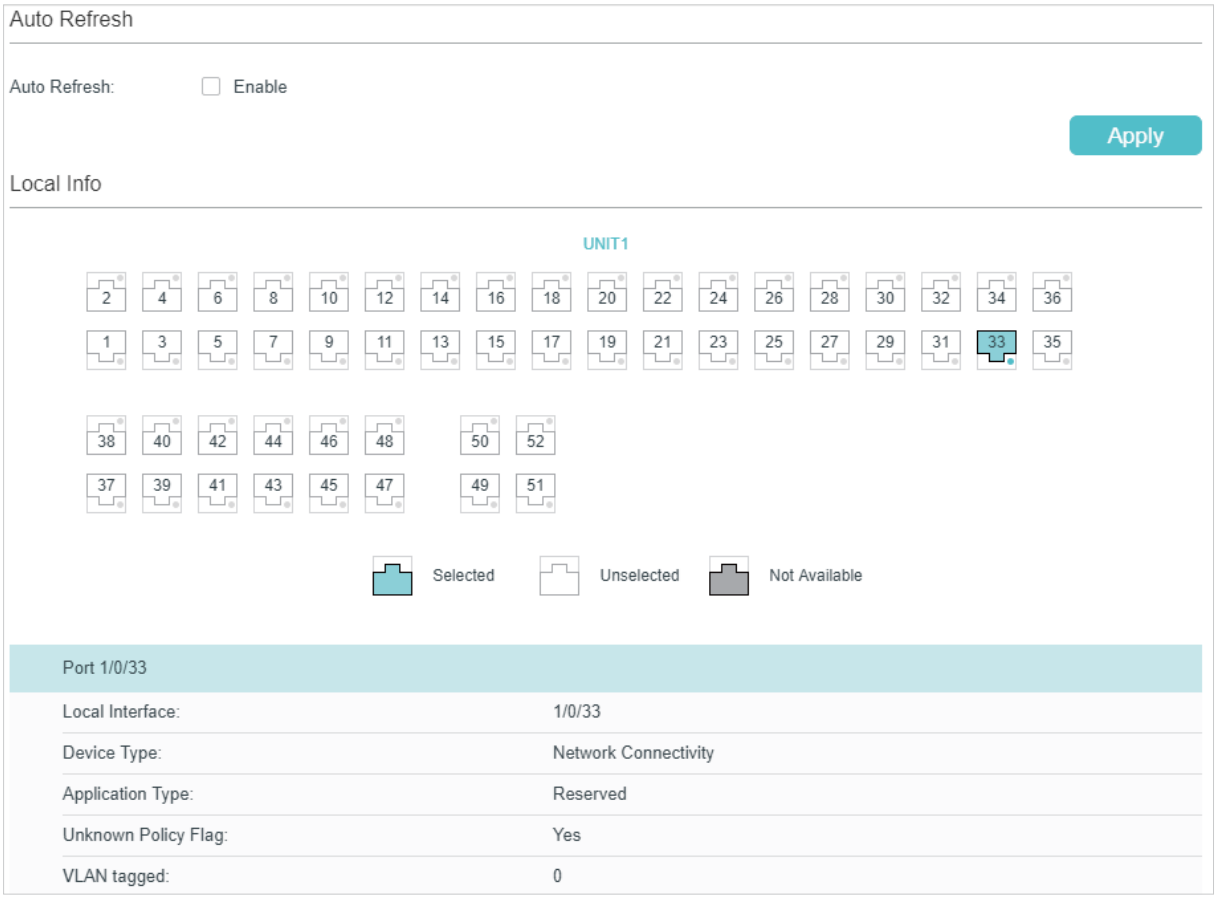
5 Viewing LLDP-MED Settings

5.1 Using GUI

Choose the menu **L2 FEATURES** > **LLDP** > **LLDP-MED Config** > **Local Info** to load the following page.

- 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.

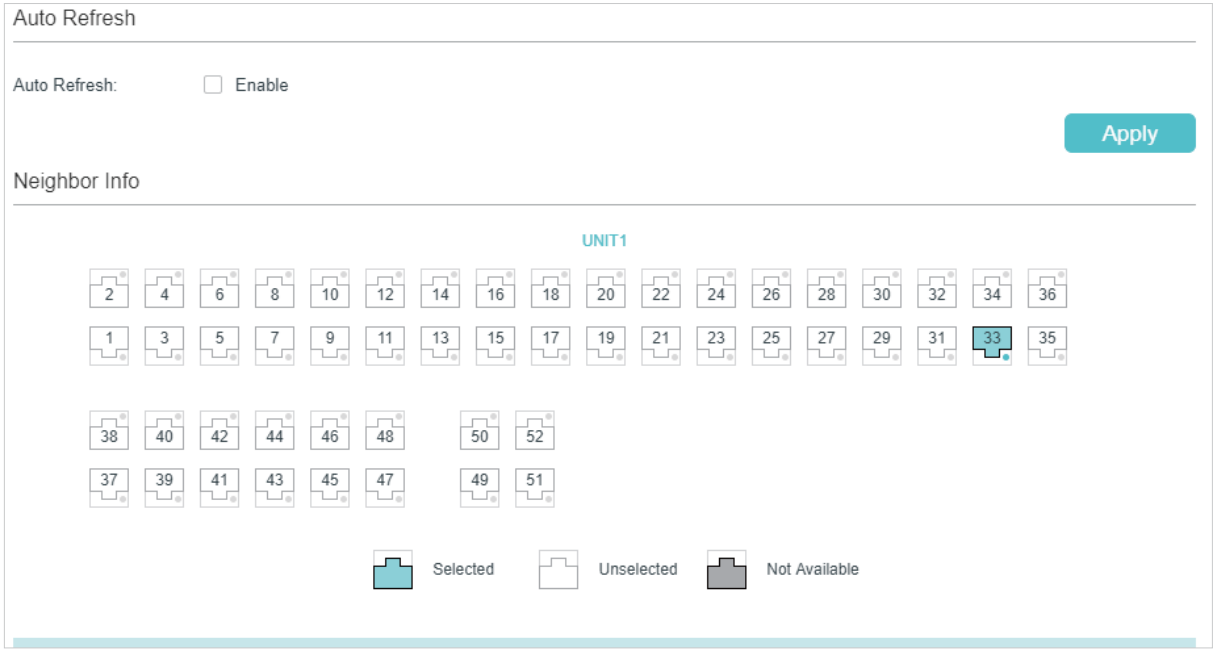
Local Interface	Displays the local port ID.
Device Type	Displays the local device type defined by LLDP-MED.LLDP-MED.

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

Choose the menu **L2 FEATURES** > **LLDP** > **LLDP-MED Config** > **Neighbor Info** to load the following page.

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 **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 Network Requirements

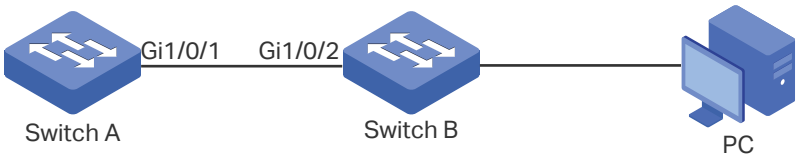
The network administrator needs view the information of the devices in the company network to know about the link situation and network topology so that he can troubleshoot the potential network faults in advance.

6.2 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



6.3 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.

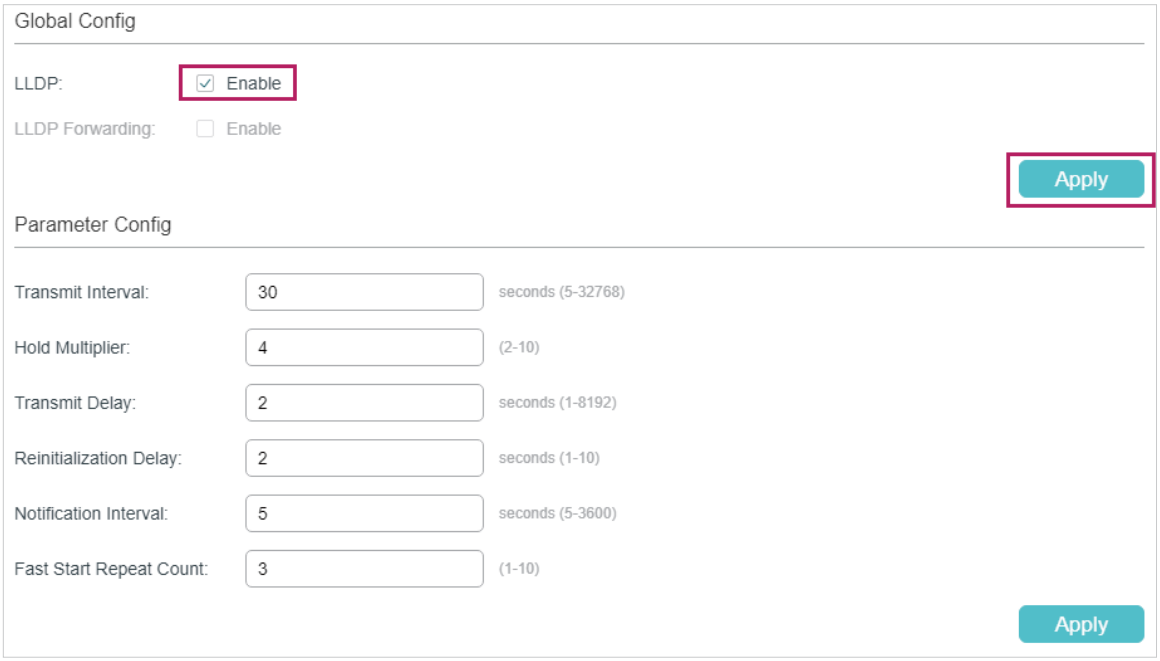
Configuring Switch A and Switch B:

The configurations of Switch A and Switch B are similar. The following introductions take Switch A as an example. Demonstrated with T1600G-52TS, this chapter provides configuration procedures in two ways: using the GUI and using the CLI.

6.4 Using the GUI

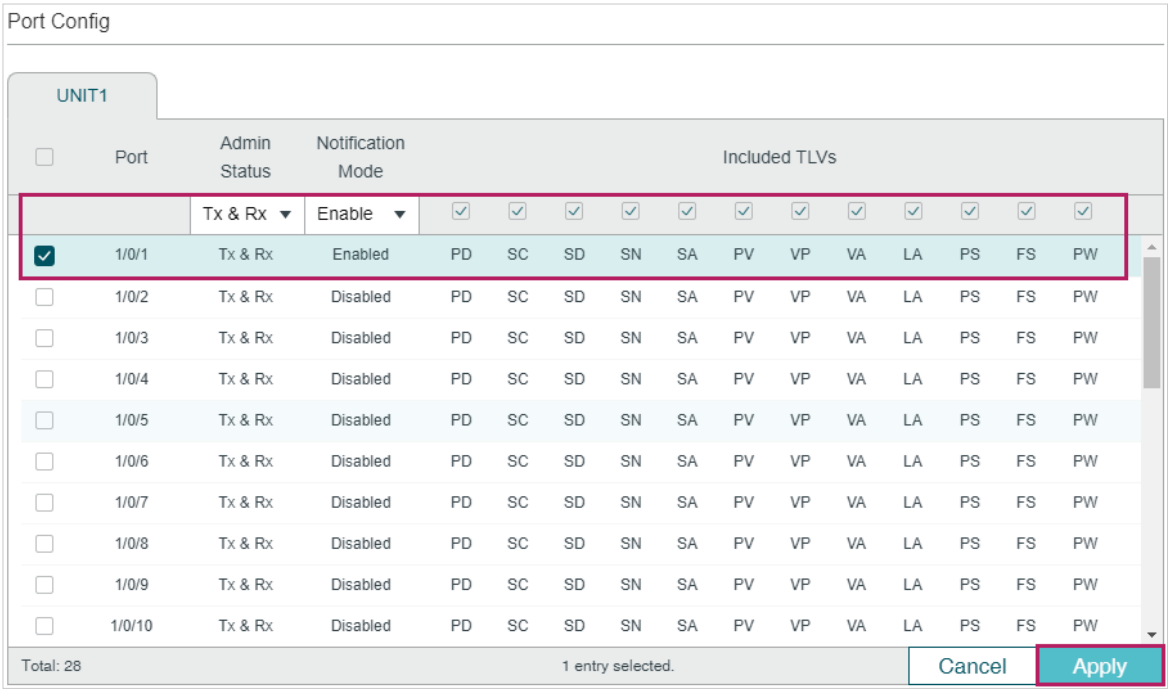
1) Choose the menu **L2 FEATURES** > **LLDP** > **LLDP Config** > **Global Config** to load the following page. Enable LLDP globally and configure the related parameters. Here we take the default settings as an example.

Figure 6-2 LLDP Global Config



2) Choose the menu **L2 FEATURES** > **LLDP** > **LLDP Config** > **Port Config** to load the following page. Set the Admin Status of port Gi1/0/1 as Tx&Rx, enable Notification Mode and configure all the TLVs included in the outgoing LLDP packets.

Figure 6-3 LLDP Port Config



6.5 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: T1600G-52TS

System description: JetStream 48-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: T1600G-52TS 3.0
Firmware Revision: Reserved
Software Revision: 3.0.0 Build 20170918 Rel.71414(s)
Serial Number: Reserved
Manufacturer Name: TP-Link
Model Name: T1600G-52TS 3.0
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

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
Reinitialization Delay	2 seconds
Notification Interval	5 seconds
Fast Start Repeat Count	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 Repeat Count	4
LLDP-MED Status (port)	Disable
Included TLVs	All

Part 13

Configuring Layer 3 Interfaces

CHAPTERS

1. Overview
2. Layer 3 Interface Configurations
3. Appendix: Default Parameters

1 Overview

Interfaces are used to exchange data and interact with interfaces of other network devices. Interfaces are classified into Layer 2 interfaces and Layer 3 interfaces.

- Layer 2 interfaces are the physical ports on the switch panel. They forward packets based on MAC address table.
- Layer 3 interfaces are used to forward IPv4 and IPv6 packets using static or dynamic routing protocols. You can use Layer 3 interfaces for IP routing and inter-VLAN routing.

This chapter introduces the configurations for Layer 3 interfaces. The supported types of Layer 3 interfaces are shown as below:

Table 1-1 Supported Types of Layer 3 interfaces

Type	Description
VLAN Interface	A Layer 3 interface with which acts as the default gateway of all the hosts in the corresponding VLAN.
Loopback Interface	An interface of which the status is always up.
Routed Port	A physical port configured as an Layer 3 port.
Port-channel Interface	Several routed ports are bound together and configured as an Layer 3 interface.

2 Layer 3 Interface Configurations

To complete IPv4 interface configuration, follow these steps:

1) Create an 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:

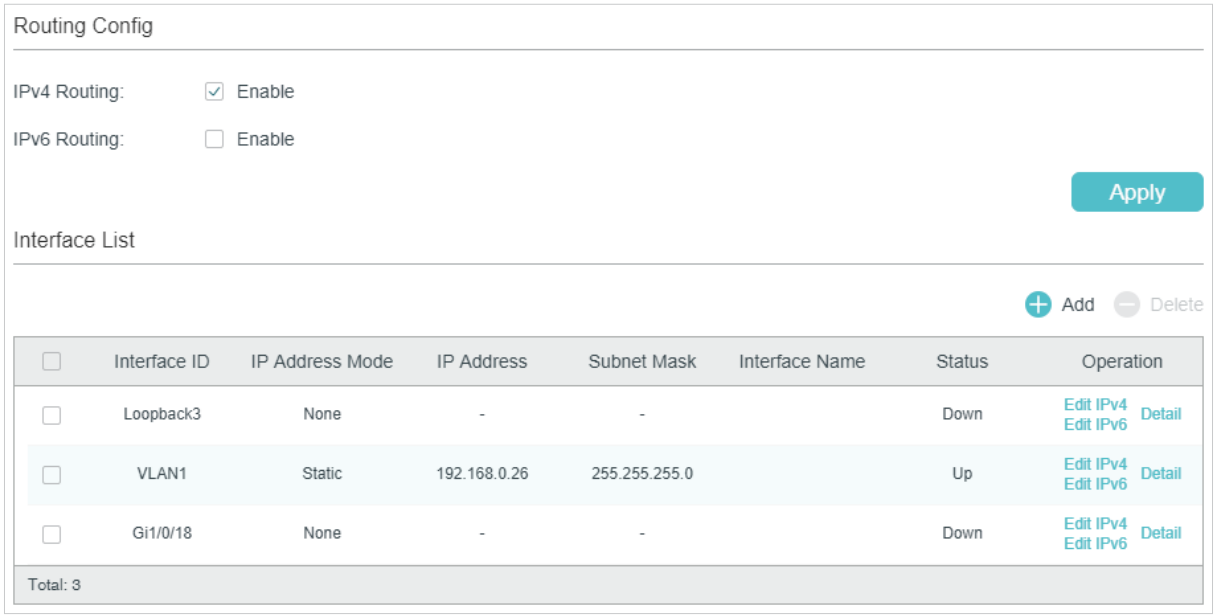
1) Create an Layer 3 interface
2) Configure IPv6 parameters of the created interface
3) View detailed information of the created interface

2.1 Using the GUI

2.1.1 Creating an Layer 3 Interface

Choose the menu **L3 FEATURES> Interface** to load the following page.

Figure 2-1 Creating an Layer 3 Interface



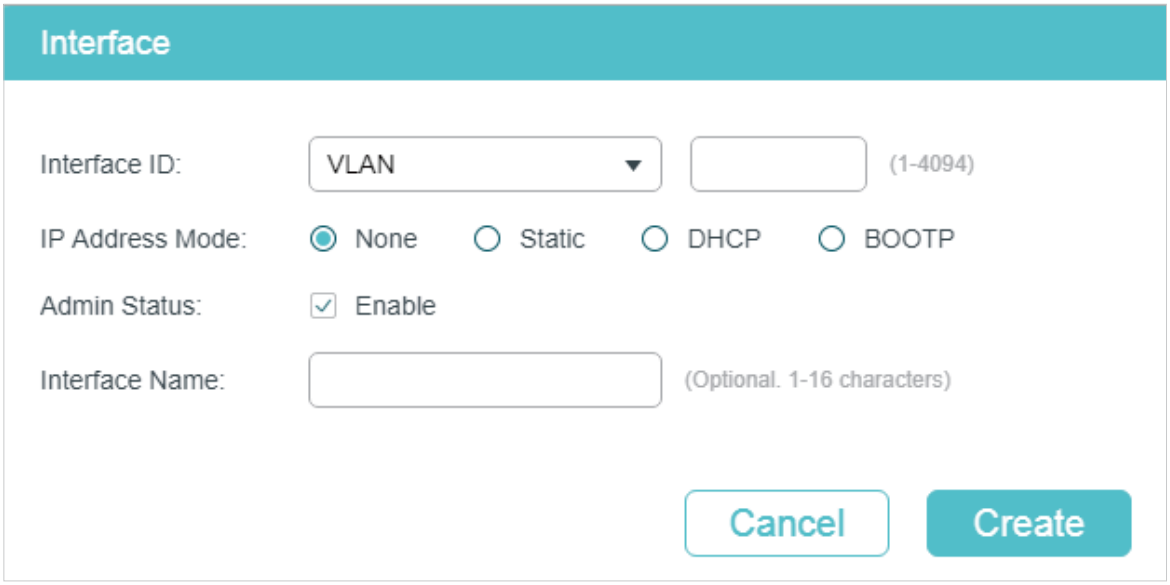
Follow these steps to create an Layer 3 interface.

1) In the **Routing Config** section, enable IPv4 routing or IPv6 routing. Then click **Apply**.

IPv4 Routing	Enable IPv4 routing function globally for all Layer 3 interfaces. It is enabled by default.

IPv6 Routing	(Optional) Enable IPv6 routing function globally for all Layer 3 interfaces. It is disabled by default.

2) In the **Interface List** section, click Add to load the following page, and configure the corresponding parameters for the Layer 3 interface. 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 to the interface. **Static:** Assign an IP address to the interface manually. **DHCP:** Assign an IP address to the interface through the DHCP server. **BOOTP:** Assign an IP address to the interface through the BOOTP server.
DHCP Option 12	If you select DHCP as the IP Address Mode, configure the Option 12 here. DHCP Option 12 is used to specify the client's name.
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 a name for the interface.

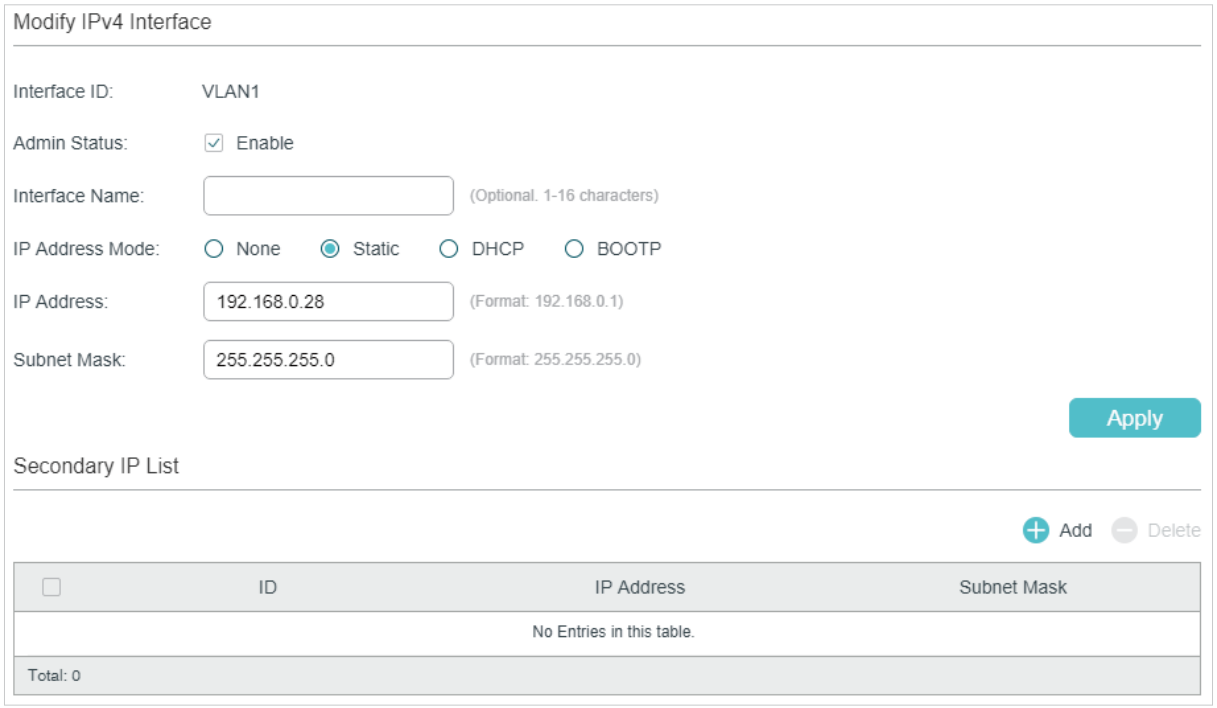
Note:

The created interface is an IPv4 interface. To configure the IPv6 features, please click "Edit IPv6" after the interface is created.

2.1.2 Configuring IPv4 Parameters of the Interface

In **Figure 2-1** you can view the corresponding interface you have created in the **Interface List** section. On the corresponding interface entry, click **Edit IPv4** to load the following page and edit the IPv4 parameters of the interface.

Figure 2-2 Configuring the IPv4 Parameters

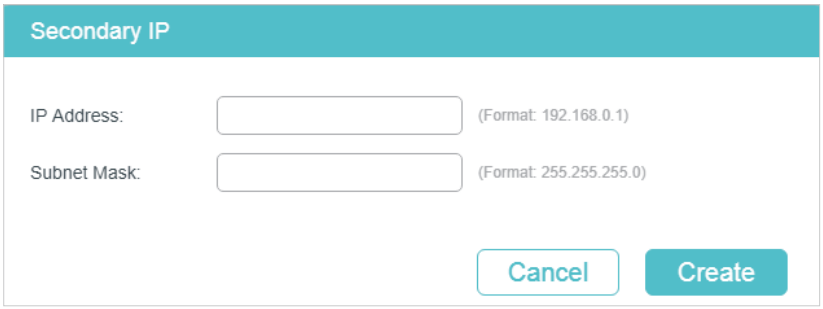


1) In the **Modify IPv4 Interface** section, configure relevant parameters for the interface according to your actual needs. Then click **Apply**.

Interface ID	Displays the interface ID.
Admin Status	Enable the Layer 3 capabilities for the interface.
Interface Name	(Optional) Enter a name for 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:** Obtain an IP address through DHCP. **BOOTP:** Obtain 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.

DHCP Option 12	If you select DHCP as the IP Address Mode, configure the Option 12 here. DHCP Option 12 is used to specify the client's name.

2) In the **Secondary IP List** section, click Add to add a secondary IP for the specified interface which allows you to have two logical subnets. Then click **Create**.



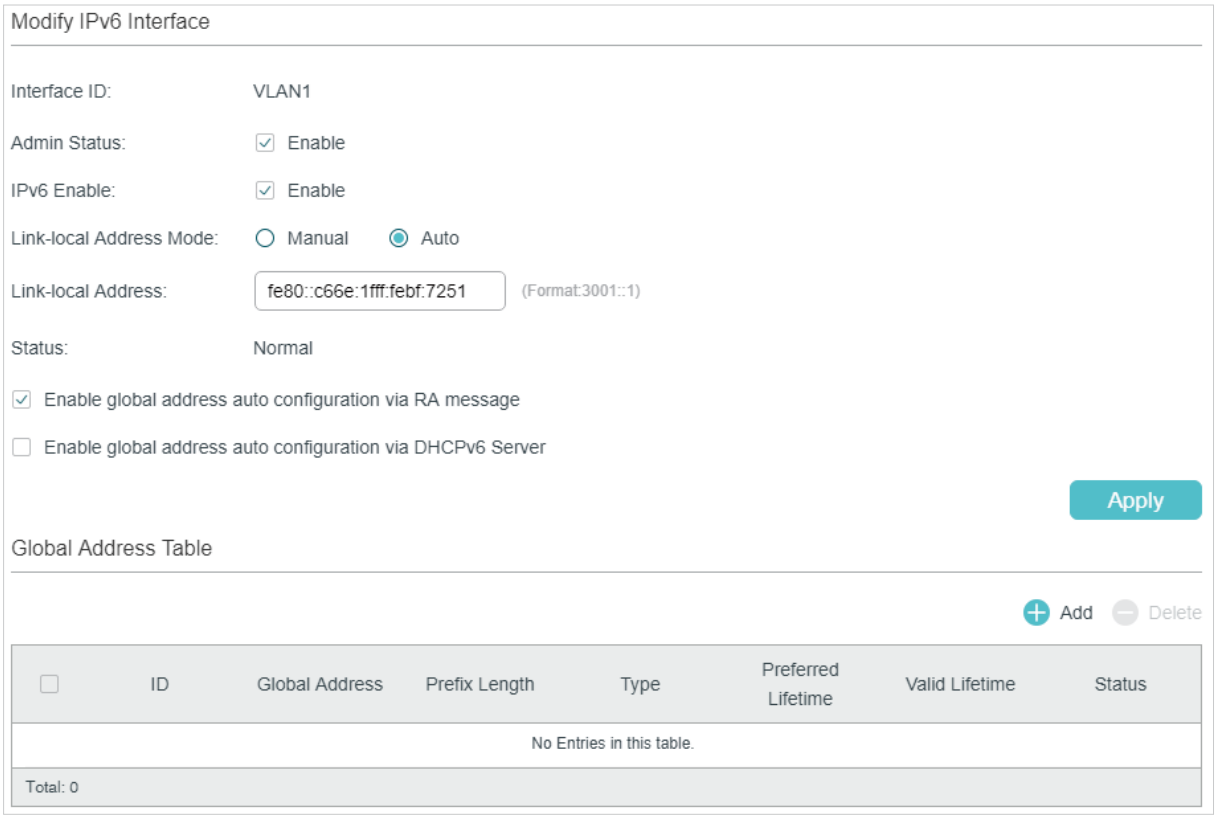
IP Address	Specify the secondary IP address of the interface.
Subnet Mask	Specify the subnet mask of the secondary IP address.

3) (Optional) In the **Secondary IP List** section, you can view the corresponding secondary IP entry you have created.

2.1.3 Configuring IPv6 Parameters of the Interface

In **Figure 2-1**, you can view the corresponding interface entry you have created 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) In the **Modify IPv6 Interface** section, enable IPv6 feature for the interface and configure the corresponding parameters . Then click **Apply**.

Interface ID	Displays the interface ID.
Admin Status	Enable the Layer 3 capabilities for the interface.
IPv6 Enable	Enable the IPv6 feature of the interface.
Link-local Address 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 generates a link-local address automatically.
Link-local Address	Enter a link-local address if you choose “Manual” as the Link-Local Address Mode.

Status	Displays the status of the link-local address. An IPv6 address cannot be used before pass the DAD (Duplicate Address Detection), which is used to detect the address conflicts. In the DAD process, the IPv6 address may in three different status: **Normal:** Indicates that the link-local address passes the DAD and can be used normally. **Try:** Indicates that the link-local address is in the progress of DAD and cannot be used right now. **Repeat:** Indicates that the link-local address is duplicated, this address is already used by another node and cannot be used by the interface.

2) Configure IPv6 global address of the interface via following three ways:

Via RA Message:

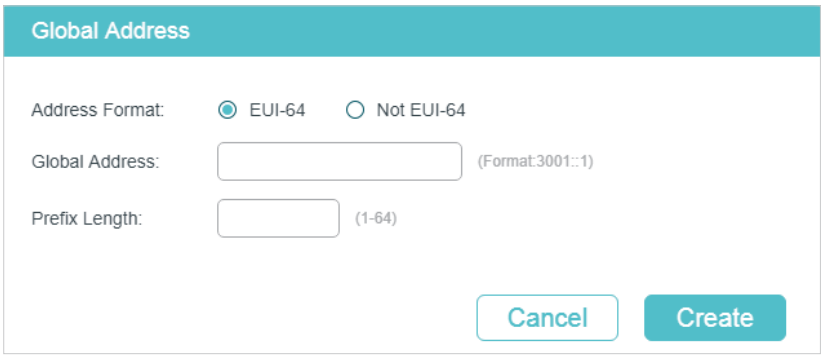
Enable global address auto configuration via RA message	With this option enabled, the interface automatically generates a global address and other information according to the address prefix and other configuration parameters from the received RA (Router Advertisement) message.

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:

In the **Global Address Table** section, click Add to manually assign an IPv6 global address to the interface.



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.

Prefix Length	Configure the prefix length of the global address.

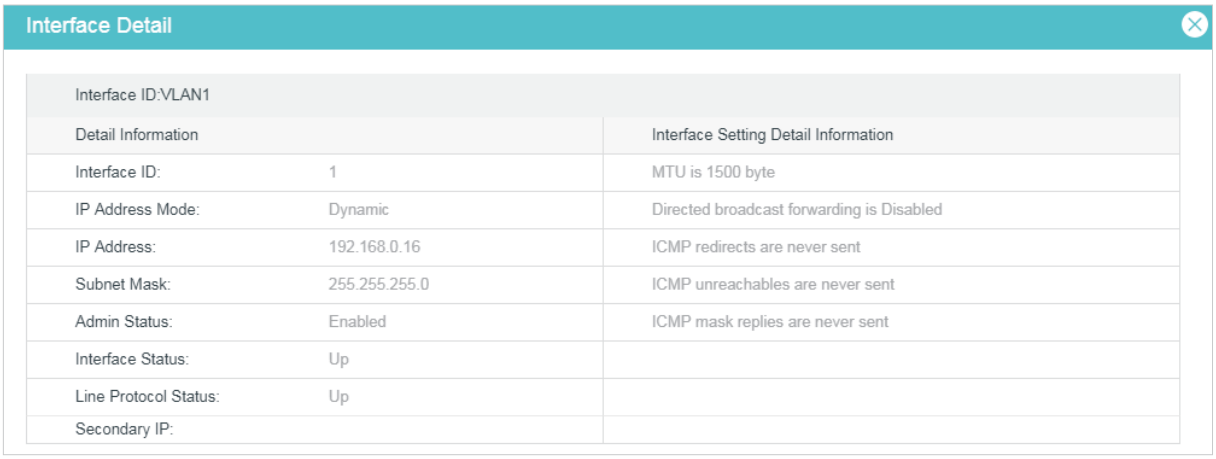
3) View the global address entry in the Global Address Table.

Global Address	View or modify the global address.
Prefix Length	View or 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. Preferred lifetime is the length of time that a valid IPv6 address is preferred. When the preferred time expires, the address becomes deprecated but still can be used, and you need to switch to another address.
Valid Lifetime	Displays the valid lifetime of the global address. Valid lifetime is the length of time that an IPv6 address is in the valid state. When the valid lifetime expires, the address become invalid and can be no longer usable.
Status	Displays the status of the link-local address. An IPv6 address cannot be used before pass the DAD (Duplicate Address Detection), which is used to detect the address conflicts. In the DAD process, the IPv6 address may in three different status: **Normal:** Indicates that the global address passes the DAD and can be normally used. **Try:** Indicates that the global address is in the progress of DAD and cannot be used right now. **Repeat:** Indicates that the global address is duplicated, this address is already used by another node. This address cannot be used by the interface.

2.1.4 Viewing Detail Information of the Interface

In **Figure 2-1** you can view the corresponding interface entry you have created 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 an Layer 3 Interface

Follow these steps to create an 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 { port-cahnnel** *port-channel* **| range port-channel** *port-channel-list* **}** Enter interface configuration mode. *port-channel*: Specify the port channel, the valid value ranges from 1 to 14. *port-channel-list:* Specify the list of the port-channel interface, for example 1-3, 5. **no switchport** Switch the port channel to an Layer 3 port channel interface.
Step 3	**description** *string* Specify a description for the Layer 3 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-id*} Enter Layer 3 interface configuration mode. *interface-type*: Type of the Layer 3 interface, including fastEthernet, gigabitEthernet, ten-gigabitEthernet, loopback and VLAN. *interface-id:* The interface ID.
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. 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-id* } Enter Layer 3 interface configuration mode. *interface-type*: Type of the Layer 3 interface, including fastEthernet, gigabitEthernet, ten-gigabitEthernet, loopback and VLAN. *interface-id:* The interface ID.
Step 3	**ipv6 enable** Enable the IPv6 feature on the specified 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 Default Settings of Routing Config

Parameter	Default Setting
IPv4 Routing	Enable
IPv6 Routing	Disable

Table 3-2 Configuring the IPv4 Parameters of the Interface

Parameter	Default Setting
Interface ID	VLAN
IP Address Mode	None
Admin Status	Enable

Table 3-3 Configuring the IPv6 Parameters of the Interface

Parameter	Default Setting
Admin Status	Enable
IPv6 Enable	Enable
Link-local Address Mode	Auto
Enable global address auto configuration via RA message	Enable
Enable global address auto configuration via DHCPv6 Server	Disable

Part 14

Configuring Routing

CHAPTERS

1. Overview
2. IPv4 Static Routing Configuration
3. IPv6 Static Routing Configuration
4. Viewing Routing Table
5. Example for Static Routing

1 Overview

Routing table is used for a Layer 3 device (in this configuration guide, it means the switch) to forward packets to the correct destination. When the switch receives packets of which the source IP address and destination IP address are in different subnets, it will check the routing table, find the correct outgoing interface then forward the packets.

The routing table mainly contains two types of routing entries: dynamic routing entries and static routing entries.

Dynamic routing entries are automatically generated by the switch. The switch use dynamic routing protocols to automatically calculate the best route to forward packets.

Static routing entries are manually added none-aging routing entries. In 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.

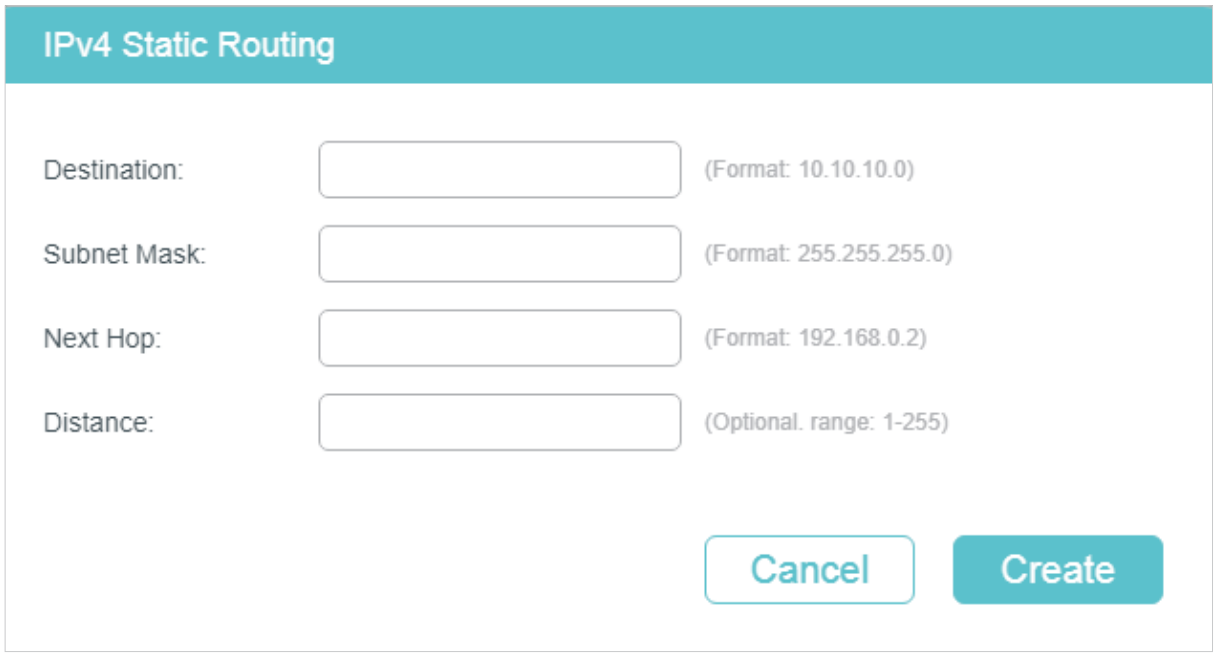
The switch supports IPv4 static routing and IPv6 static routing configuration.

2 IPv4 Static Routing Configuration

2.1 Using the GUI

Choose the menu **L3 FEATURES > Static Routing > IPv4 Static Routing** and click Add to load the following page.

Figure 2-1 Configuring the IPv4 Static Routing



Configure the corresponding parameters to add an IPv4 static routing entry. 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 the trust rating of a routing entry. A higher value means a lower trust rating. Among the routes to the same destination, the route with the lowest distance value will be recorded in the IPv4 routing table. The valid value ranges from 1 to 255 and the default value is 1.

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

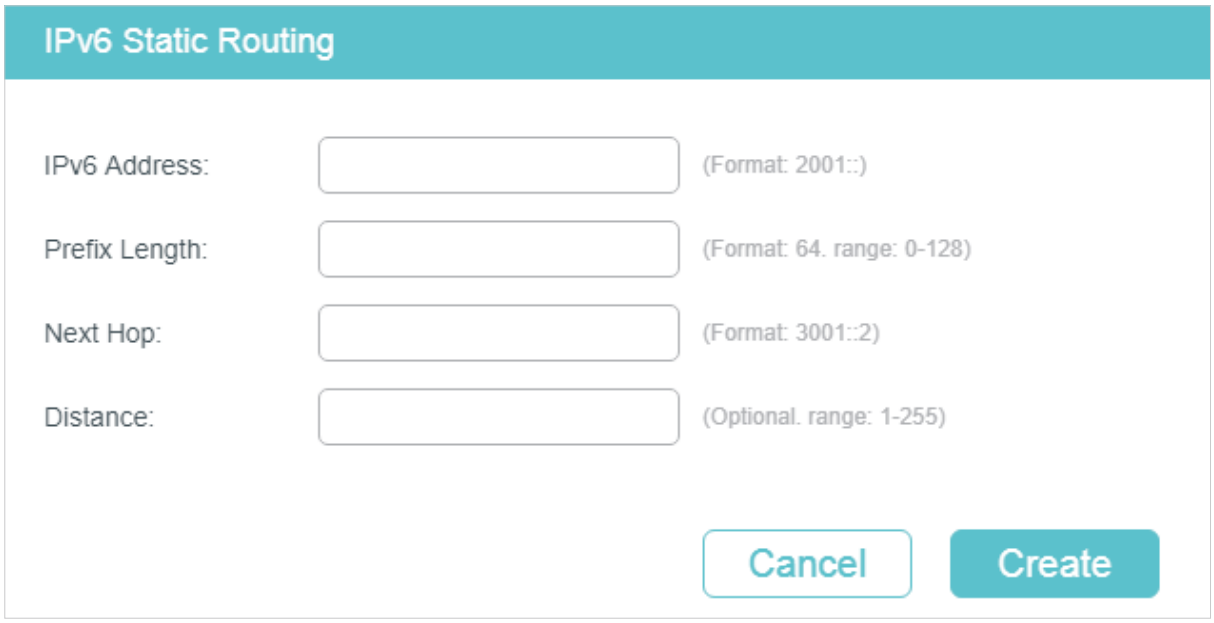
Switch#copy running-config startup-config

3 IPv6 Static Routing Configuration

3.1 Using the GUI

Choose the menu **L3 FEATURES > Static Routing > IPv6 Static Routing > IPv6 Static Routing Table** and click Add to load the following page.

Figure 3-1 Configuring the IPv6 Static Routing



Configure the corresponding parameters to add an IPv6 static routing entry. 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 the trust rating of a routing entry. A higher value means a lower trust rating. Among the routes to the same destination, the route with the lowest distance value will be recorded in the IPv6 routing table. The valid value ranges from 1 to 255 and the default value is 1

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 the 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 **L3 FEATURES > Routing Table > IPv4 Routing Table > IPv4 Routing Information Summary** to load the following page.

Figure 4-1 Viewing IPv4 Routing Table

Protocol	Destination Network	Next Hop	Distance	Metric	Interface Name
Connected	192.168.0.0/24	192.168.0.26	0	1	
Static	192.168.30.0/24	192.168.0.36	5	0	
Total: 2					

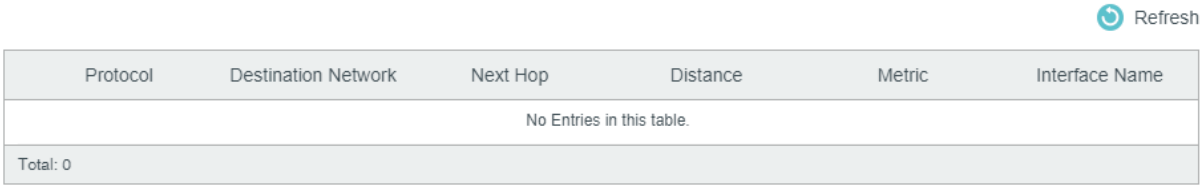
View the IPv4 routing entries.

Protocol	Displays the type of the routing entry. **Connected**: The destination network is directed connected to the switch. **Static**: The routing entry is a manually added static routing 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 the trust rating of a routing entry. A higher value means a lower trust rating. Among the routes to the same destination, the route with the lowest distance value will be recorded in the IPv6 routing table.
Metric	Displays the metric to reach the destination IP address.
Interface Name	Displays the name of the gateway interface.

4.1.2 Viewing IPv6 Routing Table

Choose the menu **L3 FEATURES> Routing Table > IPv6 Routing Table > IPv6 Routing Information Summary** to load the following page.

Figure 4-2 Viewing IPv6 Routing Table



View the IPv6 routing entries.

Protocol	Displays the type of the routing entry. **Connected**: The destination network is directed connected to the switch. **Static**: The routing entry is a manually added static routing entry.
Destination Network	Displays the destination IPv6 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 the trust rating of a routing entry. A higher value means a lower trust rating. Among the routes to the same destination, the route with the lowest distance value will be recorded in the IPv6 routing table.
Metric	Displays the metric to reach the destination IPv6 address.
Interface Name	Displays the name of the gateway interface.

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.

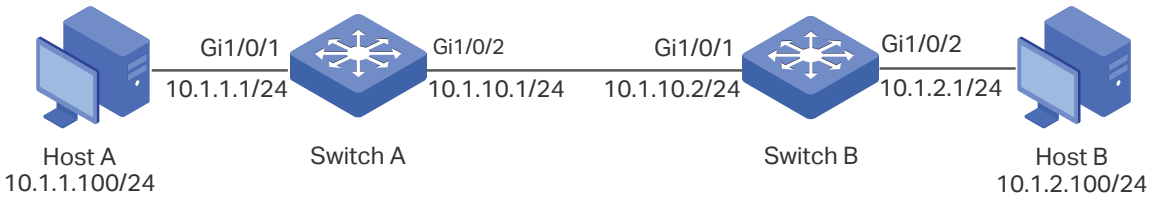
connected: View the connected IPv6 routes.

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 to 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 T1600G-52TS, 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 **L3 FEATURES > Interface** to 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

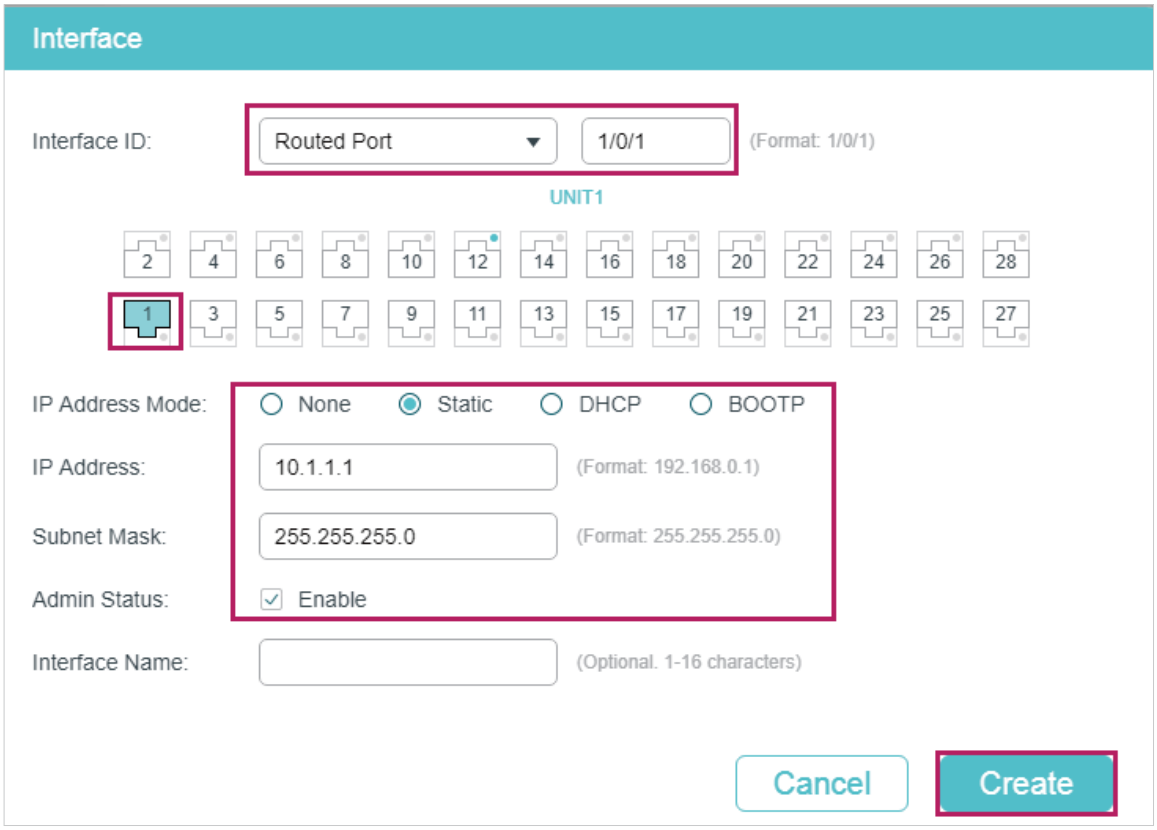
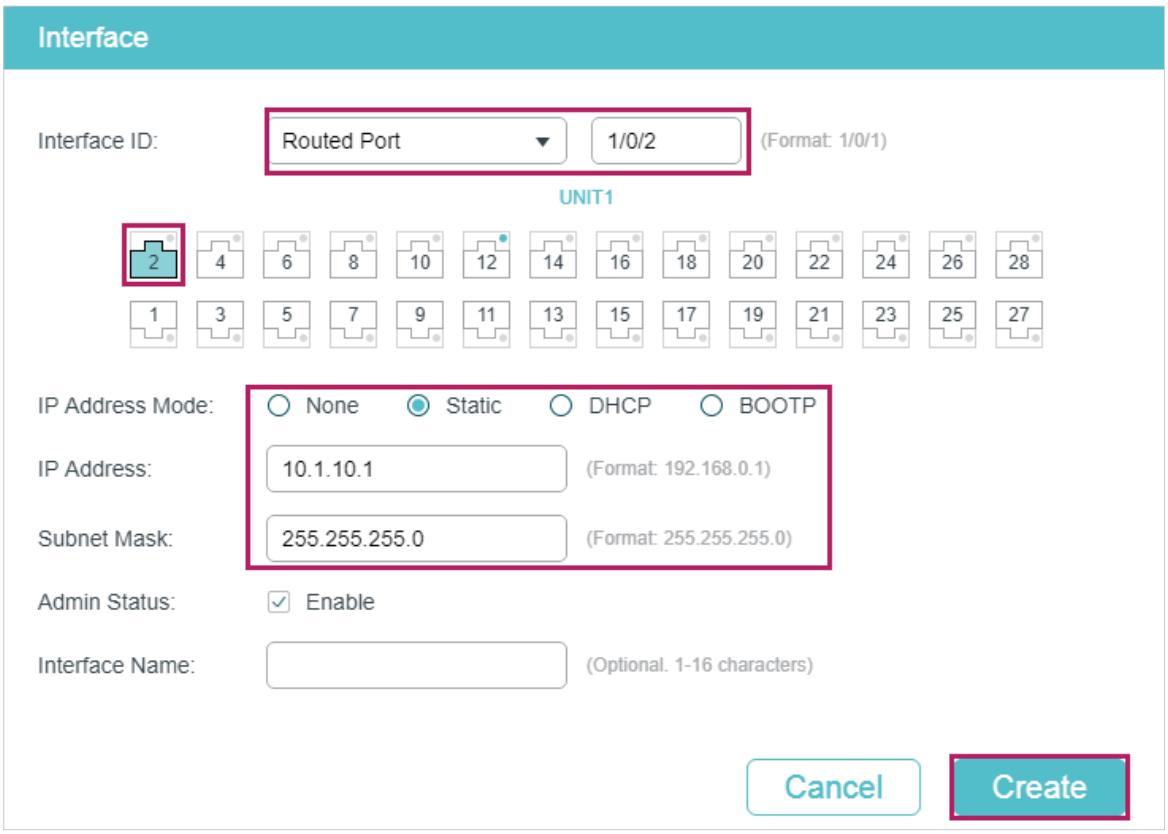


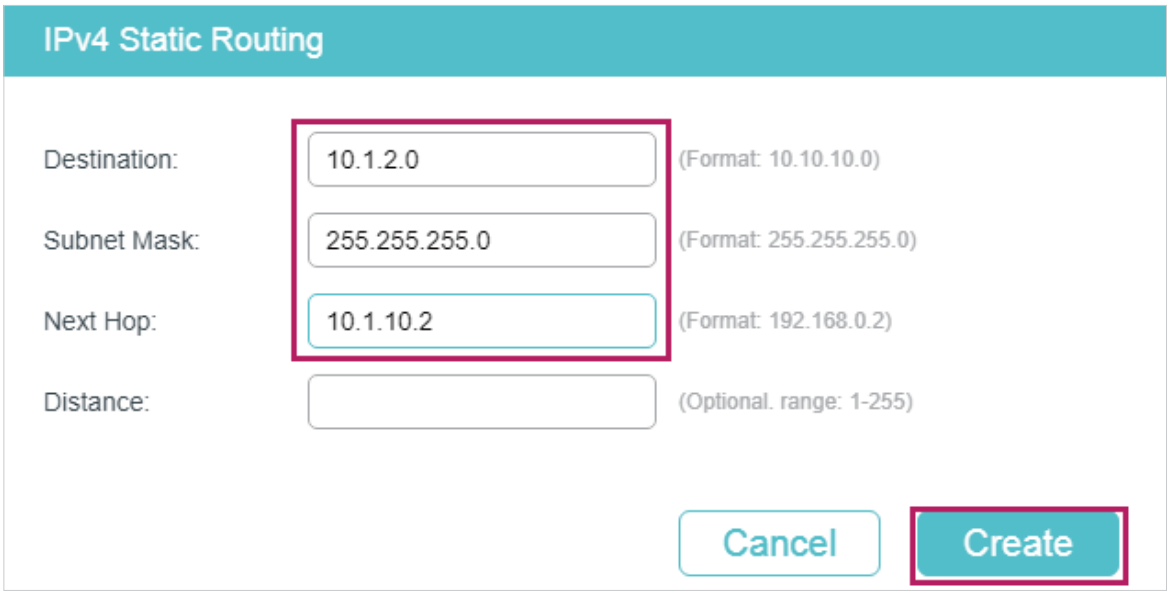
Figure 5-3 Create a Routed Port Gi1/0/2 for Switch A



2) Choose the menu **L3 FEATURES > Static Routing > IPv4 Static Routing** to load the following page. Add a static routing 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

Part 15

Configuring DHCP Service

CHAPTERS

1. DHCP
2. DHCP Server Configuration
3. DHCP Relay Configuration
4. DHCP L2 Relay Configuration
5. Configuration Examples
6. Appendix: Default Parameters

1 DHCP

1.1 Overview

DHCP (Dynamic Host Configuration Protocol) is widely used to automatically assign IP addresses and other network configuration parameters to network devices, enhancing the utilization of IP address.

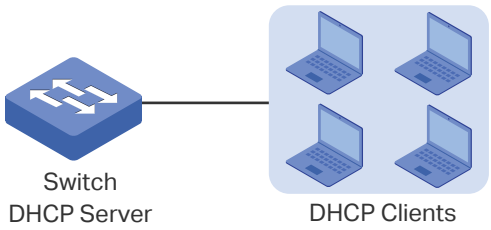
1.2 Supported Features

The supported DHCP features of the switch include DHCP Server, DHCP Relay and DHCP L2 Relay.

DHCP Server

DHCP Server is used to dynamically assign IP addresses, default gateway and other parameters to DHCP clients. As the following figure shows, the switch acts as a DHCP server and assigns IP addresses to the clients.

Figure 1-1 Application Scenario of DHCP Server



DHCP Relay

DHCP Relay is used to process and forward DHCP packets between different subnets or VLANs.

The DHCP client broadcasts DHCP request packets to require for an IP address. Since the transmission of broadcast packets are always limited in one LAN, so if the DHCP server are not in the same LAN with the client, the client can never obtain an IP address from the DHCP server. Therefore, each LAN should be equipped with a DHCP server, thus increasing the costs of network construction and bringing trouble for central network management.

DHCP Relay solves this problem. The DHCP Relay device acts as a relay agent and forwards DHCP packets between DHCP clients and DHCP servers in different LANs, so that DHCP clients in different LANs can share one DHCP server.

DHCP Relay includes three features: Option 82, DHCP Interface Relay and DHCP VLAN Relay.

Option 82

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.

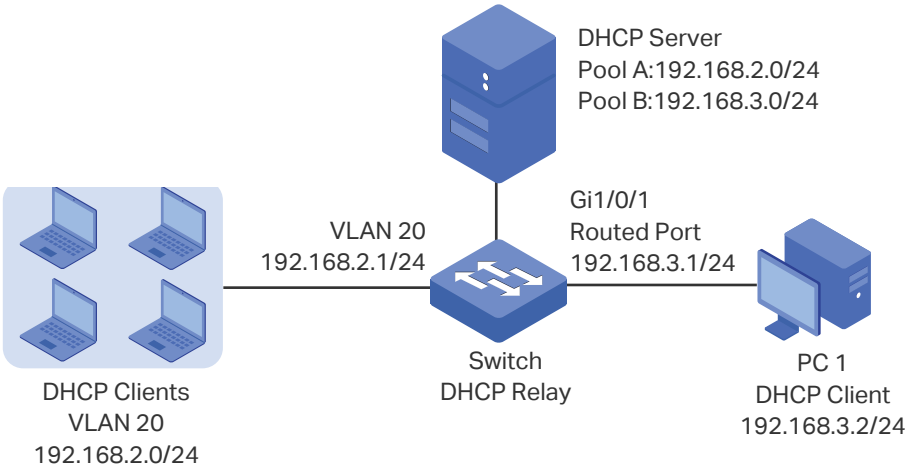
DHCP Interface Relay

DHCP Interface Relay is used for the clients in different subnets to obtain IP addresses from the DHCP server that is not in the same subnet as the clients.

In DHCP Interface Relay, you can specify a DHCP server for an Layer 3 interface that the clients are connected to. 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 based 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 1-2 Application Scenario of DHCP Interface Relay



DHCP VLAN Relay

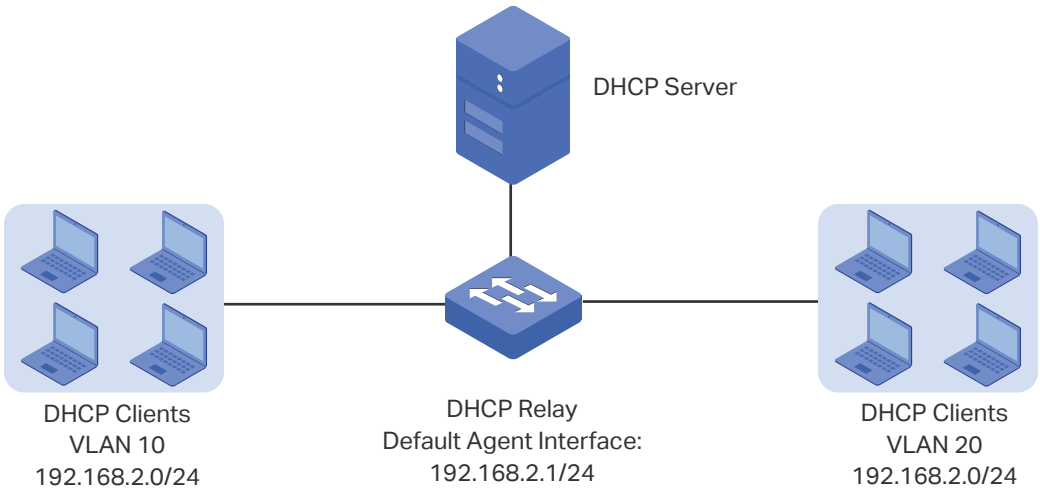
DHCP VLAN Relay allows clients in different VLANs to obtain IP addresses from the DHCP server using a single agent interface IP address.

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 1-3 Application Scenario of DHCP VLAN Relay



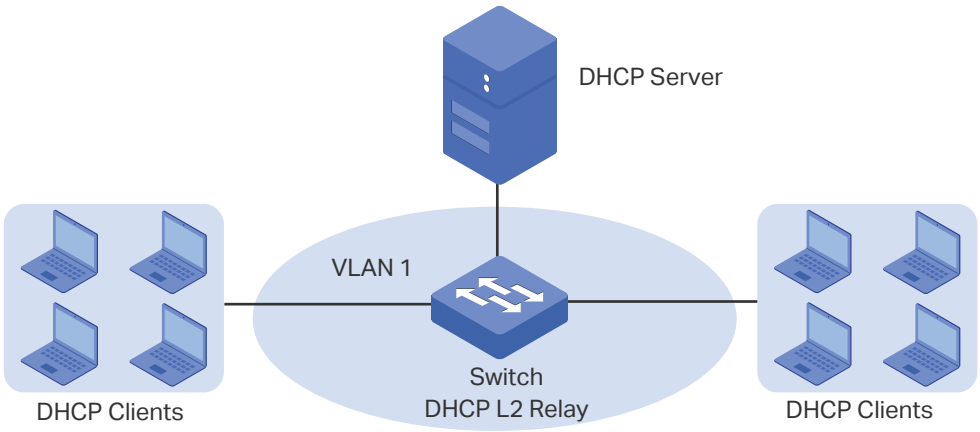
Note:

- 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 1-4 Application Scenario of DHCP L2 Relay



2 DHCP Server Configuration

To complete DHCP server configuration, follow these steps:

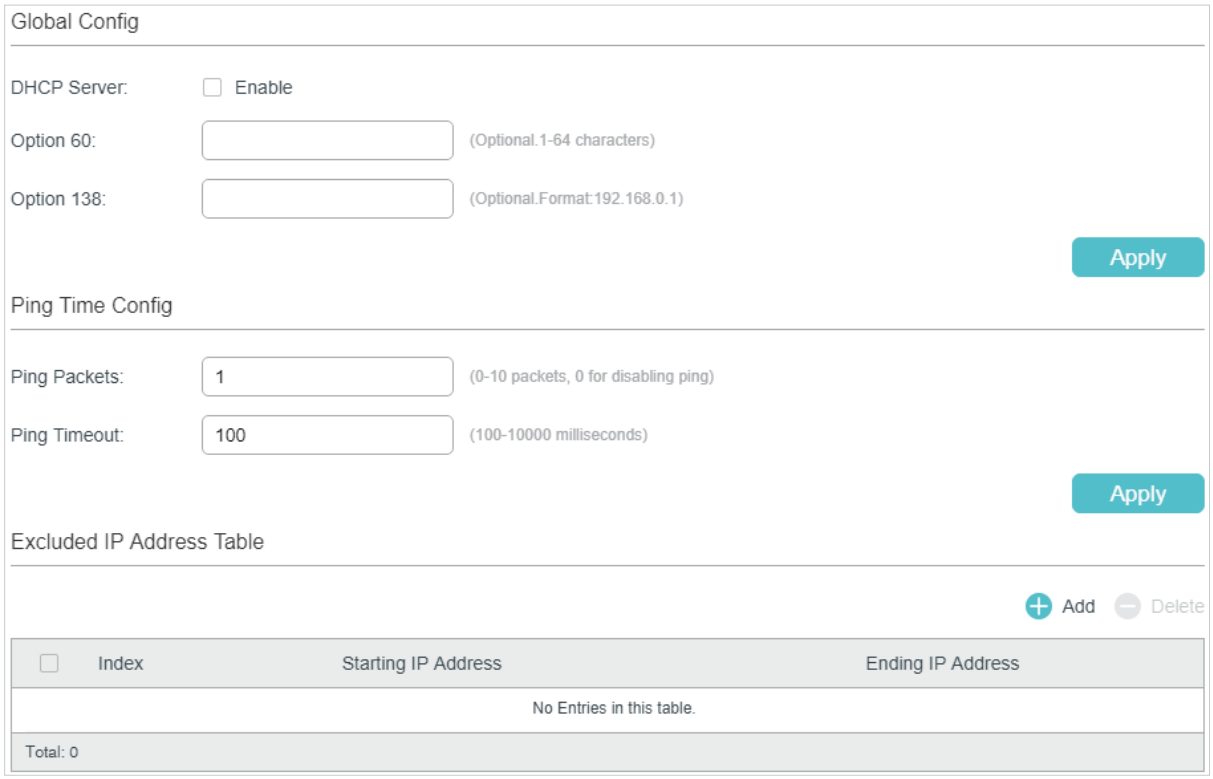
1) Enable the DHCP Server feature on the switch.
2) Configure the DHCP Server Pool.
3) (Optional) Manually assign static IP addresses for some clients if necessary.

2.1 Using the GUI

2.1.1 Enabling DHCP Server

Choose the menu **L3 FEATURES> DHCP Service > 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**.

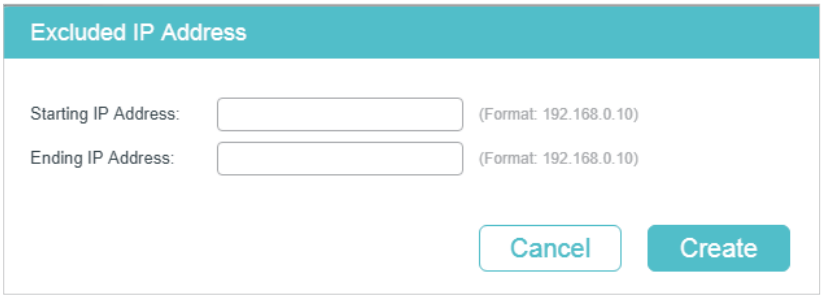
DHCP Server	Enable DHCP Server. By default, it is disabled.

Option 60	(Optional) Specify the option 60 for device identification. Mostly it is used in 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 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 Table** section, click Add to load the following page to specify the IP addresses that should not be assigned to the clients.



Enter the Starting IP Address and Ending IP Address to specify the range of reserved IP addresses. Click **Create**.

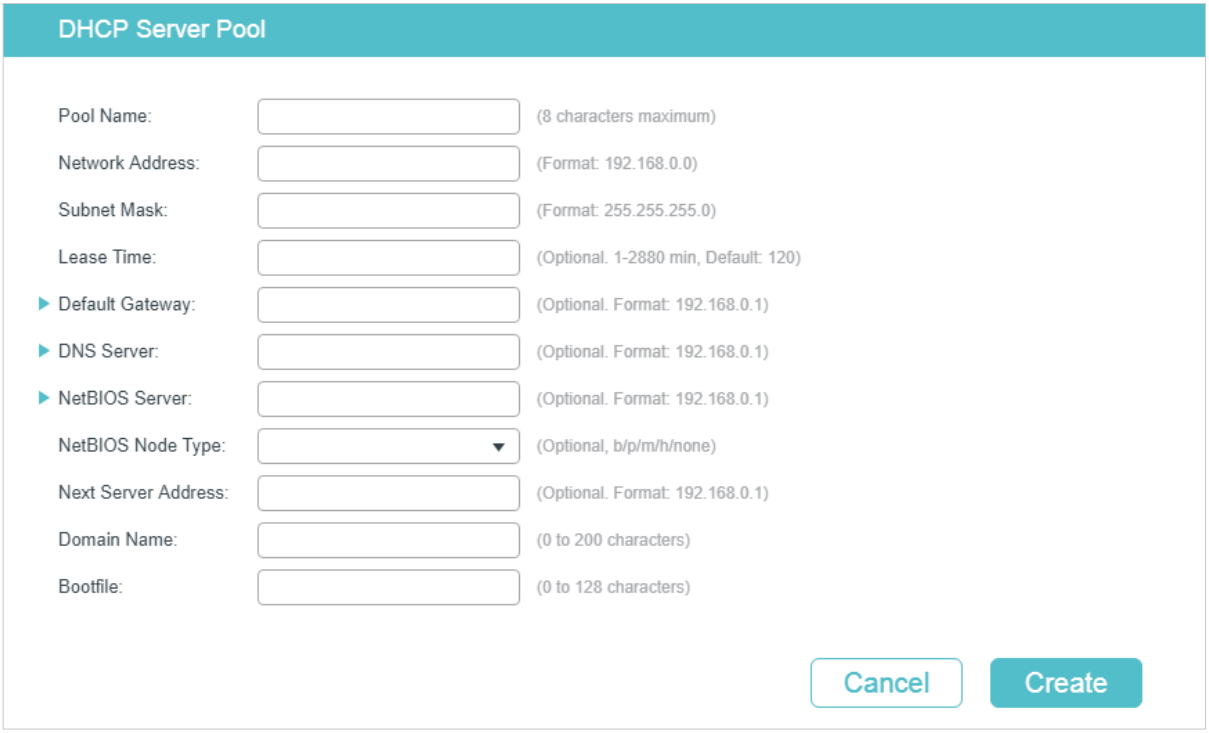
Starting IP Address/ Ending IP Address	Specify the start IP address and end IP address of the excluded IP address range. If the start IP address and the end IP address are the same, the server excludes only one IP address. When configuring DHCP Server, you need to reserve certain IP addresses for each subnet, such as default gateway address, broadcast address and DNS server address.

2.1.2 Configuring DHCP Server Pool

The DHCP Server Pool defines the parameters that will be assigned to the DHCP clients.

Choose the menu **L3 FEATURES > DHCP Service >DHCP Server > Pool Setting** and click Add to load the following page.

Figure 2-2 Pool Setting



Configure the parameters for the DHCP Server Pool. Then click **Create**.

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.

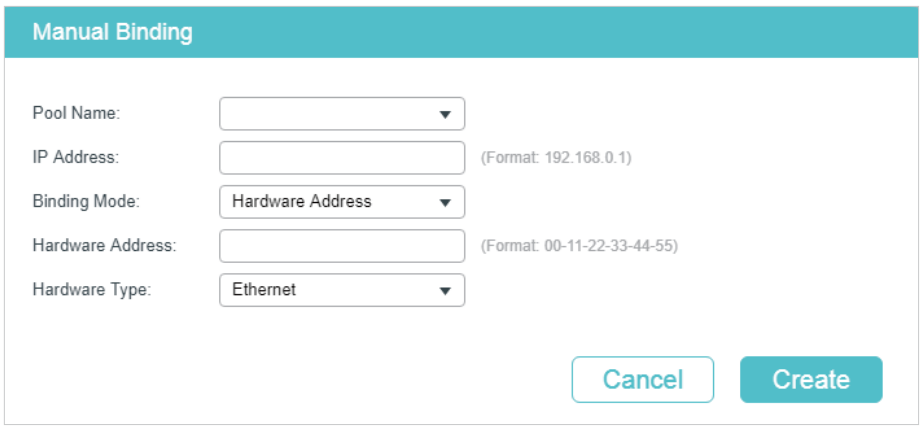
Netbios Server	(Optional) Specify the NetBIOS name server. You can specify up to 8 NetBIOS servers for each DHCP server pool. When a DHCP client uses the Network NetBIOS (Basic Input Output System) protocol for communication, the host name must be mapped to IP address. NetBIOS name server can resolve 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.

2.1.3 Configuring Manual Binding

Some devices like web servers require static IP addresses. To meet this requirement, you can manually bind the MAC address or client ID of the device to an IP address, and the DHCP server will reserve the bound IP address to this device at all times.

Choose the menu **L3 FEATURES > DHCP Service >DHCP Server > Manual Binding** and click Add to load the following page.

Figure 2-3 Manual Binding



Select a pool name and enter the IP address to be bound. Select a binding mode and finish the configuration accordingly. Click **Create**.

Pool Name	Select a DHCP server pool from the drop-down list.
IP Address	Enter the IP address to be bound to the client.
Binding Mode	Select the binding mode: **Client ID**: Bind the IP address to the client ID of the client. **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.

2.2 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** *vender* (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. *vender*: 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 starting IP address and ending IP address of the excluded IP address range. If the starting IP address and the ending 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 starting IP address and ending 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 Relay Configuration

To complete DHCP Relay configuration, follow these steps:

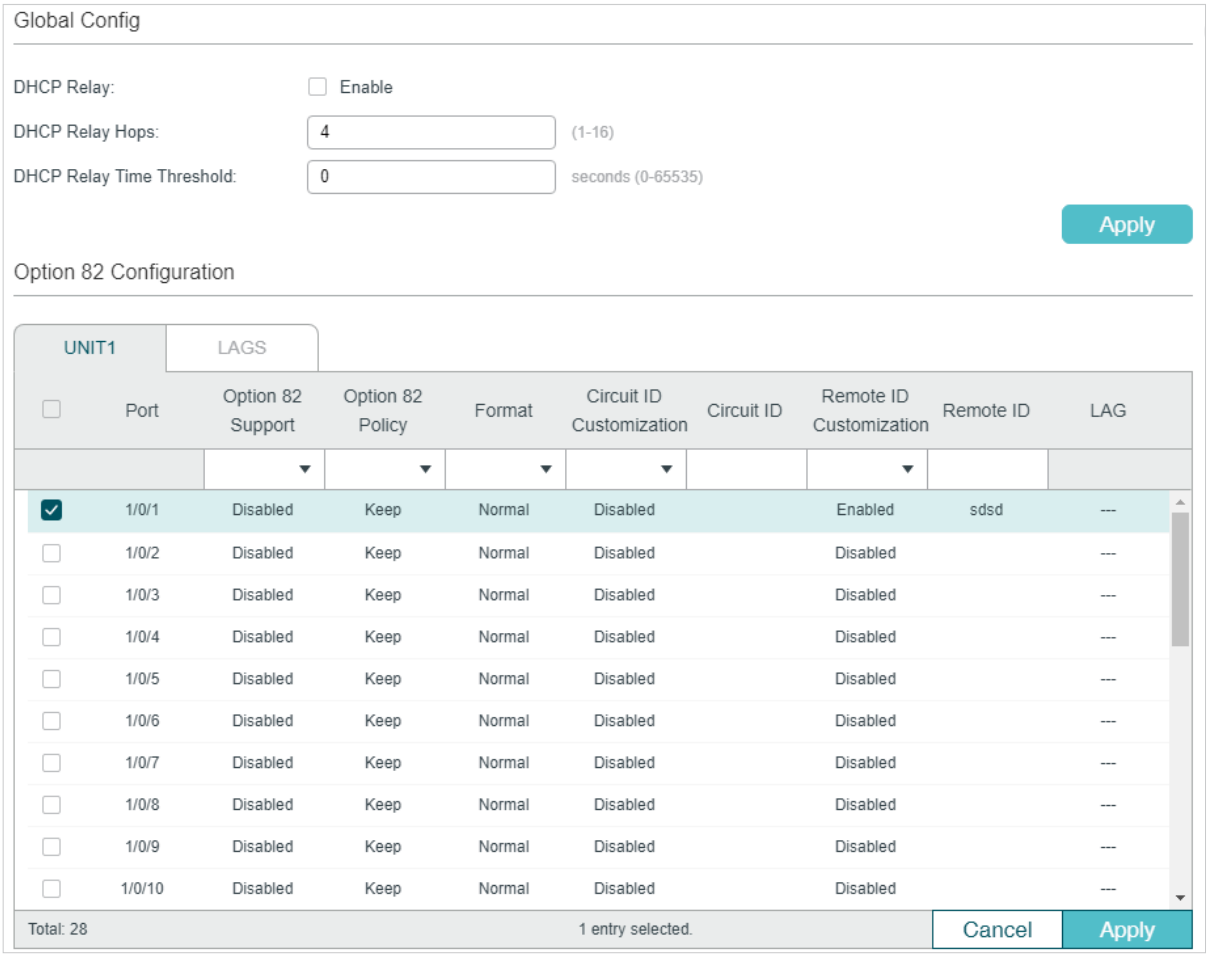
1) Enable DHCP Relay. Configure Option 82 if needed.
2) Specify DHCP server for the Interface or VLAN.

3.1 Using the GUI

3.1.1 Enabling DHCP Relay and Configuring Option 82

Choose the menu **L3 FEATURES > DHCP Service > DHCP Relay > DHCP Relay Config** to load the following page.

Figure 3-1 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 globally and configure the relay hops and the time threshold. Click **Apply**.

DHCP Relay	Enable DHCP Relay globally.
DHCP Relay Hops	Specify the DHCP relay hops. DHCP Relay Hops defines the maximum number of hops (DHCP Relay agent) that the DHCP packets can be relayed. If a packet's hop count is more than the value you set here, the packet will be dropped.
DHCP Relay Time Threshold	Specify the DHCP relay time threshold. The valid value ranges from 0 to 65535 seconds. DHCP relay time is the time elapsed since client began address acquisition or renewal process. When the time is greater than the value set here, the DHCP packet will be dropped by the switch. Value 0 means the switch will not examine this field of the DHCP packets.

2) (Optional) In the **Option 82 Configuration** section, 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.
Option 82 Policy	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 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.

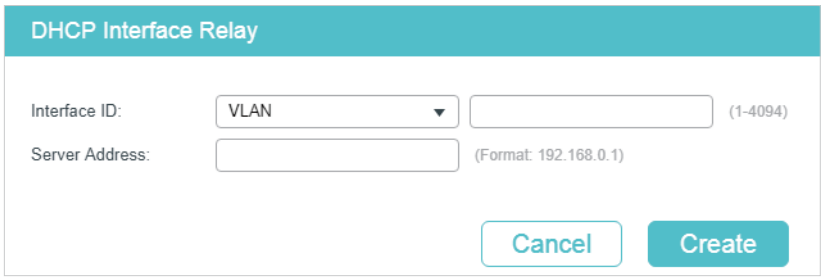
3) Click **Apply**.

3.1.2 Configuring DHCP Interface Relay

DHCP Interface Relay is used for the clients that are connected to a Layer 3 interface to obtain IP addresses from the DHCP server, which is not in the same subnet as the clients.

Choose the menu **L3 FEATURES > DHCP Service > DHCP Relay > DHCP Interface Relay** and click Add to load the following page.

Figure 3-2 Configuring DHCP Interface Relay



Select the interface type and enter the interface ID, then enter the IP address of the DHCP server. Click **Create**.

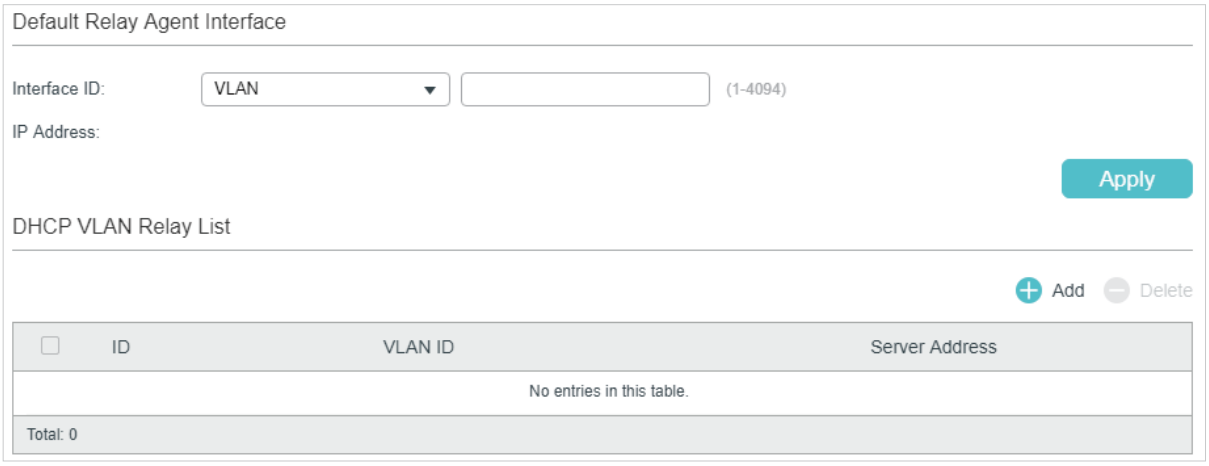
Interface ID	Specify the type and ID of the interface. It is the layer 3 interface that connecting to the DHCP clients. The interface should be an existing layer 3 interface.
Server Address	Enter the IP address of the DHCP server.

3.1.3 Configuring DHCP VLAN Relay

DHCP VLAN Relay is used for the clients in VLANs but do not have a layer 3 interface as the gateway to obtain IP addresses from the DHCP server, which is not in the same subnet as the clients.

Choose the menu **L3 FEATURES > DHCP Service > DHCP Relay > DHCP VLAN Relay** to load the following page.

Figure 3-3 Specify DHCP Server for VLAN



Follow these steps to specify DHCP Server for the specific VLAN:

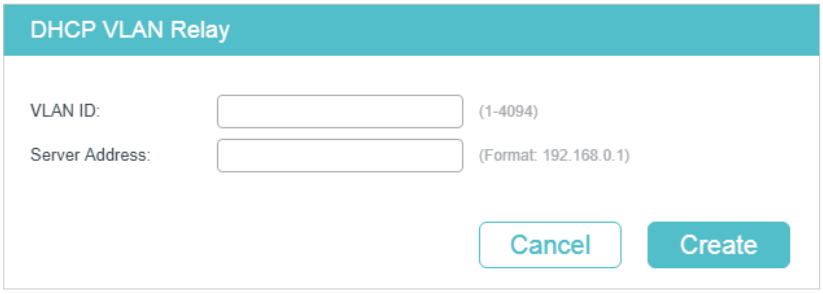
1) In the **Default Relay Agent Interface** section, specify a Layer 3 interface as the default relay agent interface. Then click **Apply**.

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.
IP Address	Displays the IP address of this interface.

Note:

- If the VLAN the clients belong to already has an IP address, the switch will use the client's own VLAN interface as the relay agent interface. The manually specified default relay agent 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 **DHCP VLAN Relay List** section, click Add to load the configuration page.



Specify the VLAN the clients belongs to and the server address. Click **Create**.

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.

3.2 Using the CLI

3.2.1 Enabling DHCP Relay

Follow these steps to enable DHCP Relay and configure the corresponding parameters:

Step 1	**configure** Enter global configuration mode.
Step 2	**service dhcp relay** Enable DHCP Relay.
Step 3	**ip dhcp relay hops** *hops* Specify the maximum hops (DHCP Relay agent) that the DHCP packets can be relayed. If a packet's hop count is more than the value you set here, the packet will be dropped. *hops:* Specify the maximum hops for DHCP packets. The valid value ranges from the 1 to 16, and the default value is 4.
Step 4	**ip dhcp relay time** *time* Specify the DHCP relay time threshold. DHCP relay time is the time elapsed since client began address acquisition or renewal process. When the elapsed time of the DHCP packet is greater than the value set here, the DHCP packet will be dropped by the switch. *time:* Specify the DHCP relay time threshold. The valid value ranges from 1 to 65535. The default value is 0, which means the switch will not examine this field of the DHCP packets.
Step 5	**show ip dhcp relay** 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 Relay, configure the relay hops as 5 and configure the relay time as 10 seconds :

Switch#configure

Switch(config)#service dhcp relay

Switch(config)#show ip dhcp relay

Switch(config)#ip dhcp relay hops 5

Switch(config)#ip dhcp relay time 10

DHCP relay state: enabled

DHCP relay hops: 5

DHCP relay Time Threshold: 10 seconds

.....

Switch(config)#end

Switch#copy running-config startup-config

3.2.2 (Optional) Configuring Option 82

Follow these steps to configure Option 82:

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 relay information option** Enable the Option 82 feature on the port.
Step 4	**ip dhcp relay 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 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 the value you configure for the related sub-option.

Step 6	**ip dhcp relay 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 relay 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 relay information interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-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 relay information option

Switch(config-if)#ip dhcp relay information strategy replace

Switch(config-if)#ip dhcp relay information format normal

Switch(config-if)#ip dhcp relay information circut-id VLAN20

Switch(config-if)#ip dhcp relay information remote-id Host1

Switch(config-if)#show ip dhcp relay information 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

3.2.3 Configuring DHCP Interface Relay

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.

Follow these steps to DHCP Interface Relay:

Step 1	**configure** Enter global configuration mode.
Step 2	Enter Layer 3 interface configuration mode: Enter VLAN interface configuration mode: **interface vlan** *vlan-id* *vlan-id*: Specify an IEEE 802.1Q VLAN ID that already exists, ranging from 1 to 4094. Enter routed port configuration mode: **interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}** Enter interface configuration mode. *port*: Specify the Ethernet port number, for example 1/0/1. **no switchport** Switch the Layer 2 port into the Layer 3 routed port. Enter port-channel interface configuration mode: **interface { port-cahnnel** *port-channel* **}** Enter interface configuration mode. *port-channel*: Specify the port channel, the valid value ranges from 1 to 14. **no switchport** Switch the port channel to a Layer 3 port channel interface.
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

3.2.4 Configuring 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: Enter VLAN interface configuration mode: **interface vlan** *vlan-id* *vlan-id*: Specify an IEEE 802.1Q VLAN ID that already exists, ranging from 1 to 4094. Enter routed port configuration mode: **interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}** Enter interface configuration mode. *port*: Specify the Ethernet port number, for example 1/0/1. **no switchport** Switch the Layer 2 port into the Layer 3 routed port. Enter port-channel interface configuration mode: **interface { port-cahnnel** *port-channel* **}** Enter interface configuration mode. *port-channel*: Specify the port channel, the valid value ranges from 1 to 14. **no switchport** Switch the port channel to a Layer 3 port channel 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)#no switchport

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

4 DHCP L2 Relay Configuration

To complete DHCP L2 Relay configuration, follow these steps:

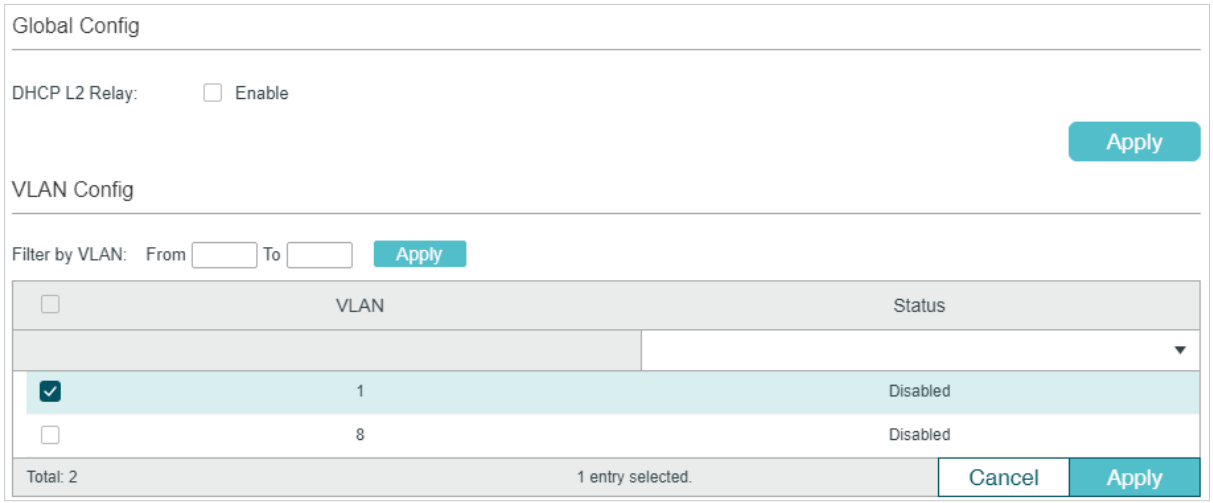
1) Enable DHCP L2 Relay.
2) Configure Option 82 for ports.

4.1 Using the GUI

4.1.1 Enabling DHCP L2 Relay

Choose the menu **L3 FEATURES > DHCP Service > DHCP L2 Relay > Global Config** to load the following page.

Figure 4-1 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. Click **Apply**.

DHCP L2 Relay	Enable DHCP Relay globally.

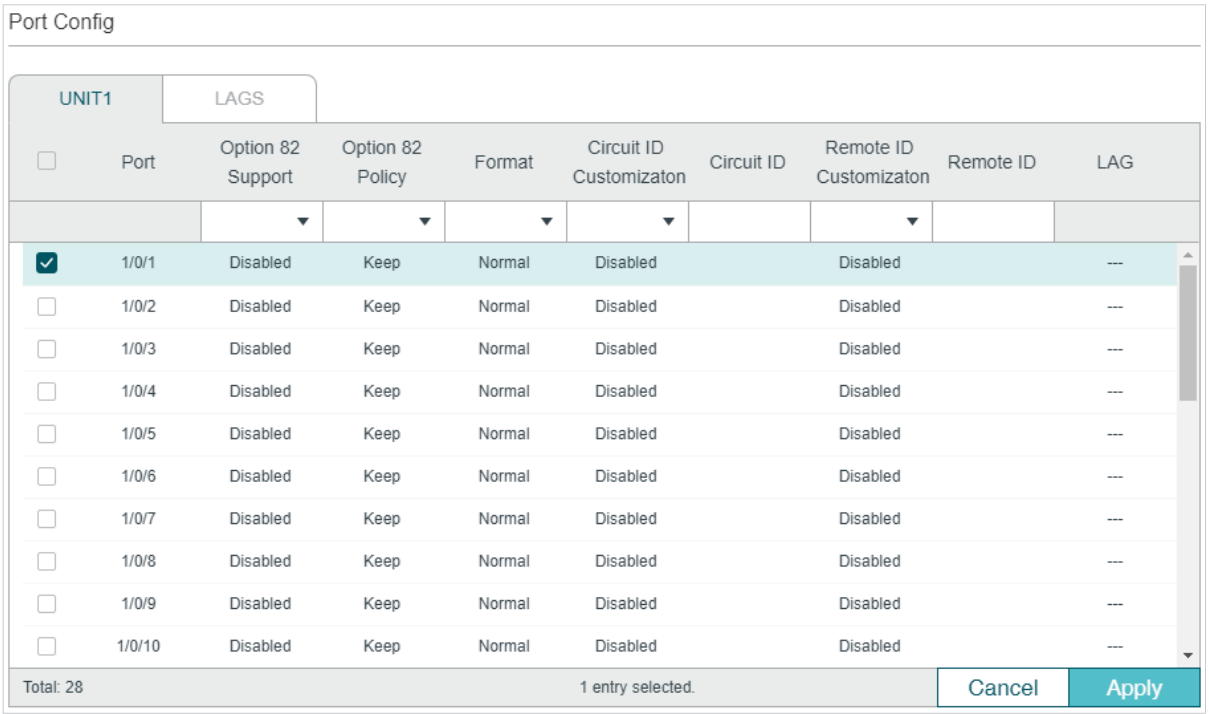
2) In the **VLAN Config** section, enable DHCP L2 Relay for the specified VLAN. Click **Apply**.

VLAN	Displays the VLAN ID.
Status	Enable DHCP L2 Relay for the specified VLAN..

4.1.1 Configuring Option 82 for Ports

Choose the menu **L3 FEATURES > DHCP Service > DHCP L2 Relay > Port Config** to load the following page.

Figure 4-1 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.
Option 82 Policy	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 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**

4.2 Using the CLI

4.2.1 Enabling DHCP 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 vlan 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

4.2.2 Configuring Option 82 for Ports

Follow these steps to configure Option 82:

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 information 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 circut-id VLAN20

Switch(config-if)#ip dhcp l2relay information remote-id Host1

Switch(config-if)#show ip dhcp l2relay information 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

5 Configuration Examples

5.1 Example for DHCP Server

5.1.1 Network Requirements

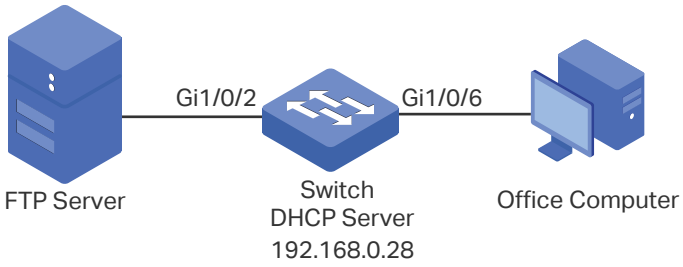
The administrator uses the switch as the DHCP server to assign IP addresses to all the connected devices. The connected devices include FTP servers which need static IP addresses, and office computers that can dynamically obtain IP addresses from the DHCP server.

5.1.2 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. Port 1/0/2 is connected to the FTP server and port 1/0/6 is connected to the office computer.

Figure 5-1 Network Topology for DHCP Server

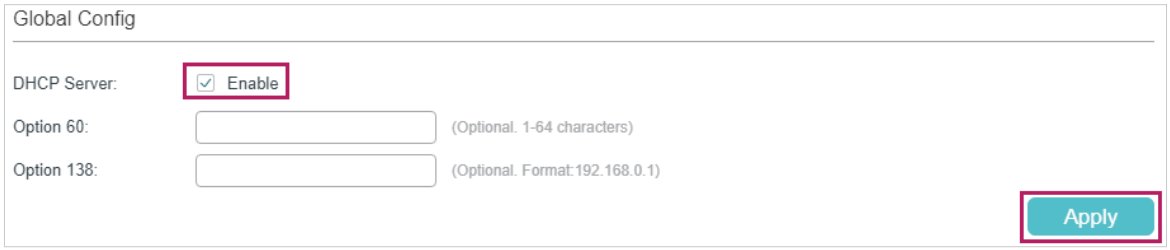


Demonstrated with T1600G-52TS, this chapter provides configuration procedures in two ways: using the GUI and using the CLI.

5.1.3 Using the GUI

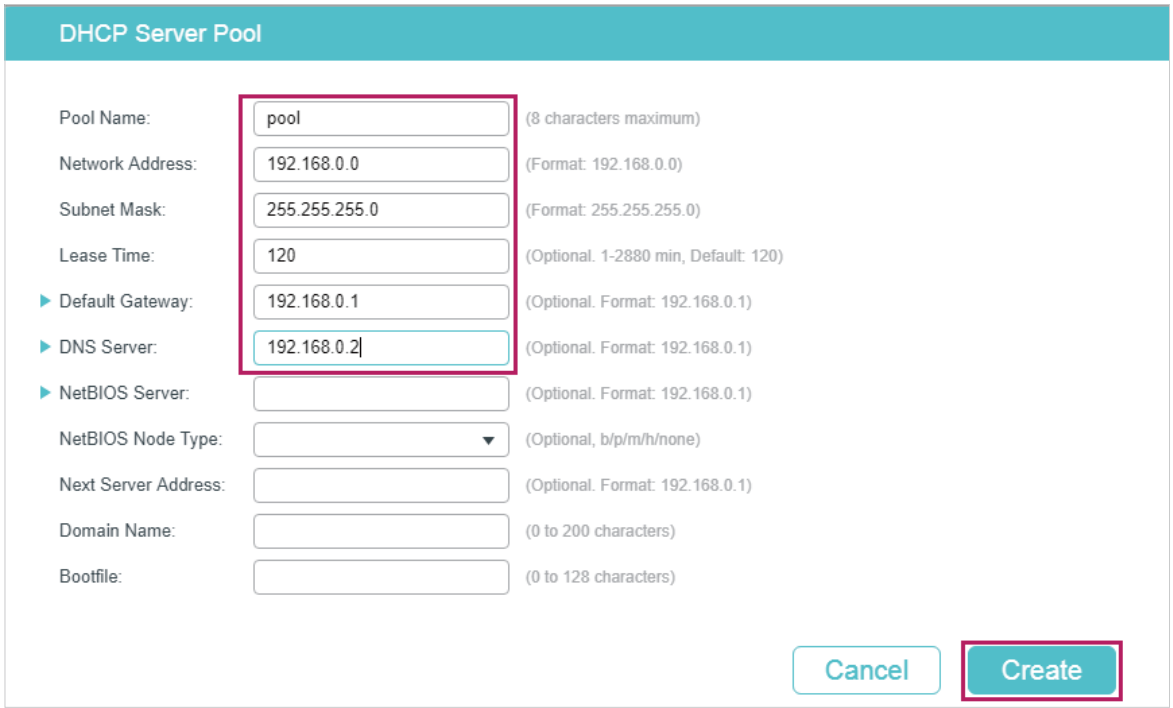
1) Choose the menu **L3 FEATURES > DHCP Service > DHCP Server > DHCP Server** to load the following page. In the **Global Config** section, enable DHCP Server.

Figure 5-2 Configuring DHCP Server



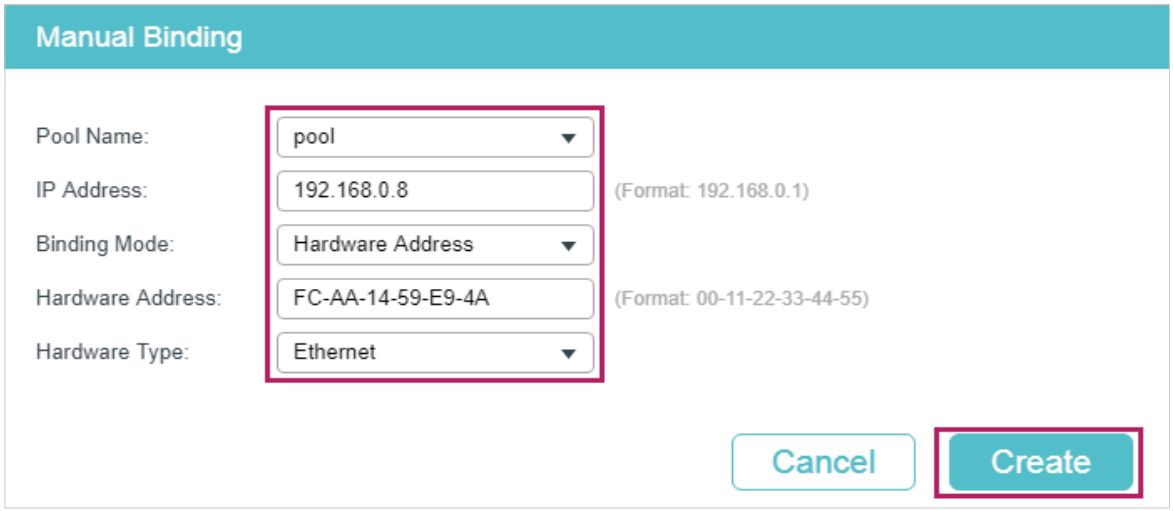
2) Choose the menu **L3 FEATURES > DHCP Service > DHCP Server > Pool Setting** and click Add to load the following page. Specify the Pool Name, Network Address, Subnet Mask, Lease Time, Default Gateway and DNS Server as shown below. Click **Create**.

Figure 5-3 Configuring DHCP Server Pool



3) Choose the menu **L3 FEATURES > DHCP Service > DHCP Server > Manual Binding** and click Add 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 5-4 Configuring Manual Binding



4) Click Save to save the settings.

5.1.4 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.

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 192.168.0.2

Switch(dhcp-config)#exit

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

5.2 Example for DHCP Interface Relay

5.2.1 Network Requirements

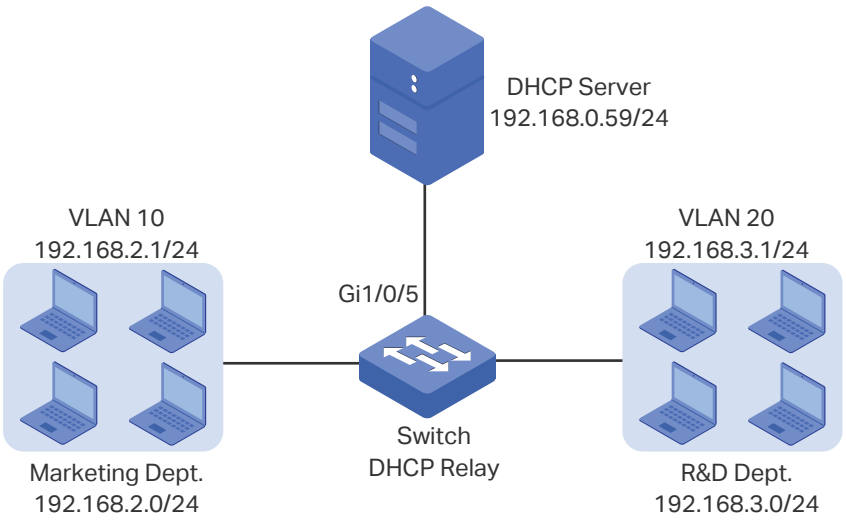
A company wants to assign IP addresses to all computers in two departments, and there is only one DHCP server available. It is required that computers in the same department should be on the same subnet, while computers in different departments should be on different subnets.

5.2.2 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 5-1 Network Topology for DHCP Relay



The overview of the configurations are as follows:

1) Before configuring DHCP Relay, create two DHCP IP pools on the DHCP server, one is on 192.168.2.0/24 network segment and the other is on 192.168.3.0/24 network

segment. 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 Layer 3 Interfaces*.

4) Configure DHCP Relay on the switch. Enable DHCP Relay, and add DHCP server address to each VLAN. After these configurations are finished, the DHCP server can assign IP addresses to computers in the two departments which are in different subnets.

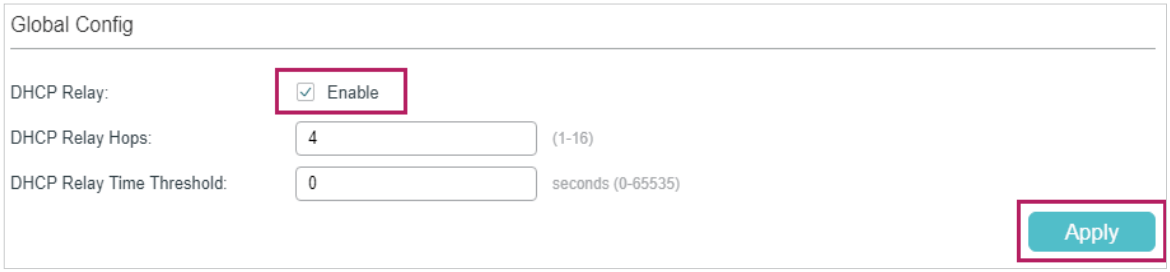
Demonstrated with T1600G-52TS, this chapter provides configuration procedures in two ways: using the GUI and using the CLI.

5.2.3 Using the GUI

Follow these steps to configure DHCP Relay:

1) Choose the menu **L3 FEATURES > DHCP Service > DHCP Relay > DHCP Relay Config** to load the following page. In the **Global Config** section, enable DHCP Relay, and click **Apply**.

Figure 5-1 Enable DHCP Relay



2) Choose the menu **L3 FEATURES > DHCP Service > DHCP Relay > DHCP Interface Relay** and click Add to load the following page. Specify the DHCP server address to assign IP addresses for clients in VLAN 10 and VLAN 20.

Figure 5-2 Specify DHCP Server for Interface VLAN 10

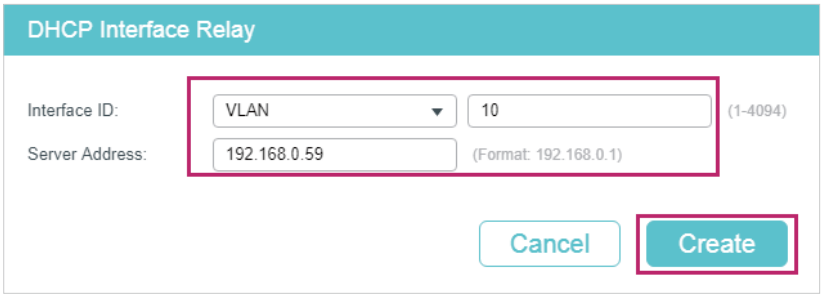
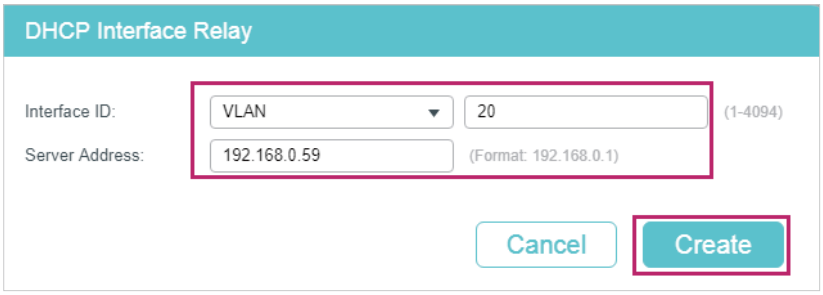


Figure 5-3 Specify DHCP Server for Interface VLAN 20



3) Click Save to save the settings.

5.2.4 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

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

...

6 Appendix: Default Parameters

Default settings of DHCP Server are listed in the following table.

Table 6-1 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 6-2 Default Settings of DHCP Relay

Parameter	Default Setting
DHCP Relay	
DHCP Relay	Disable
DHCP Relay Hops	4
DHCP Relay Time Threshold	0
Option 82 Configuration	
Option 82 Support	Disabled
Option 82 Policy	Keep
Format	Normal
Circuit ID Customization	Disable
Circuit ID	None
Remote ID Customization	Disabled
Remote ID	None
DHCP Interface Relay	
Interface ID	None
Server Address	None

Parameter	Default Setting
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 6-3 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

Part 16

Configuring ARP

CHAPTERS

1. Overview
2. ARP Configurations
3. Appendix: Default Parameters

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.

1.1 Supported Features

ARP Table

The ARP table displays all the ARP entries, including dynamic entries and static entries.

Dynamic Entry: Automatically learned and will be deleted after aging time.

Static Entry: Added manually and will be remained unless modified or deleted manually.

Static ARP

You can manually add ARP entries by specifying the IP addresses and MAC addresses.

Gratuitous ARP

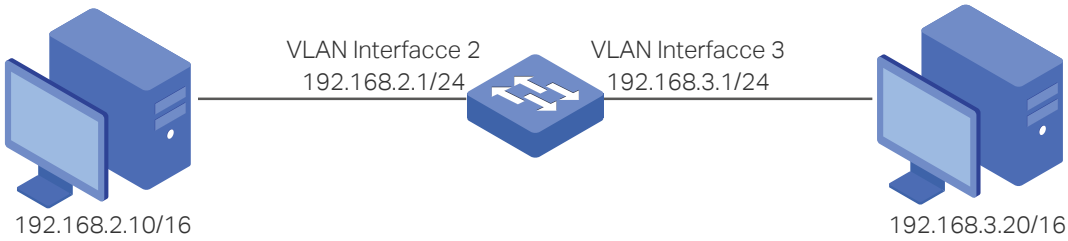
Gratuitous ARP is a special kind of ARP. Both the source and destination addresses of the gratuitous ARP packet are the sender its own IP address. It is used to detect duplicate IP address. If an interface sends a gratuitous ARP packet and no replies are received, then the sender knows its IP address is not used by other devices.

Proxy ARP

Normally, the ARP packets can only be transmitted in one broadcast domain, which means if two devices in the same network segment are connected to different Layer 3 interfaces, they cannot communicate with each other because they cannot learn each other's MAC address using ARP packets.

Proxy ARP solves this problem. As shown below, when a host sends an ARP request to another device that is not in the same broadcast domain but on the same network segment, the Layer 3 interface with Proxy ARP enabled will respond the ARP request with its own MAC address if the destination IP is reachable. After that, the ARP request sender sends packets to the switch, and the switch forwards the packets to the intended device.

Figure 1-1 Proxy ARP Application

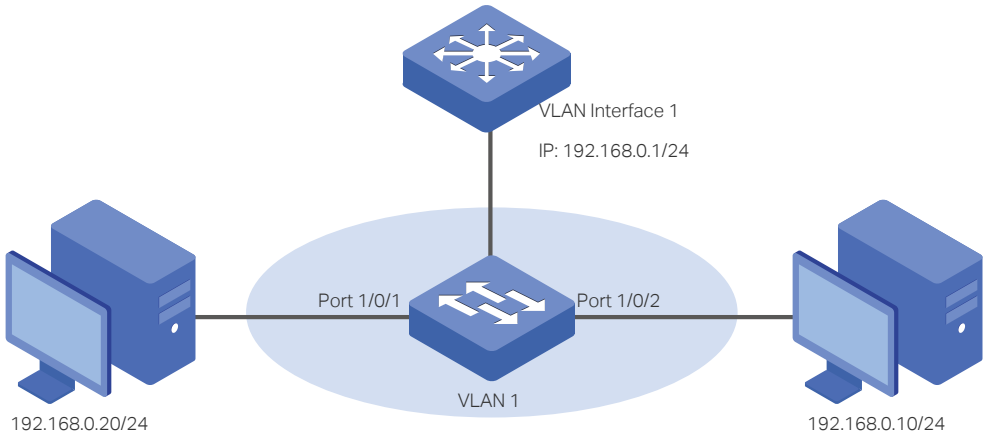


Local Proxy ARP

Local Proxy ARP is similar with Proxy ARP. As shown below, two hosts are in the same VLAN and connected to VLAN interface 1, but port 1/0/1 and port 1/0/2 are isolated on Layer 2. In this case, both of the hosts cannot receive each other's ARP request. So they cannot communicate with each other because they cannot learn each other's MAC address using ARP packets.

To solve this problem, you can enable Local Proxy ARP on the Layer 3 interface and the interface will respond the ARP request sender with its own MAC address. After that, the ARP request sender sends packets to the Layer 3 interface, and the interface forwards the packets to the intended device.

Figure 1-2 Local Proxy ARP Application



2 ARP Configurations

With ARP configurations, you can:

- View dynamic and static ARP entries.
- Add or delete static ARP entries.

To configure the Gratuitous ARP feature:

- Configure the Gratuitous ARP globally and set the Gratuitous ARP sending interval

To configure the Proxy ARP feature:

- Enable Proxy function for VLAN interfaces or routed ports.

To configure the Local Proxy ARP feature:

- Enable Local Proxy function for VLAN interfaces or routed ports.

2.1 Using the GUI

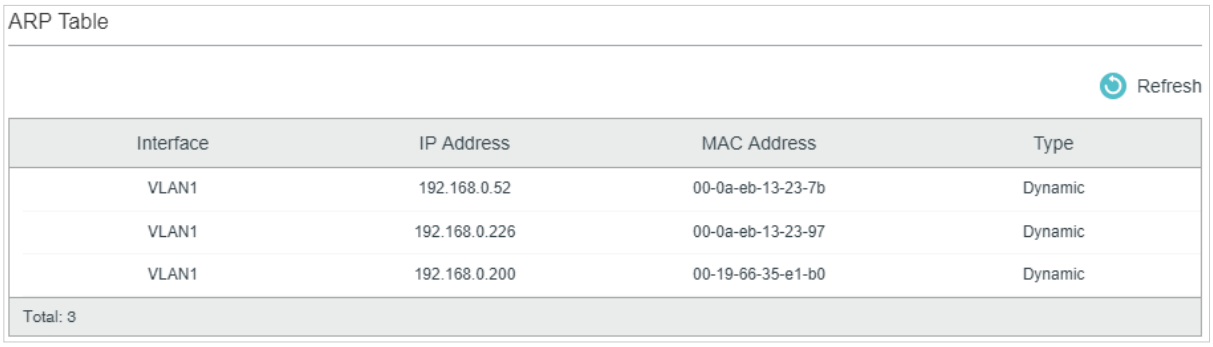
2.1.1 Viewing the ARP Entries

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 **L3 FEATURES > ARP > ARP Table > ARP Table** to load the following page.

Figure 2-1 Viewing the ARP Entries



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.

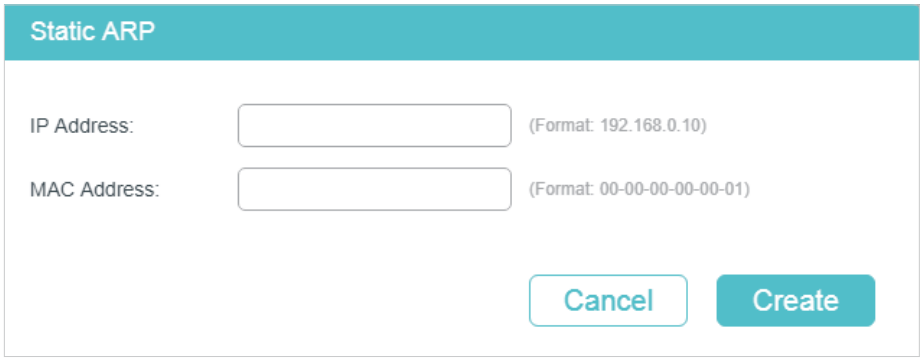
Type	Displays the type of an ARP entry. **Static**: The entry is added manually and will always remain the same. **Dynamic**: The entry that will be deleted after the aging time leased. The default aging time value is 600 seconds. If you want to change the aging time, you can use the CLI to configure it.

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 **L3 FEATURES > ARP > Static ARP** and click Add to load the following page.

Figure 2-2 Adding Static ARP Entries



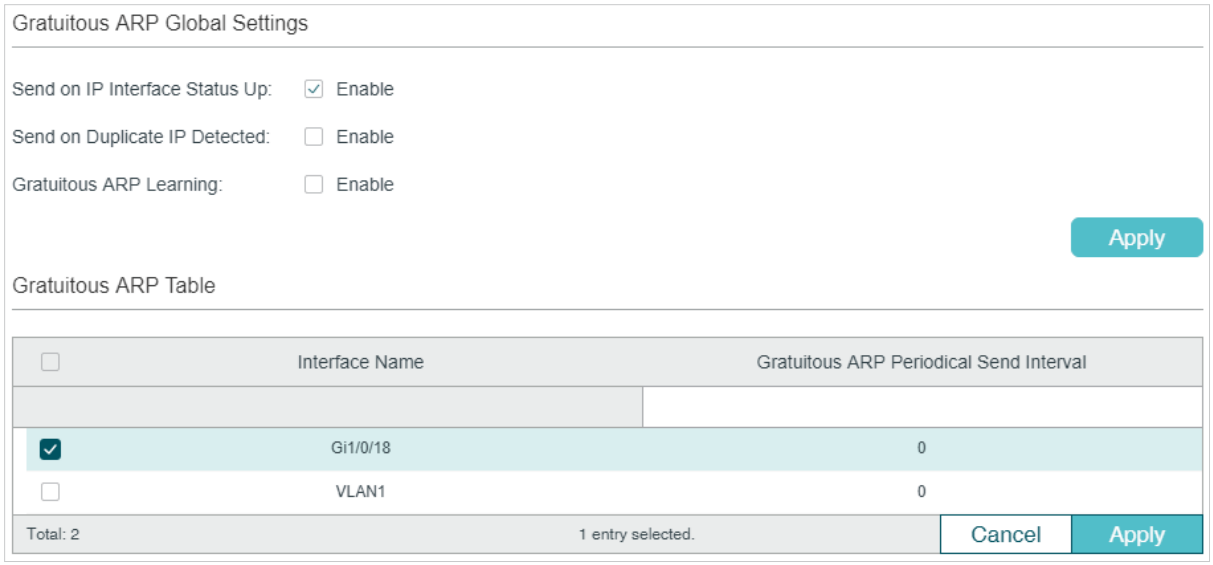
Enter the IP address and MAC address, then click **Create**.

IP address	Specify the IP address of the static ARP entry.
MAC address	Specify the MAC address.of the static ARP entry.

2.1.3 Configuring Gratuitous ARP

Choose the menu **L3 FEATURES > ARP > Gratuitous ARP** to load the following page.

Figure 2-3 Configuring Gratuitous ARP



Follow these steps to configure the Gratuitous feature for the interface.

1) In the **Gratuitous ARP Global Settings** section, configure the global parameters for gratuitous ARP. Then click **Apply**.

Send on IP Interface Status Up	With this option enabled, the interface will send gratuitous ARP request packets when its status becomes up. This is used to announce the interface's IP address to the other hosts. It is enabled by default.
Send on Duplicate IP Detected	With this option enabled, the interface will send gratuitous ARP request packets when a gratuitous ARP request packet is received for which the IP address is the same as the interface's. In this case, the switch knows that another host is using the same IP address as its own. To claim the IP address for the correct owner, the interface sends gratuitous ARP packets. It is disabled by default.
Gratuitous ARP Learning	Normally, the switch only updates the MAC address table by learning from the ARP reply packet or normal ARP request packet. With this option enabled, the switch will also update the MAC address table by learning from the received gratuitous ARP packets. It is disabled by default.

2) In the **Gratuitous ARP Table** section, configure the interval of sending gratuitous ARP request packets for the interface. Then click **Apply**.

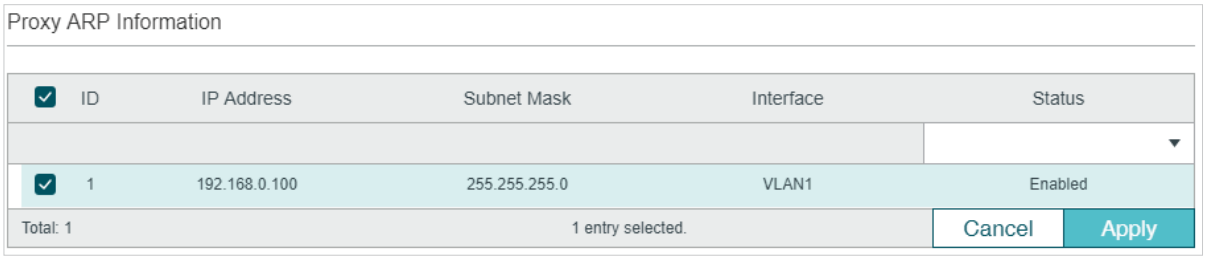
Interface Name	Displays the Interface ID of the Layer 3 interface.
Gratuitous ARP Periodical Send Interval	Enter the interval of sending gratuitous ARP request packets for the interface. A value of 0 means the interface will not send gratuitous ARP request packets periodically.

2.1.4 Configuring Proxy ARP

Proxy ARP is used in the situation that two devices are in the same network segment but connected to different Layer 3 interfaces.

Choose the menu **L3 FEATURES> ARP > Proxy ARP > Proxy ARP** to load the following page.

Figure 2-4 Configuring Proxy ARP



Select the desired interface and enable proxy ARP. Then click **Apply**.

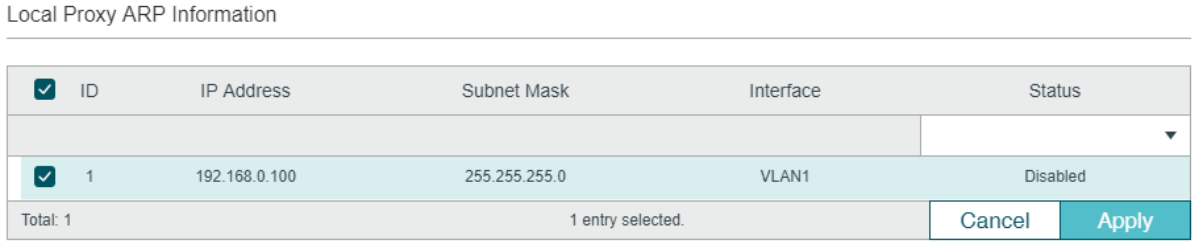
IP Address	Displays the IP address of the Layer 3 interface
Subnet Mask	Displays the subnet mask of the IP address.
Status	Enable proxy ARP feature on the interface. The interface will respond the ARP request sender with its own MAC address.

2.1.5 Configuring Local Proxy ARP

Local Proxy ARP is used in the situation that two devices are in the same VLAN but isolated on the layer 2 ports.

Choose the menu **L3 FEATURES > ARP > Proxy ARP > Local Proxy ARP** to load the following page.

Figure 2-5 Configuring Local Proxy ARP



Select the desired interface and enable local proxy ARP. Then click **Apply**.

IP Address	Displays the IP address of the Layer 3 interface
Subnet Mask	Displays the subnet mask of the IP address.
Status	Enable local proxy ARP feature on the interface. The interface will respond the ARP request sender with its own MAC address.

2.2 Using the CLI

2.2.1 Configuring the ARP Entry

■ Adding Static ARP Entries

Follow these steps to add static 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*] *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	**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 1200 seconds.
Step 3	**end** Return to privileged EXEC mode.
Step 4	**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:

Switch#configure

Switch(config)#arp timeout 1000

Switch(config)#end

Switch#copy running-config startup-config

■ Clearing Dynamic Entries

Step 1	**configure** Enter global configuration 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.

■ Renewing Dynamic ARP Entries Automatically

Step 1	**configure** Enter global configuration mode.
Step 2	**arp dunamicrenew** Enable the switch to automatically renew dynamic ARP entries. By default, it is enabled..
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*]

ip: Specify the IP address of your desired ARP entry.

mac: Specify the MAC address of your desired ARP entry.

show ip arp { fastEthernet *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *lagid* **| vlan** *vid* **}**

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.

vid: Specify the VLAN interface ID.

2.2.2 Configuring the Gratuitous ARP

■ Configuring Gratuitous ARP Globally

Follow these steps to add static ARP entries:

Step 1	**configure** Enter global configuration mode.
Step 2	**gratuitous-arp intf-status-up enable** Enable the Layer 3 interface to send a gratuitous ARP packet to detect if its IP address is used by other devices. It is enabled by default
Step 3	**gratuitous-arp dup-ip-detected enable** (Optional) Enable the Layer 3 interface to send a gratuitous packet when the interface received a gratuitous ARP packet with the same IP address with its own. It is disabled by default.
Step 4	**gratuitous-arp learning enable** (Optional) Enable the switch to learn MAC address entries from gratuitous ARP packets. Generally, the switch only learn MAC address entries form normal ARP packets. With this option enabled, the switch will also learn MAC address entries from gratuitous ARP packets. By default, it is disabled.
Step 5	**show gratuitous-arp** Show the gratuitous ARP configuration.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

This example shows how to enable Send on IP Interface Status Up, Send on Duplicate IP Detected and Gratuitous ARP Learning features:

Switch#configure

Switch(config)#gratuitous-arp dup-ip-detected enable

Switch(config)#gratuitous-arp intf-status-up enable

Switch(config)#gratuitous-arp learning enable

Switch(config)#show gratuitous-arp

Send on IP interface Status up : Enabled

Send on Duplicate IP Detected : Enabled

Gratuitous ARP Learning : Enabled

Interface Gratuitous ARP Periodical Send Interval

--- ---

Gi1/0/18 0

VLAN1 0

Switch(config)#end

Switch#copy running-config startup-config

Configuring Interval of Sending Gratuitous ARP Packets

Follow these steps to configure gratuitous ARP packets for Layer 3 interfaces:

Step 1	**configure** Enter global configuration mode.
Step 2	There are three types of Layer 3 interface that are able to send gratuitous ARP packets: routed port, port-channel and VLAN interface. **interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| ten-range gigabitEthernet** *port-list* **| port-channel** *port-channel* **| range port-channel** *port-channel-list* **|}** **no switch port** Enter interface configuration mode and change the port or port-channel to be a Layer 3 interface.
	Interface vlan *vlan-id* Enter the vlan interface configuration mode. *vlan-id:* Enter the interface VLAN ID.
Step 3	**gratuitous-arp send-interval** *interval* Specify the periodical interval at which the interface sends the gratuitous ARP packet. *interval:* Specify the interval in seconds. The valid value ranges from 0 to 65535. Value 0 means the interface does not periodically send gratuitous ARP packets.

Step 4	**show gratuitous-arp** Show the gratuitous ARP configuration.
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 interval of sending gratuitous ARP packets for VLAN interface 1 as 10 seconds:

Switch#configure

Switch(config)#interface vlan 1

Switch(config-if)#gratuitous-arp send-interval 10

Switch(config-if)#show gratuitous-arp

...

Interface Gratuitous ARP Periodical Send Interval

--- ---

VLAN1 10

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.3 Configuring Proxy ARP

You can configure proxy ARP and local proxy ARP.

- Configuring Proxy ARP

Follow these steps to Proxy ARP on the VLAN interface, routed port or port channel.

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

Step 2	There are three types of Layer 3 interface can be enabled with Proxy ARP: routed port, port-channel and VLAN interface. **interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| ten-range gigabitEthernet** *port-list* **| port-channel** *port-channel* **| range port-channel** *port-channel-list* **|}** **no switch port** Enter interface configuration mode and change the port or port-channel to be a Layer 3 interface.
	Interface vlan *vlan-id* Enter the vlan interface configuration mode. *vlan-id:* Enter the interface VLAN ID.
Step 3	**ip proxy-arp** Enable Proxy ARP function on the specified Layer 3 interface..
Step 4	**show ip proxy-arp** Show the Proxy ARP configuration..
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 Proxy ARP function for VLAN interface 1:

Switch#configure

Switch(config)#interface vlan 1

Switch(config-if)#ip proxy-arp

Switch(config-if)#show ip proxy-arp

Interface	IP Address	IP Mask	Status
vlan 1	192.168.0.1	255.255.255.0	Enabled

Switch(config-if)#end

Switch#copy running-config startup-config

Configuring Local Proxy ARP

Follow these steps to Local Proxy ARP on the VLAN interface, routed port or port channel.

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

Step 2	There are three types of Layer 3 interface can be enabled with Local Proxy ARP: routed port, port-channel and VLAN interface. **interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| ten-range gigabitEthernet** *port-list* **| port-channel** *port-channel* **| range port-channel** *port-channel-list* **|}** **no switch port** Enter interface configuration mode and change the port or port-channel to be a Layer 3 interface.
	Interface vlan *vlan-id* Enter the vlan interface configuration mode. *vlan-id:* Enter the interface VLAN ID.
Step 3	**ip local-proxy-arp** Enable Local Proxy ARP function on the specified Layer 3 interface..
Step 4	**show ip local-proxy-arp** Show the Local Proxy ARP configuration..
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 Local Proxy ARP function for VLAN interface 1:

Switch#configure

Switch(config)#interface vlan 1

Switch(config-if)#ip local-proxy-arp

Switch(config-if)#show ip local-proxy-arp

Interface	IP Address	IP Mask	Status
---	---	---	---
vlan 1	192.168.0.1	255.255.255.0	Enabled

Switch(config-if)#end

Switch#copy running-config startup-config

3 Appendix: Default Parameters

Default ARP settings are listed in the following tables.

Table 3-1 Default Gratuitous Settings

Parameter	Default Setting
Send on IP Interface Status Up	Enable
Send on Duplicate IP Detected	Disable
Gratuitous ARP Learning	Disable
Gratuitous ARP Periodical Send Interval	0 second

Part 17

Configuring QoS

CHAPTERS

1. QoS
2. Class of Service Configuration
3. Bandwidth Control Configuration
4. Voice VLAN Configuration
5. Auto VoIP Configuration
6. Configuration Examples
7. 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, VoIP, 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 differentiated services to certain types of traffic.

1.2 Supported Features

You can configure the class of service, bandwidth control, Voice VLAN and Auto VoIP features on the switch to maximize the network performance and bandwidth utilization.

Class of Service

The switch classifies the ingress packets, maps the packets to different priority queues and then forwards the packets according to specified scheduler settings to implement QoS function.

- Priority Mode: Three modes are supported, Port Priority, 802.1p Priority and DSCP Priority.
- Scheduler Mode: Two scheduler type are supported, Strict and Weighted.

Bandwidth Control

Bandwidth Control functions to control the traffic rate and traffic threshold on each port to ensure network performance.

- Rate limit functions to limit the ingress/egress traffic rate on each port. In this way, the network bandwidth can be reasonably distributed and utilized.
- Storm Control function allows the switch to monitor 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.

Voice VLAN and Auto VoIP

The voice VLAN and Auto VoIP features are 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 Voice VLAN or Auto VoIP.

These two features can be enabled on the ports that transmit voice traffic only or transmit both voice traffic and data traffic. Voice VLAN can change the voice packets' 802.1p priority and transmit the packets in desired VLAN. Auto VoIP can inform the voice devices of send the packets with specific configuration by working with the LLDP-MED feature.

2 Class of Service 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 802.1p priority, and then mapped to the queue according to the 802.1p to queue mapping.

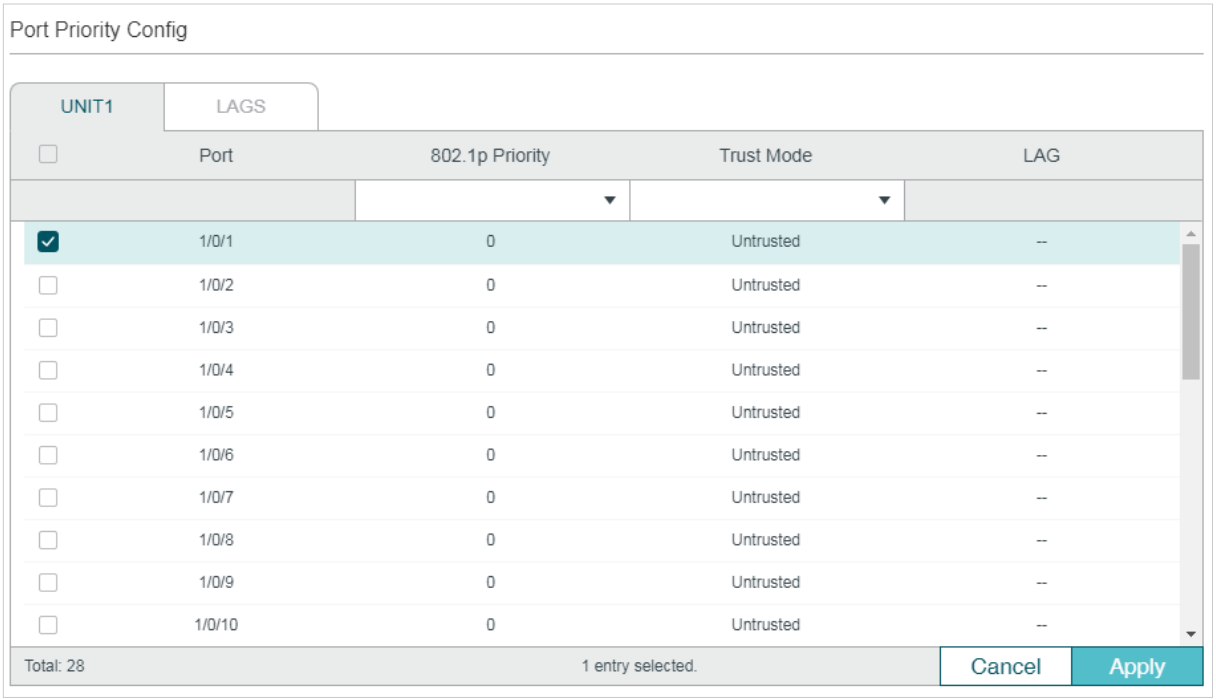
2.1 Using the GUI

2.1.1 Configuring Port Priority

- Configuring the Trust Mode and Port to 802.1p Mapping

Choose the menu **QoS > Class of Service > 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 Untrusted.

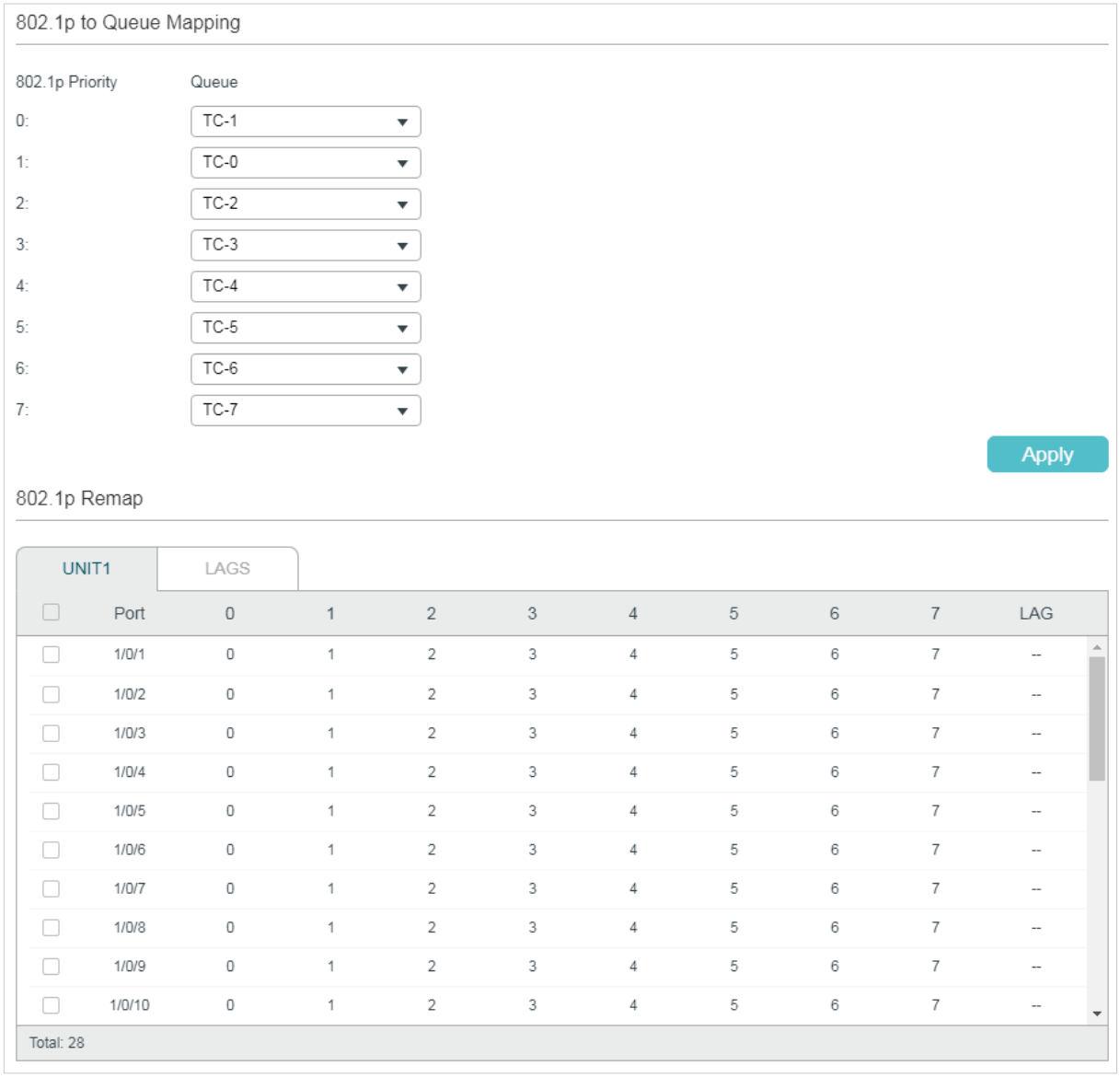
802.1p Priority	Specify the port to 802.1p mapping for the desired port. The ingress packets from one port are first mapped to 802.1p priority based on the port to 802.1p mapping, then to TC queues based on the 802.1p to queue mapping. The untagged packets from one port will be added an 802.1p priority value according to the port to 802.1p priority mapping.
Trust Mode	Select the Trust mode as Untrusted. 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 > Class of Service > 802.1p Priority** to load the following page.

Figure 2-2 Configuring the 802.1p to Queue Mapping



In the **802.1p to Queue Mapping** section, configure the mappings and click **Apply**.

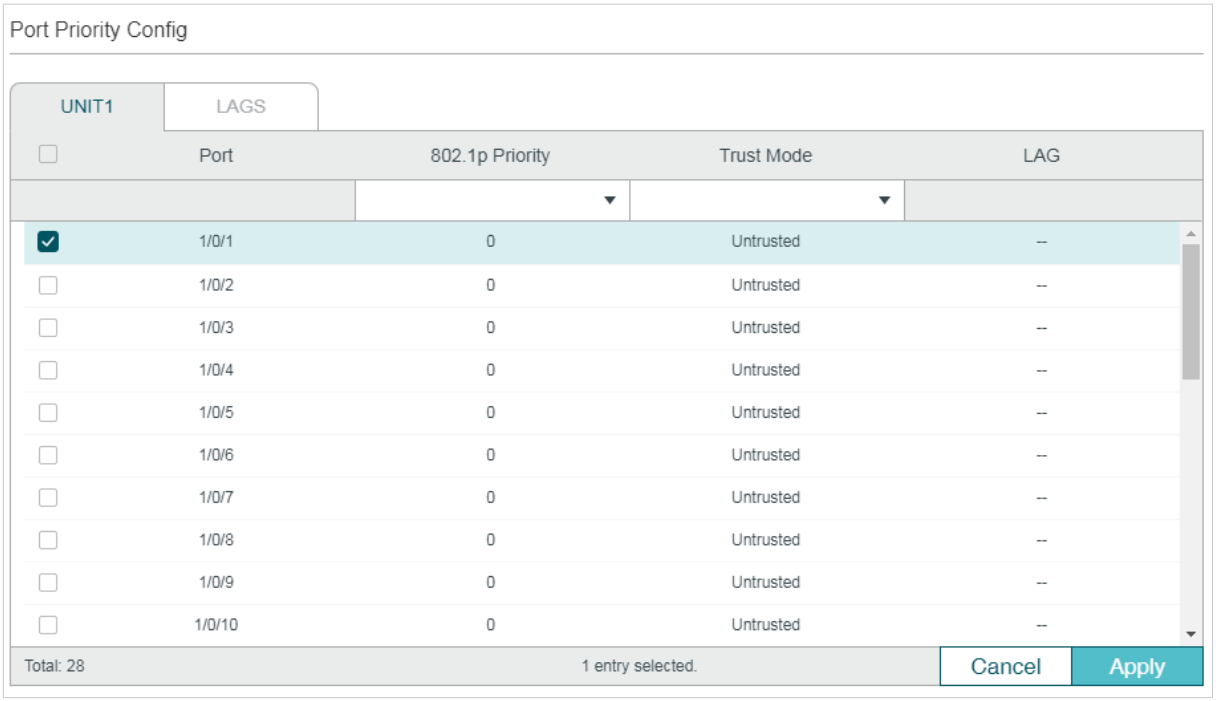
802.1p Priority	Displays the number of 802.1p priority. In QoS, 802.1p priority is used to represent class of service.
Queue	Select the TC queue for the desired 802.1p priority. The packets with the desired 802.1p priority will be put in the corresponding queue.

2.1.2 Configuring 802.1p Priority

■ Configuring the Trust Mode

Choose the menu **QoS > Class of Service > 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.

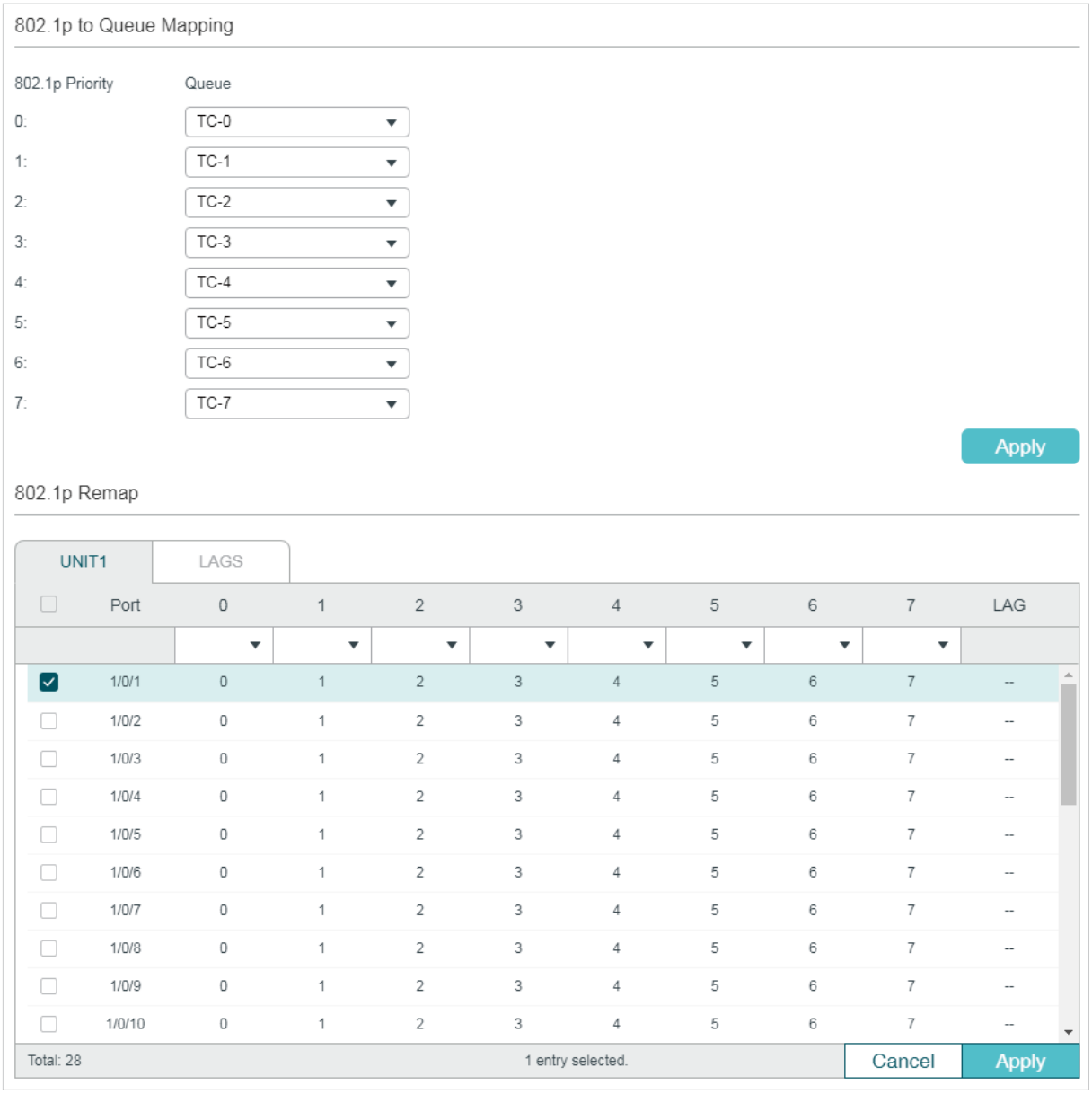
Trust Mode	Select the Trust mode as Trust 802.1p. In this mode, the tagged packets will be processed according to the 802.1p priority configuration and the untagged packets will be processed according to the port priority configuration.

2) Click **Apply**.

Configuring the 802.1p to Queue Mapping and 802.1p Remap

Choose the menu **QoS > Class of Service > 802.1p Priority** to load the following page.

Figure 2-4 Configuring the 802.1p to Queue Mapping and 802.1p Remap



Follow these steps to configure the parameters of the 802.1p priority:

1) In the **802.1p to Queue Mapping** section, configure the mappings and click **Apply**.

802.1p Priority	Displays the number of 802.1p priority. In QoS, 802.1p priority is used to represent class of service. IEEE 802.1p standard defines three bits in 802.1Q tag as PRI filed. The PRI values are called 802.1p priority and used to represent the priority of the layer 2 packets. This function requires packets with VLAN tags.
Queue	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) (Optional) In the **802.1p Remap** section, configure the 802.1p to 802.1p mappings and click **Apply**.

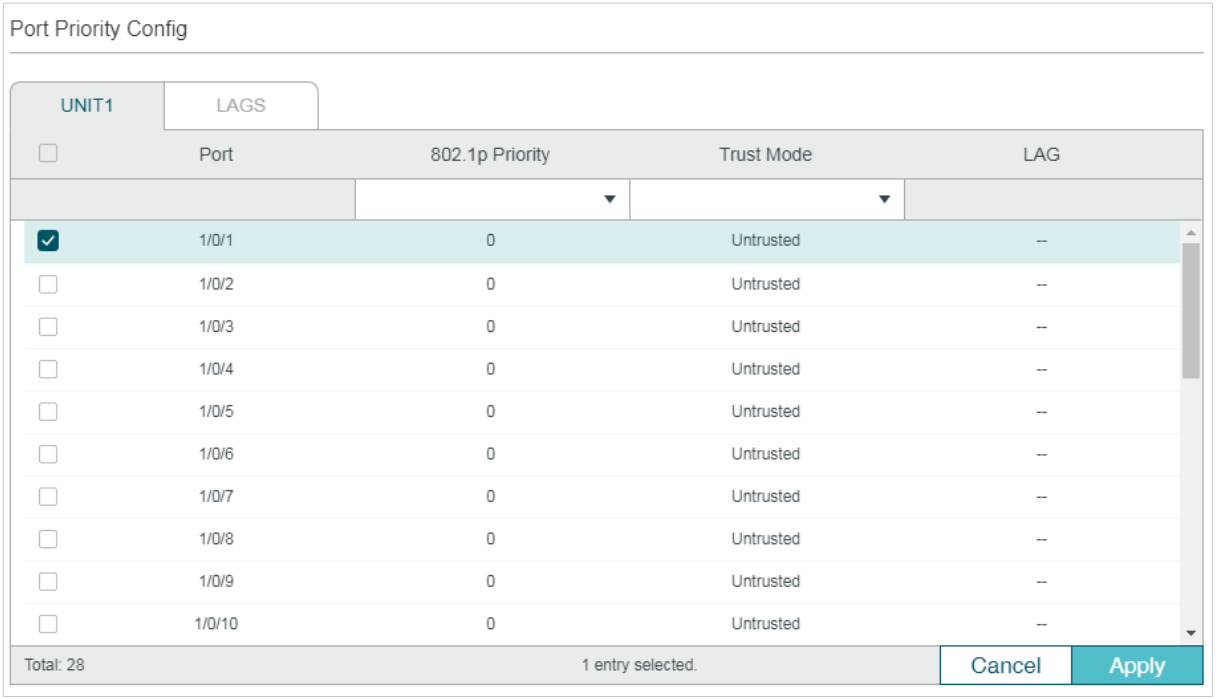
0 - 7	Select the number of 802.1p priority to which the desired 802.1p priority will be remapped. 802.1p Remap is used to modify the 802.1p priority of the ingress packets. When the switch detects the packets with desired 802.1p priority, it will modify the value of 802.1p priority according to the map.

2.1.3 Configuring DSCP Priority

■ Configuring the Trust Mode

Choose the menu **QoS > Class of Service > Port Priority** to load the following page.

Figure 2-5 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.

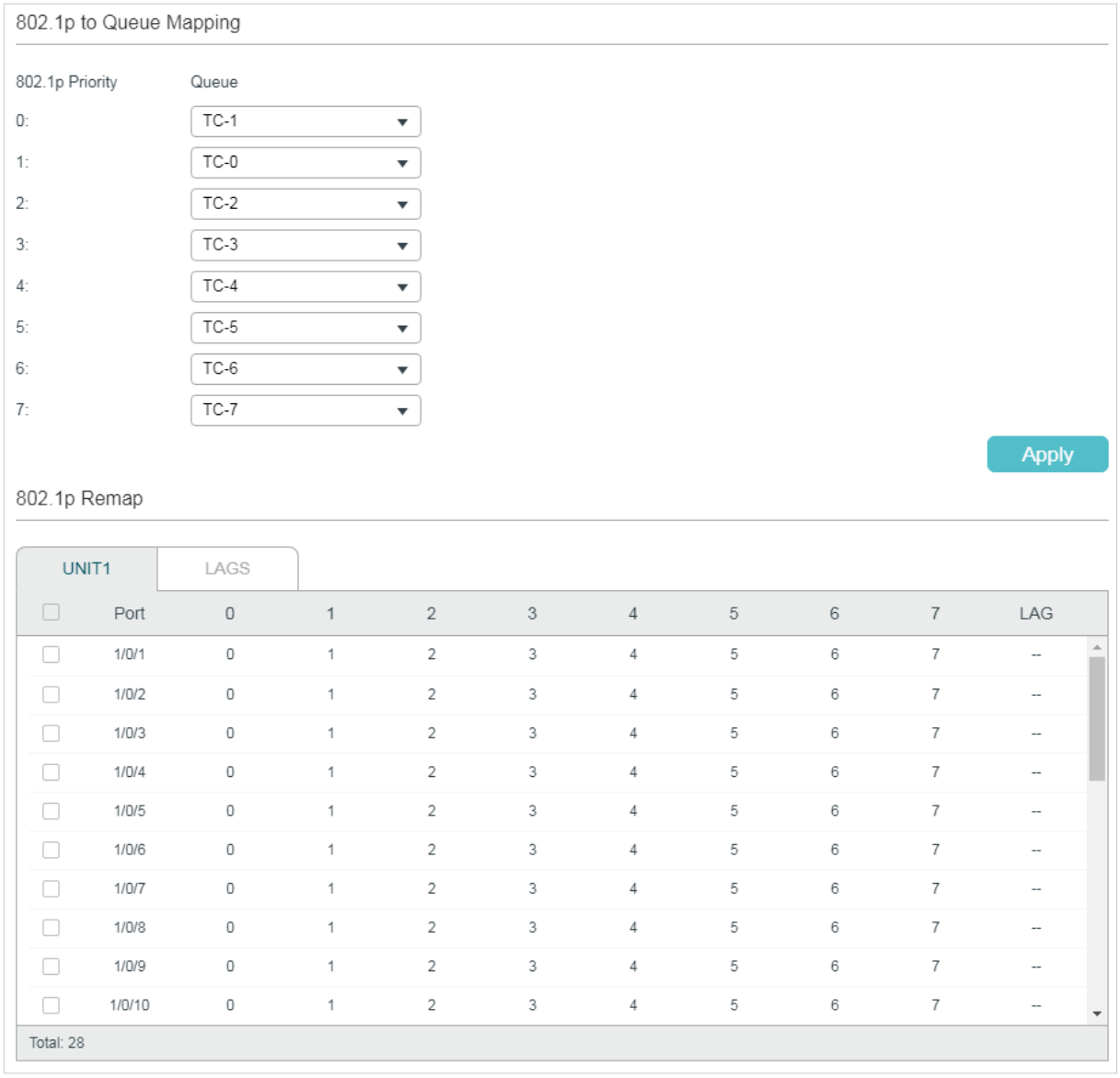
Trust Mode	Select the Trust mode as Trust DSCP. In this mode, the IP packets will be processed according to the DSCP priority configuration and the non-IP packets will be processed according to the port priority configuration.

2) Click **Apply**.

Configuring the 802.1p to Queue Mapping

Choose the menu **QoS > Class of Service > 802.1p Priority** to load the following page.

Figure 2-6 Configuring the 802.1p to Queue Mapping



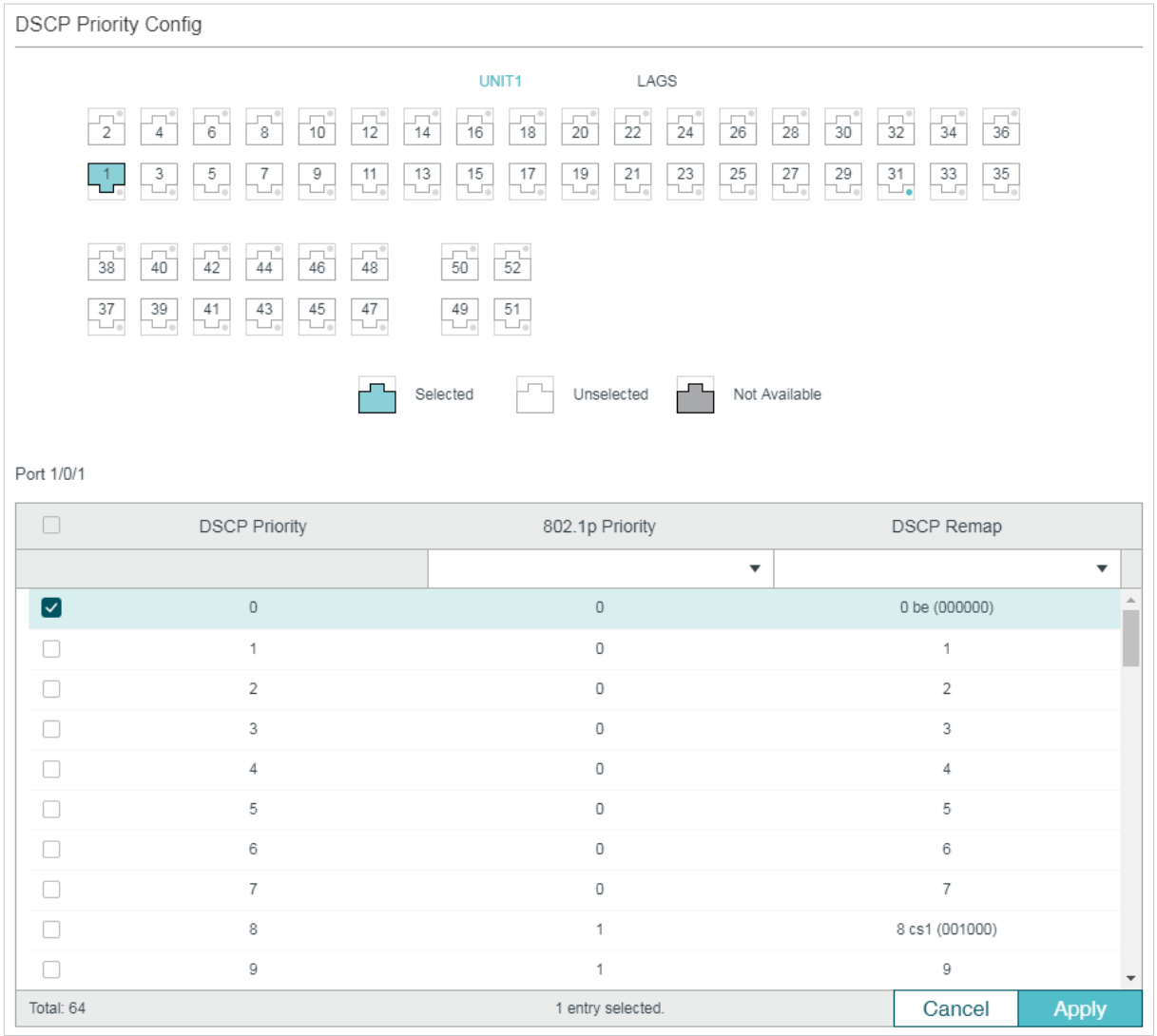
In the **802.1p to Queue Mapping** section, configure the mappings and click **Apply**.

802.1p Priority	Displays the number of 802.1p priority. In QoS, 802.1p priority is used to represent class of service.
Queue	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.

Configuring the DSCP to 802.1p Mapping and the DSCP Remap

Choose the menu **QoS > Class of Service >DSCP Priority** to load the following page.

Figure 2-7 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 Priority	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.
802.1p 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 Remap	(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:

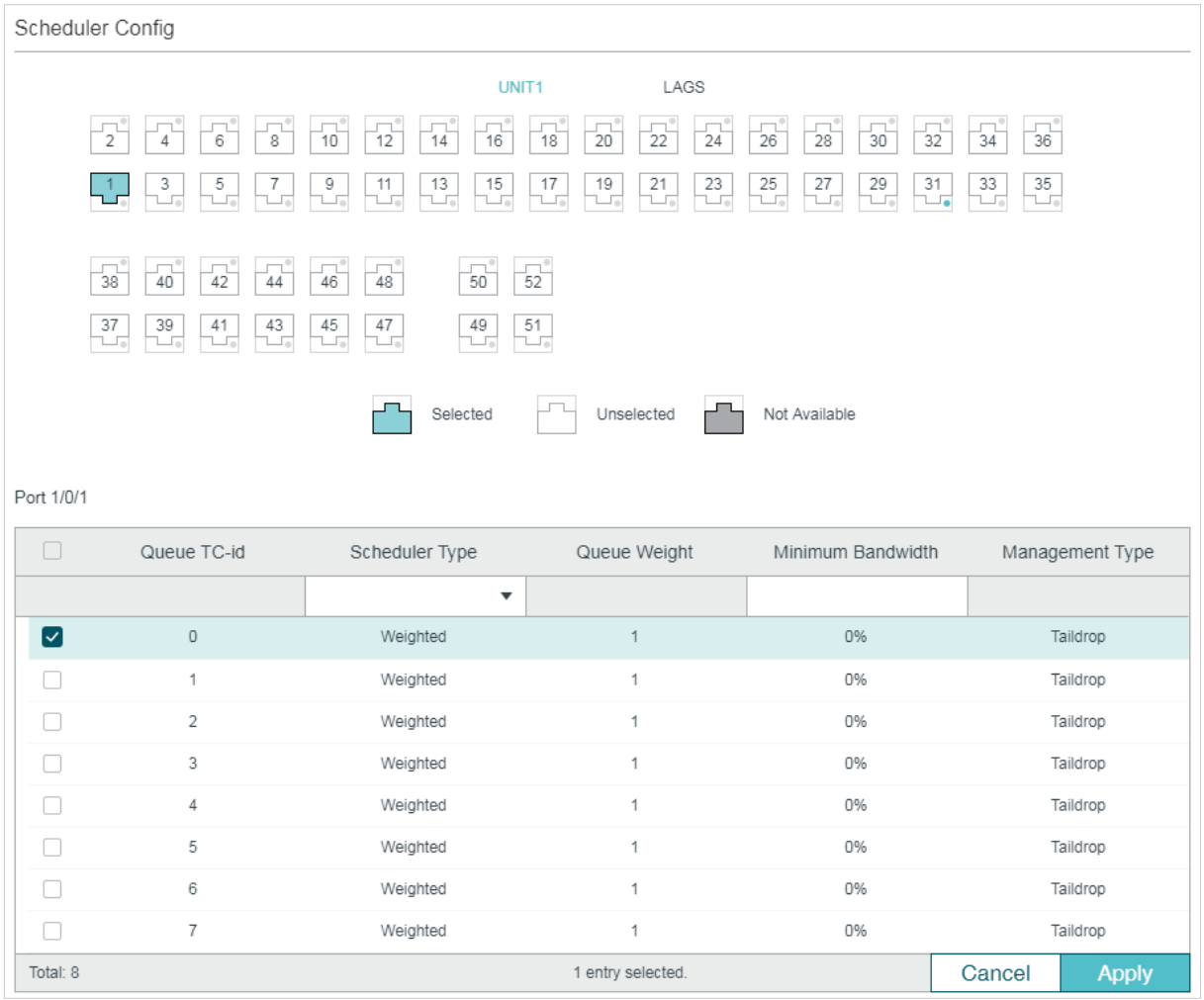
All the ports in the same LAG should be assigned with the same port priority.

2.1.4 Specifying the Scheduler Settings

Specify the scheduler settings to control the forwarding sequence of different TC queues when congestion occurs.

Choose the menu **QoS > Class of Service > Scheduler Settings** to load the following page.

Figure 2-8 Specifying the Scheduler Settings



Follow these steps to configure the schedule mode:

1) In the **Scheduler Config** section, select the desired port.
2) Select the desired queue and configure the parameters.

Queue TC-id	Displays the ID number of priority Queue.

Scheduler Type	Select the type of scheduling used for corresponding queue. When the network congestion occurs, the egress queue will determine the forwarding sequence of the packets according to the type. **Strict:** In this mode, the egress queue will use SP (Strict Priority) to process the traffic in different queues. When congestion occurs, the traffic will be transmitted according to its queue priority strictly. The queue with higher priority occupies the whole bandwidth. Packets in the queue with lower priority are sent only when the queue with higher priority is empty. **Weighted:** In this mode, the egress queue will use WRR (Weighted Round Robin) to process the traffic in different queues. When congestion occurs, all the traffic will be transmitted, but the bandwidth that each traffic queue occupies will be allocated based on the queue weight.
Queue Weight	Specify the queue weight for the desired queue. This value can be set only in the Weighted mode. The valid values are from 1 to 127.
Minimum Bandwidth	Specify the minimum guaranteed bandwidth for the desired queue. The valid values are from 0 to 100 and 0 means Minimum Bandwidth is disabled. If the queue bandwidth calculated according to the weight is smaller than the minimum bandwidth, the switch will be forced to allocated the minimum bandwidth to the queue, and the other queue will share the rest bandwidth based on the weight.
Management Type	Displays the Management Type for the queues. The switch supports Taildrop mode. When the traffic exceeds the limit, the additional traffic will be dropped.

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* **|** *dot1p* **|** *dscp***}** Select the trust mode for the port. By default, it is untrust. Here we set the trust mode as untrust. *untrust:* Specify the ports' trust mode 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 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 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 {***untrust* **|** *dot1p* **|** *dscp***}** Select the trust mode for the port. By default, it is untrust. Here we set the trust mode as dot1p. *dot1p:* Specify the ports' trust mode as dot1p. In this mode, the tagged packets will be processed according to the 802.1p priority configuration and the untagged packets will be processed according to the port priority configuration.
Step 4	**show qos trust 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 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 {***untrust* **|** *dot1p* **|** *dscp***}** Select the trust mode for the port. By default, it is untrust. Here we set the trust mode as dscp. *dscp:* Specify the ports' trust mode as dscp. In this mode, the IP packets will be processed according to the DSCP priority configuration and the non-IP packets will be processed according to the port priority configuration.
Step 4	**show qos trust 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 Remp

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. 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 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.

Note:

All the ports in the same LAG should be assigned with the same port priority.

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 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 Specifying the Scheduler Settings

Follow these steps to specify the scheduler settings to control the forwarding sequence of different TC queues when congestion occurs.

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 queue** *tc-queue* **mode {**sp **|** wrr**} [weight** *weight***]** Specify the type of scheduling used for corresponding queue. When the network congestion occurs, the egress queue will determine the forwarding sequence of the packets according to the type. By default, it is wrr mode and the all the queue weights are 1. *tc-queue*: Specify the ID number of TC queue. The valid values are from 0 to 7. sp: In sp mode, the egress queue will use SP (Strict Priority) to process the traffic in different queues. When congestion occurs, the traffic will be transmitted according to its queue priority strictly. The queue with higher priority occupies 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, the egress queue will use WRR (Weighted Round Robin) to process the traffic in different queues. When congestion occurs, all the traffic will be transmitted, but the bandwidth that each traffic queue occupies will be allocated based on the queue weight. *weight*: Specify the queue weight for the desired queue. This value can be set only in the wrr mode. The valid values are from 1 to 127.
Step 4	**qos queue** *tc-queue* **bandwidth** *rate* Specify the minimum guaranteed bandwidth for the desired queue. If the queue bandwidth calculated according to the weight is smaller than the minimum bandwidth, the switch will be forced to allocated the minimum bandwidth to the queue, and the other queue will share the rest bandwidth based on the weight. *tc-queue:* Specify the ID number of the TC queue. The valid values are from 0 to 7. *rate:* Specify the rate for the desired TC queue. The valid values are from 1 to 100. The default value is 0.
Step 5	**show qos queue interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]** Verify the scheduler settings..
Step 6	**end** Return to privileged EXEC mode.

Step 7	**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 specify the scheduler settings for port 1/0/1. Set the scheduler mode of TC1 as sp mode, set the scheduler mode of TC4 as wrr mode and set the queue weight as 5. Set the minimum bandwidth of TC4 as 10.

Switch#configure

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

Switch(config-if)#qos queue 1 **mode** sp

Switch(config-if)#qos queue 4 **mode** wrr **weight** 5

Switch(config-if)#qos queue 4 **bandwidth** 10

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

Gi1/0/1----LAG: N/A

Queue	Schedule Mode	Weight	Min Bandwidth(%)
TC0	WRR	1	0%
TC1	Strict	N/A	0%
TC2	WRR	1	0%
TC3	WRR	1	0%
TC4	WRR	5	10%
TC5	WRR	1	0%
TC6	WRR	1	0%
TC7	WRR	1	0%

Switch(config-if)#end

Switch#copy running-config startup-config

3 Bandwidth Control Configuration

With bandwidth control configurations, you can:

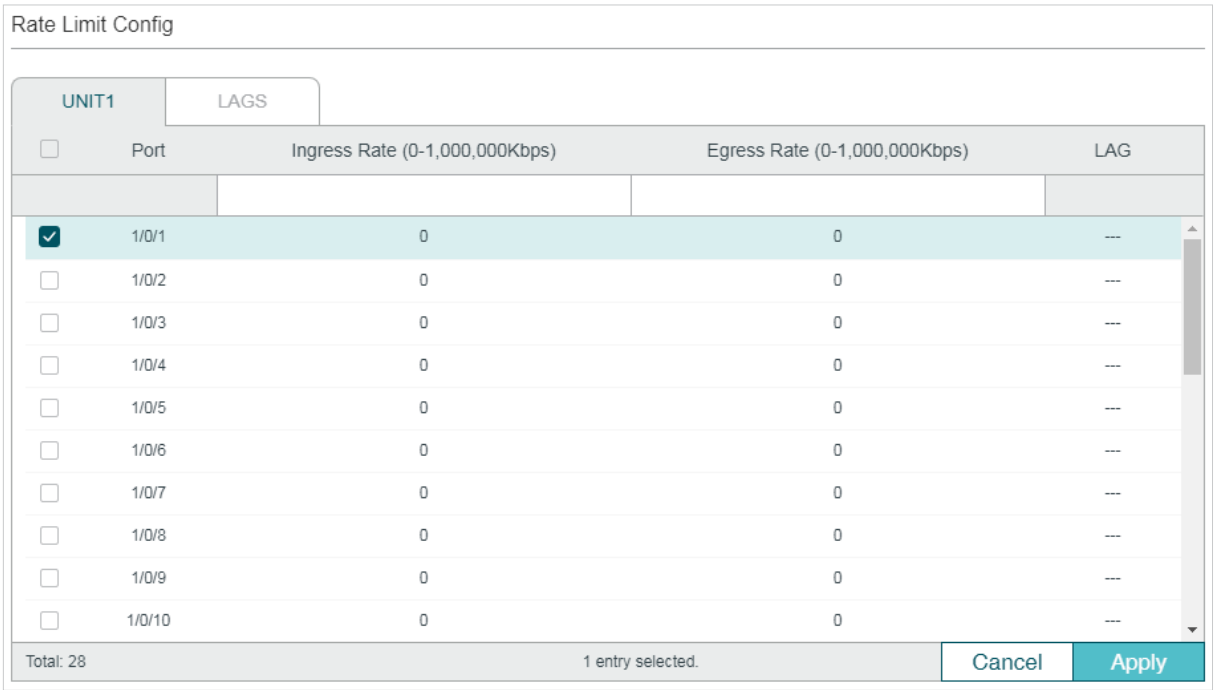
- Configure rate limit
- Configure storm control

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 Configuring Rate Limit



Follow these steps to configure the Rate Limit function:

1) Select the desired port and configure the upper rate limit to receive and send packets.

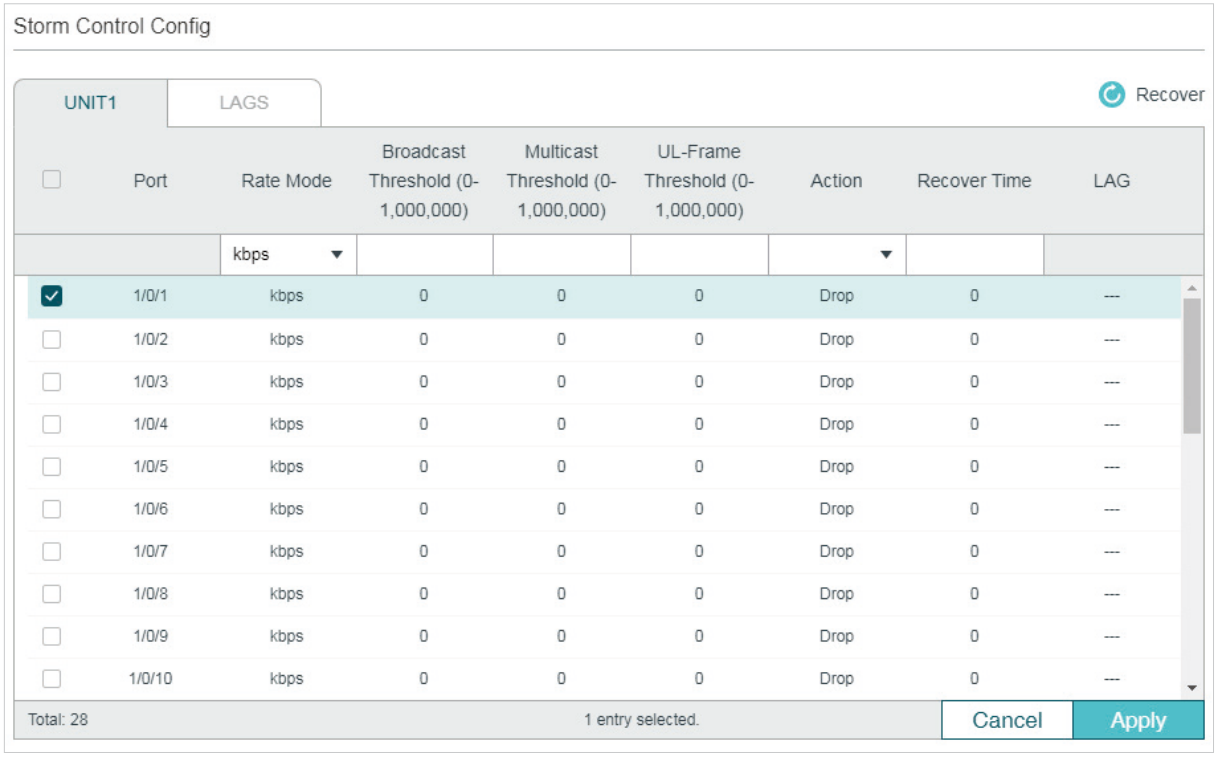
Ingress Rate (0-1,000,000Kbps)	Configure the upper rate limit for receiving packets on the port. The valid values are from 0 to 1000000 Kbps and 0 means the ingress rate limit is disabled.
Egress Rate (0-1,000,000Kbps)	Configure the bandwidth for sending packets on the port. The valid values are from 0 to 1000000 Kbps and 0 means the egress rate limit is disabled.

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 Configuring Storm Control



Follow these steps to configure the Storm Control function:

1) Select the desired port and configure the upper rate limit for forwarding broadcast packets, multicast packets and UL-frames (Unknown unicast frames).

Rate Mode	Specify the Rate Mode for the broadcast threshold, multicast threshold and UL-Frame threshold on the desired port. **kbps:** The switch will limit the maximum speed of the specific kinds of traffic in kilo-bits per second. **ratio:** The switch will limit the percentage of bandwidth utilization for specific kinds of traffic. **pps:** The switch will limit the maximum number of packets per second for specific kinds of traffic.
Broadcast Threshold (0-1,000,000)	Specify the upper rate limit for receiving broadcast packets. The valid values differ among different rate modes. The value 0 means the broadcast threshold is disabled. The broadcast traffic exceeding the limit will be processed according to the Action configurations.
Multicast Threshold (0-1,000,000)	Specify the upper rate limit for receiving multicast packets. The valid values differ among different rate modes. The value 0 means the multicast threshold is disabled. The multicast traffic exceeding the limit will be processed according to the Action configurations.

UL-Frame Threshold (0-1,000,000)	Specify the upper rate limit for receiving unknown unicast frames. The valid values differ among different rate modes. The value 0 means the unknown unicast threshold is disabled. The traffic exceeding the limit will be processed according to the Action configurations.
Action	Select the action that the switch will take when the traffic exceeds its corresponding limit. **Drop:** Set the Action as Drop. The port will drop the subsequent packets when the traffic exceeds the limit. **Shutdown:** Set the Action as Shutdown. The port will be shutdown when the traffic exceeds the limit.
Recover Time	Specify the recover time for the port. It takes effect only when the action is set as shutdown. The valid values are from 0 to 3600 seconds. When the port is shutdown, it can recover to its normal state after the recover time passed. If the recover time is specified as 0, which means the port will not recover to its normal state automatically and you can recover the port manually.

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.

3.2 Using the CLI

3.2.1 Configuring Rate Limit

Follow these steps to 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* **| 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	**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 0 to 1000000 Kbps. *egress-rate:* Configure the upper rate limit for sending packets on the port. The valid values are from 0 to 1000000 Kbps.

Step 4	**show bandwidth interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]** 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

Follow these steps to 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* **| 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 **storm-control rate-mode {**kbps **|** ratio **|** pps**}**

Specify the Rate Mode for the broadcast threshold, multicast threshold and UL-Frame threshold on the desired port.

kbps: The switch will limit the maximum speed of the specific kinds of traffic in kilo-bits per second.

ratio: The switch will limit the percentage of bandwidth utilization for specific kinds of traffic.

pps: The switch will limit the maximum number of packets per second for specific kinds of traffic.

Step 4 **storm-control broadcast** *rate*

Specify the upper rate limit for receiving broadcast packets. The broadcast traffic exceeding the limit will be processed according to the Action configurations.

rate: Enter the upper rate. In kbps mode, the valid values are from 1 to 1000000 Kbps. In ratio mode, the valid values are from 1 to100 percent. In pps mode, the valid values are from 1 to 1488000 packets per second.

Step 5 **storm-control multicast** *rate*

Specify the upper rate limit for receiving multicast packets. The multicast traffic exceeding the limit will be processed according to the Action configurations.

rate: Enter the upper rate. In kbps mode, the valid values are from 1 to 1000000 Kbps. In ratio mode, the valid values are from 1 to100 percent. In pps mode, the valid values are from 1 to 1488000 packets per second.

Step6 **storm-control unicast** *rate*

Specify the upper rate limit for receiving unknown unicast frames. The traffic exceeding the limit will be processed according to the Action configurations.

rate: Enter the upper rate. In kbps mode, the valid values are from 1 to 1000000 Kbps. In ratio mode, the valid values are from 1 to100 percent. In pps mode, the valid values are from 1 to 1488000 packets per second.

Step 7 **storm-control exceed {**drop **|** shutdown**} [recover-time** *time***]**

Specify the action and the recover time. The switch will perform the action when the traffic exceeds its corresponding limit. By default, it is drop.

drop**:** Set the Action as Drop. The port will drop the subsequent packets when the traffic exceeds the limit.

shutdown**:** Set the Action as Shutdown. The port will be shutdown when the traffic exceeds the limit.

time: Specify the recover time for the port. It takes effect only when the action is set as shutdown. The valid values are from 0 to 3600 and the default value is 0. When the port is shutdown, it can recover to its normal state after the recover time passed. If the recover time is specified as 0, which means the port will not recover to its normal state automatically and you can recover the port manually.

Step 8	**storm-control recover** (Optional) Recover the port manually. When the recover time is specified as 0, the port will not recover to its normal state automatically. In this condition, you need to use this command to recover the port manually.
Step 9	**show storm-control interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id***]** 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 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 upper rate limit of broadcast packets as 148800 pps, Specify the action as shutdown and set the recover time as 10 for port 1/0/5:

Switch#configure

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

Switch(config-if)#storm-control rate-mode pps

Switch(config-if)#storm-control broadcast 148800

Switch(config-if)#storm-control exceed shutdown **recover-time** 10

Switch(config-if)#show storm-control interface gigabitEthernet 1/0/5

Port	Rate Mode	BcRate	McRate	UlRate	Exceed	Recover Time	LAG
Gi1/0/5	pps	148800	0	0	shutdown	10	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

4 Voice VLAN Configuration

To complete the voice VLAN configurations, follow these steps:

1) Create a 802.1Q VLAN
2) Configure OUI addresses
3) Configure Voice VLAN globally
4) Add ports to Voice VLAN

Configuration Guidelines

- Before configuring voice VLAN, you need to create a 802.1Q VLAN for voice traffic. For details about 802.1Q VLAN Configuration, please refer to *802.1Q VLAN Configuration*.
- 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.

4.1 Using the GUI

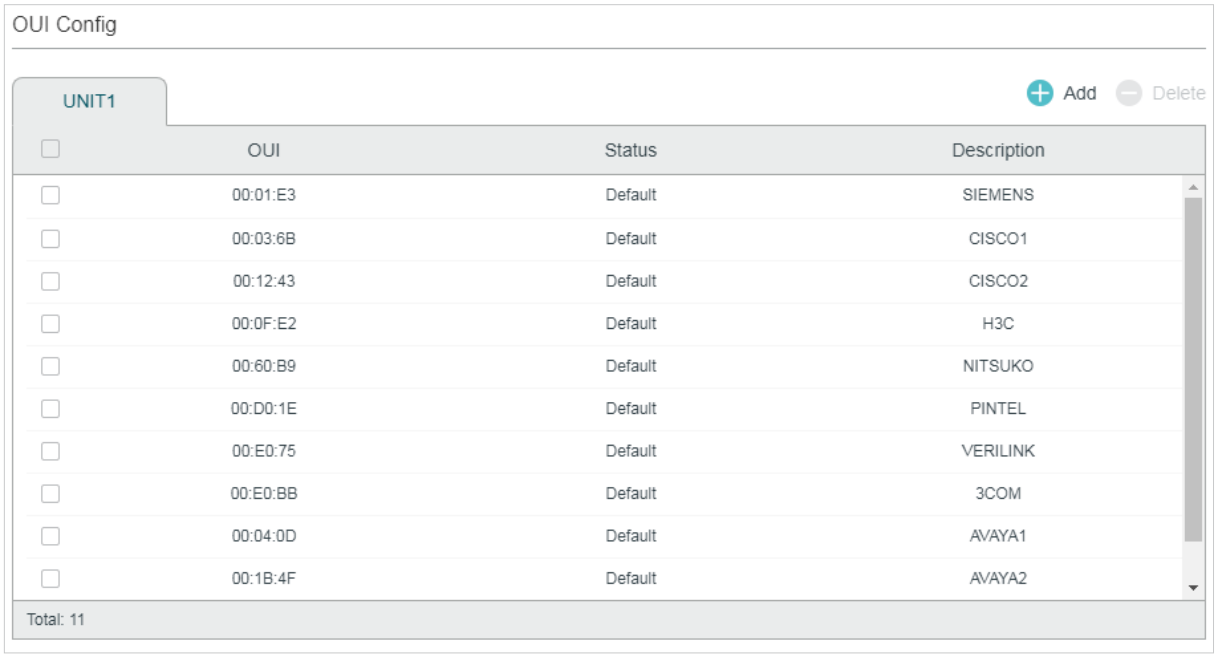
4.1.1 Configuring OUI Addresses

The OUI address is assigned as a unique identifier by IEEE (Institute of Electrical and Electronics Engineers) to a device vendor. It is used by the switch to determine whether a packet is a voice packet.

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.

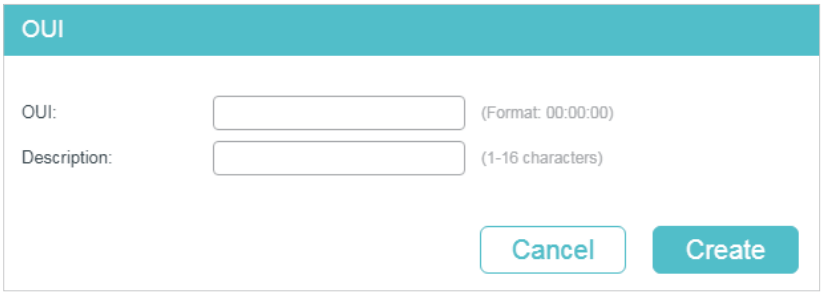
Figure 4-1 Configuring OUI Addresses



Follow these steps to configure the OUI addresses:

1) Click Add to load the following page.

Figure 4-2 Creating an OUI Entry



2) Specify the OUI and the Description.

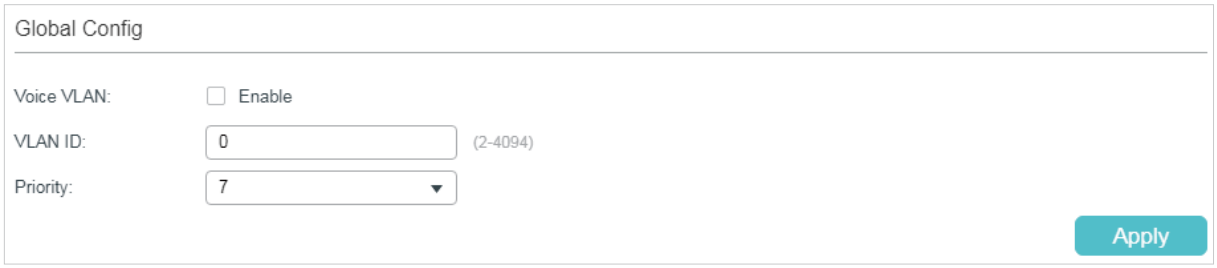
OUI	Enter the OUI address of your voice devices. The OUI address is used by the switch to determine whether a packet is a voice packet. An OUI address is the first 24 bits of a MAC address, and is assigned as a unique identifier by IEEE (Institute of Electrical and Electronics Engineers) to a device vendor. If the source MAC address of a packet matches the OUI addresses in the OUI list, the switch identifies the packet as a voice packet and prioritizes it in transmission.
Description	Give an OUI address description for identification.

3) Click **Create**.

4.1.1 Configuring Voice VLAN Globally

Choose the menu **QoS > Voice VLAN > Global Config** to load the following page.

Figure 4-3 Configuring Voice VLAN Globally



Follow these steps to configure voice VLAN globally:

1) Enable the voice VLAN feature and specify the parameters.

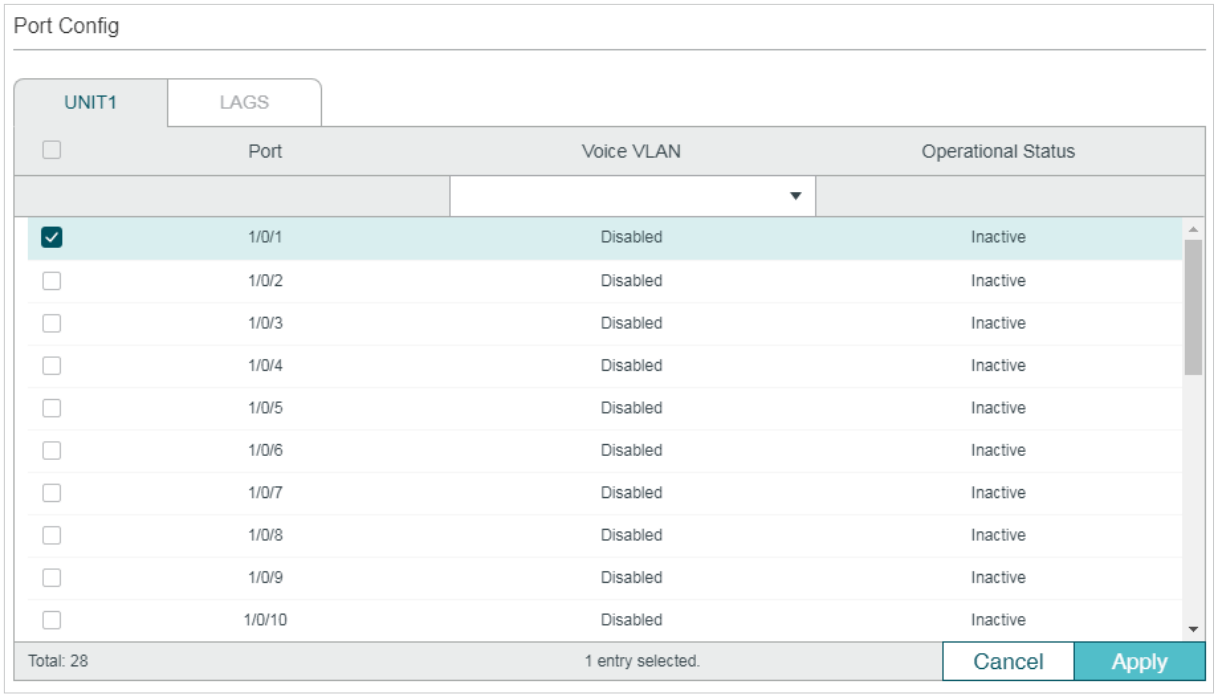
VLAN ID	Specify the 802.1Q VLAN ID to set the 802.1Q VLAN as the voice VLAN.
Priority	Select the priority that will be assigned to voice packets. A bigger value means a higher priority. This is an IEEE 802.1p priority, and you can further configure its scheduler mode in Class of Service if needed.

2) Click **Apply**.

4.1.1 Adding Ports to Voice VLAN

Choose the menu **QoS > Voice VLAN > Port Config** to load the following page.

Figure 4-4 Adding Ports to Voice VLAN



Follow these steps to configure voice VLAN globally:

1) Select the desired ports and choose Enable in Voice VLAN filed.

Voice VLAN	Select Enable to enable the voice VLAN feature on ports and add the desired ports to Voice VLAN.

Optional Status	Displays the state of the Voice VLAN on the corresponding port. **Active:** Indicates that Voive VLAN function is enabled on the port. **Inactive:** Indicates that Voive VLAN function is disabled on the port.

2) Click **Apply**.

4.2 Using the CLI

Follow these steps to configure voice VLAN:

Step 1	**configure** Enter global configuration mode.
Step 2	**show voice vlan oui-table** Check whether the OUI address of your voice device is in the OUI table. 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 matches the OUI addresses in the OUI list, the switch identifies the packet as a voice packet and prioritizes it in transmission.
Step 3	**voice vlan oui** *oui-prefix* **oui-desc** *string* If the OUI address of your voice device is not in the OUI table, add the OUI address to the table. *oui-prefix*: Enter the OUI address for your voice device in the format of XX:XX:XX. *string*: Give an OUI address description for identification. It contains 16 characters at most.
Step 4	**voice vlan** *vid* Enable the voice VLAN feature and specify an existing 802.1Q VLAN as the voice VLAN. *vid:* Enter the 802.1Q VLAN ID to set the 802.1Q VLAN as the voice VLAN.
Step 5	**voice vlan priority** *pri* Specify the priority that will be assigned to voice packets. *pri:* Enter the priority that will be assigned to voice packets. A bigger value means a higher priority. The valid values are from 0 to 7 and the default value is 7. This is an IEEE 802.1p priority, and you can further configure its scheduler mode in Class of Service if needed.
Step 6	**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 7	**voice vlan** Enable the voice VLAN feature on ports and add the desired ports to voice VLAN.

Step 8	**show voice vlan interface** Verify the voice VLAN configuration information.
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 show the OUI table, set VLAN 8 as voice VLAN, set the priority as 6 and enable voice VLAN feature on port 1/0/3:

Switch#configure

Switch(config)#show voice vlan oui-table

00:01:E3 Default SIEMENS

00:03:6B Default CISCO1

00:12:43 Default CISCO2

00:0F:E2 Default H3C

00:60:B9 Default NITSUKO

00:D0:1E Default PINTEL

00:E0:75 Default VERILINK

00:E0:BB Default 3COM

00:04:0D Default AVAYA1

00:1B:4F Default AVAYA2

00:04:13 Default SNOM

Switch(config)#voice vlan 8

Switch(config)#voice vlan priority 6

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

Switch(config-if)#voice vlan

Switch(config-if)#show voice vlan interface

Voice VLAN ID 8

Priority 6

Interface Voice VLAN Mode Operational Status LAG

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

Gi1/0/1 disabled Down N/A

Gi1/0/2	disabled	Down	N/A
Gi1/0/3	enabled	Up	N/A
Gi1/0/4	disabled	Down	N/A
Gi1/0/5	disabled	Down	N/A

.....

Switch(config-if)#end

Switch#copy running-config startup-config

5 Auto VoIP Configuration

Configuration Guidelines

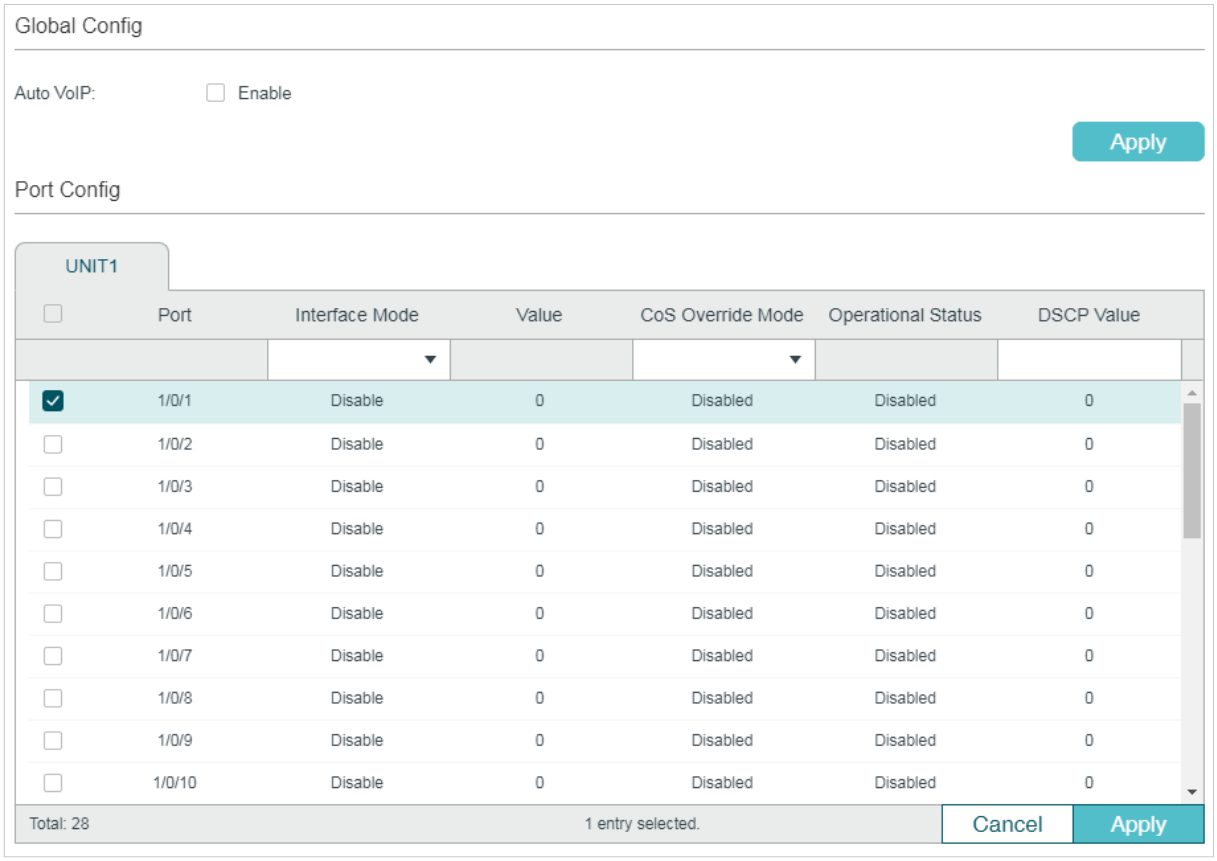
- Before configuring Auto VoIP, you need to enable LLDP-MED on ports and configure the relevant parameters. For details about LLDP-MED configuration, please refer to *LLDP Configurations*.

- Auto VoIP provide flexible solutions for optimizing the voice traffic. It can work with other features such as VLAN and Class of Service to process the voice packets with specific fields. You can choose and configure Auto VoIP and other features according to your needs.

5.1 Using the GUI

Choose the menu **QoS > Auto VoIP** to load the following page.

Figure 5-1 Configuring Auto VoIP



Follow these steps to configure the OUI addresses:

1) In the **Global Config** section, enable the Auto VoIP function gloablly.
2) In the **Port Config** section, select the desired and configure the parameters.

Interface Mode	Select the interface mode for the port. **Disable:** Disable the Auto VoIP function on the corresponding port. **None:** Allow the voice devices to use its own configuration to send voice traffic. **VLAN ID:** The voice devices will send voice packets with desired VLAN tag. If this mode is selected, it is necessary to specify the VLAN ID in the Value field. In addition, you need to configure the 802.1Q VLAN to ensure the corresponding ports can forward the packets normally. **Dot1p:** The voice devices will send voice packets with desired 802.1p priority. If this mode is selected, it is necessary to specify 802.1p priority in the Value field. In addition, you can configure the Class of Service to make the switch process the packets according to the 802.1p priority. **Untagged:** The voice devices will send untagged voice packets.
Value	Enter the value of VLAN ID or 802.1p priority for the port according to the Interface Mode configurations.
CoS Override Mode	Enable or disable the Class of Service override mode. **Enabled:** Enable CoS override. The switch will ignore the 802.1p priority in the voice packets and put the packets in TC-5 directly. **Disabled:** Disable CoS override. The switch will then put the voice packets in the corresponding TC queue according to the 802.1p priority of the packets.
Operational Status	Displays the operating status of the Voice VLAN feature on the interface. To make it enabled, you must enable the Voice VLAN both globally and on the interface.
DSCP Value	Enter the value of DSCP priority. The voice device will send the packets with the corresponding DSCP value. In addition, you can configure the Class of Service to make the switch process the packets according to the DSCP priority.

3) Click **Apply**.

5.2 Using the CLI

Follow these steps to configure Auto VoIP:

Step 1	**configure** Enter global configuration mode.
Step 2	**auto-voip** Enable Auto VoIP globally.

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 Select the interface mode for the port.

no auto-voip

Specify the interface mode as disabled, which means the Auto VoIP function is disabled on the corresponding port.

auto-voip none

Specify the interface mode as none. In this mode, the switch allows the voice devices to use its own configuration to send voice traffic.

auto-voip *vlan-id*

Specify the interface mode as VLAN ID. In this mode, the voice devices will send voice packets with desired VLAN tag. If this mode is selected, it is necessary to specify the 802.1Q VLAN ID. The valid values are from 1 to 4093.

In addition, you need to configure the 802.1Q VLAN to ensure the corresponding ports can forward the packets normally.

auto-voip dot1p *dot1p*

Specify the interface mode as dot1p. In this mode, the voice devices will send voice packets with desired 802.1p priority. If this mode is selected, it is necessary to specify 802.1p priority. The valid values are from 0 to 7.

In addition, you can configure the Class of Service to make the switch process the packets according to the 802.1p priority.

auto-voip untagged

Specify the interface mode as untagged. In this mode, the voice devices will send untagged voice packets.

Step 5 **auto-voip data priority {**trust **|** untrust**}**

Enable or disable the Class of Service override mode. By default, it is trust, which means the Class of Service override mode is disabled.

trust: In this mode, the switch will then put the voice packets in the corresponding TC queue according to the 802.1p priority of the packets.

untrust: In this mode, the switch will ignore the 802.1p priority in the voice packets and put the packets in TC-5 directly.

Step 6 **auto-voip dscp** *value*

Specify the value of DSCP priority. The voice device will send the packets with the corresponding DSCP value.

In addition, you can configure the Class of Service to make the switch process the packets according to the DSCP priority.

value: Enter the value of DSCP priority. The valid values are from 0 to 63 and the default value is 0.

Step 7	**show auto-voip** Verify the global state of Auto VoIP.
Step 8	**show auto-voip interface** Verify the Auto VoIP configuration information of 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 set the interface mode as dot1p, specify the 802.1p priority as 4, specify the DSCP priority as 10 and enable the CoS override mode for port 1/0/3:

Switch#configure

Switch(config)#auto-voip

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

Switch(config-if)#auto-voip dot1p 4

Switch(config-if)#auto-voip dscp 10

Switch(config-if)#auto-voip data priority untrust

Switch(config-if)#show auto-voip

Administrative Mode: Enabled

Switch(config-if)#show auto-voip interface

Interface.Gi1/0/1

Auto-VoIP Interface Mode. Disabled

Auto-VoIP COS Override. False

Auto-VoIP DSCP Value. 0

Auto-VoIP Port Status. Disabled

Interface.Gi1/0/2

Auto-VoIP Interface Mode. Disabled

Auto-VoIP COS Override. False

Auto-VoIP DSCP Value. 0

Auto-VoIP Port Status. Disabled

Interface.Gi1/0/3

Auto-VoIP Interface Mode. Enabled

Auto-VoIP Priority. 4

Auto-VoIP COS Override. True

Auto-VoIP DSCP Value. 10

Auto-VoIP Port Status. Enabled

.....

Switch(config-if)#end

Switch#copy running-config startup-config

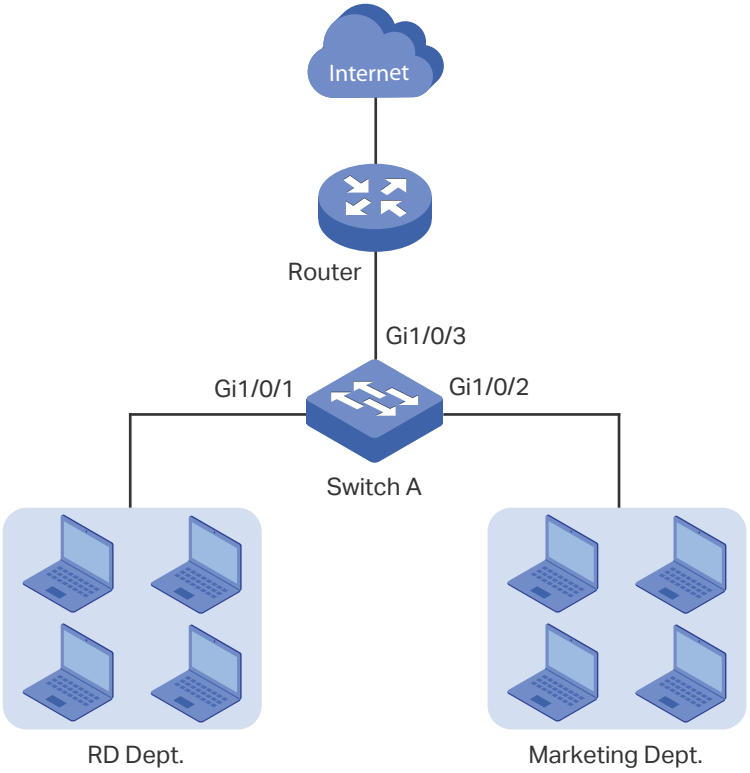
6 Configuration Examples

6.1 Example for Class of Service

6.1.1 Network Requirements

As shown below, both RD department and Marketing department can access the internet. When congestion occurs, the traffic from two departments can both be forwarded and the traffic from the Marketing department should take precedence.

Figure 6-1 QoS Application Topology



6.1.2 Configuration Scheme

To implement this requirement, you can configure Port Priority to put the packets from the Marketing department into the queue with the higher priority than the packets from the RD department.

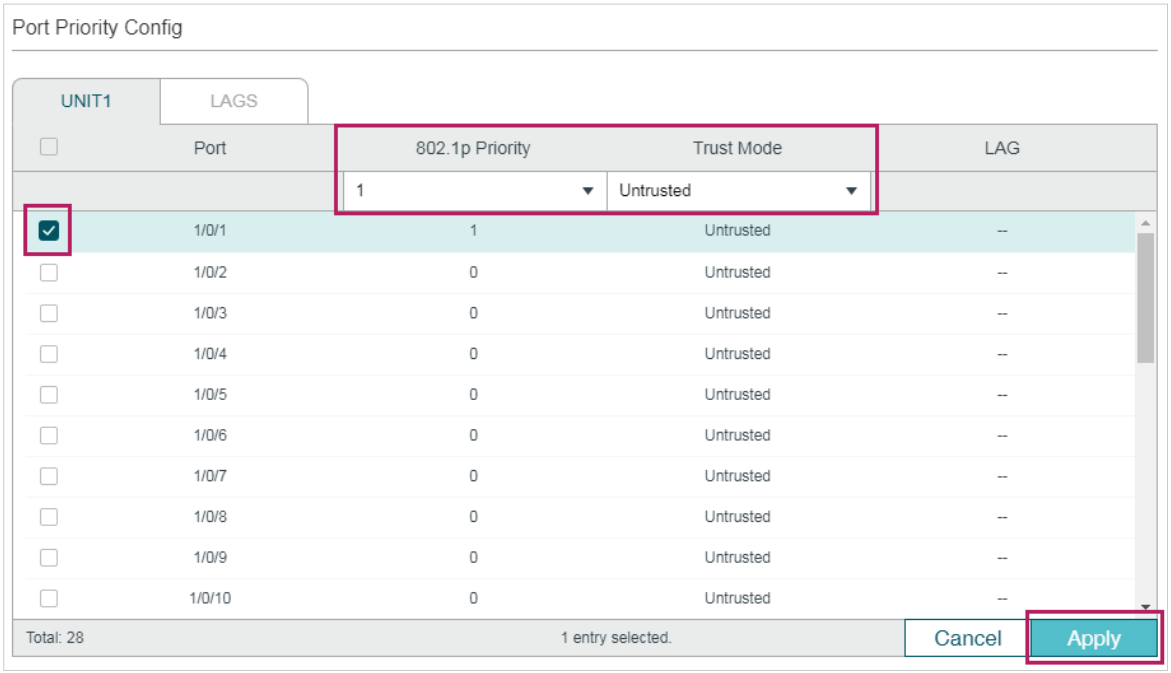
1) Configure the trust mode of port 1/0/1 and port 1/0/2 as untrusted and map the ports to different queues.
2) Set the scheduler type of the queues as weighted for port 1/0/3 and specify the queue weight to make the traffic from the Marketing department take precedence.

Demonstrated with T1600G-52TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

6.1.3 Using the GUI

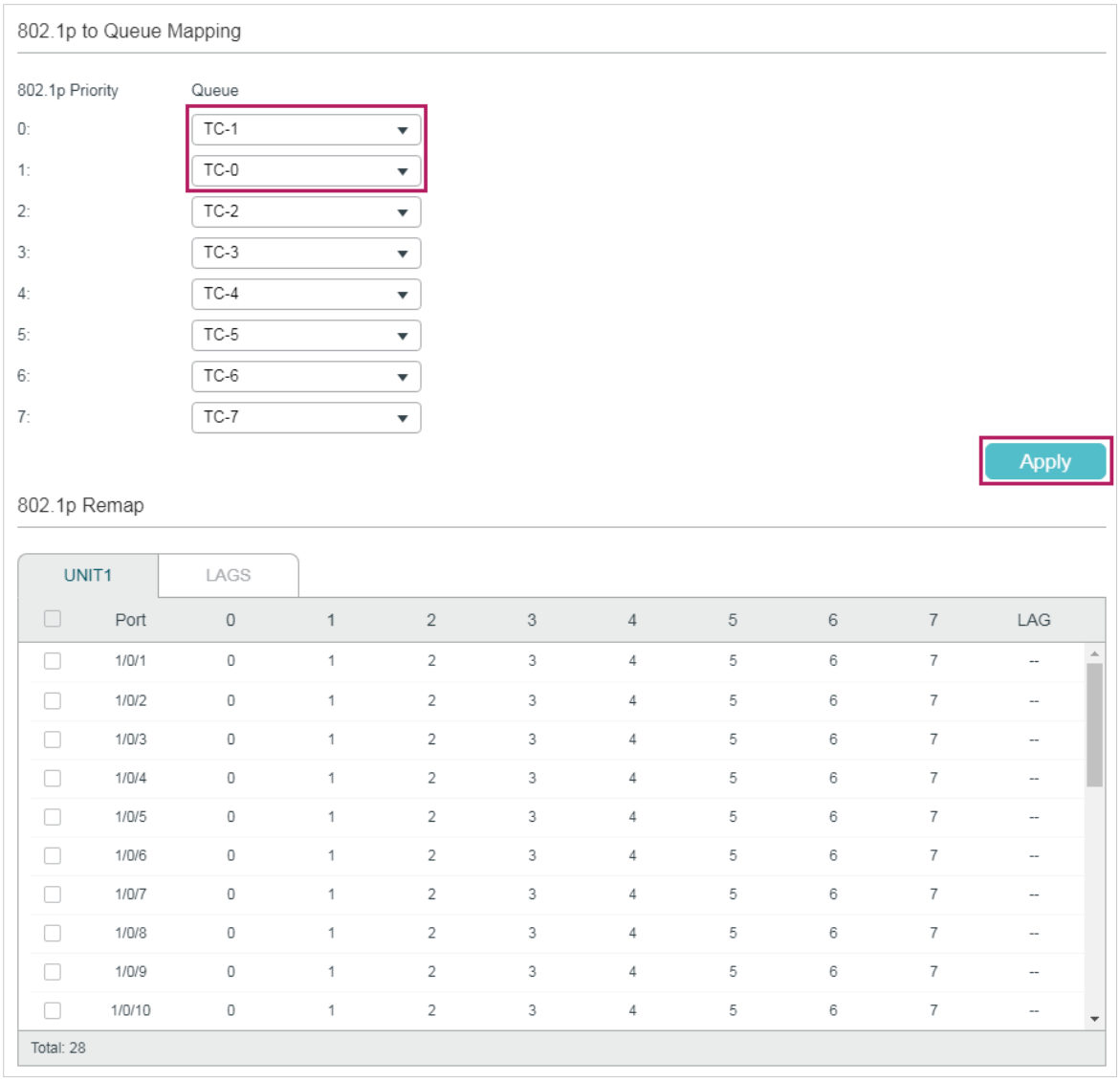
1) Choose the menu **QoS > Class of Service > Port Priority** to load the following page. Set the trust mode of port 1/0/1 and 1/0/2 as untrusted. Specify the 802.1p priority of port 1/0/1 as 1 and specify the 802.1p priority of port 1/0/2 as 0. Click **Apply**.

Figure 6-2 Configuring Port Priority



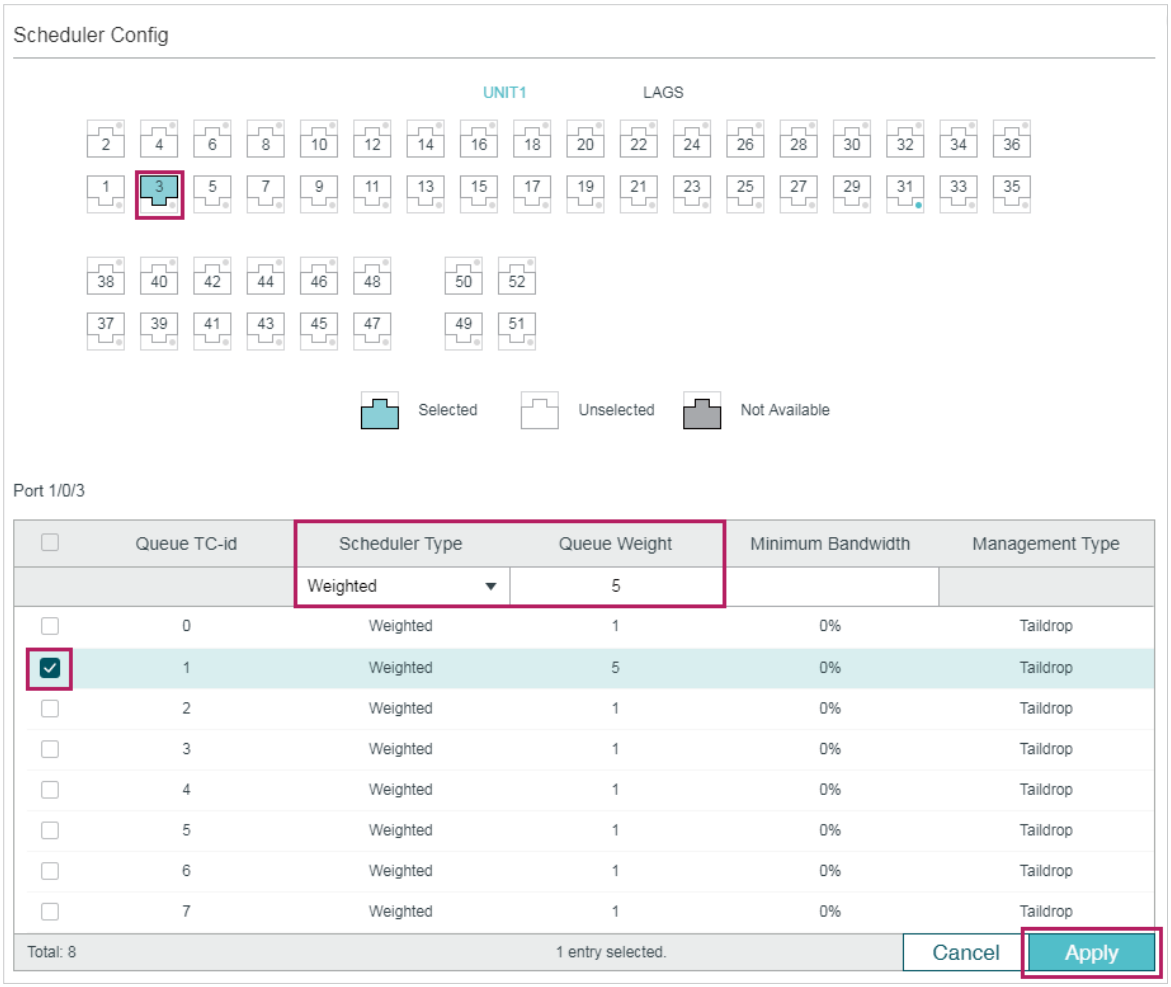
2) Choose the menu **QoS > Class of Service > 802.1p Priority** to load the following page. Map the 802.1p priority 0 to TC-1 and map the 802.1p priority 1 to TC-0. Click **Apply**.

Figure 6-3 Configuring the 802.1p to Queue Mappings



3) Choose the menu **QoS > Class of Service > Scheduler Settings** to load the following page. Select the port 1/0/3 and set the scheduler type of TC-0 and TC-1 as Weighted. Specify the queue weight of TC-0 as 1 and specify the queue weight of TC-1 as 5. Click **Apply**.

Figure 6-4 Configuring the Egress Queue



4) Click Save to save the settings.

6.1.4 Using the CLI

1) Set the trust mode of port 1/0/1 as untrusted and specify the 802.1p priority as 1.

Switch_A#configure

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

Switch_A(config-if)#qos trust mode untrust

Switch_A(config-if)#qos port-priority 1

Switch_A(config-if)#exit

2) Set the trust mode of port 1/0/2 as untrusted and specify the 802.1p priority as 0.

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

Switch_A(config-if)#qos trust mode untrust

Switch_A(config-if)#qos port-priority 0

Switch_A(config-if)#exit

3) Map the 802.1p priority 0 to TC-1 and map the 802.1p priority 1 to TC-0.

Switch_A(config)#qos cos-map 0 1

Switch_A(config)#qos cos-map 1 0

4) Set the scheduler type of TC-0 and TC-1 as Weighted for egress port 1/0/3. Specify the queue weight of TC-0 as 1 and specify the queue weight of TC-1 as 5.

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

Switch_A(config-if)#qos queue 0 mode wrr weight 1

Switch_A(config-if)#qos queue 1 mode wrr weight 5

Switch_A(config-if)#end

Switch_A#copy running-config startup-config

Verify the configurations

Verify the trust mode of the port:

Switch_A#show qos trust interface

Port	Trust Mode	LAG
Gi1/0/1	untrust	N/A
Gi1/0/2	untrust	N/A
Gi1/0/3	untrust	N/A
Gi1/0/4	untrust	N/A

...

Verify the port to 802.1p mappings:

Switch_A#show qos port-priority interface

Port	CoS Value	LAG
Gi1/0/1	CoS 1	N/A
Gi1/0/2	CoS 0	N/A
Gi1/0/3	CoS 0	N/A
Gi1/0/4	CoS 0	N/A

...

Verify the 802.1p to queue mappings:

```
Switch_A#show qos cos-map
-----+-----+-----+-----+-----+-----+-----+----+----
Tag |0     |1     |2     |3     |4     |5     |6    |7
-----+-----+-----+-----+-----+-----+-----+----+----
TC   |TC1  |TC0  |TC2  |TC4  |TC4 |TC5  |TC6 |TC7
-----+-----+-----+-----+-----+-----+-----+----+----
```

Verify the scheduler mode of the egress port:

```
Switch _A#show qos queue interface gigabitEthernet 1/0/3
Gi1/0/3----LAG: N/A
```

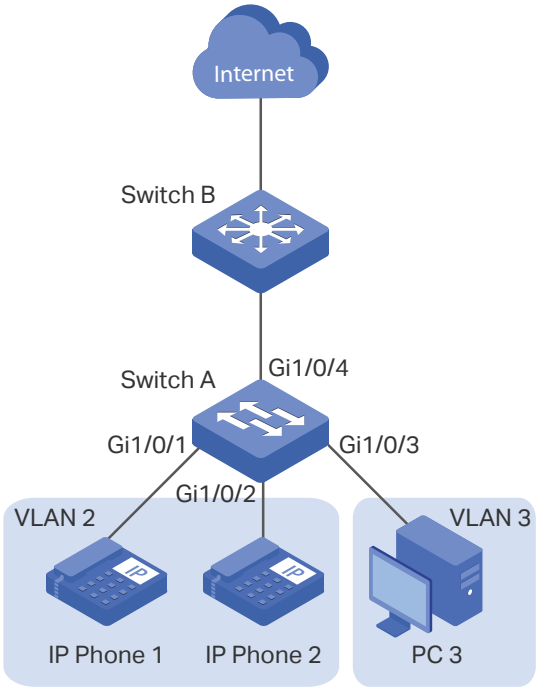
Queue	Schedule Mode	Weight	Min Bandwidth(%)
TC0	WRR	1	0%
TC1	WRR	5	0%
TC2	WRR	1	0%
TC3	WRR	1	0%
TC4	WRR	1	0%
TC5	WRR	1	0%
TC6	WRR	1	0%
TC7	WRR	1	0%

6.2 Example for Voice VLAN

6.2.1 Network Requirements

As shown below, the company plans to install IP phones in the office area. To ensure the good voice quality, IP phones and the computers will be connected to the different ports of the switch, and the voice traffic requires a higher priority than the data traffic.

Figure 6-5 Voice VLAN Application Topology



6.2.2 Configuration Scheme

To implement this requirement, you can configure Voice VLAN to ensure that the voice traffic can be transmitted in the same VLAN and the data traffic is transmitted in another VLAN. In addition, specify the priority to make the voice traffic can take precedence when the congestion occurs.

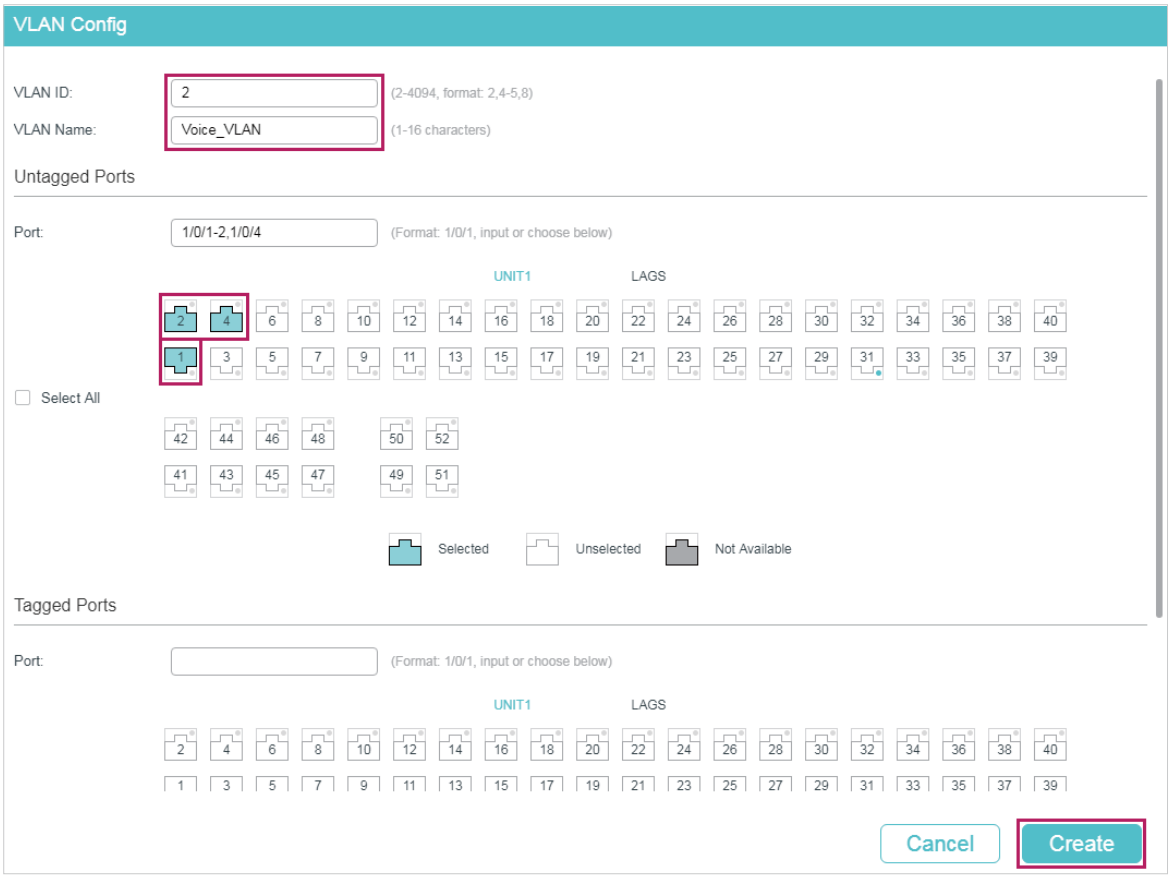
1) Configure 802.1Q VLAN for port 1/0/1, port 1/0/2. port 1/0/3 and port 1/0/4.
2) Configure Voice VLAN feature on port 1/0/1 and port 1/0/2.

Demonstrated with T1600G-52TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

6.2.3 Using the GUI

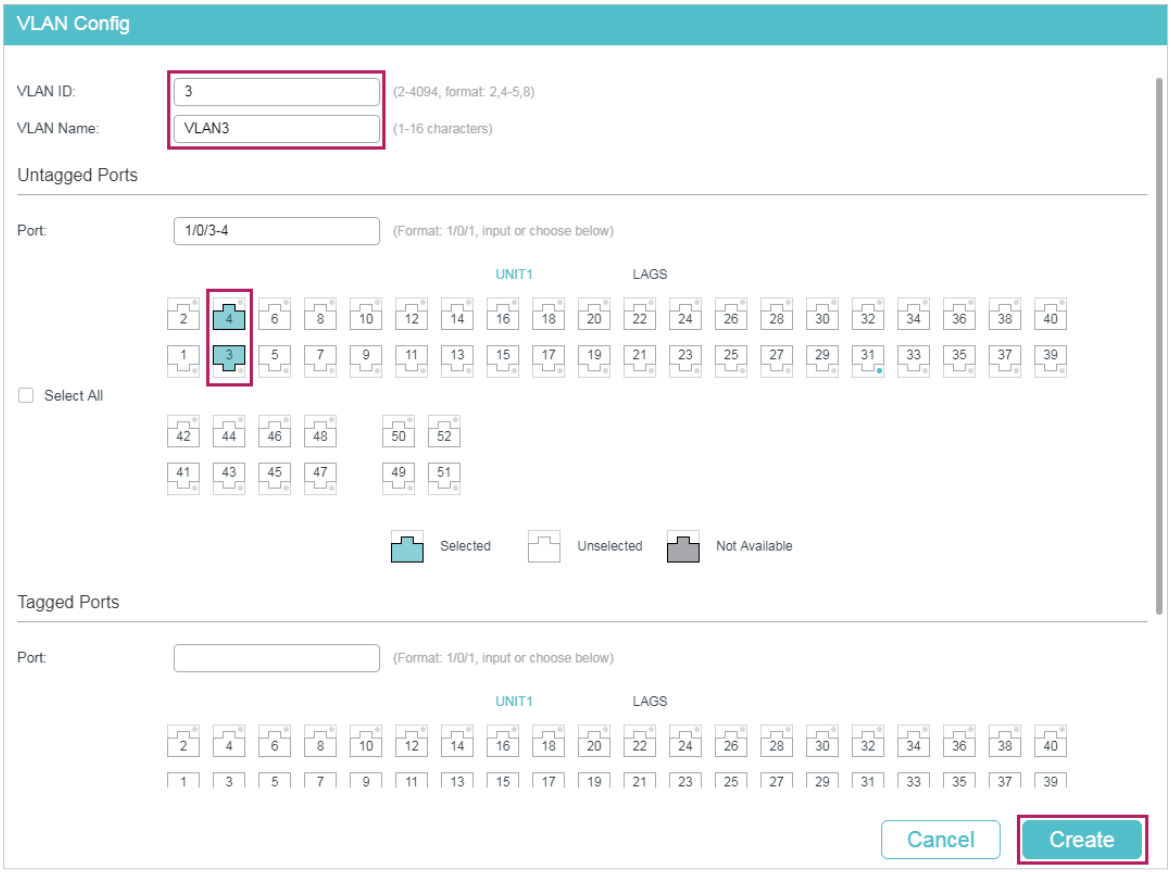
1) Choose the menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** and click Add to load the following page. Create VLAN 2 and add untagged port 1/0/1, port 1/0/2 and port 1/0/4 to VLAN 2. Click **Create**.

Figure 6-6 Configuring VLAN 2



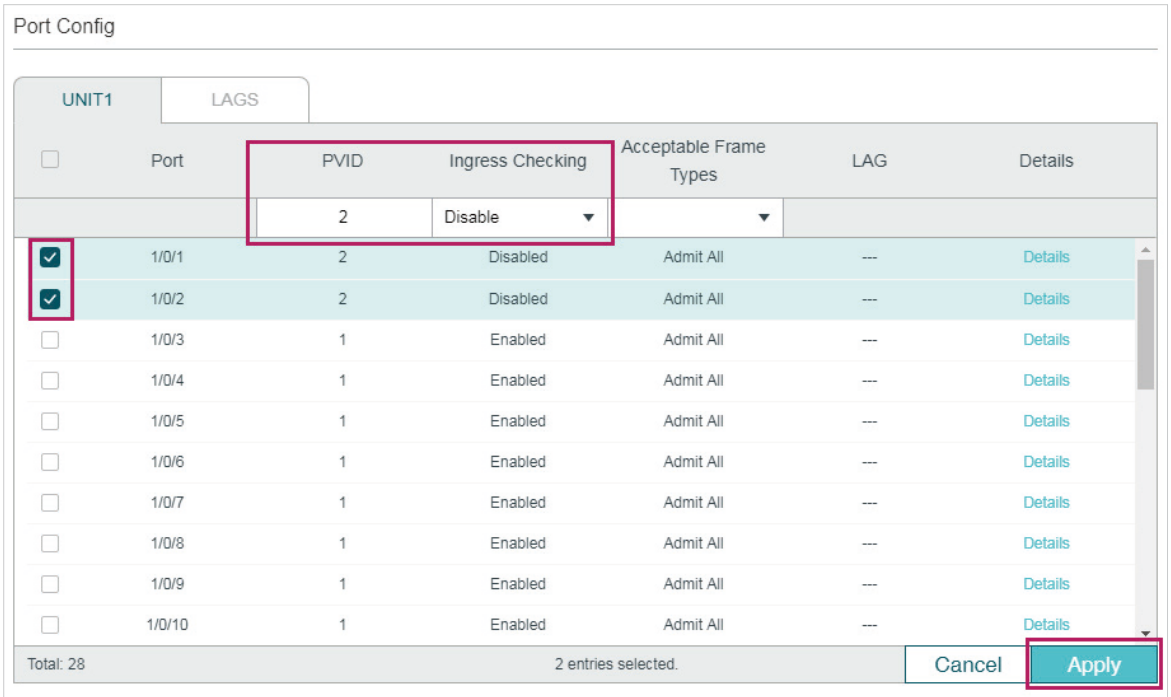
2) Click Add to load the following page. Create VLAN 3 and add untagged port 1/0/3 and port 1/0/4 to VLAN 3. Click **Create**.

Figure 6-7 Configuring VLAN 3



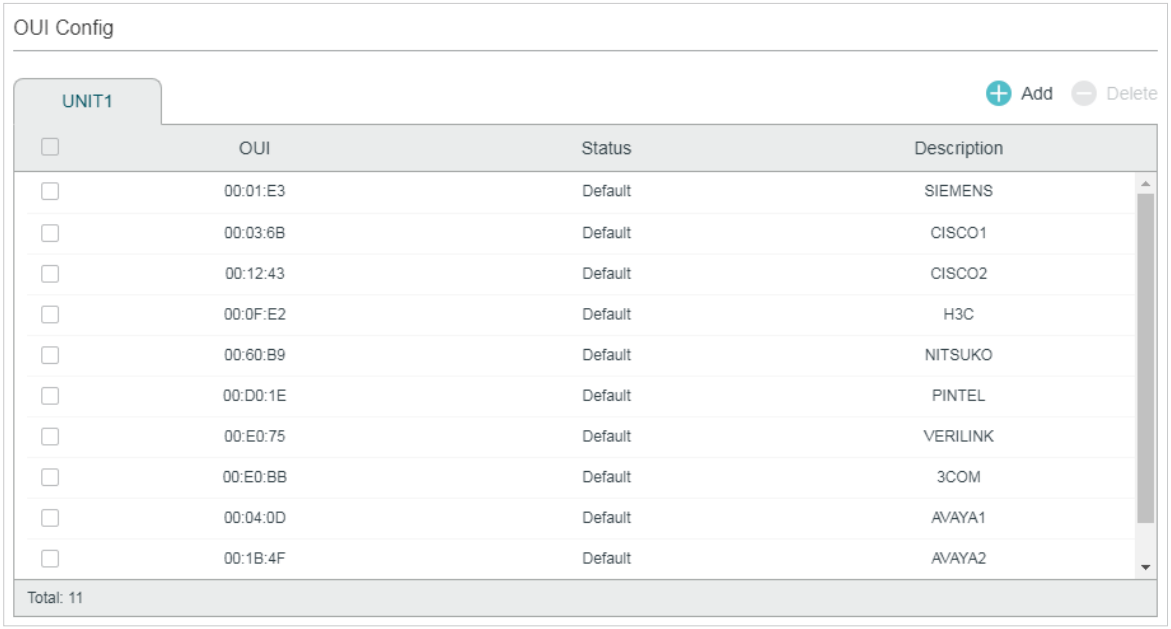
3) Choose the menu **L2 FEATURES > VLAN > 802.1Q VLAN > Port Config** to load the following page. Disable the Ingress Checking feature on port 1/0/1 and port 1/0/2 and specify the PVID as 2. Click **Apply**.

Figure 6-8 Specifying the Parameters of the Ports



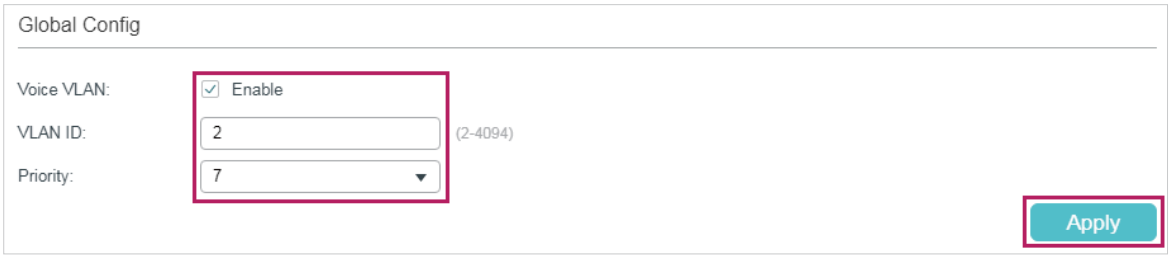
4) Choose the menu **QoS > Voice VLAN > OUI Config** to load the following page. Check the OUI table.

Figure 6-9 Checking the OUI Table



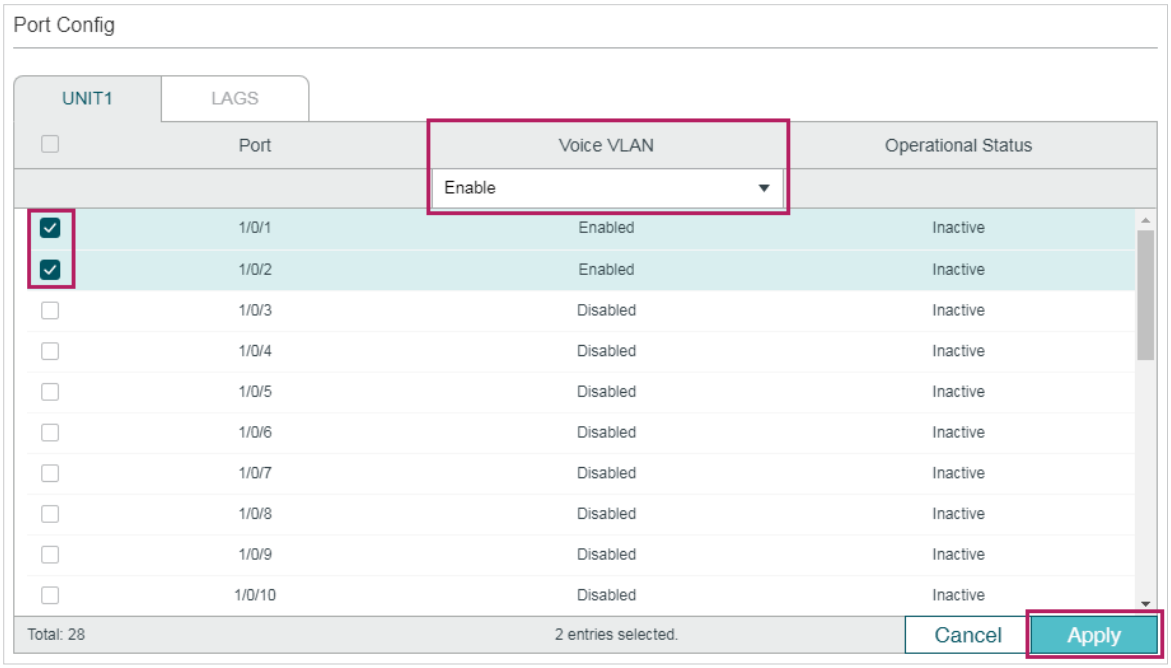
5) Choose the menu **QoS > Voice VLAN > Global Config** to load the following page. Enable Voice VLAN globally. Specify the VLAN ID as 2 and set the priority as 7. Click **Apply**.

Figure 6-10 Configuring Voice VLAN Globally



6) Choose the menu **QoS > Voice VLAN > Port Config** to load the following page. Enable Voice VLAN on port 1/0/1 and port 1/0/2. Click **Apply**.

Figure 6-11 Enabling Voice VLAN on Ports



7) Click Save to save the settings.

6.2.4 Using the CLI

1) Create VLAN 2 and add untagged port 1/0/1, port 1/0/2 and port 1/0/4 to VLAN 2.

```
Switch_A#configure
Switch_A(config)#vlan 2
Switch_A(config-vlan)#name VoiceVLAN
Switch_A(config-vlan)#exit
Switch_A(config)#interface gigabitEthernet 1/0/1
Switch_A(config-if)#switchport general allowed vlan 2 untagged
Switch_A(config-if)#exit
Switch_A(config)#interface gigabitEthernet 1/0/2
Switch_A(config-if)#switchport general allowed vlan 2 untagged
Switch_A(config-if)#exit
Switch_A(config)#interface gigabitEthernet 1/0/4
Switch_A(config-if)#switchport general allowed vlan 2 untagged
Switch_A(config-if)#exit
```

2) Create VLAN 3 and add untagged port 1/0/3 and port 1/0/4 to VLAN 3.

```
Switch_A(config)#vlan 3
```

Switch_A(config-vlan)#name VLAN3

Switch_A(config-vlan)#exit

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

Switch_A(config-if)#switchport general allowed vlan 3 untagged

Switch_A(config-if)#exit

Switch_A(config)#interface gigabitEthernet 1/0/4

Switch_A(config-if)#switchport general allowed vlan 3 untagged

Switch_A(config-if)#exit

3) Disable the Ingress Checking feature on port 1/0/1 and port 1/0/2 and specify the PVID as 2.

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

Switch_A(config-if)#no switchport check ingress

Switch_A(config-if)#switchport pvid 2

Switch_A(config-if)#exit

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

Switch_A(config-if)#no switchport check ingress

Switch_A(config-if)#switchport pvid 2

Switch_A(config-if)#exit

4) Check the OUI table.

Switch(config)#show voice vlan oui

00:01:E3	Default	SIEMENS
00:03:6B	Default	CISCO1
00:12:43	Default	CISCO2
00:0F:E2	Default	H3C
00:60:B9	Default	NITSUKO
00:D0:1E	Default	PINTEL
00:E0:75	Default	VERILINK
00:E0:BB	Default	3COM
00:04:0D	Default	AVAYA1
00:1B:4F	Default	AVAYA2
00:04:13	Default	SNOM

5) Enable Voice VLAN globally. Specify the VLAN ID as 2 and set the priority as 7.

```
Switch_A(config)#voice vlan 2
Switch_A(config)#voice vlan priority 7
```

6) Enable Voice VLAN on port 1/0/1 and port 1/0/2.

```
Switch_A(config)#interface gigabitEthernet 1/0/1
Switch_A(config-if)#voice vlan
Switch_A(config-if)#exit
Switch_A(config)#interface gigabitEthernet 1/0/2
Switch_A(config-if)#voice vlan
Switch_A(config-if)#end
Switch_A#copy running-config startup-config
```

Verify the configurations

Verify the basic VLAN configuration:

```
Switch_A(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,
                                  ...
                                  Gi1/0/49, Gi1/0/50, Gi1/0/51, Gi1/0/52
2      VoiceVLAN        active    Gi1/0/1, Gi1/0/2, Gi1/0/4
3      VLAN3            active    Gi1/0/3, Gi1/0/4
```

Verify the Voice VLAN configuration:

```
Switch_A(config)#show voice vlan interface
Voice VLAN ID            2
Priority                 7
Interface    Voice VLAN Mode   Operational Status   LAG
---------    ---------------   ------------------   ---
Gi1/0/1      enabled           Up                   N/A
```

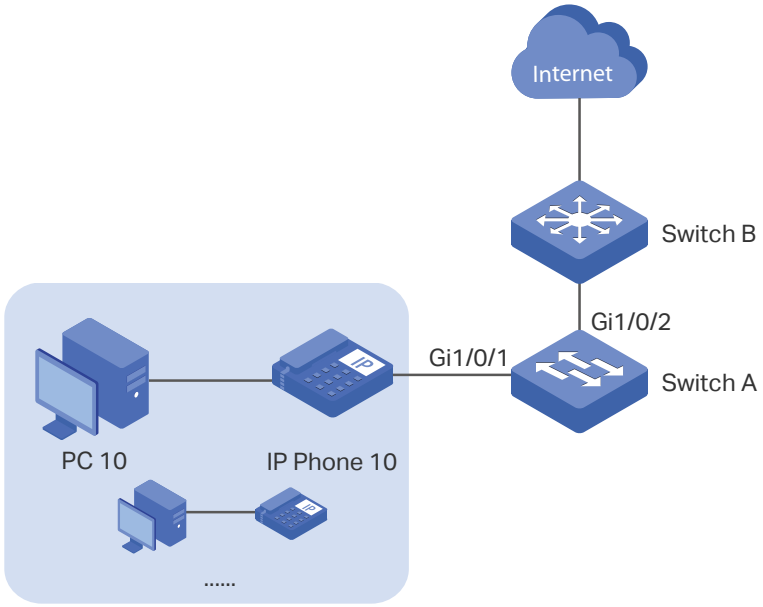
Gi1/0/2	enabled	Up	N/A
Gi1/0/3	disabled	Down	N/A
Gi1/0/4	disabled	Down	N/A
Gi1/0/5	disabled	Down	N/A
...			
Gi1/0/52	disabled	Down	N/A

6.3 Example for Auto VoIP

6.3.1 Network Requirements

As shown below, the company plans to install IP phones in the office area. IP phones share switch ports used by computers, because no more ports are available for IP phones. To ensure the good voice quality, the voice traffic requires a higher priority than the data traffic.

Figure 6-12 Auto VoIP Application Topology



6.3.2 Configuration Scheme

To optimize voice traffic, configure Auto VoIP and LLDP-MED to instruct IP Phones to send traffic with desired DSCP priority. Voice traffic is put in the desired queue and data traffic is put in other queues according to the Class of Service configurations. Make sure that the voice traffic can take precedence when congestion occurs.

1) Enable the Auto VoIP feature and configure the DSCP value of ports.
2) Configure Class of Service.

3) Enable LLDP-MED and configure the corresponding parameters.

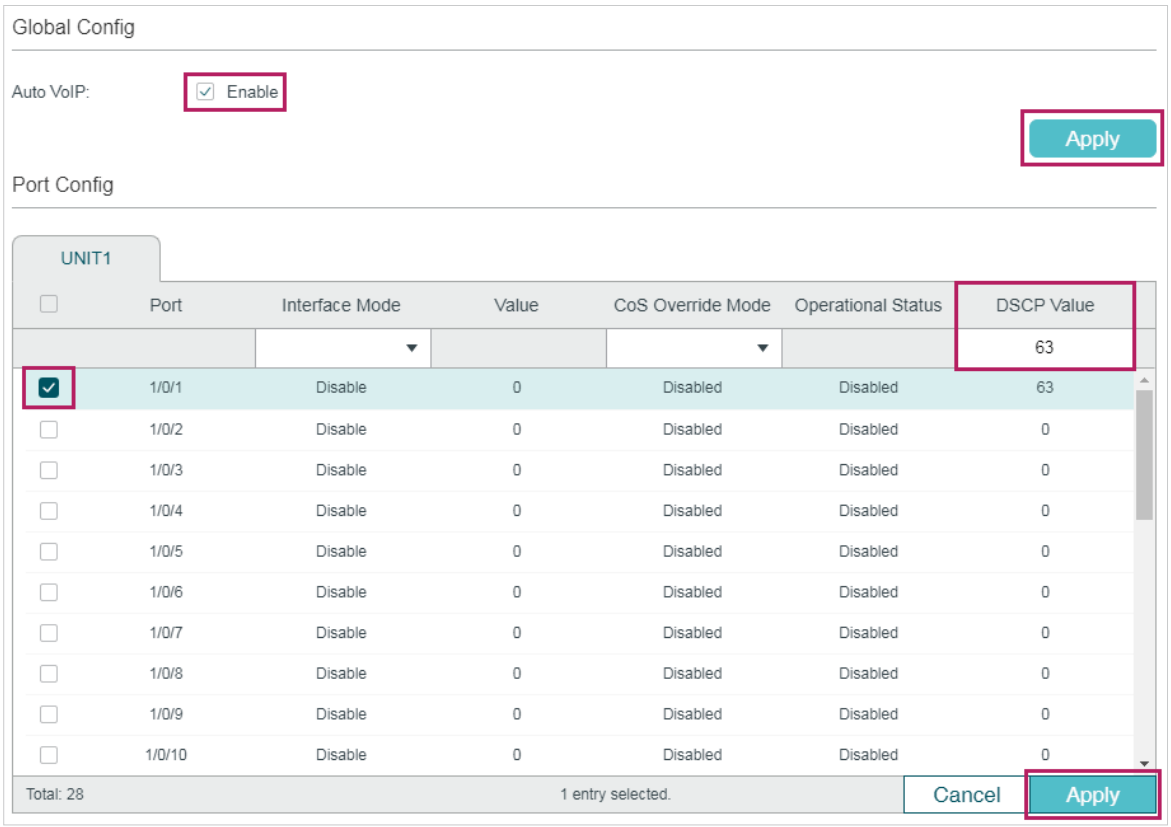
Demonstrated with T1600G-52TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

6.3.3 Using the GUI

Auto VoIP configurations for port1/0/1 and other ports connected to the IP phone are the same, the following configuration procedures take port 1/0/1 as example.

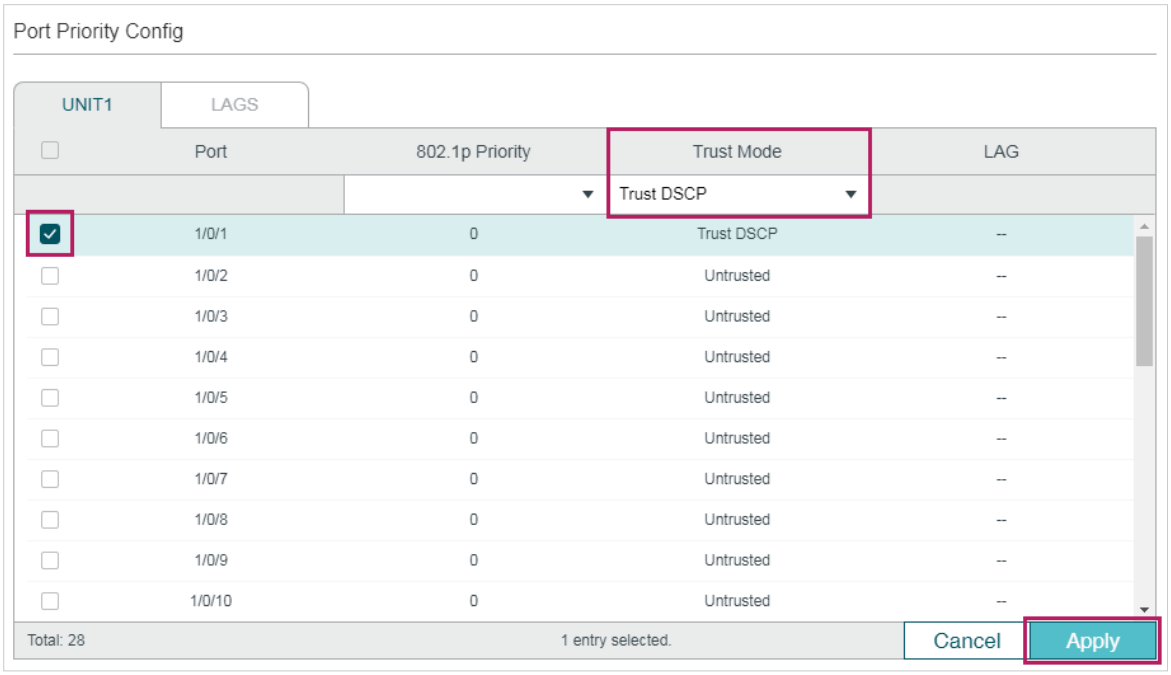
1) Choose the menu **QoS > Auto VoIP** to load the following page. Enable Auto VoIP globally and specify the DSCP value of port 1/0/1 as 63. Click **Apply**.

Figure 6-13 Configuring Auto VoIP



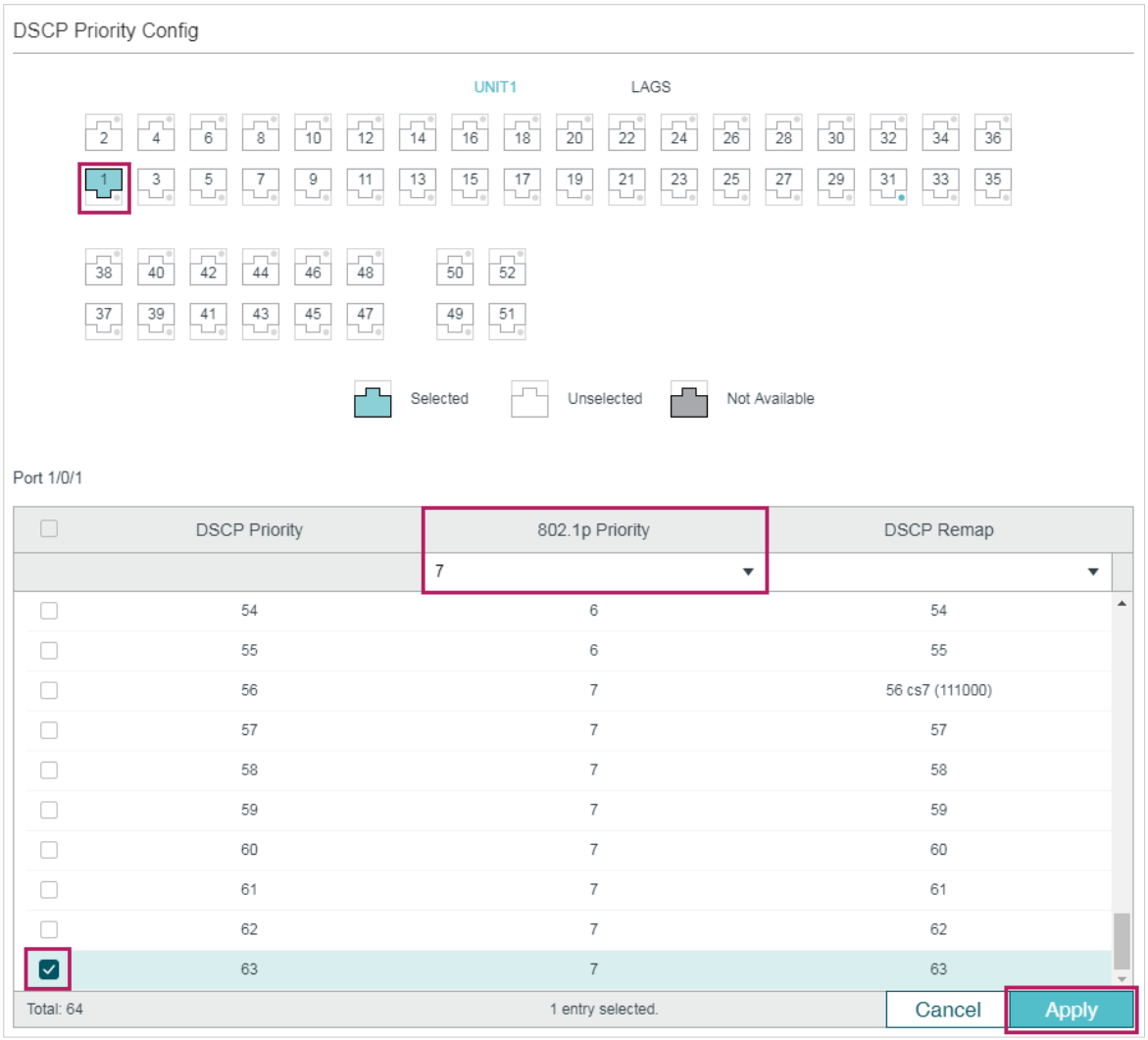
2) Choose the menu **QoS > Class of Service > Port Priority** to load the following page. Set the trust mode of port 1/0/1 as trust DSCP. Click **Apply**.

Figure 6-14 Configuring Port Priority



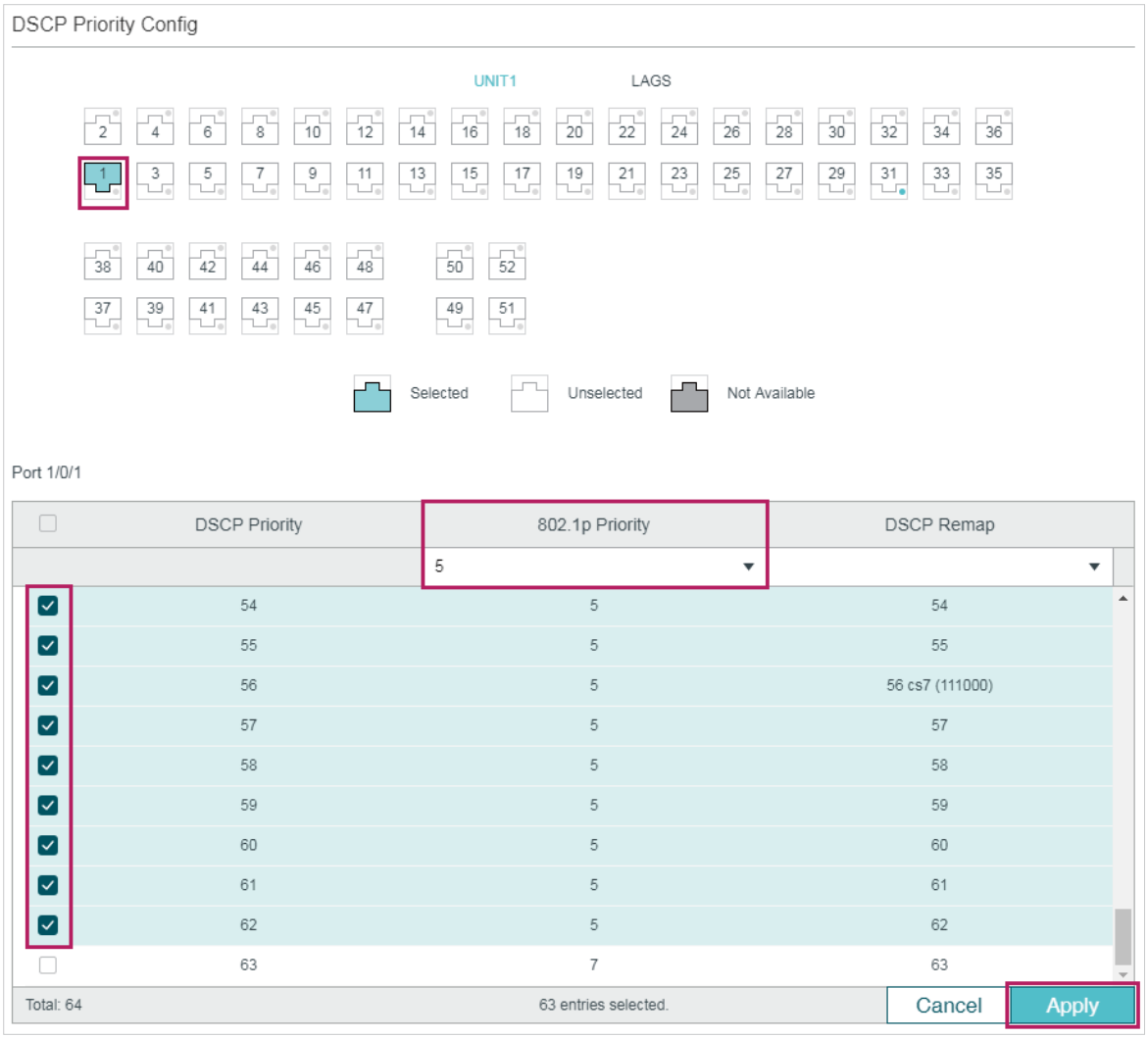
3) Choose the menu **QoS > Class of Service > DSCP Priority** to load the following page. Select port 1/0/1 and specify the 802.1p priority as 7 for DSCP priority 63. Click **Apply**.

Figure 6-15 Specifying the 802.1p priority for DSCP priority 63



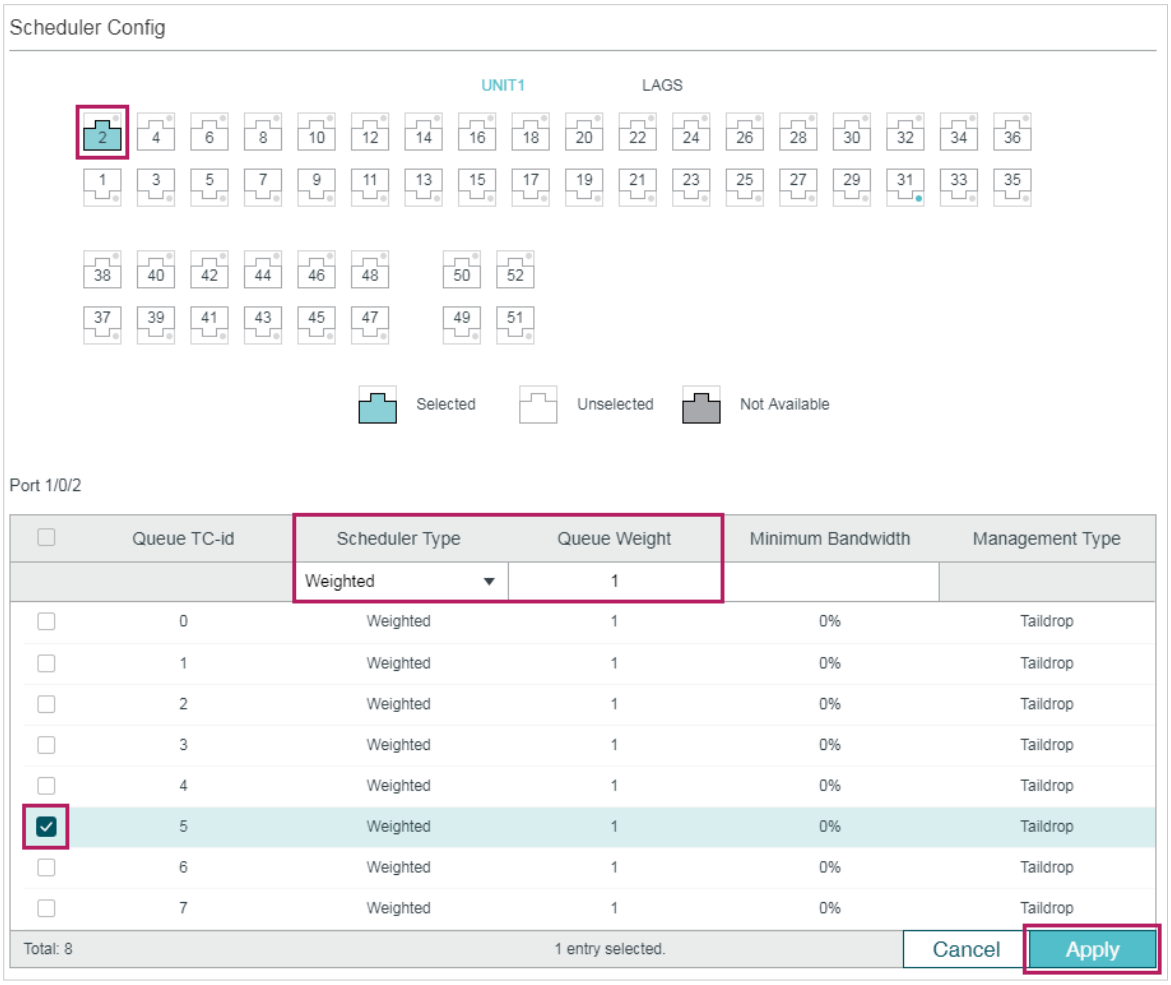
4) Select port 1/0/1 and specify the 802.1p priority as 5 for other DSCP priorities. Click **Apply**.

Figure 6-16 Specifying the 802.1p priority for Other DSCP priorities



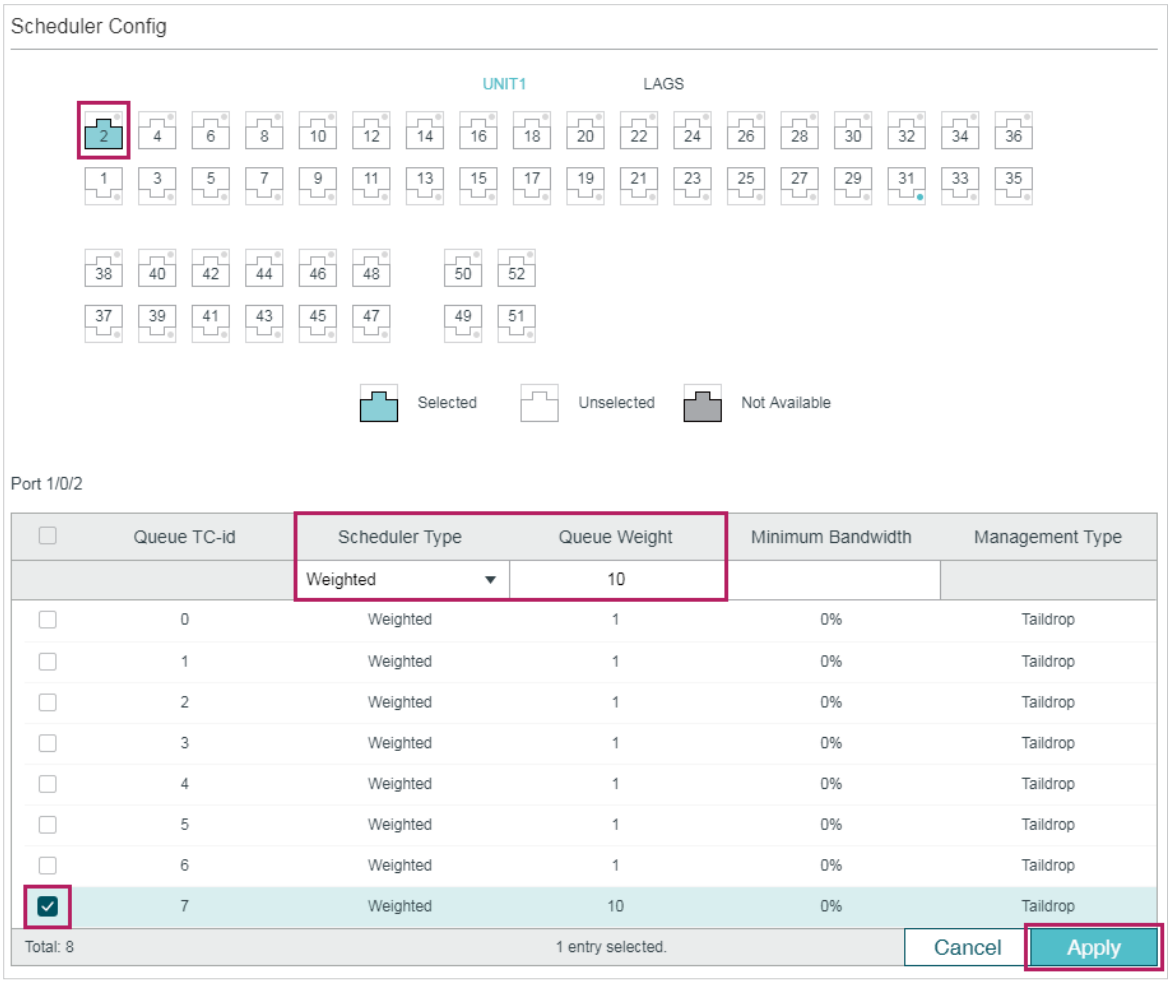
5) Choose the menu **QoS > Class of Service > Scheduler Settings** to load the following page. Select port 1/0/2. Set the scheduler mode as weighted and specify the queue weight as 1 for TC-5. Click **Apply**.

Figure 6-17 Configuring the TC-5 for the Port



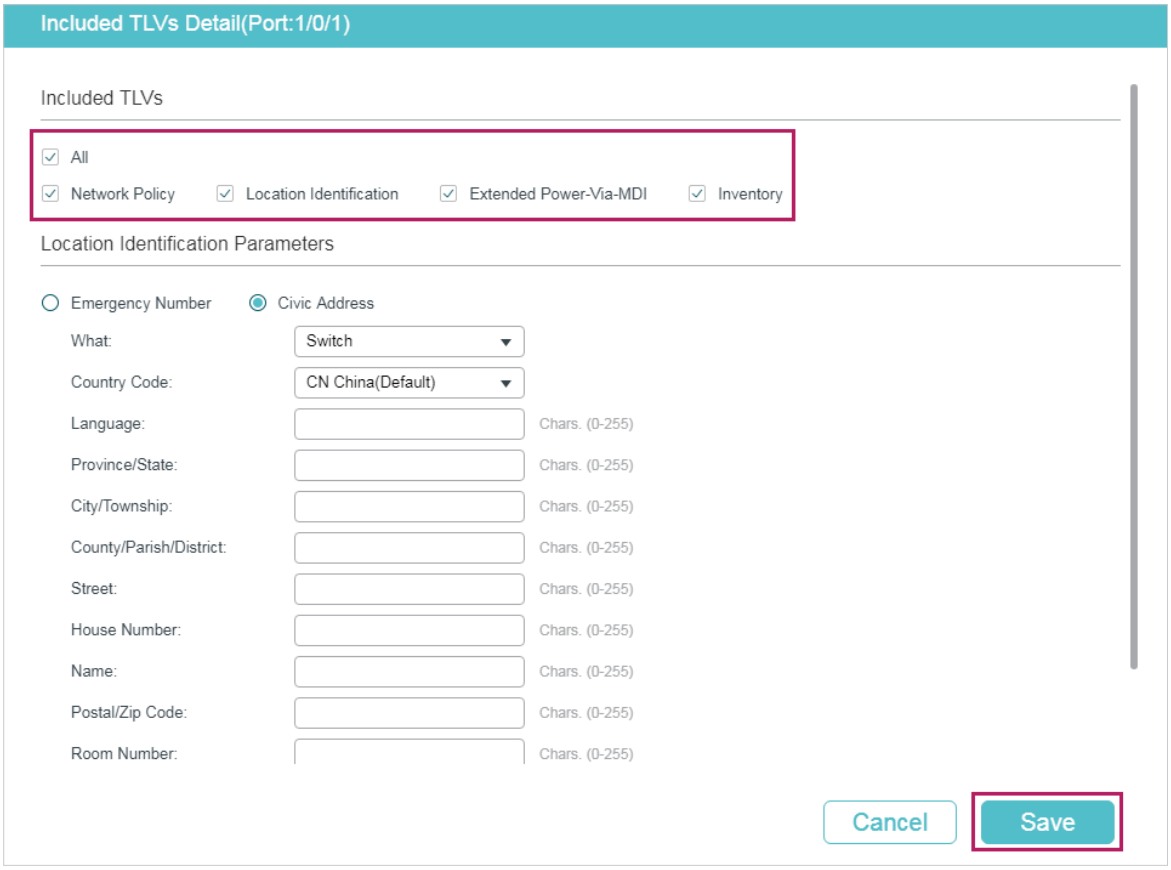
6) Select port 1/0/2. Set the scheduler mode as weighted and specify the queue weight as 10 for TC-7. Click **Apply**.

Figure 6-18 Configuring the TC-7 for the Port



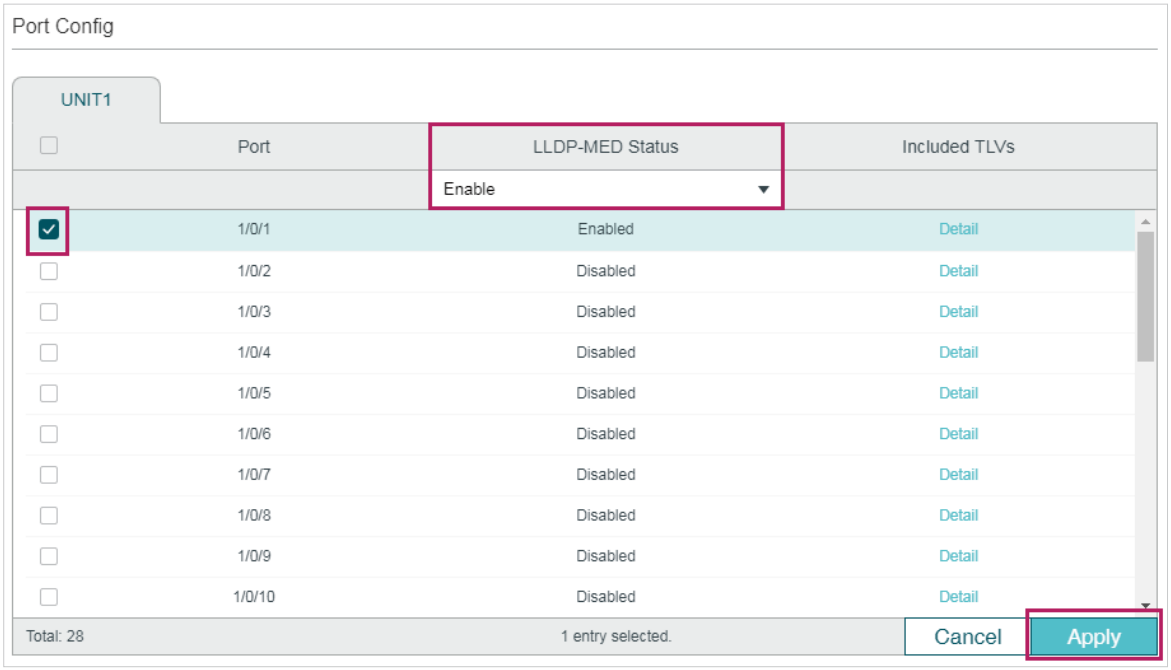
7) Choose the menu **L2 FEATURES > LLDP > LLDP-MED Config > Port Config** click Detail to of port1/0/1 to load the following page. Check the boxes of all the TLVs. Click **Save**.

Figure 6-19 Configuring the TLVs



8) Choose the menu **L2 FEATURES > LLDP > LLDP-MED Config > Port Config** to load the following page. Enable LLDP-MED on port 1/0/1. Click **Apply**.

Figure 6-20 Enabling LLDP-MED on the Port



9) Click Save to save the settings.

6.3.4 Using the CLI

1) Enable Auto VoIP globally and specify the DSCP value of port 1/0/1 as 63.

   Switch_A#configure

   Switch_A(config)#auto-voip

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

   Switch_A(config-if)#auto-voip dscp 63

   Switch_A(config-if)#exit

2) Set the trust mode of port 1/0/1 as trust DSCP. Specify the 802.1p priority as 7 for DSCP priority 63 and specify 802.1p priority as 5 for other DSCP priorities.

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

   Switch_A(config-if)#qos trust mode dscp

   Switch_A(config-if)#qos dscp-map 63 7

   Switch_A(config-if)#qos dscp-map 0-62 5

   Switch_A(config-if)#exit

3) On port 1/0/1, set the scheduler mode as weighted and specify the queue weight as 1 for TC-5. Set the scheduler mode as weighted and specify the queue weight as 10 for TC-7.

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

   Switch_A(config-if)#qos queue 5 mode wrr weight 1

   Switch_A(config-if)#qos queue 7 mode wrr weight 10

   Switch_A(config-if)#exit

4) Enable LLDP-MED on port 1/0/1 and select all the TLVs to be included in outgoing LLDPDU.

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

   Switch_A(config-if)#lldp med-status

   Switch_A(config-if)#lldp med-tlv-select all

   Switch_A(config-if)#end

   Switch_A#copy running-config startup-config

Verify the configurations

Verify the configuration of Auto VoIP:

```
Switch_A(config)#show auto-voip
Administrative Mode:    Enabled
```

Verify the Auto VoIP configuration of ports:

```
Switch_A(config)#show auto-voip interface
Interface.Gi1/0/1
Auto-VoIP Interface Mode.          Disabled
Auto-VoIP COS Override.            False
Auto-VoIP DSCP Value.              63
Auto-VoIP Port Status.             Disabled

Interface.Gi1/0/2
Auto-VoIP Interface Mode.          Disabled
Auto-VoIP COS Override.            False
Auto-VoIP DSCP Value.              0
Auto-VoIP Port Status.             Disabled

Interface.Gi1/0/3
Auto-VoIP Interface Mode.          Disabled
Auto-VoIP COS Override.            False
Auto-VoIP DSCP Value.              0
Auto-VoIP Port Status.             Disabled
...
```

Verify the configuration of Class of Service:

```
Switch_A(config)#show qos trust interface gigabitEthernet 1/0/1
Port        Trust Mode      LAG
--------    ---------       ------
Gi1/0/1     trust DSCP      N/A
```

```
Switch_A(config)#show qos cos-map
-----+-----+-----+-----+-----+-----+-----+----+----
Tag  |0    |1    |2    |3    |4    |5    |6   |7
-----+-----+-----+-----+-----+-----+-----+----+----
TC   |TC1  |TC0  |TC2  |TC3  |TC4  |TC5  |TC6 |TC7
-----+-----+-----+-----+-----+-----+-----+----+----
Switch_A(config)#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  5   5   5   5   5   5   5   5
                   ---- ---- ---- ---- ---- ---- ---- ----
DSCP:              8   9   10  11  12  13  14  15
DSCP to 802.1P  5   5   5   5   5   5   5   5
                   ---- ---- ---- ---- ---- ---- ---- ----
DSCP:              16  17  18  19  20  21  22  23
DSCP to 802.1P  5   5   5   5   5   5   5   5
                   ---- ---- ---- ---- ---- ---- ---- ----
DSCP:              24  25  26  27  28  29  30  31
DSCP to 802.1P  5   5   5   5   5   5   5   5
                   ---- ---- ---- ---- ---- ---- ---- ----
DSCP:              32  33  34  35  36  37  38  39
DSCP to 802.1P  5   5   5   5   5   5   5   5
                   ---- ---- ---- ---- ---- ---- ---- ----
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  5   5   5   5   5   5   5   5
                   ---- ---- ---- ---- ---- ---- ---- ----
```

DSCP:	56	57	58	59	60	61	62	63
DSCP to 802.1P	5	5	5	5	5	5	5	7

Verify the configuration of LLDP-MED:

Switch_A(config)#show lldp interface

LLDP interface config:

gigabitEthernet 1/0/1:

Admin Status:	TxRx
SNMP Trap:	Disabled
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

...

7 Appendix: Default Parameters

Default settings of Class of Service are listed in the following tables.

Table 7-1 Default Settings of Port Priority Configuration

Parameter	Default Setting
802.1P Priority	0
Trust Mode	Untrusted

Table 7-2 Default Settings of 802.1p to Queue Mapping

802.1p Priority	Queues (8)
0	TC1
1	TC0
2	TC2
3	TC3
4	TC4
5	TC5
6	TC6
7	TC7

Table 7-3 Default Settings of 802.1p Remap Configuration

Original 802.1p Priority	New 802.1p Priority
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Table 7-4 Default Settings of DSCP to 802.1p Mapping

DSCP	802.1p Priority
0 to 7	0
8 to 15	1

DSCP	802.1p Priority
16 to 23	2
24 to 31	3
32 to 39	4
40 to 47	5
48 to 55	6
56 to 63	7

Table 7-5 Default Settings of DSCP Remap Configuration

Original DSCP	New DSCP	Original DSCP	New DSCP	Original DSCP	New DSCP
0	0 be (000000)	22	22 af23 (010110)	44	44
1	1	23	23	45	45
2	2	24	24 cs3 (011000)	46	46 ef (101110)
3	3	25	25	47	47
4	4	26	26 af31 (011010)	48	48 cs6 (110000)
5	5	27	27	49	49
6	6	28	28 af32 (011100)	50	50
7	7	29	29	51	51
8	8 cs1 (001000)	30	30 af33 (011110)	52	52
9	9	31	31	53	53
10	10 af11 (001010)	32	32 cs4 (100000)	54	54
11	11	33	33	55	55
12	12 af12 (001100)	34	34 af41 (100010)	56	56 cs7 (111000)
13	13	35	35	57	57
14	14 af13 (001110)	36	36 af42 (100100)	58	58
15	15	37	37	59	59
16	16 cs2 (010000)	38	38 af43 (100110)	60	60
17	17	39	39	61	61
18	18 af21 (010010)	40	40 cs5 (101000)	62	62
19	19	41	41	63	63
20	20 af22 (010100)	42	42		
21	21	43	43		

Table 7-6 Default Settings of Scheduler Settings Configuration

Parameter	Default Setting
Scheduler Type	Weighted
Queue Weight	1
Minimum Bandwidth	0%
Management Type	Taildrop

Default settings of Class of Service are listed in the following tables.

Table 7-7 Default Settings of Bandwidth Control

Parameter	Default Setting
Ingress Rate (0-1,000,000Kbps)	0
Egress Rate (0-1,000,000Kbps)	0

Table 7-8 Default Settings of Storm Control

Parameter	Default Setting
Rate Mode	kbps
Broadcast Threshold (0-1,000,000)	0
Multicast Threshold (0-1,000,000)	0
UL-Frame Threshold (0-1,000,000)	0
Action	Drop
Recover Time	0

Default settings of Voice VLAN are listed in the following tables.

Table 7-9 Default Settings of Global Configuration

Parameter	Default Setting
Voice VLAN	Disabled
VLAN ID	None
Priority	7

Table 7-10 Default Settings of Port Configuration

Parameter	Default Setting
Voice VLAN	Disabled

Table 7-11 Default Settings of OUI Table

OUI	Status	Description
00:01:E3	Default	SIEMENS
00:03:6B	Default	CISCO1
00:12:43	Default	CISCO2
00:0F:E2	Default	H3C
00:60:B9	Default	NITSUKO
00:D0:1E	Default	PINTEL
00:E0:75	Default	VERILINK
00:E0:BB	Default	3COM
00:04:0D	Default	AVAYA1
00:1B:4F	Default	AVAYA2
00:04:13	Default	SNOM

Default settings of Auto VoIP are listed in the following tables.

Table 7-12 Default Settings of Auto VoIP

Parameter	Default Setting
Interface Mode	Disabled
Value	None
Cos Override Mode	Disabled
DSCP Value	0

Part 18

Configuring Access Security

CHAPTERS

1. Access Security
2. Access Security Configurations
3. Appendix: Default Parameters

1 Access Security

1.1 Overview

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

1.2 Supported Features

Access Control

This function is used to control the users' access to the switch based on IP address, MAC address or port.

HTTP

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

HTTPS

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

SSH

This 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.

Telnet

This function is based on the Telnet protocol subjected to TCP/IP protocol. Through Telnet, users can log on to the switch remotely.

2 Access Security Configurations

With access security configurations, you can:

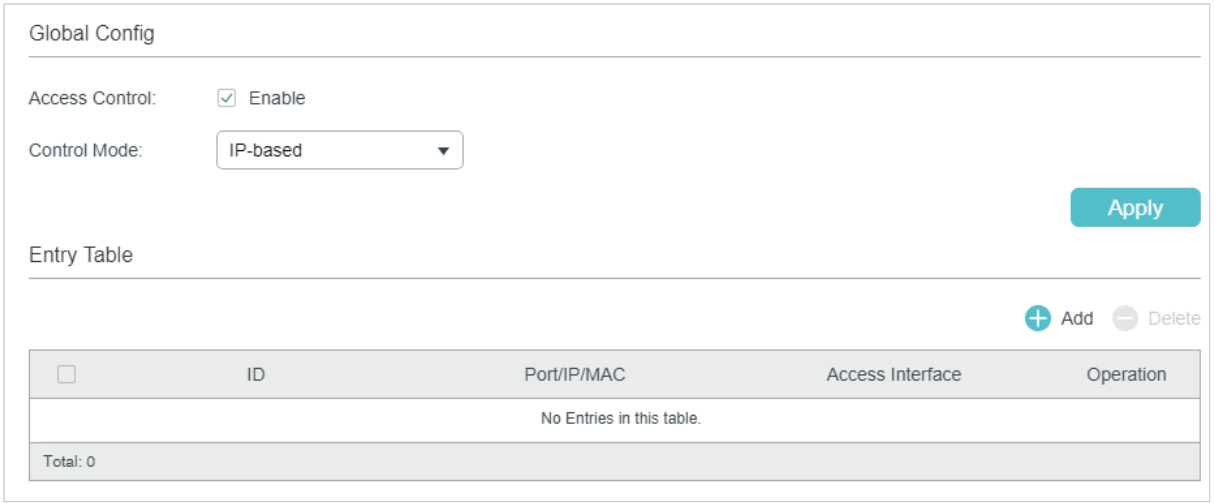
- Configure the Access Control feature
- Configure the HTTP feature
- Configure the HTTPS feature
- Configure the SSH feature
- Configure the Telnet function

2.1 Using the GUI

2.1.1 Configuring the Access Control Feature

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

Figure 2-1 Configuring the Access Control



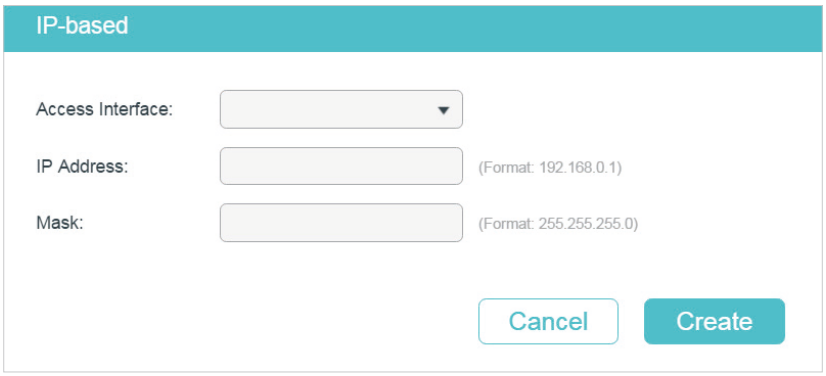
1) In the **Global Config** section, enable Access Control, select one control mode and click **Apply**.

Control Mode	Select the control mode for users to log in to the web management page. **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.

2) In the **Entry Table** section, click Add to add an Access Control entry.

When the **IP-based** mode is selected, the following window will pop up.

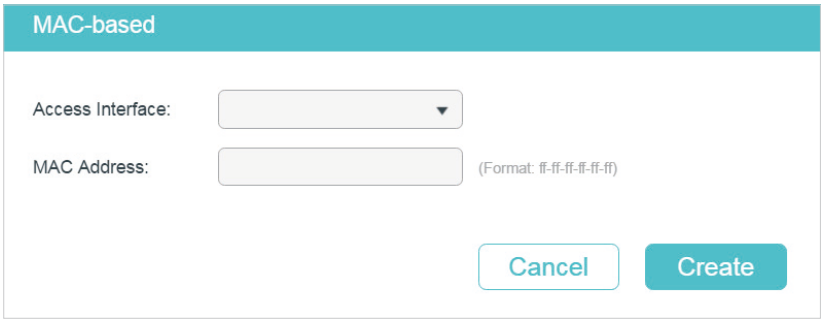
Figure 2-2 Configuring Access Control Entry-IP Based



Access Interface	Select the interface to control the methods for users' accessing. **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	Enter the IP address and mask to specify an IP range. Only the users within this IP range can access the switch.

When the **MAC-based** mode is selected, the following window will pop up.

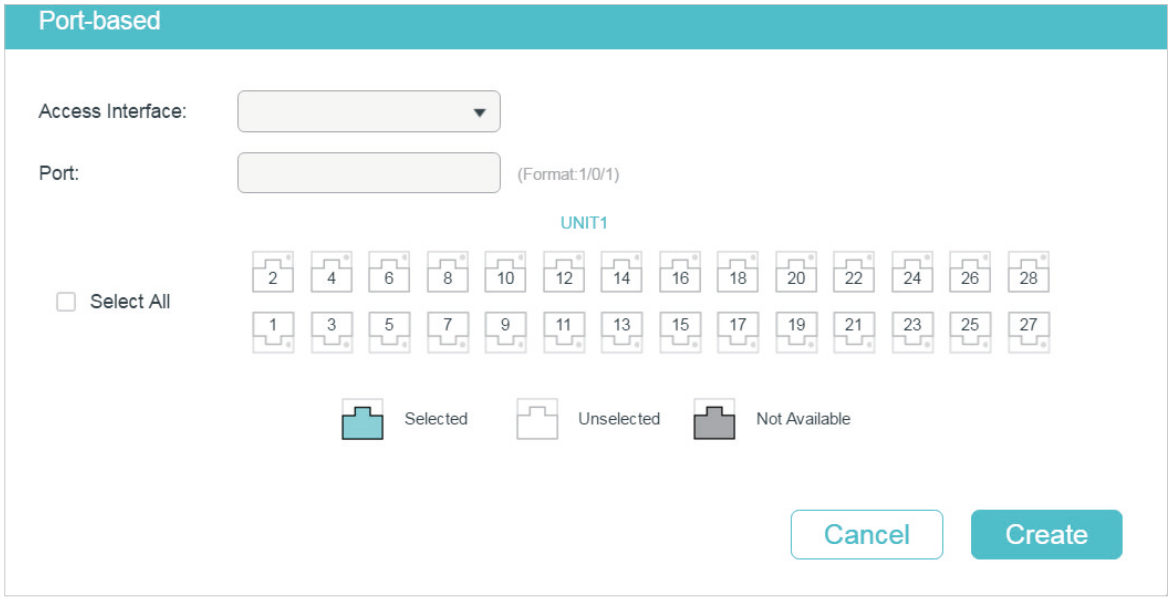
Figure 2-3 Configuring Access Control Entry-MAC Based



Access Interface	Select the interface to control the methods for users' accessing. **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.
MAC Address	Specify the MAC address. Only the users with the correct MAC address can access the switch.

When the **Port-based** mode is selected, the following window will pop up.

Figure 2-4 Configuring Access Control Entry-Port Based



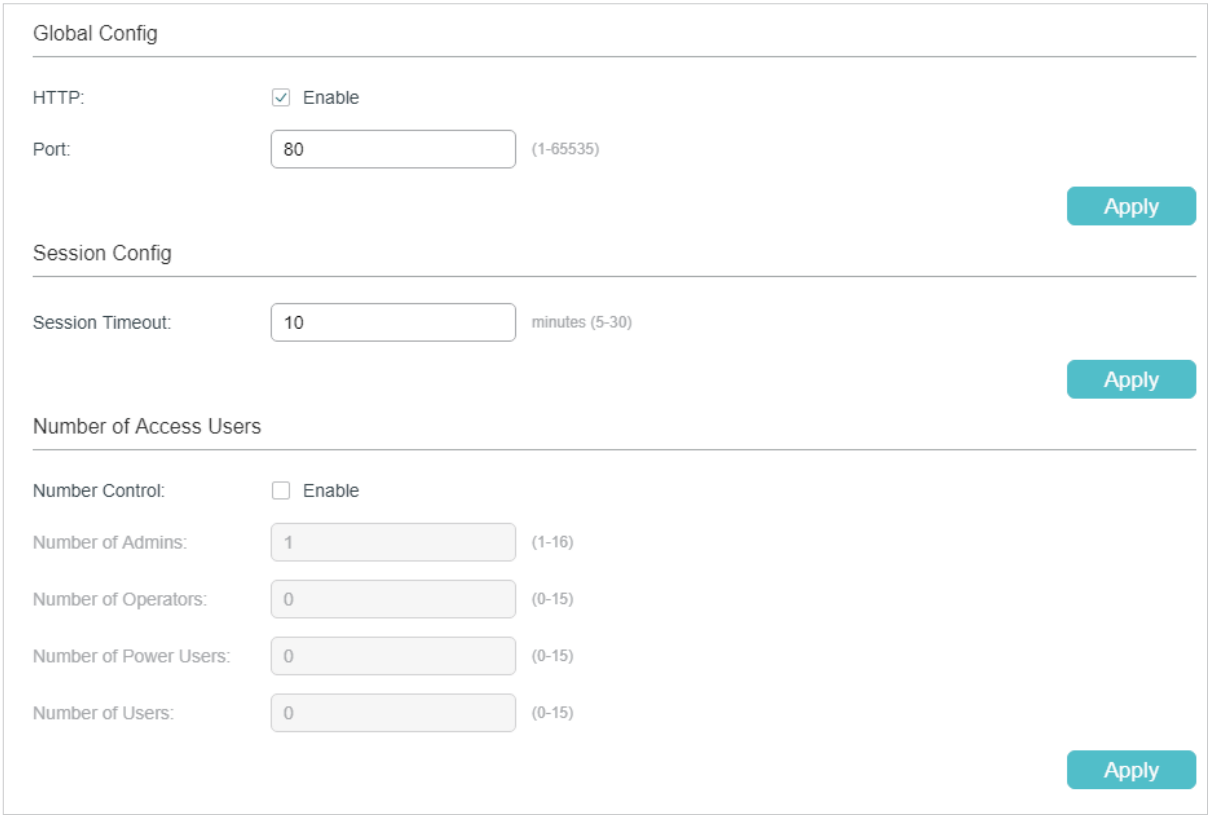
Access Interface	Select the interface to control the methods for users' accessing. **SNMP**: A function to manage the network devices via NMS. **Telnet**: A connection type for users to remote login. **SSH**: A connection type based on SSH protocol. **HTTP**: A connection type based on HTTP protocol. **HTTPS**: A connection type based on SSL protocol. **Ping**: A communication protocol to test the connection of the network.
Port	Select one or more ports to configure. Only the users connected to these ports are allowed to access the switch.

3) Click **Create**. Then you can view the created entries in the **Entry Table**.

2.1.2 Configuring the HTTP Function

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

Figure 2-5 Configuring the HTTP Function



1) In the **Global Control** section, enable HTTP function, specify the port using for HTTP, 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.
Port	Specify the port number for HTTP service.

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 **Number of Access Users** section, enable Number Control function, specify the following parameters and click **Apply**.

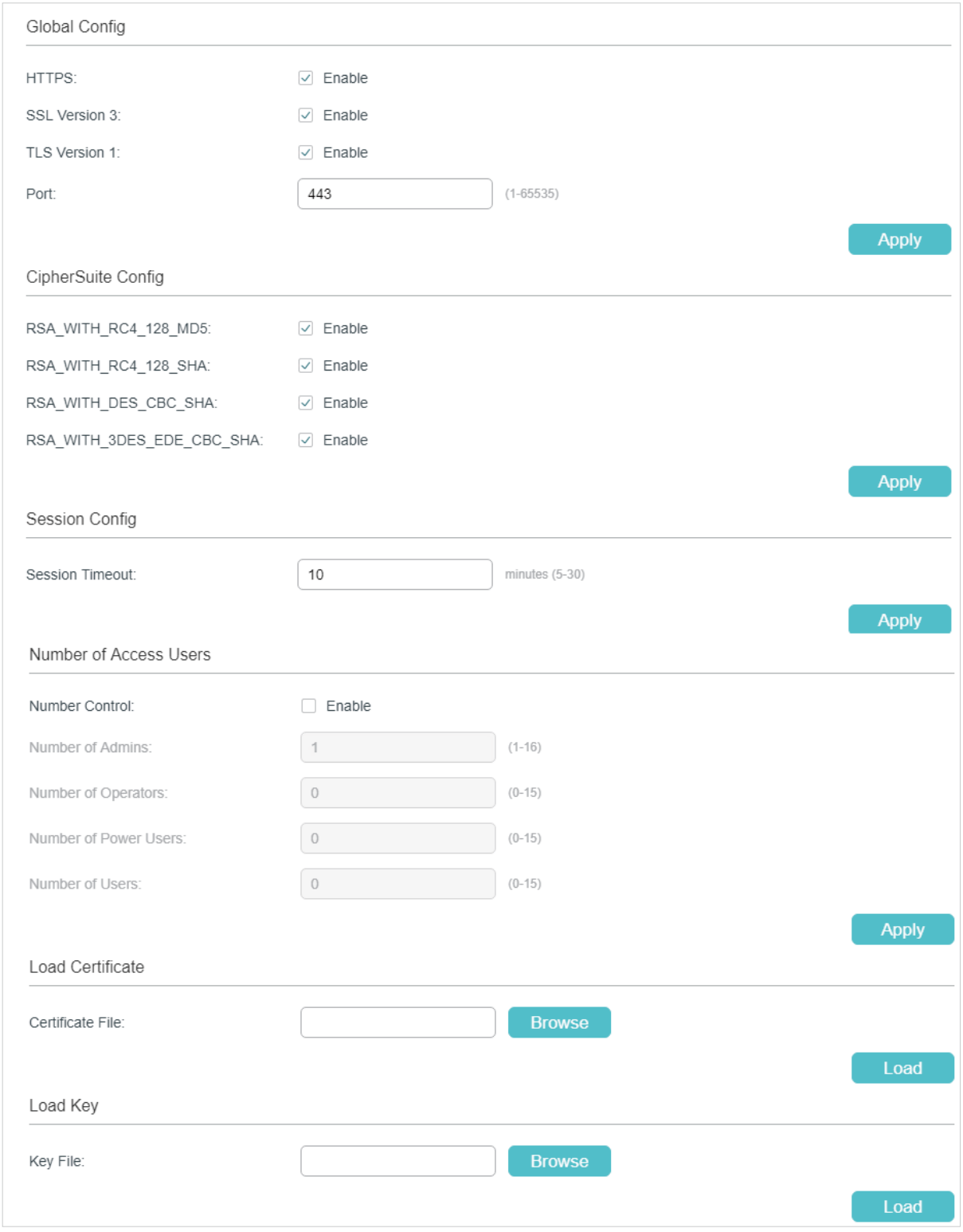
Number Control	Enable or disable Number Control. With this option enabled, you can control the number of the users logging on to the web management page at the same time. The total number of users should be no more than 16.
Number of Admins	Specify the maximum number of users whose access level is Admin.

Number of Operators	Specify the maximum number of users whose access level is Operator.
Number of Power Users	Specify the maximum number of users whose access level is Power User.
Number of Users	Specify the maximum number of users whose access level is User.

2.1.3 Configuring the HTTPS Function

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

Figure 2-6 Configuring the HTTPS Function



1) In the **Global Config** section, enable HTTPS function, select the protocol the switch supports and specify the port using for HTTPS. Click **Apply**.

HTTPS	Enable or disable 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	Enable or disable SSL Version 3 protocol on the switch. SSL is a transport protocol. It can provide server authentication, encryption and message integrity to allow secure HTTP connection.
TLS Version 1	Enable or disable TLS Version 1 protocol on the switch. 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 **Number of Access Users** section, enable Number Control function, specify the following parameters and click **Apply**.

Number Control	Enable or disable Number Control. With this option enabled, you can 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.
Number of Admins	Specify the maximum number of users whose access level is Admin.
Number of Operators	Specify the maximum number of users whose access level is Operator.
Number of Power Users	Specify the maximum number of users whose access level is Power User.
Number of Users	Specify the maximum number of users whose access level is User.

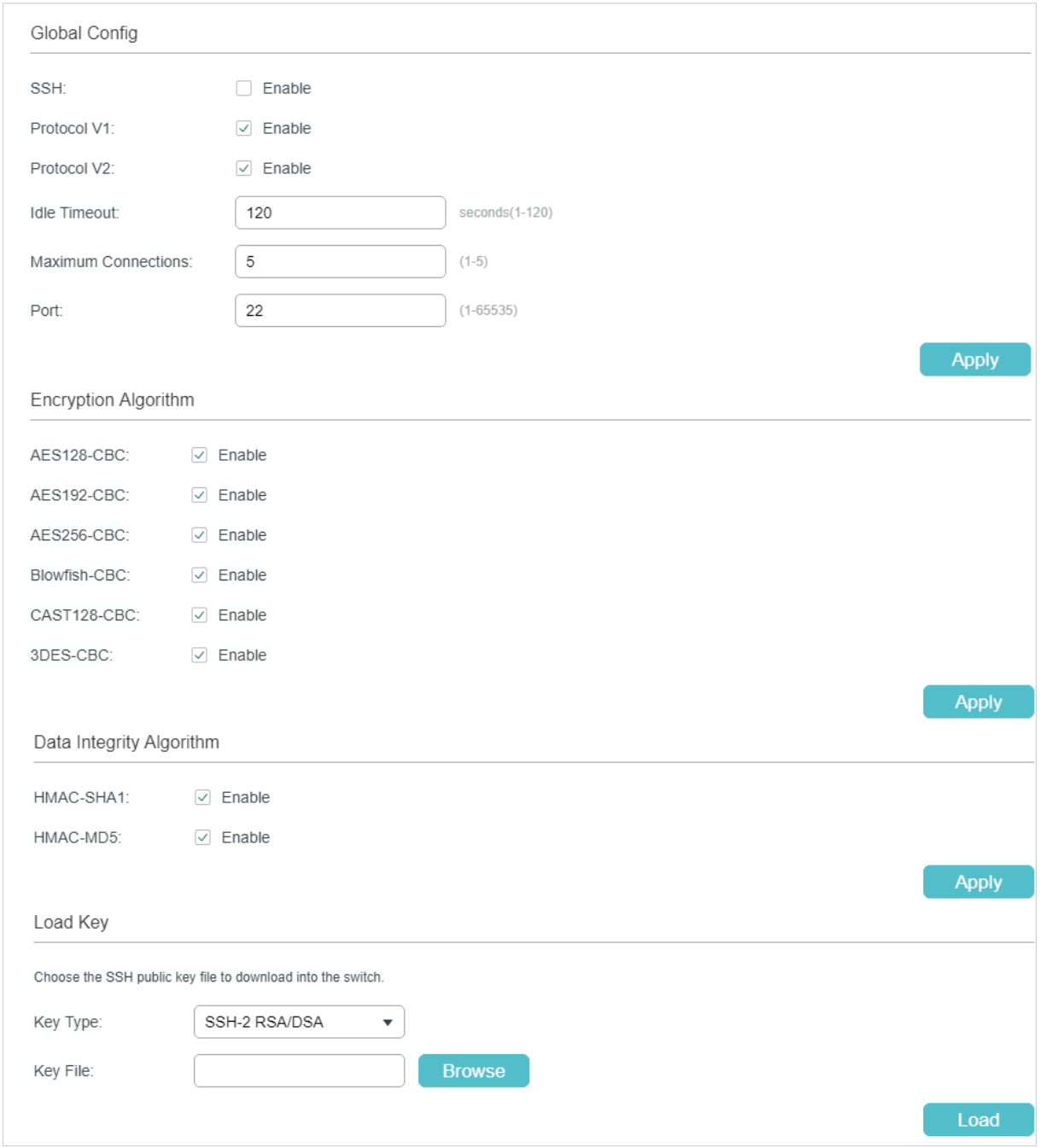
5) In the **Load Certificate** and **Load Key** section, download the certificate and key.

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.

2.1.4 Configuring the SSH Feature

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

Figure 2-7 Configuring the SSH Feature



1) In the **Global Config** section, select **Enable** to enable SSH function and specify following 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.
Maximum Connections	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.
Port	Specify the port using for SSH.

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

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

4) In **Import Key File** section, select key type from the drop-down list and click **Browse** to download the desired key file.

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.

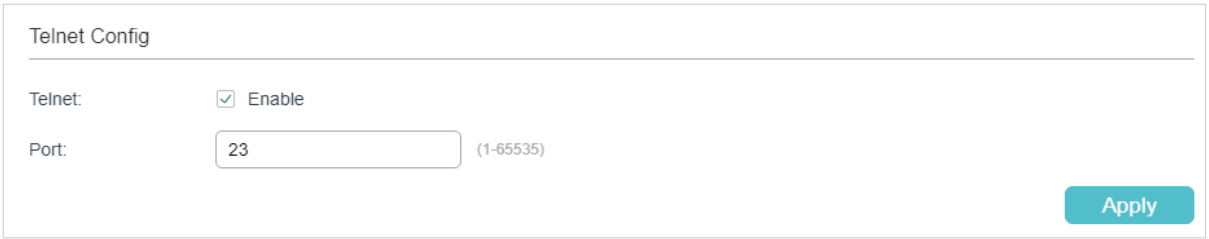
Note:

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

2.1.5 Configuring the Telnet Function

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

Figure 2-8 Configuring the Telnet Function



Enable Telnet 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.
Port	Specify the port using for Telnet.

2.2 Using the CLI

2.2.1 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 enable** Configure the control mode as IP-based. **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 enable** Configure the control mode as MAC-based. **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 enable** Configure the control mode as Port-based. **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 255.255.255.255 and make the switch support snmp, telnet, http and https.

Switch#configure

Switch(config)#user access-control ip-based enable

Switch(config)#user access-control ip-based 192.168.0.100 255.255.255.255 snmp telnet http https

Switch(config)#show user configuration

User authentication mode: IP based

Index	IP Address	Access Interface
1	192.168.0.100/32	SNMP Telnet HTTP HTTPS

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 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 operator-num poweruser-num user-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. *operator-num*: Enter the maximum number of users whose access level is Operator. The valid values are from 0 to 15. *poweruser-num*: Enter the maximum number of users whose access level is Power User. The valid values are from 0 to 15. *user-num*: Enter the maximum number of users whose access level is 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 operator number as 2, the maximum power user number as 2, the maximum user number as 2.

Switch#configure

Switch(config)#ip http server

Switch(config)#ip http session timeout 9

Switch(config)#ip http max-user 6 2 2 2

Switch(config)#show ip http configuration

HTTP Status:	Enabled
HTTP Port:	80
HTTP Session Timeout:	9
HTTP User Limitation:	Enabled
HTTP Max Users as Admin:	6
HTTP Max Users as Operator:	2
HTTP Max Users as Power User:	2
HTTP Max Users as User:	2

Switch(config)#end

Switch#copy running-config startup-config

2.2.3 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 operator-num poweruser-num user-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 values are from 1 to 16. *operator-num*: Enter the maximum number of users whose access level is Operator. The valid values are from 0 to 15. *poweruser-num*: Enter the maximum number of users whose access level is Power User. The valid values are from 0 to 15. *user-num*: Enter the maximum number of users whose access level is User. The valid values 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 maximum admin number as 2, the maximum operator number as 2, the maximum power user number as 2, the maximum user 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 2 2 2 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
HTTPS Port:	443
SSL Protocol Level(s):	ssl3 tls1
SSL CipherSuite:	3des-ede-cbc-sha
HTTPS Session Timeout:	15
HTTPS User Limitation:	Enabled
HTTPS Max Users as Admin:	2
HTTPS Max Users as Operator:	2
HTTPS Max Users as Power User:	2
HTTPS Max Users as User:	2

Switch(config)#end

Switch#copy running-config startup-config

2.2.4 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

Port: 22

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

2.2.5 Configuring 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	**telnet port** *port* Specify the port using for Telnet. It ranges from 1 to 65535.
Step 4	**end** Return to privileged EXEC mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

3 Appendix: Default Parameters

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

Table 3-1 Default Settings of Access Control Configuration

Parameter	Default Setting
Access Control	Disabled

Table 3-2 Default Settings of HTTP Configuration

Parameter	Default Setting
HTTP	Enabled
Port	80
Session Timeout	10 minutes
Number Control	Disabled

Table 3-3 Default Settings of HTTPS Configuration

Parameter	Default Setting
HTTPS	Enabled
SSL Version 3	Enabled
TLS Version 1	Enabled
Port	443
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 3-4 Default Settings of SSH Configuration

Parameter	Default Setting
SSH	Disabled
Protocol V1	Enabled
Protocol V2	Enabled
Idle Timeout	120 seconds
Maximum Connections	5

Parameter	Default Setting
Port	22
AES128-CBC	Enabled
AES192-CBC	Enabled
AES256-CBC	Enabled
Blowfish-CBC	Enabled
Cast128-CBC	Enabled
3DES-CBC	Enabled
HMAC-SHA1	Enabled
HMAC-MD5	Enabled
Key Type:	SSH-2 RSA/DSA

Table 3-5 Default Settings of Telnet Configuration

Parameter	Default Setting
Telnet	Enabled
Port	23

Part 19

Configuring AAA

CHAPTERS

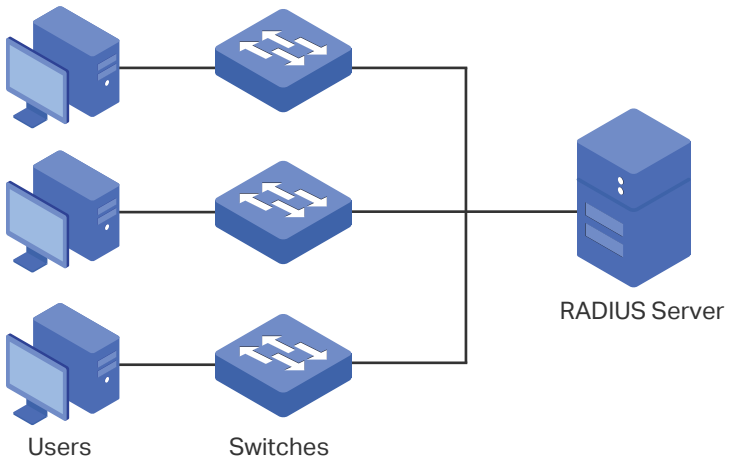
1. Overview
2. AAA Configuration
3. Configuration Example
4. Appendix: Default Parameters

1 Overview

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 1-1 Network Topology of AAA



2 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) Add the servers.
2) Configure the server groups.
3) Configure the method list.
4) Configure the AAA application list.
5) Configure the login account and the Enable password.

Configuration Guidelines

The basic concepts and working mechanism of AAA are as follows:

- AAA Default Setting

By default, the AAA feature is enabled and cannot be disabled.

- 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: Telnet, SSH and HTTP. You can select the configured authentication method lists for each application.

2.1 Using the GUI

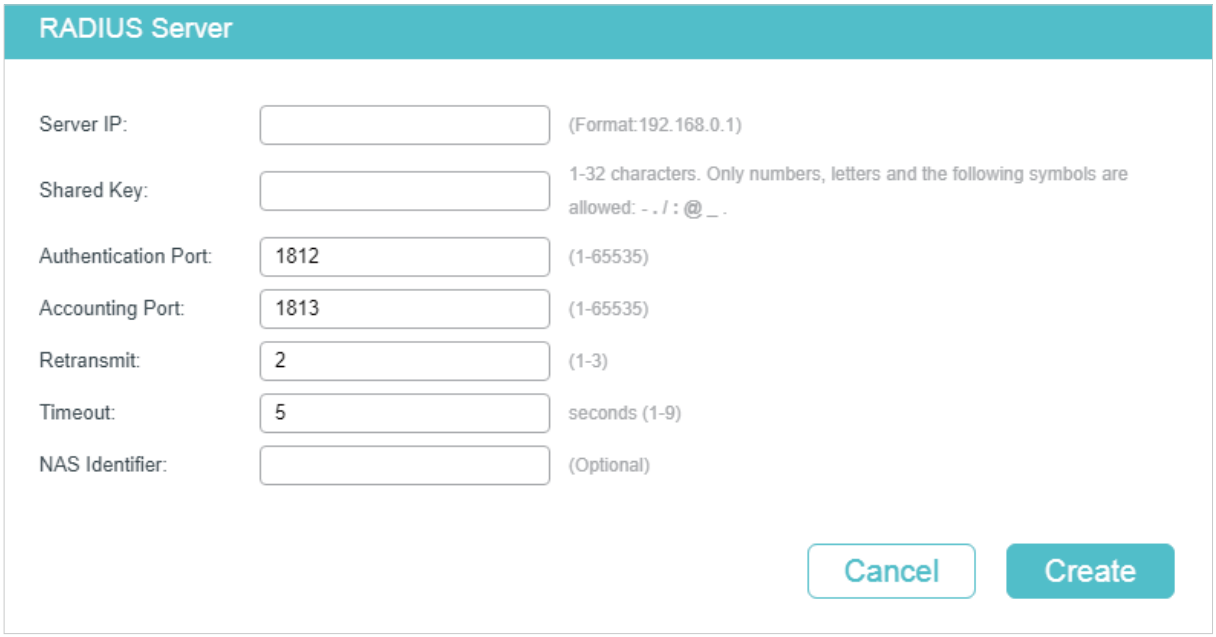
2.1.1 Adding Servers

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 **SECURITY > AAA > RADIUS Config** and click Add to load the following page.

Figure 2-1 RADIUS Server Configuration



Follow these steps to add a RADIUS server:

1) 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.
Authentication Port	Specify the UDP destination port on the RADIUS server for authentication requests. The default setting is 1812.

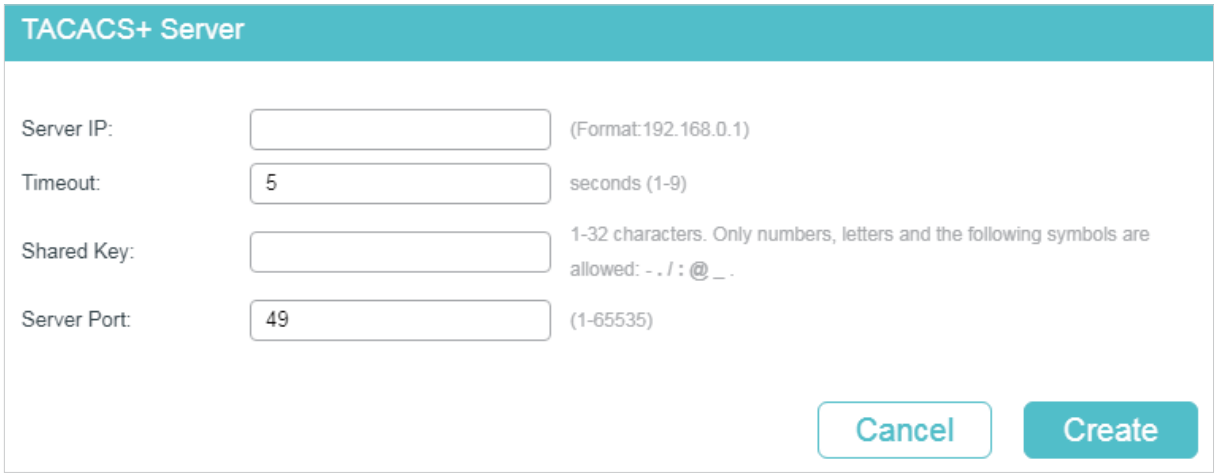
Accounting Port	Specify the UDP destination port on the RADIUS server for accounting requests. The default setting is 1813. Usually, it is used in the 802.1x feature.
Retransmit	Specify the number of times a request is resent to the server if the server does not respond. The default setting is 2.
Timeout	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 **Create** to add the RADIUS server on the switch.

■ Adding TACACS+ Server

Choose the menu **SECURITY > AAA > TACACS+ Config** and click Add to load the following page.

Figure 2-2 TACACS+ Server Configuration



Follow these steps to add a TACACS+ server:

1) 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.

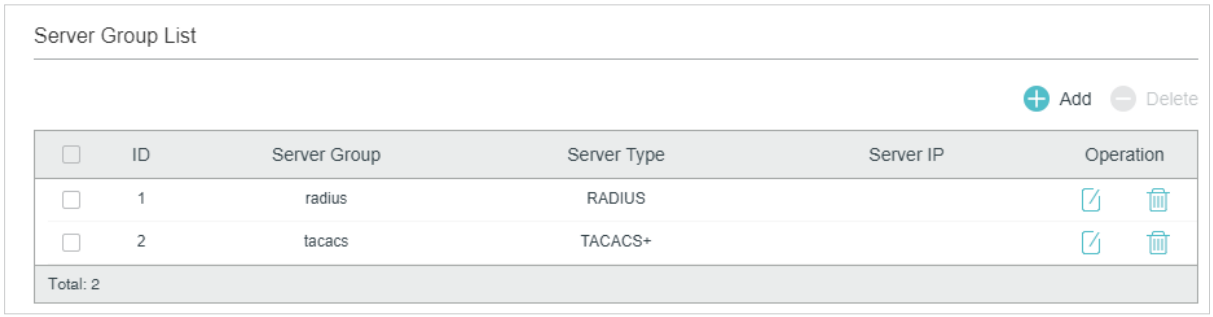
2) Click **Create** to add the TACACS+ server on the switch.

2.1.2 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 **SECURITY > AAA > Server Group** to load the following page.

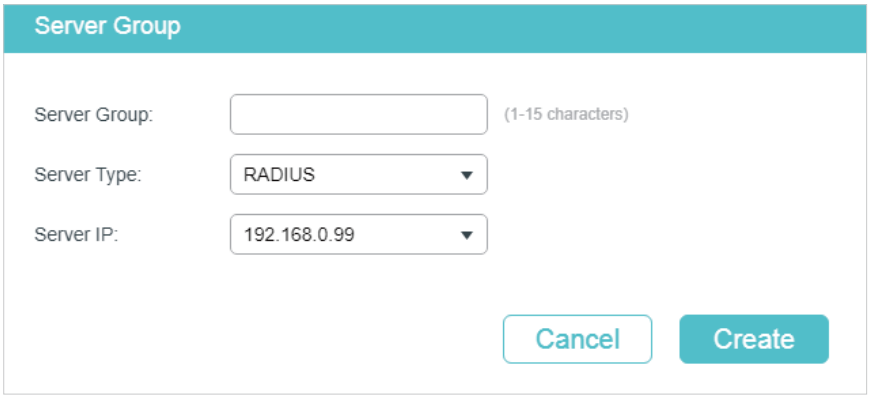
Figure 2-3 Add New Server Group



There are two default server groups in the list. You can edit the default server groups or follow these steps to configure a new server group:

1) Click Add and the following window will pop up.

Figure 2-4 Add Server Group



Configure the following parameters:

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+.
Server IP	Select the IP address of the server which will be added to the server group.

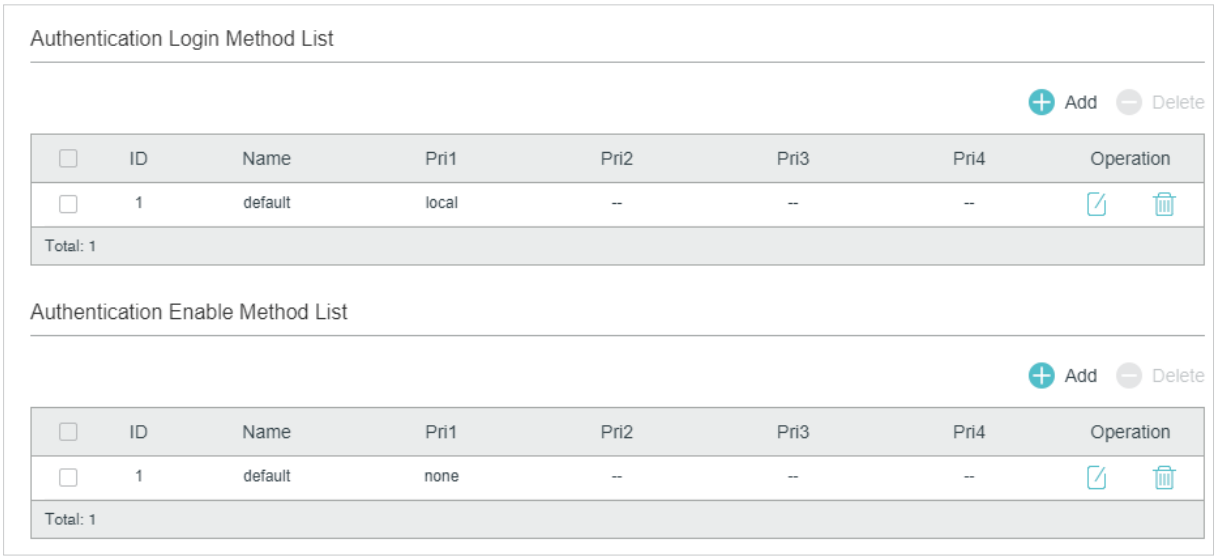
2) Click **Create**.

2.1.3 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 **SECURITY > AAA > Method List** to load the following page.

Figure 2-5 Method List

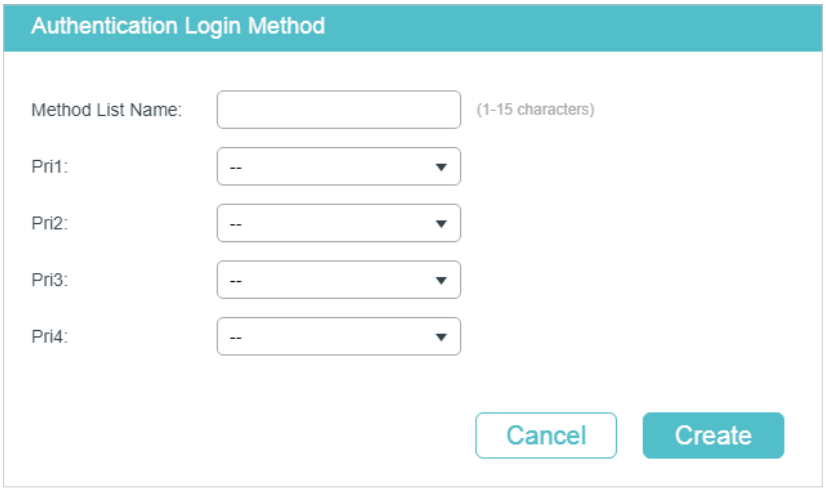


There are two default methods respectively for the Login authentication and the Enable authentication.

You can edit the default methods or follow these steps to add a new method:

1) Click Add in the **Authentication Login Method List** section or **Authentication Enable Method List** section to add corresponding type of method list. The following window will pop up.

Figure 2-6 Add New Method



Configure the parameters for the method to be added.

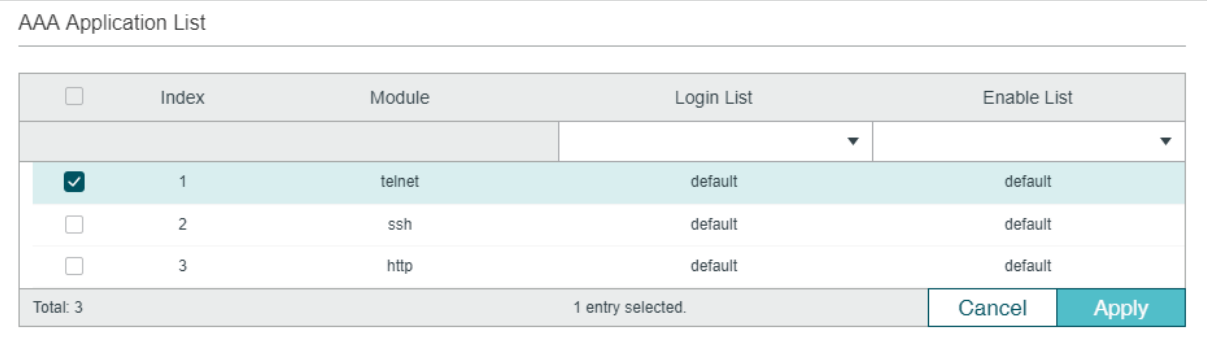
Method List Name	Specify a name for the method.
Pri1- Pri4	Specify the authentication methods in order. The method with priority 1 authenticates a user first, the method with priority 2 is tried if the previous method does not respond, and so on. **local**: Use the local database in the switch for authentication. **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 **Create** to add the new method.

2.1.4 Configuring the AAA Application List

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

Figure 2-7 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: 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**.

2.1.5 Configuring Login Account and Enable Password

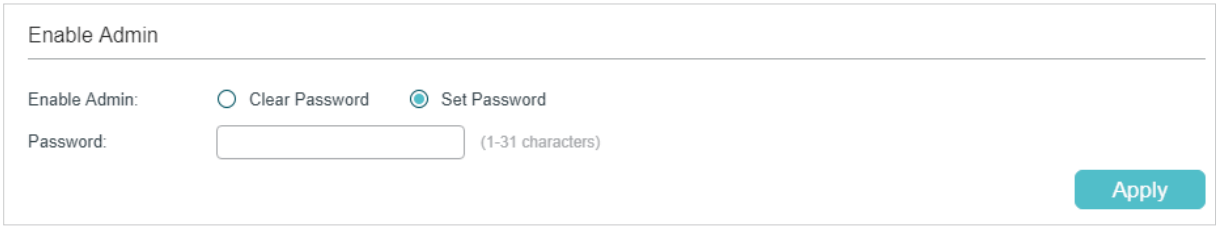
The login account and Enable password can be configured locally on the switch or centrally on the RADIUS/TACACS+ server(s).

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 **SECURITY > AAA > Global Config** to load the following page.

Figure 2-8 Configure Enable Password



There are two options: **Clear Password** and **Set Password**. You can choose whether the local Enable password is required when the guests try to get administrative privileges. Click **Apply**.

Tips: The logged-in guests can enter the local 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.

2.2 Using the CLI

2.2.1 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 32 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 32 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

2.2.2 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

2.2.3 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

2.2.4 Configuring the AAA Application List

You can configure authentication method lists on the following access applications: Telnet, SSH and HTTP.

- 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
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
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
Telnet	default	default
Ssh	default	default
Http	Login1	Enable1

Switch(config)#end

Switch#copy running-config startup-config

2.2.5 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.

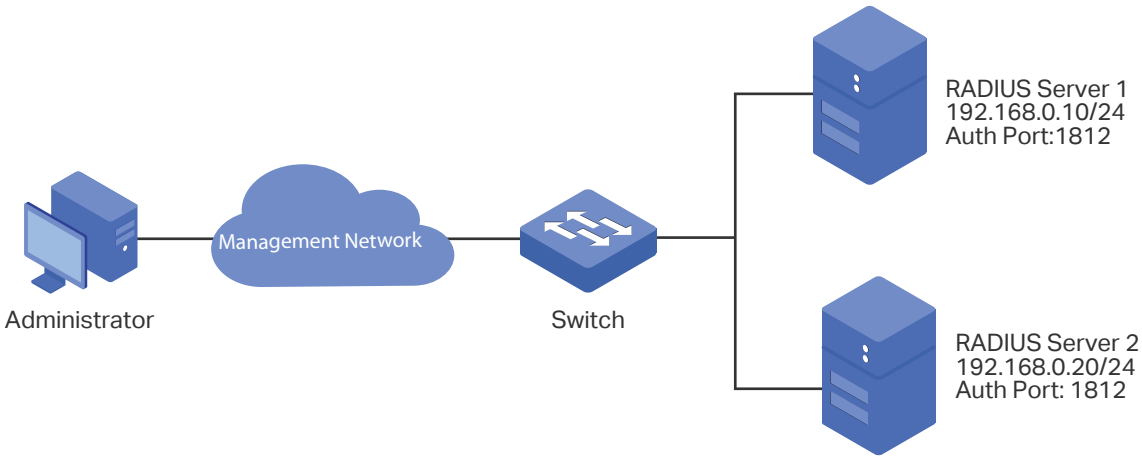
3 Configuration Example

3.1 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 3-1 Network Topology



3.2 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:

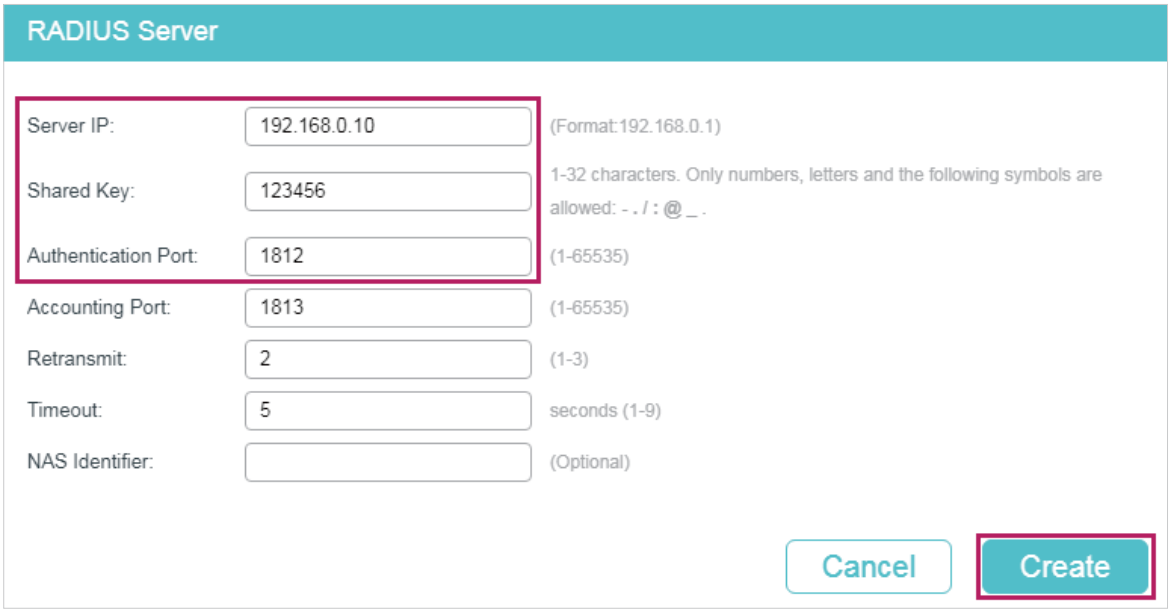
1) Add the two RADIUS servers on the switch.
2) Create a new RADIUS server group and add the two servers to the group. Make sure that RADIUS Server 1 is the first server for authentication.
3) Configure the method list.
4) Configure the AAA application list.

Demonstrated with T1600G-52TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

3.3 Using the GUI

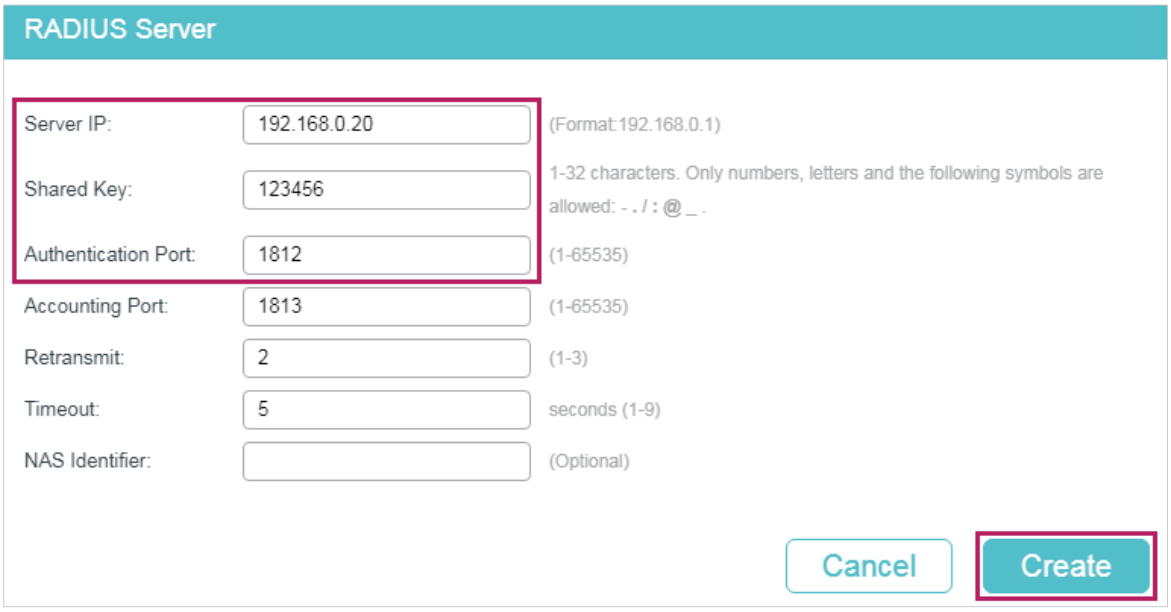
1) Choose the menu **SECURITY > AAA > RADIUS Config** and click Add to load the following page. Configure the Server IP as 192.168.0.10, the Shared Key as 123456, the Authentication Port as 1812, and keep the other parameters as default. Click **Create** to add RADIUS Server 1 on the switch.

Figure 3-2 Add RADIUS Server 1



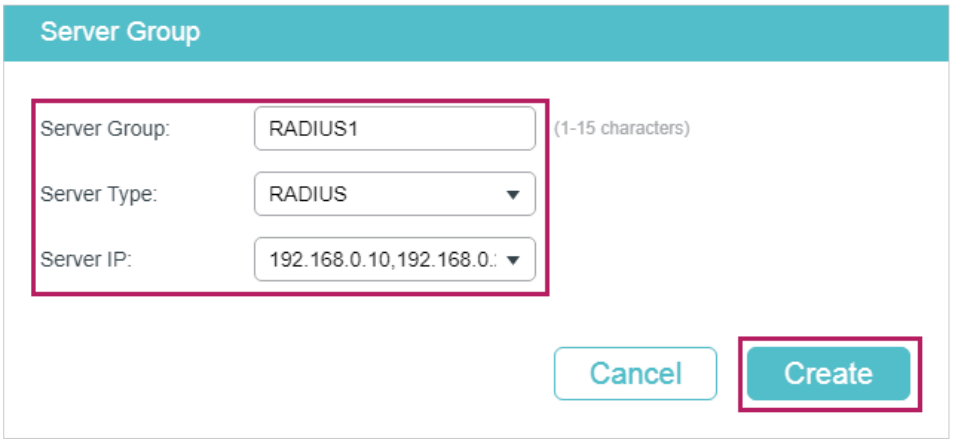
2) On the same page, click Add to load the following page. Configure the Server IP as 192.168.0.20, the Shared Key as 123456, the Auth Port as 1812, and keep the other parameters as default. Click **Create** to add RADIUS Server 2 on the switch

Figure 3-3 Add RADIUS Server 2



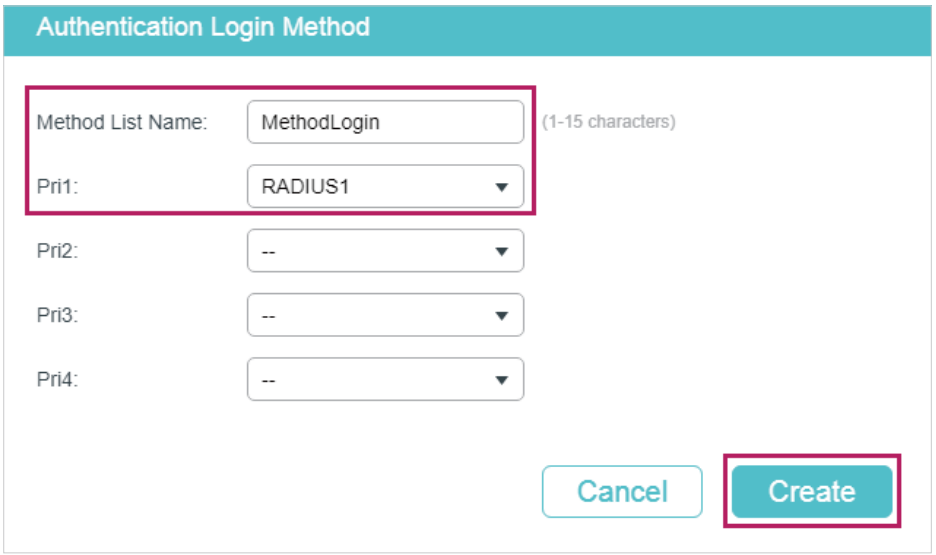
3) Choose the menu **SECURITY > AAA > Server Group** to load the following page. Click Add. Specify the group name as RADIUS1 and the server type as RADIUS. Select 192.168.0.10 and 192.168.0.20 to from the drop-down list. Click **Create** to create the server group.

Figure 3-4 Create Server Group



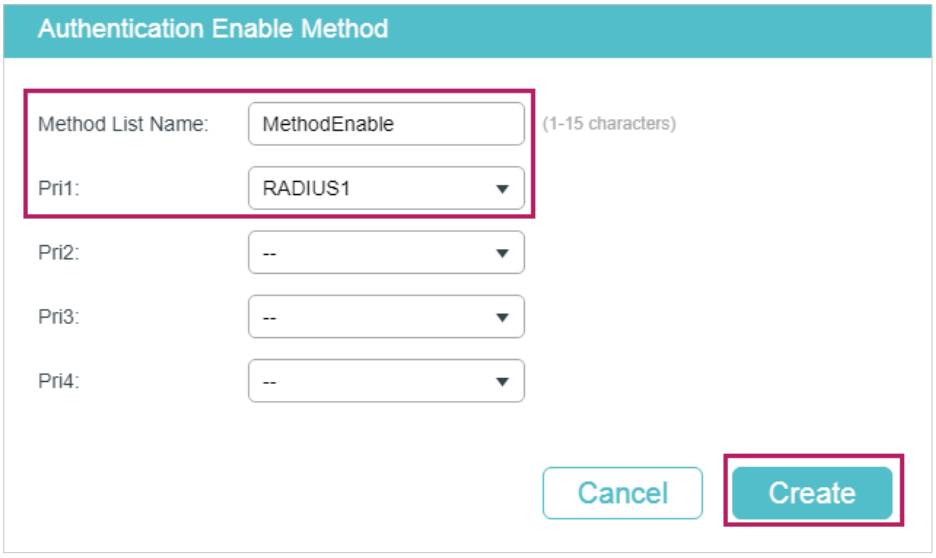
4) Choose the menu **SECURITY > AAA > Method List** and click Add in the **Authentication Login Method List** section. Specify the Method List Name as MethodLogin and select the Pri1 as RADIUS1. Click **Create** to set the method list for the Login authentication.

Figure 3-5 Configure Login Method List



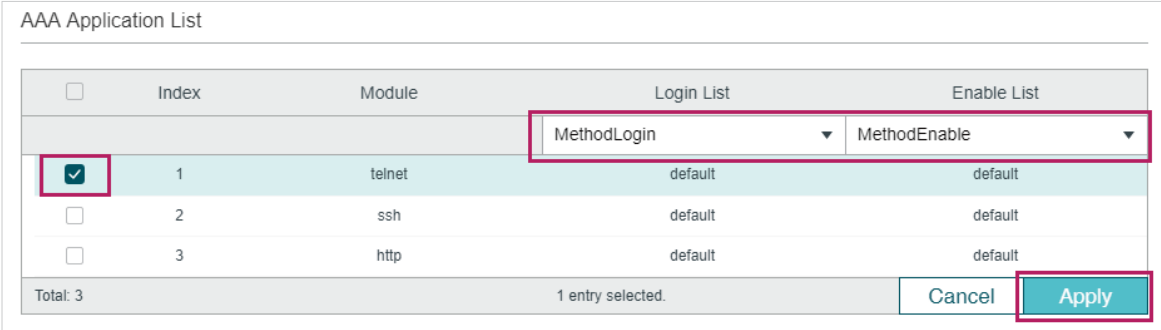
5) On the same page, click Add in the **Authentication Eanble Method List** section. Specify the Method List Name as MethodEnable and select the Pri1 as RADIUS1. Click **Create** to set the method list for the Enable password authentication.

Figure 3-6 Configure Enable Method List



6) Choose the menu **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 3-7 Configure AAA Application List



7) Click Save to save the settings.

3.4 Using the CLI

1) 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

2) 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

3) 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

4) 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

Module	Login List	Enable List
Telnet	Method-Login	Method-Enable
SSH	default	default
Http	default	default

4 Appendix: Default Parameters

Default settings of AAA are listed in the following tables.

Table 4-1 AAA

Parameter	Default Setting
Global Config	
AAA Feature	Enable
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

Parameter	Default Setting
AAA Application List	
telnet	Login List: default Enable List: default
ssh	Login List: default Enable List: default
http	Login List: default Enable List: default

Part 20

Configuring 802.1x

CHAPTERS

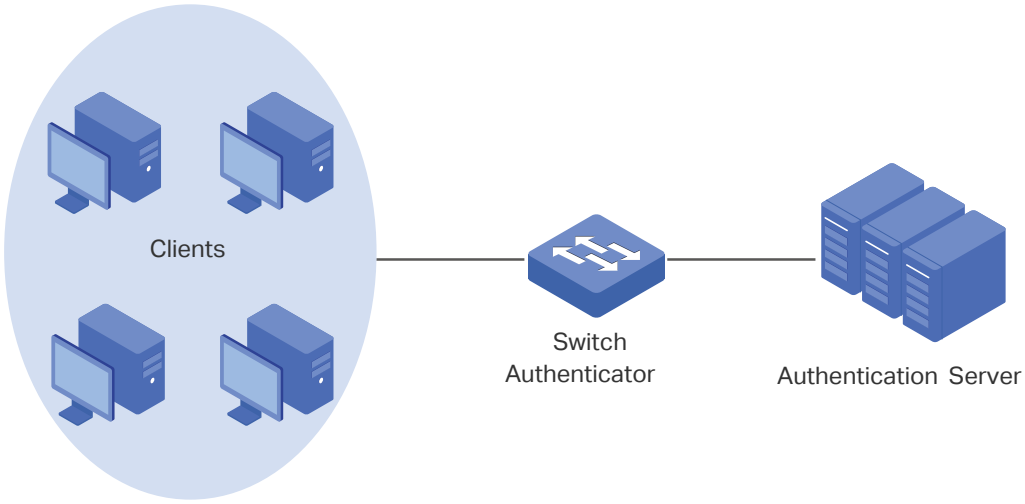
1. Overview
2. 802.1x Configuration
3. Configuration Example
4. Appendix: Default Parameters

1 Overview

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 client-server model which contains three device roles: client/supplicant, authenticator and authentication server. This is described in the figure below:

Figure 1-1 802.1x 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.

2 802.1x 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.

In addition, you can view the authenticator state.

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.

2.1 Using the GUI

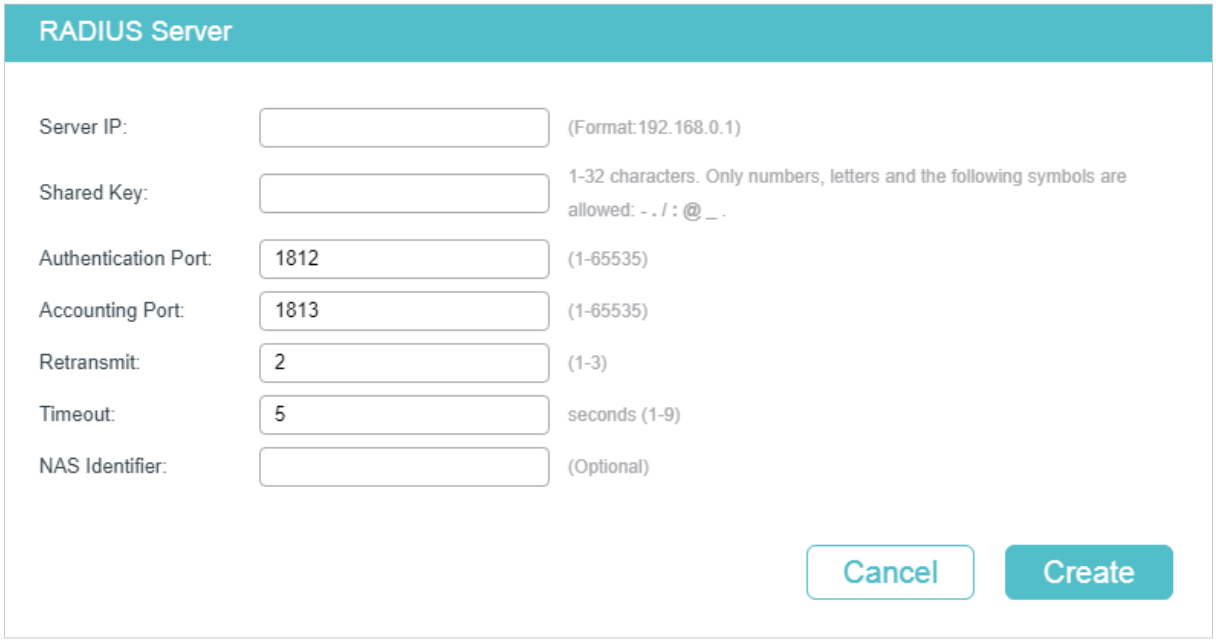
2.1.1 Configuring the RADIUS Server

Configure the parameters of RADIUS sever and configure the RADIUS server group.

- Adding the RADIUS Server

Choose the menu **SECURITY > AAA > RADIUS Config** and click Add to load the following page.

Figure 2-1 Adding RADIUS Server



Follow these steps to add a RADIUS server:

1) Configure the parameters of the RADIUS server.

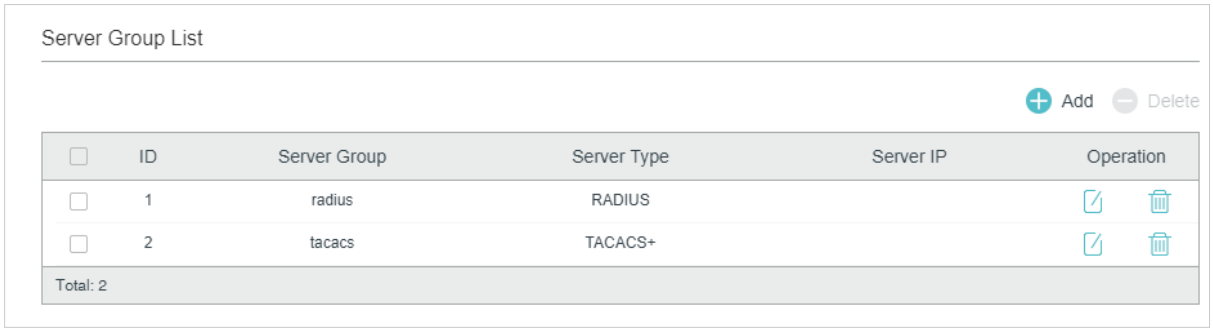
Server IP	Enter the IP address of the server running the RADIUS secure protocol.
Shared Key	Enter the shared key between the RADIUS server and the switch. The RADIUS server and the switch use the key string to encrypt passwords and exchange responses.
Authentication Port	Specify the UDP destination port on the RADIUS server for authentication requests. The default setting is 1812.
Accounting 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.

2) Click **Apply**.

Configuring the RADIUS Server Group

Choose the menu **SECURITY > AAA > Server Group** to load the following page.

Figure 2-2 Adding a Server Group

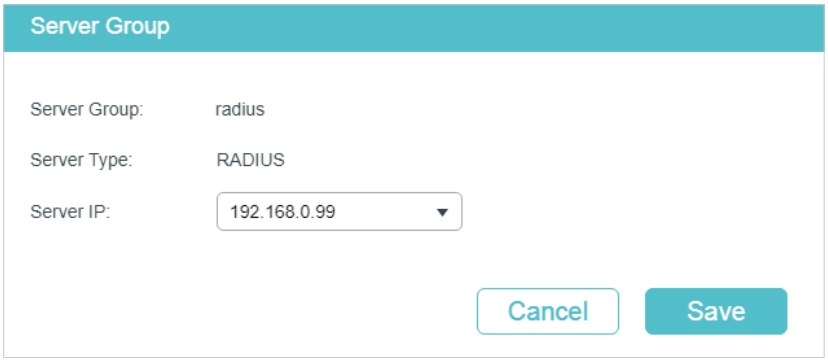


Follow these steps to add the RADIUS server to a server group:

1) Click to edit the default **radius** server group or click Add to add a new server group.

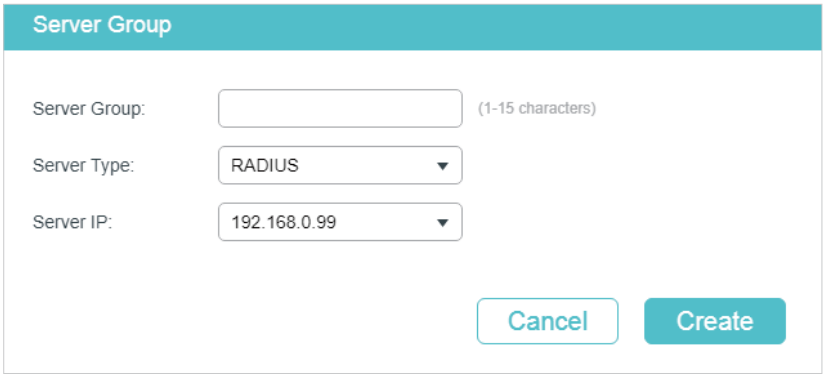
   If you click , the following window will pop up. Select a RADIUS server and click **Save**.

Figure 2-3 Editing Server Group



If you click Add , the following window will pop up. Specify a name for the server group, select the server type as RADIUS and select the IP address of the RADIUS server. Click **Save**.

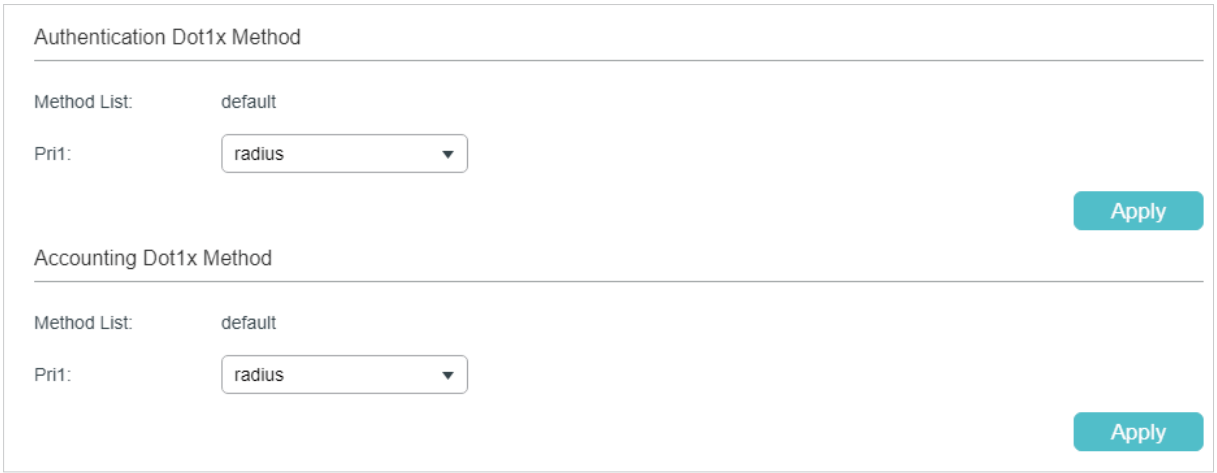
Figure 2-4 Adding Server Group



Configuring the Dot1x List

Choose the menu **SECURITY > AAA > Dot1x List** to load the following page.

Figure 2-5 Configuring the Dot1x List



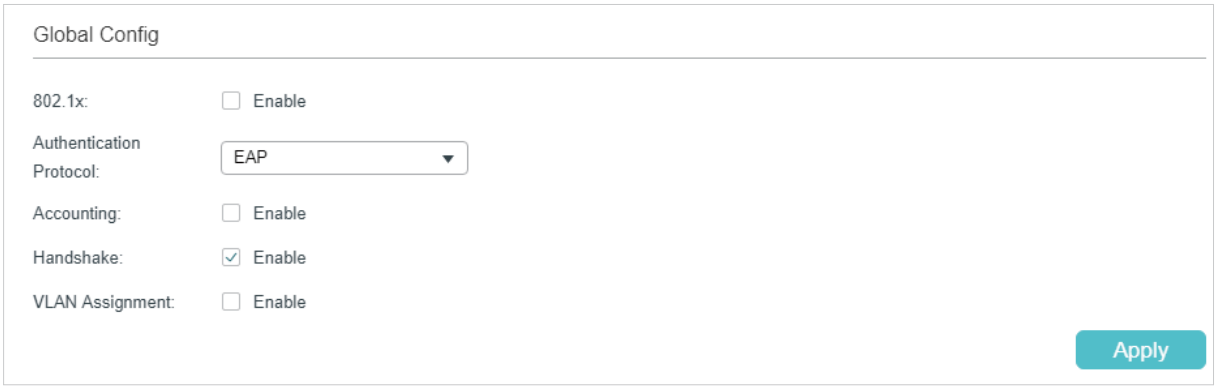
Follow these steps to configure RADIUS server groups for 802.1x authentication and accounting:

1) In the **Authentication Dot1x Method** section, select an existing RADIUS server group for authentication from the Pri1 drop-down list and click **Apply**.
2) In the **Accounting Dot1x Method** section, select an existing RADIUS server group for accounting from the Pri1 drop-down list and click **Apply**.

2.1.2 Configuring 802.1x Globally

Choose the menu **SECURITY > 802.1x > Global Config** to load the following page.

Figure 2-6 Global Config



Follow these steps to configure 802.1x global parameters:

1) In the **Global Config** section, configure the following parameters.

802.1x	Enable or disable 802.1x globally.
Auth Protocol	Select the 802.1x authentication protocol. **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.
Accounting	Enable or disable 802.1x accounting feature.
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.

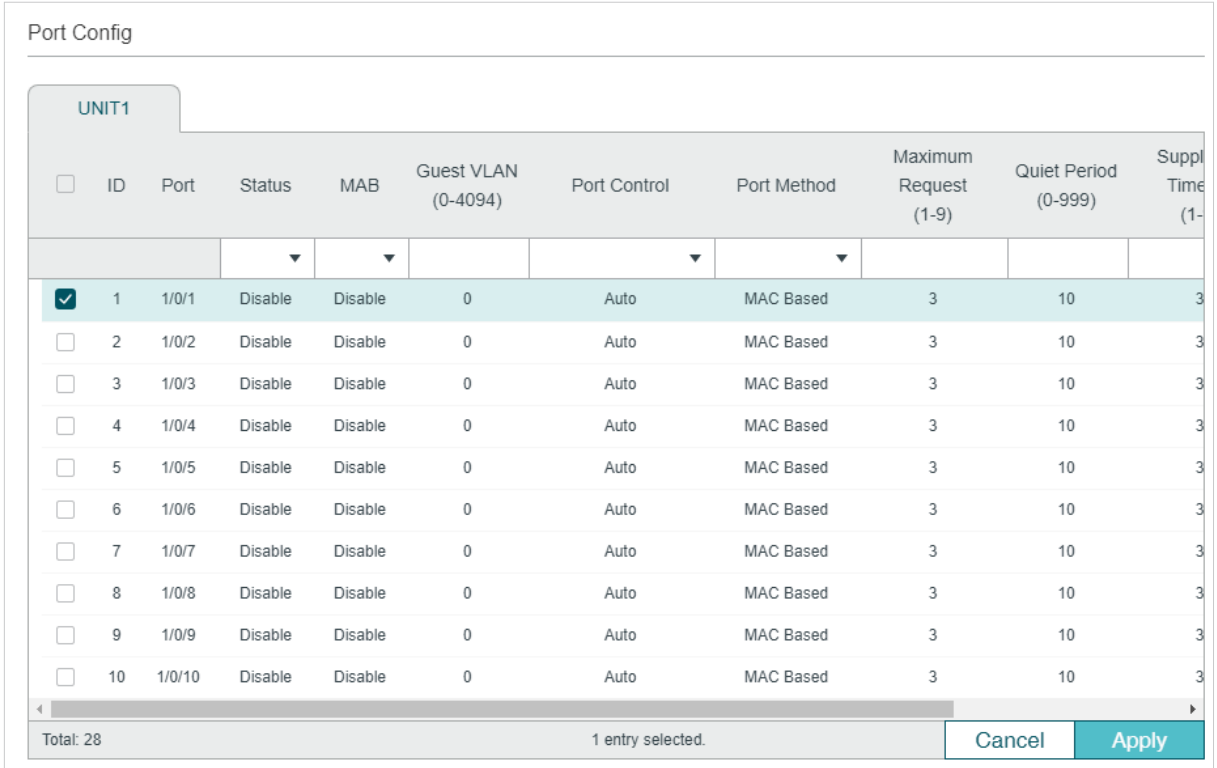
VLAN Assignment	Enable or disable the 802.1x VLAN assignment feature. 802.1x VLAN assignment is a technology allowing the RADIUS server to send the VLAN assignment to the port when the port is authenticated. If the assigned VLAN does not exist on the switch, the switch will create the related VLAN automatically, 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) Click **Apply**.

2.1.3 Configuring 802.1x on Ports

Choose the menu **SECURITY > 802.1x > Port Config** to load the following page.

Figure 2-7 Port Config



Follow these steps to configure 802.1x authentication on the desired port:

1) Select one or more ports and configure the following parameters:

Status	Enable 802.1x authentication 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. *Note:* MAB cannot work if Guest VLAN is enabled.
Guest VLAN	Specify a Guest VLAN ID. 0 means that Guest VLAN is disabled. The configured VLAN must be an existing 802.1Q VLAN. With Guest VLAN 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.
Port Control	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.
Port Method	Select the port method. 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.
Maximum Request (1-9)	Specify the maximum number of attempts to send the authentication packet. It ranges from 1 to 9 times and the default is 3 times.
Quiet Period (1-999)	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.
Supplicant Timeout (1-9)	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.
Authorized	Displays whether the port is authorized or not.
LAG	Displays the LAG the port belongs to.

2) Click **Apply**.

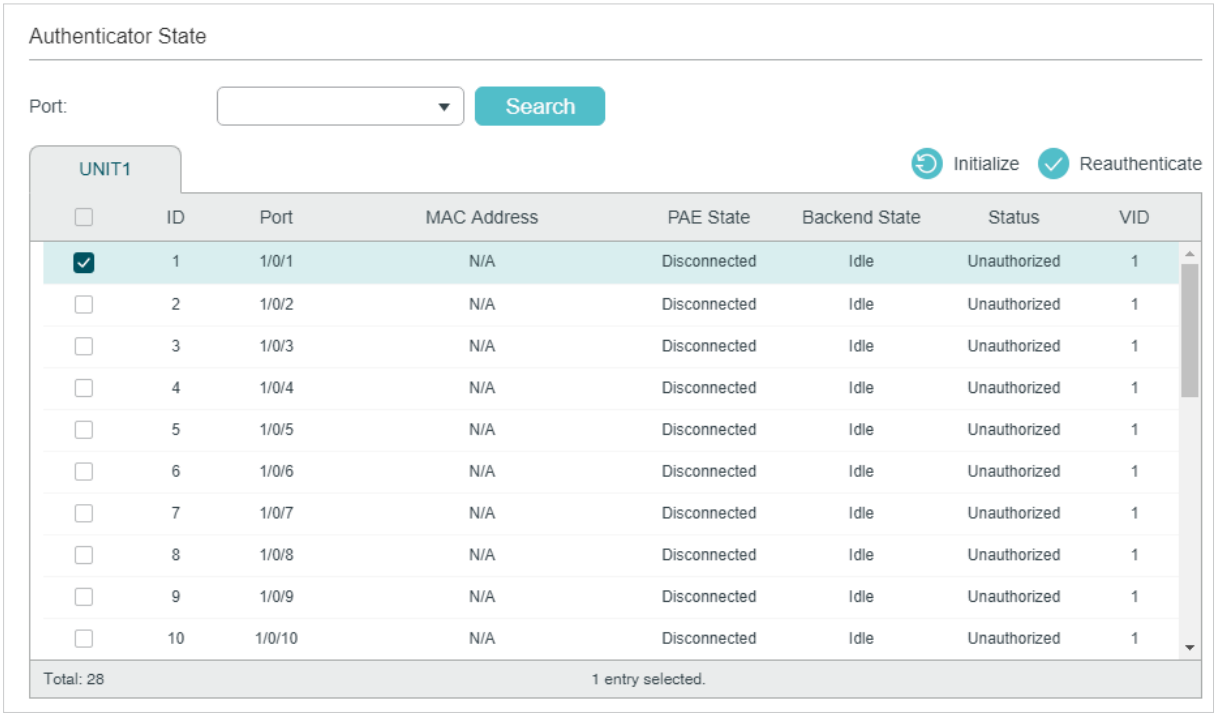
Note:

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.

2.1.4 View the Authenticator State

Choose the menu **SECURITY > 802.1x > Authenticator State** to load the following page.

Figure 2-8 View Authenticator State



On this page, you can view the authentication status of each port:

Port	Displays the port number.
MAC Address	Displays the MAC address of the authenticated device. When the port method is Port Based, the MAC address of the first authenticated device wil be displayed with a suffix “p”.
PAE State	Displays the current state of the authenticator PAE state machine. Possible values are: Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized and ForceUnauthorized.
Backend State	Displays the current state of the backend authentication state machine. Possible values are: Request, Response, Success, Fail, Timeout, Initialize and Idle.
Status	Displays whether the port is authorized or not.
VID	Displays the VLAN ID assigned by the authenticator to the supplicant device when the related port is authorized. If the related port is unauthorized and there is a Guest VLAN ID, the Guest VLAN ID will be displayed.

2.2 Using the CLI

2.2.1 Configuring the RADIUS Server

Follow these steps to configure RADIUS:

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. 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 32 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	**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 4	**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 5	**exit** Return to global configuration mode.

Step 6	**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 7	**show radius-server** (Optional) Verify the configuration of RADIUS server.
Step 8	**show aaa group** [*group-name*] (Optional) Verify the configuration of server group.
Step 9	**show aaa authentication** dot1x (Optional) Verify the authentication method list.
Step 10	**show aaa accounting** dot1x (Optional) Verify the accounting method list.
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 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)#radius-server host 192.168.0.100 **auth-port** 1812 **acct-port** 1813 **key** 123456

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)#end

Switch#copy running-config startup-config

2.2.2 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-protocol** { pap | eap } Configure the 802.1x authentication protocol. pap: Specify the authentication protocol 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 protocol 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 accounting** (Optional) Enable the accounting feature.
Step 5	**dot1x handshake** (Optional) Enable 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.
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	**show dot1x global** (Optional) Verify global configurations of 802.1x.
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 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-protocol pap

Switch(config)#show dot1x global

802.1X State: Enabled

Authentication Protocol: PAP

Handshake State: Enabled

802.1X Accounting State: Disabled

802.1X VLAN Assignment State: Disabled

Switch(config)#end

Switch#copy running-config startup-config

2.2.3 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* **| ten-gigabitEthernet** *port* **| range ten-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. *Note:* MAB cannot work if Guest VLAN is enabled.

Step 5	**dot1x guest-vlan** *vid* (Optional) Configure guest VLAN on the port. *vid:* Specify the ID of the VLAN to be configured as the guest VLAN. The valid values are from 0 to 4094. 0 means that Guest VLAN is disabled on the port. The configured VLAN must be an existing 802.1Q VLAN. Clients in the guest VLAN can only access resources from specific VLANs. *Note*: To use Guest VLAN, the control type of the port should be configured as port-based.
Step 6	**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 7	**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 8	**dot1x max-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	**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 10	**dot1x timeout supp-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 11	**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 12	**end** Return to privileged EXEC mode.
Step 13	**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 keep other parameters as default:

Switch#configure

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

Switch(config-if)#dot1x

Switch(config-if)#dot1x port-method port-based

Switch(config-if)#show dot1x interface gigabitEthernet 1/0/2

Port	State	MAB State	GuestVLAN	PortControl	PortMethod
----	-----	---------	---------	----------	----------
Gi1/0/2	disabled	disabled	0	auto	port-based

MaxReq	QuietPeriod	SuppTimeout	Authorized	LAG
------	----------	----------	----------	---
3	10	3	unauthorized	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.4 Viewing Authenticator State

You can view the authenticator state. If needed, you can also initialize or reauthenticate the specific client:

Step 1	**show dot1x auth-state** Displays the authenticator state.
Step 2	**configure** Enter global configuration mode.

Step 3	**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:* Enter the ID of the port to be configured.
Step 4	**dot1x auth-init** [**mac** *mac-address*] Initialize the specific client. To access the network, the client needs to provide the correct information to pass the authentication again. *mac-address:* Enter the MAC address of the client that will be unauthorized.
Step 5	**dot1x auth-reauth** [**mac** *mac-address*] Reauthenticate the specific client. *mac-address:* Enter the MAC address of the client that will be reauthenticated.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

3 Configuration Example

3.1 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 only the authenticated clients can access the internet.

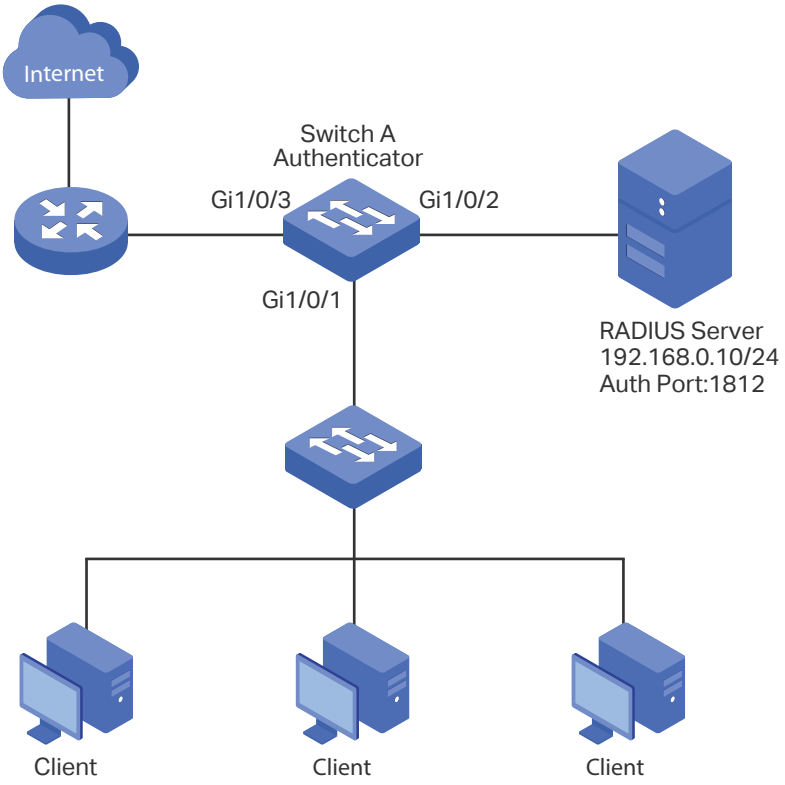
3.2 Configuration Scheme

- 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.

3.3 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 3-1 Network Topology

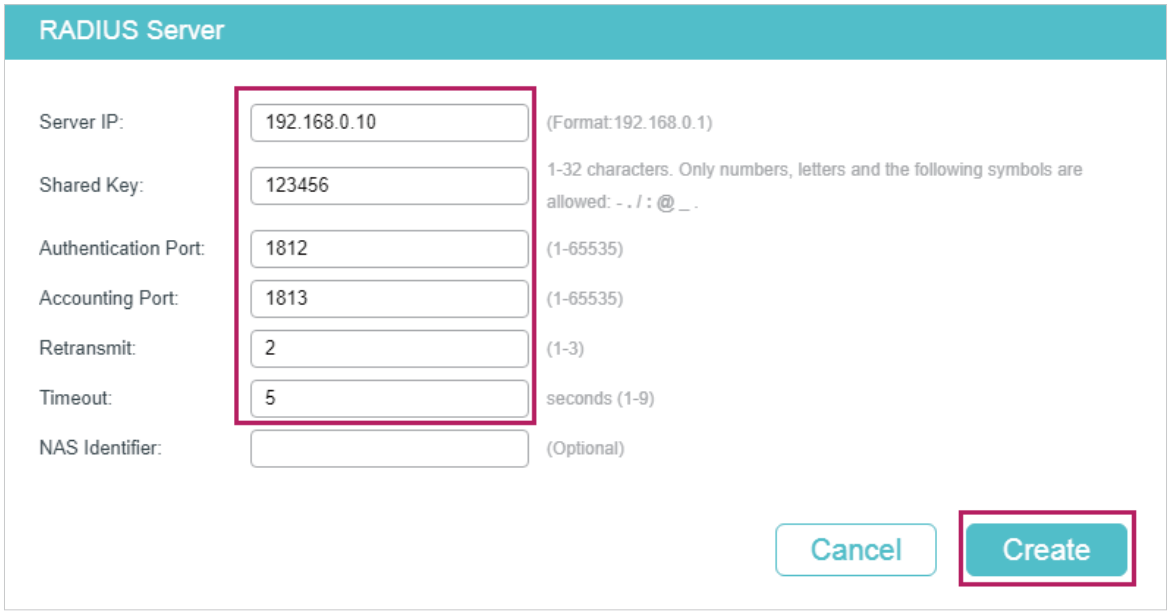


Demonstrated with T1600G-52TS acting as the authenticator, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

3.4 Using the GUI

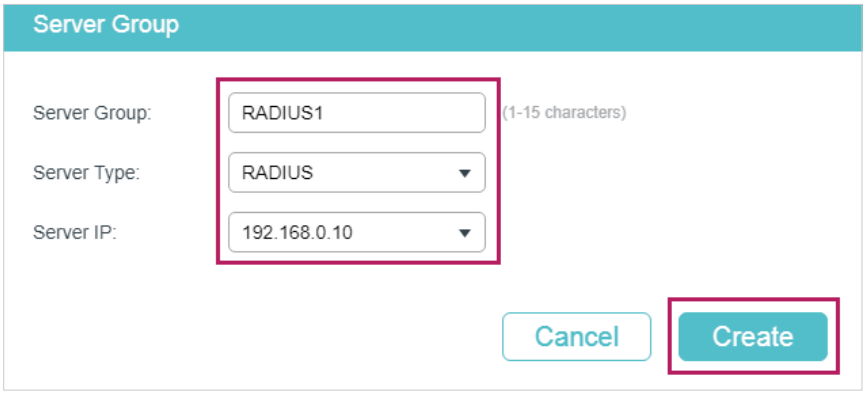
1) Choose the menu **SECURITY > AAA > RADIUS Config** and click Add to load the following page. Configure the parameters of the RADIUS server and click **Create**.

Figure 3-2 Adding RADIUS Server



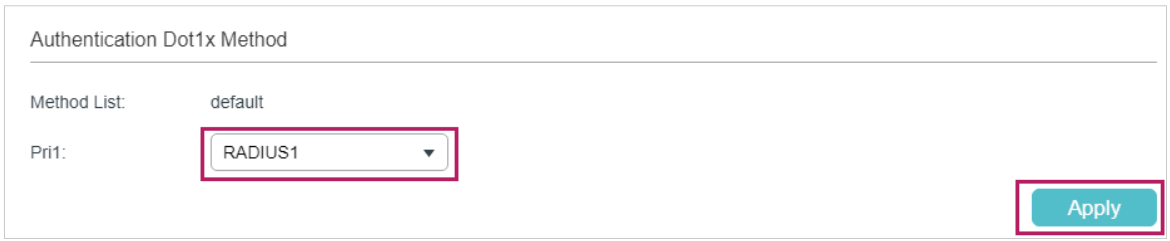
2) Choose the menu **SECURITY > AAA > Server Group** and click Add to load the following page. Specify the group name as RADIUS1, select the server type as RADIUS and server IP as 192.168.0.10. Click **Create**.

Figure 3-3 Creating Server Group



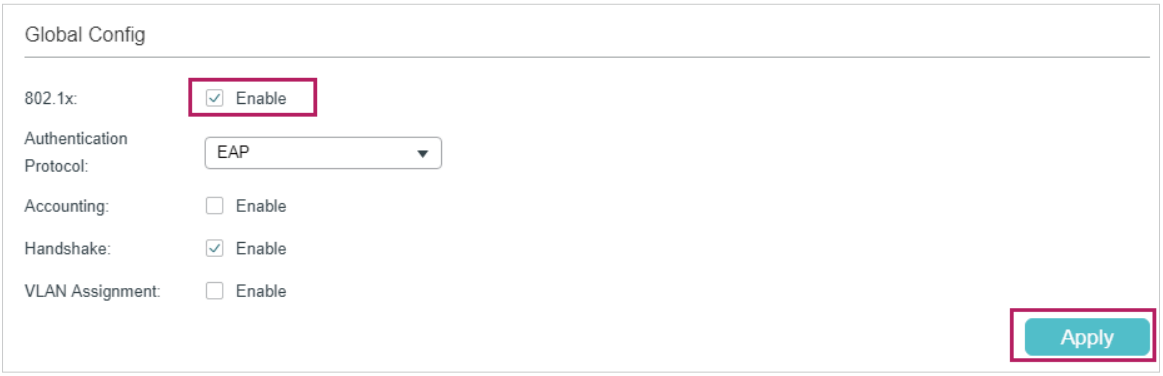
3) Choose the menu **SECURITY > AAA > Dot1x List** to load the following page. In the **Authentication Dot1x Method** section, select RADIUS1 as the RADIUS server group for authentication, and click **Apply**.

Figure 3-4 Configuring Authentication RADIUS Server



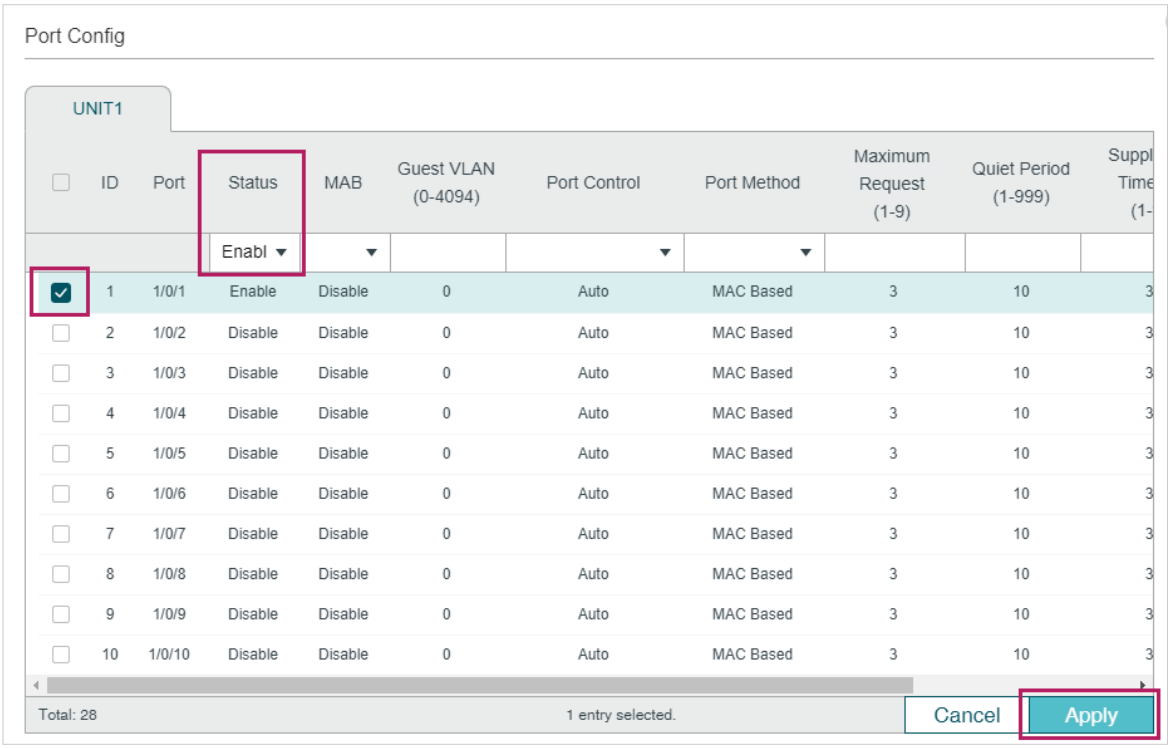
4) Choose the menu **SECURITY > 802.1x > Global Config** to load the following page. Enable 802.1x authentication and configure the Authentication Method as EAP. Keep the default authentication settings. Click **Apply**.

Figure 3-5 Configuring Global Settings



5) Choose the menu **SECURITY > 802.1x > 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 3-6 Configuring Port



6) Click Save to save the settings.

3.5 Using the CLI

1) Configure the RADIUS parameters.

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

2) Globally enable 802.1x authentication and set the authentication protocol.

Switch_A(config)#dot1x system-auth-control

Switch_A(config)#dot1x auth-protocol eap

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 Protocol:     EAP
 Handshake State:             Enabled
 802.1X Accounting State:     Disabled
 802.1X VLAN Assignment State:  Disabled
```

Verify the configurations of 802.1x authentication on the port:

```
Switch_A#show dot1x interface
Port       State      MAB State   GuestVLAN   PortControl     PortMethod
----       -----      ---------   ---------   -----------     ----------
Gi1/0/1    enabled    disabled    0           auto            mac-based
Gi1/0/2    disabled   disabled    0           auto            mac-based
Gi1/0/3    disabled   disabled    0           auto            mac-based
......
MaxReq   QuietPeriod  SuppTimeout  Authorized     LAG
------   -----------  -----------  ----------     ---
3        10           3            unauthorized   N/A
```

3 10 3 unauthorized N/A

3 10 3 unauthorized N/A

.....

Verify the configurations of RADIUS :

Switch_A#show aaa global

Module	Login List	Enable List
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

4 Appendix: Default Parameters

Default settings of 802.1x are listed in the following table.

Table 4-1 Default Settings of 802.1x

Parameter	Default Setting
Global Config	
802.1x Authentication	Disable
Authentication Method	EAP
Handshake	Enable
Accounting	Disable
VLAN Assignment	Disable
Port Config	
802.1x Status	Disable
MAB	Disable
Guest VLAN	Disable
Port Control	Auto
Guest VLAN	0
Maximum Request	3
Quiet Period	10 seconds
Supplicant Timeout	3 seconds
Port Method	MAC Based
Dot1X List	
Authentication Dot1x Method List	List Name: default Pri1: radius
Accounting Dot1x Method List	List Name: default Pri1: radius

Part 21

Configuring Port Security

CHAPTERS

1. Overview
2. Port Security Configuration
3. Appendix: Default Parameters

1 Overview

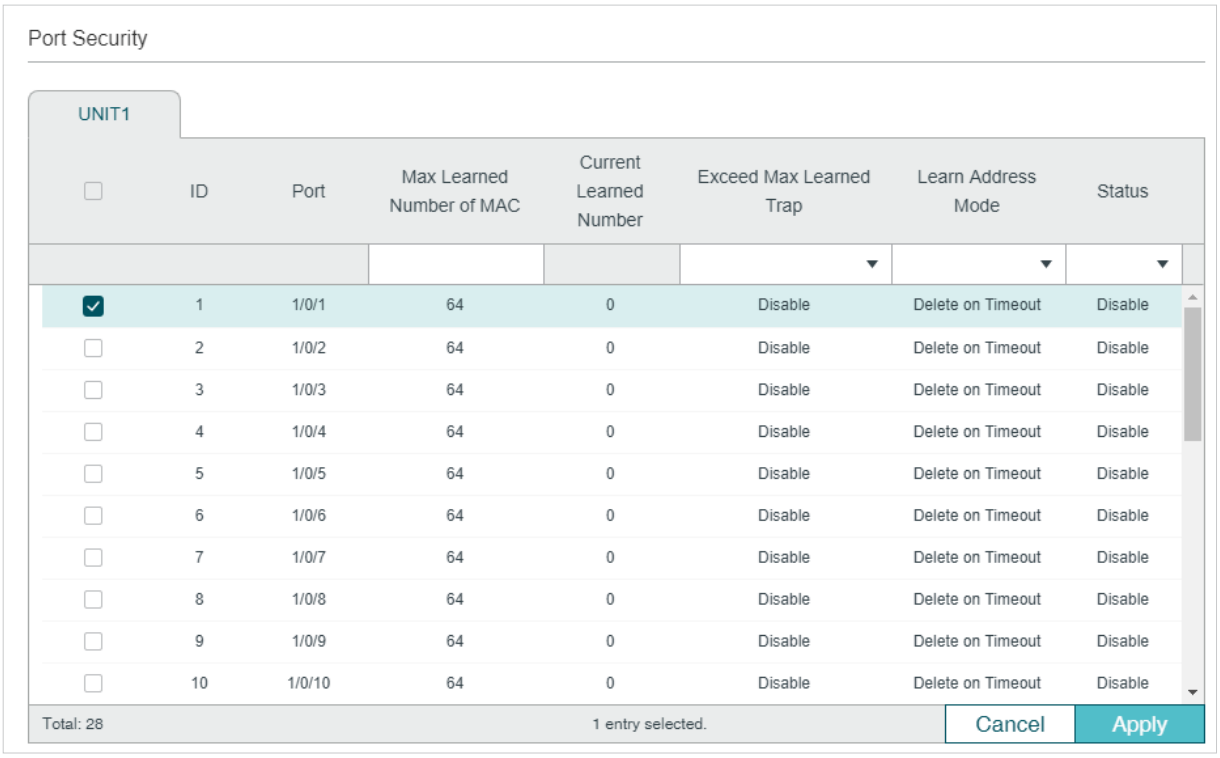
You can use the Port Security feature to limit the number of MAC addresses that can be learned on each port, thus preventing the MAC address table from being exhausted by the attack packets. In addtion, the switch can send a notification if the number of learned MAC addresses on the port exceeds the limit.

2 Port Security Configuration

2.1 Using the GUI

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

Figure 2-1 Port Security



Follow these steps to configure Port Security:

1) Select one or more ports and configure the following parameters.

Port	Displays the port number.
Max Learned Number of 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. It ranges from 0 to 64. The default value is 64.
Current Learned MAC	Displays the current number of MAC addresses that have been learned on the port.
Exceed Max Learned Trap	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.

Learn Address Mode	Select the learn mode of the MAC addresses on the port. Three modes are provided: **Delete on Timeout**: The switch will delete the MAC addresses that are not used or updated within the aging time. It is the default setting. **Delete on Reboot**: 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.
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.

2) Click **Apply**.

Note:

- Port Security cannot be enabled on the member ports 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.

2.2 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* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **}** Enter interface configuration mode.

Step 3	**mac address-table max-mac-count { [max-number** *num*] **[exceed-max-learned** enable | disable**] [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. **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. enable: Enable exceed-max-learned. disable: Disable exceed-max-learned. **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* **| ten-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.

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.

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

Switch#configure

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

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

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

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

Switch(config-if)#end

Switch#copy running-config startup-config

3 Appendix: Default Parameters

Default settings of Port Security are listed in the following table.

Table 3-1 Default Parameters of Port Security

Parameter	Default Setting
Max Learned Number of MAC	64
Current Learned Number	0
Exceed Max Learned Trap	Disable
Learn Address Mode	Delete on Timeout
Status	Disable

Part 22

Configuring ACL

CHAPTERS

1. Overview
2. ACL Configuration
3. Configuration Example for ACL
4. Appendix: Default Parameters

1 Overview

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.

To configure ACL, follow these steps:

1) Configure a time range during which the ACL is in effect.
2) Create an ACL and configure the rules to filter different packets.
3) Bind the ACL 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, the packets will be forwarded without being processed by the ACL. If there is configured ACL rules and no matching rule is found, the packets will be dropped.

2 ACL Configuration

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 a time range for the ACL. For details about Time Range configuration, please refer to *Managing System*.

2.1.2 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.

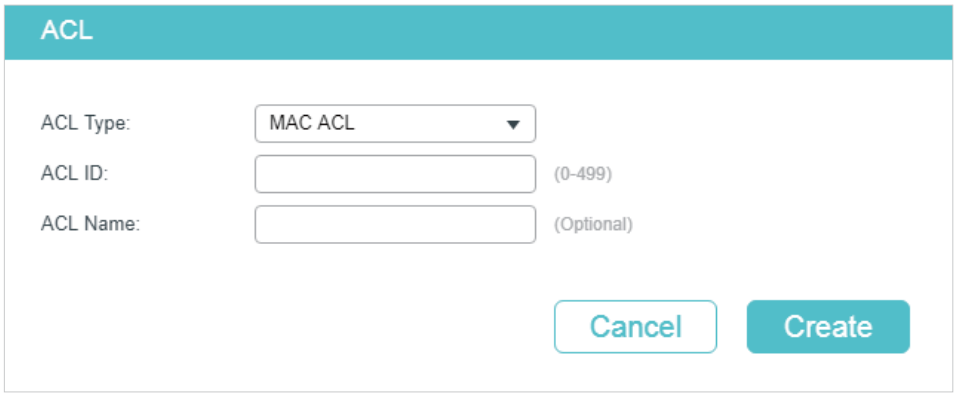
MAC ACL: MAC ACL uses source and destination MAC address for matching operations.

IP ACL: IP ACL uses source and destination IP address, IP protocols and so on for matching operations.

IPv6 ACL: IPv6 ACL uses source and destination IPv6 address for matching operations.

Choose the menu **SECURITY > ACL > ACL Config** and click Add to load the following page.

Figure 2-1 Creating an ACL



Follow these steps to create an ACL:

1) Choose one ACL type and enter a number to identify the ACL.
2) (Optional) Assign a name to the ACL.
3) Click **Create**.

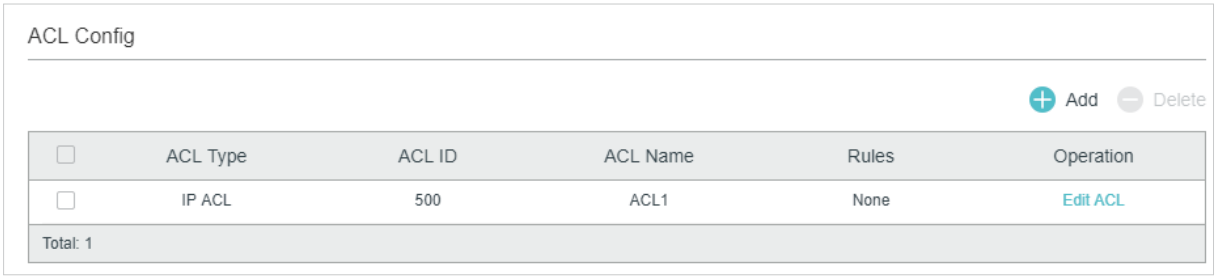
Note:

The supported ACL type and ID range varies on different switch models. Please refer to the on-screen information.

2.1.3 Configuring ACL Rules

The created ACL will be displayed on the **SECURITY > ACL > ACL Config** page.

Figure 2-2 Editing ACL



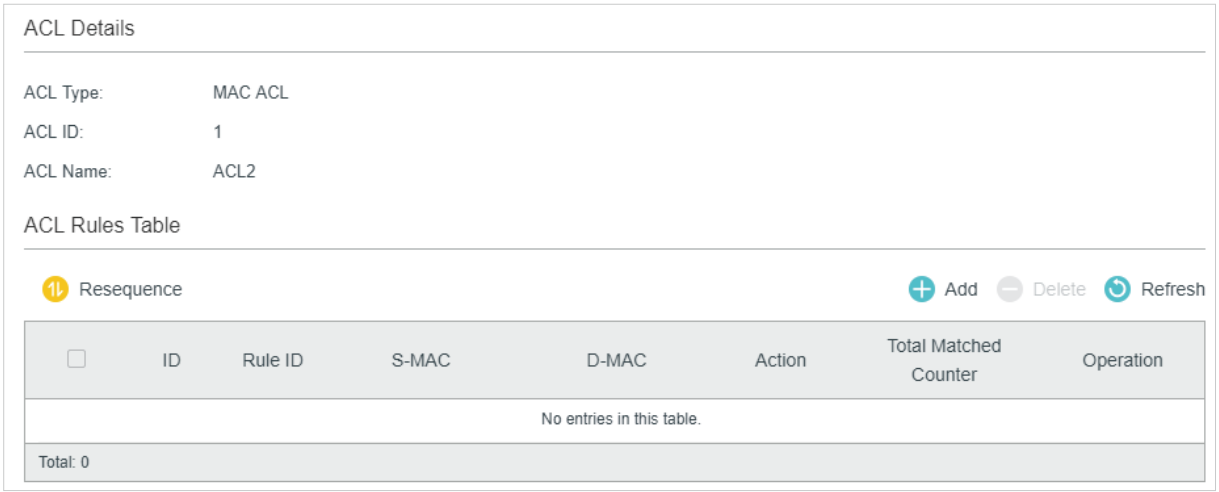
Click **Edit ACL** in the **Operation** column. Then you can configure rules for this ACL.

The following sections introduce how to configure MAC ACL, IP ACL,and IPv6 ACL.

Configuring MAC ACL Rule

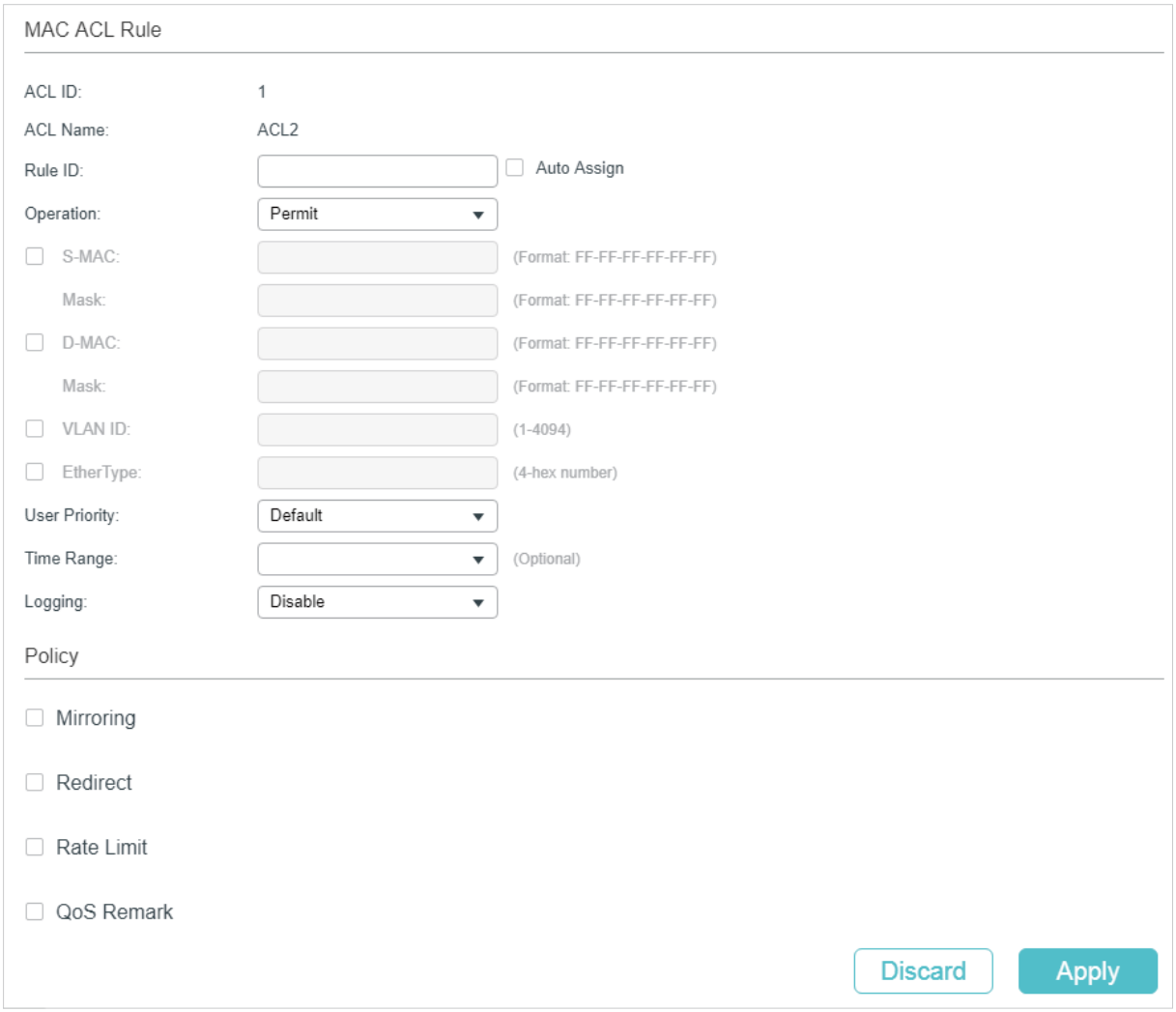
Click **Edit ACL** for a MAC ACL entry to load the following page.

Figure 2-3 Configuring the MAC ACL Rule



In **ACL Rules Table** section, click Add and the following page will appear.

Figure 2-4 Configuring the MAC ACL Rule



Follow these steps to configure the MAC ACL rule:

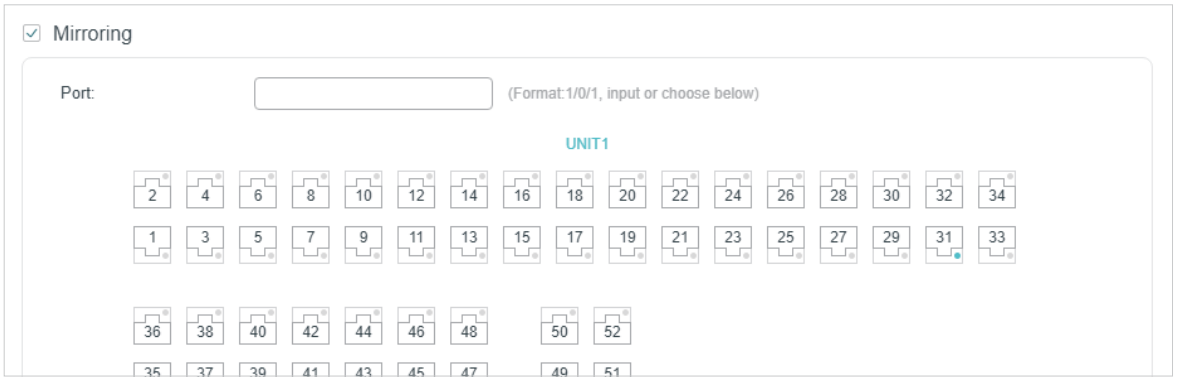
1) In the **MAC ACL Rule** section, configure the following parameters:

Rule ID	Enter an ID number to identify the rule. It should not be the same as any current rule ID in the same ACL. If you select Auto Assign, the rule ID will be assigned automatically and the interval between rule IDs is 5.
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.
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 MAC 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.
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. The Time Range referenced here can be created on the **SYSTEM > Time Range** page.
Logging	Enable Logging function for the ACL rule. Then the times that the rule is matched will be logged every 5 minutes and a related trap will be generated. You can refer to Total Matched Counter in the ACL Rules Table to view the matching times.

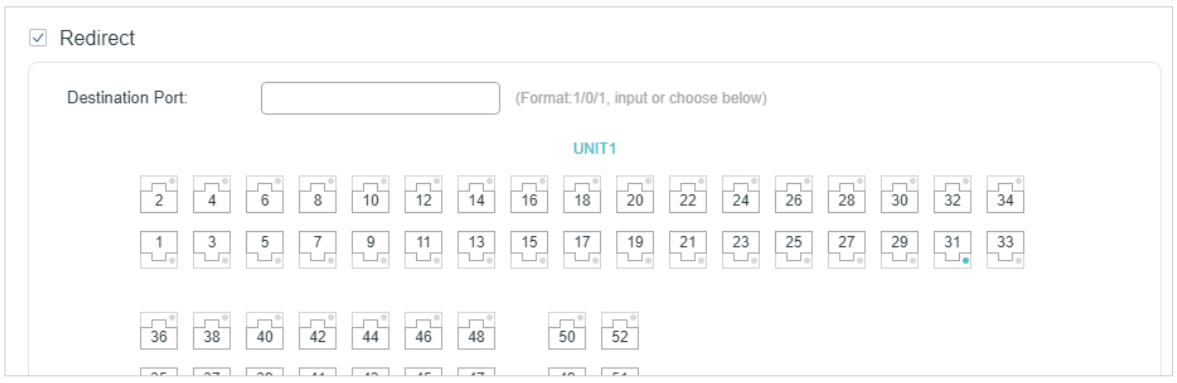
2) In the **Policy** section, enable or disable the Mirroring feature for the matched packets. With this option enabled, choose a destination port to which the packets will be mirrored.

Figure 2-5 Configuring Mirroring



3) In the **Policy** section, enable or disable the Redirect feature for the matched packets. With this option enabled, choose a destination port to which the packets will be redirected.

Figure 2-6 Configuring Redirect

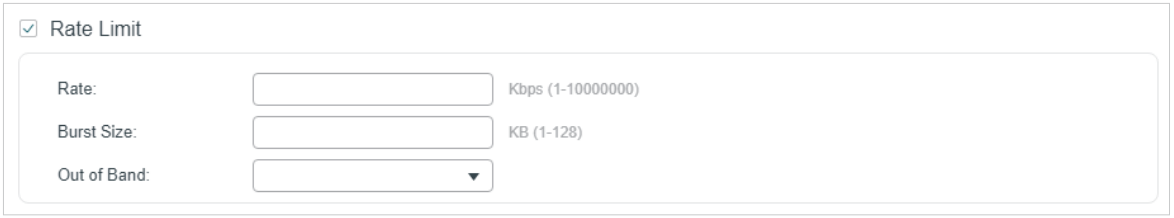


Note:

In the Mirroring feature, the matched packets will be copied to the destination port and the original forwarding will not be affected. While in the Redirect feature, the matched packets will be forwarded only on the destination port.

4) In the **Policy** section, enable or disable the Rate Limit feature for the matched packets. With this option enabled, configure the related parameters.

Figure 2-7 Configuring Rate Limit



Rate	Specify the transmission rate for the matched packets.
Burst Size	Specify the maximum number of bytes allowed in one second.
Out of Band	Select the action for the packets whose rate is beyond the specified rate. **None:** The packets will be forwarded normally. **Drop:** The packets will be discarded. **Remark DSCP:** You can specify a DSCP value, and the DSCP field of the packets will be changed to the specified one.

5) In the **Policy** section, enable or disable the QoS Remark feature for the matched packets. With this option enabled, configure the related parameters, and the remarked values will take effect in the QoS processing on the switch.

Figure 2-8 Configuring QoS Remark



DSCP	Specify the DSCP field for the matched packets. The DSCP field of the packets will be changed to the specified one.
Local Priority	Specify the local priority for the matched packets. The local priority of the packets will be changed to the specified one.
802.1p Priority	Specify the 802.1p priority for the matched packets. The 802.1p priority of the packets will be changed to the specified one.

6) Click **Apply**.

Configuring IP ACL Rule

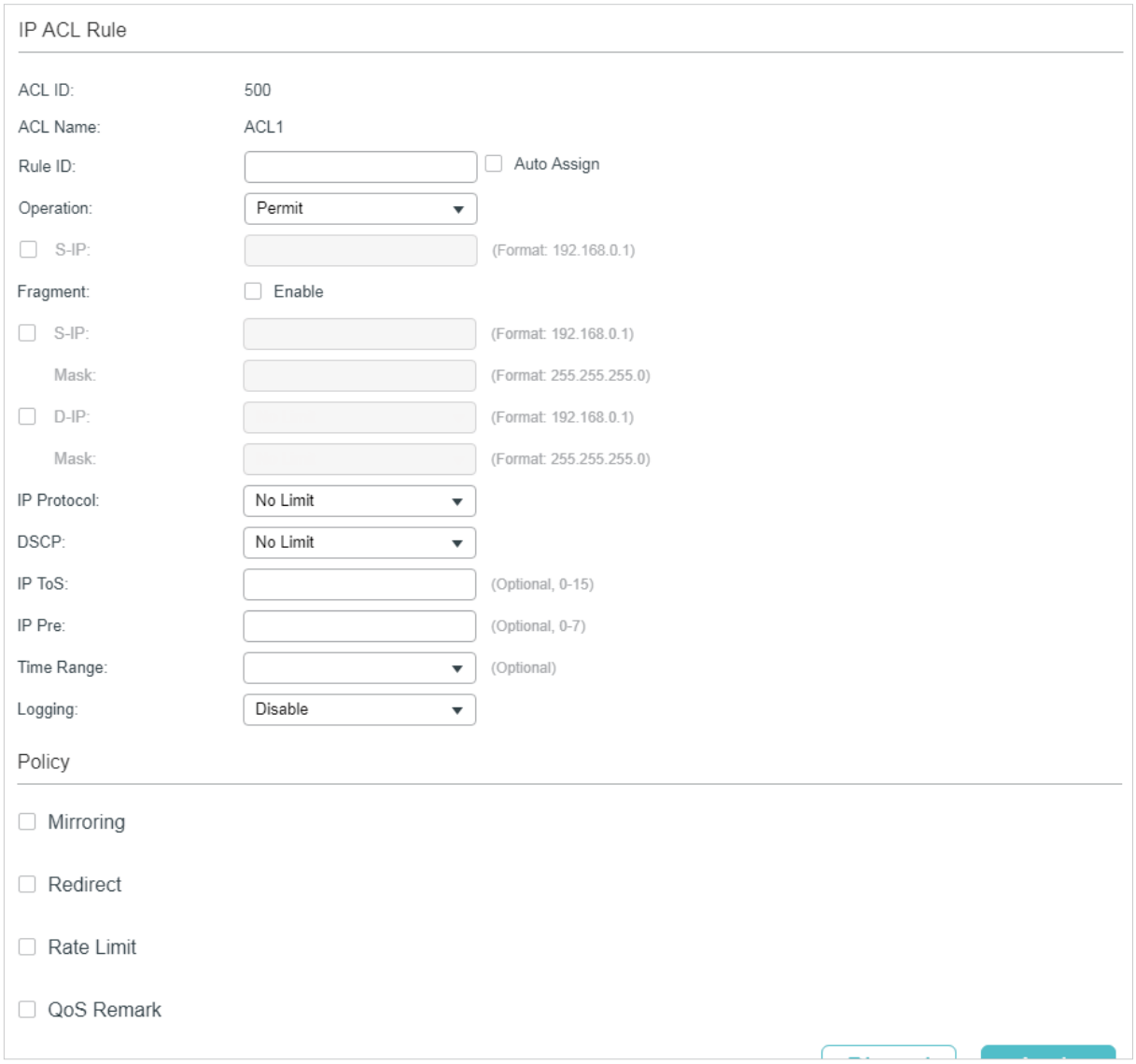
Click **Edit ACL** for an IP ACL entry to load the following page.

Figure 2-9 Configuring the IP ACL Rule



In **ACL Rules Table** section, click Add and the following page will appear.

Figure 2-10 Configuring the IP ACL Rule



Follow these steps to configure the IP ACL rule:

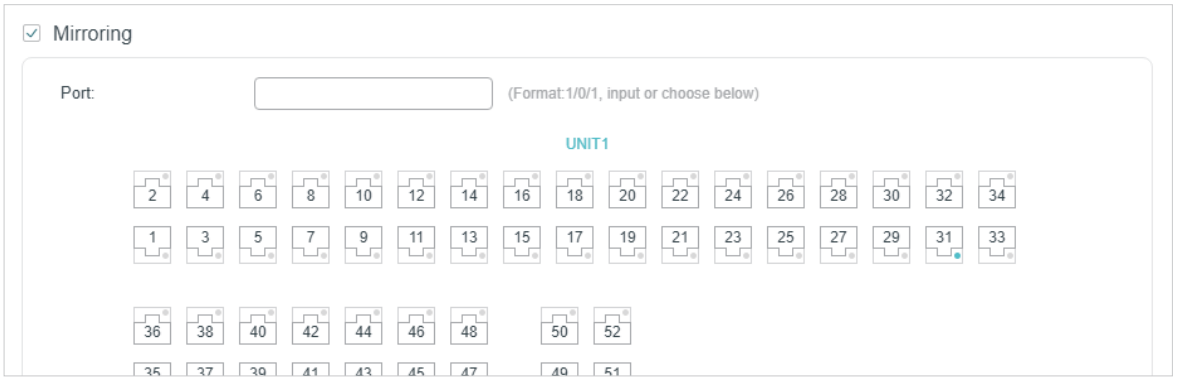
1) In the **IP ACL Rule** section, configure the following parameters:

Rule ID	Enter an ID number to identify the rule. It should not be the same as any current rule ID in the same ACL. If you select Auto Assign, the rule ID will be assigned automatically and the interval between rule IDs is 5.
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.
Fragment	With this option selected, the rule will be applied to all fragment packets except for the last fragment packet in the fragment packet group.
S-IP/Mask	Enter 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	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.
IP Protocol	Select a protocol type from the drop-down list. The default is No Limit, which indicates that packets of all protocols will be matched. You can also select User-defined to customize the IP protocol.
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	If TCP/UDP is selected as the IP protocol, specify the source and destination port number with a mask. **Value**: Specify the port number. **Mask**: Specify the port mask with 4 hexadacimal numbers.
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.
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. The Time Range referenced here can be created on the **SYSTEM > Time Range** page.
Logging	Enable Logging function for the ACL rule. Then the times that the rule is matched will be logged every 5 minutes and a related trap will be generated. You can refer to Total Matched Counter in the ACL Rules Table to view the matching times.

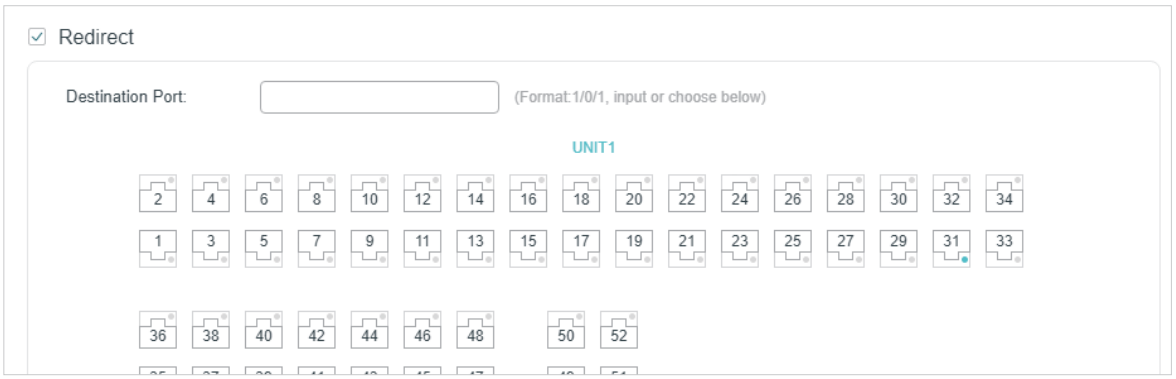
2) In the **Policy** section, enable or disable the Mirroring feature for the matched packets. With this option enabled, choose a destination port to which the packets will be mirrored.

Figure 2-11 Configuring Mirroring



3) In the **Policy** section, enable or disable the Redirect feature for the matched packets. With this option enabled, choose a destination port to which the packets will be redirected.

Figure 2-12 Configuring Redirect

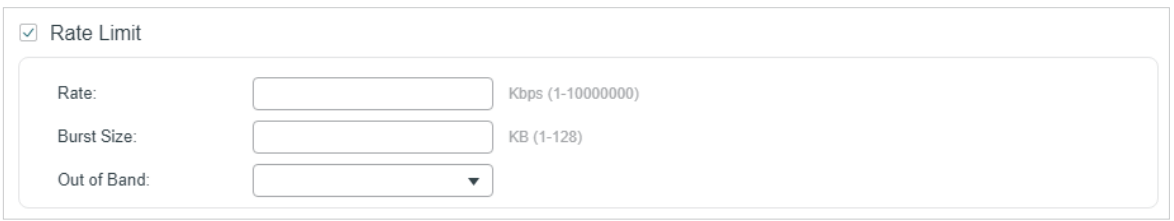


Note:

In the Mirroring feature, the matched packets will be copied to the destination port and the original forwarding will not be affected. While in the Redirect feature, the matched packets will be forwarded only on the destination port.

4) In the **Policy** section, enable or disable the Rate Limit feature for the matched packets. With this option enabled, configure the related parameters.

Figure 2-13 Configuring Rate Limit

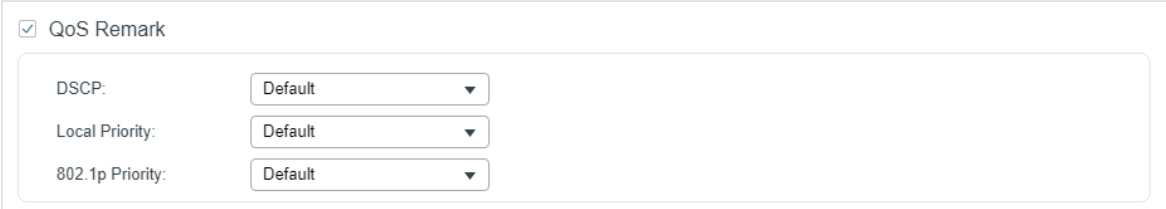


Rate	Specify the transmission rate for the matched packets.
Burst Size	Specify the maximum number of bytes allowed in one second.

Out of Band	Select the action for the packets whose rate is beyond the specified rate. **None:** The packets will be forwarded normally. **Drop:** The packets will be discarded. **Remark DSCP:** You can specify a DSCP value, and the DSCP field of the packets will be changed to the specified one.

5) In the **Policy** section, enable or disable the QoS Remark feature for the matched packets. With this option enabled, configure the related parameters, and the remarked values will take effect in the QoS processing on the switch.

Figure 2-14 Configuring QoS Remark



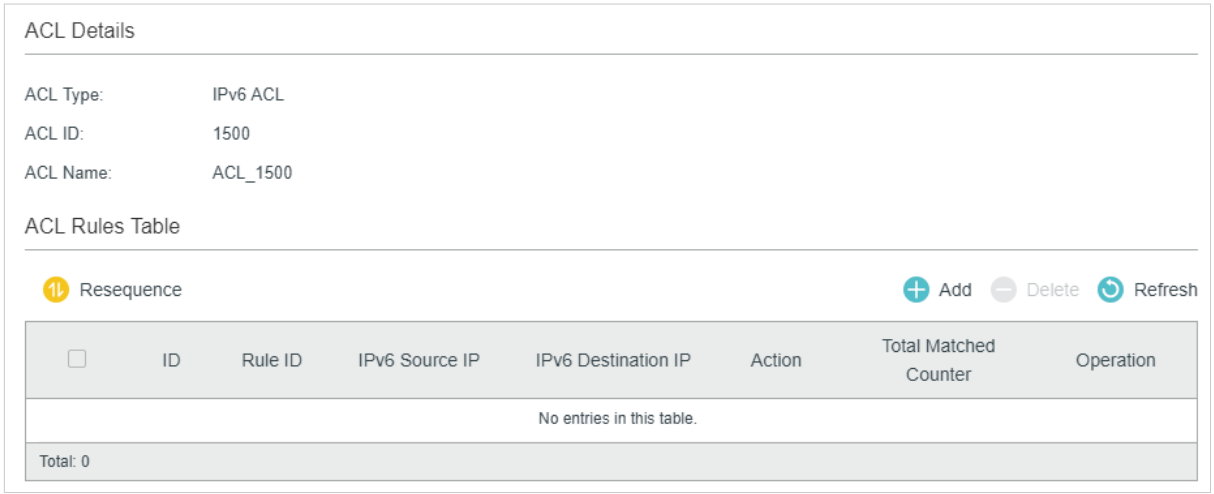
DSCP	Specify the DSCP field for the matched packets. The DSCP field of the packets will be changed to the specified one.
Local Priority	Specify the local priority for the matched packets. The local priority of the packets will be changed to the specified one.
802.1p Priority	Specify the 802.1p priority for the matched packets. The 802.1p priority of the packets will be changed to the specified one.

6) Click **Apply**.

Configuring the IPv6 ACL Rule

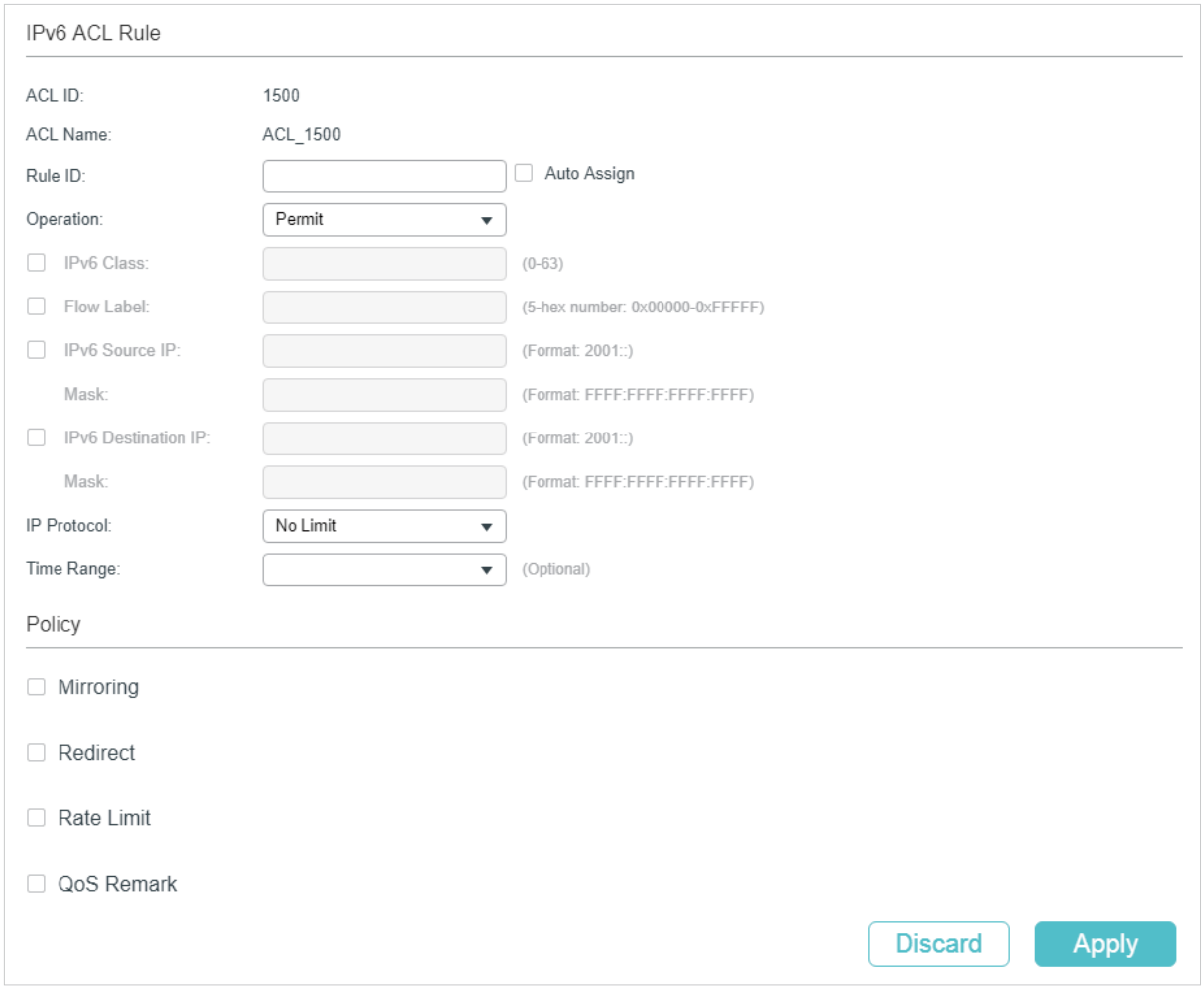
Click **Edit ACL** for an IPv6 ACL entry to load the following page.

Figure 2-15 Configuring the IPv6 ACL Rule



In **ACL Rules Table** section, click Add and the following page will appear.

Figure 2-16 Configuring the IPv6 ACL Rule



Follow these steps to configure the IPv6 ACL rule:

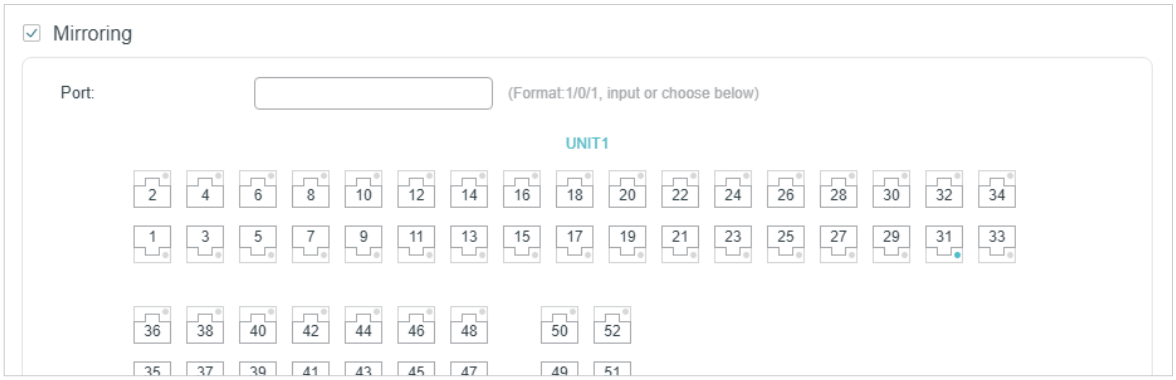
1) In the **IPv6 ACL Rule** section, configure the following parameters:

Rule ID	Enter an ID number to identify the rule. It should not be the same as any current rule ID in the same ACL. If you select Auto Assign, the rule ID will be assigned automatically and the interval between rule IDs is 5.
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.
IPv6 Class	Specify an IPv6 class value to be matched. The switch will check the class field of the IPv6 header.
Flow Label	Specify a Flow Label value to be matched.
IPv6 Source 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	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.
IP Protocol	Select a protocol type from the drop-down list. **No Limit:** Packets of all protocols will be matched. **UDP:** Specify the source port and destination port for the UDP packet to be matched. **TCP**: Specify the source port and destination port for the TCP packet to be matched. **User-defined**: You can customize an IP protocol.
S-Port / D-Port	If TCP/UDP is selected as the IP protocol, specify the source and destination port numbers.
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. The Time Range referenced here can be created on the **SYSTEM > Time Range** page.

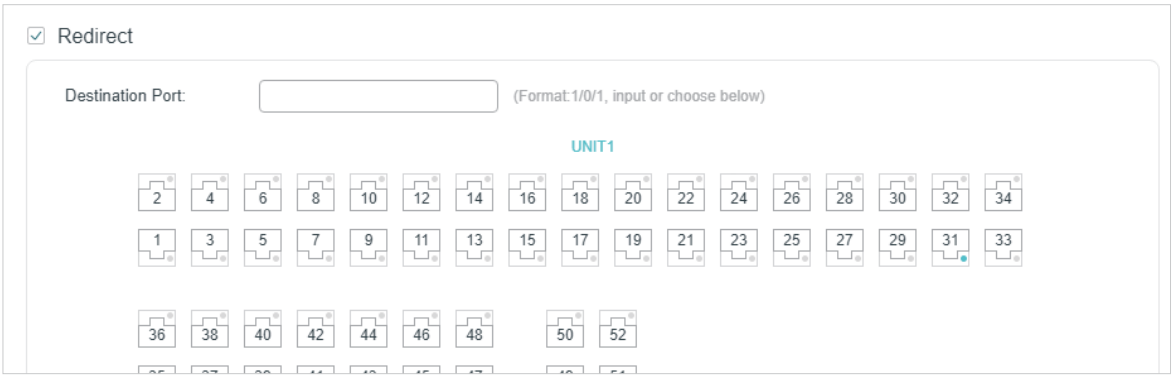
2) In the **Policy** section, enable or disable the Mirroring feature for the matched packets. With this option enabled, choose a destination port to which the packets will be mirrored.

Figure 2-17 Configuring Mirroring



3) In the **Policy** section, enable or disable the Redirect feature for the matched packets. With this option enabled, choose a destination port to which the packets will be redirected.

Figure 2-18 Configuring Redirect

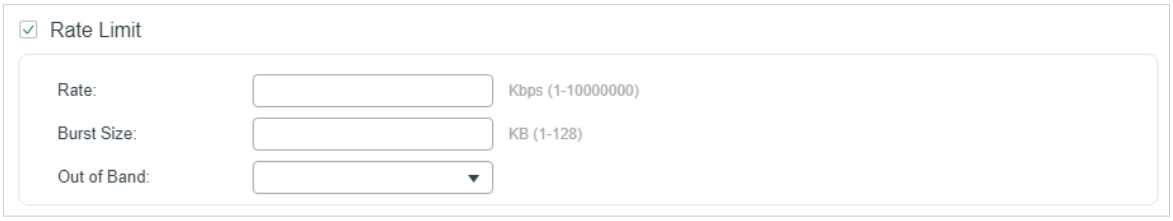


Note:

In the Mirroring feature, the matched packets will be copied to the destination port and the original forwarding will not be affected. While in the Redirect feature, the matched packets will be forwarded only on the destination port.

4) In the **Policy** section, enable or disable the Rate Limit feature for the matched packets. With this option enabled, configure the related parameters.

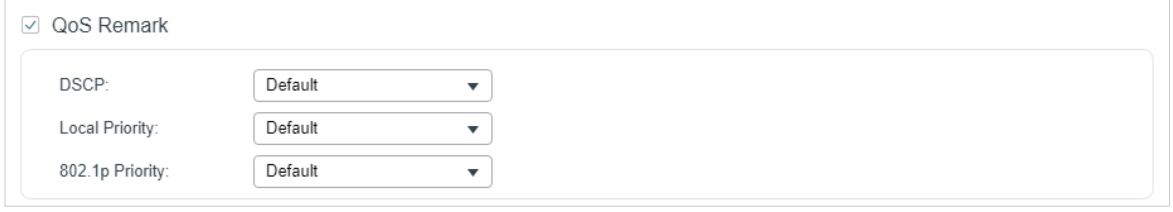
Figure 2-19 Configuring Rate Limit



Rate	Specify the transmission rate for the matched packets.
Burst Size	Specify the number of bytes allowed in one second.
Out of Band	Select the action for the packets whose rate is beyond the specified rate. **None:** The packets will be forwarded normally. **Drop:** The packets will be discarded. **Remark DSCP:** You can specify a DSCP value, and the DSCP field of the packets will be changed to the specified one.

5) In the **Policy** section, enable or disable the QoS Remark feature for the matched packets. With this option enabled, configure the related parameters, and the remarked values will take effect in the QoS processing on the switch.

Figure 2-20 Configuring QoS Remark



DSCP	Specify the DSCP field for the matched packets. The DSCP field of the packets will be changed to the specified one.
Local Priority	Specify the local priority for the matched packets. The local priority of the packets will be changed to the specified one.
802.1p Priority	Specify the 802.1p priority for the matched packets. The 802.1p priority of the packets will be changed to the specified one.

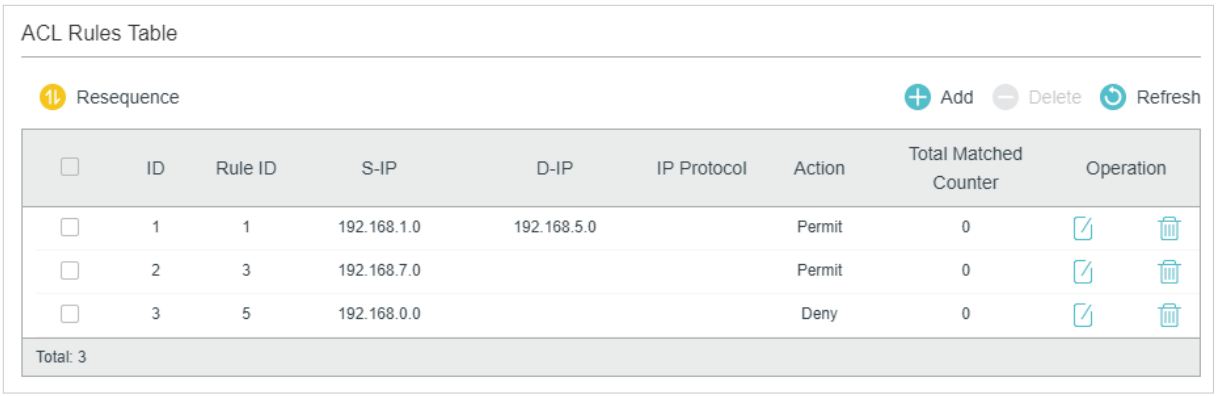
6) Click **Apply**.

Viewing the ACL Rules

The rules in an ACL are listed in ascending order of their rule IDs. The switch matches a received packet with the rules in order. When a packet matches a rule, the switch stops the match process and performs the action defined in the rule.

Click **Edit ACL** for an entry you have created and you can view the rule table. We take IP ACL rules table for example.

Figure 2-21 Viewing ACL Rules Table



Here you can view and edit the ACL rules. You can also click **Resequence** to resequence the rules by providing a Start Rule ID and Step value.

2.1.4 Configuring ACL Binding

You can bind the ACL to a port or a VLAN. The received packets on the port or in the VLAN will then be matched and processed according to the ACL rules. An ACL takes effect only after it is bound to a port or VLAN.

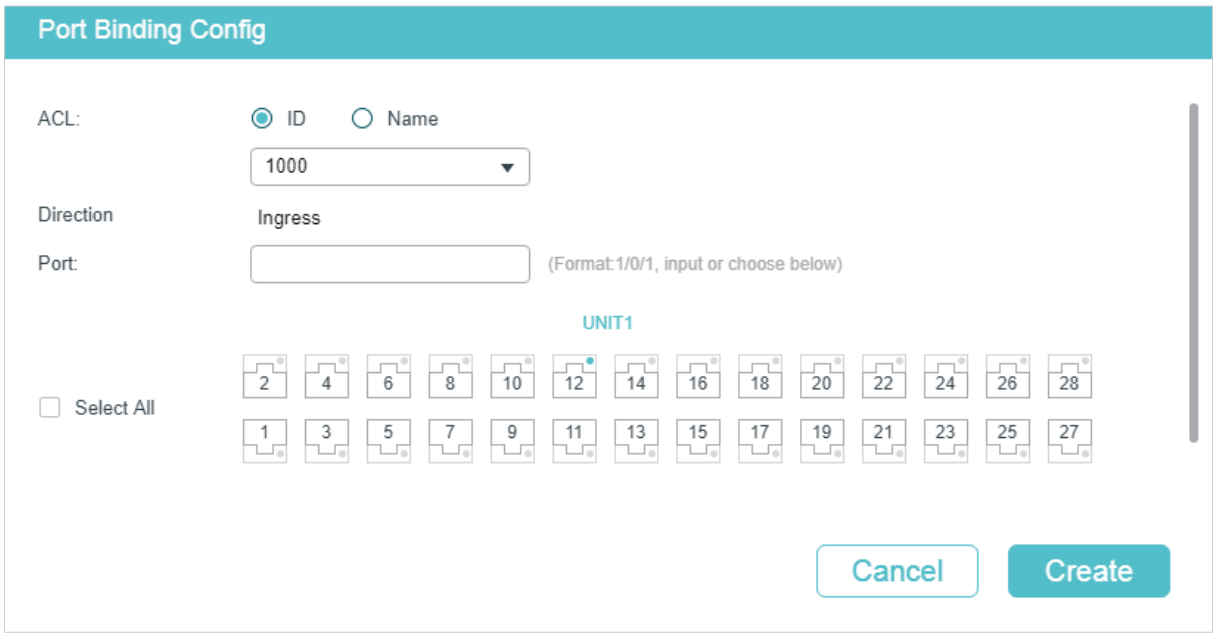
Note:

- Different types of ACLs cannot be bound to the same port or VLAN.
- Multiple ACLs of the same type can be bound to the same port or VLAN. The switch matches the received packets using the ACLs in order. The ACL that is bound earlier has a higher priority.

Binding the ACL to a Port

Choose the menu **SECURITY > ACL > ACL Binding > Port Binding** and click Add to load the following page.

Figure 2-22 Binding the ACL to a Port



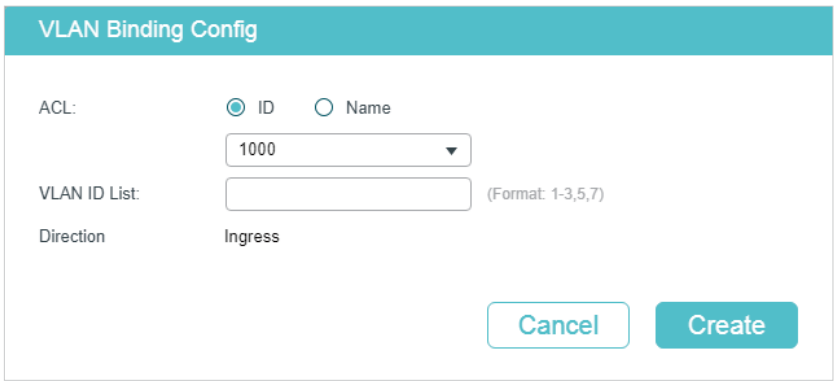
Follow these steps to bind the ACL to a Port:

1) Choose ID or Name to be used for matching the ACL. Then select an ACL from the drop-down list.
2) Specify the port to be bound.
3) Click **Create**.

Binding the ACL to a VLAN

Choose the menu **SECURITY > ACL > ACL Binding > VLAN Binding** to load the following page.

Figure 2-23 Binding the ACL to a VLAN



Follow these steps to bind the ACL to a VLAN:

1) Choose ID or Name to be used for matching the ACL. Then select an ACL from the drop-down list.
2) Enter the ID of the VLAN to be bound.
3) Click **Create**.

2.2 Using the CLI

2.2.1 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 a time range for the ACL. For details about Time Range Configuration, please refer to *Managing System*.

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	**access-list create** *acl-id* **[name** *acl-name***]** Create a MAC ACL. *acl-id*: Enter an ACL ID. The ID ranges from 0 to 499. *acl-name*: Enter a name to identify the ACL.

Step 3	**access-list mac** *acl-id-or-name* **rule** { auto | *rule-id* } { deny | permit } **logging** {enable | disable} [**smac** *source-mac* **smask** *source-mac-mask*] [**dmac** *destination-mac* **dmask** *destination-mac-mask*] [**type** ether-type] [**pri** *dot1p-priority*] [**vid** *vlan-id*] [**tseg** *time-range-name*] Add a MAC ACL Rule. *acl-id-or-name*: Enter the ID or name of the ACL that you want to add a rule for. *auto:* The rule ID will be assigned automatically and the interval between rule IDs is 5. *rule-id*: Assign an ID to the rule. deny | permit: Specify the action to be taken with the packets that match the rule. By default, it is set to permit. The packets will be discarded if “deny” is selected and forwarded if “permit” is selected. **logging** {enable | disable}: Enable or disable Logging function for the ACL rule. If "enable" is selected, the times that the rule is matched will be logged every 5 minutes. With ACL Counter trap enabled, a related trap will be generated if the matching times changes. *source-mac*: Enter the source MAC address. The format is FF:FF:FF:FF:FF:FF. *source-mac-mask*: Enter the mask of the source MAC address. This is required if a source MAC address is entered. The format is FF:FF:FF:FF:FF:FF. *destination-mac*: Enter the destination MAC address. The format is FF:FF:FF:FF:FF:FF. *destination-mac-mask*: Enter the mask of the destination MAC address. This is required if a destination MAC address is entered. The format is FF:FF:FF:FF:FF:FF. ether-type: Specify an Ethernet-type with 4 hexadecimal numbers. *dot1p-priority*: The user priority ranges from 0 to 7. The default is No Limit. *vlan-id*: The VLAN ID ranges from 1 to 4094. *time-range-name*: The name of the time-range. The default is No Limit.
Step 4	**exit** Return to global configuration mode.
Step 5	**show access-list** [*acl-id-or-name*] Display the current ACL configuration. *acl-id-or-name*: The ID number or name 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)#access-list create 50

Switch(config-mac-acl)#access-list mac 50 **rule** 5 **permit logging** disable **smac** 00:34:A2:D4:34:B5 **smask** FF:FF:FF:FF:FF:FF

Switch(config-mac-acl)#exit

Switch(config)#show access-list 50

MAC access list 50 name: ACL_50

rule 5 permit logging disable smac 00:34:a2:d4:34:b5 smask ff:ff:ff:ff:ff:ff

Switch(config)#end

Switch#copy running-config startup-config

IP ACL

Step 1	**configure** Enter global configuration mode.
Step 2	**access-list create** *acl-id* **[name** *acl-name***]** Create an IP ACL. *acl-id*: Enter an ACL ID. The ID ranges from 500 to 999. *acl-name*: Enter a name to identify the ACL.
Step 3	**access-list ip** *acl-id-or-name* **rule** {auto | *rule-id* } {deny | permit} **logging** {enable | disable} [**sip** *sip-address* **sip-mask** *sip-address-mask*] [**dip** *dip-address* **dip-mask** *dip-address-mask*] [**dscp** *dscp-value*] [**tos** *tos-value*] [**pre** *pre-value*] [**frag** {enable | disable}] [**protocol** *protocol* [**s-port** *s-port-number* **s-port-mask** *s-port-mask*] [**d-port** *d-port-number* **d-port-mask** *d-port-mask*] [**tcpflag** *tcpflag*]] [**tseg** *time-range-name*] Add rules to the ACL. *acl-id-or-name*: Enter the ID or name of the ACL that you want to add a rule for. *auto:* The rule ID will be assigned automatically and the interval between rule IDs is 5. *rule-id*: Assign an ID to the rule. deny | permit: Specify the action to be taken with the packets that match the rule. Deny means to discard; permit means to forward. By default, it is set to permit. **logging** {enable | disable}: Enable or disable Logging function for the ACL rule. If "enable" is selected, the times that the rule is matched will be logged every 5 minutes. With ACL Counter trap enabled, a related trap will be generated if the matching times changes. *sip-address:* Enter the source IP address. *sip-address-mask*: Enter the mask of the source IP address. This is required if a source IP address is entered. *dip-address:* Enter the destination IP address. *dip-address-mask:* Enter the mask of the destination IP address. This is required if a destination IP address is entered.

dscp-value: Specify the DSCP value between 0 and 63.

tos-value: Specify an IP ToS value to be matched between 0 and 15.

pre-value: Specify an IP Precedence value to be matched between 0 and 7.

frag {enable | disable}**:** Enable or disable matching of fragmented packets. The default is disable. When enabled, the rule will apply to all fragmented packets and always permit to forward the last fragment of a packet.

protocol: Specify a protocol number between 0 and 255.

s-port-number: With TCP or UDP configured as the protocol, specify the source port number.

s-port-mask: With TCP or UDP configured as the protocol, specify the source port mask with 4 hexadacimal numbers.

d-port-number: With TCP or UDP configured as the protocol, specify the destination port number.

d-port-mask: With TCP or UDP configured as the protocol, specify the destination port mask with 4 hexadacimal numbers.

tcpflag: With TCP configured as the protocol, specify the flag value using either binary numbers or * (for example, 01*010*). The default is *, which indicates that the flag will not be matched.

The flags are URG (Urgent flag), ACK (Acknowledge Flag), PSH (Push Flag), RST (Reset Flag), SYN (Synchronize Flag) and FIN (Finish Flag).

time-range-name: The name of the time-range. The default is No Limit.

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 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 ip 600 **rule** 1 **permit logging** disable **sip** 192.168.1.100 **sip-mask** 255.255.255.255

Switch(config)#show access-list 600

IP access list 600 name: ACL_600

rule 1 permit logging disable sip 192.168.1.100 smask 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 create** *acl-id* **[name** *acl-name***]**

Create an IPv6 ACL.

acl-id: Enter an ACL ID. The ID ranges from 1500 to 1999.

acl-name: Enter a name to identify the ACL.

Step 3 **access-list ipv6** *acl-id-or-name* **rule** {auto | *rule-id* } {deny | permit} **logging** {enable | disable} [**class** *class-value*] [**flow-label** *flow-label-value*] [**sip** *source-ip-address* **sip-mask** *source-ip-mask*] [**dip** *destination-ip-address* **dip-mask** *destination-ip-mask*] [**s-port** *source-port-number*] [**d-port** *destination-port-number*] [**tseg** *time-range-name*]

Add rules to the ACL.

acl-id-or-name: Enter the ID or name of the ACL that you want to add a rule for.

auto: The rule ID will be assigned automatically and the interval between rule IDs is 5.

rule-id: Assign an ID to the rule.

deny | permit: Specify the action to be taken with the packets that match the rule. Deny means to discard; permit means to forward. By default, it is set to permit.

logging {enable | disable}: Enable or disable Logging function for the ACL rule. If "enable" is selected, the times that the rule is matched will be logged every 5 minutes. With ACL Counter trap enabled, a related trap will be generated if the matching times changes.

class-value: Specify a class value to be matched. It ranges from 0 to 63.

flow-label-value: Specify a Flow Label value to be matched.

source-ip-address: Enter the source IP address. Enter the destination IPv6 address to be matched. All types of IPv6 address will be checked. You may enter a complete 128-bit IPv6 address but only the first 64 bits will be valid.

source-ip-mask: Enter the source IP address mask. The mask is required if the source IPv6 address is entered. Enter the mask in complete format (for example, ffff:ffff:0000:ffff). The mask specifies which bits in the source IPv6 address to match the rule.

destination-ip-address: Enter the destination IPv6 address to be matched. All types of IPv6 address will be checked. You may enter a complete 128-bit IPv6 addresses but only the first 64 bits will be valid.

destination-ip-mask: Enter the source IP address mask. The mask is required if the source IPv6 address is entered. Enter the mask in complete format (for example, ffff:ffff:0000:ffff). The mask specifies which bits in the source IPv6 address to match the rule.

source-port-number: Enter the TCP/UDP source port if TCP/UDP protocol is selected.

destination-port-number: Enter the TCP/UDP destination port if TCP/UDP protocol is selected.

time-range-name: The name of the time-range. The default is No Limit.

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 1600 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 1600

Switch(config)#access-list ipv6 1600 **rule** 1 **deny logging** disable **sip** CDCD:910A:2222:5498:8475:1111:3900:2020 **sip-mask** ffff:ffff:ffff:ffff

Switch(config)#show access-list 1600

IPv6 access list 1600 name: ACL_1600

rule 1 deny logging disable 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

Resequencing Rules

You can resequence the rules by providing a Start Rule ID and Step value.

Step 1	**configure** Enter global configuration mode.
Step 2	**access-list resequence** *acl-id-or-name* **start** *start-rule-id* **step** *rule-id-step-value* Resequence the rules of the specific ACL. *acl-id-or-name*: Enter the ID or name of the ACL. *start-rule-id*: Enter the start rule ID. *rule-id-step-value*: Enter the Step 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 resequence the rules of MAC ACL 100: set the start rule ID as 1 and the step value as 10:

Switch#configure

Switch(config)#access-list resequence 100 **start** 1 **step** 10

Switch(config)#show access-list 100

MAC access list 100 name: "ACL_100"

rule 1 deny logging disable smac aa:bb:cc:dd:ee:ff smask ff:ff:ff:ff:ff:ff

rule 11 permit logging disable vid 18

rule 21 permit logging disable dmac aa:cc:ee:ff:dd:33 dmask ff:ff:ff:ff:ff:ff

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 configure the policy actions for an ACL rule.

Step 1	**configure** Enter global configuration mode.
Step 2	**access-list action** *acl-id-or-name* **rule** *rule-id* Configure the policy actions for an ACL rule. *acl-id-or-name*: Enter the ID or name of the ACL. *rule-id*: Enter the ID of the ACL rule.

Step 3	**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* **burst** *burst-size* **osd** { **none | discard | remark dscp** *dscp* } (Optional) Define the policy to monitor the rate of the matched packets. *rate*: Specify a rate from 1 to 1000000 kbps. *burst-size*: Specify the number of bytes allowed in one second ranging from 1 to 128. **osd**: Select either "none", "discard" or "remark dscp" as the action to be taken for the packets whose rate is beyond the specified rate. The default is None. When "remark dscp" is selected, you also need to specify the DSCP value for the matched packets. The DSCP value ranges from 0 to 63. **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 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

Redirect the matched packets to port 1/0/4 for rule 1 of MAC ACL 10:

Switch#configure

Switch(config)#access-list action 10 rule 1

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

Switch(config-action)#exit

Switch(config)#show access-list 10

MAC access list 10 name: ACL_10

rule 5 permit logging disable action redirect Gi1/0/4

Switch(config)#end

Switch#copy running-config startup-config

2.2.4 Configuring ACL Binding

You can bind the ACL to a port or a VLAN. The received packets on the port or in the VLAN will then be matched and processed according to the ACL rules. An ACL takes effect only after it is bound to a port or VLAN.

Note:

- Different types of ACLs cannot be bound to the same port or VLAN.
- Multiple ACLs of the same type can be bound to the same port or VLAN. The switch matches the received packets using the ACLs in order. The ACL that is bound earlier has a higher priority.

Follow the steps below to bind ACL to a port or a VLAN:

Step 1	**configure** Enter global configuration mode
Step 2	**access-list bind** *acl-id-or-name* **interface** { [**vlan** *vlan-list*]	[**fastEthernet** *port-list*]	[**gigabitEthernet** *port-list*]	[**ten-gigabitEthernet** *port-list*] } Bind the ACL to a port or a VLAN. *acl-id-or-name*: Enter the ID or name of the ACL that you want to add a rule for. *vlan-list*: Specify the ID or the ID list of the VLAN(s) that you want to bind the ACL to. The valid values are from 1 to 4094, for example, 2-3,5. *port-list*: Specify the number or the list of the Ethernet port that you want to bind the ACL to.
Step 3	**show access-list bind** View the ACL binding 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 bind ACL 1 to port 3 and VLAN 4:

Switch#configure

Switch(config)#access-list bind 1 **interface vlan** 4 **gigabitEthernet** 1/0/3

SSwitch(config)#show access-list bind

ACL ID ACL NAME Interface/VID Direction Type

1	ACL_1	Gi1/0/3	Ingress	Port
1	ACL_1	4	Ingress	VLAN

Switch(config)#end

Switch#copy running-config startup-config

2.2.5 Viewing ACL Counting

You can use the following command to view the number of matched packets of each ACL in the privileged EXEC mode and any other configuration mode:

show access-list *acl-id-or-name* **counter**

View the number of matched packets of the specific ACL.

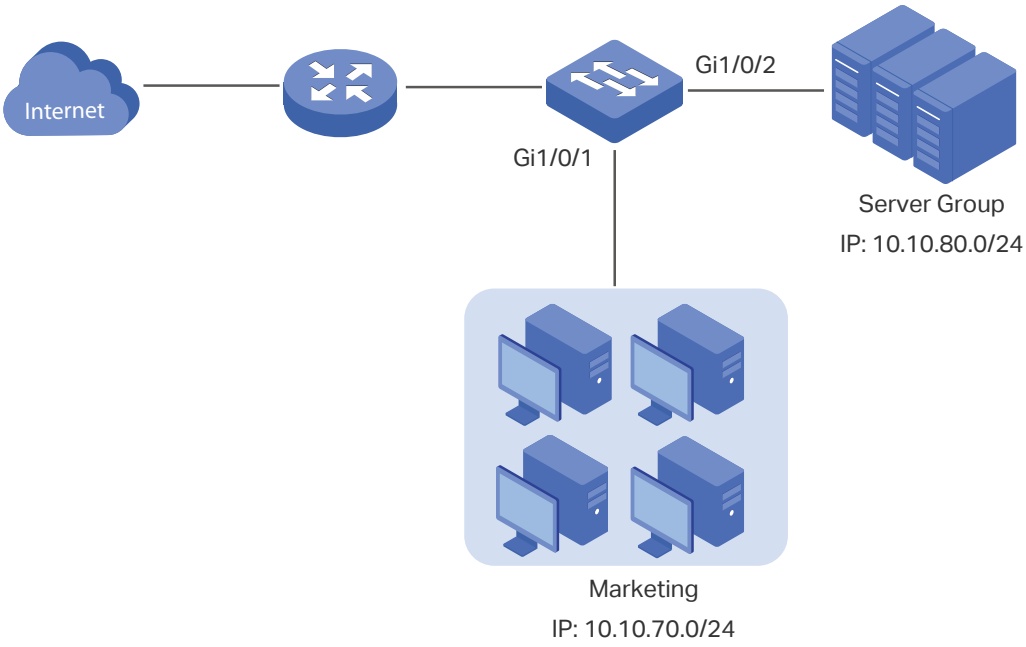
acl-id-or-name: Specify the ID or name of the ACL to be viewed.

3 Configuration Example for ACL

3.1 Network Requirements

As shown below, a company's internal server group can provide different types of services. 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



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 Configuration Scheme

To meet the requirements above, you can set up packet filtering by creating an IP ACL and configuring rules for it.

- ACL Configuration

Create an IP ACL and configure the following rules for it:

- 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.

- Configure four 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.
- Configure a deny rule to match the packets with source IP address 10.10.70.0/24. 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

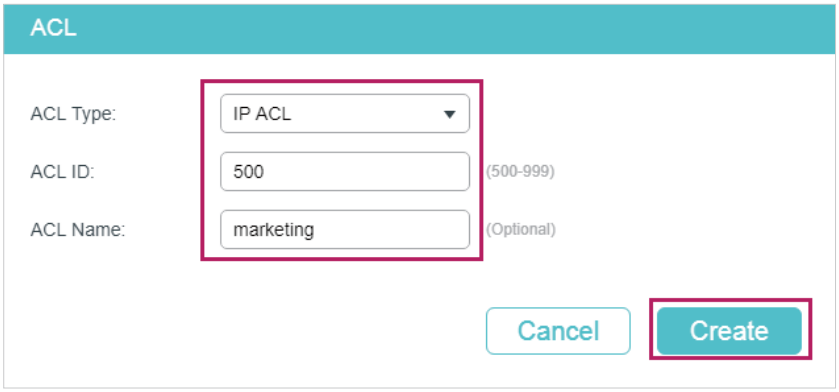
Bind the IP ACL to port 1/0/1 so that the ACL rules will apply to the Marketing department only.

Demonstrated with T1600G-52TS, the following sections explain the configuration procedure in two ways: using the GUI and using the CLI.

3.3 Using the GUI

1) Choose the menu **SECURITY > ACL > ACL Config** and click Add to load the following page. Then create an IP ACL for the marketing department.

Figure 3-2 Creating an IP ACL



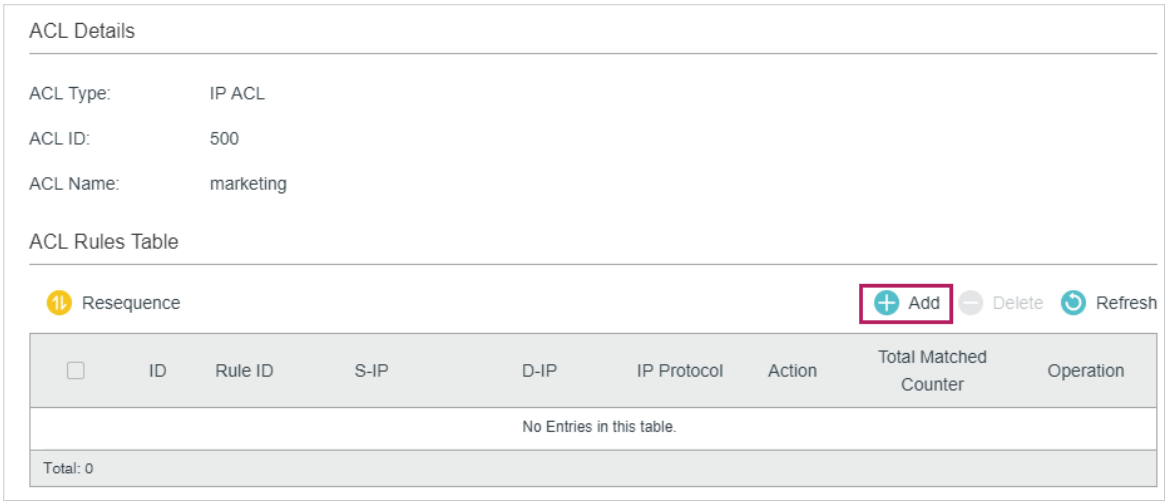
2) Click **Edit ACL** in the Operation column.

Figure 3-3 Editing IP ACL



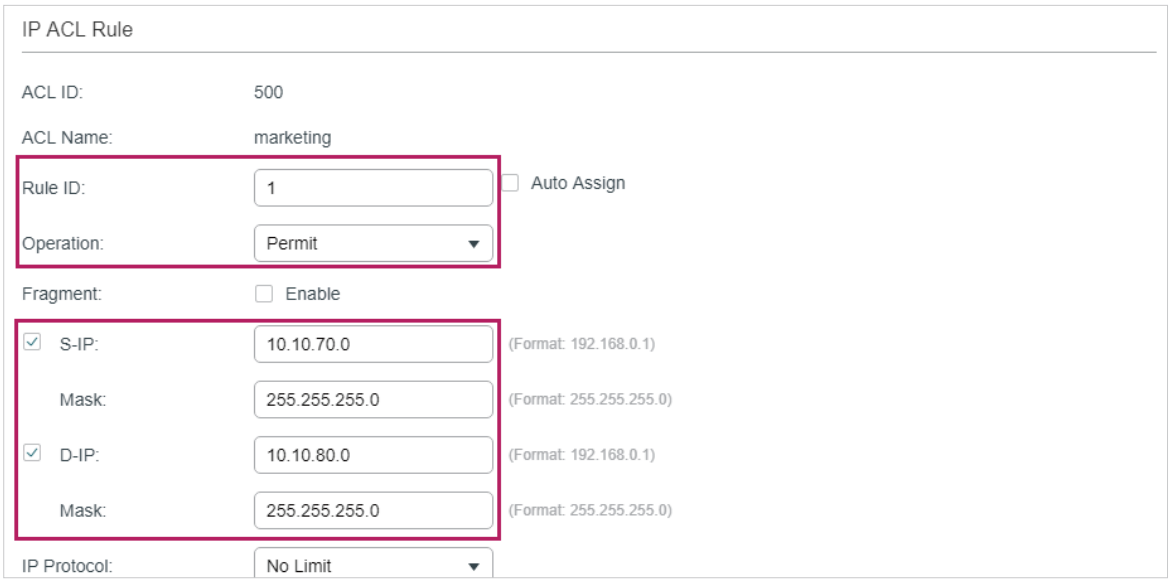
3) On the ACL configuration page, click Add.

Figure 3-4 Editing IP ACL



4) Configure rule 1 to permit packets with the source IP address 10.10.70.0/24 and destination IP address 10.10.80.0/24.

Figure 3-5 Configuring Rule 1



5) In the same way, 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 TCP 443 (https service port).

Figure 3-6 Configuring Rule 2

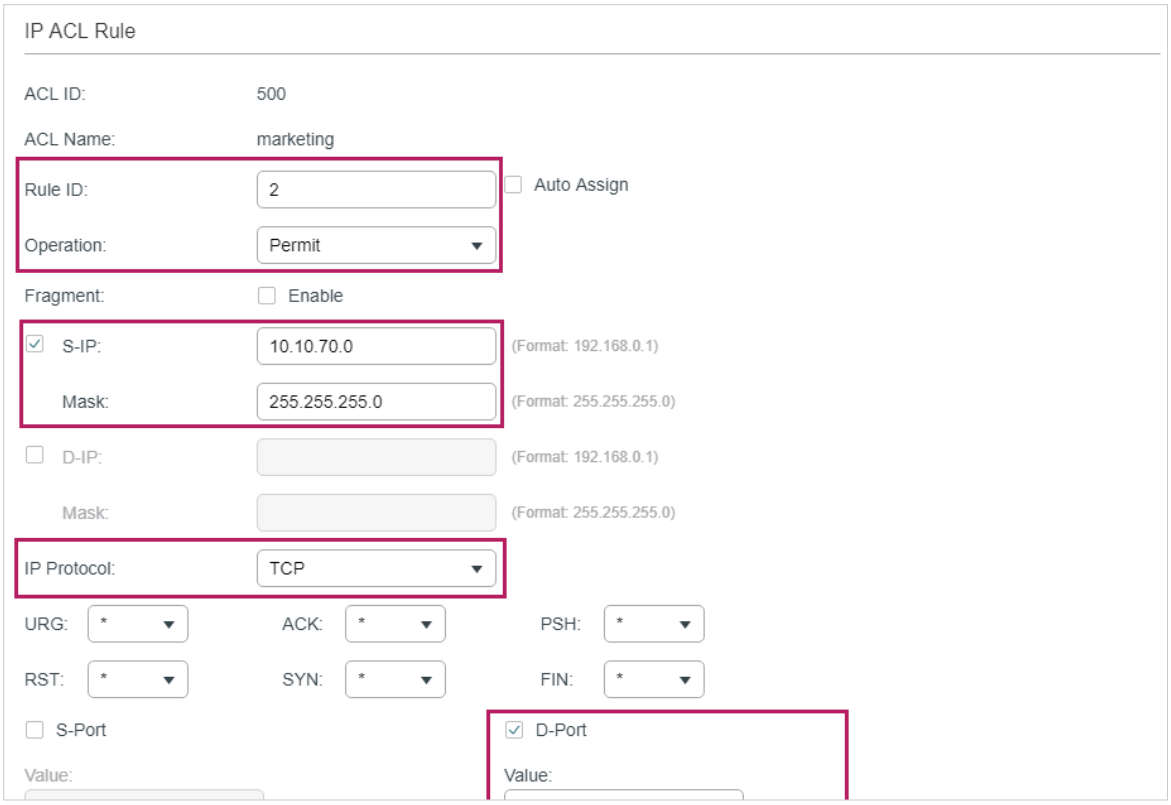
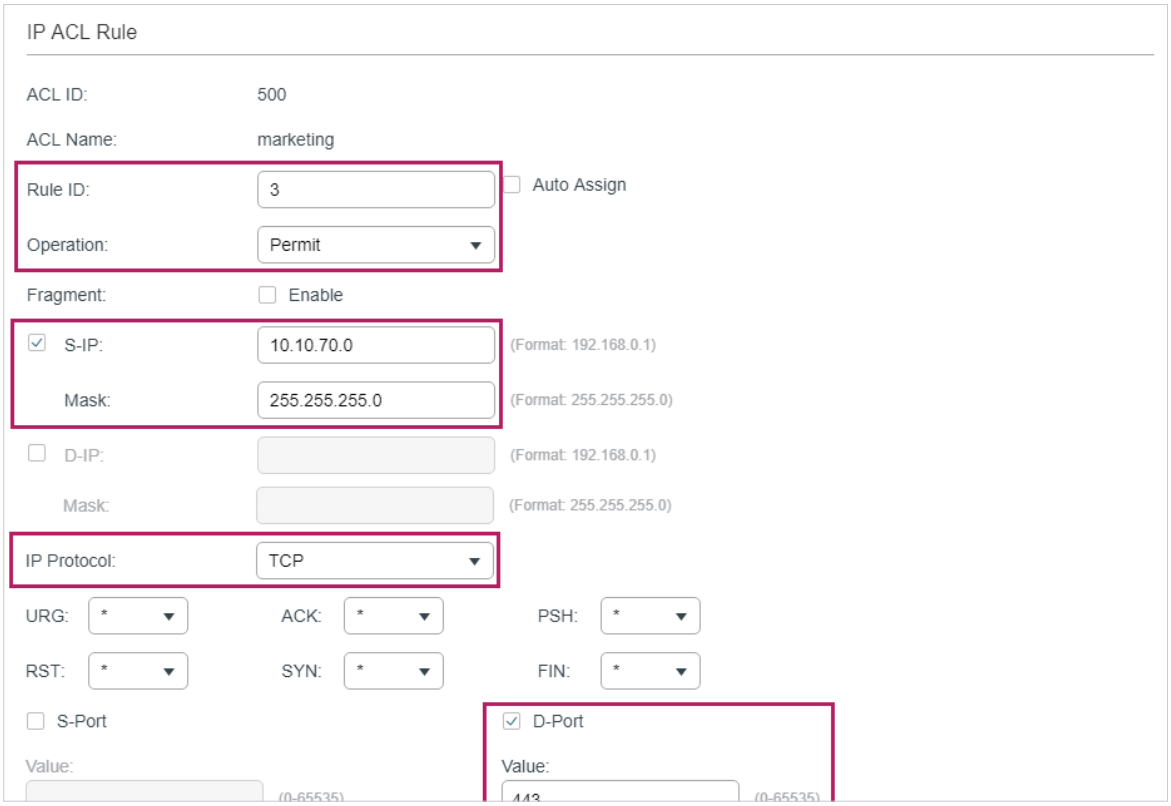


Figure 3-7 Configuring Rule 3



6) In the same way, 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 3-8 Configuring Rule 4

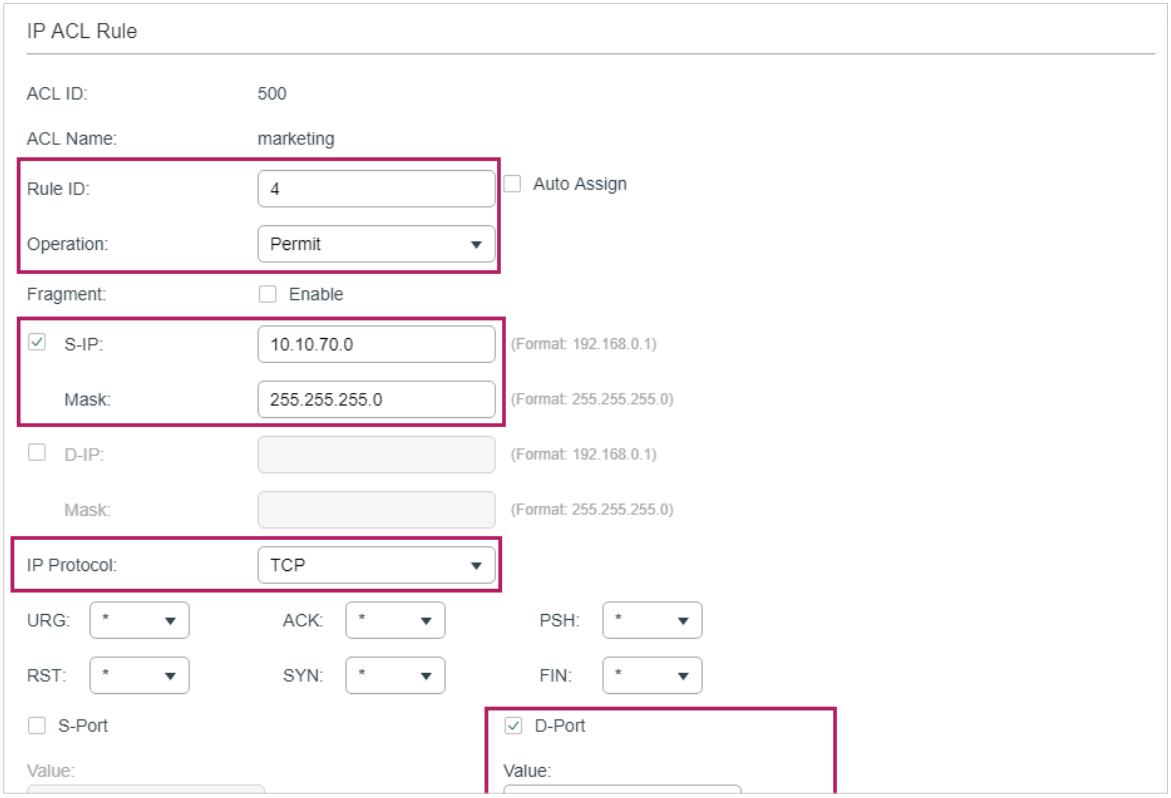
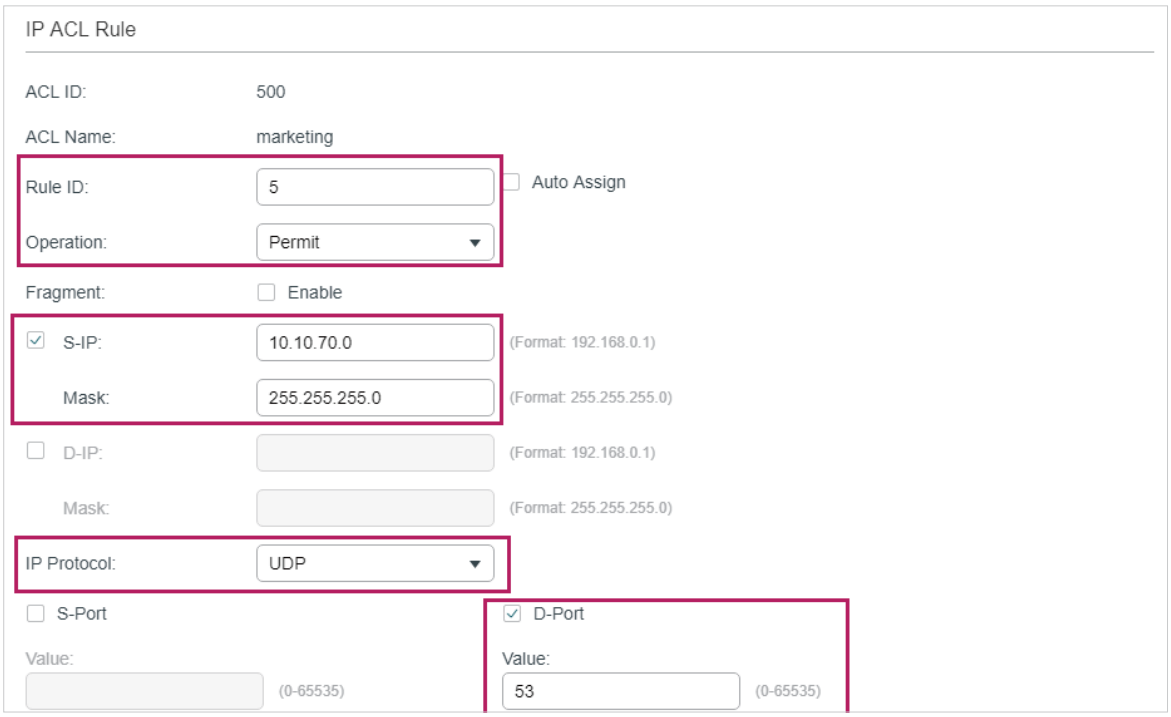
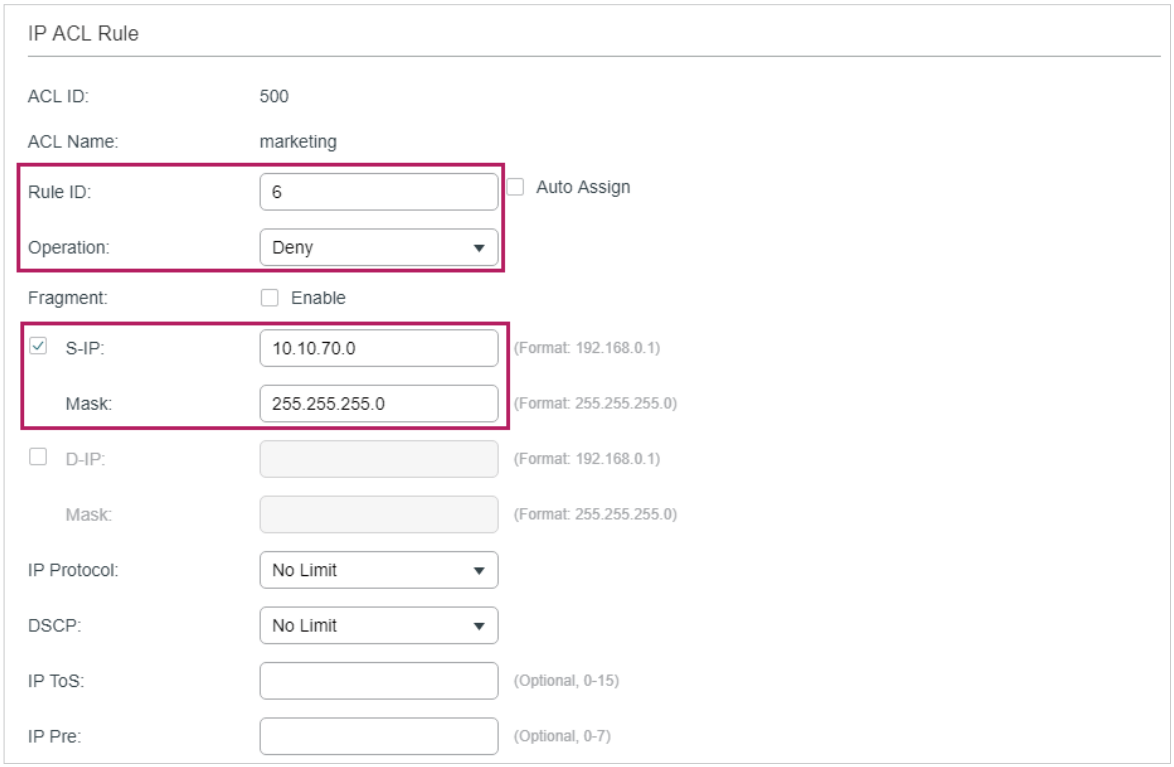


Figure 3-9 Configuring Rule 5



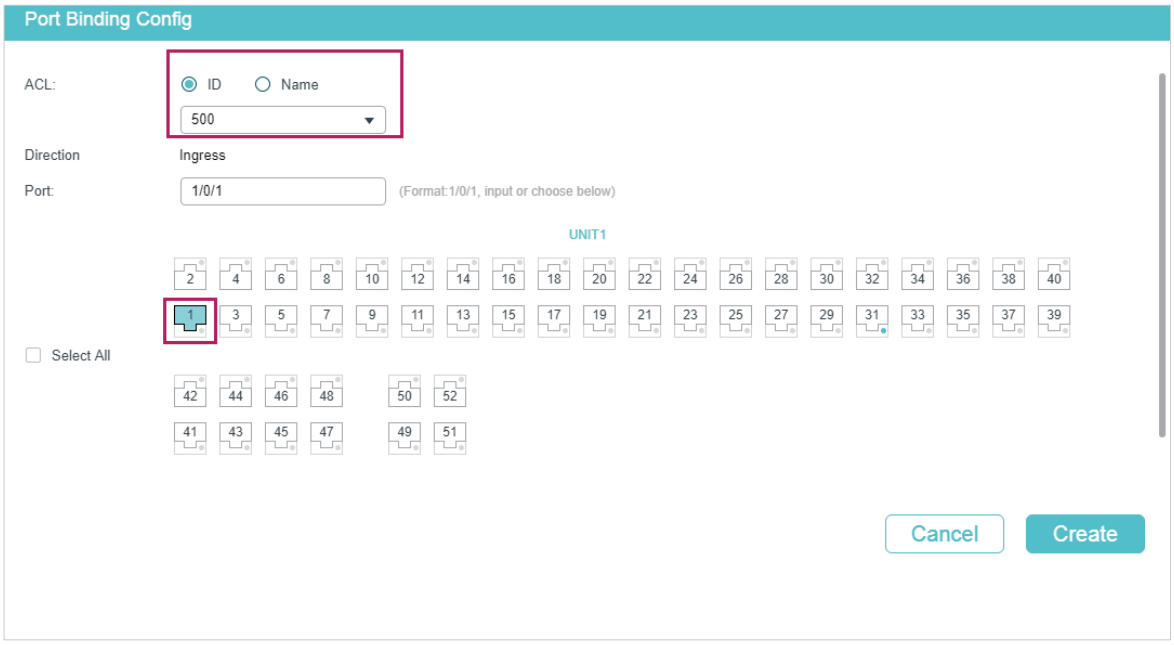
7) In the same way, configure rule 6 to deny packets with source IP 10.10.70.0.

Figure 3-10 Configuring Rule 6



8) Choose the menu **SECURITY > ACL > ACL Binding** and click Add to load 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 to save the settings.

3.4 Using the CLI

1) Create an IP ACL.

Switch#configure

Switch(config)#access-list create 500 name marketing

2) Configure rule 1 to permit packets with source IP 10.10.70.0/24 and destination IP 10.10.80.0/24.

Switch(config)#access-list ip 500 rule 1 permit logging disable sip 10.10.70.0 sip-mask 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 10.10.70.0/24, and destination port TCP 80 (http service port) or TCP 443 (https service port).

Switch(config)#access-list ip 500 rule 2 permit logging disable sip 10.10.70.0 sip-mask 255.255.255.0 protocol 6 d-port 80 d-port-mask ffff

Switch(config)#access-list ip 500 rule 3 permit logging disable sip 10.10.70.0 sip-mask 255.255.255.0 protocol 6 d-port 443 d-port-mask ffff

4) Configure rule 4 and rule 5 to permit packets with source IP 10.10.70.0/24, and destination port TCP53 or UDP 53.

Switch(config)#access-list ip 500 rule 4 permit logging disable sip 10.10.70.0 sip-mask 255.255.255.0 protocol 6 d-port 53 d-port-mask ffff

Switch(config)#access-list ip 500 rule 5 permit logging disable sip 10.10.70.0 sip-amask 255.255.255.0 protocol 17 d-port 53 d-port-mask ffff

5) Configure rule 6 to deny packets with source IP 10.10.70.0/24.

Switch(config)#access-list ip 500 rule 2 deny logging disable sip 10.10.70.0 sip-mask 255.255.255.0

6) Bind ACL500 to port 1.

Switch(config)#access-list bind 500 interface gigabitEthernet 1/0/1

Switch(config)#end

Switch#copy running-config startup-config

Verify the Configurations

Verify the IP ACL 500:

Switch#show access-list 500

rule 1 permit logging disable sip 10.10.70.0 smask 255.255.255.0 dip 10.10.80.0 dmask 255.255.255.0

rule 2 permit logging disable sip 10.10.70.0 smask 255.255.255.0 protocol 6 d-port 80

rule 3 permit logging disable sip 10.10.70.0 smask 255.255.255.0 protocol 6 d-port 443

rule 4 permit logging disable sip 10.10.70.0 smask 255.255.255.0 protocol 6 d-port 53

rule 5 permit logging disable sip 10.10.70.0 smask 255.255.255.0 protocol 17 d-port 53

```
rule 6  deny logging disable sip 10.10.70.0 smask 255.255.255.0
Switch#show access-list bind
ACL ID      ACL NAME            Interface/VID    Direction   Type
------      --------            -------------    --------    ----
500         marketing            Gi1/0/1          Ingress     Port
```

4 Appendix: Default Parameters

The default settings of ACL are listed in the following tables:

Table 4-1 MAC ACL

Parameter	Default Setting
Operation	Permit
User Priority	No Limit
Time-Range	No Limit

Table 4-2 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

Table 4-3 IPv6 ACL

Parameter	Default Setting
Operation	Permit
Time-Range	No Limit

Table 4-4 Policy

Parameter	Default Setting
Mirroring	Disabled
Redirect	Disabled

Parameter	Default Setting
Rate Limit	Disabled
QoS Remark	Disabled

Part 23

Configuring IPv4 IMPB

CHAPTERS

1. IPv4 IMPB
2. IP-MAC Binding Configuration
3. ARP Detection Configuration
4. IPv4 Source Guard Configuration
5. Configuration Examples
6. Appendix: Default Parameters

1 IPv4 IMPB

1.1 Overview

IPv4 IMPB (IP-MAC-Port Binding) is used to bind the IP address, MAC address, VLAN ID and the connected port number of the specified host. Basing on the 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.

1.2 Supported Features

IP-MAC Binding

This feature is used to add binding entries. The binding entries can be manually configured, or learned by ARP scanning or DHCP snooping. The features ARP Detection and IPv4 Source Guard are based on the IP-MAC Binding entries.

ARP Detection

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 Detection can prevent the network from these ARP attacks.

- Prevent ARP Cheating Attacks

Based on the IP-MAC Binding entries, the ARP Detection 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

You can limit the receiving speed of the legal ARP packets on the port to avoid ARP flooding attack.

IPv4 Source Guard

IPv4 Source Guard is used to filter the IPv4 packets based on the IP-MAC Binding table. Only the packets that match the binding rules are forwarded.

2 IP-MAC Binding Configuration

You can add IP-MAC Binding entries in three ways:

- Manual Binding
- Via ARP Scanning
- Via DHCP Snooping

Additionally, you can view, search and edit the entries in the Binding Table.

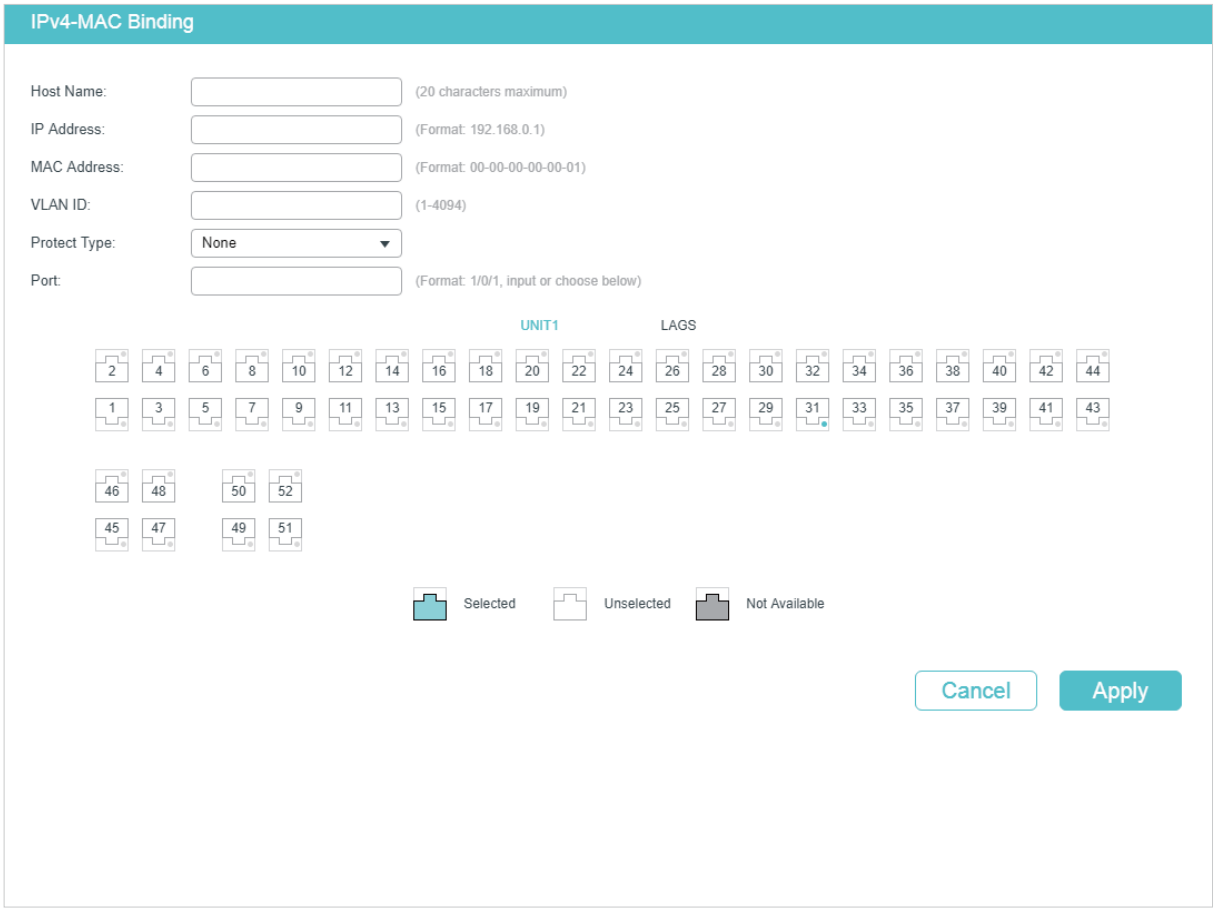
2.1 Using the GUI

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 detailed information of the hosts.

Choose the menu **SECURITY > IPv4 IMPB > IP-MAC Binding > Manual Binding** and click Add to load the following page.

Figure 2-1 Manual Binding



Follow these steps to manually create an IP-MAC Binding entry:

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. The entry will be applied to to the specific feature. The following options are provided: **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 IPv4 Source Guard feature. **Both**: This entry will be applied to both of the features.

3) Enter or select the port that is connected to this host.

4) Click **Apply**.

2.1.2 Binding Entries via ARP Scanning

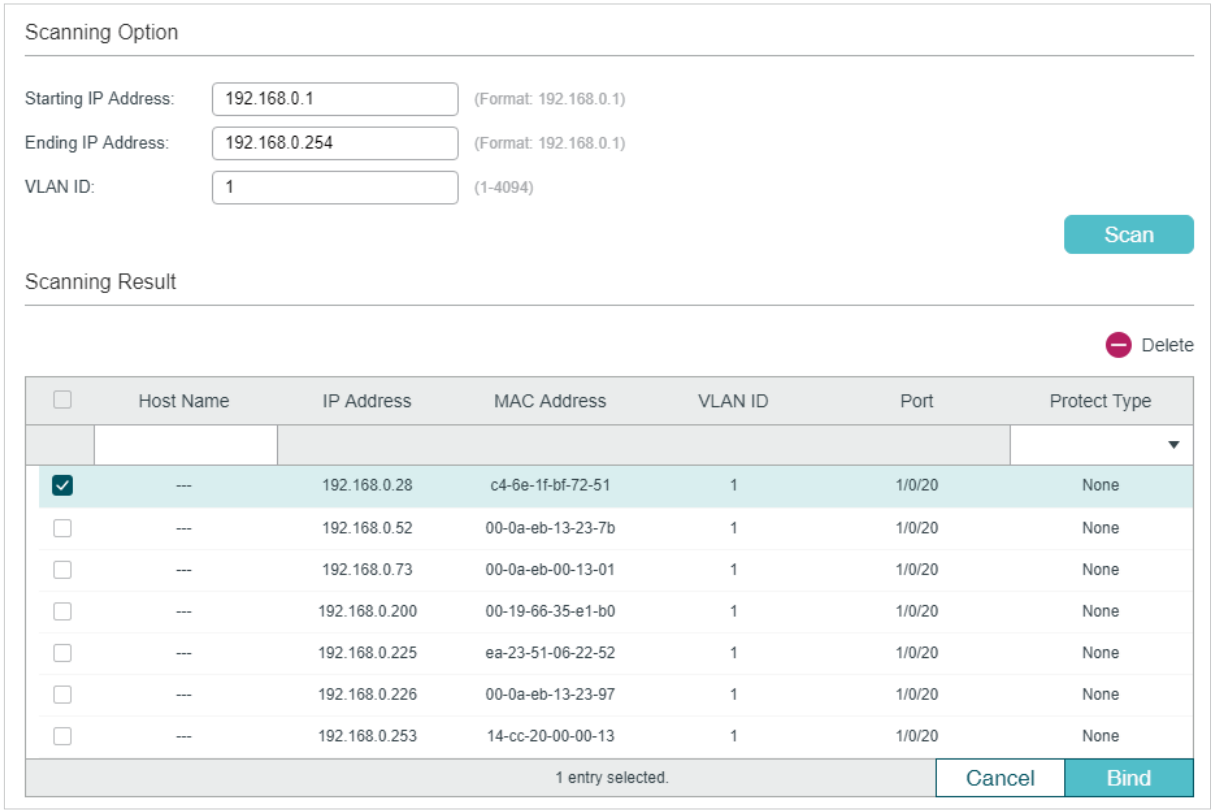
With ARP Scanning, the switch sends the ARP request packets of the specified IP field to the hosts. Upon receiving the ARP reply packet, the switch can get the IP address, MAC address, VLAN ID and the connected port number of the host. You can bind these entries conveniently.

Note:

Before using this feature, make sure that your network is safe and the hosts are not suffering from ARP attacks at present; otherwise, you may obtain incorrect IP-MAC Binding entries. If your network is being attacked, it's recommended to bind the entries manually.

Choose the menu **SECURITY > IPv4 IMPB > 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.

Starting IP Address/Ending 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 **Bind**.

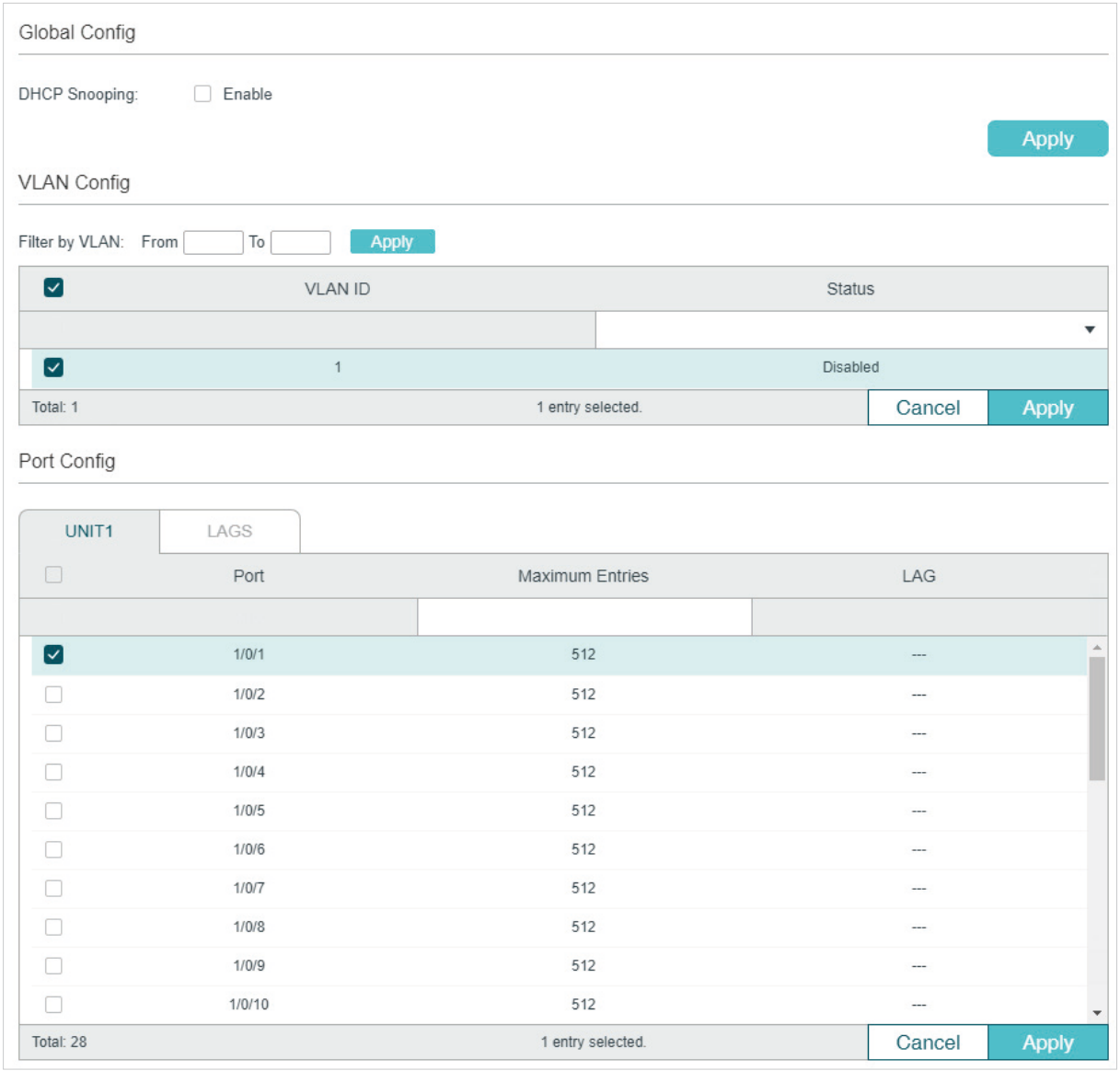
Host Name	Enter a host name for identification.
IP Address	Displays the IP address.
MAC Address	Displays the MAC address.
VLAN ID	Displays the VLAN ID.
Port	Displays the port number.
Protect Type	Select the protect type for the entry. The entry will be applied to to the specific feature. The following options are provided: **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. **Both** This entry will be applied to both of the features.

2.1.3 Binding Entries via 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.

Choose the menu **SECURITY > IPv4 IMPB > IP-MAC Binding > DHCP Snooping** to load the following page.

Figure 2-3 DHCP Snooping



Follow these steps to configure IP-MAC Binding via DHCP Snooping:

1) In the **Global Config** section, globally enable DHCP Snooping. Click **Apply**.

2) In the **VLAN Config** section, enable DHCP Snooping on a VLAN or range of VLANs. Click **Apply**.

VLAN ID	Displays the VLAN ID.
Status	Enable or disable DHCP Snooping on the VLAN.

3) In the **Port Config** section, configure the maximum number of binding entries a port can learn via DHCP snooping. Click **Apply**.

Port	Displays the port number.

Maximum Entries	Configure the maximum number of binding entries a port can learn via DHCP snooping
LAG	Displays the LAG that the port is in.

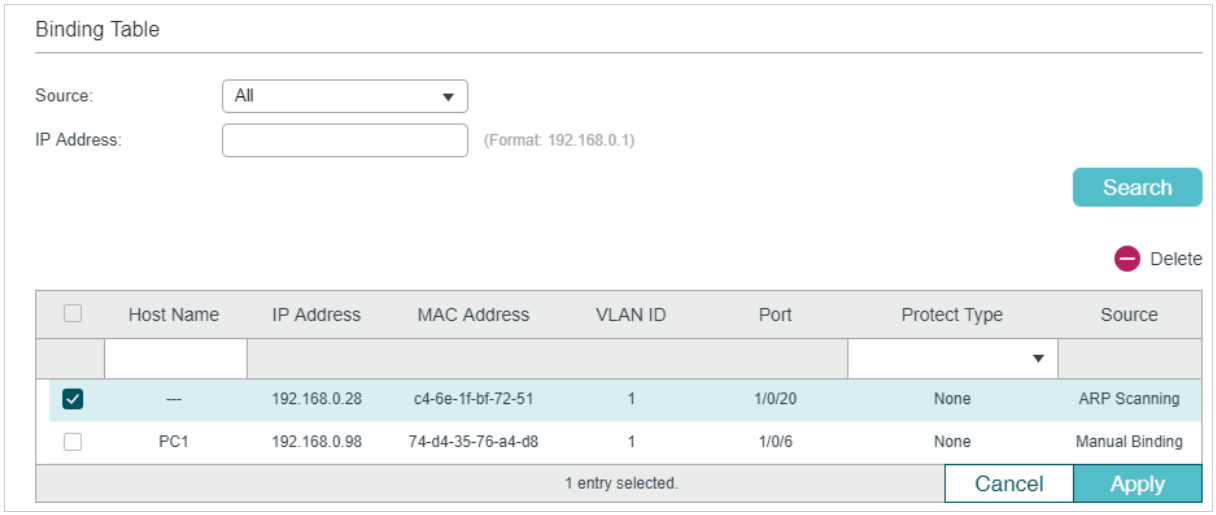
4) The learned entries will be displayed in the Binding Table. You can go to **SECURITY > IPv4 IMPB > IP-MAC Binding > Binding Table** to view or edit the entries.

2.1.4 Viewing the Binding Entries

In the Binding Table, you can view, search and edit the specified binding entries.

Choose the menu **SECURITY > IPv4 IMPB > IP-MAC Binding > Binding Table** to load the following page.

Figure 2-4 Binding Table



You can 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 Binding**: Displays the manually bound entries. **ARP Scanning**: Displays the binding entries learned from ARP Scanning. **DHCP Snooping**: Displays the binding entries learned from DHCP Snooping.
IP	Enter an IP address and click **Search** to search the specific entry.

Additionally, you select one or more entries to edit the host name and protect type 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. The entry will be applied to to the specific feature. The following options are provided: **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. **Both**: This entry will be applied to both of the features.
Source	Displays the source of the entry.

2.2 Using the CLI

Binding entries via ARP scanning is not supported by the CLI. The following sections introduce how to bind entries manually and via DHCP Snooping 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 detailed 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 { fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **port-channel** *port-channel-id* **} {** none | arp-detection | ip-verify-source | both **}** 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. *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 any feature; arp-detection indicates this entry will be applied to ARP Detection; ip-verify-source indicates this entry will be applied to IPv4 Source Guard.
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 74:d4:35:76:a4:d8, 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 74:d4:35:76:a4:d8 **vlan** 10 **interface gigabitEthernet** 1/0/5 arp-detection

Switch(config)#show ip source binding

U	Host	IP-Addr	MAC-Addr	VID	Port	ACL	SOURCE
-	----	-------	--------	---	----	---	------
1	host1	192.168.0.55	74:d4:35:76:a4:d8	10	Gi1/0/5	ARP-D	Manual

Notice:

1.Here, 'ARP-D' for 'ARP-Detection',and'IP-V-S' for 'IP-Verify-Source'.

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Binding Entries via DHCP Snooping

Follow these steps to bind entries via DHCP Snooping:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip dhcp snooping** Globally enable DHCP Snooping.
Step 3	**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 4	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| interface port-channel** *port-channel-id* **| interface range port-channel** *port-channel-id-list* **}** Enter interface configuration mode.
Step 5	**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 6	**show ip dhcp snooping** Verify global configuration of DHCP Snooping.
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 DHCP Snooping globally and on VLAN 5, and set the maximum number of binding entries port 1/0/1 can learn via DHCP snooping as 100:

Switch#configure

Switch(config)#ip dhcp snooping

Switch(config)#ip dhcp snooping vlan 5

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

Switch(config-if)#ip dhcp snooping max-entries 100

Switch(config-if)#show ip dhcp snooping

Global Status: Enable

VLAN ID: 5

Switch(config-if)#show ip dhcp snooping interface gigabitEthernet 1/0/1

Interface max-entries LAG

--- --- ---

Gi1/0/1 100 N/A

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.3 Viewing Binding Entries

On privileged EXEC mode or any other configuration mode, you can use the following command to view binding entries:

show ip source binding

View the information of binding entries, including the host name, IP address, MAC address, VLAN ID, port number and protect type.

3 ARP Detection Configuration

To complete ARP Detection configuration, follow these steps:

1) Add IP-MAC Binding entries.
2) Enable ARP Detection.
3) Configure ARP Detection on ports.
4) View ARP statistics.

3.1 Using the GUI

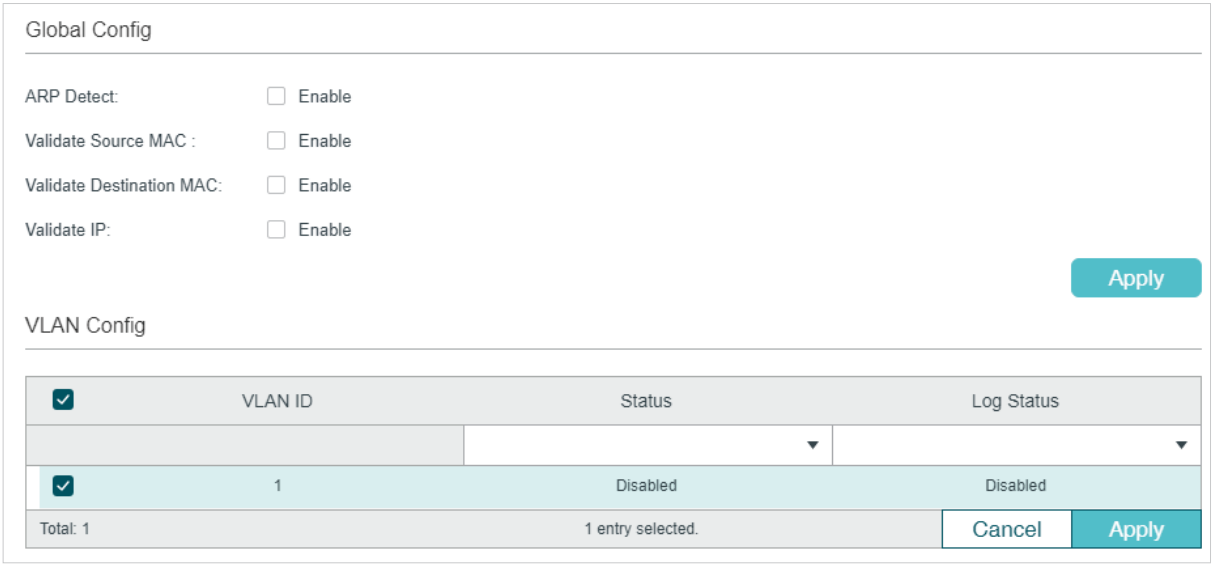
3.1.1 Adding IP-MAC Binding Entries

In ARP Detection, the switch detects the ARP packets based on the binding entries in the IP-MAC Binding Table. So before configuring ARP Detection, you need to complete IP-MAC Binding configuration. For details, refer to *IP-MAC Binding Configuration*.

3.1.2 Enabling ARP Detection

Choose the menu **SECURITY > IPv4 IMPB > ARP Detection > Global Config** to load the following page.

Figure 3-1 ARP Detection Global Config



Follow these steps to enable ARP Detection:

1) In the **Global Config** section, enable ARP Detection and configure the related parameters. Click **Apply**.

ARP Detect	Enable or disable ARP Detection globally.
Validate Source MAC	Enable or disable the switch to check whether the source MAC address and the sender MAC address are the same when receiving an ARP packet. If not, the ARP packet will be discarded.
Validate Destination MAC	Enable or disable the switch to check whether the destination MAC address and the target MAC address are the same when receiving an ARP reply packet. If not, the ARP packet will be discarded.
Validate IP	Enable or disable the switch to check whether the sender IP address of all ARP packets and the target IP address of ARP reply packets are legal. The illegal ARP packets will be discarded, including broadcast addresses, multicast addresses, Class E addresses, loopback addresses (127.0.0.0/8) and the following address: 0.0.0.0.

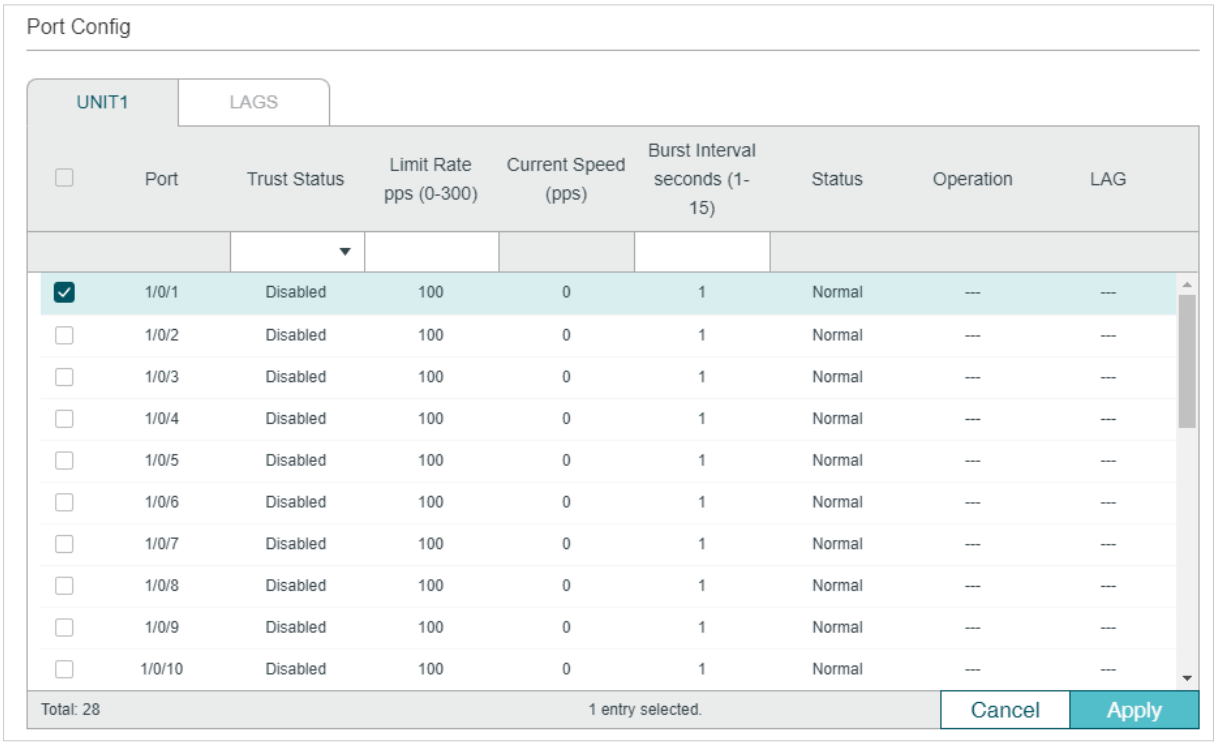
2) In the **VLAN Config** section, enable ARP Detection on the selected VLANs. Click **Apply**.

VLAN ID	Displays the VLAN ID.
Status	Enable or disable ARP Detection on the VLAN.
Log Status	Enable or disable Log feature on the VLAN. With this feature enabled, the switch generates a log when an illegal ARP packet is discarded.

3.1.3 Configuring ARP Detection on Ports

Choose the menu **SECURITY > IPv4 IMPB > ARP Detection >Port Config** to load the following page.

Figure 3-2 ARP Detection on Port



Follow these steps to configure ARP Detection on ports:

1) Select one or more ports and configure the parameters.

Trust Status	Enable or disable this port to be a trusted port. On a trusted port, the ARP packets are forwarded directly without checked. The specific ports, such as up-link ports and routing ports are suggested to be set as trusted.
Limit Rate	Specify the maximum number of the ARP packets that can be received on the port per second.
Current Speed	Displays the current speed of receiving the ARP packets on the port.
Burst Interval	Specify a time range. If the speed of received ARP packets reaches the limit for this time range, the port will be shut down.
Status	Displays the status of the ARP attack: **Normal**: The forwarding of ARP packets on the port is normal. **Down:** The transmission speed of the legal ARP packet exceeds the defined value. The port will be shut down for 300 seconds. You can also click the Recovery button to recover
Operation	If Status is changed to Down, there will be a **Recover** button. You can click the button to restore the port to the normal status.
LAG	Displays the LAG that the port is in.

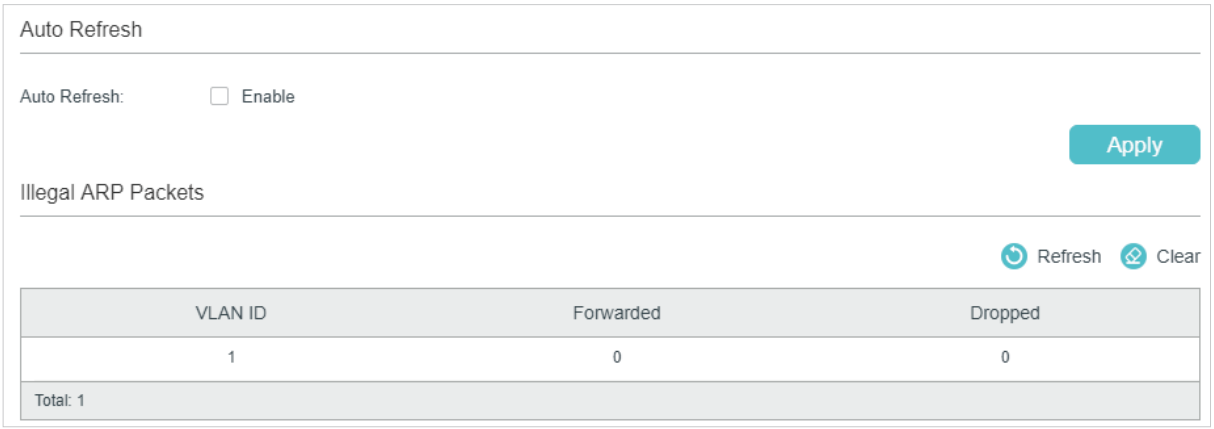
2) Click **Apply**.

3.1.4 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 **SECURITY > IPv4 IMPB > ARP Detection > ARP Statistics** to load the following page.

Figure 3-3 View 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 in each VLAN.

VLAN ID	Displays the VLAN ID.
Forwarded	Displays the number of forwarded ARP packets in this VLAN.
Dropped	Displays the number of dropped ARP packets in this VLAN.

3.2 Using the CLI

3.2.1 Adding IP-MAC Binding Entries

In ARP Detection, the switch detects the ARP packets based on the binding entries in the IP-MAC Binding Table. So before configuring ARP Detection, you need to complete IP-MAC Binding configuration. For details, refer to *IP-MAC Binding Configuration*.

3.2.2 Enabling ARP Detection

Follow these steps to enable ARP Detection:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip arp inspection** Globally enable the ARP Detection feature.
Step 3	**ip arp inspection validate {** src-mac | dst-mac | ip **}** Configure the switch to check the IP address or MAC address of the received packets. src-mac: Enable the switch to check whether the source MAC address and the sender MAC address are the same when receiving an ARP packet. If not, the ARP packet will be discarded. dst-mac: Enable the switch to check whether the sender IP address of all ARP packets and the target IP address of ARP reply packets are legal. The illegal packets will be discarded. ip: Enable or disable the switch to check whether the sender IP address of all ARP packets and the target IP address of ARP reply packets are legal. The illegal ARP packets will be discarded, including broadcast addresses, multicast addresses, Class E addresses, loopback addresses (127.0.0.0/8) and the following address: 0.0.0.0.
Step 4	**ip arp inspection vlan** *vlan-list* Enable ARP Detection on one or more 802.1Q VLANs that already exist. *vlan-list*: Enter the VLAN ID. The format is 1,5-9.

Step 5	**ip arp inspection vlan** *vlan-list* **logging** (Optional) Enable the Log feature to make the switch generate a log when an ARP packet is discarded. *vlan-list*: Enter the VLAN ID. The format is 1,5-9.
Step 6	**show ip arp inspection** Verify the ARP Detection configuration.
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 Detection globally and on VLAN 2, and enable the switch to check whether the source MAC address and the sender MAC address are the same when receiving an ARP packet:

Switch#configure

Switch(config)#ip arp inspection

Switch(config)#ip arp inspection validate src-mac

Switch(config)#ip arp inspection vlan 2

Switch(config)#show ip arp inspection

Global Status: Enable

Verify SMAC: Enable

Verify DMAC: Disable

Verify IP: Disable

Switch(config)#show ip arp inspection vlan

VID	Enable status	Log Status
----	----------	----------
1	Disable	Disable
2	Enable	Disable

Switch(config)#end

Switch#copy running-config startup-config

3.2.3 Configuring ARP Detection on Ports

Follow these steps to configure ARP Detection on 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 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 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 0 to 300 pps (packets/second), and the default value is 100.
Step 5	**ip arp inspection burst-interval** *value* Specify a time range. If the speed of received ARP packets reaches the limit for this time range, the port will be shut down. *value:* Specify the time range. The valid values are from 1 to 15 seconds, and the default value is 1 second.
Step 6	**show ip arp inspection interface** View the configurations and status of the ports.
Step 7	**show ip arp inspection vlan** View the configurations and status of the VLANs.
Step 8	**ip arp inspection recover** (Optional) For ports on which the speed of receiving ARP packets has exceeded the limit, use this command to restore the port from Down status to Normal status.
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 set port 1/02 as a trusted port, and set limit-rate as 20 pps and burst interval as 2 seconds on port 1/0/2:

Switch#configure

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

Switch(config-if)#ip arp inspection trust

Switch(config-if)#ip arp inspection limit-rate 20

Switch(config-if)#ip arp inspection burst-interval 2

Switch(config-if)#show ip arp inspection interface gigabitEthernet 1/0/2

Interface	Trust state	limit Rate(pps)	Current speed(pps)	Burst Interval	Status	LAG
---	---	---	---	---	---	---
Gi1/0/2	Enable	20	0	2	---	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 Down status to Normal status:

Switch#configure

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

Switch(config-if)#ip arp inspection recover

Switch(config-if)#end

Switch#copy running-config startup-config

3.2.4 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 the number of forwarded ARP packets and the number of dropped ARP packets.

4 IPv4 Source Guard Configuration

To complete IPv4 Source Guard configuration, follow these steps:

1) Add IP-MAC Binding entries.
2) Configure IPv4 Source Guard.

4.1 Using the GUI

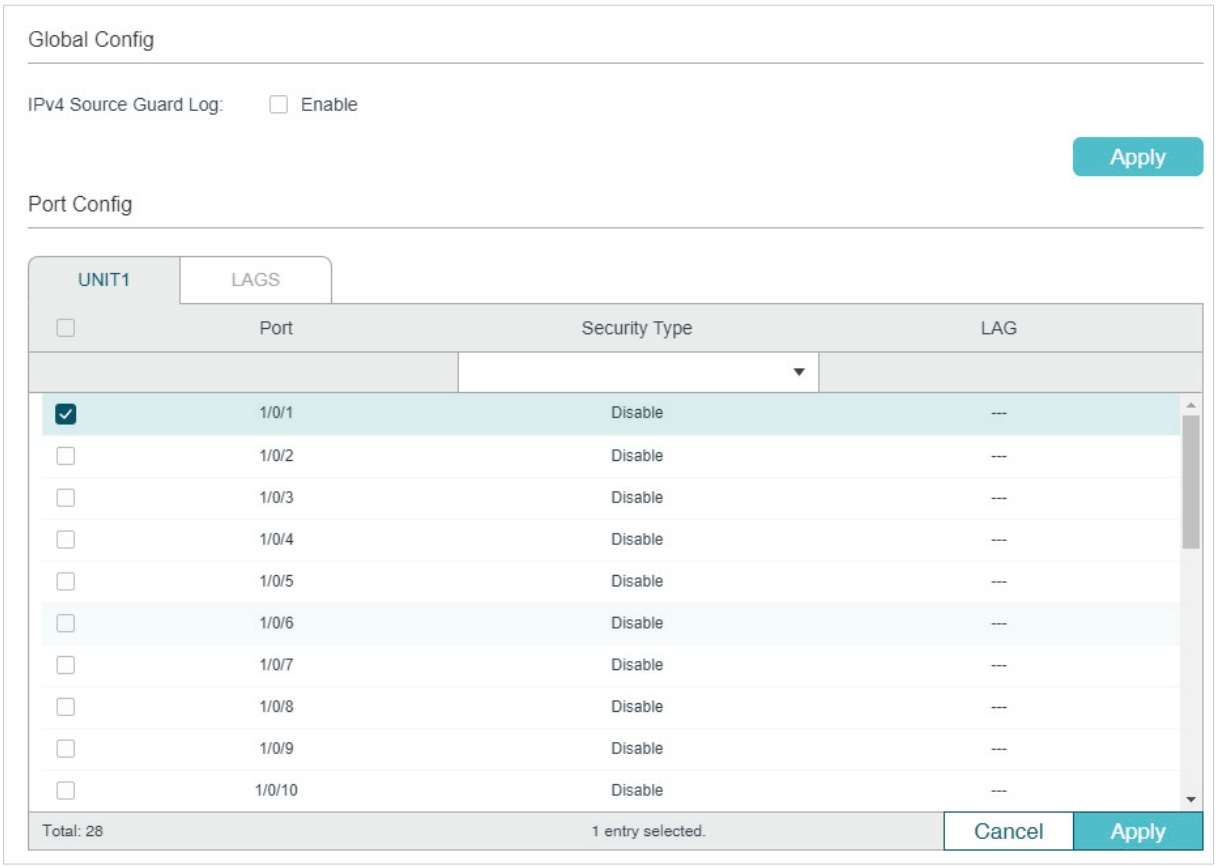
4.1.1 Adding IP-MAC Binding Entries

In IPv4 Source Guard, the switch filters the packets that do not match the rules of IPv4-MAC Binding Table. So before configuring ARP Detection, you need to complete IP-MAC Binding configuration. For details, refer to *IP-MAC Binding Configuration*.

4.1.2 Configuring IPv4 Source Guard

Choose the menu **SECURITY > IPv4 IMPB > IPv4 Source Guard** to load the following page.

Figure 4-1 IPv4 Source Guard Config



Follow these steps to configure IPv4 Source Guard:

1) In the **Global Config** section, choose whether to enable the Log feature. Click **Apply**.

Pv4 Source Guard Log	Enable or disable IPv4 Source Guard Log feature. With this feature enabled, the switch generates a log when illegal packets are received.

2) In the **Port Config** section, configure the protect type for ports and click **Apply**.

Port	Displays the port number.
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 IPv4-MAC binding rules can be processed, otherwise the packet will be discarded.
LAG	Displays the LAG that the port is in.

4.2 Using the CLI

4.2.1 Adding IP-MAC Binding Entries

In IPv4 Source Guard, the switch filters the packets that do not match the rules of IPv4-MAC Binding Table. So before configuring ARP Detection, you need to complete IP-MAC Binding configuration. For details, refer to *IP-MAC Binding Configuration*.

4.2.2 Configuring IPv4 Source Guard

Follow these steps to configure IPv4 Source Guard:

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 verify source {** sip+mac | sip **}** 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.

Step 4	**show ip verify source [interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id* **}]** Verify the IP Source Guard configuration for IPv4 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 IPv4 Source Guard on port 1/0/1:

Switch#configure

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

Switch(config-if)#ip verify source sip+mac

Switch(config-if)#show ip verify source interface gigabitEthernet 1/0/1

Port	Security-Type	LAG
----	----------	----
Gi1/0/1	SIP+MAC	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

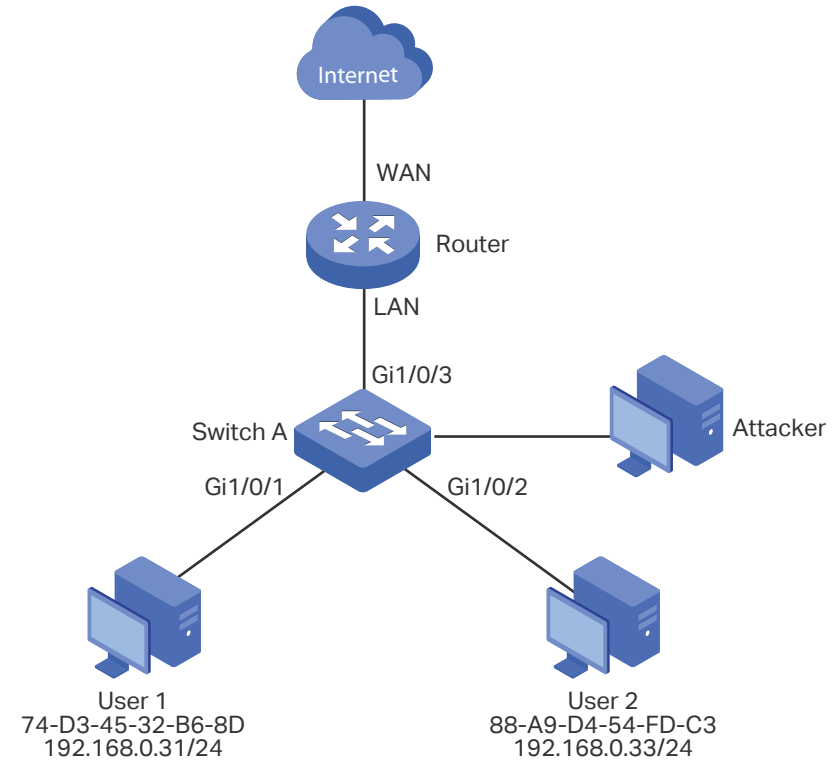
5 Configuration Examples

5.1 Example for ARP Detection

5.1.1 Network Requirements

As shown below, User 1 and User 2 are legal users in the LAN and connected to port 1/0/1 and port 1/0/2. Both of them are in the default VLAN 1. The router has been configured with security feature to prevent attacks from the WAN. Now the network administrator wants to configure Switch A to prevent ARP attacks from the LAN.

Figure 5-1 Network Topology



5.1.2 Configuration Scheme

To meet the requirement, you can configure ARP Detection to prevent the network from ARP attacks in the LAN.

The overview of configurations on the switch is as follows:

1) Configure IP-MAC Binding. The binding entries for User 1 and User 2 should be manually bound.
2) Configure ARP Detection globally.

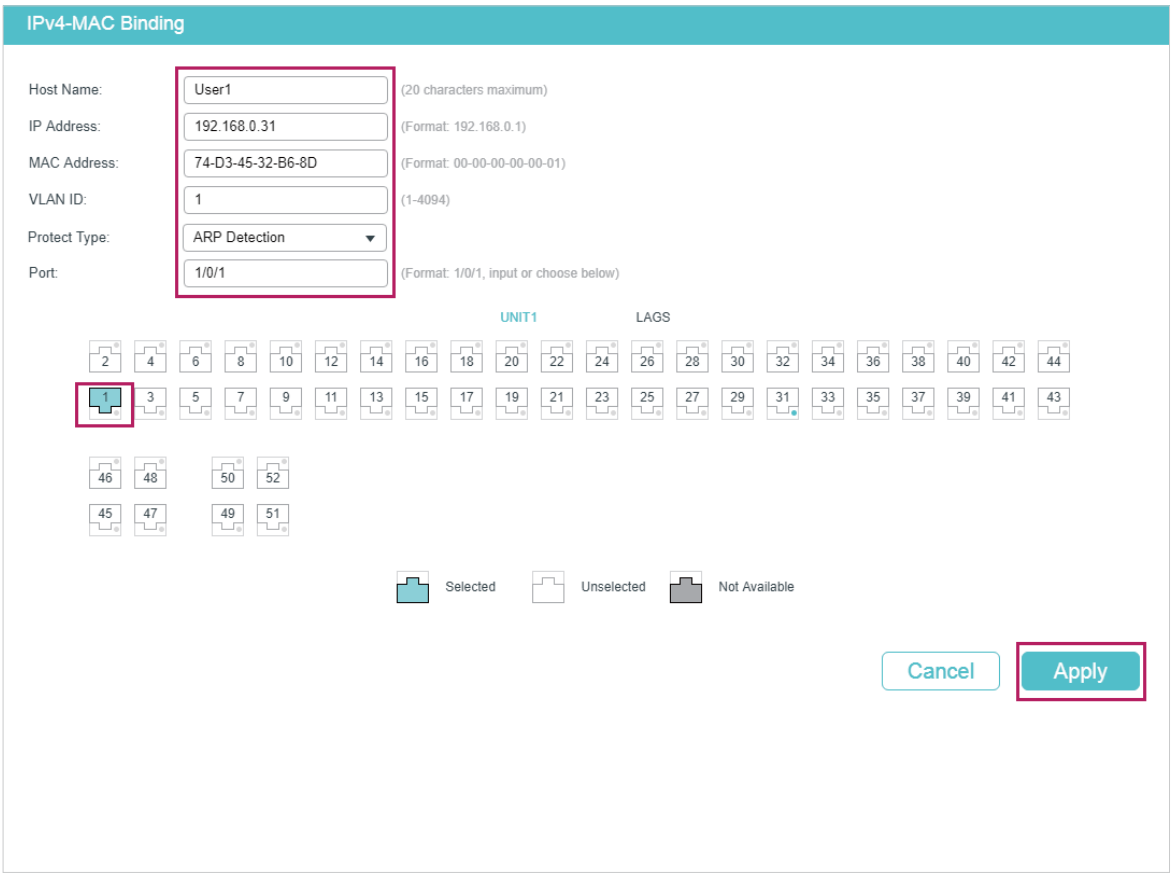
3) Configure ARP Detection on ports. Since port 1/0/3 is connected to the gateway router, set port 1/0/3 as trusted port. To prevent ARP flooding attacks, limit the speed of receiving the legal ARP packets on all ports.

Demonstrated with T1600G-52TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

5.1.3 Using the GUI

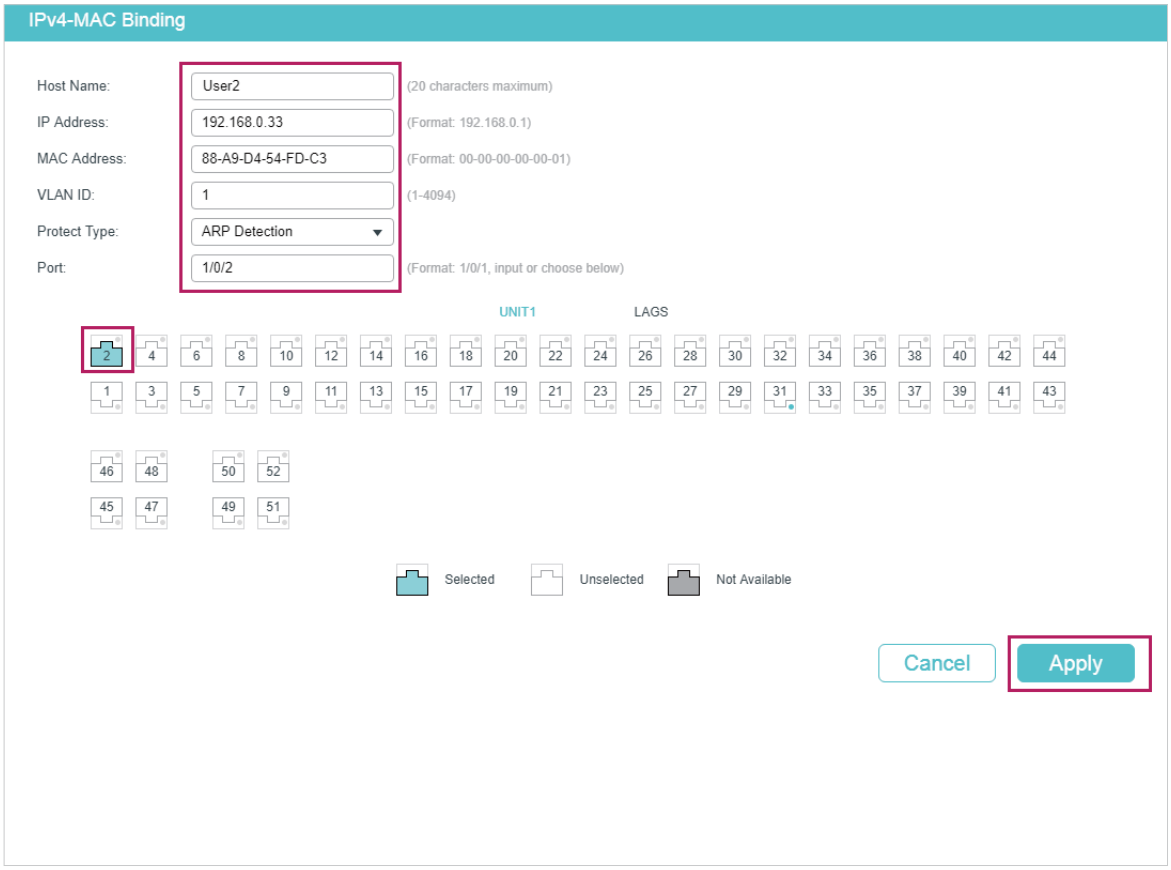
1) Choose the menu **SECURITY > IPv4 IMBP > IP-MAC Binding > Manual Binding** and click Add to load the following page. Enter the host name, IP address, MAC address and VLAN ID of User 1, select the protect type as ARP Detection, and select port 1/0/1 on the panel. Click **Apply**.

Figure 5-2 Binding Entry for User 1



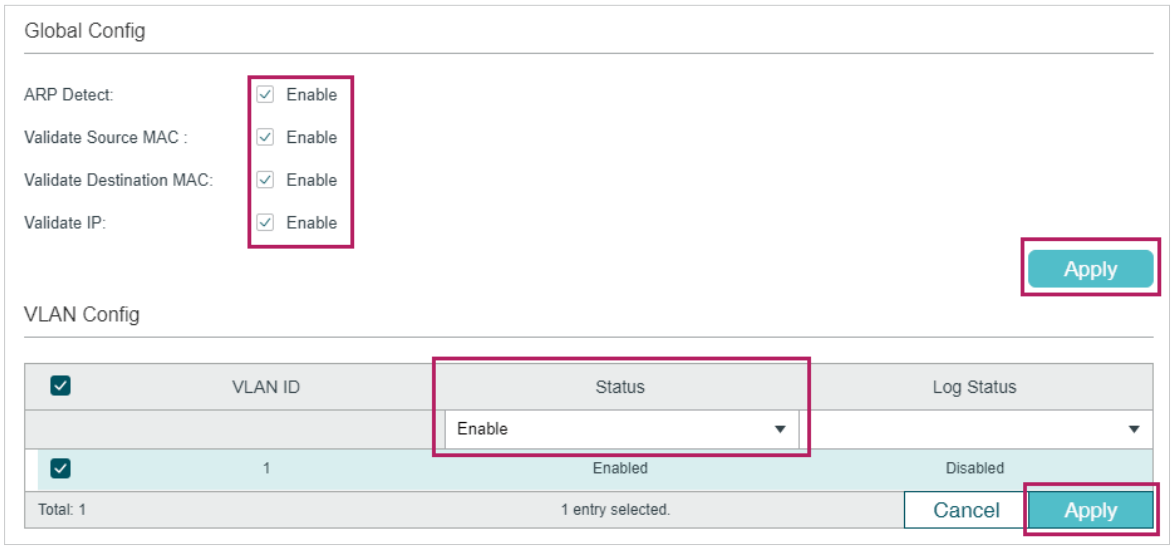
2) On the same page, add a binding entry for User 2. Enter the host name, IP address, MAC address and VLAN ID of User 2, select the protect type as ARP Detection, and select port 1/0/2 on the panel. Click **Apply**.

Figure 5-3 Binding Entry for User 2



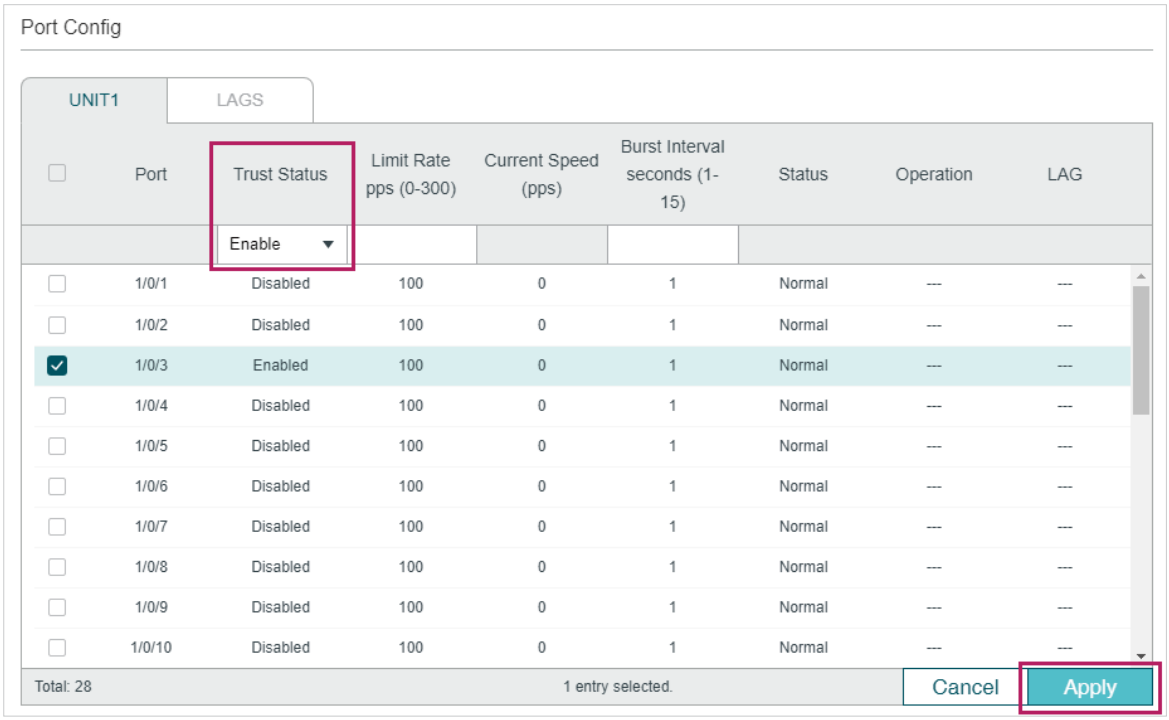
3) Choose the menu **SECURITY > IPv4 IMBP > ARP Detection > Global Config** to load the following page. Enable APP Detect, Validate Source MAC, Validate Destination MAC and Validate IP, and click **Apply**. Select VLAN 1, change Status as Enabled and click **Apply**.

Figure 5-4 Enable ARP Detection



4) Choose the menu **SECURITY > IPv4 IMBP > ARP Detection > Port Config** to load the following page. By default, all ports are enabled with ARP Detection and ARP flooding defend. Configure port 1/0/3 as trusted port and keep other defend parameters as default. Click **Apply**.

Figure 5-5 Port Config



5) Click Save to save the settings.

5.1.4 Using the CLI

1) Manually bind the entries for User 1 and User 2.

Switch_A#configure

Switch_A(config)#ip source binding User1 192.168.0.31 74:d3:45:32:b6:8d vlan 1 interface gigabitEthernet 1/0/1 arp-detection

Switch_A(config)#ip source binding User1 192.168.0.32 88:a9:d4:54:fd:c3 vlan 1 interface gigabitEthernet 1/0/2 arp-detection

2) Enable ARP Detection globally and on VLAN 1.

Switch_A(config)#ip arp inspection

Switch_A(config)#ip arp inspection vlan 1

3) Configure port 1/0/3 as trusted port.

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

Switch_A(config-if)#ip arp inspection trust

Switch_A(config-if)#end

Switch_A#copy running-config startup-config

Verify the Configuration

Verify the IP-MAC Binding entries:

Switch_A#show ip source binding

U	Host	IP-Addr	MAC-Addr	VID	Port	ACL	SOURCE
-	---	---	---	---	---	---	---
1	User1	192.168.0.31	74:d3:45:32:b6:8d	1	Gi1/0/1	ARP-D	Manual
1	User2	192.168.0.33	88:a9:d4:54:fd:c3	1	Gi1/0/2	ARP-D	Manual

Notice:

1.Here, 'ARP-D' for 'ARP-Detection',and'IP-V-S' for 'IP-Verify-Source'.

Verify the global configuration of ARP Detection:

Switch_A#show ip arp inspection

Global Status: Enable

Verify SMAC: Enable

Verify DMAC: Enable

Verify IP: Enable

Verify the ARP Detection configuration on VLAN:

Switch_A#show ip arp inspection vlan

VID	Enable status	Log Status
---	---	---
1	Enable	Disable

Verify the ARP Detection configuration on ports:

Switch_A#show ip arp inspection interface

Interface	Trust state	limit Rate(pps)	Current speed(pps)	Burst Interval	Status	LAG
---	---	---	---	---	---	---
Gi1/0/1	Disable	100	0	1	---	N/A
Gi1/0/2	Disable	100	0	1	---	N/A
Gi1/0/3	Enable	100	0	1	---	N/A

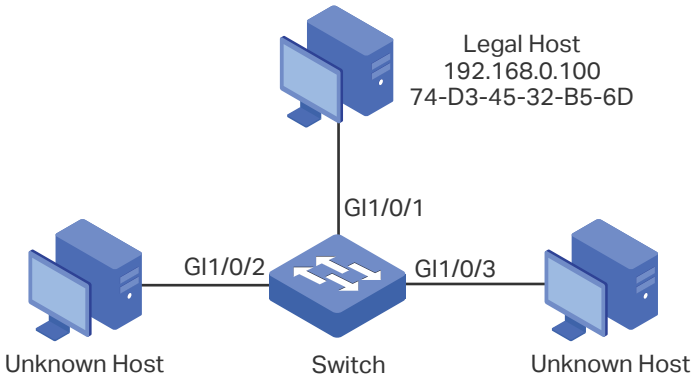
...

5.2 Example for IP Source Guard

5.2.1 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 5-6 Network Topology



5.2.2 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:

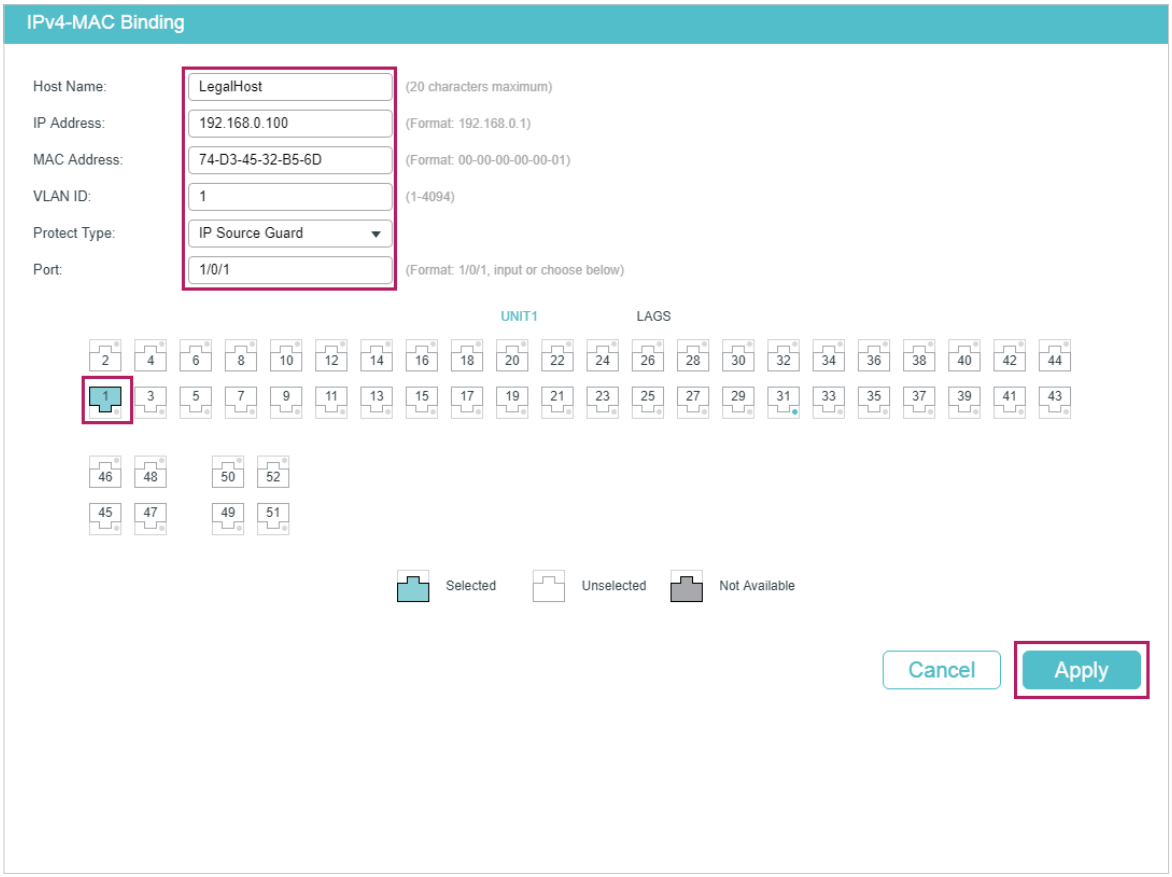
1) Bind the MAC address, IP address, connected port number and VLAN ID of the legal host with IP-MAC Binding.
2) Enable IP Source Guard on ports 1/0/1-3.

Demonstrated with T1600G-52TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

5.2.3 Using the GUI

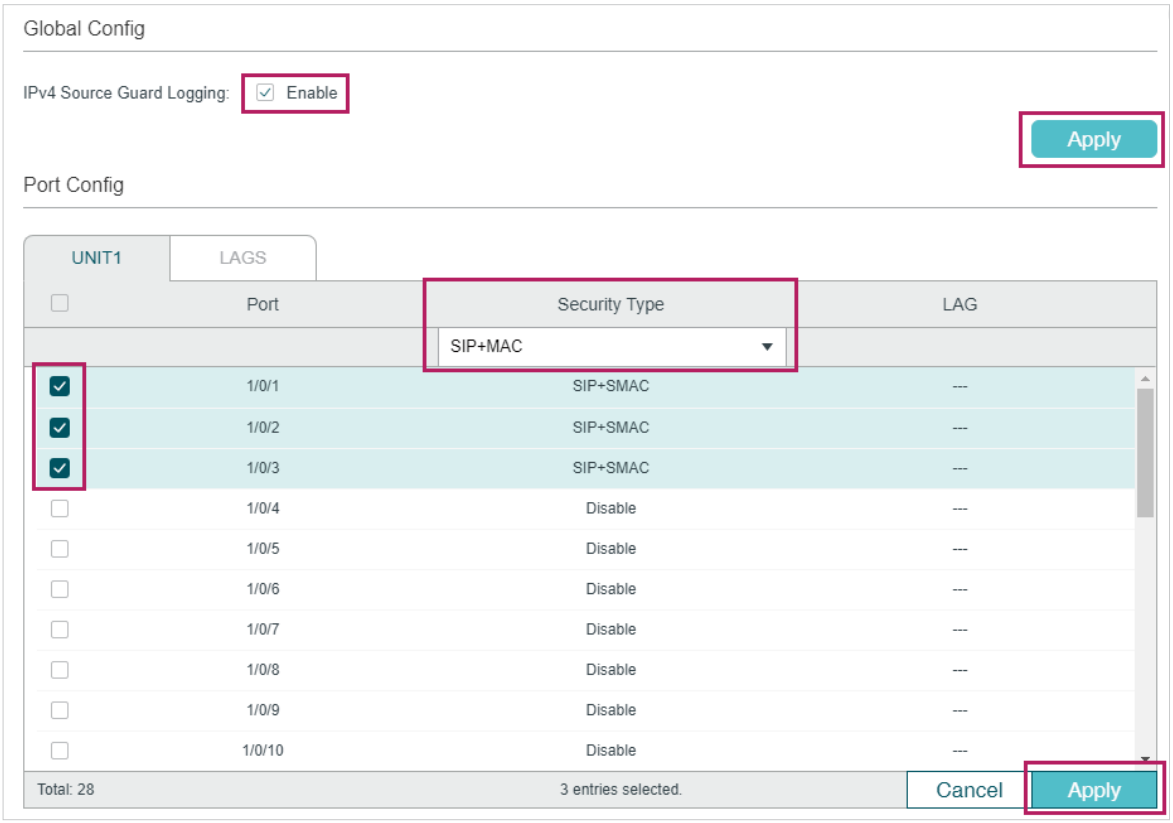
1) Choose the menu **SECURITY > IPv4 IMPB > IP-MAC Binding > Manual Binding** and click Add to load the following page. Enter the host name, IP address, MAC address and VLAN ID of the legal host, select the protect type as , and select port 1/0/1 on the panel. Click **Apply**.

Figure 5-7 Manual Binding



2) Choose the menu **SECURITY > IPv4 IMPB > IPv4 Source Guard** to load the following page. Enable IPv4 Source Guard Logging to make the switch generate logs when receiving illegal packets, and click **Apply**. Select ports 1/0/1-3, configure the Security Type as SIP+MAC, and click **Apply**.

Figure 5-8 IPv4 Source Guard



3) Click Save to save the settings.

5.2.4 Using the CLI

1) Manually bind the IP address, MAC address, VLAN ID and connected port number of the legal host, and apply this entry to the IP Source Guard feature.

Switch#configure

Switch(config)#ip source binding legal-host 192.168.0.100 74:d3:45:32:b5:6d vlan 1 interface gigabitEthernet 1/0/1 ip-verify-source

2) Enable the log feature and IP Source Guard on ports 1/0/1-3.

Switch(config)# ip verify source logging

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	Host	IP-Addr	MAC-Addr	VID	Port	ACL	SOURCE
-	----	-------	--------	---	----	---	------
1	User1	192.168.0.100	74:d3:45:32:b5:6d	1	Gi1/0/1	IP-V-S	Manual

Notice:

1.Here, 'ARP-D' for 'ARP-Detection',and'IP-V-S' for 'IP-Verify-Source'.

Verify the configuration of IP Source Guard:

Switch#show ip verify source

IP Source Guard log: Enabled

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

...

6 Appendix: Default Parameters

Default settings of DHCP Snooping are listed in the following table:

Table 6-1 DHCP Snooping

Parameter	Default Setting
Global Config	
DHCP Snooping	Disable
VLAN Config	
Status	Disable
Port Config	
Maximum Entry	512

Default settings of ARP Detection are listed in the following table:

Table 6-2 ARP Detection

Parameter	Default Setting
Global Config	
ARP Detect	Disable
Validate Source MAC	Disable
Validate Destination MAC	Disable
Validate IP	Disable
VLAN Config	
Status	Disable
Log Status	Disable
Port Config	
Trust Status	Disable
Limit Rate	100 pps

Parameter	Default Setting
Burst Interval	1 second
ARP Statistics	
Auto Refresh	Disable
Refresh Interval	5 seconds

Default settings of IPv4 Source Guard are listed in the following table:

Table 6-3 ARP Detection

Parameter	Default Setting
Global Config	
IPv4 Source Guard Log:	Disable
Port Config	
Security Type	Disable

Part 24

Configuring IPv6 IMPB

CHAPTERS

1. IPv6 IMPB
2. IPv6-MAC Binding Configuration
3. ND Detection Configuration
4. IPv6 Source Guard Configuration
5. Configuration Examples
6. Appendix: Default Parameters

1 IPv6 IMPB

1.1 Overview

IPv6 IMPB (IP-MAC-Port Binding) is used to bind the IPv6 address, MAC address, VLAN ID and the connected port number of the specified host. Basing on the binding table, the switch can prevent ND attacks with the ND Detection feature and filter the packets that don't match the binding entries with the IPv6 Source Guard feature.

1.2 Supported Features

IPv6-MAC Binding

This feature is used to add binding entries. The binding entries can be manually configured, or learned by ND Snooping or DHCPv6 snooping. The features ND Detection and IPv6 Source Guard are based on the IPv6-MAC Binding entries.

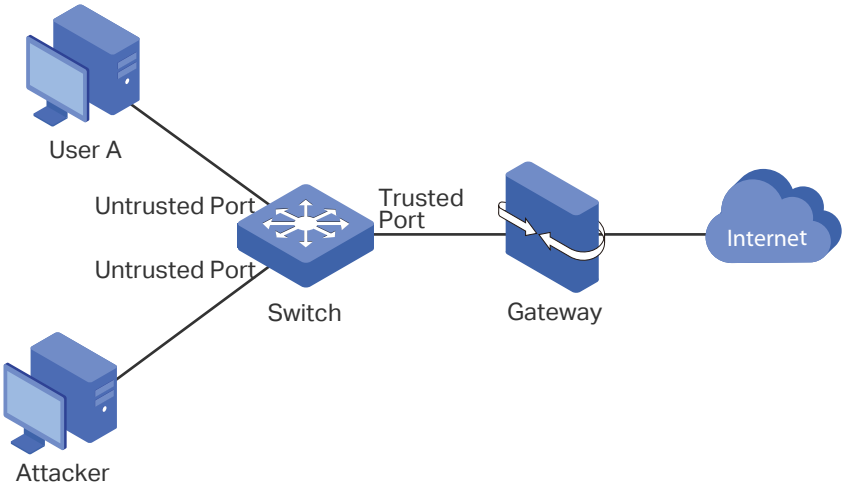
ND Detection

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 1-1 Network Topology of ND Detection



IPv6 Source Guard

IPv6 Source Guard is used to filter the IPv6 packets based on the IPv6-MAC Binding table. Only the packets that match the binding rules are forwarded.

2 IPv6-MAC Binding Configuration

You can add IPv6-MAC Binding entries in three ways:

- Manual Binding
- Via ND Snooping
- Via DHCPv6 Snooping

Additionally, you can view, search and edit the entries in the Binding Table.

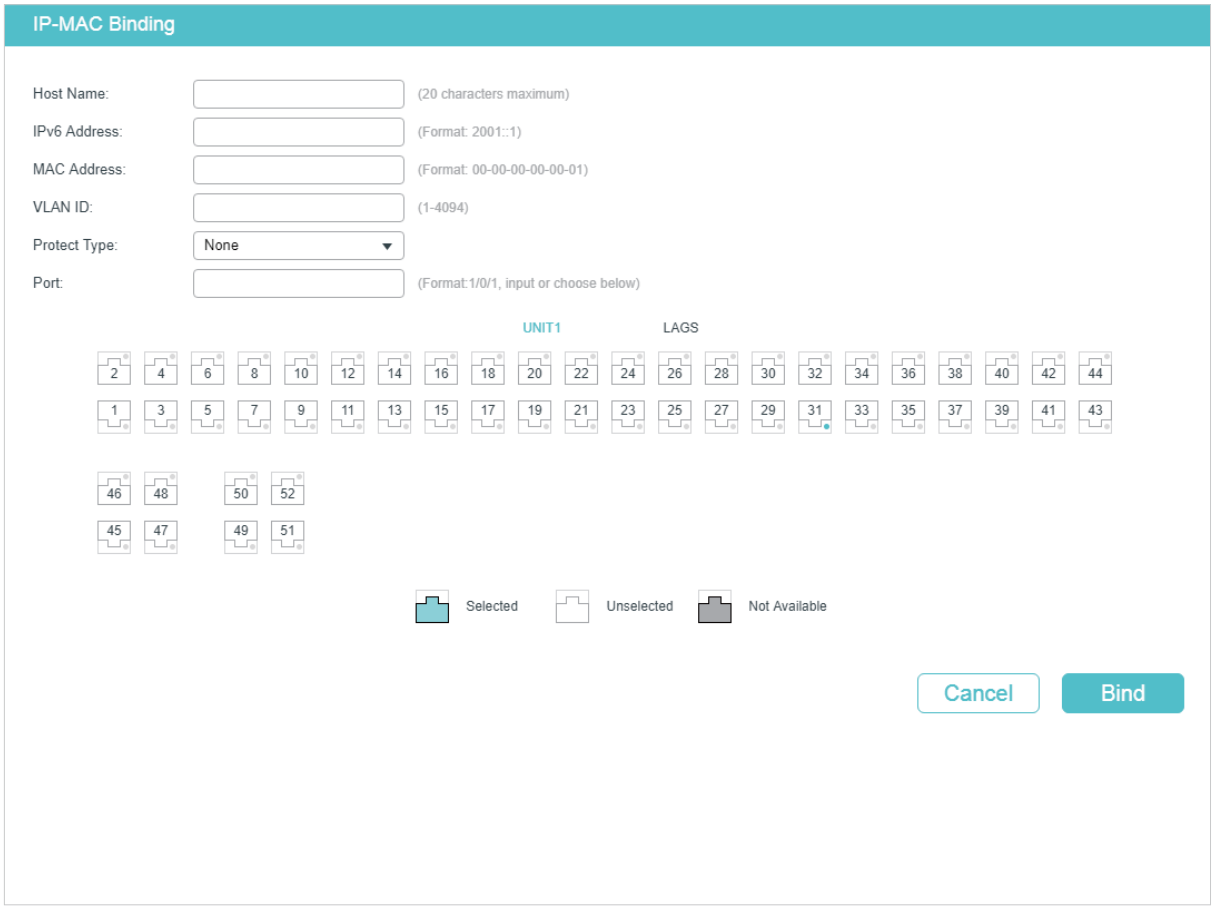
2.1 Using the GUI

2.1.1 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 detailed information of the hosts.

Choose the menu **SECURITY > IPv6 IMPB > IPv6-MAC Binding > Manual Binding** and click Add to load the following page.

Figure 2-1 Manual Binding



Follow these steps to manually create an IPv6-MAC Binding entry:

1) Enter the following information to specify a host.

Host Name	Enter the host name for identification.
IPv6 Address	Enter the IPv6 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. The entry will be applied to to the specific feature. The following options are provided: **None**: This entry will not be applied to any feature. **ND Detection**: This entry will be applied to the ND Detection feature. **IPv6 Source Guard**: This entry will be applied to the IPv6 Source Guard feature. **Both**: This entry will be applied to both of the features.

3) Enter or select the port that is connected to this host.

4) Click **Apply**.

2.1.2 Binding Entries via ND Snooping

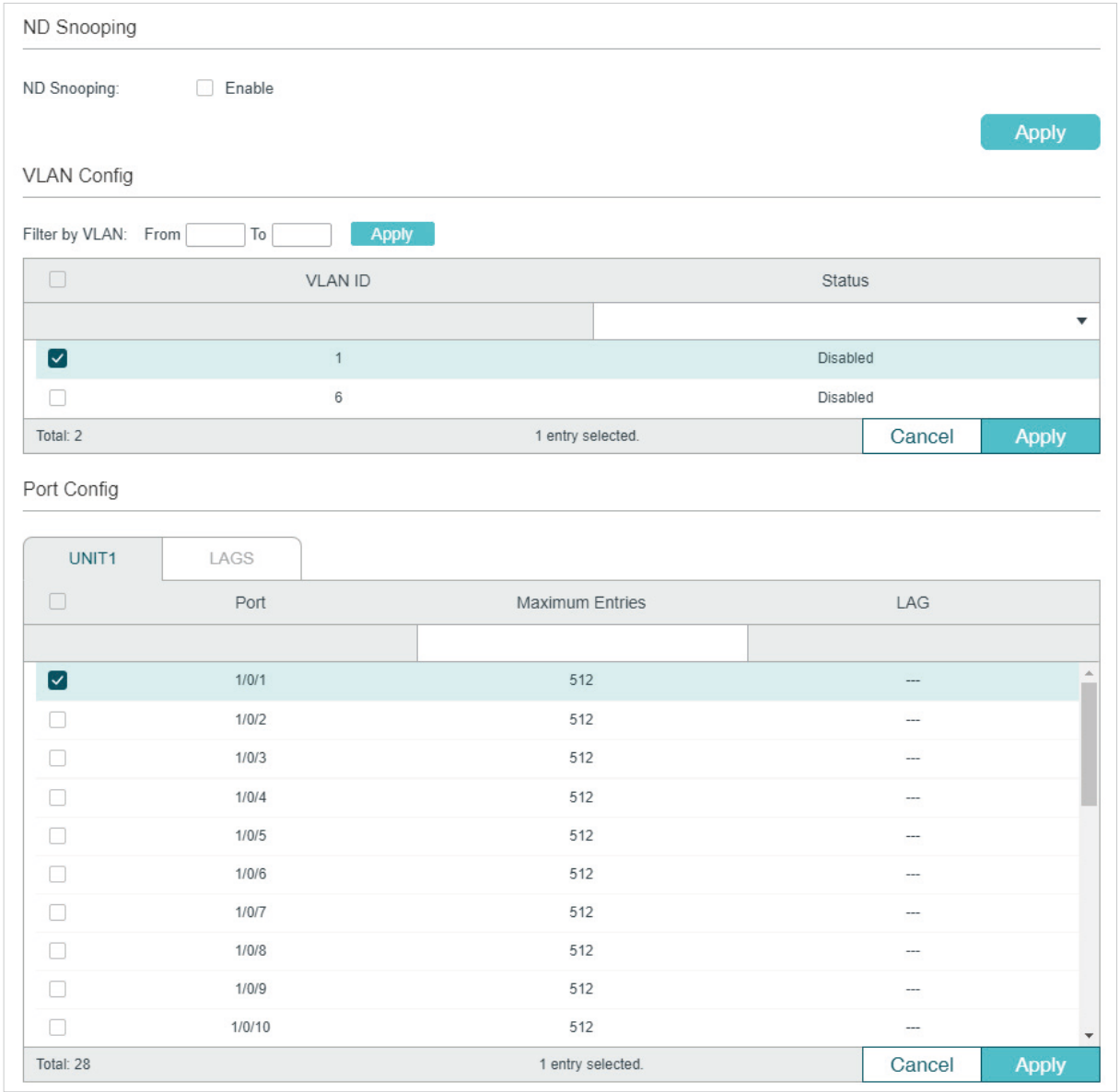
With ND Snooping, the switch monitors the ND packets, and records the IPv6 addresses, MAC addresses, VLAN IDs and the connected port numbers of the IPv6 hosts. You can bind these entries conveniently.

Note:

Before using this feature, make sure that your network is safe and the hosts are not suffering from ND attacks at present; otherwise, you may obtain incorrect IPv6-MAC Binding entries. If your network is being attacked, it's recommended to bind the entries manually.

Choose the menu **SECURITY > IPv6 IMPB > IPv6-MAC Binding > ND Snooping** to load the following page.

Figure 2-2 ND Snooping



Follow these steps to configure IPv6-MAC Binding via ND Snooping:

1) In the **ND Snooping** section, enable ND Snooping and click **Apply**.
2) In the **VLAN Config** section, select one or more VLANs and enable ND Snooping. Click **Apply**.

VLAN ID	Displays the VLAN ID.
Status	Enable or disable ND Snooping on the VLAN.

3) In the **Port Config** section, configure the maximum number of entries a port can learn via ND snooping. Click **Apply**.

Port	Displays the port number.
Maximum Entries	Configure the maximum number of binding entries a port can learn via ND snooping.
LAG	Displays the LAG that the port is in.

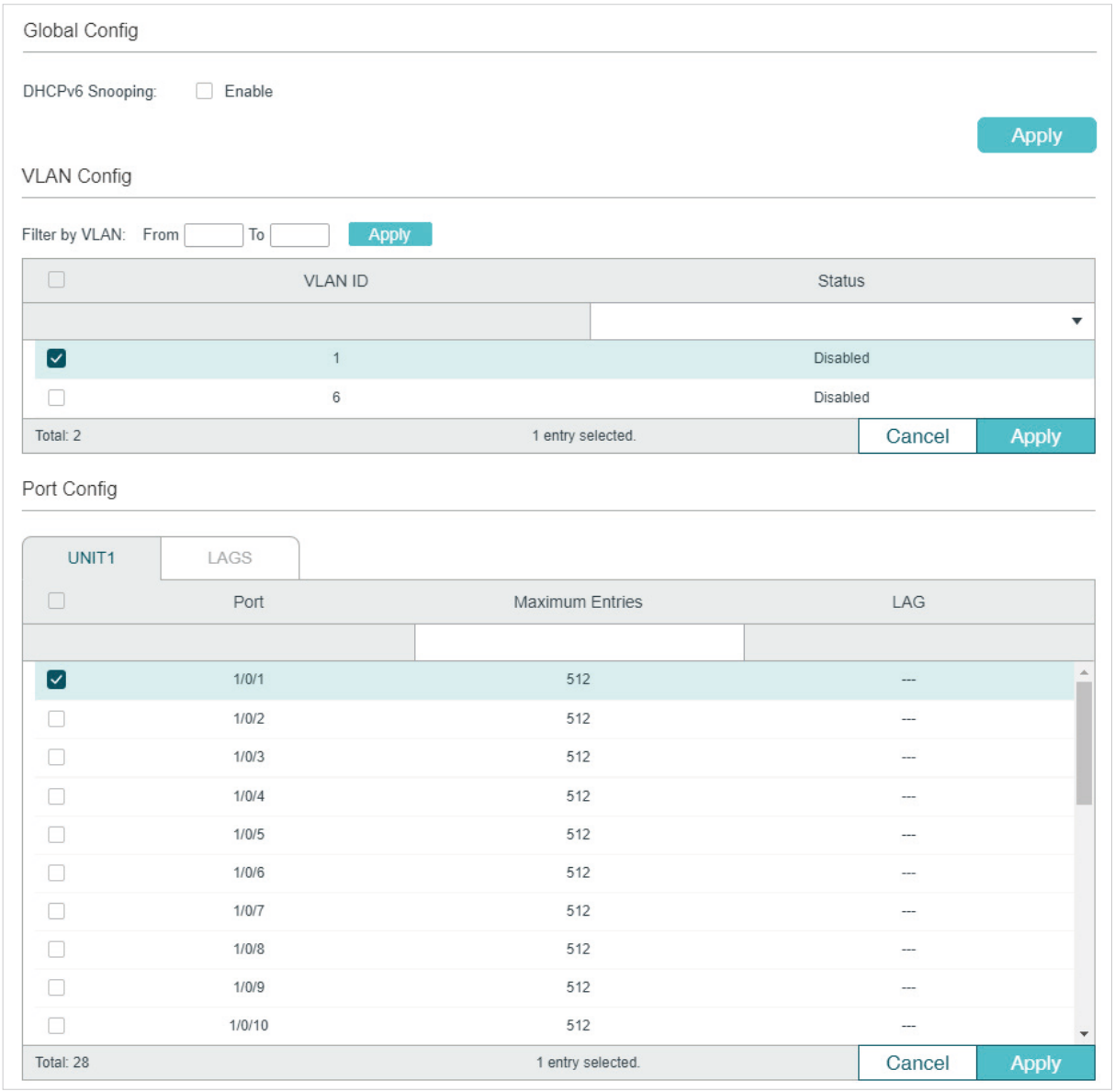
4) The learned entries will be displayed in the Binding Table. You can go to **SECURITY > IPv6 IMPB > IPv6-MAC Binding > Binding Table** to view or edit the entries.

2.1.3 Binding Entries via DHCPv6 Snooping

With DHCPv6 Snooping enabled, the switch can monitor the IP address obtaining process of the host, and record the IPv6 address, MAC address, VLAN ID and the connected port number of the host.

Choose the menu **SECURITY > IPv6 IMPB > IPv6-MAC Binding > DHCPv6 Snooping** to load the following page.

Figure 2-3 DHCPv6 Snooping



Follow these steps to configure IPv6-MAC Binding via DHCPv6 Snooping:

1) In the **Global Config** section, globally enable DHCPv6 Snooping. Click **Apply**.

2) In the **VLAN Config** section, enable DHCPv6 Snooping on a VLAN or range of VLANs. Click **Apply**.

VLAN ID	Displays the VLAN ID.
Status	Enable or disable DHCPv6 Snooping on the VLAN.

3) In the **Port Config** section, configure the maximum number of binding entries a port can learn via DHCPv6 snooping. Click **Apply**.

Port	Displays the port number.

Maximum Entries	Configure the maximum number of binding entries a port can learn via DHCPv6 snooping.
LAG	Displays the LAG that the port is in.

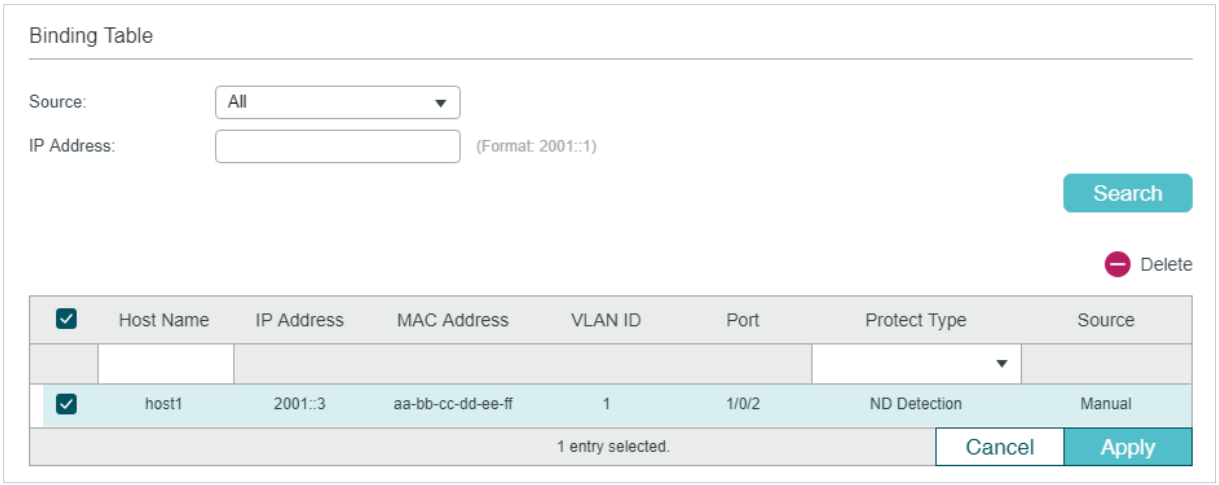
4) The learned entries will be displayed in the Binding Table. You can go to **SECURITY > IPv6 IMPB > IPv6-MAC Binding > Binding Table** to view or edit the entries.

2.1.4 Viewing the Binding Entries

In the Binding Table, you can view, search and edit the specified binding entries.

Choose the menu **SECURITY > IPv6 IMPB > IPv6-MAC Binding > Binding Table** to load the following page.

Figure 2-4 Binding Table



You can 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 Binding**: Displays the manually bound entries. **ND Snooping**: Displays the binding entries learned from ND Snooping. **DHCPv6 Snooping**: Displays the binding entries learned from DHCP Snooping.
IP	Enter an IP address and click **Search** to search the specific entry.

Additionally, you select one or more entries to edit the host name and protect type 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. The entry will be applied to to the specific feature. The following options are provided: **None**: This entry will not be applied to any feature. **ND Detection**: This entry will be applied to the ND Detection feature. **IPv6 Source Guard**: This entry will be applied to the IP Source Guard feature. **Both**: This entry will be applied to both of the features.
Source	Displays the source of the entry.

2.2 Using the CLI

The following sections introduce how to bind entries manually and via ND Snooping and DHCP Snooping, and how to view the binding entries.

2.2.1 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 detailed 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* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id* **} {** none | nd-detection | ipv6-verify-source | both **}** 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. *hostname*: Specify a name for the host. It contains 20 characters at most. *ipv6-addr*: Enter the IPv6 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 | 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 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, 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	Host	IP-Addr	MAC-Addr	VID	Port	ACL	Source
-	----	-------	--------	---	----	---	------
1	host1	2001:0:9d38:90d5::34	aa:bb:cc:dd:ee:ff	10	Gi1/0/5	ND-D	Manual

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 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* **| ten-gigabitEthernet** *port* **| range ten-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* **| ten-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

2.2.3 Binding Entries via DHCPv6 Snooping

Follow these steps to bind entries via DHCP 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* **| ten-gigabitEthernet** *port* **| range ten-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 max-entries** *value* Configure the maximum number of binding entries the port can learn via DHCPv6 snooping. *value:* Enter the value of maximum number of entries. The valid values are from 0 to 512.

Step 6	**show ip dhcp snooping** Verify global configuration of DHCPv6 Snooping.
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 DHCPv6 Snooping globally and on VLAN 5, and set the maximum number of binding entries port 1/0/1 can learn via DHCPv6 snooping as 100:

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 max-entries 100

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 max-entries LAG

--- --- ---

Gi1/0/1 100 N/A

Switch(config-if)#end

Switch#copy running-config startup-config

2.2.4 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, IP address, MAC address, VLAN ID, port number and protect type.

3 ND Detection Configuration

To complete ND Detection configuration, follow these steps:

1) Add IPv6-MAC Binding entries.
2) Enable ND Detection.
3) Configure ND Detection on ports.
4) View ND statistics.

3.1 Using the GUI

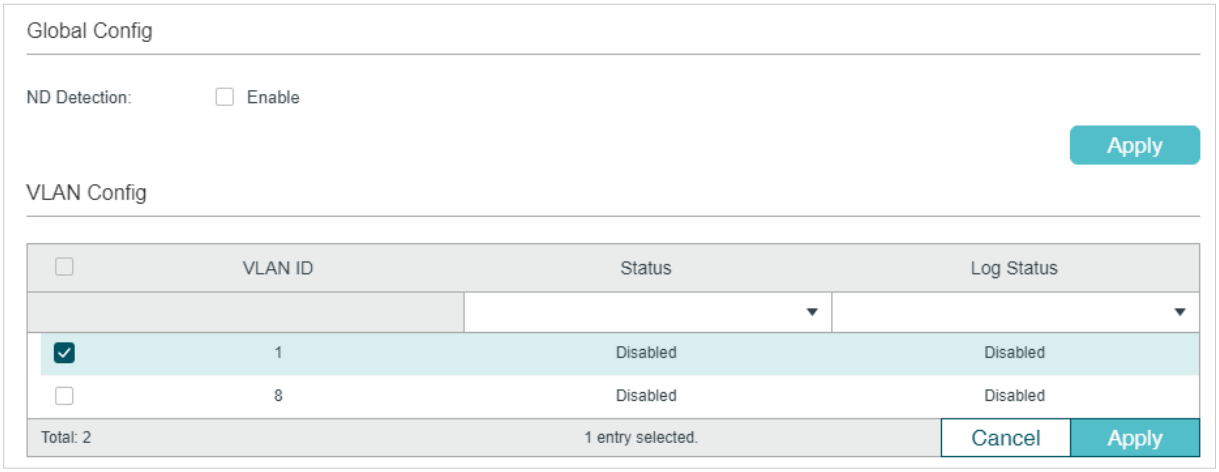
3.1.1 Adding IPv6-MAC Binding Entries

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 Configuration*.

3.1.2 Enabling ND Detection

Choose the menu **SECURITY > IPv6 IMPB > ND Detection > Global Config** to load the following page.

Figure 3-1 ND Detection Global Config



Follow these steps to enable ND Detection:

1) In the **Global Config** section, enable ND Detection and configure the related parameters. Click **Apply**.

ND Detection	Enable or disable ND Detection globally.

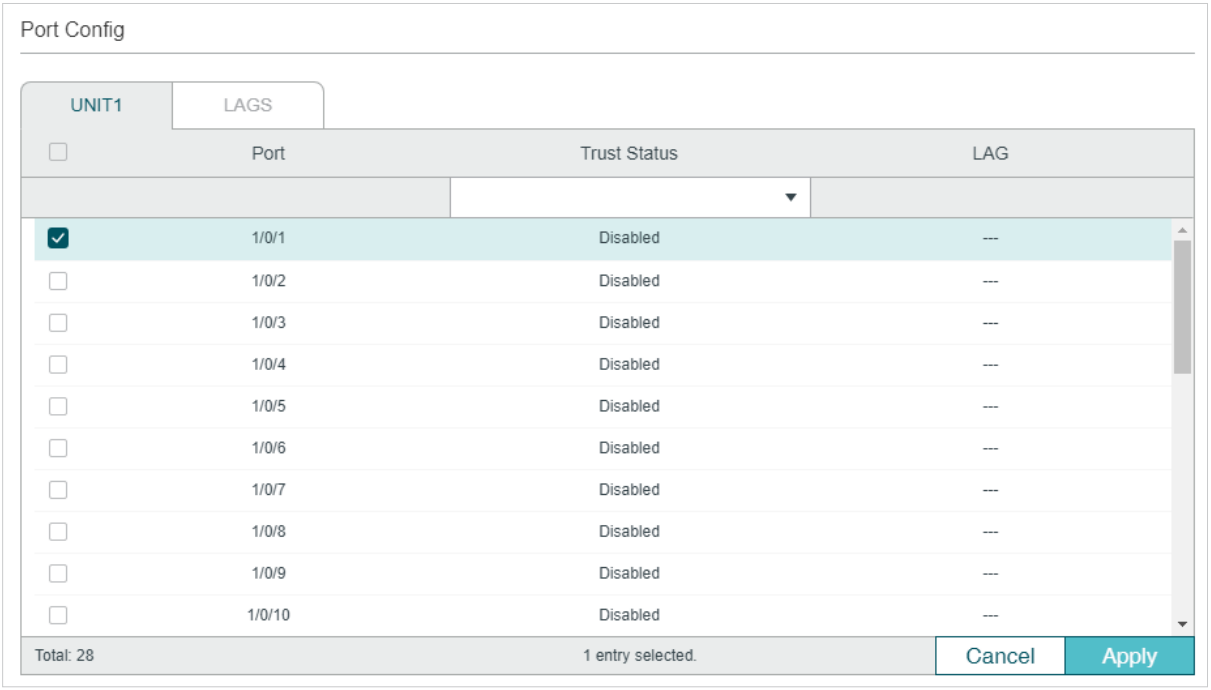
2) In the **VLAN Config** section, enable ND Detection on the selected VLANs. Click **Apply**.

VLAN ID	Displays the VLAN ID.
Status	Enable or disable ND Detection on the VLAN.
Log Status	Enable or disable Log feature on the VLAN. With this feature enabled, the switch generates a log when an illegal ND packet is discarded.

3.1.3 Configuring ND Detection on Ports

Choose the menu **SECURITY > IPv6 IMPB > ND Detection >Port Config** to load the following page.

Figure 3-2 ND Detection on Port



Follow these steps to configure ND Detection on ports:

1) Select one or more ports and configure the parameters.

Port	Displays the port number.
Trust Status	Enable or disable this port to be a trusted port. On a trusted port, the ND packets are forwarded directly without checked. The specific ports, such as up-link ports and routing ports are suggested to be set as trusted.
LAG	Displays the LAG that the port is in.

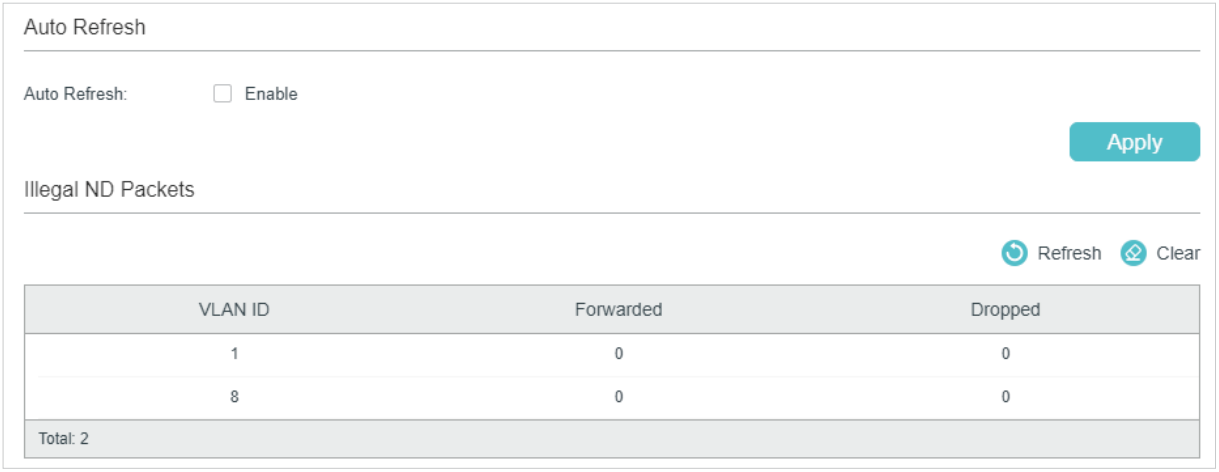
2) Click **Apply**.

3.1.4 Viewing ND Statistics

You can view the number of the illegal ND packets received on each port, which facilitates you to locate the network malfunction and take the related protection measures.

Choose the menu **SECURITY > IPv6 IMPB > ND Detection > ND Statistics** to load the following page.

Figure 3-3 View ND 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 ND Packet** section, you can view the number of illegal ND packets in each VLAN.

VLAN ID	Displays the VLAN ID.
Forwarded	Displays the number of forwarded ND packets in this VLAN.
Dropped	Displays the number of dropped ND packets in this VLAN.

3.2 Using the CLI

3.2.1 Adding IPv6-MAC Binding Entries

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 Configuration*.

3.2.2 Enabling ND Detection

Follow these steps to enable 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	**ipv6 nd detection vlan** *vlan-range* **logging** (Optional) Enable the Log feature to make the switch generate a log when an ND packet is discarded. *vlan-range:* Enter the vlan range in the format of 1-3, 5.
Step 5	**show ipv6 nd detection** Verify the global ND Detection 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 ND Detection globally and on VLAN 1:

Switch#configure

Switch(config)#ipv6 nd detection

Switch(config)#ipv6 nd detection vlan 1

Switch(config)#show ipv6 nd detection

Global Status: Enable

Switch(config)#show ipv6 nd detection vlan

VID	Enable status	Log Status
----	----------	----------
1	Enable	Disable

Switch(config)#end

Switch#copy running-config startup-config

3.2.3 Configuring ND Detection on Ports

Follow these steps to configure ND Detection on 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	**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 4	**show ipv6 nd detection interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id* **}** Verify the global ND Detection configuration 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 configure port 1/0/1 as trusted port:

Switch#configure

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

Switch(config-if)#ipv6 nd detection trust

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

3.2.4 Viewing ND Statistics

On privileged EXEC mode or any other configuration mode, you can use the following command to view ND statistics:

show ipv6 nd detection statistics

View the ND statistics on each port, including the number of forwarded ND packets and the number of dropped ND packets.

4 IPv6 Source Guard Configuration

To complete IPv6 Source Guard configuration, follow these steps:

1) Add IP-MAC Binding entries.
2) Configure IPv6 Source Guard.

4.1 Using the GUI

4.1.1 Adding IPv6-MAC Binding Entries

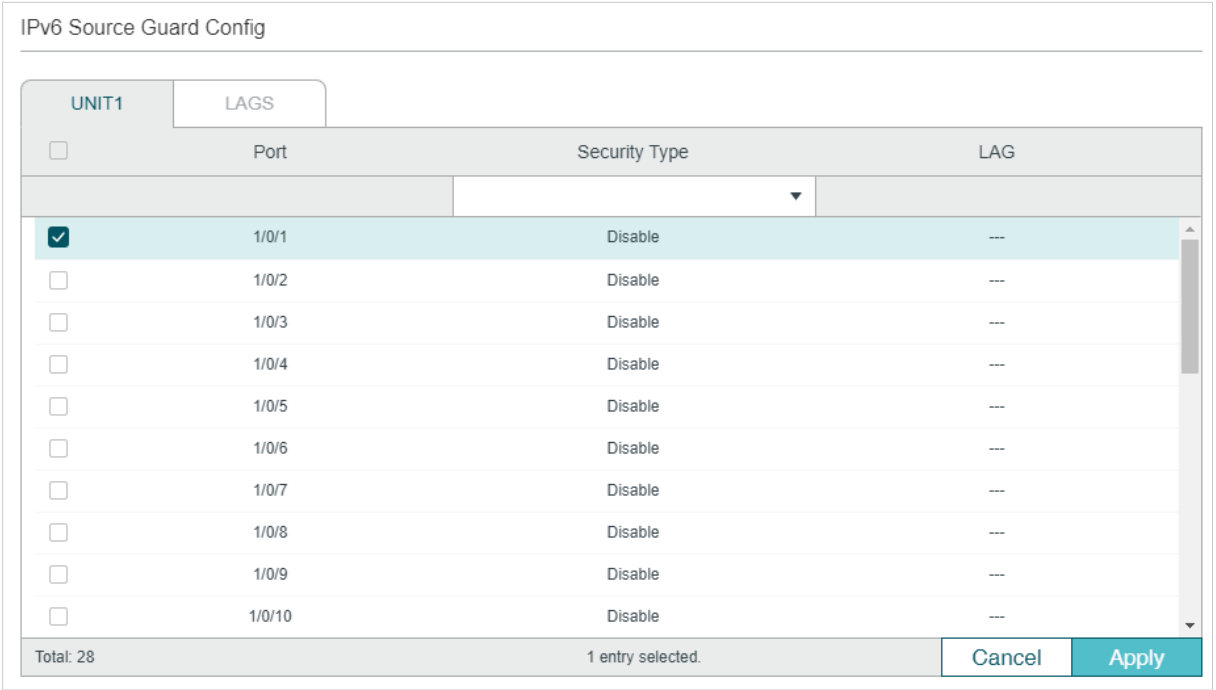
The ND Detection feature allows the switch to detect the ND packets based on the binding entries in the IPv6-MAC Binding Table and filter out the illegal ND packets. Before configuring ND Detection, complete IPv6-MAC Binding configuration. For details, refer to *IPv6-MAC Binding Configuration*.

4.1.2 Configuring IPv6 Source Guard

Before configuring IPv6 Source Guard, you need to configure the SDM template as EnterpriseV6.

Choose the menu **SECURITY > IPv6 IMPB > IPv6 Source Guard** to load the following page.

Figure 4-1 IPv6 Source Guard Config



Follow these steps to configure IPv6 Source Guard:

1) Select one or more ports and configure the protect type for ports.

Port	Displays the port number.
Security Type	Select Security Type on the port for IPv6 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 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**.

4.2 Using the CLI

4.2.1 Adding IPv6-MAC Binding Entries

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 Configuration*.

4.2.2 Configuring IPv6 Source Guard

Before configuring IPv6 Source Guard, you need to configure the SDM template as EnterpriseV6.

Follow these steps to configure IPv6 Source Guard:

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	**ipv6 verify source {** sipv6+mac **}** Enable IPv6 Source Guard for IPv6 packets. sipv6+mac*:* Only the packet with its source IP address, source MAC address and port number matching the IPv6-MAC binding rules can be processed, otherwise the packet will be discarded.

Step 4	**show ipv6 verify source [interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id* **}]** 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 IPv6 Source Guard on port 1/0/1:

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

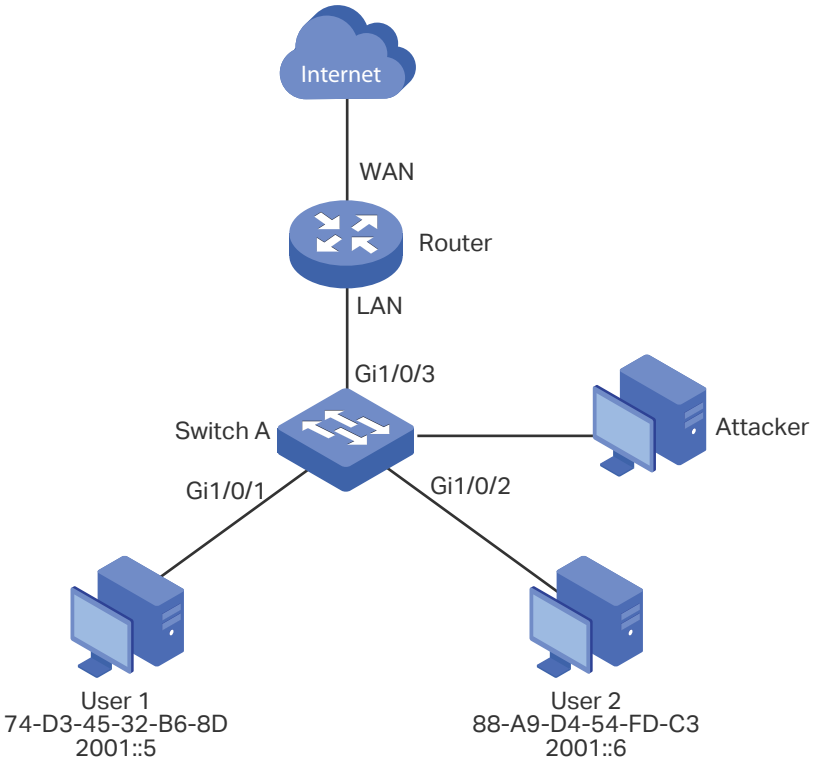
5 Configuration Examples

5.1 Example for ND Detection

5.1.1 Network Requirements

As shown below, User 1 and User 2 are legal IPv6 users in the LAN and connected to port 1/0/1 and port 1/0/2. Both of them are in the default VLAN 1. The router has been configured with security feature to prevent attacks from the WAN. Now the network administrator wants to configure Switch A to prevent ND attacks from the LAN.

Figure 5-1 Network Topology



5.1.2 Configuration Scheme

To meet the requirement, you can configure ND Detection to prevent the network from ND attacks in the LAN.

The overview of configurations on the switch is as follows:

1) Configure IPv6-MAC Binding. The binding entries for User 1 and User 2 should be manually bound.
2) Configure ND Detection globally.

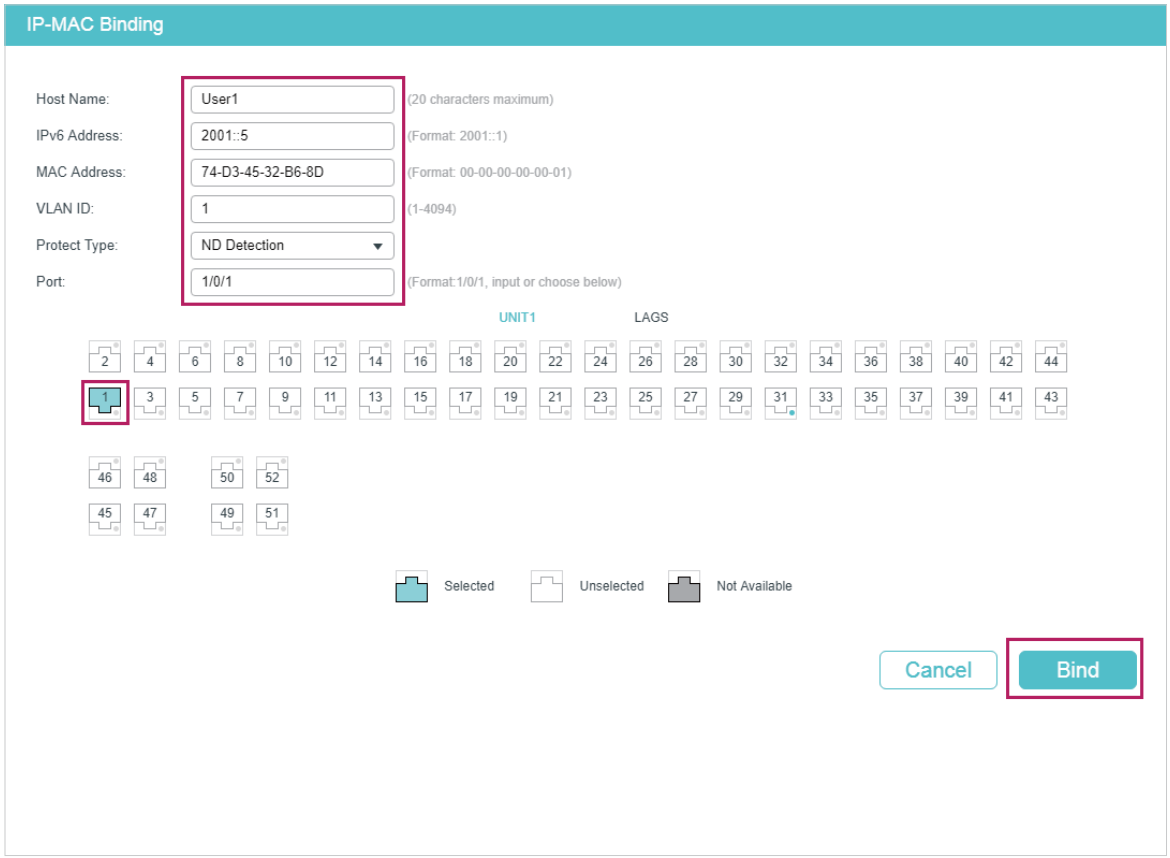
3) Configure ND Detection on ports. Since port 1/0/3 is connected to the gateway router, set port 1/0/3 as trusted port.

Demonstrated with T1600G-52TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

5.1.3 Using the GUI

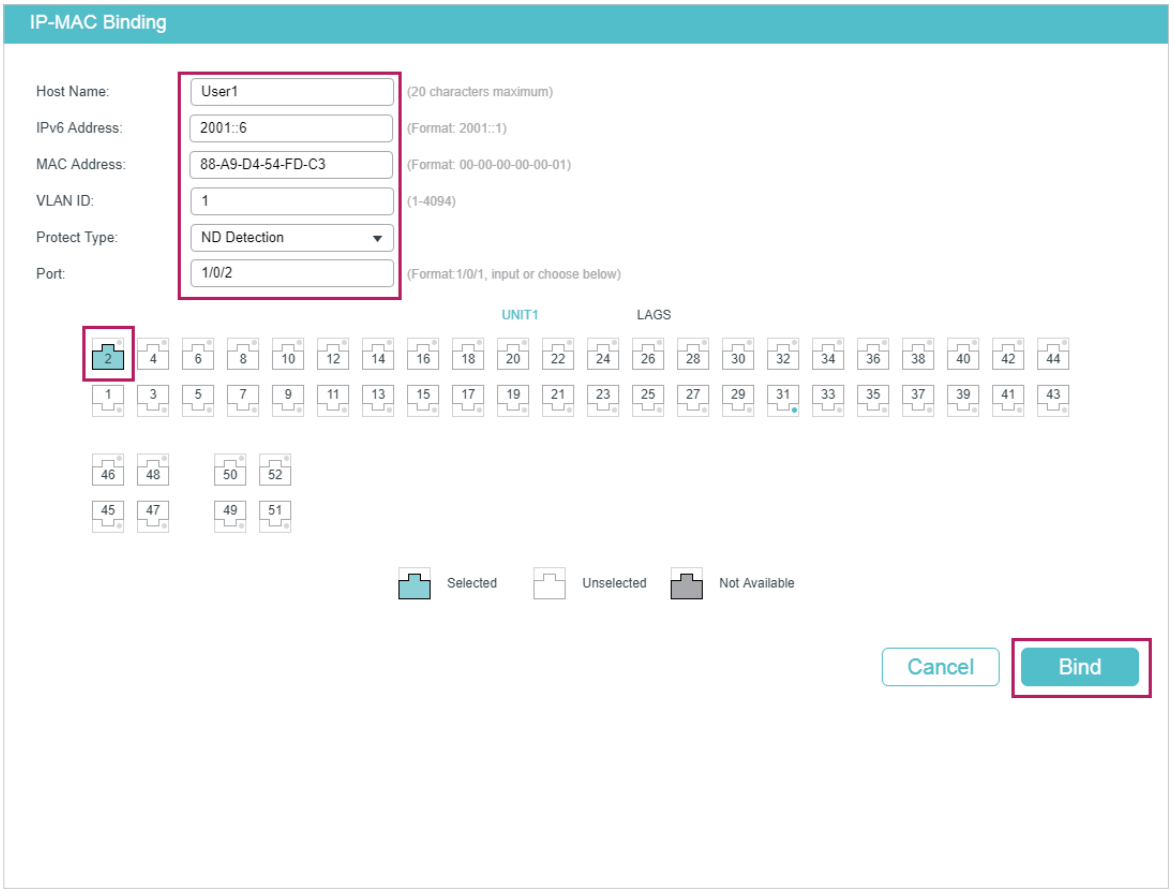
1) Choose the menu **SECURITY > IPv6 IMBP > IPv6-MAC Binding > Manual Binding** and click Add to load the following page. Enter the host name, IPv6 address, MAC address and VLAN ID of User 1, select the protect type as ND Detection, and select port 1/0/1 on the panel. Click **Apply**.

Figure 5-2 Binding Entry for User 1



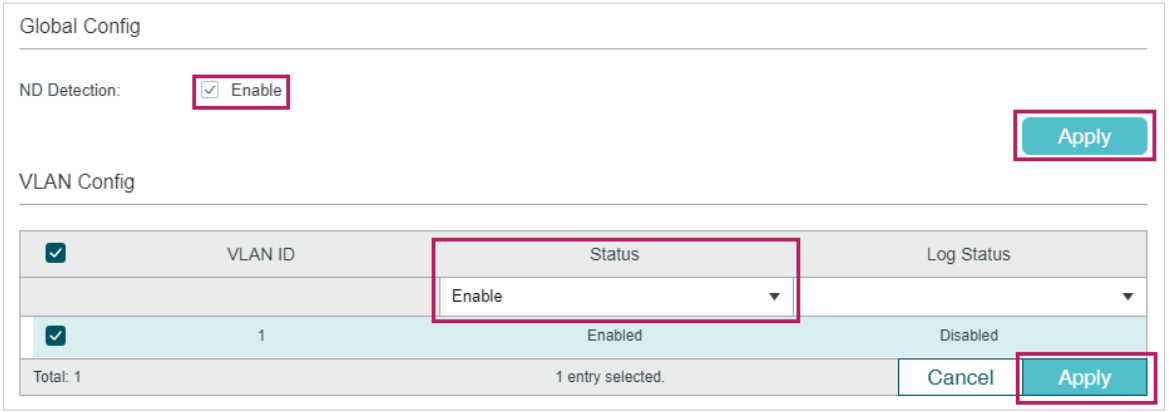
2) In the same way, add a binding entry for User 2. Enter the host name, IPv6 address, MAC address and VLAN ID of User 2, select the protect type as ND Detection, and select port 1/0/2 on the panel. Click **Apply**.

Figure 5-3 Binding Entry for User 2



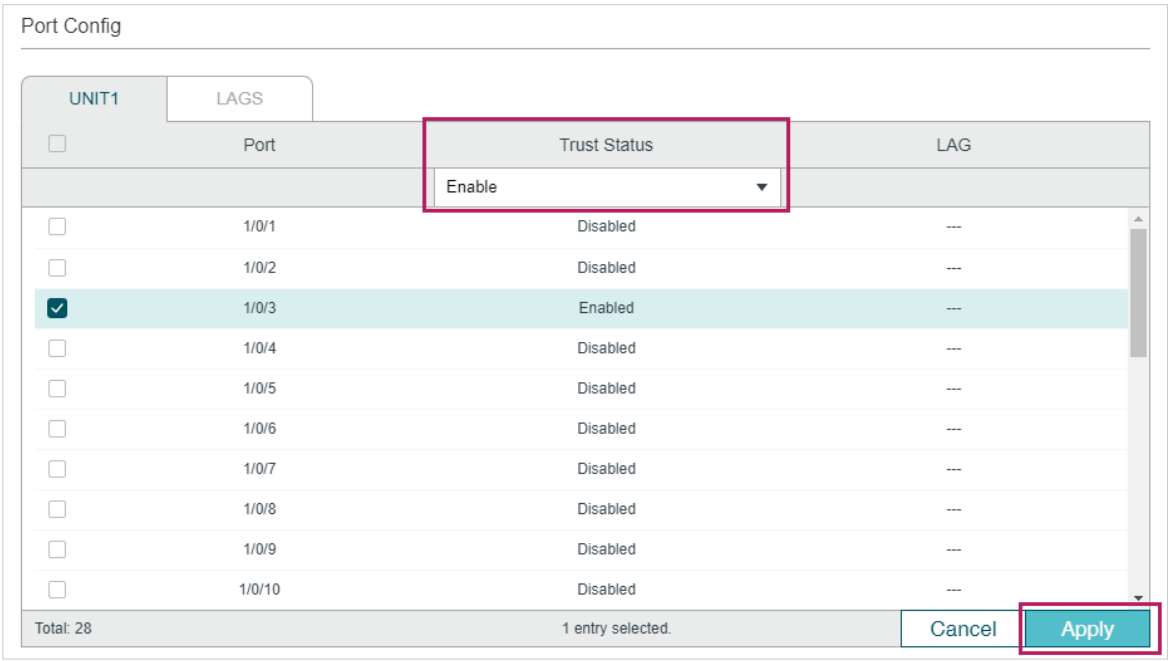
3) Choose the menu **SECURITY > IPv6 IMBP > ND Detection > Global Config** to load the following page. Enable ND Detection and click **Apply**. Select VLAN 1, change Status as Enabled and click **Apply**.

Figure 5-4 Enable ND Detection



4) Choose the menu **SECURITY > IPv6 IMBP > ND Detection > Port Config** to load the following page. By default, all ports are enabled with ND Detection. Since port 1/0/3 is connected to the gateway router, configure port 1/0/3 as trusted port. Click **Apply**.

Figure 5-5 Port Config



5) Click Save to save the settings.

5.1.4 Using the CLI

1) Manually bind the entries for User 1 and User 2.

Switch_A#configure

Switch_A(config)#ipv6 source binding User1 2001::5 74:d3:45:32:b6:8d vlan 1 interface gigabitEthernet 1/0/1 nd-detection

Switch_A(config)#ip source binding User1 2001::6 88:a9:d4:54:fd:c3 vlan 1 interface gigabitEthernet 1/0/2 nd-detection

2) Enable ND Detection globally and on VLAN 1.

Switch_A(config)#ipv6 nd detection vlan 1

3) Configure port 1/0/3 as trusted port.

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

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 IPv6-MAC Binding entries:

Switch_A#show ipv6 source binding

U	Host	IP-Addr	MAC-Addr	VID	Port	ACL	SOURCE
-	----	-------	--------	---	----	---	------
1	User1	2001::5	74:d3:45:32:b6:8d	1	Gi1/0/1	ND-D	Manual
1	User2	2001::6	88:a9:d4:54:fd:c3	1	Gi1/0/2	ND-D	Manual

Notice:

1.Here, 'ND-D' for 'ND-Detection',and'IP-V-S' for 'IP-Verify-Source'.

Verify the global configuration of ND Detection:

Switch_A#show ipv6 nd detection

Global Status: Enable

Verify the ND Detection configuration on VLAN:

Switch_A#show ipv6 nd detection vlan

VID	Enable status	Log Status
----	----------	----------
1	Enable	Disable

Verify the ND Detection configuration on ports:

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	Enable	N/A

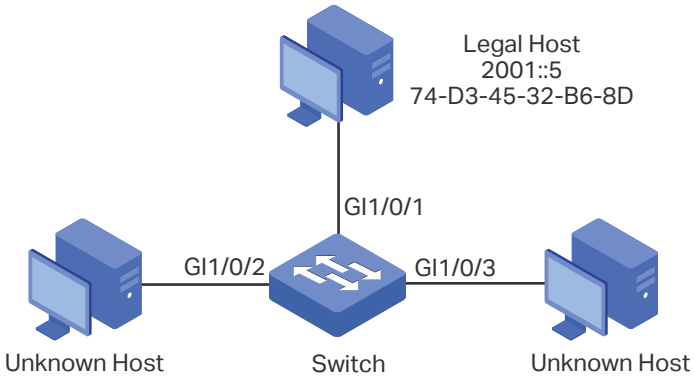
...

5.2 Example for IPv6 Source Guard

5.2.1 Network Requirements

As shown below, the legal IPv6 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 5-6 Network Topology



5.2.2 Configuration Scheme

To implement this requirement, you can use IPv6-MAC Binding and IPv6 Source Guard to filter out the packets received from the unknown hosts. The overview of configuration on the switch is as follows:

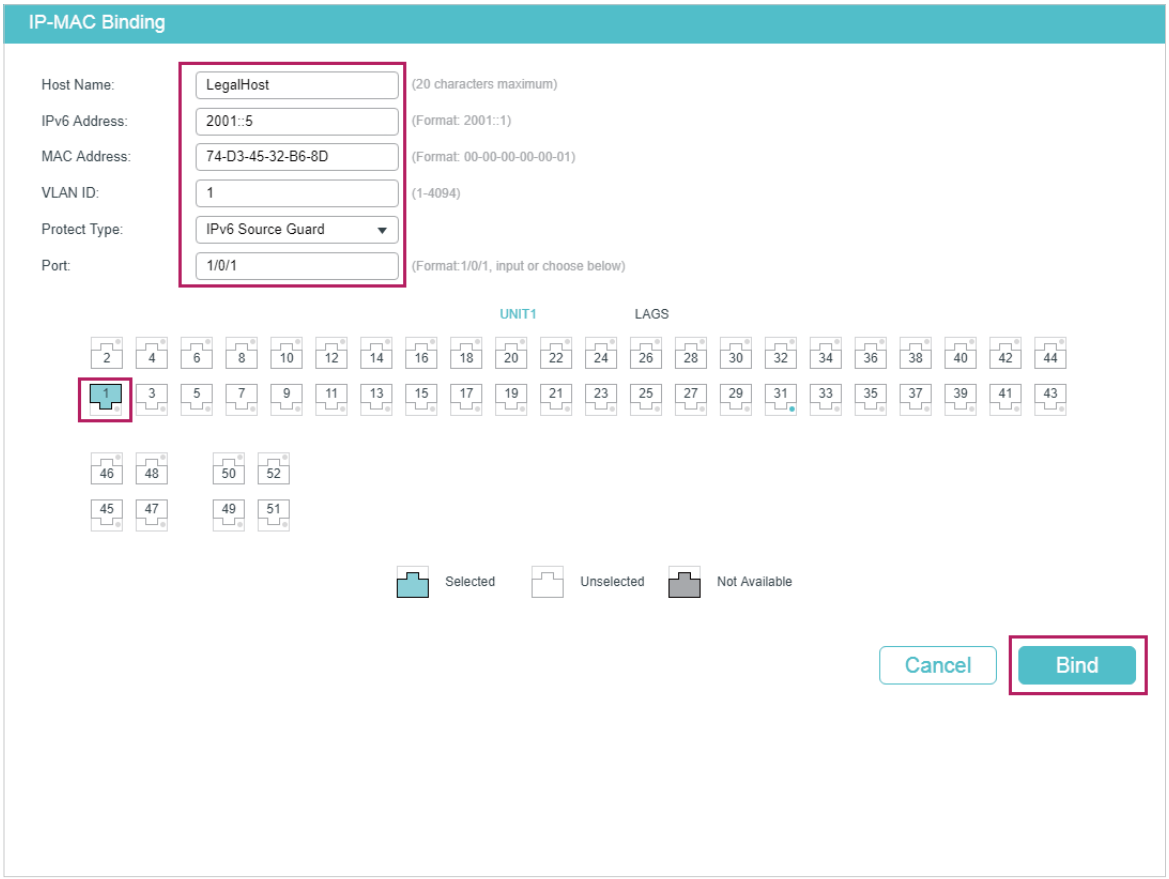
1) Bind the MAC address, IPv6 address, connected port number and VLAN ID of the legal host with IPv6-MAC Binding.
2) Enable IPv6 Source Guard on ports 1/0/1-3.

Demonstrated with T1600G-52TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

5.2.3 Using the GUI

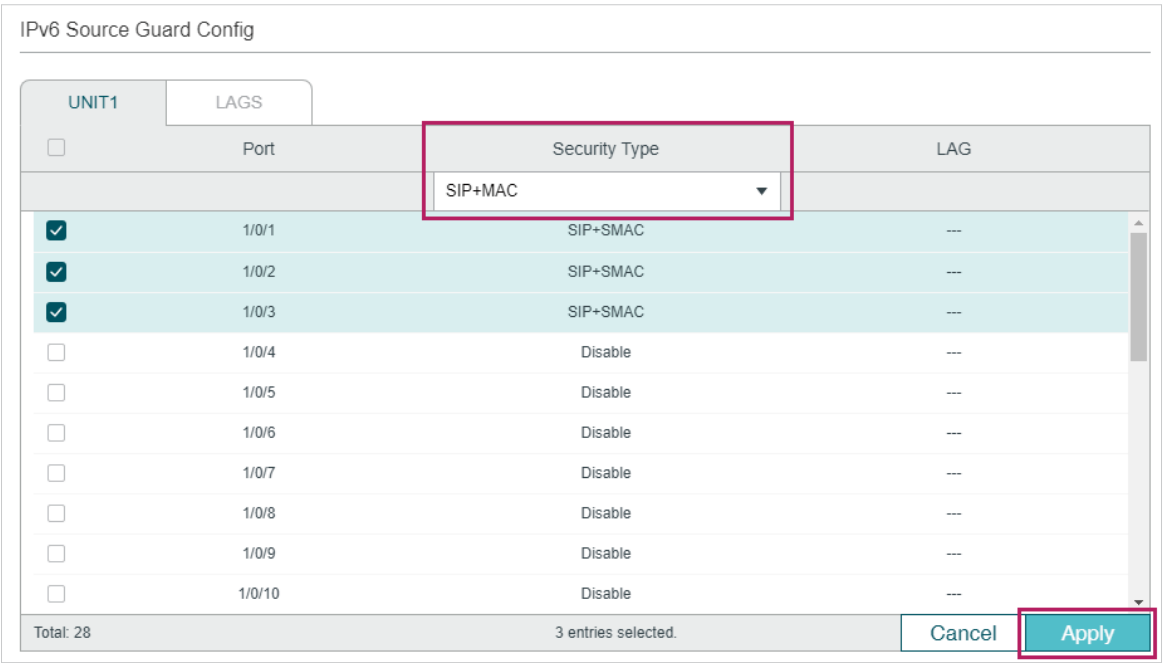
1) Choose the menu **SECURITY > IPv6 IMPB > IPv6-MAC Binding > Manual Binding** and click Add to load the following page. Enter the host name, IPv6 address, MAC address and VLAN ID of the legal host, select the protect type as , and select port 1/0/1 on the panel. Click **Apply**.

Figure 5-7 Manual Binding



2) Choose the menu **SECURITY > IPv6 IMPB > IPv6 Source Guard** to load the following page. Select ports 1/0/1-3, configure the Security Type as SIP+MAC, and click **Apply**.

Figure 5-8 IPv6 Source Guard



3) Click Save to save the settings.

5.2.4 Using the CLI

1) Manually bind the IPv6 address, MAC address, VLAN ID and connected port number of the legal host, and apply this entry to the IPv6 Source Guard feature.

   Switch#configure

   Switch(config)#ipv6 source binding legal-host 2001::5 74:d3:45:32:b6:8d vlan 1 interface gigabitEthernet 1/0/1 ipv6-verify-source

2) Enable IPv6 Source Guard on ports 1/0/1-3.

   Switch(config)# ipv6 verify source

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

   Switch(config-if-range)#ipv6 verify source sipv6+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	Host	IP-Addr	MAC-Addr	VID	Port	ACL	SOURCE
-	----	-------	--------	---	----	---	------
1	legal-host	2001::5	74:d3:45:32:b6:8d	1	Gi1/0/1	IP-V-S	Manual

Notice:

1.Here, 'ND-D' for 'ND-Detection',and'IP-V-S' for 'IP-Verify-Source'.

Verify the configuration of IPv6 Source Guard:

Switch#show ipv6 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

.....

6 Appendix: Default Parameters

Default settings of DHCP Snooping are listed in the following table:

Table 6-1 DHCPv6 Snooping

Parameter	Default Setting
Global Config	
DHCPv6 Snooping	Disable
VLAN Config	
Status	Disable
Port Config	
Maximum Entry	512

Default settings of ND Detection are listed in the following table:

Table 6-2 ND Detection

Parameter	Default Setting
Global Config	
ND Detection	Disable
VLAN Config	
Status	Disable
Log Status	Disable
Port Config	
Trust Status	Disable
ND Statistics	
Auto Refresh	Disable
Refresh Interval	5 seconds

Default settings of IPv6 Source Guard are listed in the following table:

Table 6-3 ND Detection

Parameter	Default Setting
Port Config	
Security Type	Disable

Part 25

Configuring DHCP Filter

CHAPTERS

1. DHCP Filter
2. DHCPv4 Filter Configuration
3. DHCPv6 Filter Configuration
4. Configuration Examples
5. Appendix: Default Parameters

1 DHCP Filter

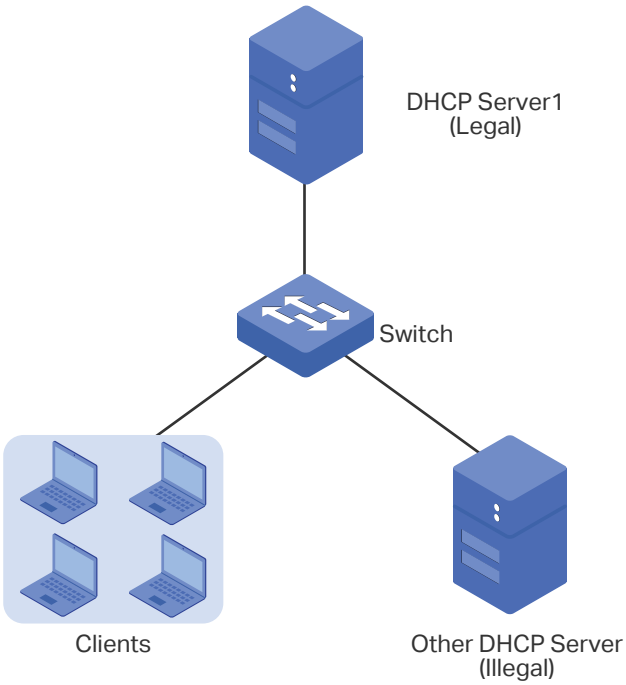
1.1 Overview

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 Filter resolves this problem.

With DHCP Filter configured, the switch can check whether the received DHCP packets are legal and discard the illegal ones. In this way, DHCP Filter ensures that users get IP addresses only from the legal DHCP server and enhances the network security.

As the following figure shows, there are both legal and illegal DHCP servers on the network. You can configure DHCP Server1 as a legal DHCP server by providing the IP address and port number of DHCP Server1. When receiving the DHCP respond packets, the switch will forward the packets from the legal DHCP server.

Figure 1-1 Network Topology



Additionally, you can limit the forwarding rate of DHCP packets on each port.

1.2 Supported Features

The switch supports DHCPv4 Filter and DHCPv6 Filter.

DHCPv4 Filter

DHCPv4 Filter is used for DHCPv4 servers and IPv4 clients.

DHCPv6 Filter

DHCPv6 Filter is used for DHCPv6 servers and IPv6 clients.

2 DHCPv4 Filter Configuration

To complete DHCPv4 Filter configuration, follow these steps:

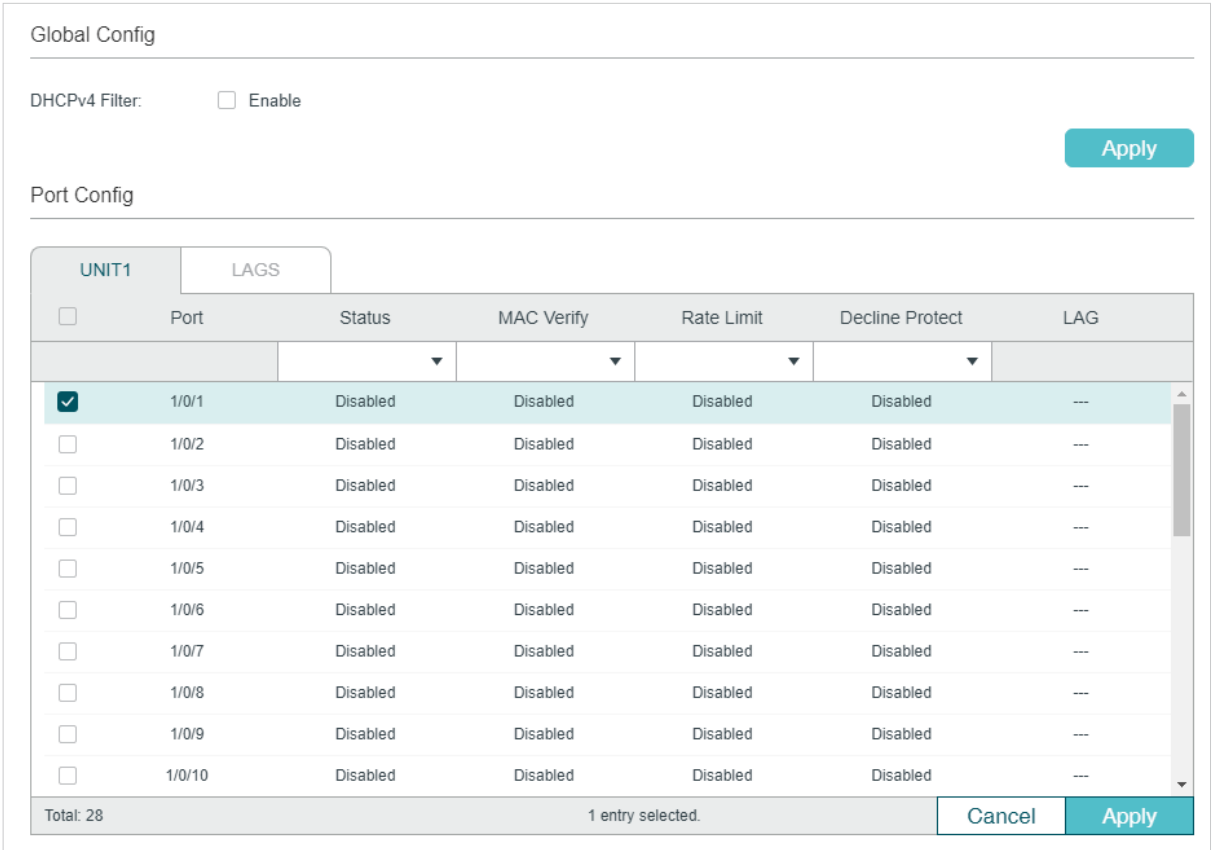
1) Configure the basic DHCPv4 Filter parameters.
2) Configure legal DHCPv4 servers.

2.1 Using the GUI

2.1.1 Configuring the Basic DHCPv4 Filter Parameters

Choose the menu **SECURITY > DHCP Filter > DHCPv4 Filter > Basic Config** to load the following page.

Figure 2-1 DHCPv4 Filter Basic Config



Follow these steps to complete the basic settings of DHCPv4 Filter:

1) In the **Global Config** section, enable DHCPv4 globally.
2) In the **Port Config** section, select one or more ports and configure the related parameters.

Port	Displays the port number.
Status	Enable or disable DHCPv4 Filter feature on the port.
MAC Verify	Enable or disable the MAC Verify feature. There are two fields in the DHCPv4 packet that contain the MAC address of the host. The MAC Verify feature compares the two fields of a DHCPv4 packet and discards the packet if the two fields are different. This prevents the IP address resource on the DHCPv4 server from being exhausted by forged MAC addresses.
Rate Limit	Select to enable the rate limit feature and specify the maximum number of DHCPv4 packets that can be forwarded on the port per second. The excessive DHCPv4 packets will be discarded.
Decline Protect	Select to enable the decline protect feature and specify the maximum number of Decline packets that can be forwarded on the port per second. The excessive Decline packets will be discarded.
LAG	Displays the LAG that the port is in.

3) Click **Apply**.



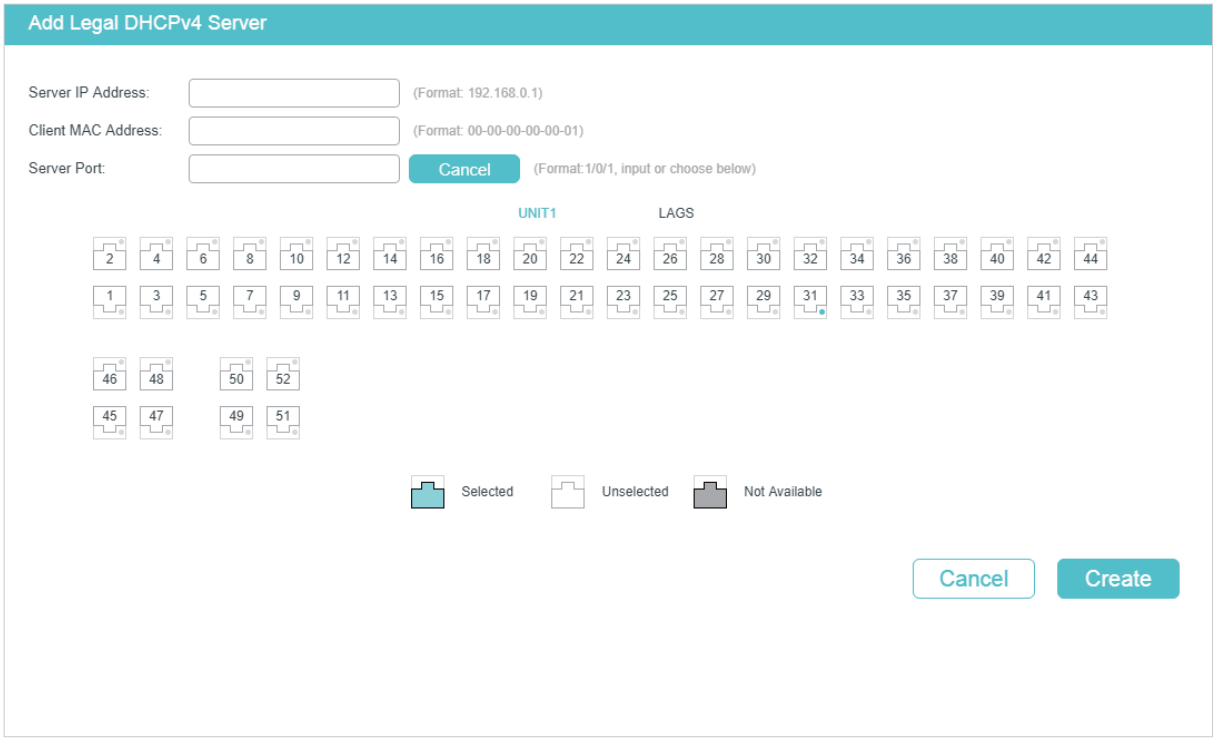
Note:

The member port of an LAG (Link Aggregation Group) follows the configuration of the LAG and not its own. The configurations of the port can take effect only after it leaves the LAG.

2.1.2 Configuring Legal DHCPv4 Servers

Choose the menu **SECURITY > DHCP Filter > DHCPv4 Filter > Legal DHCPv4 Servers** and click Add to load the following page.

Figure 2-2 Adding Legal DHCPv4 Server



Follow these steps to add a legal DHCPv4 server:

1) Configure the following parameters:

Server IP Address	Specify the IP address of the legal DHCPv4 server.
Client MAC Address	(Optional) Specify the MAC address of the DHCP Client. You can also keep this field empty, which represents for all DHCP clients.
Server Port	Select the port that the legal DHCPv4 server is connected.

2) Click **Create**.

2.2 Using the CLI

2.2.1 Configuring the Basic DHCPv4 Filter Parameters

Follow these steps to complete the basic settings of DHCPv4 Filter:

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

Step 2	**ip dhcp filter** Enable DHCPv4 Filter globally.
Step 3	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| interface port-channel** *port-channel-id* **| interface range port-channel** *port-channel-id-list* **}** Enter interface configuration mode.
Step 4	**ip dhcp filter** Enable DHCPv4 Filter on the port.
Step 5	**ip dhcp filter 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 6	**ip dhcp filter 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 7	**ip dhcp filter 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 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 8	**show ip dhcp filter** Verify the global DHCPv4 Filter configuration.
Step 9	**show ip dhcp filter interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id* **]** Verify the DHCPv4 Filter configuration of the port.
Step 10	**end** Return to privileged EXEC mode.
Step 11	**copy running-config startup-config** Save the settings in the configuration file.

Note:

The member port of an LAG (Link Aggregation Group) follows the configuration of the LAG and not its own. The configurations of the port can take effect only after it leaves the LAG.

The following example shows how to enable DHCPv4 Filter globally and how to enable DHCPv4 Filter, enable the MAC verify feature, set the limit rate as 10 pps and set the decline rate as 20 pps on port 1/0/1:

Switch#configure

Switch(config)#ip dhcp filter

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

Switch(config-if)#ip dhcp filter

Switch(config-if)#ip dhcp filter mac-verify

Switch(config-if)#ip dhcp filter limit rate 10

Switch(config-if)#ip dhcp filter decline rate 20

Switch(config-if)##show ip dhcp filter

Global Status: Enable

Switch(config-if)#show ip dhcp filter interface gigabitEthernet 1/0/1

Interface	state	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

2.2.2 Configuring Legal DHCPv4 Servers

Follow these steps configure legal DHCPv4 servers:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip dhcp filter server permit-entry server-ip** *ipAddr* **client-mac** macAddr **interface { fastEthernet** *port-list* **| gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **}** Create an entry for the legal DHCPv4 server. *ipAddr*: Specify the IP address of the legal DHCPv4 server. macAddr : Specify the MAC address of the DHCP Client. The value “all” means all client mac addresses. *port-list* | *port-channel-id*: Specify the port that the legal DHCPv4 server is connected to.

Step 3	**show ip dhcp filter server permit-entry** Verify configured legal DHCPv4 server information.
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 entry for the legal DHCPv4 server whose IP address is 192.168.0.100 and connected port number is 1/0/1 without client MAC address restricted:

Switch#configure

Switch(config)#ip dhcp filter server permit-entry server-ip 192.168.0.100 **client-mac** all **interface gigabitEthernet** 1/0/1

Switch(config)#show ip dhcp filter server permit-entry

Server IP Client MAC Interface

--- --- ---

192.168.0.100 all Gi1/0/1

Switch(config)#end

Switch#copy running-config startup-config

3 DHCPv6 Filter Configuration

To complete DHCPv6 Filter configuration, follow these steps:

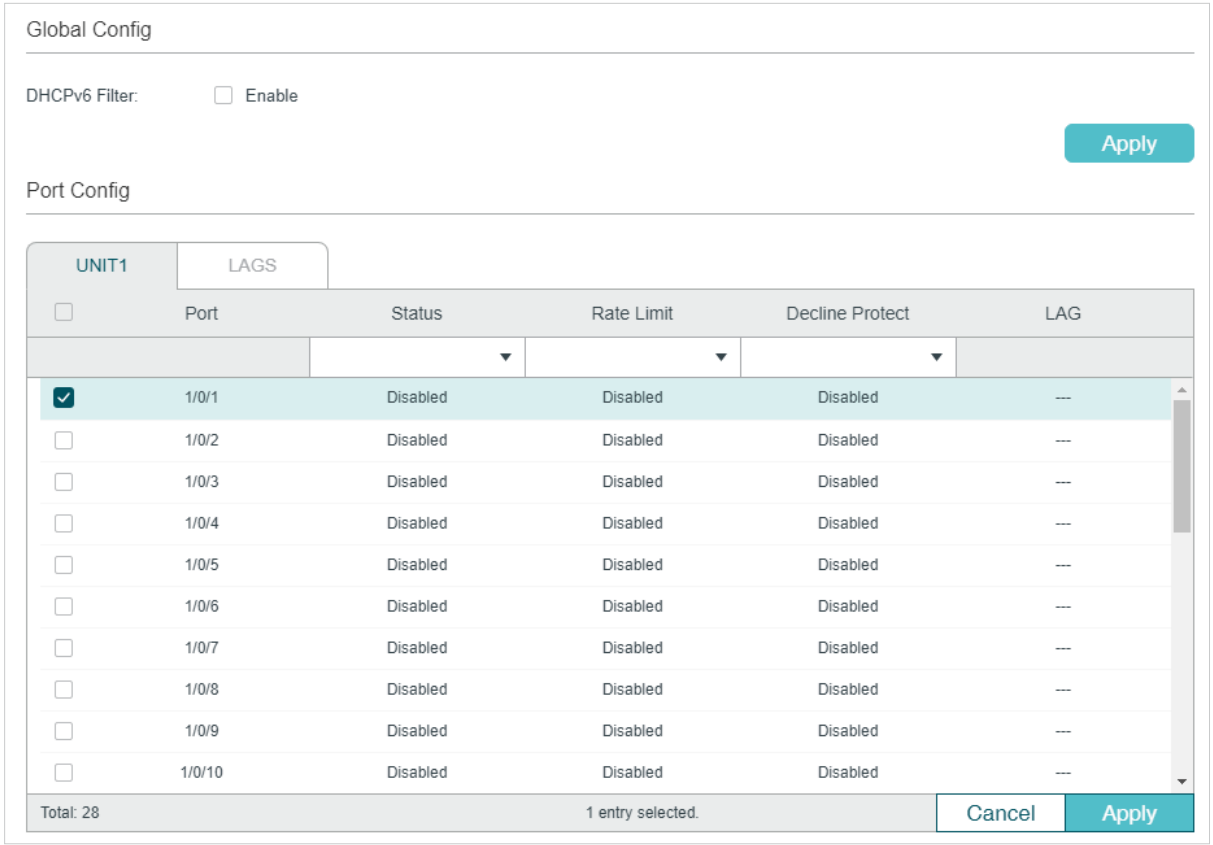
1) Configure the basic DHCPv6 Filter parameters.
2) Configure legal DHCPv6 servers.

3.1 Using the GUI

3.1.1 Configuring the Basic DHCPv6 Filter Parameters

Choose the menu **SECURITY > DHCP Filter > DHCPv6 Filter > Basic Config** to load the following page.

Figure 3-1 DHCPv6 Filter Basic Config



Follow these steps to complete the basic settings of DHCPv6 Filter:

1) In the **Global Config** section, enable DHCPv6 globally.
2) In the **Port Config** section, select one or more ports and configure the related parameters.

Port	Displays the port number.
Status	Enable or disable DHCPv6 Filter feature on the port.
Rate Limit	Select to enable the rate limit feature and specify the maximum number of DHCPv6 packets that can be forwarded on the port per second. The excessive DHCPv6 packets will be discarded.
Decline Protect	Select to enable the decline protect feature and specify the maximum number of DHCPv6 Decline packets that can be forwarded on the port per second. The excessive DHCPv6 Decline packets will be discarded.
LAG	Displays the LAG that the port is in.

3) Click **Apply**.

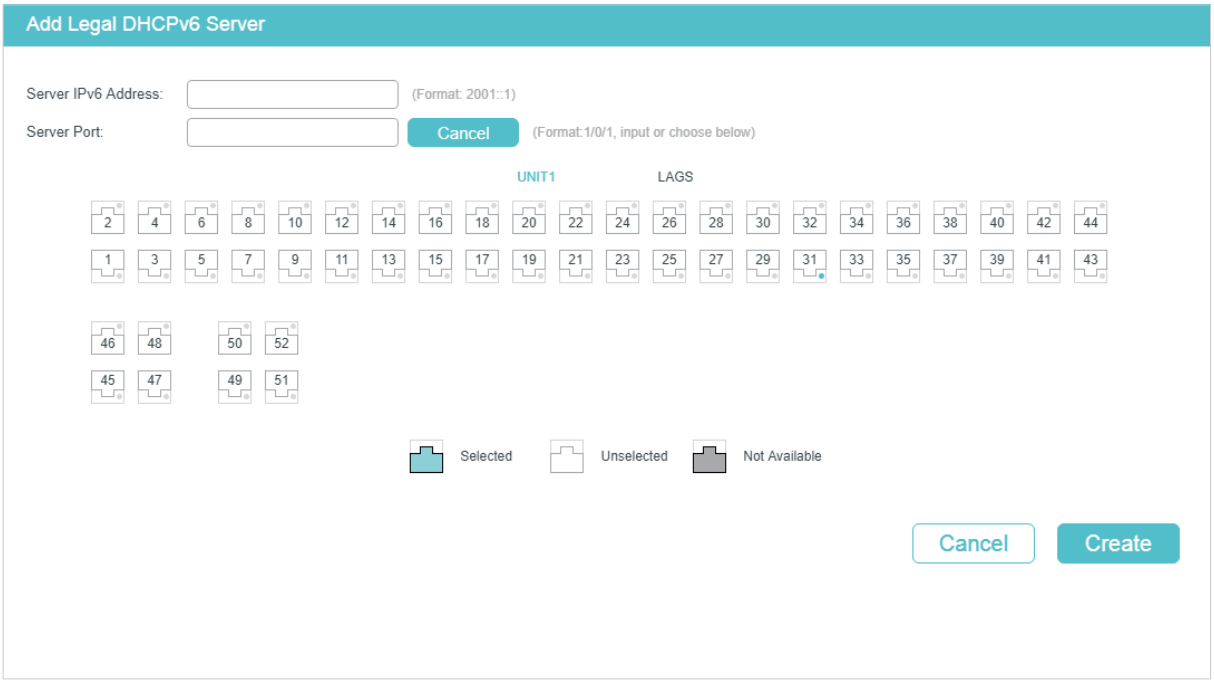
Note:

The member port of an LAG (Link Aggregation Group) follows the configuration of the LAG and not its own. The configurations of the port can take effect only after it leaves the LAG.

3.1.2 Configuring Legal DHCPv6 Servers

Choose the menu **SECURITY > DHCP Filter > DHCPv6 Filter > Legal DHCPv6 Servers** and click Add to load the following page.

Figure 3-2 Adding Legal DHCPv6 Server



Follow these steps to add a legal DHCPv6 server:

1) Configure the following parameters:

Server IPv6 Address	Specify the IP address of the legal DHCPv6 server.
Server Port	Select the port that the legal DHCPv6 server is connected.

2) Click **Create**.

3.2 Using the CLI

3.2.1 Configuring the Basic DHCPv6 Filter Parameters

Follow these steps to complete the basic settings of DHCPv6 Filter:

Step 1	**configure** Enter global configuration mode.
Step 2	**ipv6 dhcp filter** Enable DHCPv6 Filter globally.
Step 3	**interface { fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list* **| interface port-channel** *port-channel-id* **| interface range port-channel** *port-channel-id-list* **}** Enter interface configuration mode.
Step 4	**ipv6 dhcp filter** Enable DHCPv6 Filter on the port.
Step 5	**ipv6 dhcp filter 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	**ipv6 dhcp filter 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 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	**show ipv6 dhcp filter** Verify the global DHCPv6 Filter configuration.
Step 8	**show ipv6 dhcp filter interface [fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **| port-channel** *port-channel-id* **]** Verify the DHCPv6 Filter 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.



Note:

The member port of an LAG (Link Aggregation Group) follows the configuration of the LAG and not its own. The configurations of the port can take effect only after it leaves the LAG.

The following example shows how to enable DHCPv6 Filter globally and how to enable DHCPv6 Filter, set the limit rate as 10 pps and set the decline rate as 20 pps on port 1/0/1:

Switch#configure

Switch(config)#ipv6 dhcp filter

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

Switch(config-if)#ipv6 dhcp filter

Switch(config-if)#ipv6 dhcp filter limit rate 10

Switch(config-if)#ipv6 dhcp filter decline rate 20

Switch(config-if)##show ipv6 dhcp filter

Global Status: Enable

Switch(config-if)#show ip dhcp filter interface gigabitEthernet 1/0/1

Interface	state	Limit-Rate	Dec-rate	LAG
---	---	---	---	---
Gi1/0/1	Enable	10	20	N/A

Switch(config-if)#end

Switch#copy running-config startup-config

3.2.2 Configuring Legal DHCPv6 Servers

Follow these steps configure legal DHCPv6 servers:

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

Step 2	**ipv6 dhcp filter server permit-entry server-ip** *ipAddr* **interface { fastEthernet** *port-list* **| gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **}** Create an entry for the legal DHCPv6 server. *ipAddr*: Specify the IPv6 address of the legal DHCPv6 server. *port-list* | *port-channel-id*: Specify the port that the legal DHCPv6 server is connected to.
Step 3	**show ip dhcp filter server permit-entry** Verify configured legal DHCPv6 server information.
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 entry for the legal DHCPv6 server whose IPv6 address is 2001::54 and connected port number is 1/0/1:

Switch#configure

Switch(config)#ipv6 dhcp filter server permit-entry server-ip 2001::54 **interface gigabitEthernet** 1/0/1

Switch(config)#show ipv6 dhcp filter server permit-entry

Server IP Interface

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

2001::54 Gi1/0/1

Switch(config)#end

Switch#copy running-config startup-config

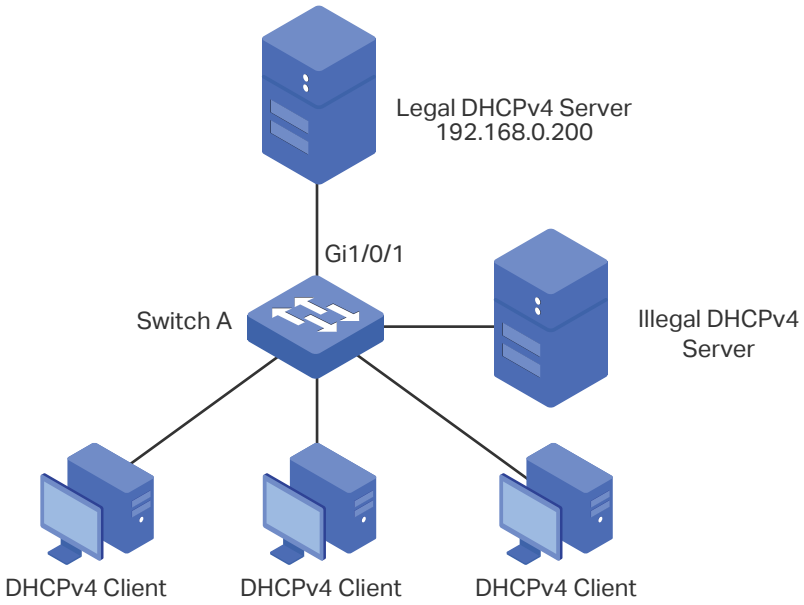
4 Configuration Examples

4.1 Example for DHCPv4 Filter

4.1.1 Network Requirements

As shown below, all the DHCPv4 clients get IP addresses from the legal DHCPv4 server, and any other DHCPv4 server in the LAN is regarded as illegal. Now it is required that only the legal DHCPv4 server is allowed to assign IP addresses to the clients.

Figure 4-1 Network Topology



4.1.2 Configuration Scheme

To meet the requirements, you can configure DHCPv4 Filter to filter the DHCPv4 packets from the illegal DHCPv4 server.

The overview of configuration is as follows:

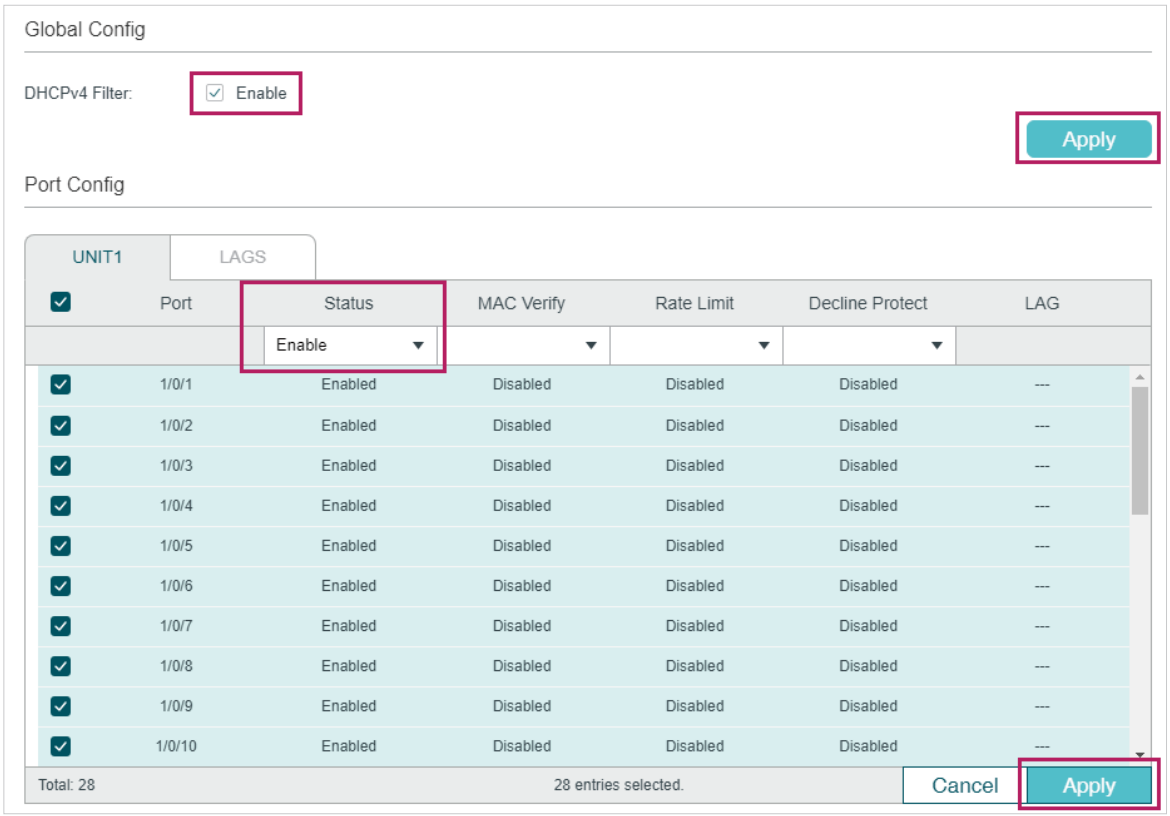
1) Enable DHCPv4 Filter globally and on all ports.
2) Create an entry for the legal DHCPv4 server.

Demonstrated with T1600G-52TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

4.1.3 Using the GUI

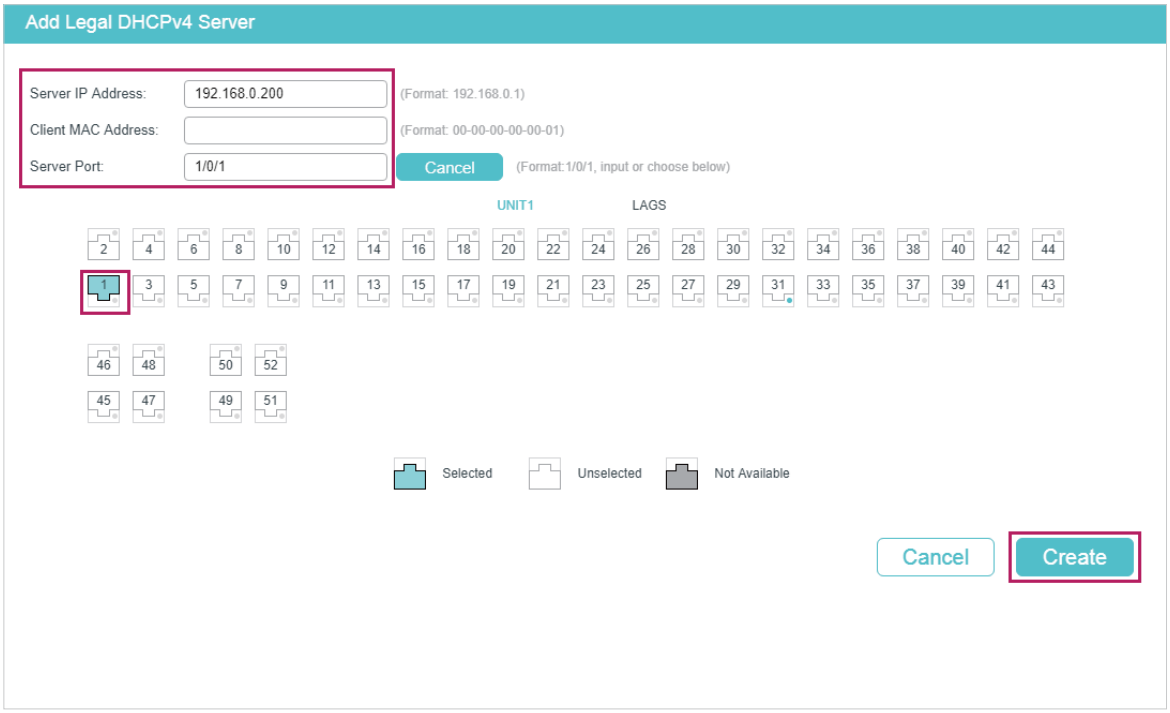
1) Choose the menu **SECURITY > DHCP Filter > DHCPv4 Filter > Basic Config** to load the following page. Enable DHCPv4 Filter globally and click **Apply**. Select all ports, change Status as Enable, and click **Apply**.

Figure 4-2 Basic Config



2) Choose the menu **SECURITY > DHCP Filter > DHCPv4 Filter > Legal DHCPv4 Servers** and click Add to load the following page. Specify the IP address and connected port number of the legal DHCPv4 server. Click **Create**.

Figure 4-3 Create Entry for Legal DHCPv4 Server



3) Click Save to save the settings.

4.1.4 Using the CLI

1) Enable DHCPv4 Filter globally and on all pots:

Switch_A#configure

Switch_A(config)#ip dhcp filter

Switch_A(config)#interface range gigabitEthernet 1/0/1-52

Switch_A(config-if-range)#ip dhcp filter

Switch_A(config-if-range)#exit

2) Create an entry for the legal DHCPv4 server:

Switch_A(config)#ip dhcp filter server permit-entry server-ip 192.168.0.200 client-mac all interface gigabitEthernet 1/0/1

Switch_A(config)#end

Switch_A#copy running-config startup-config

Verify the Configuration

Verify the global DHCPv4 Filter configuration:

Switch_A#show ip dhcp filter

Global Status: Enable

Verify the DHCPv4 Filter configuration on ports:

Switch_A#show ip dhcp filter interface

Interface	state	MAC-Verify	Limit-Rate	Dec-rate	LAG
Gi1/0/1	Enable	Disable	Disable	Disable	N/A
Gi1/0/2	Enable	Disable	Disable	Disable	N/A
Gi1/0/3	Enable	Disable	Disable	Disable	N/A
Gi1/0/4	Enable	Disable	Disable	Disable	N/A

.....

Verify the legal DHCPv4 server configuration:

Switch_A#show ip dhcp filter server permit-entry

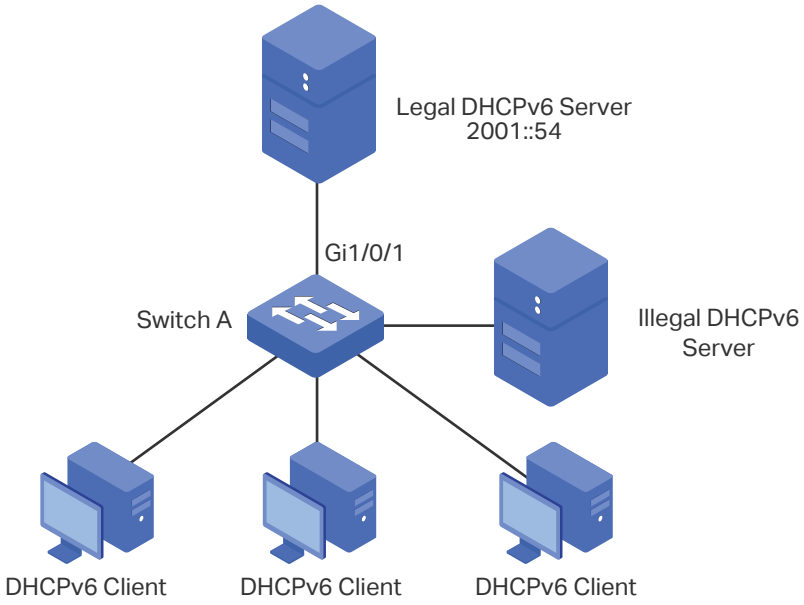
Server IP	Client MAC	Interface
192.168.0.200	all	Gi1/0/1

4.2 Example for DHCPv6 Filter

4.2.1 Network Requirements

As shown below, all the DHCPv6 clients get IP addresses from the legal DHCPv6 server, and any other DHCPv6 server in the LAN is regarded as illegal. Now it is required that only the legal DHCPv6 server is allowed to assign IP addresses to the clients.

Figure 4-1 Network Topology



4.2.2 Configuration Scheme

To meet the requirements, you can configure DHCPv6 Filter to filter the DHCPv6 packets from the illegal DHCPv6 server.

The overview of configuration is as follows:

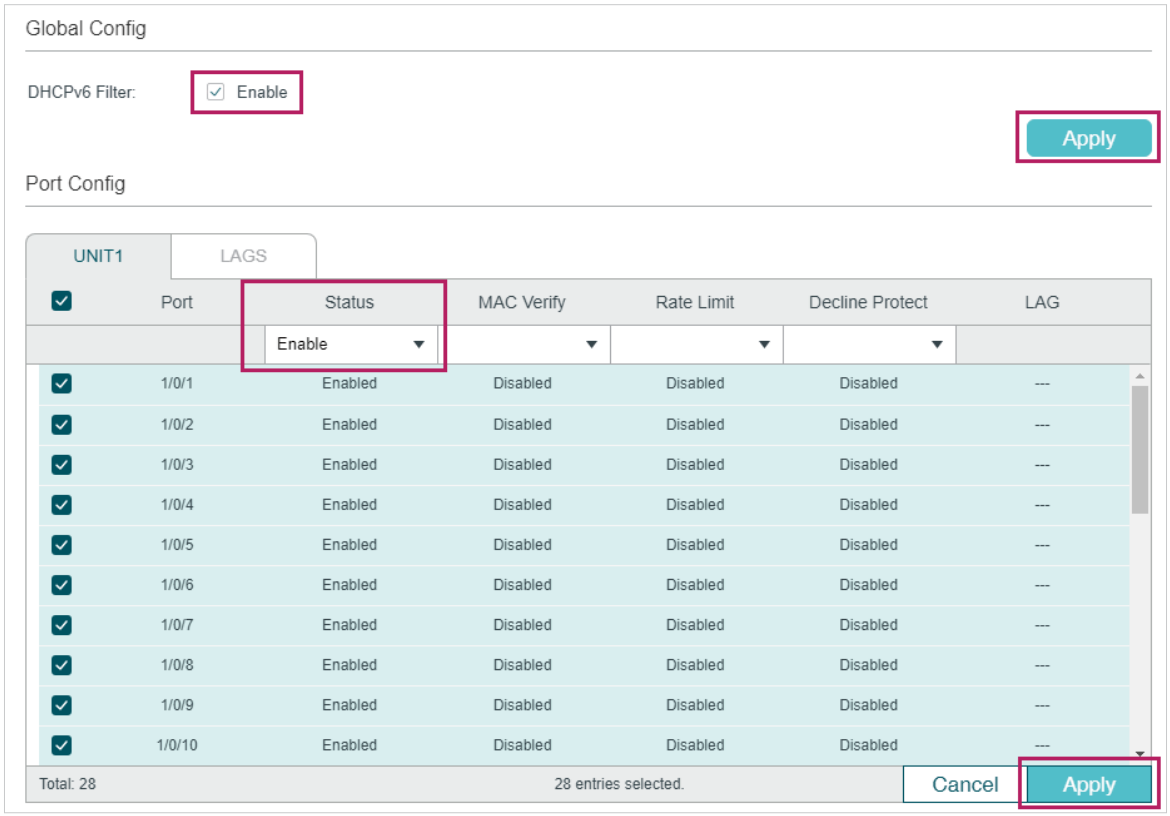
1) Enable DHCPv6 Filter globally and on all ports.
2) Create an entry for the legal DHCPv6 server.

Demonstrated with T2600G-52TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

4.2.3 Using the GUI

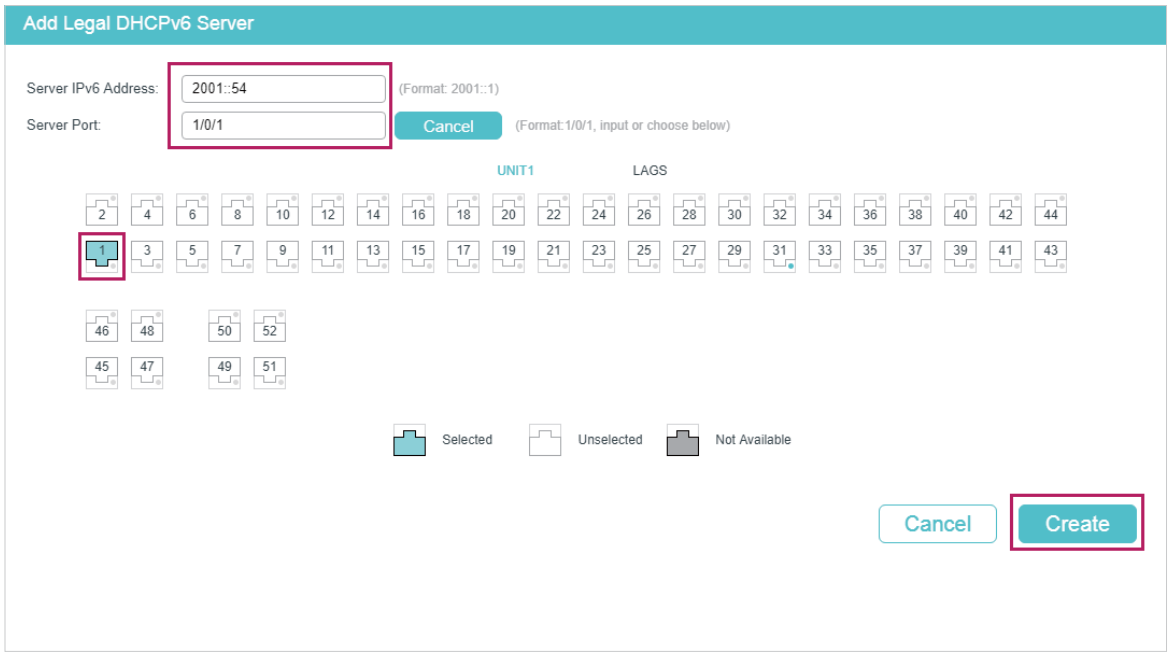
1) Choose the menu **SECURITY > DHCP Filter > DHCPv6 Filter > Basic Config** to load the following page. Enable DHCPv6 Filter globally and click **Apply**. Select all ports, change Status as Enable, and click **Apply**.

Figure 4-2 Basic Config



2) Choose the menu **SECURITY > DHCP Filter > DHCPv6 Filter > Legal DHCPv6 Servers** and click Add to load the following page. Specify the IP address and connected port number of the legal DHCPv6 server. Click **Create**.

Figure 4-3 Create Entry for Legal DHCPv6 Server



3) Click Save to save the settings.

4.2.4 Using the CLI

1) Enable DHCPv6 Filter globally and on all pots:

   Switch_A#configure

   Switch_A(config)#ipv6 dhcp filter

   Switch_A(config)#interface range gigabitEthernet 1/0/1-52

   Switch_A(config-if-range)#ipv6 dhcp filter

   Switch_A(config-if-range)#exit

2) Create an entry for the legal DHCPv6 server:

   Switch_A(config)#ipv6 dhcp filter server permit-entry server-ip 2001::54 interface gigabitEthernet 1/0/1

   Switch_A(config)#end

   Switch_A#copy running-config startup-config

Verify the Configuration

Verify the global DHCPv6 Filter configuration:

Switch_A#show ipv6 dhcp filter

Global Status: Enable

Verify the DHCPv6 Filter configuration on ports:

Switch_A#show ipv6 dhcp filter interface

Interface	state	Limit-Rate	Dec-rate	LAG
---	---	---	---	---
Gi1/0/1	Enable	Disable	Disable	N/A
Gi1/0/2	Enable	Disable	Disable	N/A
Gi1/0/3	Enable	Disable	Disable	N/A
Gi1/0/4	Enable	Disable	Disable	N/A

.....

Verify the legal DHCPv6 server configuration:

Switch_A#show ipv6 dhcp filter server permit-entry

```
Server IP          Interface
---------------    ----------
2001::54           Gi1/0/1
```

5 Appendix: Default Parameters

Default settings of DHCPv4 Filter are listed in the following table:

Table 5-1 DHCPv4 Filter

Parameter	Default Setting
Global Config	
DHCPv4 Filter	Disable
Port Config	
Status	Disable
MAC Verify	Disable
Rate Limit	Disable
Decline Protect	Disable

Table 5-2 DHCPv6 Filter

Parameter	Default Setting
Global Config	
DHCPv6 Filter	Disable
Port Config	
Status	Disable
Rate Limit	Disable
Decline Protect	Disable

Part 26

Configuring DoS Defend

CHAPTERS

1. Overview
2. DoS Defend Configuration
3. Appendix: Default Parameters

1 Overview

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.

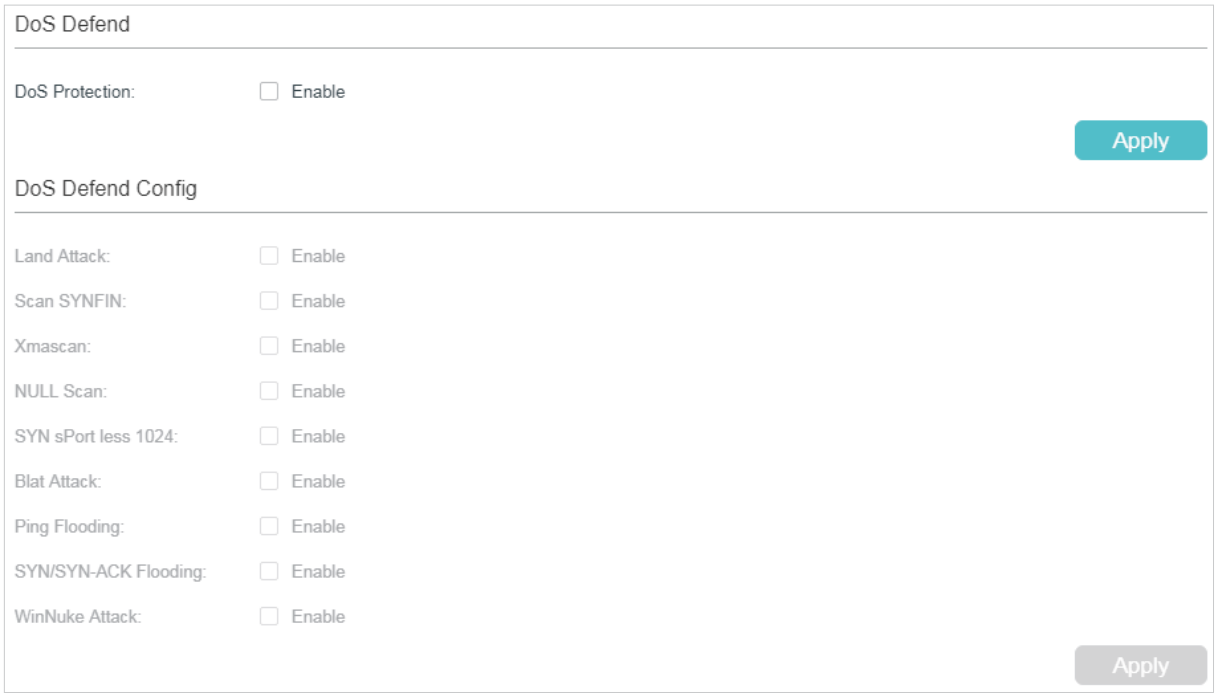
With DoS Defend feature, the switch can analyze the specific fields of the IP packets, distinguish the malicious DoS attack packets and discard them directly. Also, DoS Defend feature can limit the transmission rate of legal packets. When the number of legal packets exceeds the threshold value and may incur a breakdown of the network, the switch will discard the packets.

2 DoS Defend Configuration

2.1 Using the GUI

Choose the menu **SECURITY > DoS Defend** to load the following page.

Figure 2-1 DoS Defend



Follow these steps to configure DoS Defend:

1) In the **DoS Defend** section, enable DoS Protection and click **Apply**.
2) In the **DoS Defend Config** section, select one or more defend types according to your needs and click **Apply**. 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**.

2.2 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 | ping-of-death | smurf **}** 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

DoS Prevention State: Enabled

Type	Status
Land Attack	Enabled
Scan SYNFIN	Disabled
Xmascan	Disabled
NULL Scan	Disabled
SYN sPort less 1024	Disabled
Blat Attack	Disabled
Ping Flooding	Disabled
SYN/SYN-ACK Flooding	Disabled
WinNuke Attack	Disabled

Switch(config)#end

Switch#copy running-config startup-config

3 Appendix: Default Parameters

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

Table 3-1 DoS Defend

Parameter	Default Setting
DoS Defend	Disabled

Part 27

Monitoring the System

CHAPTERS

1. Overview
2. Monitoring the CPU
3. Monitoring the Memory

1 Overview

With System Monitor function, you can:

- Monitor the CPU utilization of the switch.
- Monitor the memory utilization of the switch.

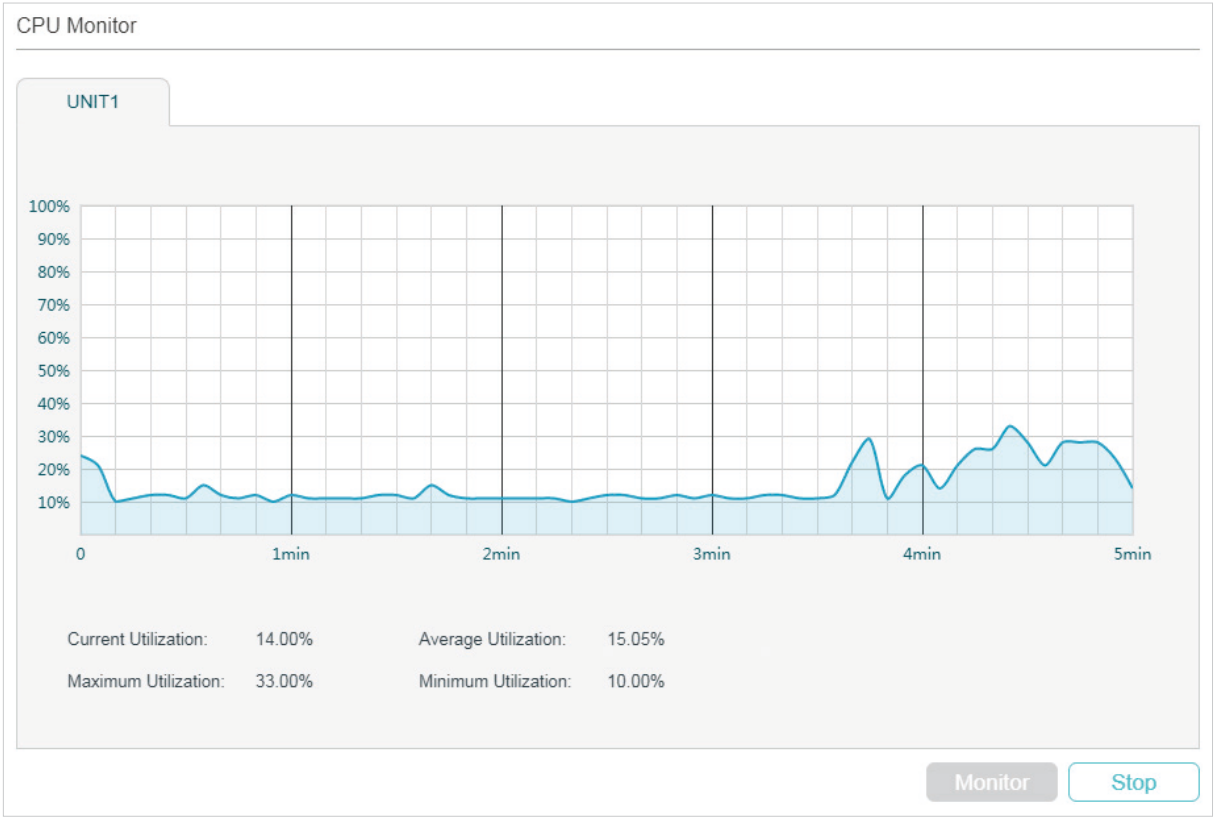
The CPU utilization should be always under 80%, and excessive use may result in switch malfunctions. For example, the switch fails to respond to management requests (ICMP ping, SNMP timeouts, slow Telnet or SSH sessions). You can monitor the system to verify a CPU utilization problem.

2 Monitoring the CPU

2.1 Using the GUI

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 five seconds.

2.2 Using the CLI

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

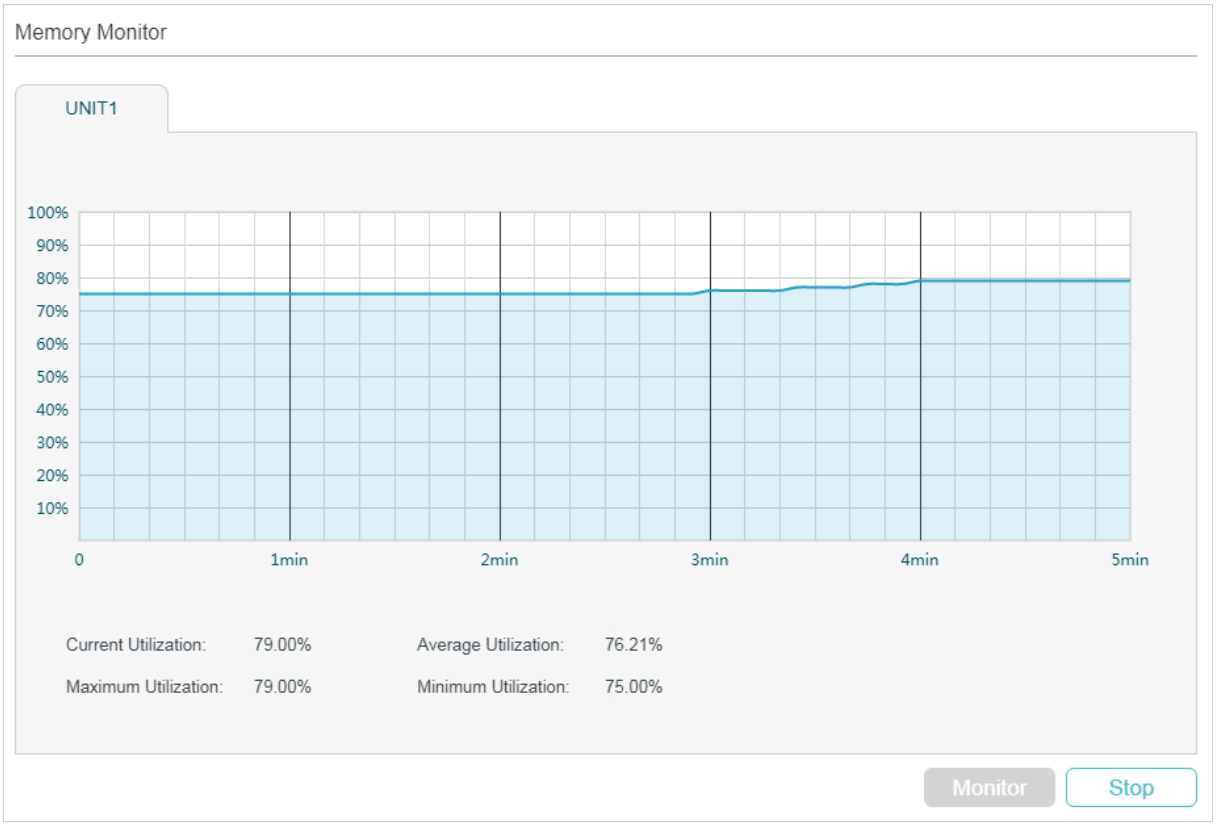
```
Unit   |                CPU Utilization
No.    |  Five-Seconds  One-Minute  Five-Minutes
------+-----------------------------------------------
1      |  13%           13%         13%
```

3 Monitoring the Memory

3.1 Using the GUI

Choose the menu **MAINTENANCE > System Monitor > Memory Monitor** to load the following page.

Figure 3-1 Monitoing the Memory



Click **Monitor** to enable the switch to monitor and display its memory utilization rate every five seconds.

3.2 Using the CLI

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 current memory utilization of the switch.

The following example shows how to monitor the memory:

Switch#show memory-utilization

```
Unit   |   Current Memory Utilization
------+--------------------------
1      |   74%
```

Part 28

Monitoring Traffic

CHAPTERS

1. Traffic Monitor
2. Appendix: Default Parameters

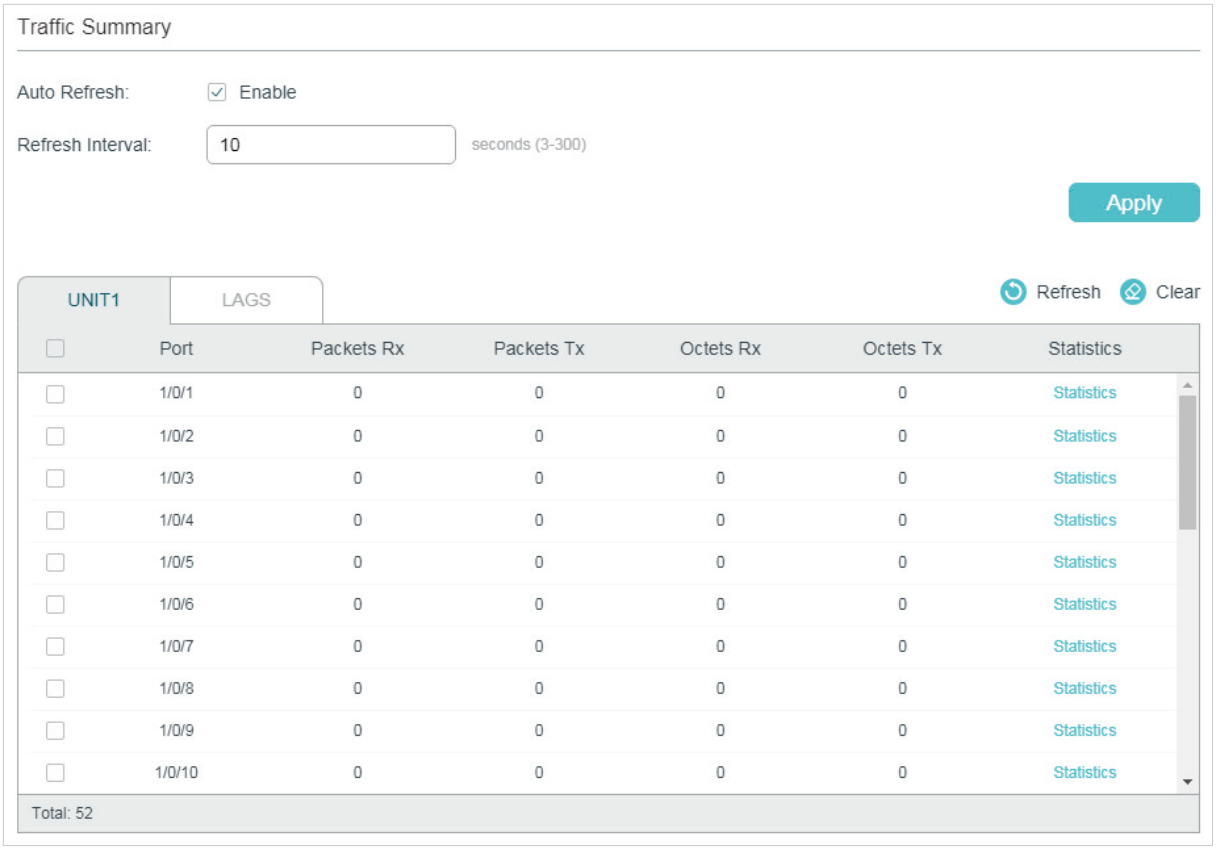
1 Traffic Monitor

With Traffic Monitor function, you can monitor each port's traffic information, including the traffic summary and traffic statistics in detail.

1.1 Using the GUI

Choose the menu **MAINTENANCE > Traffic Monitor** 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**, or click **Refresh**.

Auto Refresh:	With this option enabled, the switch will automatically refresh the traffic summary.
Refresh Interval:	Specify the time interval for the switch to refresh the traffic summary.

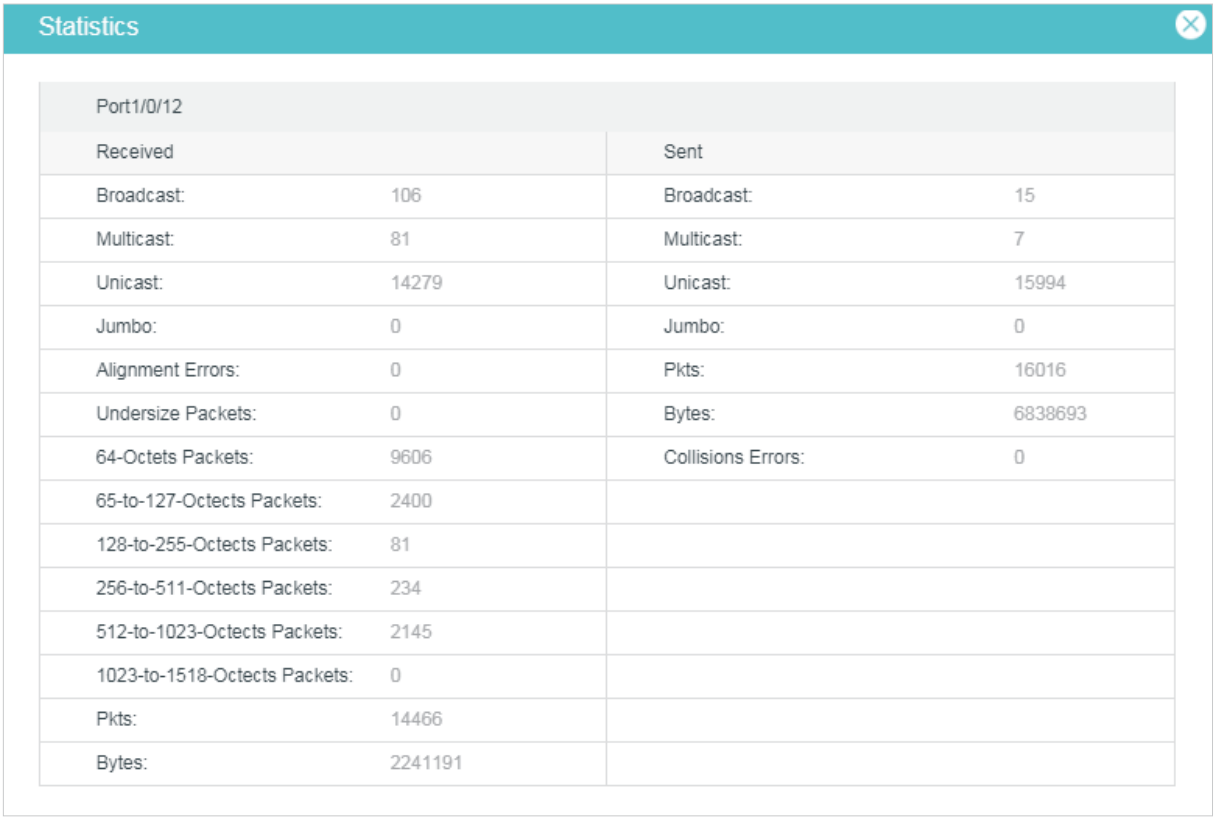
2) In the **Traffic Summary** section, click **UNIT1** to show the information of the physical ports, and click **LAGS** to show the information of the LAGs.

Packets Rx:	Displays the number of packets received on the port. Error packets are not counted.

Packets Tx:	Displays the number of packets transmitted on the port. Error packets are not counted.
Octets Rx:	Displays the number of octets received on the port. Error octets are counted.
Octets Tx:	Displays the number of octets transmitted on the port. Error octets are counted .

To view a port's traffic statistics in detail, click **Statistics** on the right side of the entry.

Figure 1-2 Traffic Statistics



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. Multicast: Displays the number of valid multicast packets received on the port. Error frames are not counted. Unicast: Displays the number of valid unicast packets received on the port. Error frames are not counted. Jumbo: Displays the number of valid jumbo packets received on the port. Error frames are not counted. 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. Undersize Packets: Displays the number of the received packets (excluding error packets) that are less than 64 bytes long. 64-Octets Packets: Displays the number of the received packets (including error packets) that are 64 bytes long. 65-to-127-Octects Packets: Displays the number of the received packets (including error packets) that are between 65 and 127 bytes long. 128-to-255-Octects Packets: Displays the number of the received packets (including error packets) that are between 128 and 255 bytes long. 256-to-511-Octects Packets: Displays the number of the received packets (including error packets) that are between 256 and 511 bytes long. 512-to-1023-Octects Packets: Displays the number of the received packets (including error packets) that are between 512 and 1023 bytes long. 1023-to-1518-Octects Packets: Displays the number of the received packets (including error packets) that are between 512 and 1023 bytes long. Pkts: Displays the number of packets received on the port. Error packets are not counted. Bytes: Displays the number of bytes received on the port. Error packets are not counted.

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. Multicast: Displays the number of valid multicast packets transmitted on the port. Error frames are not counted. Unicast: Displays the number of valid unicast packets transmitted on the port. Error frames are not counted. Pkts: Displays the number of packets transmitted on the port. Error packets are not counted. Bytes: Displays the number of bytes transmitted on the port. Error packets are not counted. 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:

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

Tx Ucast / Tx Mcast / Tx Bcast / Tx Jumbo: Displays the number of valid unicast / multicast / broadcast / jumbo packets transmitted on the port. Error frames are not counted.

Tx Pkts: Displays the number of packets transmitted on the port. Error packets are not counted.

Tx Bytes: Displays the number of bytes transmitted on the port. Error packets are not counted.

Rx Ucast / Rx Mcast / Rx Bcast / Rx Jumbo: Displays the number of valid unicast / multicast / broadcast / jumbo packets received on the port. Error frames are not counted.

Rx Alignment: 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.

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

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

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

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

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

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

Rx 1024-1518Pkts: Displays the number of the received packets (including error packets) that are between 1024 and 1518 bytes long.

Rx Pkts: Displays the number of packets received on the port. Error packets are not counted.

Rx Bytes: Displays the number of bytes received on the port. Error packets are not counted.

2 Appendix: Default Parameters

Table 2-1 Traffic Statistics Monitoring

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

Part 29

Mirroring Traffic

CHAPTERS

1. Mirroring
2. Configuration Examples
3. Appendix: Default Parameters

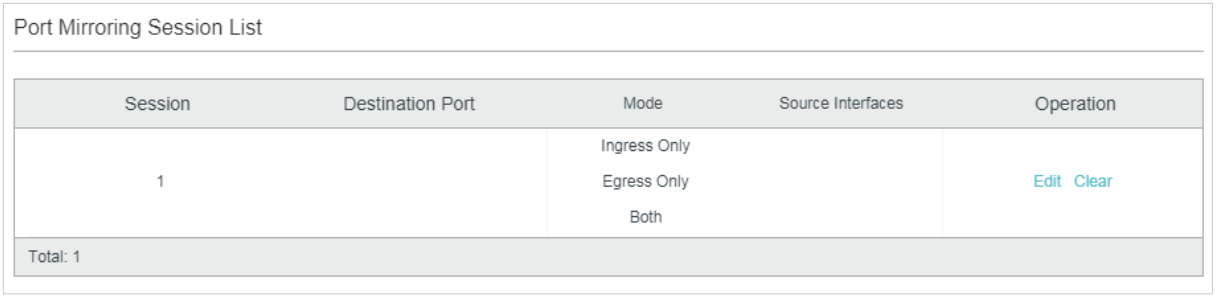
1 Mirroring

You can analyze network traffic and troubleshoot network problems using Mirroring. Mirroring allows the switch to send a copy of the traffic that passes through specified sources (ports, LAGs or the CPU) to a destination port. It does not affect the switching of network traffic on source ports, LAGs or the CPU.

1.1 Using the GUI

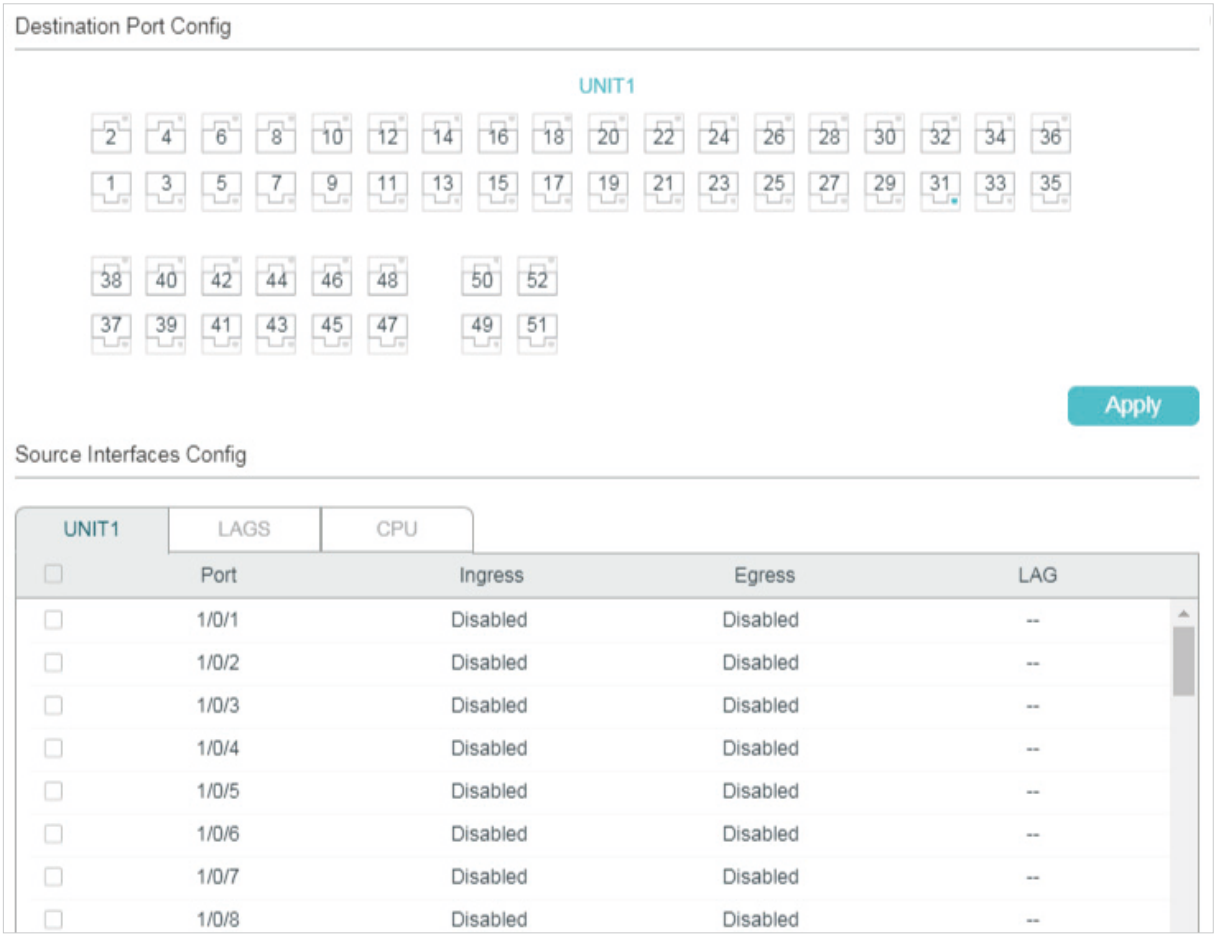
Choose the menu **MAINTENANCE > Mirroring** to load the following page.

Figure 1-1 Port Mirroring Session List



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

Figure 1-2 Configure the Mirroring Session



Follow these steps to configure the mirroring session:

1) In the **Destination Port Config** section, specify a destination port for the mirroring session, and click **Apply**.

2) In the **Source Interfaces Config** section, specify the source interfaces and click **Apply**. Traffic passing through the source interfaces will be mirrored to the destination port. There are three source interface types: port, LAG, and CPU. Choose one or more types according to your need.

UNIT1	Select the desired ports as the source interfaces. The switch will send a copy of traffic passing through the port to the destination port.
LAGS	Select the desired LAGs as the source interfaces. The switch will send a copy of traffic passing through the LAG members to the destination port.
CPU	When selected, the switch will send a copy of traffic passing through the CPU to the destination port.
Ingress	With this option enabled, the packets received by the corresponding interface (port, LAG or CPU) will be copied to the destination port. By default, it is disabled.
Egress	With this option enabled, the packets sent by the corresponding interface (port, LAG or CPU) will be copied to the destination port. By default, it is disabled.

Note:

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

1.2 Using the CLI

Follow these steps to configure Mirroring.

Step 1	**configure** Enter global configuration mode.
Step 2	**monitor session** *session_num* **destination interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port***}** Enable the port mirror function and set the destination port. *session_num*: The monitor session number. It can only be specified as 1. *port*: The destination port number. You can specify only one destination port for the mirror session.
Step 3	**monitor session** *session_num* **source { cpu** *cpu_numbr* **| interface { fastEthernet** *port-list* **| gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **}}** *mode* Configure ports or LAGs as the monitored interfaces. *session_num*: The monitor session number. It can only be specified as 1. *cpu_number*: The CPU number. It can only be specified as 1. *port-list*: List of source ports. It is multi-optional. *mode*: The monitor mode. There are three options: **rx**, **tx** and **both**: **rx**: The incoming packets of the source port will be copied to the destination port. **tx**: The outgoing packets of the source port will be copied to the destination port. **both**: Both of the incoming and outgoing packets on source port can be copied to the destination port. *Note:* You can configure one or more source interface types (ports, LAGs and the CPU) according to your needs.
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 and the CPU 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)#monitor session 1 **source cpu** 1 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

Source CPU(Ingress): cpu1

Source CPU(Egress): cpu1

Switch(config-if)#end

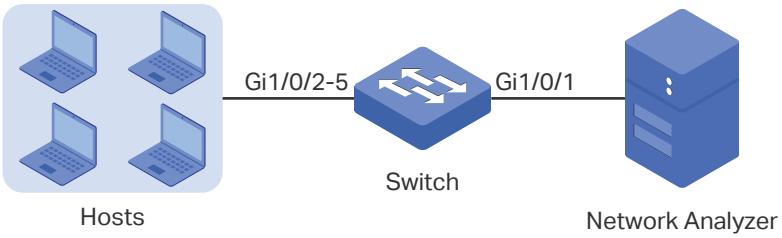
Switch#copy running-config startup-config

2 Configuration Examples

2.1 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 2-1 Network Topology



2.2 Configuration Scheme

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

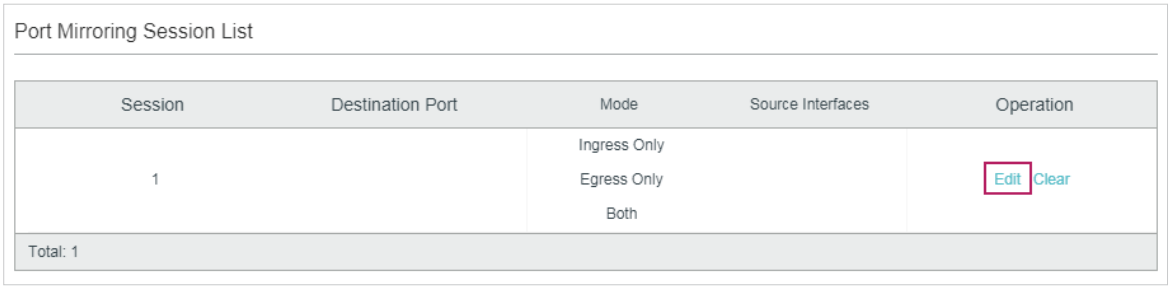
1) Specify ports 1/0/2-5 as the source ports, allowing the switch to copy the packets from the hosts.
2) Specify port 1/0/1 as the destination port so that the network analyzer can receive mirrored packets from the hosts.

Demonstrated with T1600G-52TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

2.3 Using the GUI

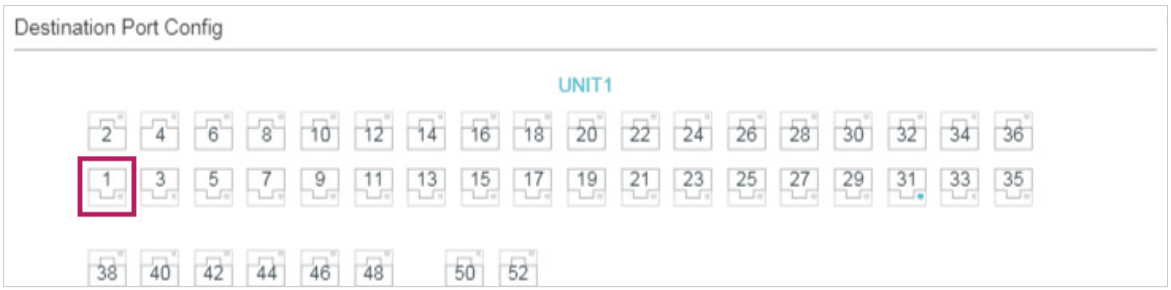
1) Choose the menu **MAINTENANCE > Mirroring** to load the following page. It displays the information of the mirroring session.

Figure 2-2 Mirror Session List



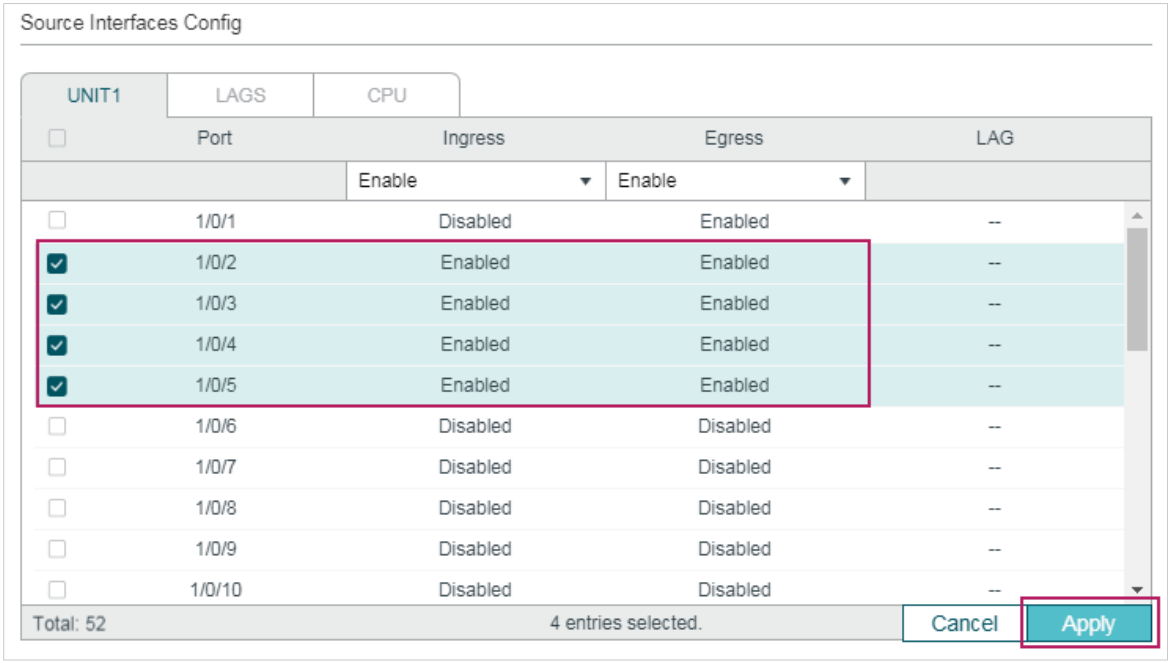
2) Click **Edit** on the above page to load the following page. In the **Destination Port Config** section, select port 1/0/1 as the destination port and click **Apply**.

Figure 2-3 Destination Port Configuration



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

Figure 2-4 Source Port Configuration



4) Click Save to save the settings.

2.4 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

3 Appendix: Default Parameters

Default settings of Switching are listed in th following tables.

Table 3-1 Configurations for Ports

Parameter	Default Setting
Ingress	Disabled
Egress	Disabled

Part 30

Configuring DLDP

CHAPTERS

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

1 Overview

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.

A unidirectional link occurs whenever traffic sent by a local device is received by its peer device but traffic from the peer device is not received by 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 DLDP Configuration

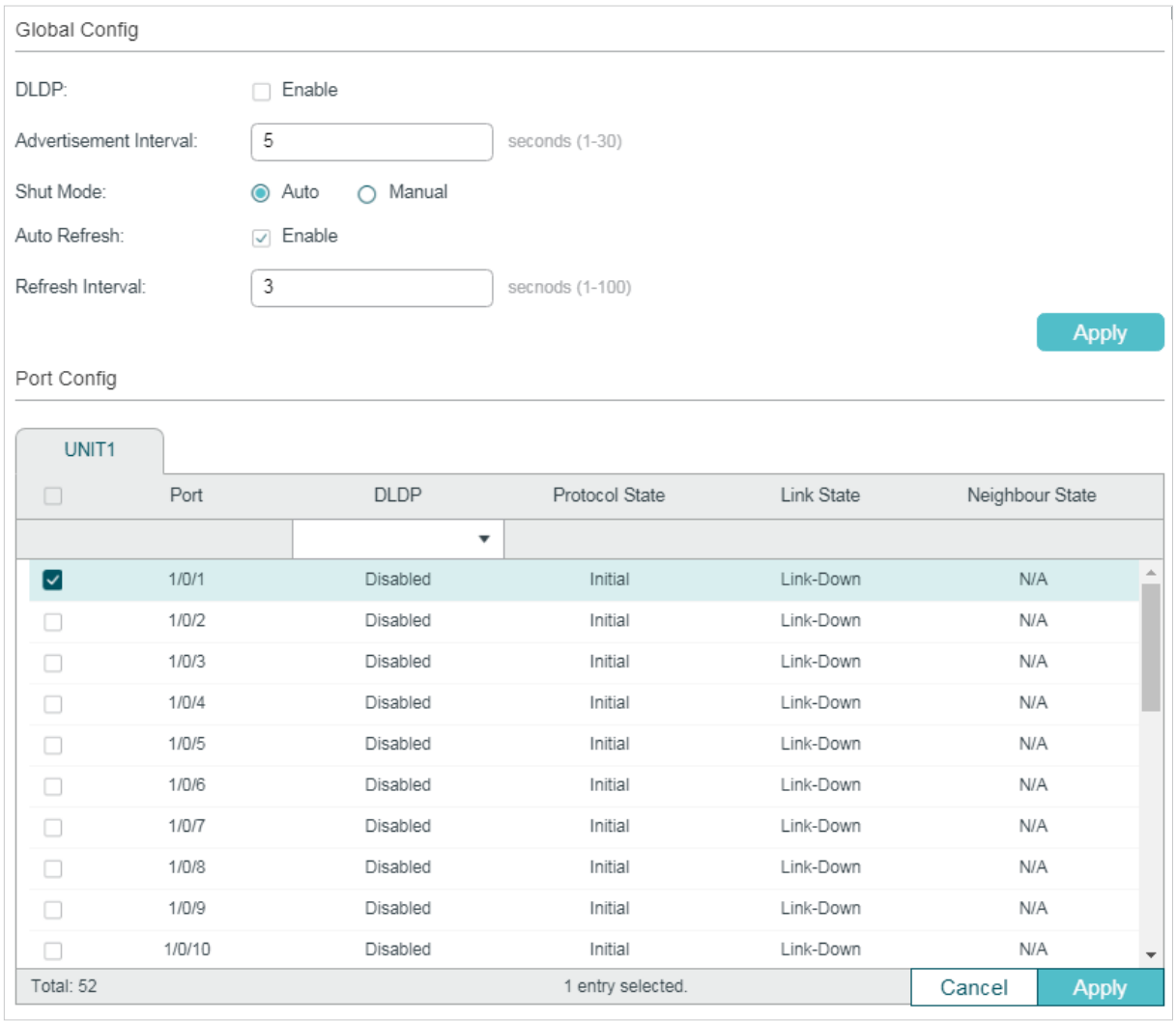
Configuration Guidelines

- A DLDP-capable port cannot detect a unidirectional link if it is connected to a DLDP-incapable port of another switch.
- To detect unidirectional links, make sure DLDP is enabled on both sides of the links.

2.1 Using the GUI

Choose the menu **MAINTENANCE > DLDP** to load the following page.

Figure 2-1 Configure DLDP



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.
Advertisement Interval	Configure the interval to send advertisement packets. 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 a unidirectional link is detected on a port, DLDP will generate logs and traps then shut down the port, and DLDP on this port will change to Disabled. **Manual**: When a unidirectional link is detected on a port, DLDP will generate logs and traps, and then users can manually shut down the unidirectional link ports.
Auto Refresh	With this option enabled, the switch will automatically refresh the DLDP information.
Refresh Interval	Specify the time interval at which the switch will refresh the DLDP information. Valid values are from 1 to 100 seconds, and the default value is 3 seconds.

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	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 (the device has established bidirectional links with all its neighbors) or DLDP has remained in an Active status 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 neighbour state. **Unknown**: Link detection 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.

2.2 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* **| ten-gigabitEthernet** *port* **| range ten-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

...

Switch(config-if)#end

Switch#copy running-config startup-config

3 Appendix: Default Parameters

Default settings of DLDP are listed in the following table.

Table 3-1 Default Settings of DLDP

Parameter	Default Setting
Global Config	
DLDP State	Disable
Advertisement Interval	5 seconds
Shut Mode	Auto
Auto Refresh	Disabled
Refresh Interval	3 seconds
Port Config	
DLDP	Disabled

Part 31

Configuring SNMP & RMON

CHAPTERS

1. SNMP
2. SNMP Configurations
3. Notification Configurations
4. RMON
5. RMON Configurations
6. Configuration Example
7. Appendix: Default Parameters

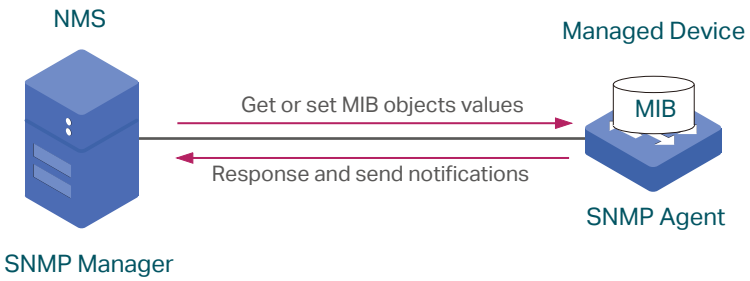
1 SNMP

1.1 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.

As the following figure shows, the SNMP system consists of an SNMP manager, an SNMP agent, and a MIB (Management Information Base). The SNMP manager can be part of an NMS such as tpNMS. The agent and MIB reside on the managed device such as the switch, router, host or printer. To configure SNMP on the switch, you define the relationship between the manager and the agent.

Figure 1-1 SNMP System



1.2 Basic Concepts

The following basic concepts of SNMP will be introduced: SNMP manager, SNMP agent, MIB (Management Information Base), SNMP entity, SNMP engine, and SNMP version.

SNMP Manager

The SNMP manager uses SNMP to monitor and control SNMP agents, providing a friendly management interface for the administrator to manage network devices conveniently. It can get an MIB objects values from an agent or store a value of MIB object into the agent. Also, it receives notifications from the agents so as to learn the condition of the network.

SNMP Agent

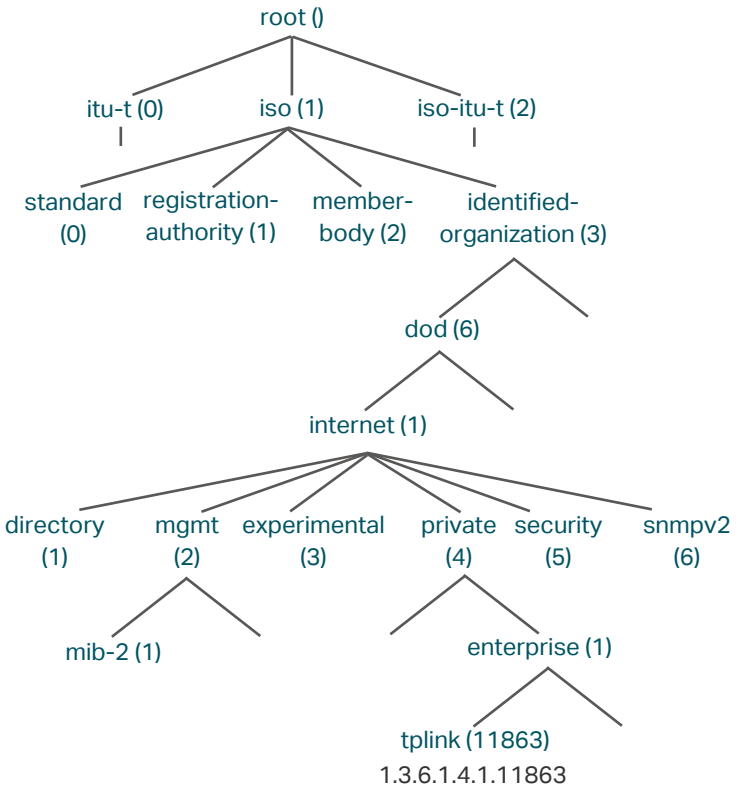
An SNMP agent is a process running on the managed device. It contains MIB objects whose values can be requested or changed by the SNMP manager. An agent can send unsolicited trap messages to notify the SNMP manager that a significant event has occurred on the agent.

MIB

A MIB is a collection of managed objects that is organized hierarchically. The objects define the attributes of the managed device, including the names, status, access rights, and data types. Each object can be addressed through an object identifier (OID).

As the following figure shows, the MIB hierarchy can be depicted as a tree with a nameless root, the levels of which are assigned by different organizations. The top-level MIB object IDs belong to different standards organizations, while lower-level object IDs are allocated by associated organizations. Vendors can define private branches that include managed objects for their own products.

Figure 1-2 MIB Tree



TP-Link switches provide private MIBs that can be identified by the OID 1.3.6.1.4.1.11863. The MIB file can be found on the provided CD or the download center of our official website: http://www.tp-link.com/en/download-center.html.

Also, TP-Link switches support the following public MIBs:

- LLDP.mib
- LLDP-Ext-Dot1.mib
- LLDP-Ext-MED.mib
- RFC1213.mib
- RFC1493-Bridge.mib
- RFC1757-RMON.mib
- RFC2618-RADIUS-Auth-Client.mib

- RFC2620-RADIUS-Acc-Client.mib
- RFC2674-pBridge.mib
- RFC2674-qBridge.mib
- RFC2863-pBridge.mib
- RFC2925-Disman-Ping.mib
- RFC2925-Disman-Traceroute.mib

For detail information about the supported public MIBs, see *Supported Public MIBs for TP-Link Switches* which can be found on the training center of our website:

http://www.tp-link.com/en/configuration-guides.html

SNMP Entity

An SNMP entity is a device running the SNMP protocol. Both the SNMP manager and SNMP agent are SNMP entities.

SNMP Engine

An SNMP engine is a part of the SNMP entity. Every SNMP entity has one and only one engine. An SNMP engine provides services for ending and receiving messages, authenticating and encrypting messages, and controlling access to managed objects.

An SNMP engine can be uniquely identified by an engine ID within an administrative domain. Since there is a one-to-one association between SNMP engines and SNMP entities, we can also use the engine ID to uniquely and unambiguously identify the SNMP entity within that administrative domain.

SNMP Version

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 SNMPv1 or SNMPv2c

1) Enable SNMP.
2) Create an SNMP view for managed objects.
3) Create a community, specify the accessible view and the corresponding access rights.

- Choose SNMPv3

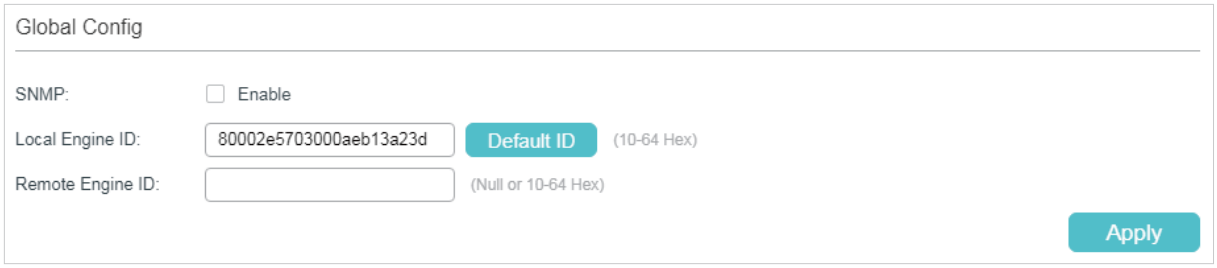
1) Enable SNMP.
2) Create an SNMP view for managed objects.
3) Create an SNMP group, and specify the access rights.
4) Create SNMP users, and configure the authentication mode, privacy mode and corresponding passwords.

2.1 Using the GUI

2.1.1 Enabling SNMP

Choose the **MAINTENANCE > SNMP > 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 and configure the local and remote engine ID.

SNMP	Enable or disable SNMP globally.

Local Engine ID	Set the engine ID of the local SNMP agent (the switch) with 10 to 64 hexadecimal digits. By default, the switch generates the engine ID using TP-Link's enterprise number (80002e5703) and its own MAC address. The local engine ID is a unique alphanumeric string used to identify the SNMP engine. As an SNMP agent contains only one SNMP engine, the local engine ID can uniquely identify the SNMP agent.
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.

2) Click **Apply**.

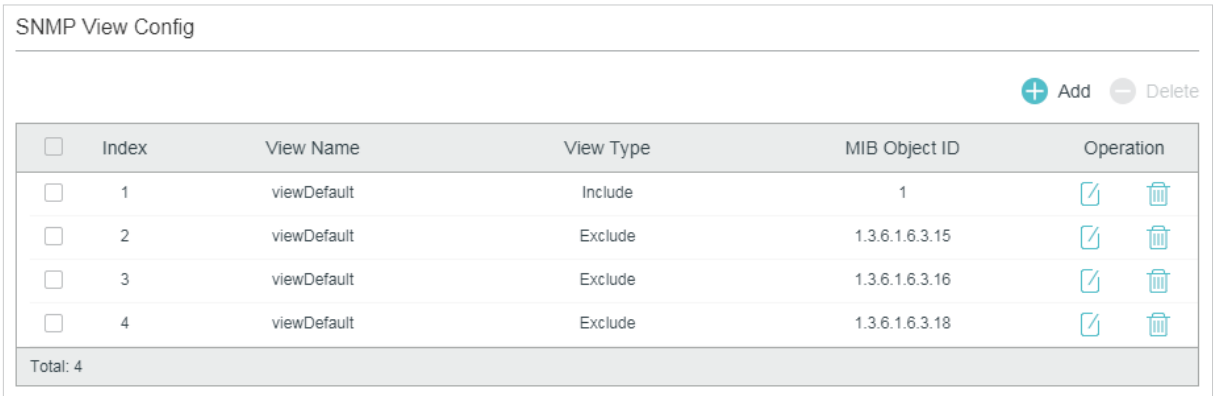
Note:

- The engine ID must contain an even number of characters.
- Changing the value of the SNMP engine ID has important side effects. In SNMPv3, a user's password is converted to an MD5 or SHA security digest based on the password and the engine ID. If the value of local engine ID changes, the switch will automatically delete all SNMPv3 local users as their security digests become invalid. Similarly, all SNMPv3 remote users will be deleted if the value of remote engine ID changes.

2.1.2 Creating an SNMP View

Choose the menu **MAINTENANCE > SNMP > Global Config** to load the following page.

Figure 2-2 SNMP View Config

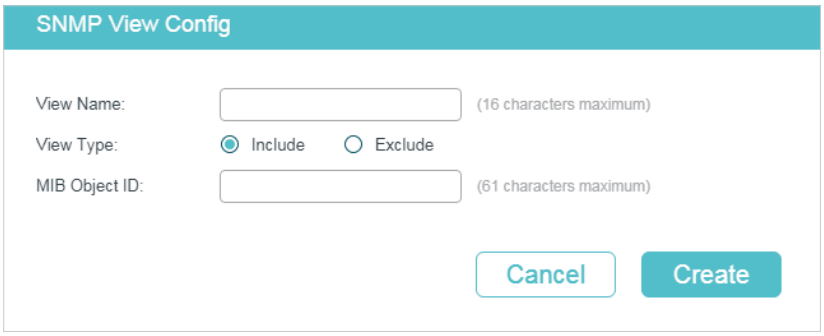


NMS manages MIB objects based on the SNMP view. An SNMP view is a subset of a MIB. The system provides a default view named viewDefault, and you can create other SNMP views according to your needs.

Follow these steps to create an SNMP view:

1) Click Add to load the following page. Enter a view name, and specify the view type and a MIB object that is related to the view.

Figure 2-3 Creating an SNMP View



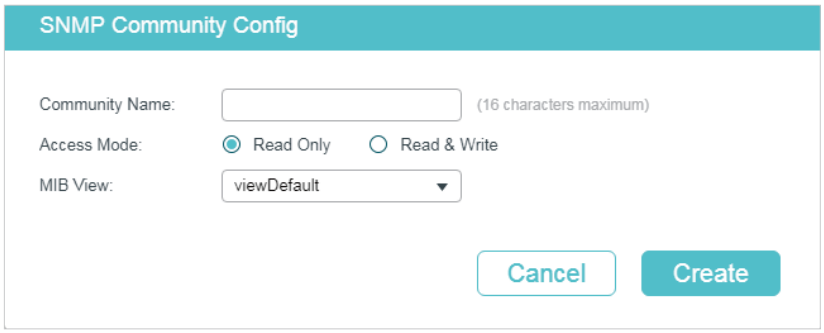
View Name	Set the view name with 1 to 16 characters. A complete view consists of all MIB objects that have the same view name.
View Type	Set the view to include or exclude the related MIB object. By default, it is include. **Include:** The NMS can view or manage the function indicated by the object. **Exclude:** The NMS cannot view or manage the function indicated by the object.
MIB Object ID	Enter a MIB Object ID to specify a specific function of the device. When a MIB Object ID is specified, all its child Object IDs are specified. For specific ID rules, refer to the device related MIBs.

2) Click **Create**.

2.1.3 Creating SNMP Communities (For SNMP v1/v2c)

Choose the menu **MAINTENANCE > SNMP > SNMP v1/v2c** and click Add to load the following page.

Figure 2-4 Creating an SNMP Community



1) Set the community name, access rights and the related view.

Community Name	Configure the community name. This community name is used like a password to give the NMS access to MIB objects in the switch's SNMP agent.
Access Mode	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 an SNMP view that allows the community to access. The default view is viewDefault.

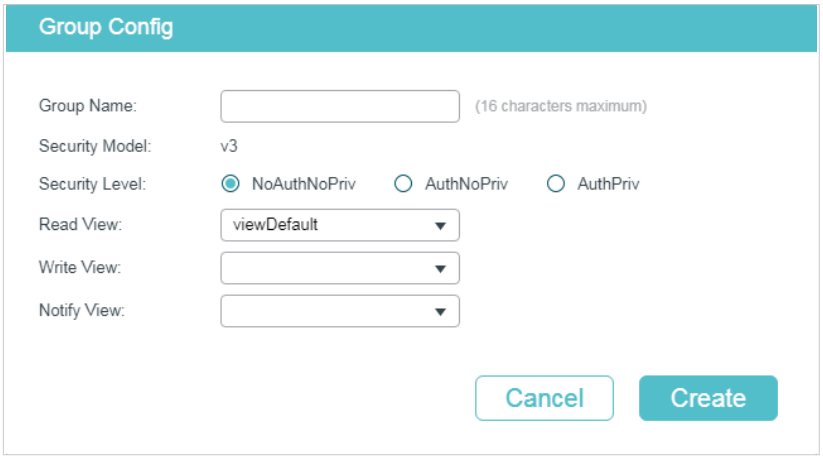
2) Click **Create**.

2.1.4 Creating an SNMP Group (For SNMP v3)

Create an SNMP group and configure related parameters.

Choose the menu **MAINTENANCE > SNMP > SNMP v3 > SNMP Group** and click Add to load the following page.

Figure 2-5 Creating an SNMP Group



Follow these steps to create an SNMP Group:

1) Assign a name to the group, then set the security level and the read view, write view and notify view.

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	Displays the security model. SNMPv3 uses v3, the most secure model.
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.
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.

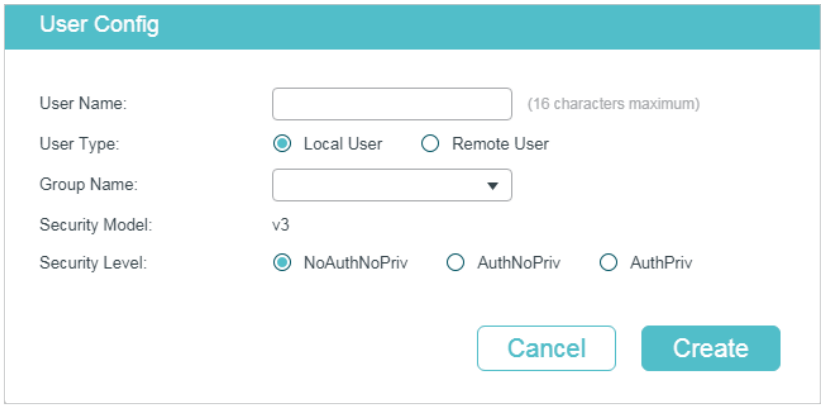
Write View	Choose a view to allow parameters to be modified but not viewed by the NMS. The default is none. The view in Write View should also be added to Read View.
Notify View	Choose a view to allow it to send notifications to the NMS.

2) Click **Create**.

2.1.5 Creating SNMP Users (For SNMP v3)

Choose the menu **MAINTENANCE > SNMP > SNMP v3 > SNMP User** and click Add to load the following page.

Figure 2-6 Creating an 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. Then 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 the NMS. As the remote engine ID and user password are used to compute the authentication and privacy digests, before configuring a remote user, you need to set the remote engine ID first.
Group Name	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	Displays the security model. SNMPv3 uses v3, the most secure model.

Security Level	Set the security level. The security level from highest to lowest is: NoAuthNoPriv, AuthNoPriv, AuthPriv, and the default is NoAuthNoPriv. The security level of the user should not be lower than the group it belongs to. **NoAuthNoPriv:** Uses a username match for authentication, and no encryption is implemented. **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 Authentication Mode or Privacy Mode. If not, skip the step.

Authentication Mode	With AuthNoPriv or AuthPriv selected, configure the authentication mode and password. Two authentication modes are provided: **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.
Authentication Password	Set the password for authentication.
Privacy Mode	With AuthPriv selected, configure the privacy mode and password for encryption. The switch uses the DES (Data Encryption Standard) algorithm for encryption.
Privacy Password	Set the password for encryption.

3) Click **Create**.

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*]} Configure the local engine ID and the remote engine ID. *local-engineID:* Enter the engine ID of the local SNMP agent (the switch) with 10 to 64 hexadecimal digits. By default, the switch generates the engine ID using TP-Link's enterprise number (80002e5703) and its own MAC address. The local engine ID is a unique alphanumeric string used to identify the SNMP engine. As an SNMP agent contains only one SNMP engine, the local engine ID can uniquely identify the SNMP agent. *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:* Changing the value of the SNMP engine ID has important side effects. In SNMPv3, a user's password is converted to an MD5 or SHA security digest based on the password and the engine ID. If the value of local engine ID changes, the switch will automatically delete all SNMPv3 local users as their security digests become invalid. Similarly, all SNMPv3 remote users will be deleted if the value of remote engine ID changes.
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: 80002e5703000aeb13a23d

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 SNMP Communities (For SNMP v1/v2c)

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. The default view is viewDefault.
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

2.2.4 Creating an SNMP Group (For SNMPv3)

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** v3] [**slev** {noAuthNoPriv | authNoPriv | authPriv}] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] Create 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. v3: Configure the security mode for the group. v3 indicates SNMPv3, the most secure model. noAuthNoPriv | authNoPriv | authPriv*:* 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 to be the Read view. Then the NMS can view parameters of the specified view. *write-view:* Set the view to be the Write view. Then the NMS can modify parameters of the specified view. Please note that the view in the Write view should also be in the Read view. *notify-view:* Set the view to be the Notify view. 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 with the group name as nms1, the security level as authPriv, and the Read and Notify view are both View1:

Switch#configure

Switch(config)#snmp-server group nms1 **smode** v3 **slev** authPriv **read** View1 **notify** View1

Switch(config)#show snmp-server group

No.	Name	Sec-Mode	Sec-Lev	Read-View	Write-View	Notify-View
---	--------	----------	----------	----------	----------	----------
1	nms1	v3	authPriv	View1		View1

Switch(config)#end

Switch#copy running-config startup-config

2.2.5 Creating SNMP Users (For SNMPv3)

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** 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. As the remote engine ID and user password are used to compute the authentication and privacy digests, before configuring a remote user, you need to set the remote engine ID first. *group-name:* Enter the name of the group which the user belongs to. The group is determined by the group name, security mode and security level. v3*:* Configure the security mode for the user. v3 indicates SNMPv3, the most secure model. noAuthNoPriv | authNoPriv | authPriv*:* Choose a security level from noAuthNoPriv (no authorization and no encryption), authNoPriv (authorization and no encryption), authPriv (authorization and encryption). The security level from highest to lowest is: noAuthNoPriv, authNoPriv, authPriv, and the default is noAuthNoPriv. The security level of the user should not be lower than the group it belongs to. none | MD5 | SHA: Choose an authentication algorithm. 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. None indicates no privacy method is used, and DES indicates DES encryption method is used. By default, the Privacy Mode is none. *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 and add it to group nms1. 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 nms1 **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	nms1	v3	authPriv	SHA	DES

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.

To configure SNMP notification, follow these steps:

1) Configure the information of NMS hosts.
2) Enable SNMP traps.

Configuration Guidelines

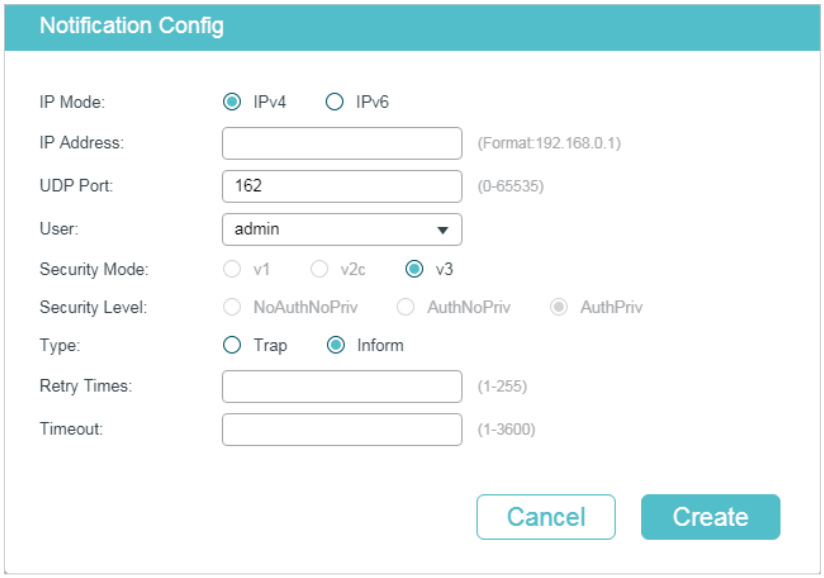
To guarantee the communication between the switch and the NMS, ensure the switch and the NMS are able to reach one another.

3.1 Using the GUI

3.1.1 Configuring the Information of NMS Hosts

Choose the menu **MAINTENANCE > SNMP > Notification > Notification Config** and click Add to load the following page.

Figure 3-1 Adding an NMS Host



Follow these steps to add an NMS host:

1) Choose the IP mode according to the network environment, and specify the IP address of the NMS host and the UDP port that receives notifications.

IP Mode	Choose an IP mode for the NMS host.
IP Address	If you set the **IP Mode** as IPv4, specify an IPv4 address for the NMS host. If you set the **IP Mode** as IPv6, specify an IPv6 address for the NMS host.
UDP Port	Specify a UDP port on the NMS host to receive 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.

2) Specify the user name or community name used by the NMS host, and configure the security model and security level based on the settings of the user or community.

User Name	Choose the user name or community name used by the NMS host.
Security Mode	If a community name (created for SNMPv1/v2c) is entered in User Name, specify the security mode as v1 or v2c. If a user name (created for SNMPv3) is entered in User Name, here displays the security mode as v3. The NMS host should use the corresponding SNMP version.
Security Level	If Security Level is v3, displays the security level of the user.

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.

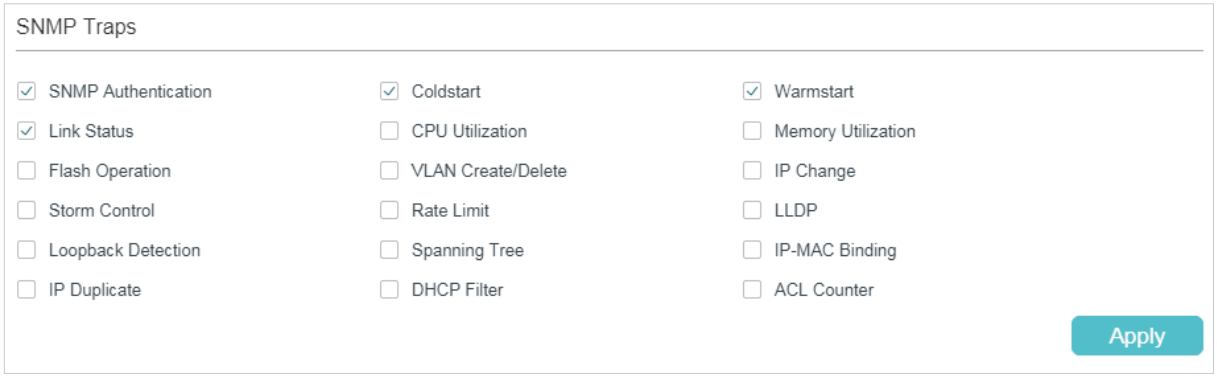
Type	Choose a notification type for the NMS host. For SNMPv1, the supported type is trap. For SNMPv2c and SNMPv3, you can configure the type as trap or inform. Trap: The switch will send Trap messages to the NMS host when certain events occur. When the NMS host receives a Trap message, it will not send a response to the switch. Thus the switch cannot tell whether a message is received or not, and the messages that are not received will not be resent. Inform: The switch will send Inform messages to the NMS host when certain events occur. When the NMS host 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 switch will resend the Inform message if it does not receive response from the NMS host 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 host after sending an inform message.

4) Click **Create**.

3.1.2 Enabling SNMP Traps

Choose the menu **MAINTENANCE > SNMP > Notification > Trap Config** to load the following page.

Figure 3-2 Enabling SNMP Traps



The supported traps are listed on the page. Follow these steps to enable any or all of these traps:

1) Select the traps to enable according to your needs.

SNMP Authentication	Triggered when a received SNMP request fails the authentication.
Coldstart	Indicates an SNMP initialization caused by the reinitialization of the switch system. The trap can be triggered when you reboot the switch.
Warmstart	Indicates the SNMP feature on the switch is reinitialized with the physical configuration unchanged. The trap can be triggered if you disable and then enable SNMP after the SNMP is completely configured and enabled.
Link Status	Triggered when the switch detects a link status change.
CPU Utilization	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.
Memory Utilization	Triggered when the memory utilization exceeds 80%.
Flash Operation	Triggered when flash is modified during operations such as backup, reset, firmware upgrade, configuration import, and so on.
VLAN Create/Delete	Triggered when certain VLANs are created or deleted successfully.
IP Change	Monitors the IP address changes of each interface. The trap can be triggered when the IP address of any interface is changed.
Storm Control	Monitors whether the storm rate has reached the limit that you have set. The trap can be triggered when the feature is enabled and broadcast/multicast/unknown-unicast frames are sent to the port with a rate higher than what you have set.

Rate Limit	Monitors whether the bandwidth has reached the limit you have set. The trap can be triggered when the Rate Limit feature is enabled and packets are sent to the port with a rate higher than what you have set.
LLDP	Indicates LLDP topology changes. The trap can be triggered when a new remote device attached to a local port, or a remote device disconnected or moved from one port to another.
Loopback Detection	Triggered when the switch detects a loopback with loopback detection feature, or when a loopback is cleared.
Spanning Tree	Indicates spanning tree changes. The trap can be triggered 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.
PoE	Only for products that support PoE feature. Allow all PoE-related traps, including: **Over-max-pwr-budget**: Triggered when the total power required by the connected PDs exceeds the maximum power the PoE switch can supply. **Port-pwr-change**: Triggered when a port starts to supply power or stops supplying power. **Port-pwr-deny**: Triggered when the switch powers off PDs on low-priority PoE ports. When the total power required by the connected PDs exceeds the system power limit, the switch will power off PDs on low-priority PoE ports to ensure stable running of the other PDs. **Port-pwr-over-30w**: Triggered when the power required by the connected PD exceeds 30 watts. **Port-pwr-overload**: Triggered when the power required by the connected PD exceeds the maximum power the port can supply. **Port-short-circuit**: Triggered when a short circuit is detected on a port. **Thermal-shutdown**: Triggered when the PSE chip overheats. The switch will stop supplying power in this case.
IP-MAC Binding	Triggered in the following two situations: the ARP Inspection feature is enabled and the switch receives an illegal ARP packet; or the IPv4 Source Guard feature is enabled and the switch receives an illegal IP packet.
IP Duplicate	Triggered when the switch detects an IP conflict event.
DHCP Filter	Triggered when the DHCPv4 Filter feature is enabled and the switch receives DHCP packets from an illegal DHCP server.
ACL Counter	Monitors matched ACL information, including the matched ACL ID, rule ID and the number of the matched packets. With both this trap and the **Logging** feature in ACL rule settings enabled, the switch will check the matched ACL information every five minutes and send SNMP traps if there is any updated information.

2) Click **Apply**.

3.2 Using the CLI

3.2.1 Configuring the NMS 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 NMS host and the switch are able to reach to each other. *udp-port:* Specify a UDP port on the NMS host to receive 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 host. When the NMS host uses SNMPv1 or SNMPv2c, enter the Community Name; when the NMS host uses SNMPv3, enter the User Name of the SNMP Group. v1 | v2c | v3: Choose the security mode used by the user from the following: SNMPv1, SNMPv2c, SNMPv3. The NMS host should use the corresponding SNMP version. 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 a notification type for the NMS host. For SNMPv1, the supported type is trap. For SNMPv2c and SNMPv3, you can configure the type as trap or inform. When the NMS host receives a trap message, it will not send a response to the switch. Thus the switch cannot tell whether a message is received or not, and the messages that are not received will not be resent. When the NMS host 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. *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 host 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 host 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 192.30.1.222, UDP port as port 162, name used by the NMS host 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 192.30.1.222 162 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	192.30.1.222	162	admin	v3	authPriv	inform	3	100

Switch(config)#end

Switch#copy running-config startup-config

3.2.2 Enabling SNMP Traps

The switch supports multiple SNMP traps like SNMP standard traps, ACL traps, and VLAN traps. You can enable any or all of the traps according to your needs.

- Enabling the SNMP Standard Traps Globally

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

Step 2	**snmp-server traps snmp [** linkup | linkdown | warmstart | coldstart | auth-failure **]** Enable the corresponding SNMP standard traps. The command without parameter enables all SNMP standard traps. All SNMP standard traps are enabled by default. linkup: Indicates a port status changes from linkdown to linkup, and can be triggered when you connect a device to a port. linkdown: Indicates a port status changes from linkup to linkdown, and can be triggered when you disconnect a device to a port. warmstart: Indicates the SNMP feature on the switch is reinitialized with the physical configuration unchanged. The trap can be triggered if you disable and then enable SNMP after the SNMP is completely configured and enabled. coldstart: Indicates an SNMP initialization caused by the reinitialization of the switch system. The trap can be triggered when you reboot the switch. auth-failure: Triggered when a received SNMP request fails the authentication.
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

■ Enabling the SNMP Extended Traps Globally

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

Step 2	**snmp-server traps** { rate-limit | cpu | flash | lldp remtableschange | lldp topologychange | loopback-detection | storm-control | spanning-tree | memory } Enable the corresponding SNMP extended traps. All SNMP extended traps are disabled by default. rate-limit: Monitors whether the bandwidth has reached the limit you have set. The trap can be triggered when the Rate Limit feature is enabled and packets are sent to the port with a rate higher than what you have set. cpu: Monitors the load status of the switch CPU. The trap can be triggered when the utilization rate of the CPU has exceeded the limit that you have set. The limit of CPU utilization rate for the switch is 80% by default. flash: Triggered when flash is modified during operations such as backup, reset, firmware upgrade, configuration import, and so on. lldp remtableschange: A lldp RemTablesChange notification is sent when the value of lldp StatsRemTableLastChangeTime changes. It can be utilized by an NMS host to trigger LLDP remote systems table maintenance polls. lldp topologychange: A notification generated by the local device to sense the change in the topology that indicates a new remote device attached to a local port, or a remote device disconnected or moved from one port to another. loopback-detection: The feature is used to detect loopbacks. And the trap is disabled by default. The system will generate the trap when a loopback is detected or cleared. storm-control: The feature is used to monitor network storms. And the trap is disabled by default. The system will generate the trap when the rate of broadcast or multicast reaches the limit of storm control. spanning-tree: The feature is used to monitor the spanning tree status. And the trap is disabled by default. The system will generate the trap in the following situations: a port changes from non-forwarding state to forwarding state or the other way round; a port receives a packet with TC flag or a TCN packet. memory: The feature is used to monitor the memory. And the trap is disabled by default. The system will generate the trap when the memory utilization exceeds 80%.
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

Enabling the VLAN Traps Globally

Step 1	**configure** Enter global configuration mode.
Step 2	**snmp-server traps vlan** [create | delete] Enable the corresponding VLAN traps. The command without parameter enables all SNMP VLAN traps. All VLAN traps are disabled by default. create: Triggered when certain VLANs are created successfully. delete: Triggered when certain VLANs are deleted successfully.
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 VLAN traps:

Switch#configure

Switch(config)#snmp-server traps vlan

Switch(config)#end

Switch#copy running-config startup-config

Enabling the SNMP Security Traps Globally

Step 1	**configure** Enter global configuration mode.
Step 2	**snmp-server traps security** { dhcp-filter | ip-mac-binding } Enable the corresponding security traps. All security traps are disabled by default. dhcp-filter: Triggered when the DHCPv4 Filter feature is enabled and the switch receives DHCP packets from an illegal DHCP server. ip-mac-binding: Triggered when the ARP Inspection feature is enabled and the switch receives an illegal ARP packet, or the IPv4 Source Guard feature is enabled and the switch receives an illegal IP packet.
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 DHCP filter trap:

Switch#configure

Switch(config)#snmp-server traps security dhcp-filter

Switch(config)#end

Switch#copy running-config startup-config

Enabling the ACL Trap Globally

Step 1	**configure** Enter global configuration mode.
Step 2	**snmp-server traps security acl** Enable the ACL trap. It is disabled by default. The trap monitors matched ACL information, including the matched ACL ID, rule ID and the number of the matched packets. With both this trap and the **Logging** feature in ACL rule settings enabled, the switch will check the matched ACL information every five minutes and send SNMP traps if there is any updated information.
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 ACL trap:

Switch#configure

Switch(config)#snmp-server traps acl

Switch(config)#end

Switch#copy running-config startup-config

Enabling the IP Traps Globally

Step 1	**configure** Enter global configuration mode.
Step 2	**snmp-server traps ip** { change | duplicate } Enable the IP traps. All IP traps are disabled by default. change: Triggered when the DHCPv4 Filter feature is enabled and the switch receives DHCP packets from an illegal DHCP server. duplicate: Monitors the IP address changes of each port. It is triggered when the IP address of any port is changed.

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 IP-Change trap:

Switch#configure

Switch(config)#snmp-server traps ip change

Switch(config)#end

Switch#copy running-config startup-config

Enabling the SNMP PoE Traps Globally

Note:

Only T1600G-52PS support PoE traps.

Step 1	**configure** Enter global configuration mode.
Step 2	**snmp-server traps power** [over-max-pwr-budget | port-pwr-change | port-pwr-deny | port-pwr-over-30w | port-pwr-overload | port-short-circuit | thermal-shutdown] Enable the PoE traps. The command without parameter enables all PoE traps. All PoE traps are disabled by default. over-max-pwr-budget: Triggered when the total power required by the connected PDs exceeds the maximum power the PoE switch can supply. port-pwr-change: Triggered when the total power required by the connected PDs exceeds the maximum power the PoE switch can supply. port-pwr-deny: Triggered when the switch powers off PDs on low-priority PoE ports. When the total power required by the connected PDs exceeds the system power limit, the switch will power off PDs on low-priority PoE ports to ensure stable running of the other PDs. port-pwr-over-30w: Triggered when the power required by the connected PD exceeds 30 watts. port-pwr-overload: Triggered when the power required by the connected PD exceeds the maximum power the port can supply. port-short-circuit: Triggered when a short circuit is detected on a port. thermal-shutdown: Triggered when the PSE chip overheats. The switch will stop supplying power in this case.
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 PoE traps:

Switch#configure

Switch(config)#snmp-server traps power

Switch(config)#end

Switch#copy running-config startup-config

■ Enabling the Link-status Trap 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* **}** 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 the link-status trap. It is triggered when the switch detects a link status change. 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

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.

- **Statistics:** Collects Ethernet statistics (like the total received bytes, the total broadcast packets, and the total packets of the specified size) on an interface.
- **History:** Collects a history group of statistics on Ethernet ports for a specified polling interval.
- **Event:** Specifies the action to take when an event is triggered by an alarm. The action can be to generate a log entry or an SNMP trap.
- **Alarm:** Monitors a specific MIB object for a specified interval, triggers an event at a specified value (rising threshold or falling threshold).

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

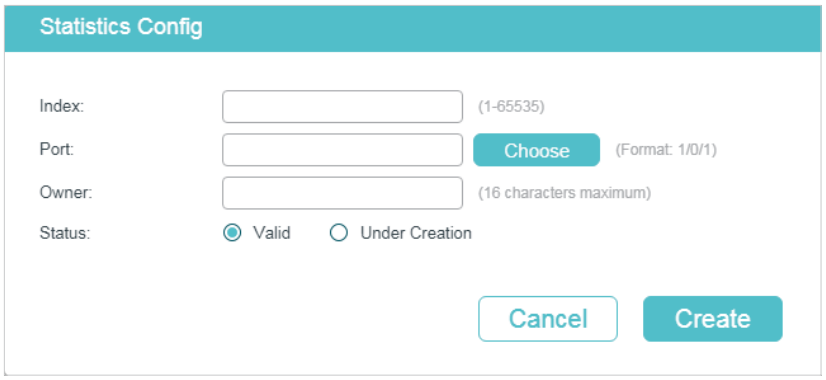
To ensure that the NMS receives notifications normally, please complete configurations of SNMP and SNMP Notification before RMON configurations.

5.1 Using the GUI

5.1.1 Configuring Statistics Group

Choose the menu **MAINTENANCE > SNMP > RMON > Statistics** and click Add to load the following page.

Figure 5-1 Creating a Statistics Entry



Follow these steps to configure the Statistics group:

1) Specify the entry index, the port to be monitored, and the owner name of the entry. Set the entry as Valid or Under Creation.

Index	Enter the index 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.

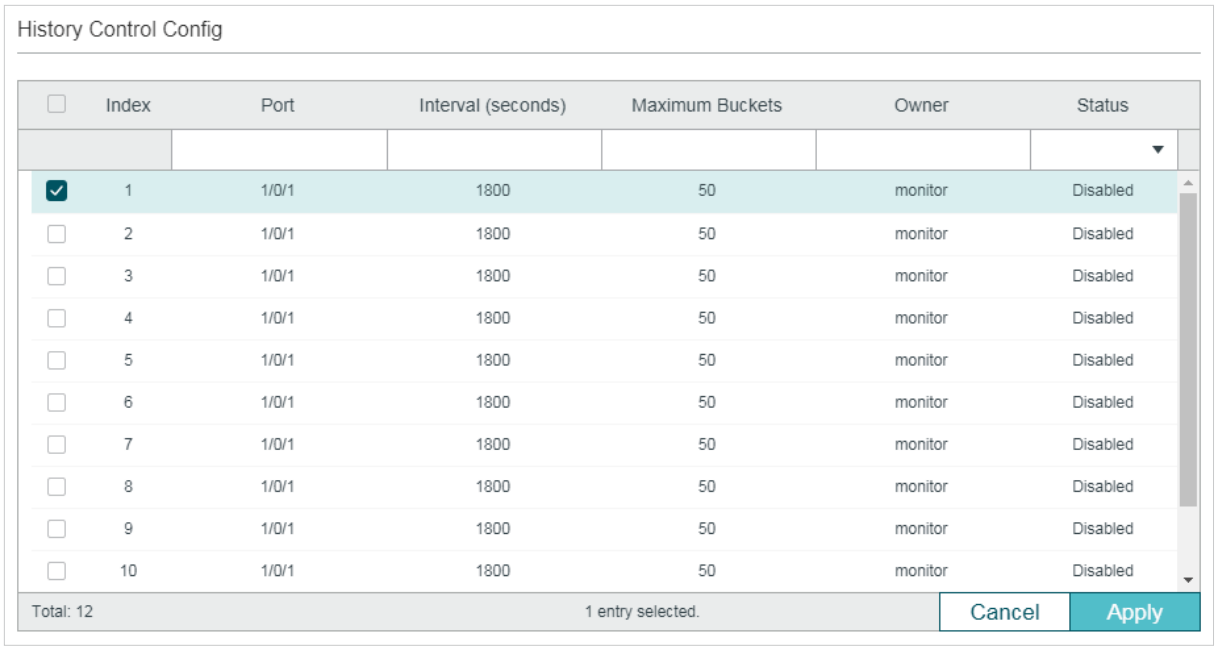
Status	Set the entry as Valid or Under Creation. By default, it is Valid. The switch start to collect Ethernet statistics for a Statistics entry since the entry status is configured as valid. **Valid**: The entry is created and valid. **Under Creation**: The entry is created but invalid.

2) Click **Create**.

5.1.2 Configuring History Group

Choose the menu **MAINTENANCE > SNMP > RMON > History** to load the following page.

Figure 5-2 Configuring the History Entry



Follow these steps to configure the History group:

1) Select a History entry, and specify a port to be monitored.

Index	Displays the index of History entries. The switch supports up to 12 History entries.
Port	Specify a port in 1/0/1 format to be monitored.

2) Set the sample interval and the maximum buckets of History entries.

Interval (seconds)	Specify the number of seconds in each polling cycle. Valid values are from 10 to 3600 seconds and the default is 1800 seconds. Every history entry has its own timer. For the monitored port, the switch samples packet information and generates a record in every interval.
Maximum 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. Valid values are from 10 to 130 and 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.

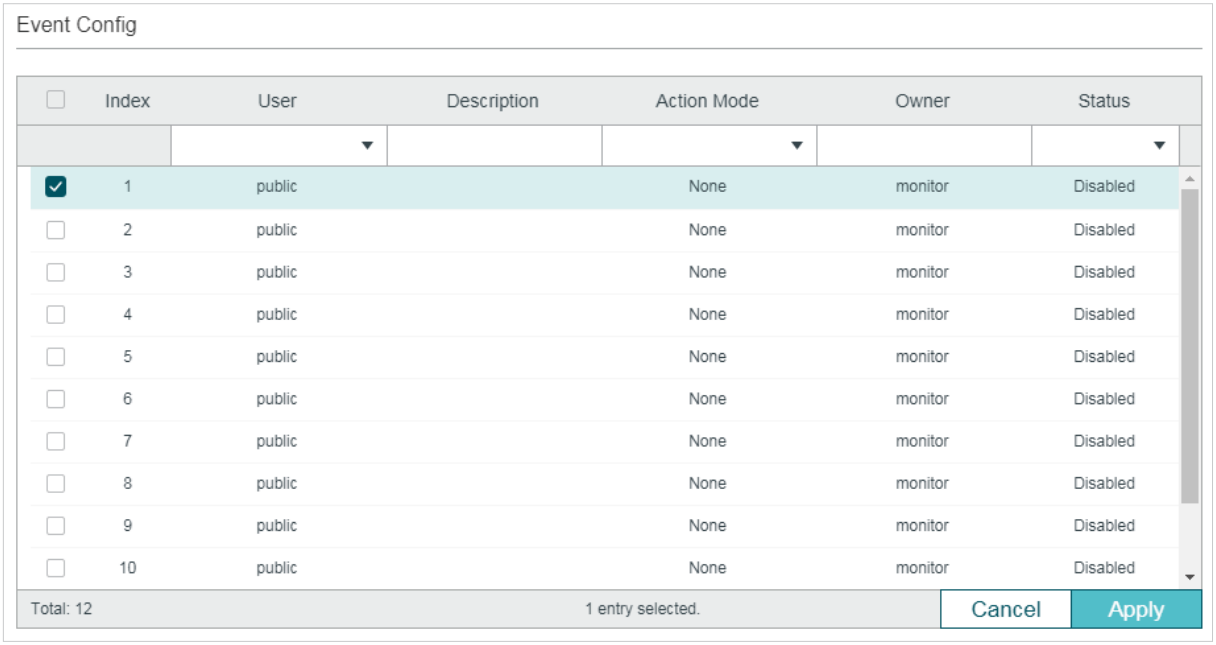
Note:

To change the parameters of a History entry, please enable the entry at the same time, otherwise the change cannot take effect.

5.1.3 Configuring Event Group

Choose the menu **MAINTENANCE > SNMP > RMON > Event** to load the following page.

Figure 5-3 Configuring the Event Entry



Follow these steps to configure the Event group:

1) Choose an Event entry, and set the SNMP User of the entry.

Index	Displays the index of Event entries. The switch supports up to 12 Event entries.
User	Choose an SNMP user name or community name for the entry. The name should be the same as what you have set in SNMP previously.

2) Set the description and action to be taken when the event is triggered.

Description	Enter an brief description of this event to make identifying it easier.

Action Mode	Specify the action for the switch to take when the event is triggered. **None**: No action. It is the default setting. **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**.

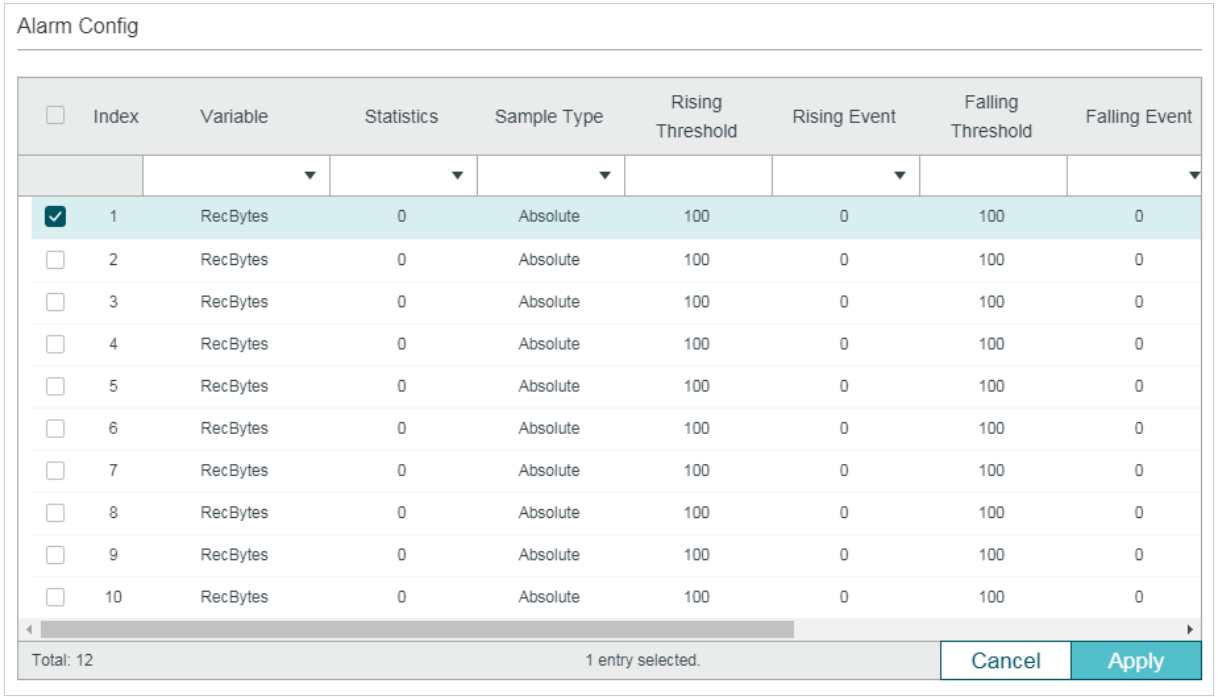
Owner	Enter the owner name of the entry with 1 to 16 characters. By default, it is monitor.
Status	Enable or disable the entry. By default, it is disabled. **Enable**: The entry is enabled. **Disable**: The entry is disabled.

5.1.4 Configuring Alarm Group

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 **MAINTENANCE > SNMP > RMON > Alarm** to load the following page.

Figure 5-4 Configuring the Alarm Entry



Follow these steps to configure the Alarm group:

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. The switch supports up to 12 Alarm entries.
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 mode, 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**. Valid values are from 1 to 2147483647 and the default is 100.
Rising Event	Specify the index of the Event entry that will be triggered when the sampled value exceeds the preset threshold. The Event entry specified here should be enabled first.

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**. Valid values are from 1 to 2147483647 and the default is 100.
Falling Event	Specify the index of the Event entry that will be triggered when the sampled value is below the preset threshold. The Event entry specified here should be enabled first.
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**.

Interval (seconds)	Set the sampling interval. Valid values are from 10 to 3600 seconds and the default is 1800 seconds.
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 interface** { **fastEthernet** *port* | **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. The switch start to collect Ethernet statistics for a Statistics entry since the entry status is configured as 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 entries are both monitor and the status are both 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, maximum 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 method of the specified variable. 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. The Event entry specified here should be enabled first. *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. The Event entry specified here should be enabled first.

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

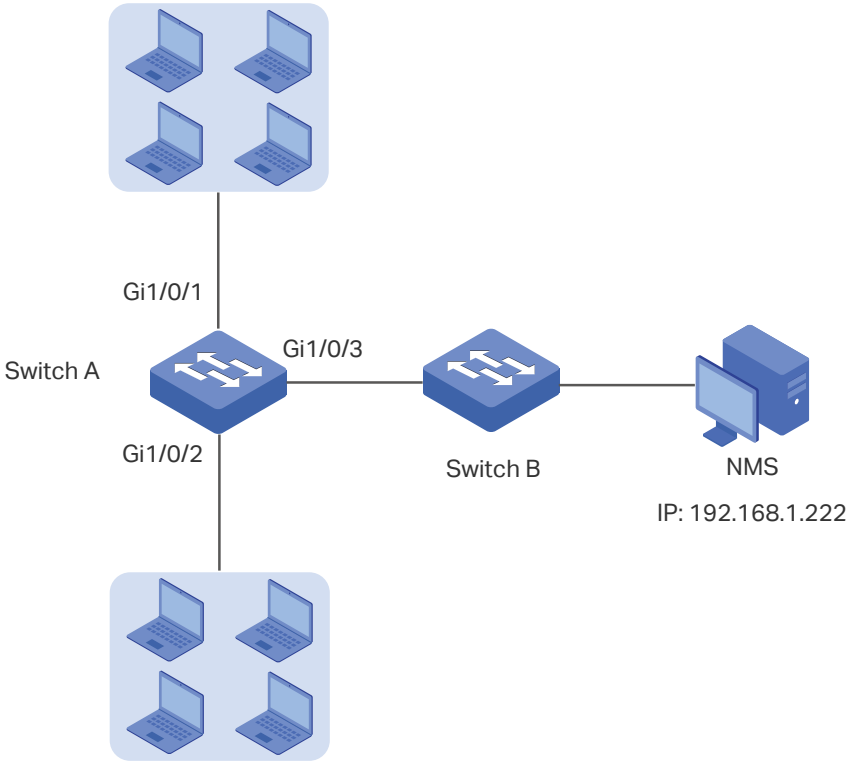
6.1 Network Requirements

The following figure shows the network topology of a company. The company has requirements as follows:

1) Monitor traffic flow of ports 1/0/1 and 1/0/2 on Switch A, 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 ports 1/0/1 and 1/0/2 on Switch A, and regularly collect and save data for follow-up checks. Specifically, during the sample interval, switch A should notify the NMS when the number of packets transmitted and received on the port exceeds the preset threshold; Switch A should record but not notify the NMS when the number of packets transmitted and received is below the threshold.

The NMS host with IP address 192.168.1.222 is connected to the core switch, Switch B. Switch A is connected to Switch B via port 1/0/3. And port 1/0/3 and the NMS are able to reach one another.

Figure 6-1 Network Topology



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.

Demonstrated with T1600G-52TS, this chapter provides configuration procedures in two ways: using the GUI and using the CLI.

6.3 Using the GUI

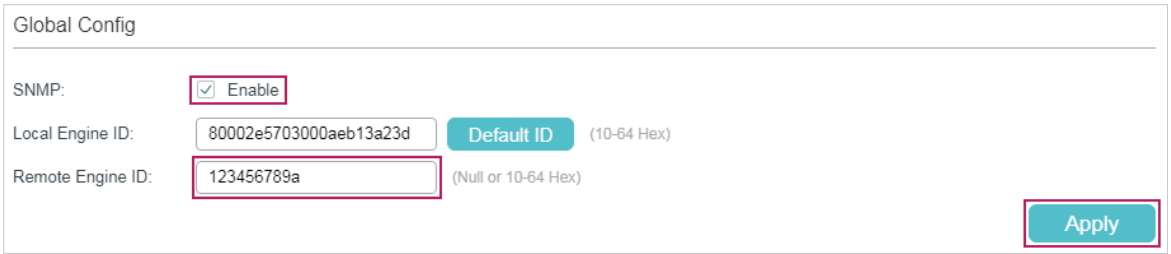
- Configuring Rate Limit on ports

  Configure the rate limit on required ports. For detailed configuration, please refer to *Configuring QoS*.

- Configuring SNMP

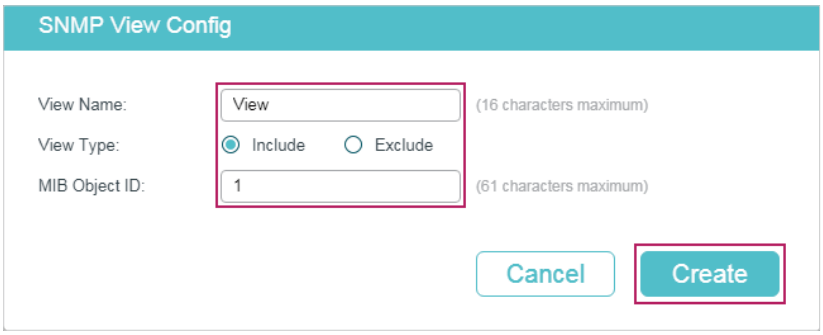
1) Choose **MAINTENANCE > SNMP > Global Config** to load the following page. In the **Global Config** section, enable SNMP, and set the Remote Engine ID as 123456789a. Click **Apply**.

Figure 6-2 Enabling SNMP



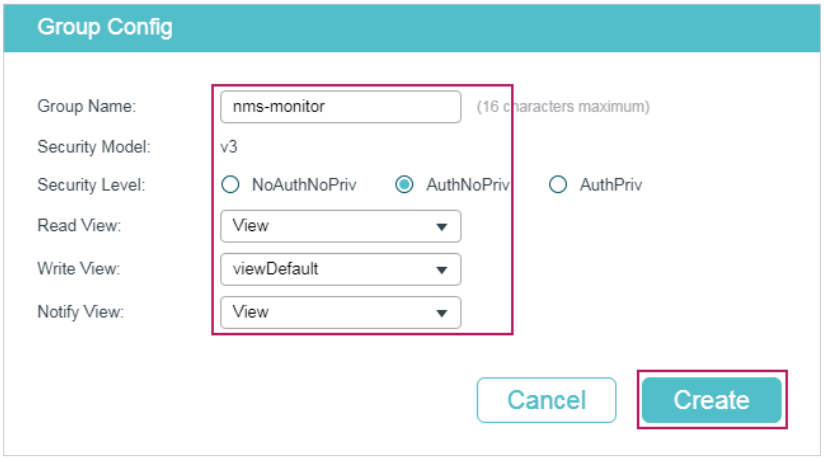
2) In the **SNMP View Config** section, click Add to load the following page. Name the SNMP view as View, set the view type as Include, and set MIB Object ID as 1 (which means all functions). Click **Create**.

Figure 6-3 Creating an SNMP View



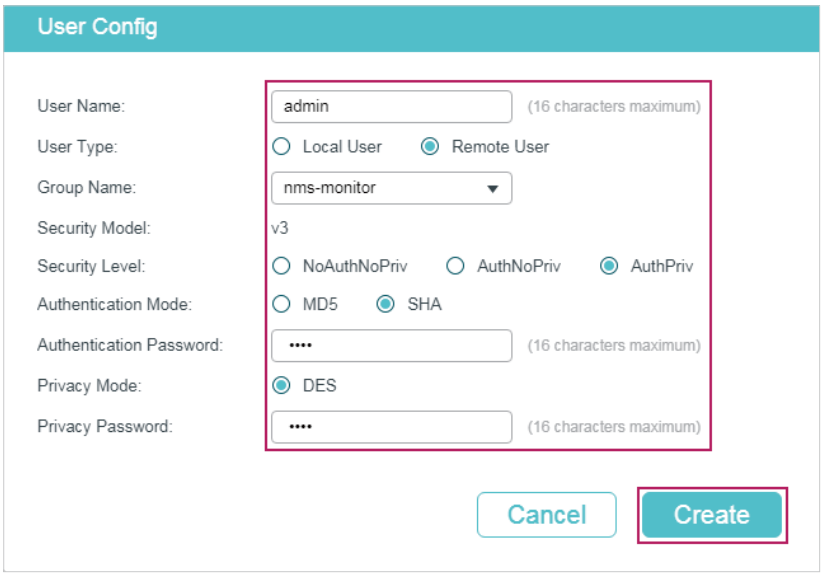
3) Choose **MAINTENANCE > SNMP > SNMP v3 > SNMP Group** and click Add to load the following page. Create a group with the name of nms-monitor, enable authentication and privacy, and add View to Read View and Notify View. Click **Create**.

Figure 6-4 Configuring an SNMP Group



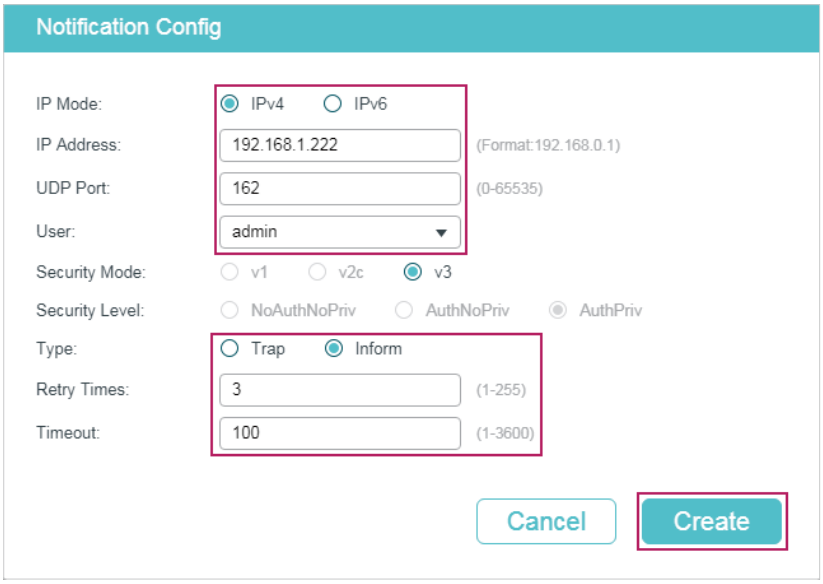
4) Choose **MAINTENANCE > SNMP > SNMP v3 > SNMP User** and click Add to load the following page. Create a user named admin for the NMS, set the user type as Remote User and specify the group name. Set the Security Level in accordance with that of the group nms-monitor. Choose SHA authentication algorithm and DES privacy algorithm, and set corresponding passwords. Click **Create**.

Figure 6-5 Creating an SNMP User



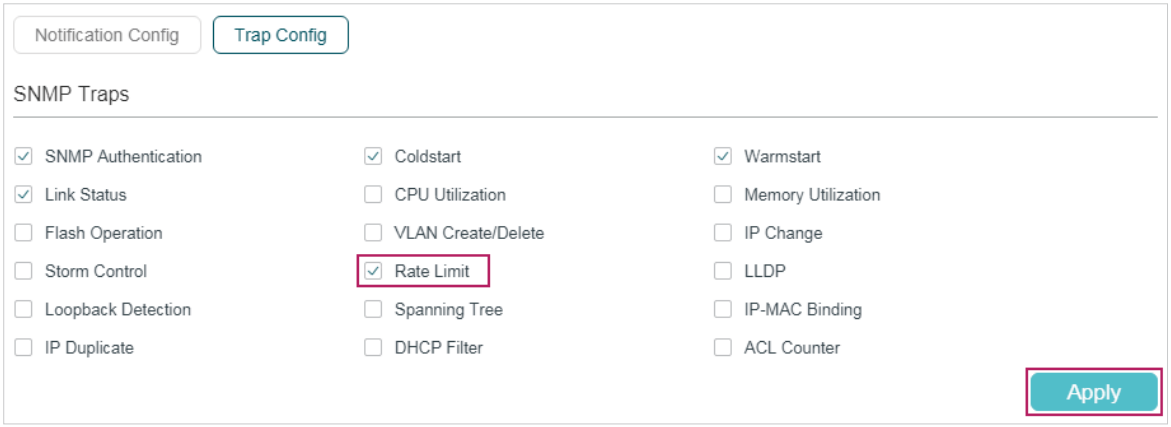
5) Choose **MAINTENANCE > SNMP > Notification > Notification Config** and click Add to load the following page. Choose the IP Mode as IPv4, and specify the IP address of the NMS host and the port of the host for transmitting notifications. Specify the User as admin and choose the type as Inform. Set the retry times as 3, with the timeout period as 100 seconds. Click **Create**.

Figure 6-6 Creating an SNMP Notification Entry



6) Choose **MAINTENANCE > SNMP > Notification > Trap Config** to load the following page. Enable Rate Limit trap and click **Apply**.

Figure 6-7 Enabling Rate Limit Trap



7) Click Save to save the settings.

Configuring RMON

1) Choose **MAINTENANCE > SNMP > RMON > Statistics** and click Add 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 6-8 Configuring Statistics Entry 1

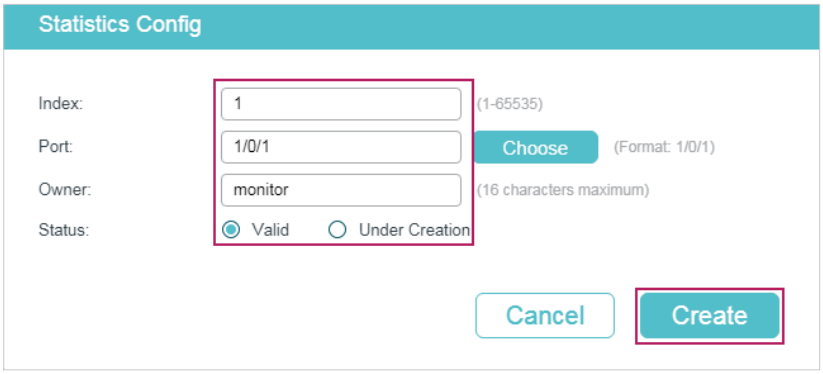
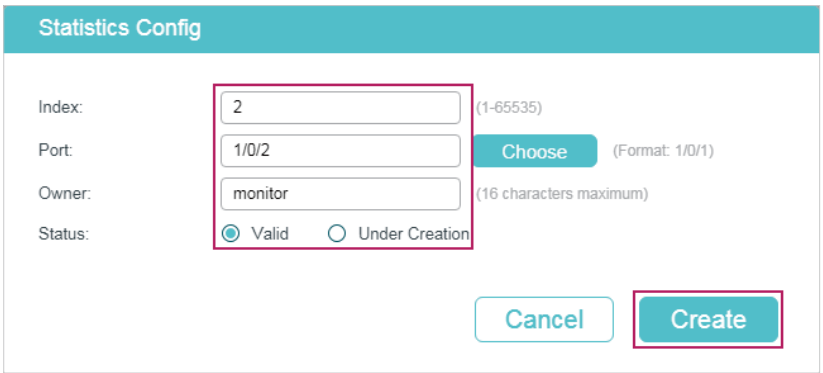
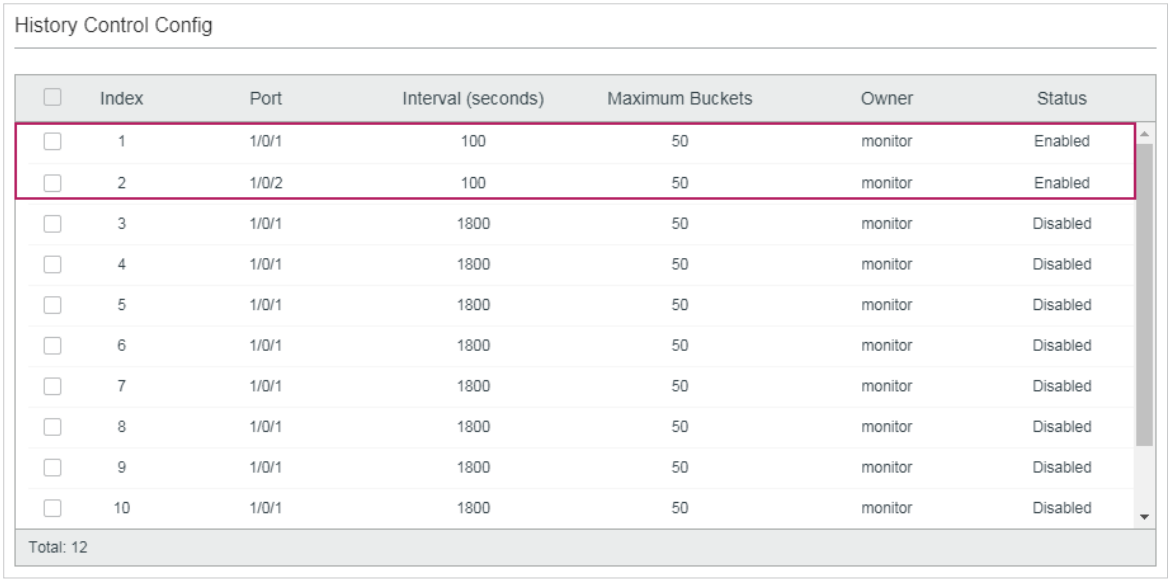


Figure 6-9 Configuring Statistics Entry 2



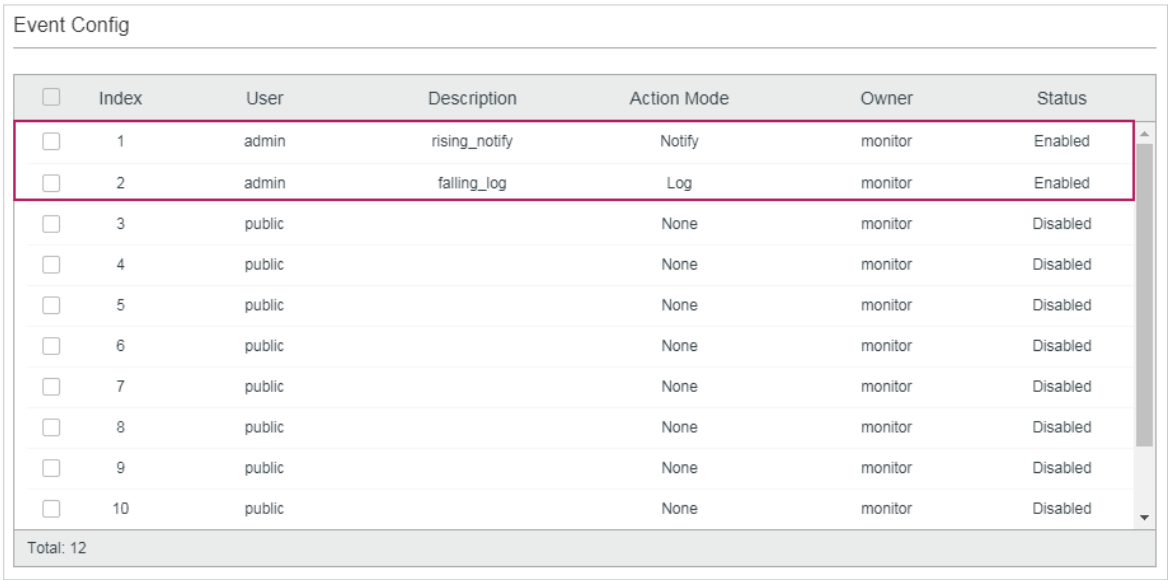
2) Choose the menu **MAINTENANCE > SNMP > RMON > History** to load the following page. Configure entries 1 and 2. Bind entries 1 and 2 to ports 1/0/1 and 1/0/2 respectively, and set the Interval as 100 seconds, Maximum Buckets as 50, the owner of the entries as monitor, and the status as Enable.

Figure 6-10 Configuring the History Entries



3) Choose the menu **MAINTENANCE > 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 6-11 Configuring the Event Entries



4) Choose **MAINTENANCE > 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 6-12 Configuring the Alarm Entries



5) Click Save to save settings.

6.4 Using the CLI

- Configuring Rate Limit on ports

  Configure the rate limit on required ports of Switch A. For detailed configuration, please refer to *Configuring QoS*.

- Configuring SNMP

1) Enable SNMP and specify the remote engine ID.

   Switch_A#configure

   Switch_A(config)#snmp-server

   Switch_A(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_A(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_A(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_A(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_A(config)#snmp-server host 192.168.1.222 162 admin smode v3 slev authPriv type inform retries 3 timeout 100

- Enable Bandwith-control Trap

Switch_A(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_A(config)#rmon statistics 1 interface gigabitEthernet 1/0/1 owner monitor status valid

   Switch_A(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_A(config)#rmon history 1 interface gigabitEthernet 1/0/1 interval 100 owner monitor buckets 50

   Switch_A(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_A(config)#rmon event 1 user admin description rising_notify type notify owner monitor

   Switch_A(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_A(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_A(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_A(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_A(config)#show snmp-server engineID

Local engine ID: 80002e5703000aeb13a23d

Remote engine ID: 123456789a

Verify SNMP view configurations:

```
Switch_A(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_A(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_A(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_A(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_A(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_A(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_A(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_A(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 tables.

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 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 7-3 Default SNMP v1/v2c Settings

Parameter	Default Setting
Community Entry	No entries
Community Name	None
Access	Read-only
MIB View	viewDefault

Table 7-4 Default SNMP v3 Settings

Parameter	Default Setting
SNMP Group	
Group Entry	No entries
Group Name	None
Security Model	v1
Security Level	NoAuthNoPriv
Read View	viewDefault
Write View	None
Notify View	None

Parameter	Default Setting
SNMP User	
User Entry	No entries
User Name	None
User Type	Local User
Group Name	None
Security Model	v1
Security Level	noAuthNoPriv
Authentication Mode	MD5 (when Security Level is configured as AuthNoPriv or AuthPriv)
Authentication Password	None
Privacy Mode	DES (when Security Level is configured as AuthPriv)
Privacy Password	None

Default settings of Notification are listed in the following table.

Table 7-5 Default Notification Settings

Parameter	Default Setting
Notification Config	
Notification Entry	No entries
IP Mode	IPv4
IP Address	None
UDP Port	162
User	None
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.
Trap Config	
Enabled SNMP Traps	SNMP Authentication, Coldstart, Warmstart, Link Status

Default settings of RMON are listed in the following tables.

Table 7-6 Default Statistics Config Settings

Parameter	Default Setting
Statistics Entry	No entries
ID	None
Port	None
Owner	None
IP Mode	Valid

Table 7-7 Default Settings for History Entries

Parameter	Default Setting
Port	1/0/1
Interval	1800 seconds
Max Buckets	50
Owner	monitor
Status	Disable

Table 7-8 Default Settings for Event Entries

Parameter	Default Setting
User	public
Description	None
Type	None
Owner	monitor
Status	Disable

Table 7-9 Default Settings for Alarm Entries

Parameter	Default Setting
Variable	RecBytes
Statistics	0, means no Statistics entries is selected.
Sample Type	Absolute
Rising Threshold	100
Rising Event	None
Falling Threshold	100
Falling Event	None
Alarm Type	All

Parameter	Default Setting
Interval	1800 seconds
Owner	monitor
Status	Disable

Part 32

Diagnosing the Device & Network

CHAPTERS

1. Diagnosing the Device
2. Diagnosing the Network
3. Appendix: Default Parameters

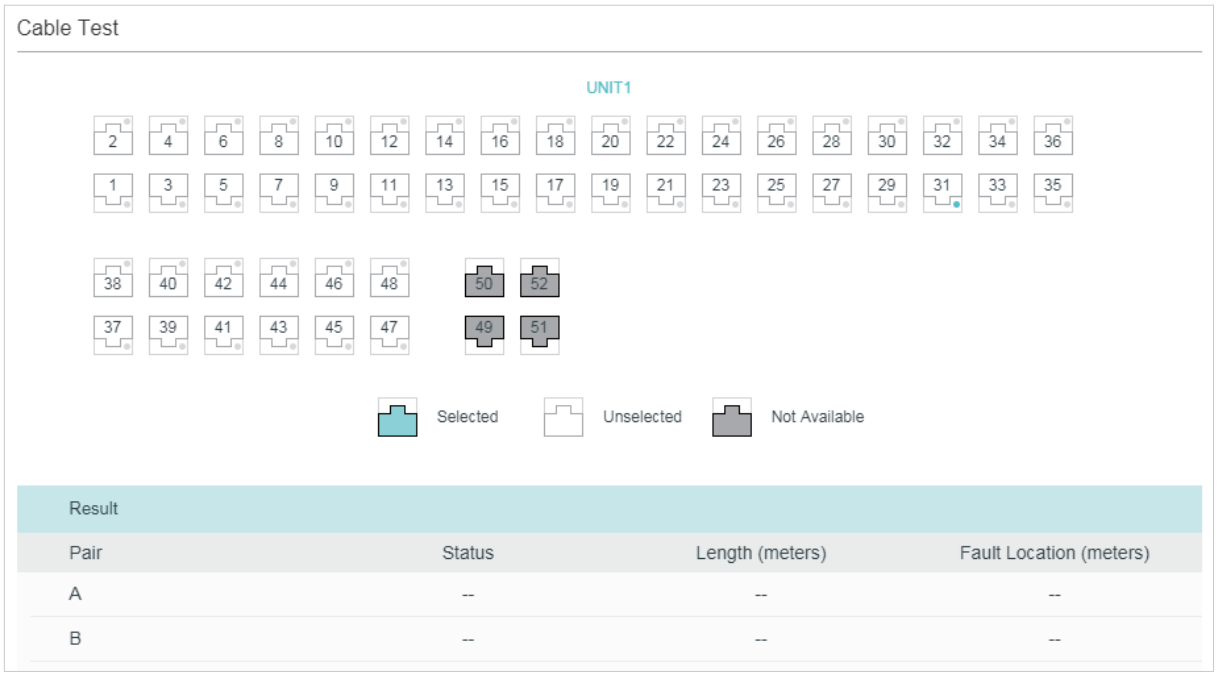
1 Diagnosing the Device

The device diagnostics feature provides cable testing, which allows you to troubleshoot based on the connection status, cable length and fault location.

1.1 Using the GUI

Choose the menu **MAINTENANCE > Device Diagnostics** to load the following page.

Figure 1-1 Diagnosing the Cable



Follow these steps to diagnose the cable:

1) Select your desired port for the test and click **Apply**.
2) Check the test results in the **Result** section.

Pair	Displays the Pair number.
Status	Displays the cable status. Test results include normal, closed, open and crosstalk. Normal : The cable is connected normally. Closed: A short circuit is being caused by abnormal contact of wires in the cable. Open: No device is connected to the other end or the connection is broken. Crosstalk: Impedance mismatch due to the poor quality of the cable.
Length	If the connection status is normal, the length range of the cable is displayed.

Fault Location	If the connection status is short, close or crosstalk, here displays the length from the port to the trouble spot.

1.2 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 { **fastEthernet** *port* | **gigabitEthernet** *port* | **ten-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 { **fastEthernet** *port* | **gigabitEthernet** *port* | **ten-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)	---

2 Diagnosing the Network

The network diagnostics feature provides Ping testing and Tracert testing. You can test connectivity to remote hosts, or to the gateways from the switch to the destination.

With Network Diagnostics, you can:

- Troubleshoot with Ping testing.
- Troubleshoot with Tracert testing.

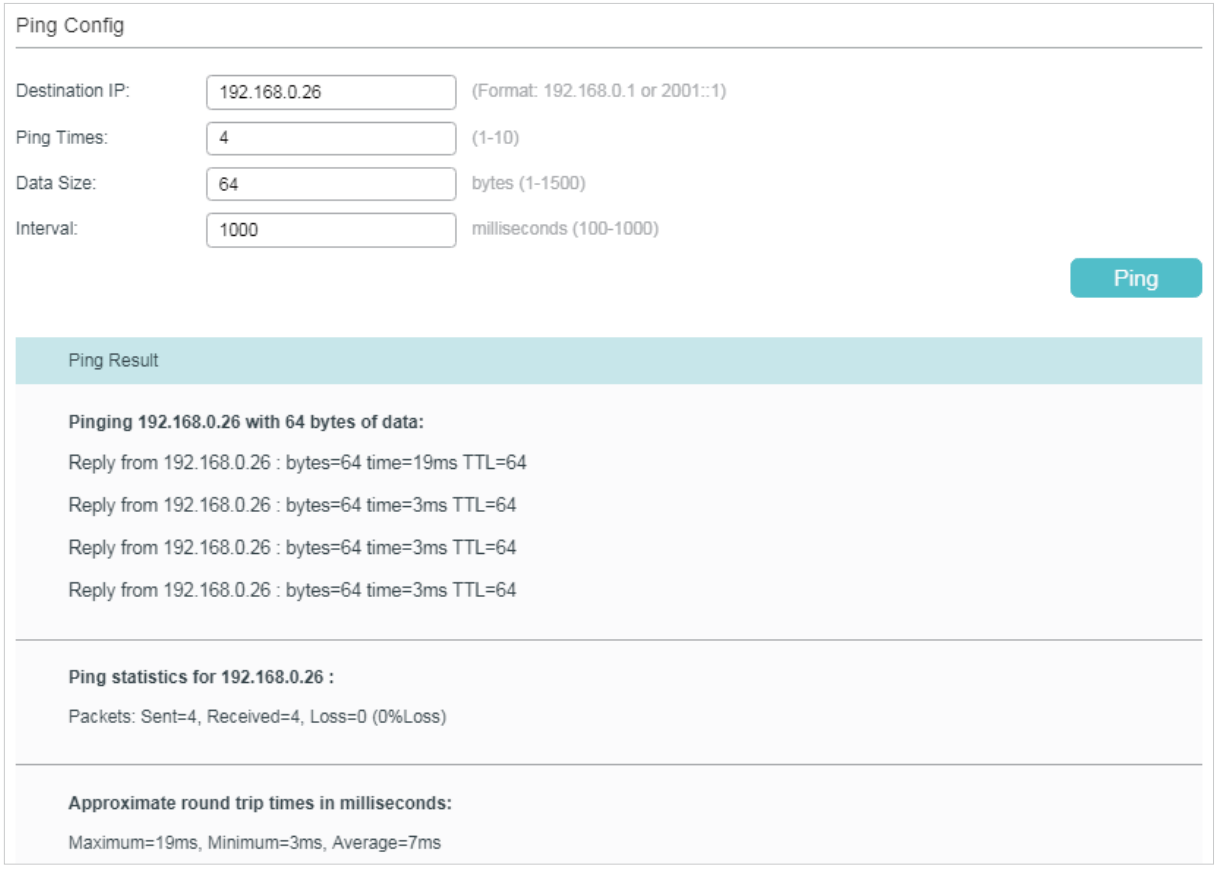
2.1 Using the GUI

2.1.1 Troubleshooting with Ping Testing

You can use the Ping tool to test connectivity to remote hosts.

Choose the menu **MAINTENANCE > Network Diagnostics > Ping** to load the following page.

Figure 2-1 Troubleshooting with Ping Testing



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 number of times test data will be sent for Ping testing. It is recommended to use the default value of 4.
Data Size	Enter the size of the data sent for Ping testing. It is recommended to keep the default value of 64 bytes.
Interval	Specify the interval at which ICMP request packets are sent. It is recommended to keep the default value of 1000 milliseconds.

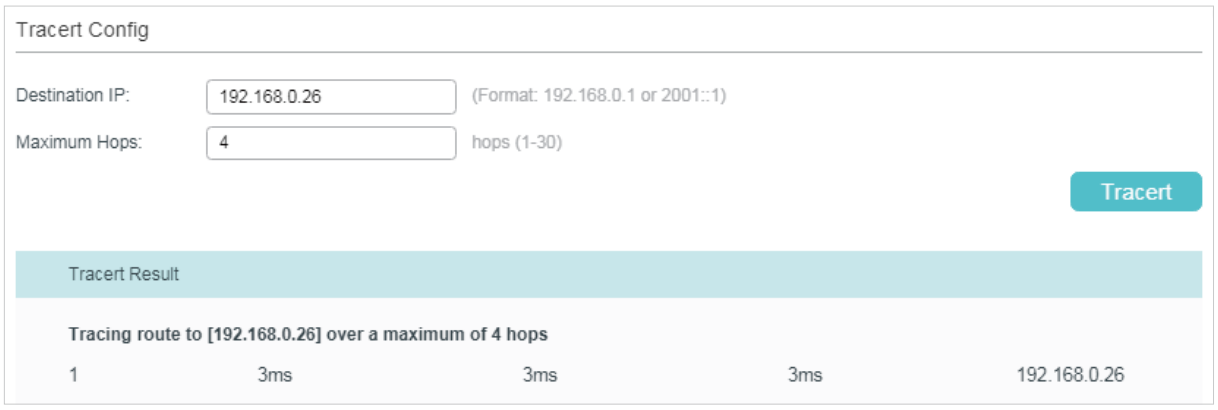
2) In the **Ping Result** section, check the test results.

2.1.2 Troubleshooting with Tracert Testing

You can use the Tracert tool to find the path from the switch to the destination, and test connectivity between the switch and routers along the path.

Choose the menu **MAINTENANCE > Network Diagnostics > Tracert** to load the following page.

Figure 2-1 Troubleshooting with Tracert Testing



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.
Maximum Hops	Specify the maximum number of the route hops the test data can pass through.

2) In the **Tracert Result** section, check the test results.

2.2 Using the CLI

2.2.1 Configuring the Ping Test

On privileged EXEC 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** *size* **] [-i** *interval* **]**

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.

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.

size: Specify the size of the sending data for ping testing. The values are from 1 to 1500 bytes; the default is 64 bytes.

interval: 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

2.2.2 Configuring the Tracert Test

On privileged EXEC 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.

3 Appendix: Default Parameters

Default settings of Network Diagnostics are listed in the following tables.

Table 3-1 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 3-2 Default Settings of Tracert Config

Parameter	Default Setting
Destination IP	192.168.0.100
Maximum Hops	4 hops

Part 33

Configuring System Logs

CHAPTERS

1. Overview
2. System Logs Configurations
3. Configuration Example
4. Appendix: Default Parameters

1 Overview

The switch generates messages in response to events, faults, or errors occurred, as well as changes in configuration or other occurrences. You can check system messages for debugging and network management.

System logs can be saved in various destinations, such as the log buffer, log file or remote log servers, depending on your configuration. Logs saved in the log buffer and log file are called local logs, and logs saved in remote log servers are called remote logs. Remote logs facilitate you to remotely monitor the running status of the network.

You can set the severity level of the log messages to control the type of log messages saved in each destination.

2 System Logs Configurations

System logs configurations include:

- Configure the local logs.
- Configure the remote logs.
- Backing up the logs.
- 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 2-1 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.

2.1 Using the GUI

2.1.1 Configuring the Local Logs

Choose the menu **MAINTENANCE > Logs > Local Logs** to load the following page.

Figure 2-1 Configuring the Local Logs



Follow these steps to configure the local logs:

1) Select your desired channel and configure the corresponding severity and status.

Channel	Local logs includes 2 channels: log buffer and log file. Log buffer indicates the RAM for saving system logs. The channel is enabled by default. Information in the log buffer is displayed on the **MAINTENANCE > Logs > Logs Table** page. It will be lost when the switch is restarted. Log file indicates the flash sector for saving system logs. Information in the log file will not be lost after the switch is restarted and can be exported on the **MAINTENANCE > Logs > Back Up Logs** page.
Severity	Specify the severity level of the log messages that are saved to the selected channel. Only log messages with a severity level value that is the same or lower than this will be saved. There are eight severity levels marked from 0 to 7. A lower value indicates a higher severity.
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**.

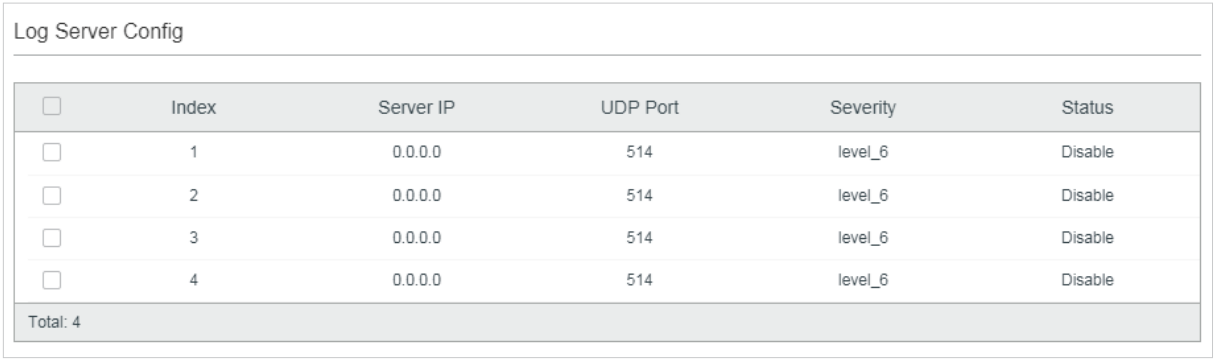
2.1.2 Configuring the Remote Logs

You can configure up to four hosts to receive the switch's system logs. These hosts are called Log Servers. The switch will forward the log message to the servers once a log

message is generated. To display the logs, the servers should run a log server software that complies with the syslog standard.

Choose the menu **MAINTENANCE > Logs > Remote Logs** to load the following page.

Figure 2-2 Configuring the Remote Logs



Follow these steps to configure the information of remote log servers:

1) Select an entry to enable the server, and then set the server IP address and severity.

Server IP	Specify an IP address of the log server.
UDP Port	Displays the UDP port used by the server to receive the log messages. The switch uses standard port 514 to send log messages.
Severity	Specify the severity level of the log messages sent to the selected log server. Only log messages with a severity level value that is the same or lower than this will be saved.
Status	Enable or disable the log server.

2) Click **Apply**.

2.1.3 Backing up the Logs

Choose the menu **MAINTENANCE > Logs > Back Up Logs** to load the following page.

Figure 2-3 Backing up the Log File

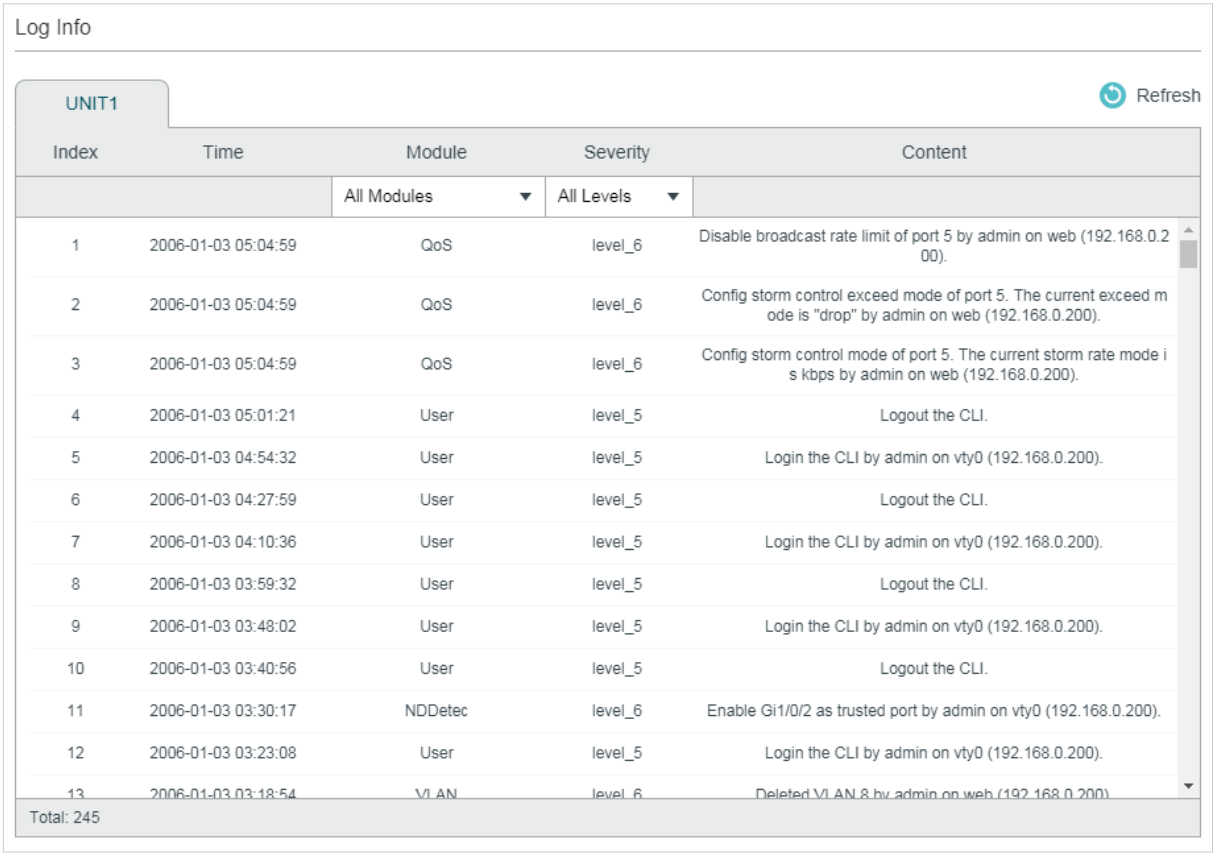


Click **Back Up Logs** to save the system logs as a file on your computer. If the switch system breaks down, you can check the file for troubleshooting.

2.1.4 Viewing the Log Table

Choose the menu **MAINTENANCE > Logs > Log Table** to load the following page.

Figure 2-4 View the Log Table



Select a module and a severity to view the corresponding log information.

Time	Displays the time the log event occurred. 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.
Content	Displays the detailed information of the log event.

2.2 Using the CLI

2.2.1 Configuring the Local Logs

Follow these steps to configure the local logs:

Step 1	**configure** Enter global configuration mode.
Step 2	**logging buffer** Configure the switch to save system messages in log buffer. Log buffer indicates the RAM for saving system logs. Information in the log buffer 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. A lower value indicates a higher severity. Only log messages with a severity level value that is the same or lower than this will 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** Configure the switch to save system messages in log file. Log file indicates the flash sector for saving system logs. Information in the log file 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 logs 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. A lower value indicates a higher severity. Only log messages with a severity level value that is the same or lower than this will be saved to the flash. The default level is 3, indicating that the log messages 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 logs.
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 logs 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)
Console	5	enable	Immediately
Monitor	5	enable	Immediately

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Configuring the Remote Logs

You can configure up to four hosts to receive the switch's system logs. These hosts are called Log Servers. The switch will forward the log message to the servers once a log message is generated. To display the logs, the servers should run a log server software 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 a remote host to receive the switch's system logs. The host is called Log Server. You can remotely monitor the settings and operation status of the switch through the log server. *idx*: Enter the index of the log server. The switch supports 4 log servers at most. *host-ip*: Enter the IP address of the log server. *level*: Specify the severity level of the log messages sent to the log server. The range is from 0 to 7, and a lower value indicates a higher severity. Only log messages with a severity level value that is the same or lower than this will be sent. The default is 6, indicating that the log information of levels 0 to 6 will be sent to the log server.
Step 3	**show logging loghost** [*index*] View the configuration information of the log server. *index*: Enter the index of the log server 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 server 2, set its IP address as 192.168.0.148, and allow logs of levels 0 to 5 to be sent to the server:

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

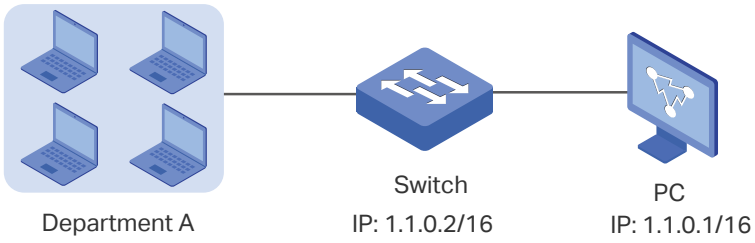
Switch#copy running-config startup-config

3 Configuration Example

3.1 Network Requirements

The company network manager needs to monitor network of department A for troubleshooting.

Figure 3-1 Network Topology



3.2 Configuration Scheme

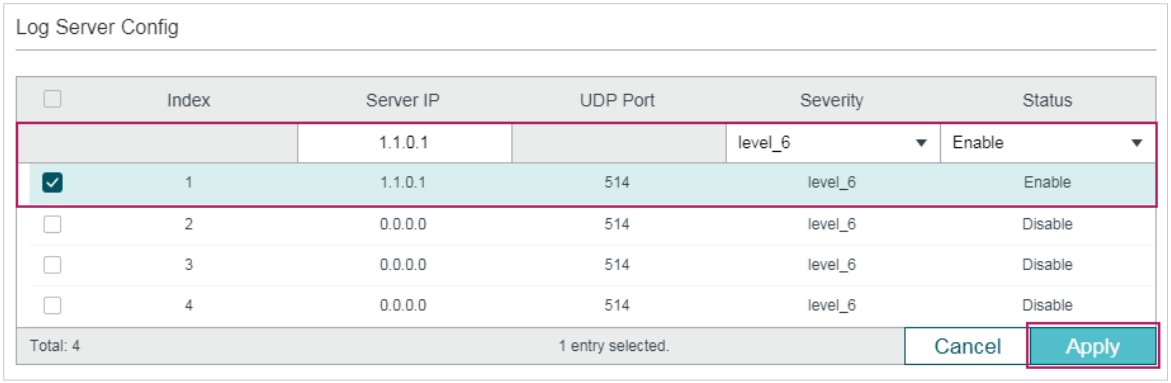
The network manager can configure the PC as a log server to receive the switch's system logs. Make sure the switch and the PC are reachable to each other; configure a log server that complies with the syslog standard on the PC and set the PC as the log server.

Demonstrated with T1600G-52TS, this chapter provides configuration procedures in two ways: using the GUI and Using the CLI.

3.3 Using the GUI

1) Choose the menu **MAINTENANCE > Logs > Remote Logs** to load the following page. Enable host 1, and set the PC's IP address 1.1.0.1 as the server IP address, and the severity as level_5; click **Apply**.

Figure 3-2 Configuring the Log Server



2) Click Save to save the settings.

3.4 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

4 Appendix: Default Parameters

Default settings of maintenance are listed in the following tables.

Table 4-1 Default Settings of Local Logs

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 4-2 Default Settings of Remote Logs

Parameter	Default Setting
Server IP	0.0.0.0
UDP Port	514
Severity	Level_6
Status	Disabled

FCC STATEMENT

Product Name: JetStream Gigabit Smart Switch

Model Number: T1600G-52TS/T1600G-52PS

Responsible party:

TP-Link USA Corporation, d/b/a TP-Link North America, Inc.

Address: 145 South State College Blvd. Suite 400, Brea, CA 92821

Website: http://www.tp-link.com/us/

Tel: +1 626 333 0234

Fax: +1 909 527 6803

E-mail: sales.usa@tp-link.com

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.

We, TP-Link USA Corporation, has determined that the equipment shown as above has been shown to comply with the applicable technical standards, FCC part 15. There is no unauthorized change is made in the equipment and the equipment is properly maintained and operated.

Issue Date: January 2018

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.

EU declaration of conformity

TP-Link hereby declares that the device is in compliance with the essential requirements and other relevant provisions of directives 2014/30/EU, 2014/35/EU, 2009/125/EC and 2011/65/EU.

The original EU declaration of conformity may be found at http://www.tp-link.com/en/ce

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	—	○	○	○	○	○

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

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.

http://www.tp-link.com