FIBERROAD

Web-based Network Management User Manual

About This Manual

Introduction
This document chapter includes an introduction to the Fiberroad L2+ Managed WebGUI Network Management, which also contains Fiberroad Industrial Grade Ethernet Switch and Commercial Grade Ethernet Switch Series.

Conventions
This document contains notices, figures, screen captures, and certain text conventions.

Figures and Screen Captures
This document provides figures and screen captures as examples. These examples contain sample data. This data may vary from the actual data on an installed system.

Copyright©2022 Fiberroad Technology Co., Ltd. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form, be it electronically, mechanically, or by any other means such as photocopying, recording or otherwise, without the prior written permission of Fiberroad Technology Co., Ltd. (Fiberroad)

Information provided by Fiberroad is believed to be accurate and reliable. However, no responsibility is assumed by Fiberroad for its use nor for any infringements of patents or other rights of third parties that may result from its use. No license is granted by implication or otherwise under any patent rights of Fiberroad.

The information contained in this publication is subject to change without notice.

Trademarks
Fiberroad's trademarks have been identified as such. However, the presence or absence of such identification does not affect the legal status of any brand.

Units of Measurement
Units of measurement in this publication conform to SI standards and practices.

Jan 01, 2022
Version number: 1.0

CONTENTS

Revision History 8
Chapter 1 System Configurations 9
1. About Web-GUI Management 9
1.1 Preparing for Web Management 9
1.2 Device Summary 10
1.3 System - Administrator 11
1.3.1 System-Administrator-Administrators 11
1.3.2 System – Administrator - Online Users 11
1.3.3 System – Administrator – Management Setting 12
1.4 System Log 12
1.4.1 System Log – Setting 12
1.4.2 System Log – View 14
1.5 Configurations 14
1.5.1 Configurations - View 14
1.5.2 Configurations – Import 15
1.5.3 Configurations – Export 15
1.5.4 Configurations – Restore Factory Default 16
1.5.5 Configurations – Date & Time 16
1.5.6 Configurations – Summer Time Setting 17
1.5.7 Configurations – Device Status 18
1.5.8 Configurations – ARP Table 19
1.5.9 Configurations – Software Upgrade 19
1.5.10 Configurations – Reboot 20
2. Management 21
2.1.1 Management - IP Interfaces – Settings 21
2.1.2 Management – IP Interfaces – DHCP Client 22
2.1.3 Management – IP Interfaces – DHCP Client(IPv6) 23
2.2 Management – SNMP 24
2.2.1 Management -SNMP - v1/v2 setting 24
2.2.2 Management – SNMP – v3 setting 25
2.2.3 Management – SNMP – Trap Setting 27
2.3 Management – LLDP 28

2.3.1 Management – LLDP - Global Setting 28
2.3.2 Management – LLDP – Port Configurations 29
Chapter 3 Base Configuration 31
3 Base Configuration 31
3.1.1Base Configuration-Port-Status And Setting....31
3.1.2 Base Configuration-Port-Description 32
3.1.3 Base Configuration-Port-Statistics....33
3.1.4 Base Configuration-Port-SFP Information 34
3.1.5 Base Configuration-Port-SFP Detail Information....35
3.1.6 Base Configuration-Port-Traffic 35
3.2 Base Configuration - VLAN....36
3.2.1 Base Configuration-VLAN-Basic Setting 36
3.2.2 Base Configuration-VLAN-Port Setting....37
3.2.3 Base Configuration-VLAN-Double VLAN 38
3.3 Base Configuration-QOS 39
3.3.1 Base Configuration-QoS- Mapping -802.1p Priority....39
3.3.2 Base Configuration-QoS- Mapping – DSCP Priority....39
3.3.3 Base Configuration-QoS- Mapping – Local Priority 40
3.4 Base Configuration-QoS- Ports....41
3.4.1 Base Configuration-QoS- Ports-Port Priority 42
3.4.2 Base Configuration-QoS- Ports-Rate Limitation 43
3.5 Base Configuration-FDB Table....44
3.5.1 Base Configuration-FDB Table- Configuration – Aging Setting 44
3.5.2 Base Configuration-FDB Table- Configuration – Static Mac Entry 44
3.5.3 Base Configuration-FDB Table- Configuration – Port Learning Ability .45
3.5.4 Base Configuration-FDB Table- FDB Table....46
3.5.5 Base Configuration-FDB Table- Delete Entries 47
3.5.6 Base Configuration-FDB Table- Port Mirror....48
3.5.7 Base Configuration-FDB Table- Port Isolate 49
3.5.8 Base Configuration-FDB Table- Storm Filters 49
4. Advanced Configuration....51
4.1 Advanced Configuration – Ports – Ports Security....51
4.2 Advanced Configuration – ACL 52

4.2.1 Advanced Configuration – ACL – ACL Group Setting.....52
4.2.2 Advanced Configuration – ACL – ACL Rule Setting.....53
4.3 Advanced Configuration – DHCP snooping.....55
4.3.1 Advanced Configuration – DHCP snooping – Global Setting.....55
4.3.2 Advanced Configuration – DHCP snooping – Port Setting.....56
4.3.3 Advanced Configuration – DHCP snooping – Binding Table 56
4.4 Advanced Configuration – DHCP Server.....57
4.4.1 Advanced Configuration – DHCP Server – Global Setting.....57
4.4.2 Advanced Configuration – DHCP Server – IP Address Pool.....58
4.4.3 Advanced Configuration – DHCP Server – IP Address Lease Information 59
4.5 Advanced Configuration – Multicast 59
4.5.1 Advanced Configuration – Multicast – Manual Address Setting 59
4.5.2 Advanced Configuration – Multicast – IGMP snooping Global Setting.60
4.5.3 Advanced Configuration – Multicast – IGMP snooping VLAN setting ...61
4.5.4 Advanced Configuration – Multicast – IGMP snooping IP Groups 62
4.5.5 Advanced Configuration – Multicast – IGMP snooping MAC Groups ..63
4.5.6 Advanced Configuration – Multicast – IGMP snooping Multicast Table 63
4.6 Advanced Configuration – GMRP 64
4.6.1 Advanced Configuration – GMRP– GMRP Setting.....64
4.7 Advanced Configuration – GVRP.....65
4.7.1 Advanced Configuration – GVRP – GVRP Setting.....65
4.8 Advanced Configuration – 802.1X 66
4.8.1 Advanced Configuration – 802.1X – Authentication Server.....66
4.8.2 Advanced Configuration – 802.1X – Global Setting.....67
4.8.3 Advanced Configuration – 802.1X – Port Configurations.....68
4.8.4 Advanced Configuration – 802.1X – User Authentication Info 69
4.9 Advanced Configuration – Link Aggregation 70
4.9.1 Advanced Configuration – Link Aggregation – Global Setting.....70
4.9.2 Advanced Configuration – Link Aggregation – Port Configuations.....71
4.9.3 Advanced Configuration – Link Aggregation – Aggregation Information 72

4.10 Advanced Configuration – Loopback 73
4.10.1 Advanced Configuration – Loopback – Global Setting 73
4.10.2 Advanced Configuration – Loopback – Port Configuration 74
4.11 Advanced Configuration – STP 75
4.11.1 Advanced – STP – Bridge Configuration 75
4.11.2 Advanced-STP-Mapping Configuration 76
4.11.3 Advanced-STP-Priority Configuration 77
4.11.4 Advanced-STP-CIST Port Configuraion 77
4.11.5 Advanced-STP-MSTI Port Configuraion 79
4.11.6 Advanced-STP-Bridges Status 80
4.11.7 Advanced-STP-Ports Status 81
4.11.8 Advanced Configuration – Statistics 81
4.12 Advanced Configuration – ERPS 82
4.12.1 Advanced Configuration – Global Setting 82
4.12.2 Advanced Configuration – ERPS - Ring Setting 82
4.12.3 Advanced Configuration – ERPS - Ring Information 83
4.13 L3 Config – Static Router Config 84
4.14 Advanced Configuration – Alarm 85
4.14.1 Advanced Configuration – Alarm –Relay Setting 85
4.13.2 Advanced Configuration – Alarm – Led Setting 85
4.13.3 Advanced Configuration – Alarm – Temperature Setting 86
4.13.4 Advanced Configuration – Alarm – Trap Setting 86
4.13.5 Advanced Configuration – Alarm – Power Setting 87
4.15 PoE Management 87
4.15.1 PoE Management – Port Configuration 87
4.15.2 PoE Management – Smart Power Configuration 89
4.15.3 PoE Management – Time Range and Time Supply Configuration 89
4.16 Extended 90
4.16.1 Extended – Port Cable Setting 90
4.16.2 Extended – Ping Test 91
5 Extension 92
5.1 Series Management 92
5.1.1 Series Managemetn- Serial Device 92

5.1.2 Series Managemetn- Serial Protocol 93
5.1.3 Series Managemetn- Serial Statistics 94

Revision History

Version	Date	Author	Reasons of Change	Section(s) Affected
1.0	2017/12/04		Initial Release	All
2.0	2022/07/4		MSTP/Port Description/Static Route/Summer Time	Portion

Chapter 1 System Configurations

This chapter describes the port configuration in detail, including but not limit to the following:

- Administrator
- Router Table
- ARP Table
- Software Upgrade

---

1. About Web-GUI Management

There is an embedded HTML web site residing in flash memory on CPU board of the switch, which offers advanced management features and allows users to manage the switch from anywhere on the network through a standard browser such as Mozilla Firefox or Chrome. (Note: Window IE is not supported) The Web-Based Management supports Mozilla Firefox 54.X or later, or Chrome 59.X or later. The Web browser is a program that can read hypertext.

1.1 Preparing for Web Management

Before using the web management, install the Ethernet Switch on the network and make sure that any one of the PCs on the network can connect with the Ethernet through the web browser.

All of the Fiberroad Network Switch default value of IP, subnet mask, username and password are listed as below:

- IP Address: 192.168.1.6
- HTTP service: Enable
- User Name: admin
- Password: admin

1.2 Device Summary

Overview the device information and port status.

L2+ Managed MAX Industrial Ethernet Switch Series

L2+ Managed Industrial Ethernet Switch with Optical Fiber Bypass Series

L2+ Managed Industrial Ethernet Switch with Serial Ports Series

L2+ Managed Industrial Ethernet Switch Series

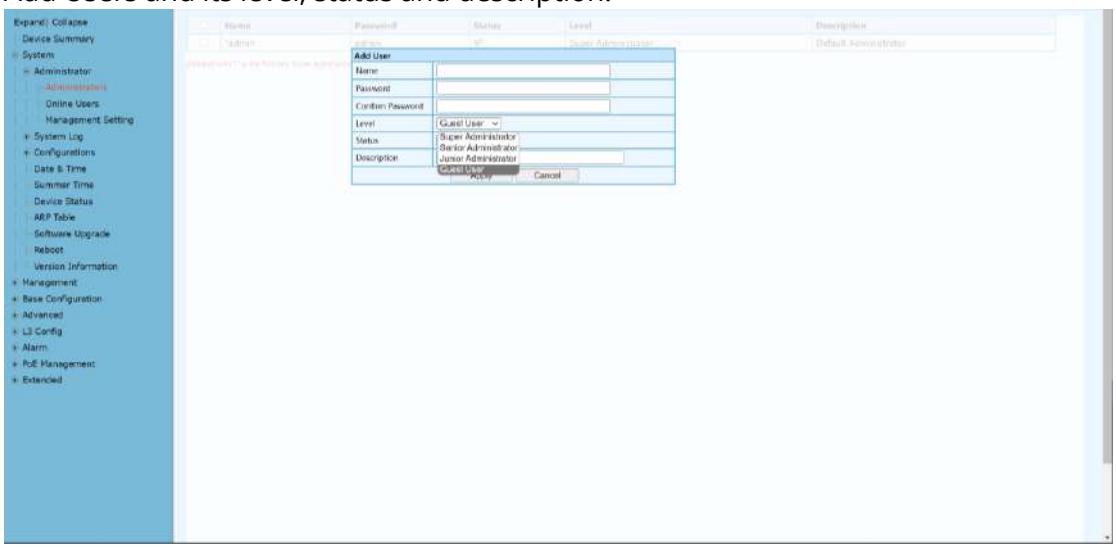
L2+ Managed Industrial Ethernet Switch Series

L2+ Managed PoE Switch Series(Commercial Grade)

1.3 System - Administrator

1.3.1 System-Administrator-Administrators

Add Users and its level, status and description.

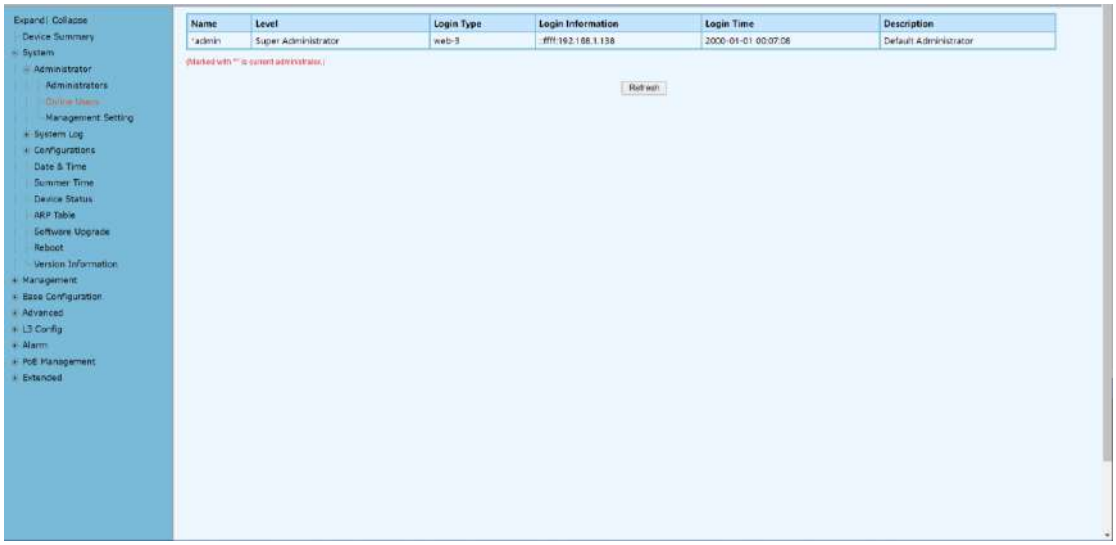


Item	Description	Notes
Name/Password/ConfirmPassword		As Needed
Level	Super/Senior/Junior/Guest	
Status	ON/OFF	
Description		As Needed

Remarks: 1. A total of 16 users can be added regardless of the level

1.3.2 System – Administrator - Online Users

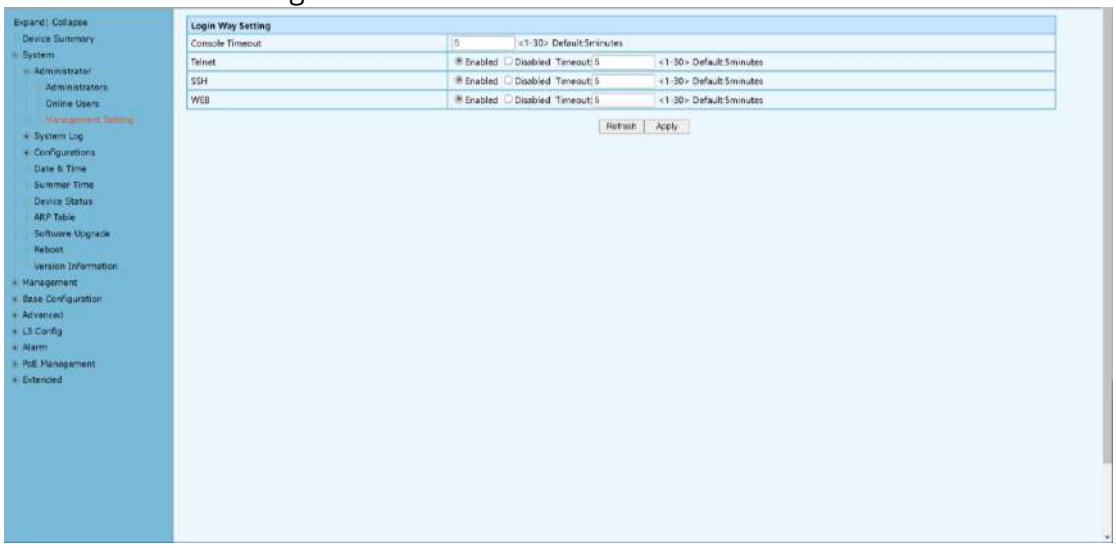
Overview online users information



Remarks: 1, Only super administrator have this privilege.

1.3.3 System – Administrator – Management Setting

Access Timeout Setting

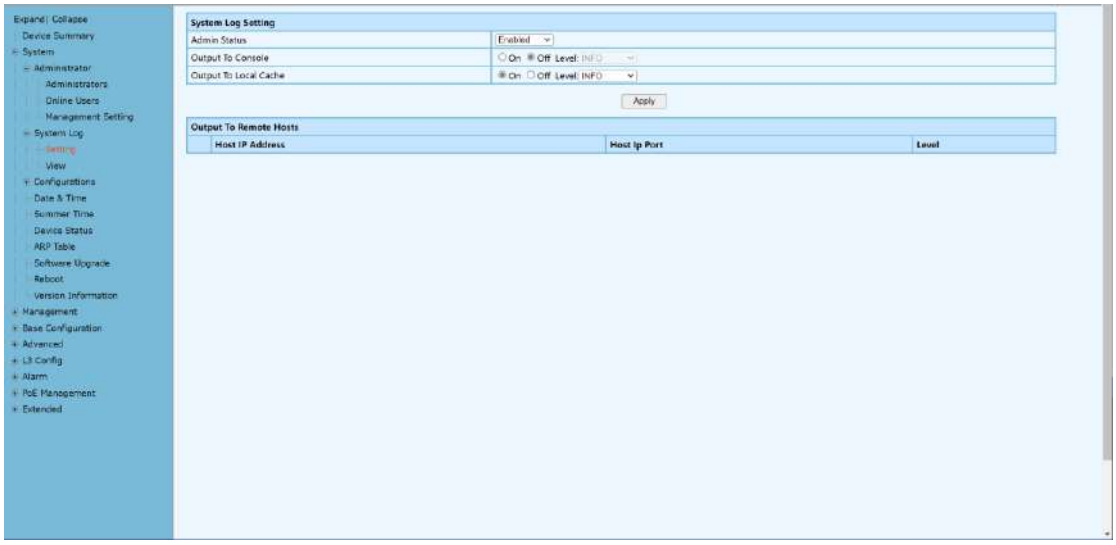


Item	Description	Notes
Consolt Timeout	1-30(When enabled)	Default:5 minutes
Telnet Timeout	1-30(When enabled)	Default:5 minutes
SSH Timeout	1-30(When enabled)	Default:5 minutes
WEB Timeout	1-30(When enabled)	Default:5 minutes

1.4 System Log

1.4.1 System Log – Setting

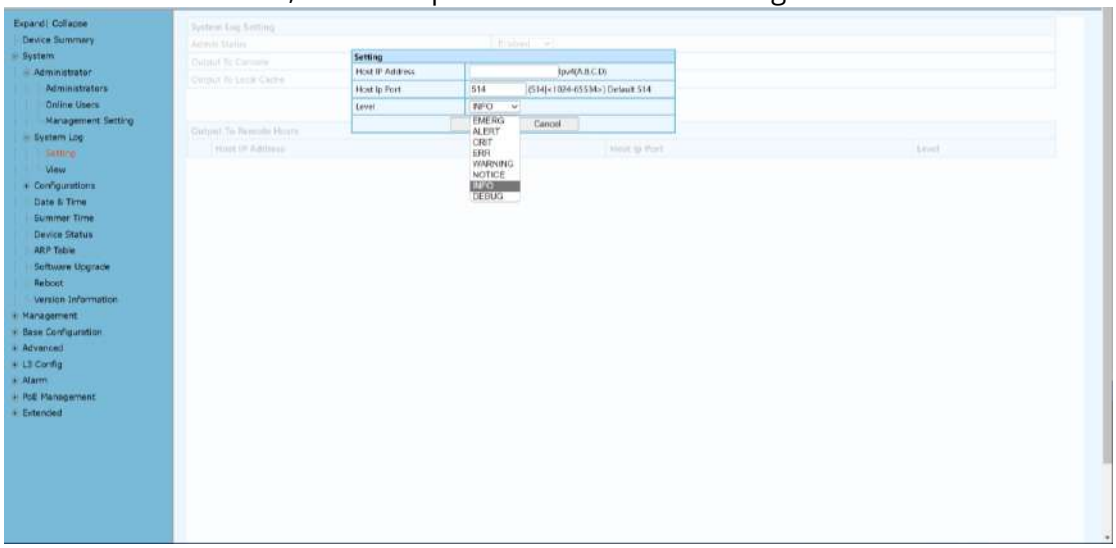
In the system log setting interface, you can view or modify system log configuration



Item	Description	Notes
Admin Status	Enable/Disable	Default: Enable
Output To Console	ON/OFF	Default:OFF
Output To Local Cache	ON/OFF	Defalt:ON
Level	System log level, divided into 8	Default: INFO

	levels according to the severity **EMERG**: level 0, the system cannot be used **ALERT** : Level 1, need to be processed immediately **CRIT**: Level 2, Severe State **ERR**: Level 3, Error Status WARNNING : Level 4, Warning Status **NOTICE** : Level 5, normal but important state **INFO** : Level 6, Notification Event **DEBUG** : Level 7, debugging information	

Click the “Add” button, to the output to remote hosts setting.

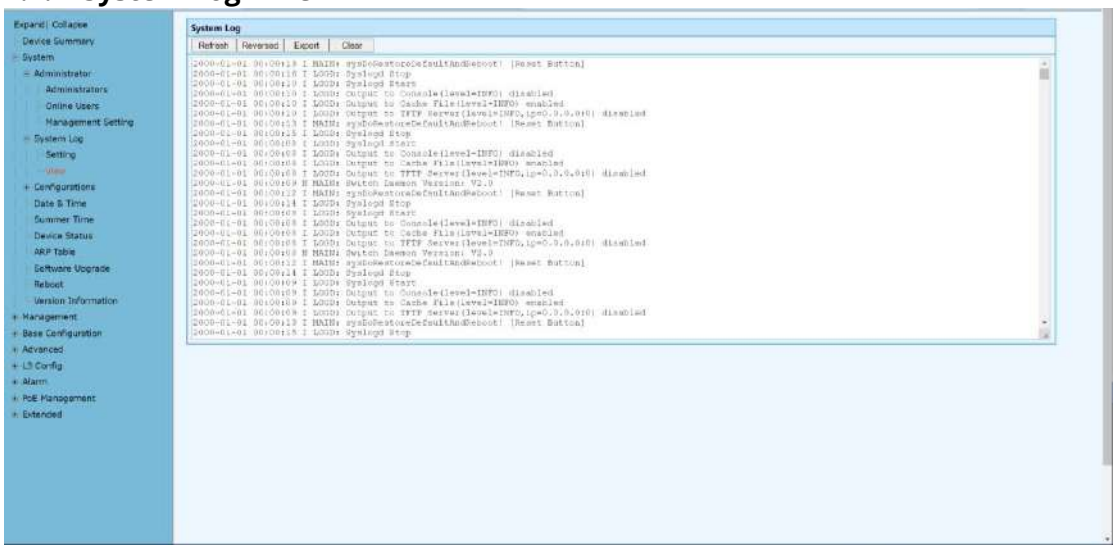


Item	Description	Notes
Host IP Address	Remote log host IP address	
Host IP Port	Remote log host port, range 514,1024-65534	Default:514
Level	System log level, divided into 8 levels according to severity **EMERG**: level 0, system cannot be used ALERT : Level 1, need to be processed immediately CRIT: Level 2, Severe State ERR : Level 3, Error Status **WARNNING** : Level 4, Warning Status **NOTICE** : Level 5, normal but important state **INFO** : Level 6, Notification Event	Default: INFO

	DEBUG : Level 7, debugging information

Remarks: 1. The smaller the log level value, the higher the level. Only logs with a level equal to or greater than the set level will be output. For example, if you set the logging level to the console to 5 (NOTICE), only logs with level 0 to 5 will be output to the console.

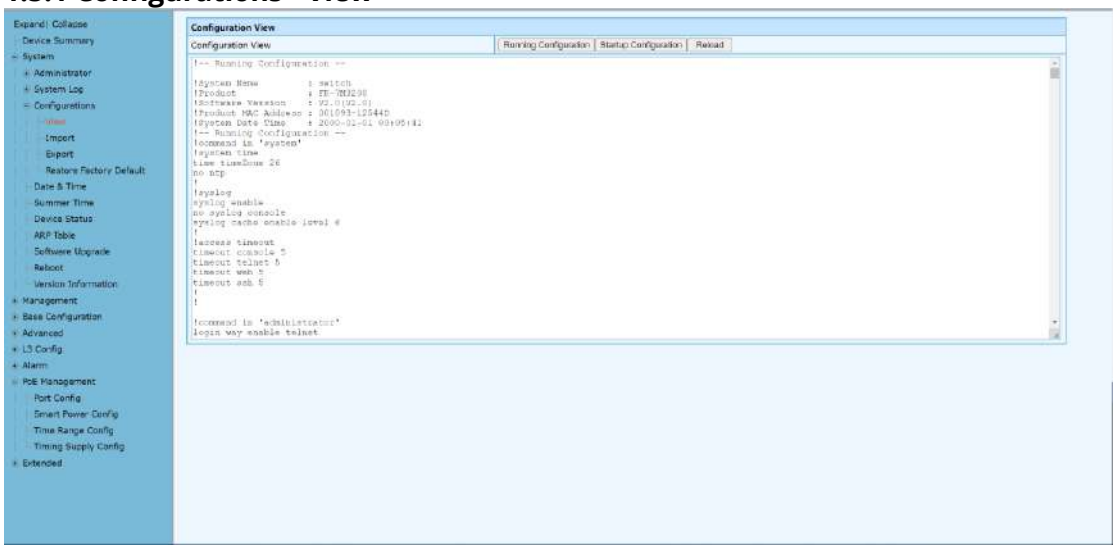
1.4.2 System Log – View



Item	Description	Notes
Refresh	Refresh the system log content	
Reversed	New to old display in chronological order	
Export	Export the contents of the system log	
Clear	Clear he contents of the system log	

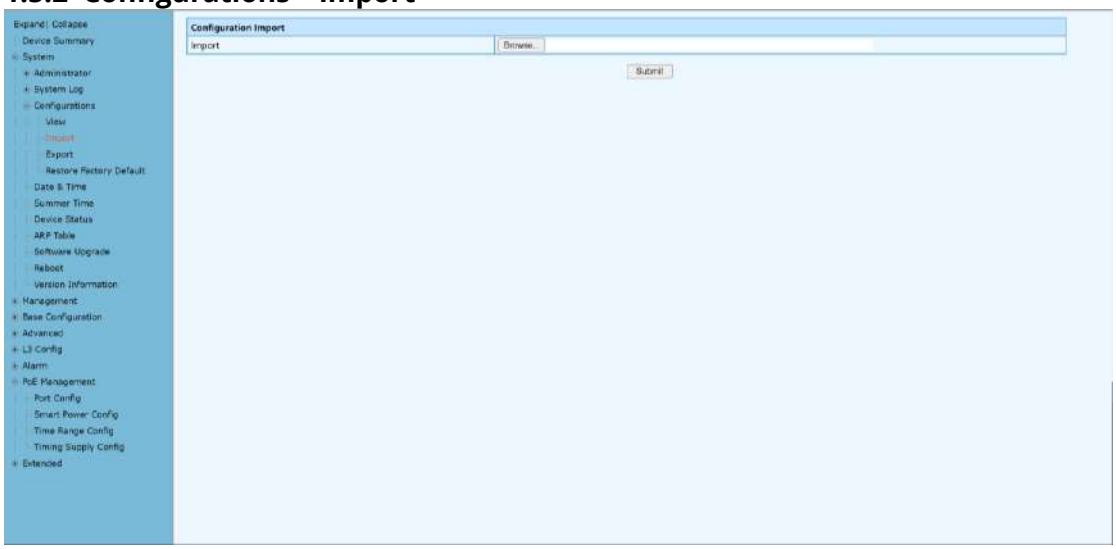
1.5 Configurations

1.5.1 Configurations - View



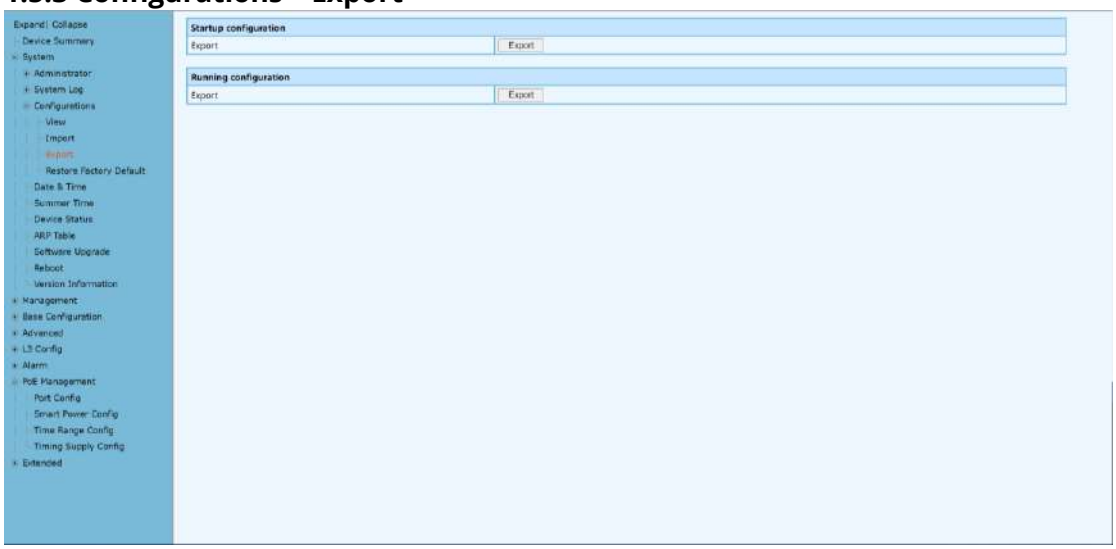
Item	Description	Notes
Running Configuration	Show system running configuration	Text Style
Startup Configuration	Show system startup configuration	Text Style
Reload	Reload the running or startup configuration	

1.5.2 Configurations – Import



Remarks: 1, In the Configurations [Import] interface, click [Browse], select the configuration file to import, and click [Submit] to start the import.

1.5.3 Configurations – Export



Remarks: 1. Export configuration is divided into startup configuration and running configuration. Click [Export] in the corresponding project to prompt up the "File Save" dialog box (different browsers may differ, here take the IE11 browser as an example), click [Save] to export the corresponding configuration file to the local.

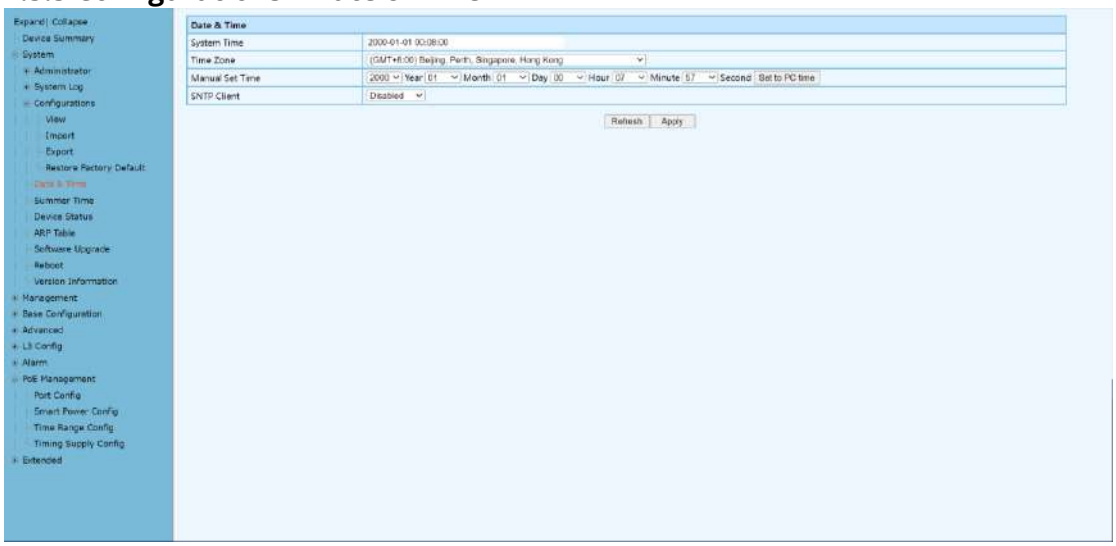
1.5.4 Configurations – Restore Factory Default

Configuration Steps

1, Click [Restore] and then click [OK] in the confirmation dialog box to restore the factory configuration.

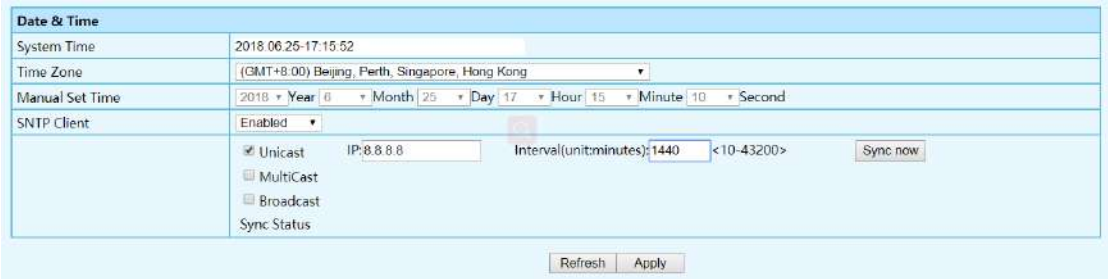
2. Click [Cancel] to cancel the factory configuration restoration. After a successful factory reset, the system automatically restarts to take effect to the factory configuration.

1.5.5 Configurations – Date & Time



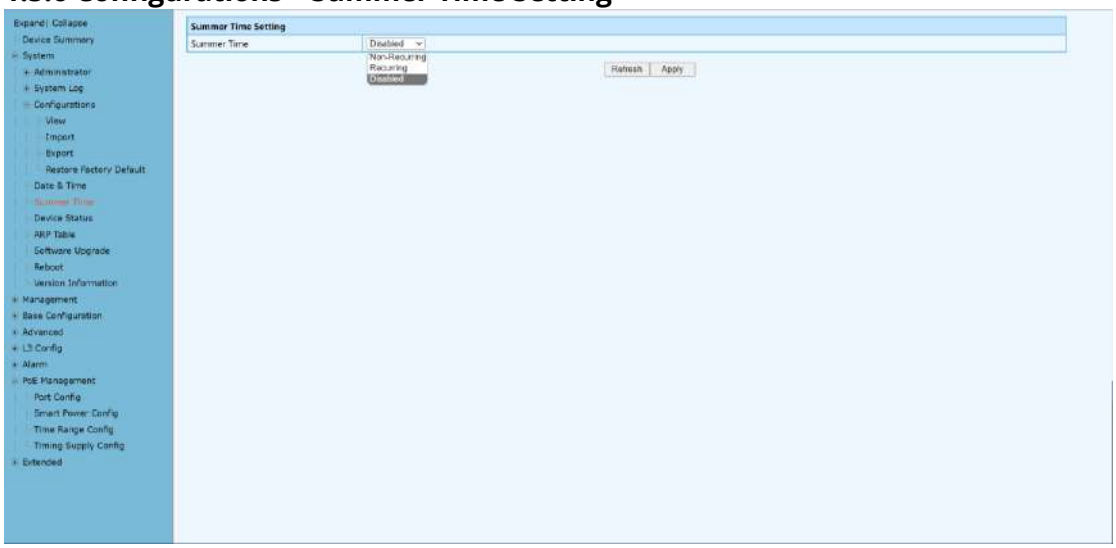
Item	Description	Notes
System Time	Display the actual effective system time.	Read Only
Time Zone	System time zone setting, select any time zone from the drop-down list.	
Manual Set Time	It can be set after the SNTP client is disabled. The year range is 1970-2037.Others are the same as the common settings.	
Set to PC time	Synchronize with PC time	
SNTP Client	Enabled: Enable the SNTP client	Default:Disabled

	Disabled: Disable the SNTP client



Item	Description	Notes
Synchronous Mode	Unicast Multicast Broadcast	These three modes are multi-selectable, but at least one must be selected
IP	IP address pf SNTP, Default IP address 8.8.8.8; Interval range 10-43200, and default value 1440	Only for unicast mode
Interval	SNTP client time synchronization interval	Only for unicast
Sync now	SNTP client immediate synchronize times	

1.5.6 Configurations – Summer Time Setting

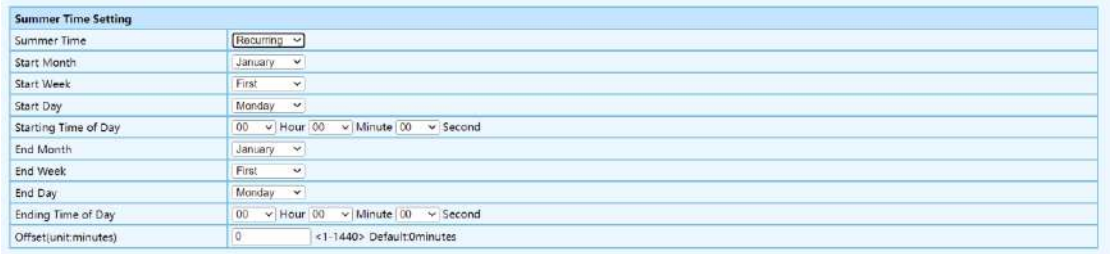


Configuration Step

1.Select [System/ Summer Time] in the navigation bar to enter the [Summer Time] interface.

Non-Recurring

Recurring



Default: Disabled

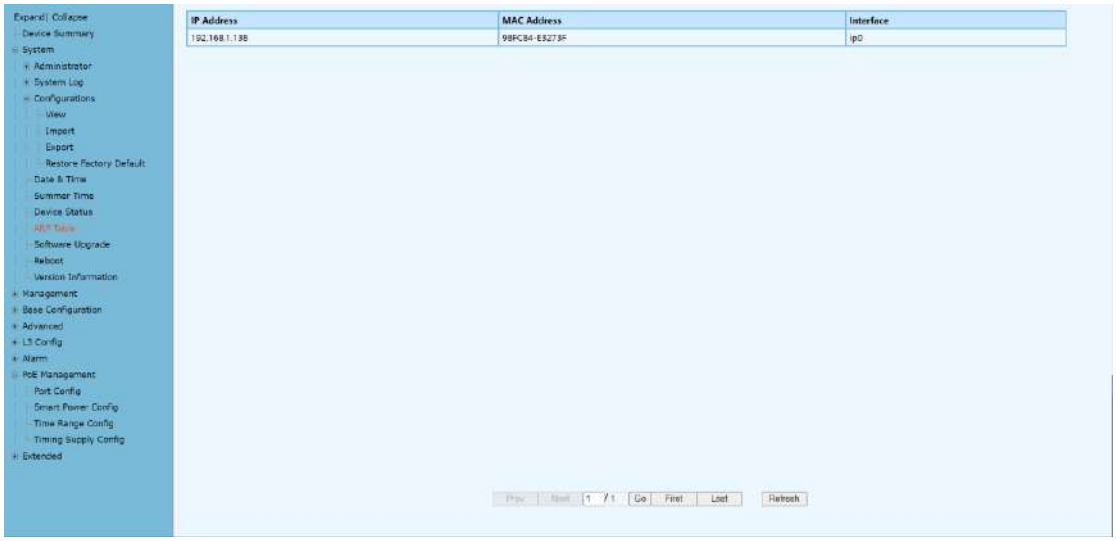
1.5.7 Configurations – Device Status

In the [Device Status] interface, the basic information and the operating status information of the device system are displayed.

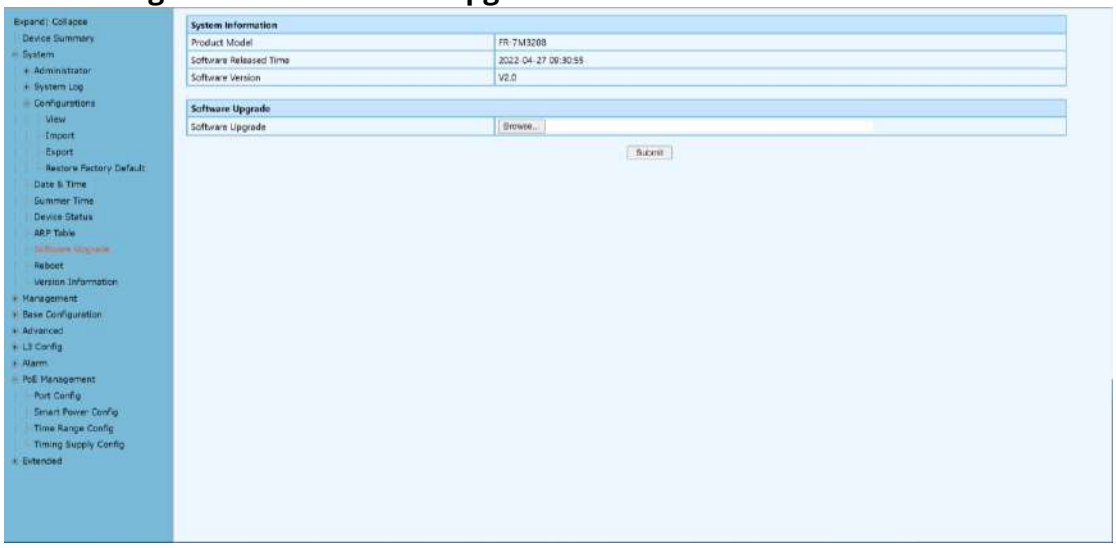
Item	Description	Notes
Product Model	The device mode	Read Only
Product MAC Address	The device MAC address	Read Only
Product Serial Number	The device product serial number	Read Only
Software Version	The software version running on	Read Only
Software Released Date	The time when running the software	Read Only
Hardware Version	The hardware version of the current device	Read Only
Date and Time	The device system time	Read Only
Operation Hours	The system running time	Read Only
CPU Usage	The system's CPU usage.	Read Only
Memory Usage	The memory usage of the device system	Read Only
Configuration Usage	Configuration space usage of the device system	Read Only

1.5.8 Configurations – ARP Table

Each switch has an ARP table to stroe the IP addresses and MAC addresses of the network devices.



1.5.9 Configurations – Software Upgrade

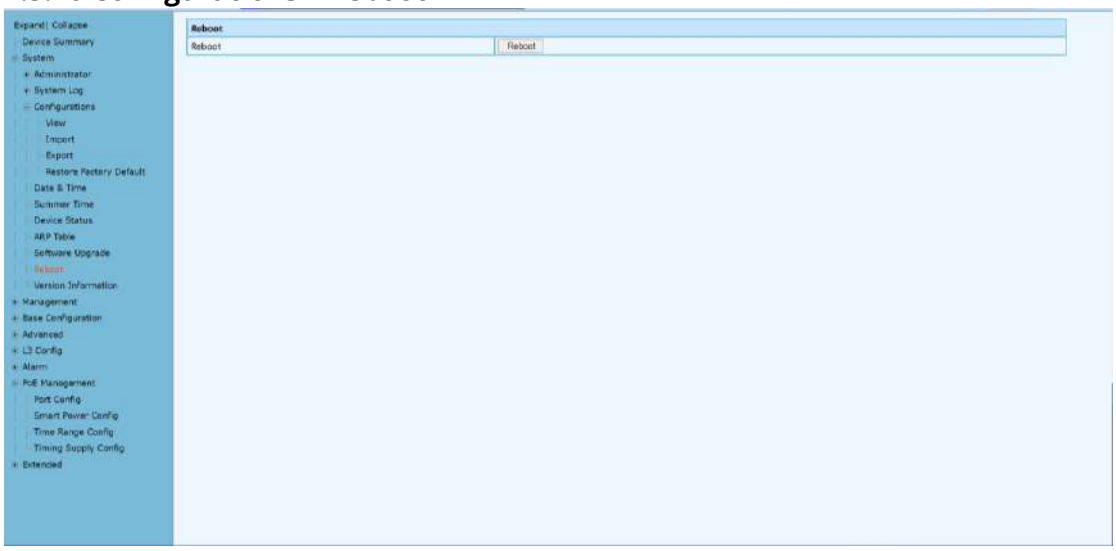


Configuration Step

1, On the [Software Upgrade] interface, click [Browse] to select the upgrade file to be imported. (The upgrade files are generally of the form .ub and .urk. Marked with "b" for BOOT files and "r" for "File System". The file is marked with k for the file with the kernel. Click [Submit]. The system starts uploading the upgrade file. After the upload is complete, the device automatically restarts to update the software after the upgrade is complete.

2, During the software upgrade, make sure that the device is powered up until the upgrade is completed.

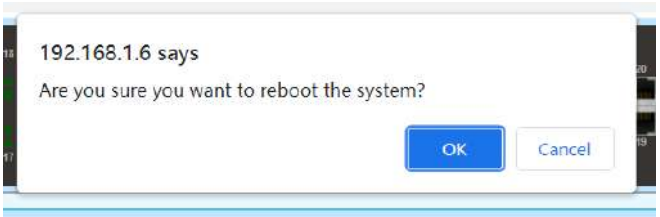
1.5.10 Configurations – Reboot

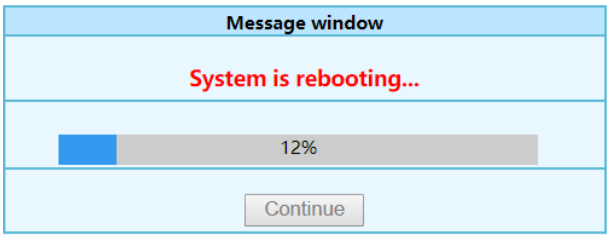


Configuration Step

1.Select [System / Configurations / Reboot] in the navigation bar to enter the [Reboot] interface

2. Click [Reboot] and the 'Confirm Restart' dialog box will pop up. Click OK to restart the device. A restart progress bar is displayed. Click [Cancel] to cancel the restart of the device.





Chapter 2 Management Configurations

This chapter describes the port configuration in detail, including but not limit to the following:

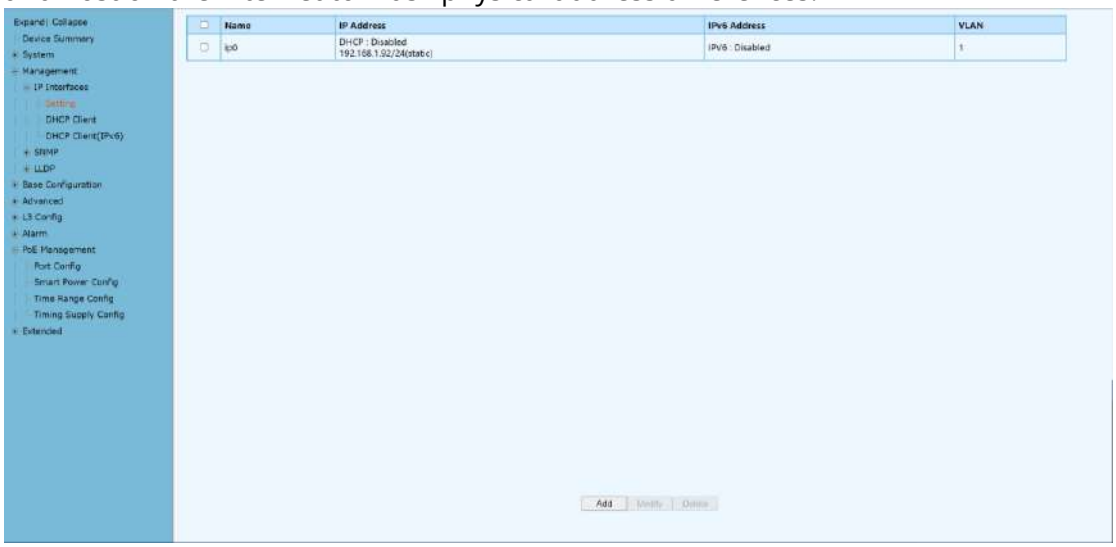
- IP Interface
- SNMP
- LLDP

---

2. Management

2.1.1 Management - IP Interfaces – Settings

IP (Internet Protocol Address) is short for IP Address. IP address is a unified address format provided by the IP protocol, which assigns a logical address to each network and host on the Internet to mask physical address differences.



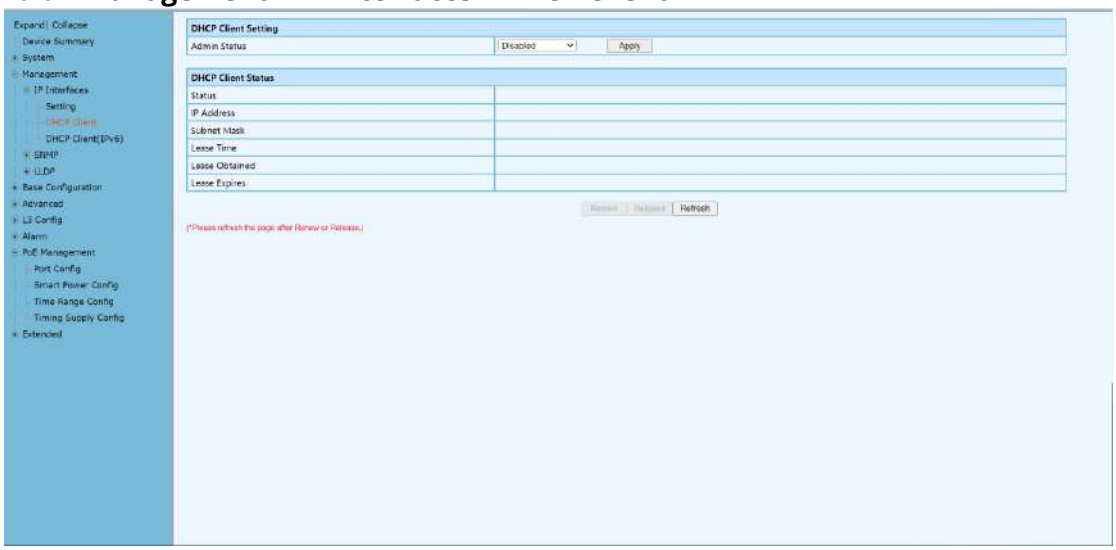
Configuration Steps

1. Select [Management / IP Interface / Setting] in the navigation bar to enter the IP interface [Setting].
2. All current IP interface and configuration information can be viewed in the IP interface [Setting],
3. To add a new IP interface, click [Add], then fill in the relevant configuration, and click [Apply],
4. To modify an IP interface, check the corresponding IP interface, click [modify], then modify the configuration, and click [Apply], the IP interface is shown.
5. To delete an IP interface, check the appropriate IP interface and click [Delete].

Setting		
Static IP Address		IPv4(A.B.C.D)
Subnet Mask		IPv4(A.B.C.D)
VLAN		<1-4094>
IPv6	Disabled	
IPv6 Address		IPv6(X::X:X:X/M)
	Apply Cancel	

Item	Description	Notes
Static IP Address	Static IPv4 address, the format is dotted decimal system, each interface IPv4 address can not be in the same network segment.	A.B.C.D
Mask	The mask of IPv4 address	A.B.C.D
VLAN	VLAN bound by assigned IP interface	<1 – 4094>
IPv6	Disabled/Enabled	Default:Disabled
IPv6 Address	X::X:X:X/M	

2.1.2 Management – IP Interfaces – DHCP Client



Configuration Step

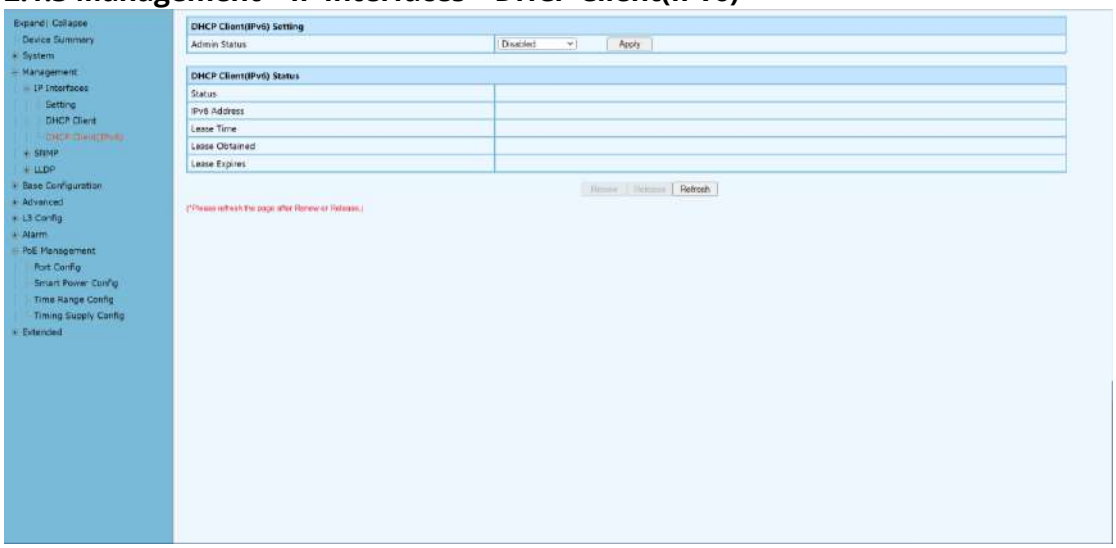
1,Select [Management / IP Interface / DHCP Client] in the navigation bar to enter the [DHCP Client] interface.

2,In the [DHCP Client] interface, you can view the current configuration information and DHCP client status.

Item	Description	Notes
Admin Status	Enable/Disable	Default: Disable
Renew	DHCP Client renew the configuration	
Release	DHCP Client release the current	

	configuration
Refresh	Refresh the configuration

2.1.3 Management – IP Interfaces – DHCP Client(IPv6)



Configuration Steps

1,Select [Management / IP Interface / DHCP Client(IPv6] in the navigation bar to enter the [DHCP Client(IPv6] interface.

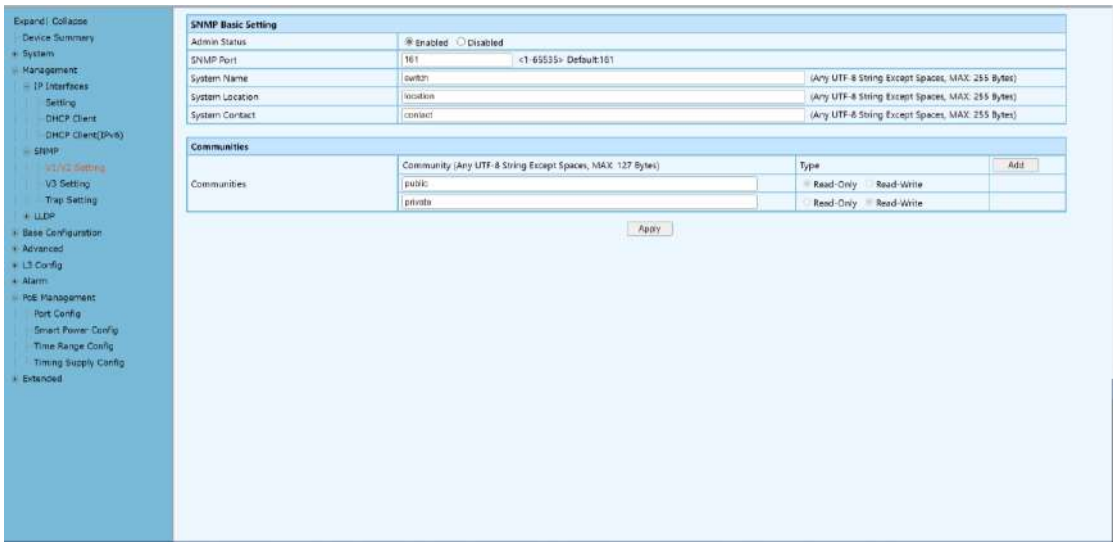
2,In the [DHCP Client(IPv6)] interface, you can view the current configuration information and DHCP client status.

Item	Description	Notes
Admin Status	Enable/Disable	Default: Disable
Renew	DHCP Client renew the configuration	
Release	DHCP Client release the current configuration	
Refresh	Refresh the configuration	

2.2 Management – SNMP

2.2.1 Management -SNMP - v1/v2 setting

The Simple Network Management Protocol (**SNMP**) is an Internet Standard protocol that is based on the manager/agent model with a simple request/response format. The network manager issues a request and the managed agents will send responses in return.



Configuration Steps

1.Select [Management / SNMP / V1/V2 Setting] in the navigation bar to enter the SNMP interface.

2.You can view the Base Setting of SNMP in the [SNMP Base Setting] interface.

3.To modify the Base Configuration, modify the corresponding configuration in the configuration box, and then click [Apply] to make effective.

4. If you want to add a group word, click [Add] and a group word is added to set the group word name and type.The system supports up to eight group characters, with the first and second being the default, so you can add up to six more.Click [Apply] to make effective.

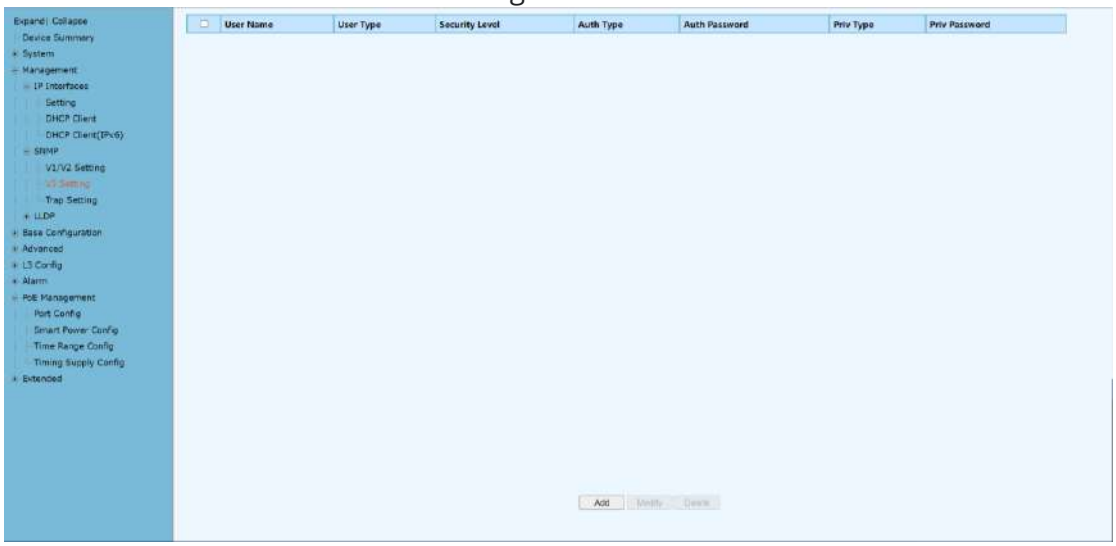
5. To delete a group word, click [Delete] on the right corresponding entry (the first and second are the system default, cannot be deleted), and click [Apply] to make effective.

Item	Description	Notes
Admin Status	Enable / Disable	Default: Enable
SNMP Port	SNMP port with Range <1-65535>	Default: 161
SNMP Name	System name, any legal character other than a space can be entered with a maximum length of 255	
System Location	System location information, any legal character other than a space can be entered with a maximum length of 255	
System Contact	System contact information, any legal character other than a space can be entered with a maximum length of 255	
Communities	**Name**: Any legal character other than a	

	space can be entered with a maximum length of 127 Type: Read and write **Note**: The system supports a maximum of 8 group characters and requires at least two group characters. The default two group characters can only change the group name, cannot change the type or delete. Click [Add] to add a group character, add a group character can change the name and type, and delete.

2.2.2 Management – SNMP – v3 setting

SNMPv3 addresses issues related to the large-scale deployment of SNMP, accounting, and fault management. Currently, SNMP is predominantly used for monitoring and performance management. SNMPv3 defines **a secure version of SNMP** and also facilitates remote configuration of the SNMP entities.



Configuration Steps

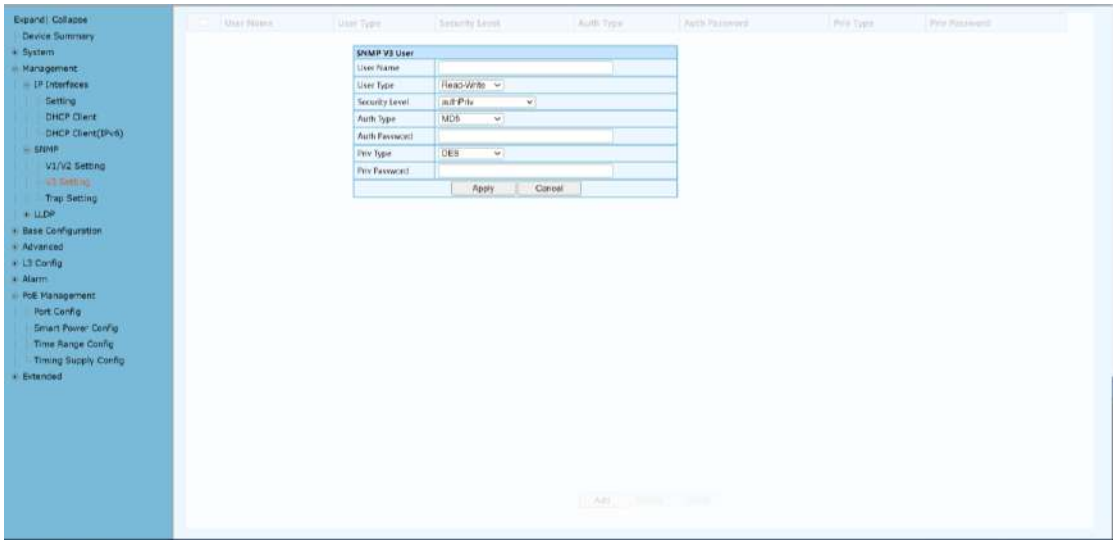
1.Select [Management / SNMP V3 Setting] in the navigation bar to enter the SNMP interface.

2.You can view the Base Setting of SNMP in the [SNMP Base Setting] interface.

3.To modify the Base Configuration, modify the corresponding configuration in the configuration box, and then click [Apply] to make effective.

4. If you want to add a group word, click [Add] and a group word is added to set the group word name and type.The system supports up to eight group characters, with the first and second being the default, so you can add up to six more.Click [Apply] to make effective.

5. To delete a group word, click [Delete] on the right corresponding entry (the first and second are the system default, cannot be deleted), and click [Apply] to make effective.



Item	Description
User Name	As Needed
User Type	Read-Write/ Read-Only
Security Level	**NoAuthNoPriv:**Communication without authentication and privacy. **AuthNoRriv:**Communication with authentication an witout privacy. **AuthRriv:**Communication with authentication and privacy.
Auth Type	**NoAuthNoPriv can't support** **MD5:** The MD5 message-digest algorithm is a cryptographically broken but still widely used hash function producing a 128-bit hash value. **SHA:** In cryptography, SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest – typically rendered as a hexadecimal number, 40 digits long.
Auth Password	As Needed
Priv Type	**Only supports AuthPriv level** **DES:** DES is based on the Feistel structure where the plaintext is divided into two halves. DES takes input as 64-bit plain text and 56-bit key to produce 64-bit Ciphertext. **AES:** AES algorithm takes 128-bit plaintext and 128-bit secret key which together forms a 128-bit block which is depicted as 4 X 4 square matrix.
Priv password	As Needed

2.2.3 Management – SNMP – Trap Setting

The Simple Network Management Protocol (SNMP) is an Internet-standard protocol used to manage devices on IP networks. The SNMP messages are used to inspect and communicate information about managed objects. The Trap message is one of the types of SNMP messages which are generated to report system events.

Configuration Steps

1. Select [Management / SNMP / Trap Setting] in the navigation bar and enter the SNMP [Trap Setting] interface.
2. The current trap configuration of SNMP can be viewed in the SNMP [Trap Setting] interface.
3. If you need to modify the Trap Setting, modify the corresponding configuration in the configuration box, and then click [Apply],
4. If you want to add a Trap server, click [Add] and the Trap server entry will occur.The system supports up to 4 groups of Trap servers, the first group is the default of the system and cannot be deleted, so you can add up to 3 groups of Trap servers, click [Apply] to make effective.
5. If you want to delete the Trap server, click [Delete] on the right of the corresponding entry (where group 1 is the default of the system and cannot be deleted), and click [Apply] to make effective.

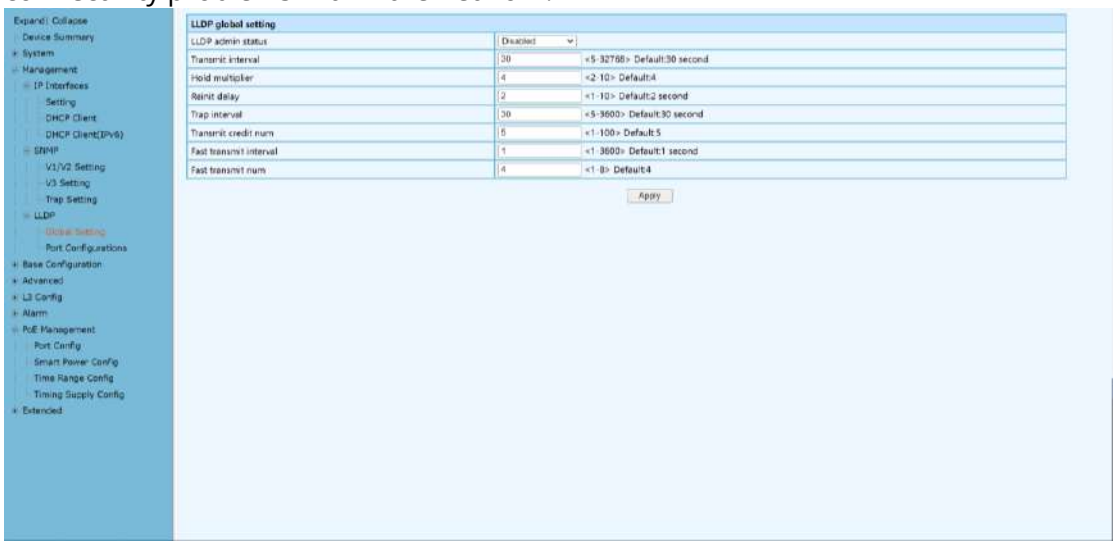
Item	Description	Notes
Admin Status	Enable / DIsable	Default: Enable
Send Authentication Failed Trap	**Enable**: Enable the Sending SNMP Authentication Failed Trap **Disable**: Disable the Sending SNMP Authentication Failed Trap	Default:Disable

Default Trap Community	Default trap Community characters, any legal character other than a space can be entered with a maximum length of 127
Trap Server	**Coummunity Characters**: Any legal character other than a space can be entered with a maximum length of 127 **Server IP Address**: The IP address of trap serve, IPv4, dot decimal format. **Server IP Port**: The IP port of trap serve, range <1-65535>, default 162 Note: The system supports up to 4 servers. Click the [Add]to add. The system default server number:1, **community character**: public, IP address: 192.168.1.166, IP port: 162. The default server cannot be deleted, but the added server can be deleted.

2.3 Management – LLDP

2.3.1 Management – LLDP - Global Setting

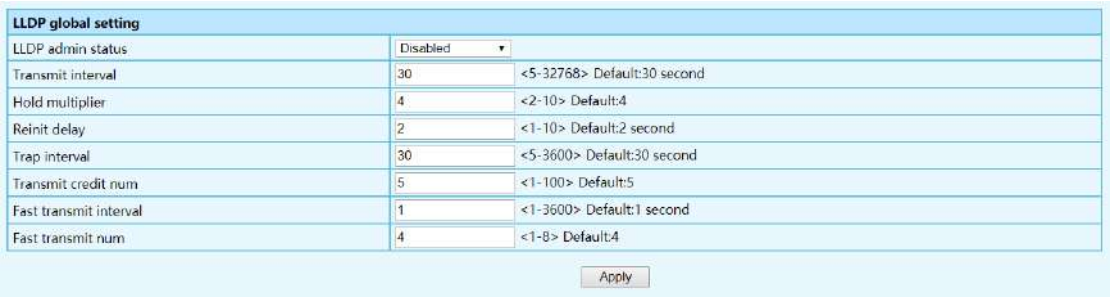
LLDP can be used in scenarios where you need to work between devices which are not Fiberroad proprietary and devices which are Fiberroad proprietary. You can use the LLDP protocol for troubleshooting purposes. The switch gives all the information about the current LLDP status of ports and you can use this information to fix connectivity problems within the network.



Configuration Steps

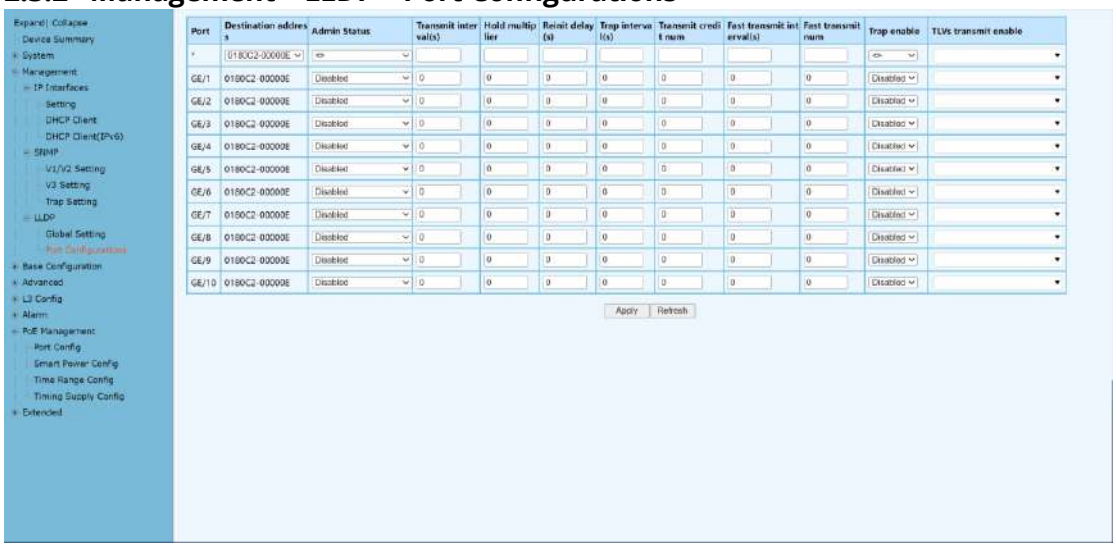
1. Select [Management / LLDP / Global Setting] in the navigation bar to enter the LLDP [Global Setting] interface.
2. The LLDP global configuration can be viewed in the LLDP [Global Setting] interface.

3. Modify the corresponding LLDP configuration in the LLDP [Global Setting] interface, and then click [Apply].



Item	Description	Notes
LLDP admin status	Enable / Disable	Default: Disable
Transmit interval	LLDP transmit interval range 5-32768	Default: 30
Hold multiplier	LLDP hold multiplier range 2-10	Default: 4
Reinit delay	LLDP reinit delay range 1-10	Default: 2
Trap interval	LLDP trap inerval range 5-3600	Default: 30
Transmit credit num	LLDP transmit credit num range 1-100	Default: 5
Fast transmit interval	LLDP fast transmit interval range 1-3600	Default: 1
Fast transmit num	LLDP fast transmit num range 1-8	Default: 4

2.3.2 Management – LLDP – Port Configurations



Configuration Steps,

1. Select [Management / LLDP / Port Configuration] in the navigation bar to enter the LLDP [Port Configuration] interface
2. The LLDP port corresponding configuration can be viewed in the LLDP [Port Configuration] interface
3. Choose the LLDP configuration of all ports corresponding to any destination address 0180C2-00000E, 0180C2-000003, 0180C2-000000 in the LLDP [Port Configuration] interface

4. To modify the LLDP configuration of a destination address port, click [Modify] after selecting the destination address, and enter the port configuration interface
4.Select or fill out the configuration items that need to be modified, and click [Apply] to make effective. There will be a corresponding prompt if the configuration item is incorrectly filled.

Item	Description	Notes
Destination Address	0180C2-00000E 0180C2-000003 0180C2-000000	

Remarks :
0x0180-C200-000E for LLDP frames destined for nearest bridge agents.
0x0180-C200-0000 for LLDP frames destined for nearest customer bridge agents.
0x0180-C200-0003 for LLDP frames destined for nearest non-TPMR bridge agents.

Item	Description	Notes
Admin Status	**Transmit Only**: Enable LLDP port transmit function **Receive Only**: Enable LLDP port receive function **Transmit and receive**: Enable LLDP port transmit and receive function **Disable**: Disable LLDP port transmit and receive function	Default: Disable
Transmit Interval(s)	Default: Use[Global Setting] transmit interval LLDP transmit interval range 5-32768	
Hold Multiplier	Default: Use[Global Setting] hold multiplier LLDP hold multiplier range 2-10	
Reinit Delay(s)	Default: Use[Global Setting] reinit delay LLDP reinit delay range 1-10	
Trap Interval(s)	Default: Use[Global Setting] trap interval LLDP trap inerval range 5-3600	
Transmist credit num	Default: Use[Global Setting] Transmist credit num LLDP transmit credit num range 1-100	
Fast transmit interval(s)	Default: Use[Global Setting] Fast transmit interval LLDP fast transmit interval range 1-3600	
Fast transmit num	Default: Use[Global Setting] Fast transmit num LLDP fast transmit num range 1-8	
Trap enable	Enable / Disable	
TLVs transmit enable	Port Description System Name System Description System Capabilities	

Chapter 3 Base Configuration

This chapter describes the port configuration in detail, including but not limit to the following:

- Ports
- VLAN
- QOS
- FDB

---

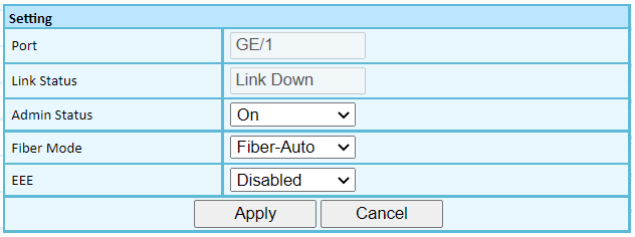
3 Base Configuration

3.1.1Base Configuration-Port-Status And Setting

	Running Status						Admin Status					
Port	Link Status	Port Type	Speed	Duplex	Rx Rate(bps)	Tx Rate(bps)	Admin Status	Speed	Duplex	Flow Control	EEE	Setting
GE/1	✔	Copper	100M	Full	0.00	32.41K	On	Auto	Auto	Off	Disabled	Modify
GE/2	✔	Copper	100M	Full	0.00	32.41K	On	Auto	Auto	Off	Disabled	Modify
GE/3	✖	Copper	10M	Half	0.00	0.00	On	Auto	Auto	Off	Disabled	Modify
GE/4	✔	Copper	100M	Full	0.00	32.41K	On	Auto	Auto	Off	Disabled	Modify
GE/5	✖	Copper	10M	Half	0.00	0.00	On	Auto	Auto	Off	Disabled	Modify
GE/6	✔	Copper	100M	Full	0.00	32.24K	On	Auto	Auto	Off	Disabled	Modify
GE/7	✔	Copper	1000M	Full	56.35K	19.94K	On	Auto	Auto	Off	Disabled	Modify
GE/8	✔	Copper	100M	Full	0.00	32.24K	On	Auto	Auto	Off	Disabled	Modify
GE/9	✖	Fiber	10M	Half	0.00	0.00	On	Fiber-Auto	Full	Off	Disabled	Modify
GE/10	✖	Fiber	10M	Half	0.00	0.00	On	Fiber-Auto	Full	Off	Disabled	Modify

Configuration Steps

1. Select [Bae Configuration / Ports / Status and Setting] in the navigation bar to enter the [Status and Setting] interface.
2. The Status and Settings interface shows the operating status and configuration information for each port.



3. If you need to modify the configuration of a port, just click the [Modify] on the right side corresponding entry. to enter the modification interface and modify the corresponding configuration item. Click the [Apply] to complete the modification, and click the [Cancel] to cancel the modification.

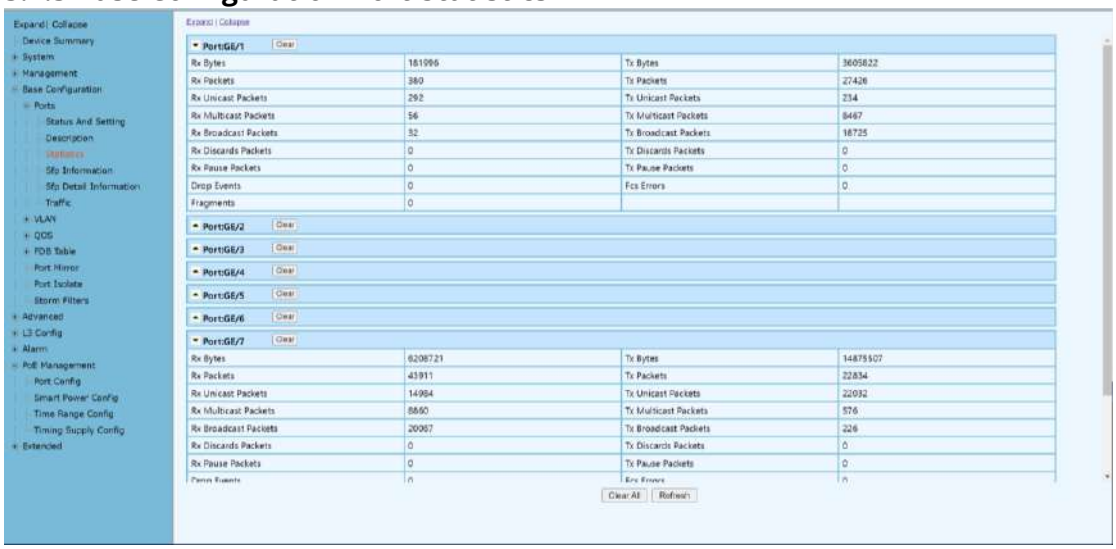
Item	Description	Notes
Port	The name and number of the port	
Link Status	Indicates that the port is linked up Indicates that the port is linked down	
Port Type	Copper or Fiber Port	
Rate	The port working speed, unconnected port is always displayed as 10M	
Duplex	The port working duplex mode, the unconnected port always shows half duplex	

Item	Description	Notes
Port		Read Only
Link Status		Read Only
Admin Status	ON/OFF	Default: ON
Fiber Mode	Fiber-Auto Fiber-100M Fiber-1000M	Default: Fiber-Auto
EEE	Energy Efficient Ethernet Enabled / Disabled	Default: Disabled

Remarks: Energy Efficient Ethernet (EEE) is an IEEE 802.3az standard that is designed to reduce power consumption in ethernet network during idle periods.

3.1.2 Base Configuration-Port-Description

3.1.3 Base Configuration-Port-Statistics



Configuration Steps

1. Select [Base Configuration / Ports / Statistics] to enter the port [Statistics] page
2. The [Statistics] shows each port statistical information. You can expand corresponding port statistics by clicking flag on the left of port entry, and click cleared button on the right to clear the statistics of the port.
3. Click the [Refresh] to update the statistics of all ports. Click [Clear All] to clear the statistics for all ports.

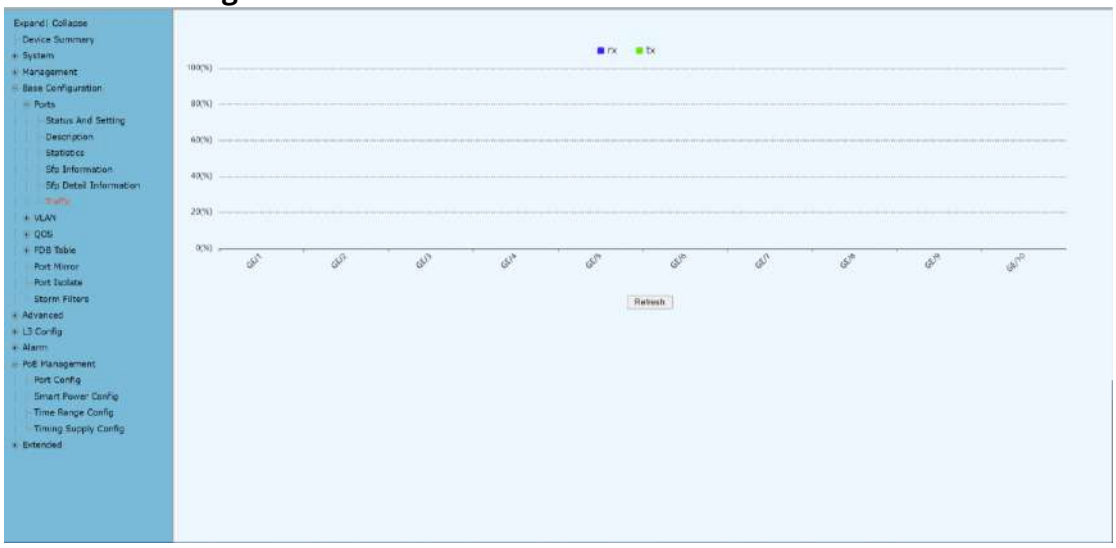
Item	Description	Notes
Rx / Tx Packets	Total received / sent packets	
Rx / Tx Unicast Packets	Total received / sent unicast packets	
Rx / Tx Multicast Packets	Total received / sent multicast packets	
Rx / Tx Broadcast Packets	Total received / sent broadcast packets	
Rx / Tx Discards Packets	Total received / sent discarded packets	
Rx / Tx Pause Packets	Total received / sent flow control packets	
Drop Events	Drop messages (interval sampling)	
FCS Errors	FCS error packet	
Fragments	Fragment packets (less than 64 bytes)	

3.1.4 Base Configuration-Port-SFP Information

Item	Description	Notes
Port	The name of information	Read Only
Status	Removed / Inserted	Read Only
Wavelength	Operating Wavelength	Read Only
Distance(m)	SFP effective transmission distance	Unit: Meter
Bit Rate	N/A / Bit Rata	Unit: MBd
Ethernet Codes	N/A / Fiber-100M / Fiber-1000M	Read Only
DDM	N/A / Supported	Read Only
Calibrated	N/A / Internally / Externally	Read Only
Tx Power(dBm)	Transmitter optical power	Unit: dBm
Rx Power(dBm)	Receiver optical power	Unit: dBm
Temperature(℃)	SFP operating temperature	Unit: ℃
Voltage(V)	SFP Voltage	Unit: V
Crrent(mA)	SFP Current	Unit: mA

3.1.5 Base Configuration-Port-SFP Detail Information

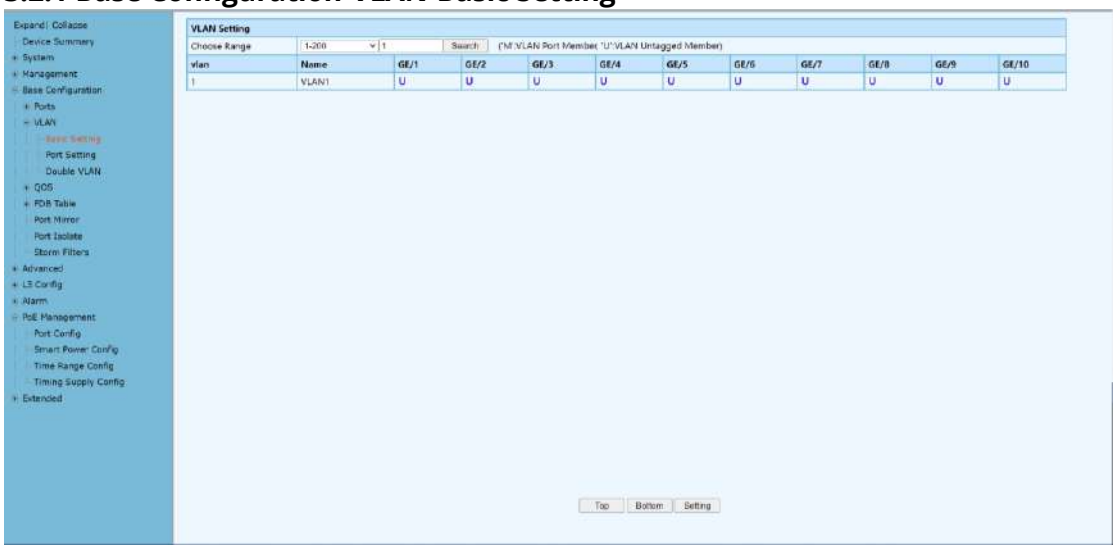
3.1.6 Base Configuration-Port-Traffic



Remarks: Real-time traffic statistics of each ports.

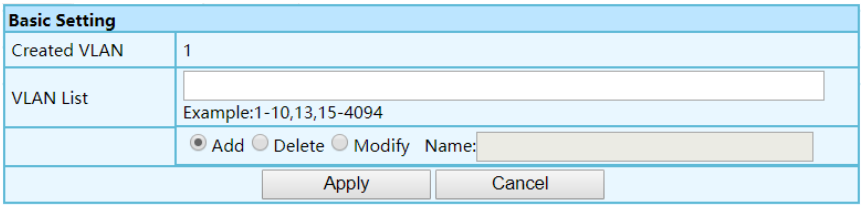
3.2 Base Configuration - VLAN

3.2.1 Base Configuration-VLAN-Basic Setting



Configuration Steps

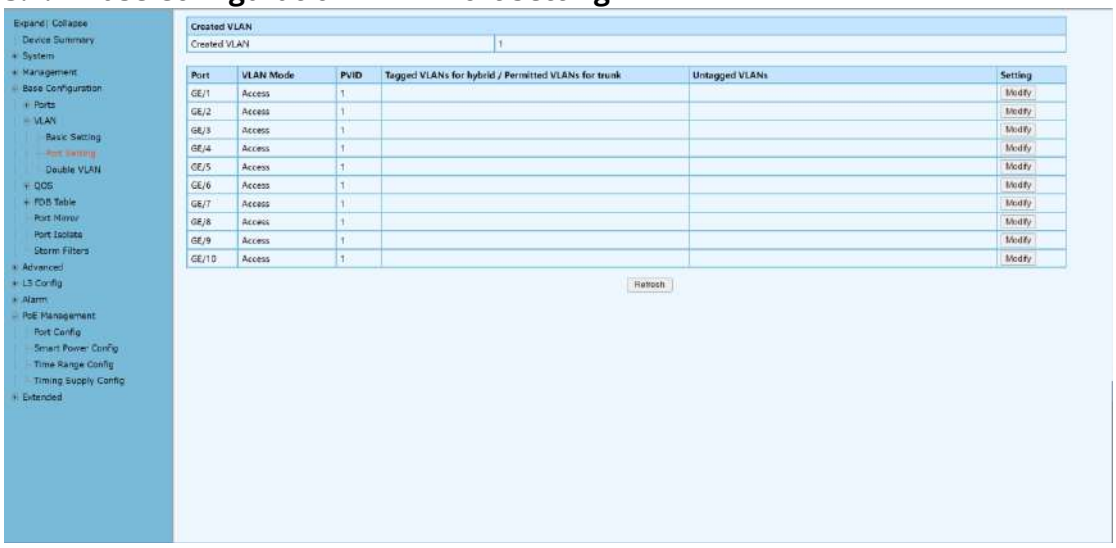
1. Select **[**Base Configuration / VLAN / Basic Setting**]** to enter the VLAN **[**Basic Setting**]** interface.
2. On **[**Basic Setting**]** interface, you can view the related configuration information of each VLAN. If you want to find information about a VLAN ID, select the range of the VLAN ID in the drop-down box, enter the specified VLAN ID in the input box, and click **[**Search**]**.
3. To add, modify, or delete VLANs, click **[**Setting**]**. Enter the VLAN to be added, modified, or deleted in the <VLAN list> box on setup interface. Then select Add, Modify, or Delete. Click **[**Apply**]**. The setting and modification options can only modify the VLAN name



Item	Description	Notes
Choose Range		
Search	To search for a VLAN ID 1. Select the interval where the VLAN to be searched in the interval selection box; 2. If you enter a specific VLAN ID in the input box, for example 11, the information bar with the VLAN number 11 turns yellow; 3. If there is no such VLAN, the corresponding information is prompted.	
Top	Display the first page of VLAN information	
Bottom	Display the last page of VLAN information	

Item	Description	Notes
VLAN List Box	It is to input the VLAN list to be set and supports multi-VLAN batch input, such as 1,2,3,4-10	
Add	To add the VLAN that is entered in the VLAN list box. VLAN 1 is the default VLAN. It already exists and does not need to be created	
Delete	To delete the VLAN input in the VLAN list box. VLAN 1 is the default VLAN and cannot be deleted.	
Modify	To modify the VLAN input in the VLAN list box. The VLAN name can be modified. The new name needs to be entered in the name box.	

3.2.2 Base Configuration-VLAN-Port Setting



Configuration Steps

1. Select [Base Configuration / VLAN / Port Setting] to enter the VLAN Port Setting interface.
2. On the [Port Setting] interface, you can view the VLAN related configuration information of each port.
3. To modify the VLAN configuration of a port, click [Modify] in the corresponding port display field to enter the port setting interface,
4. Select or fill in the configuration items that need to be modified and click [Apply]. There will be prompts if the configuration item is filled in incorrectly.

Item	Description	Notes

Port	Port Name Information	
VLAN Mode	Port VLAN Mode **Access**: Access mode **Trunk**: Trunk mode **Hybrid**: Hybrid mode	
PVID	Port PVID	<1-4094>
Tagged VLAN	List of VLANs allowed to pass through the port. It supports batch input of multiple VLANs. For example: '1,2,3,4-10'; Add: Add the tagged VLAN to the port as the input VLAN; Delete: Delete the VLAN from the tagged VLAN of the port; Replace: Replace the original tagged VLAN of the port with the input VLAN; All created VLANs: All the created VLANs are tagged VLANs of the port. Even if they are created later, they will be automatically added to the tagged VLAN of the port.	
Untagged VLAN	Port untagged VLAN list, supports multi-VLAN batch input, such as: "1,2,3,4-10"; Add: Add the incoming VLAN to the untagged VLAN of the port; Delete: Delete the incoming VLAN from the untagged VLAN of the port. Replace: Replace the original untagged VLAN of the port with the input VLAN.	

3.2.3 Base Configuration-VLAN-Double VLAN

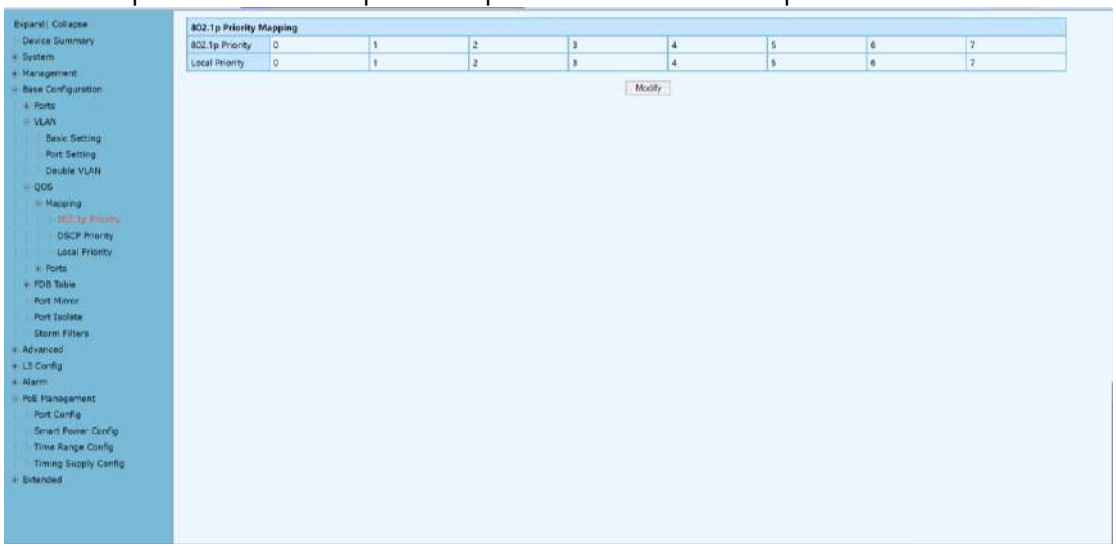
Item	Description	Notes

Port	Port Name Information	Read Only
Mode	Enabled / Disabled	Default: Disabled
Outer PVID	1, 33-46	
Ingress Mode	All / Tagged / Untagged	Default : All
Egress Mode	Tagged / Untagged	Default: Untagged

3.3 Base Configuration-QOS

3.3.1 Base Configuration-QoS- Mapping -802.1p Priority

The 802.1p determines the packet's queue in the outbound port on the switch.



Configuration Steps

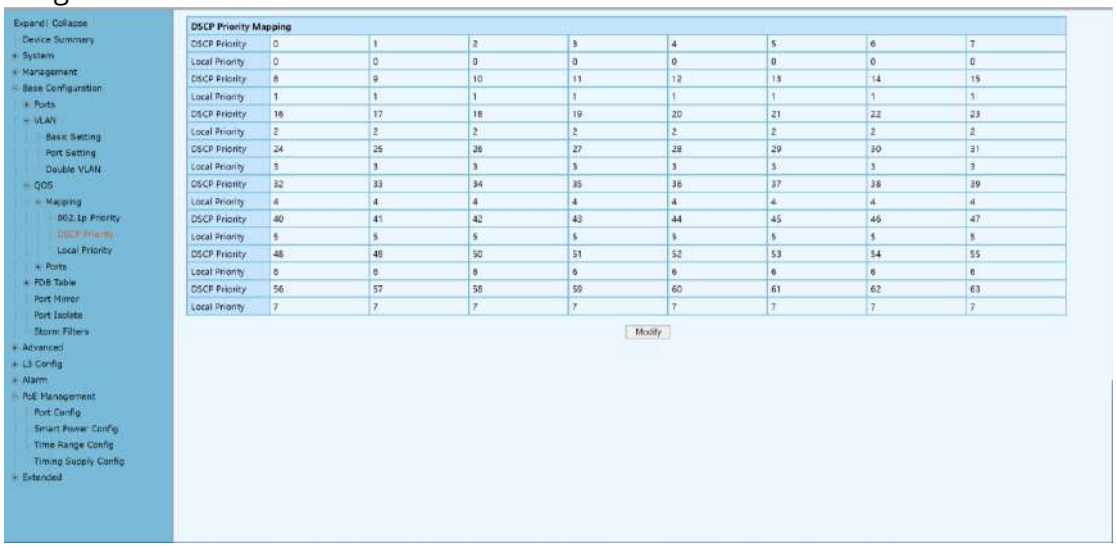
1. Select [Base Configuration / QOS / Mapping / 802.1p Priority] in the navigation bar to enter the QOS [802.1p Priority] interface.
2. On the QOS [802.1p Priority] interface, you can view the mapping from 802.1p priorities to local priorities.

3. To modify the mapping relationship, click [Modify] and select the mapped local priority for the corresponding 802.1p priority in drop-down list box.

Item	Description	Notes
Modify	Modify the mapping between 802.1p priorities and local priorities	

3.3.2 Base Configuration-QoS- Mapping – DSCP Priority

DSCP is a 6-bit packet header value used for traffic classification and priority assignment.



DSCP Priority	0	1	2	3	4	5	6	7
Local Priority	0	0	0	0	0	0	0	0
DSCP Priority	8	9	10	11	12	13	14	15
Local Priority	1	1	1	1	1	1	1	1
DSCP Priority	16	17	18	19	20	21	22	23
Local Priority	2	2	2	2	2	2	2	2
DSCP Priority	24	25	26	27	28	29	30	31
Local Priority	3	3	3	3	3	3	3	3
DSCP Priority	32	33	34	35	36	37	38	39
Local Priority	4	4	4	4	4	4	4	4
DSCP Priority	40	41	42	43	44	45	46	47
Local Priority	5	5	5	5	5	5	5	5
DSCP Priority	48	49	50	51	52	53	54	55
Local Priority	6	6	6	6	6	6	6	6
DSCP Priority	56	57	58	59	60	61	62	63
Local Priority	7	7	7	7	7	7	7	7

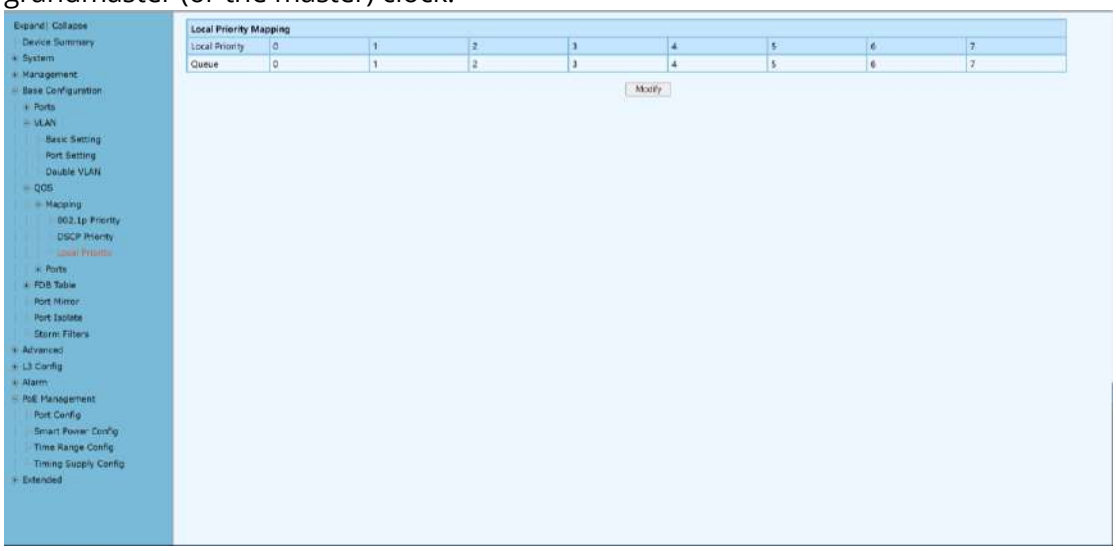
Configuration Steps

1. Select [Base Configuration / QOS / Mapping / DSCP Priority] in the navigation bar to enter the QOS DSCP Priority Mapping interface.
2. On the QOS [DSCP Priority] interface, you can view the mapping from DSCP priorities to local priorities.
3. To modify the mapping relationship, click [Modify] and select the mapped local priority for the corresponding DSCP priority in drop-down list box

Item	Description	Notes
Modify	Modify the mapping between DSCP priorities and local priorities	

3.3.3 Base Configuration-QoS- Mapping – Local Priority

The local priority is assigned to the local clock and is used if needed when the data associated with the local clock is compared with data on another potential grandmaster (or the master) clock.



Configuration Steps

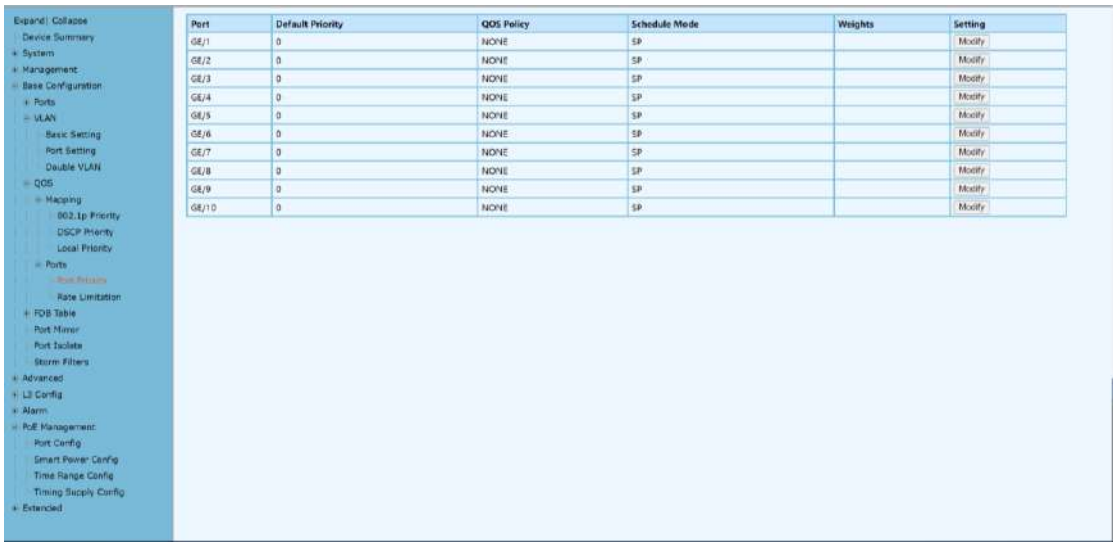
1. Select [Base Configuration / QOS / Mapping / Local Priority] in the navigation bar to enter the QOS Local Mapping.
2. You can view the mapping from the local priority to the egress queue on the QOS [Local Priority] interface.
3. To modify the mapping relationship, click [Modify] and select the mapped egress queue for the corresponding local priority in drop-down list box.

Item	Description	Notes
Modify	Modify the mapping relationship between the local precedence and the egress queue	

3.4 Base Configuration-QoS- Ports

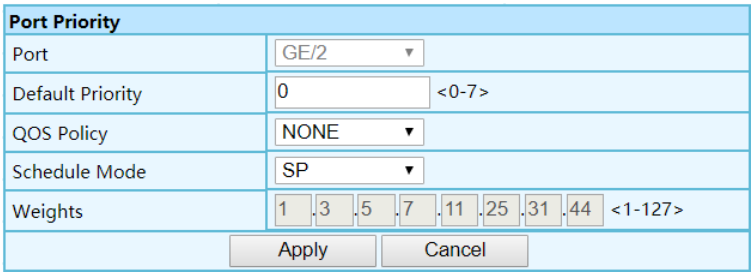
3.4.1 Base Configuration-QoS- Ports-Port Priority

Quality of Service (QoS) Port-based settings allow you to configure each port on the device for QoS Local Area Network (LAN) settings using different priority levels for network traffic. This allows the router to prioritize and handle traffic differently on each port so you may get the best performance while connecting to a range of devices.



Configuration Steps

1. Select [Base Configuration / QOS / Ports / Port Priority] in the navigation bar to enter the QOS [Port Priority] interface.
2. The QOS related configuration of the port can be viewed on the QOS [Port Priority] interface.
3. To modify the QOS configuration of a port, click [Modify] on the corresponding port display to enter the port setting interface, as shown in Figure 5.4.
4. Select or fill in the configuration items that need to be modified and click [Apply] to confirm. There will be prompts if the configuration item is filled in incorrectly.

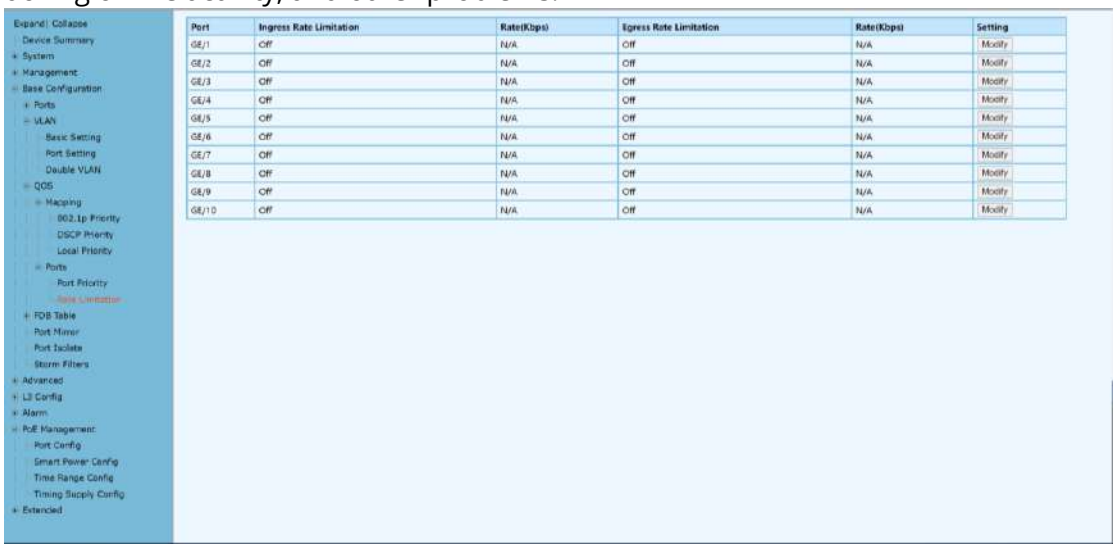


Item	Description	Notes
Port	Port name information	
Default Priority	The port default with priority	Range <0-7>
QoS Policy	NONE: indicates no policy. The port does not have a policy by default. COS: COS priority policy DSCP: DSCP priority policy OS-DSCP: COS-DSCP priority policy	
Scheduling	SP: Strict Priority scheduling strategy	

Mode	WRR: Weighted Round Robin scheduling strategy WFQ: Weighted Fair Queue scheduling strategy
Weights	If the selected scheduling mode is WRR or WFQ, you need to configure the weight of each queue, total 8 queues. To set 8 weights, the weight of all queues must be 127.

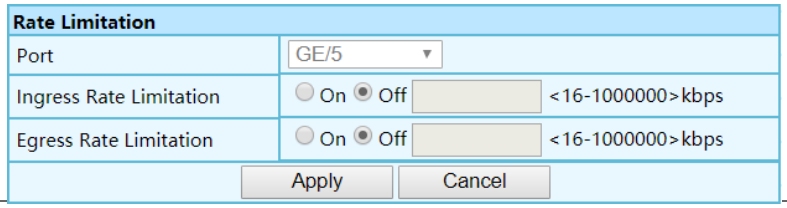
3.4.2 Base Configuration-QoS- Ports-Rate Limitation

Port-based rate limiting allows you to limit the speed at which network traffic is sent or received by a device that is connected to a port on your switch. Unlike 802.1p Quality of Service (QoS), port-based rate limiting does not prioritize information based on type. Rate limiting simply means that the switch will slow down traffic on a port to keep it from exceeding the limit that you set. If you set the rate limit on a port too low, you might see degraded video stream quality, sluggish response times during online activity, and other problems.



Configuration Steps

1. Select [Base Configuration / QOS / Port / Rate Limitation] in the navigation bar to enter the QOS [Rate Limitation] interface.
2. On the QOS [Rate Limitation] interface, you can view the related configuration of the port's speed limit.
3. To modify the port's speed limit configuration, click [Modify] in the port display column to enter the Rate Limitation setting interface.
4. Select or fill in the configuration items that need to be modified and click [Apply] to confirm. There will be prompts if the configuration item is filled in incorrectly.

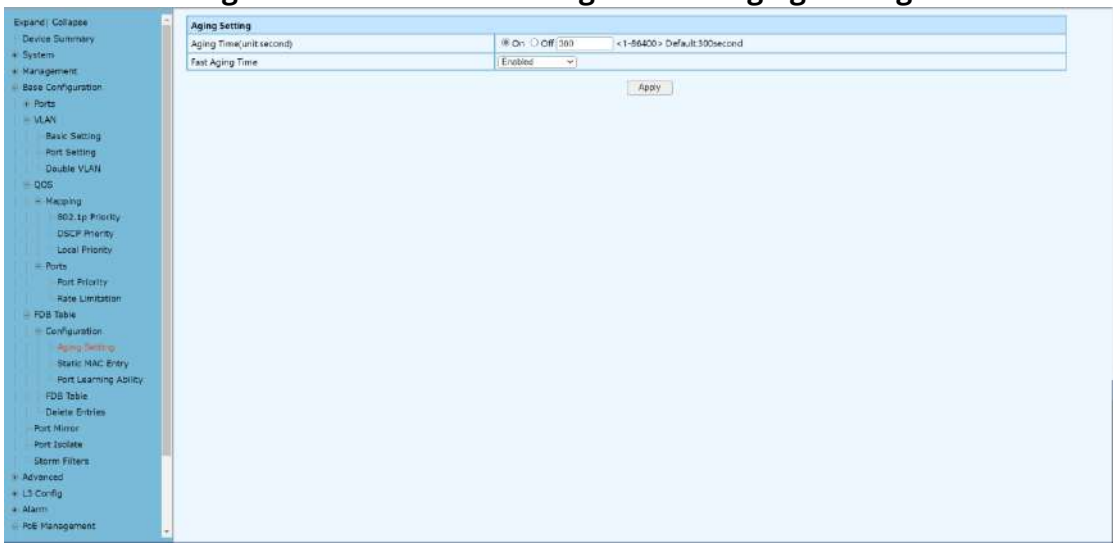


Item	Description	Notes

Port	Port name information
Ingress Rate Limitation	Set the port's entry speed limit: **On:** Enables the port to limit the rate of ingress. The rate limit ranges from <16-1000000> **OFF:** Close the port's ingress rate limit
Egress Rate Limitation	Set the port's output speed limit: **On:** Enables the port to limit the rate of egress. The rate limit ranges from <16-1000000> **OFF:** Close the port's egress rate limit

3.5 Base Configuration-FDB Table

3.5.1 Base Configuration-FDB Table- Configuration – Aging Setting

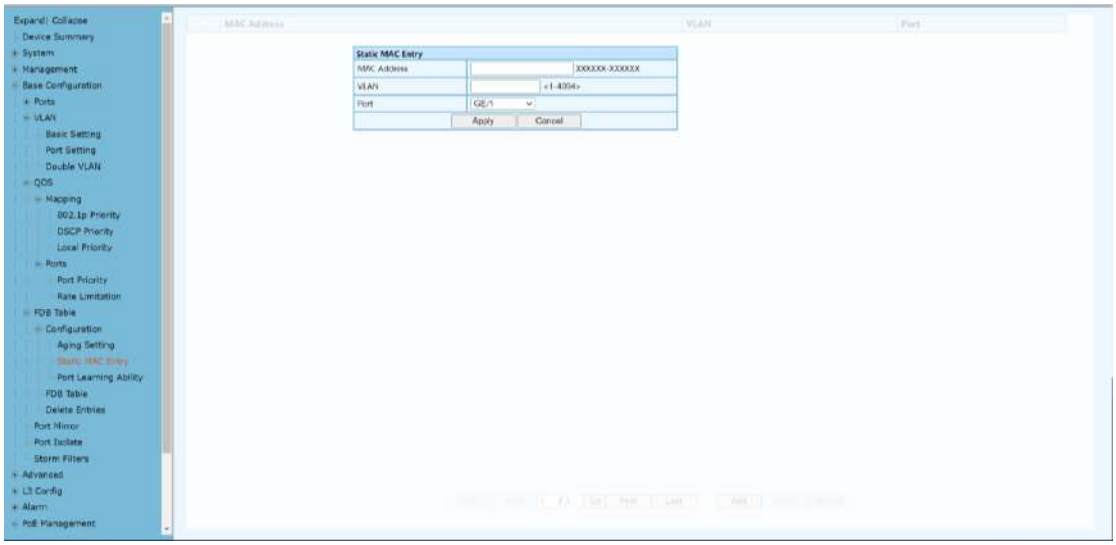


Configuration Steps

1. Select [Base Configuration / FDB Table / Configuration / Aging Time] to enter the [Aging Time] interface.
2. The aging time related configuration of the FDB Table can be viewed in the [Aging Time] interface.
3. If you need to modify the aging time configuration of the FDB Table, you can modify the corresponding configuration in the aging time configuration box and click [Apply].

Item	Description	Notes
Aging Time	The FDB Table aging time can be configured via the radio button. **Enabled**: The aging time is on. Range 1-86400 seconds, default value 300 seconds. **Disabled:** The FDB Table never aging, but the system resetting could clear the dynamic forwarding entries. Note: Default with Enable, 300 seconds.	

3.5.2 Base Configuration-FDB Table- Configuration – Static Mac Entry

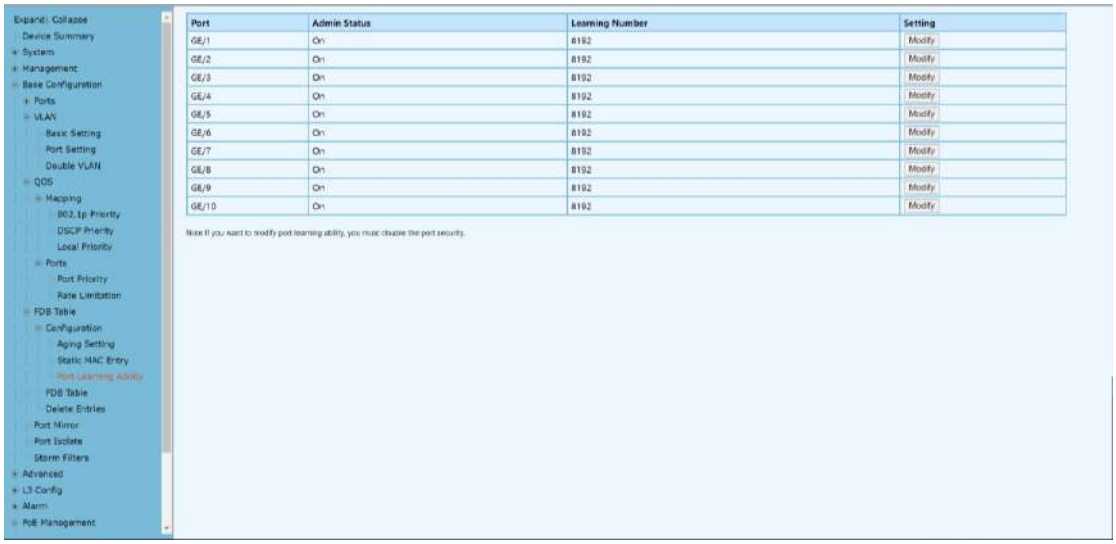


Configuration Steps

1. Select [Base Configuration / FDB Table / Configuration / Static MAC Entry] to enter the [Static MAC Entry] configuration interface.
2. On FDB Table [Static MAC Entry] interface, you can view the static MAC related configuration information of FDB Table,
3. If add a new static MAC address, click [Add] to enter the Static MAC configuration interface. Fill in the corresponding configuration items and click [Apply] to complete the addition. There will be prompts if the configuration item is filled in incorrectly.
4. If modify the static MAC address, select the corresponding static MAC address and click [Modify] to enter [Static MAC Entry] interface. To modify the corresponding configuration item, click [Apply] to complete the modification. There will be prompts if the configuration item is filled in incorrectly.
5. If delete a static MAC, select the corresponding static MAC and click [Delete] to delete the static MAC.

Item	Description	Notes
MAC Address	A valid unicast MAC address, format XXXXXX - XXXXXX	
VLAN	A valid VLAN ID, rang 1-4094	
Port	Select a specified port	

3.5.3 Base Configuration-FDB Table- Configuration – Port Learning Ability



Configuration Steps

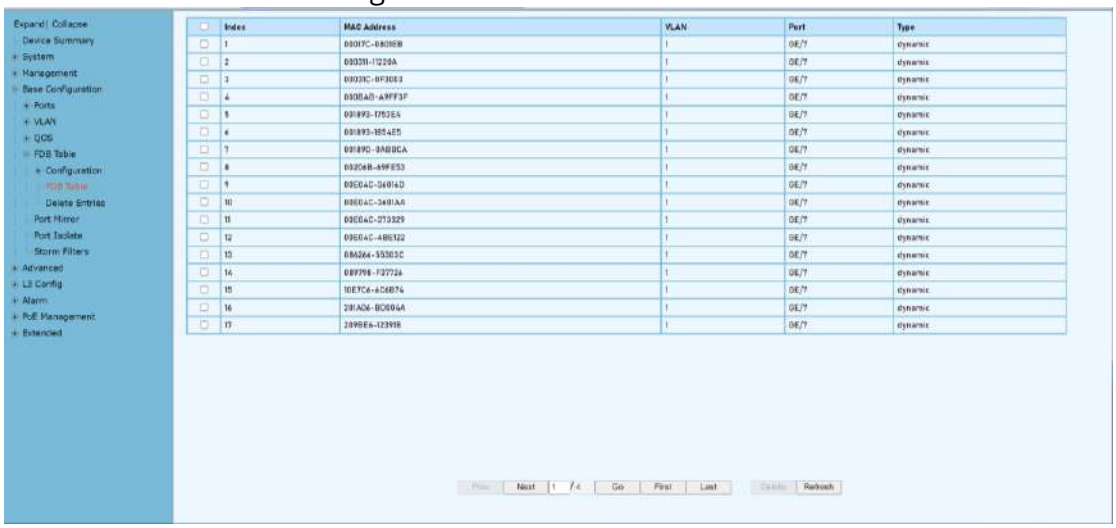
1. Select [Base Configuration / FDB Table / Configuration / Port Learning Ability] to enter the [Port Learning Ability] interface.
2. On the FDB Table [Port Learning Ability] interface, you can view the Port Learning Ability related configuration information of FDB Table.
3. To modify the Port Learning Ability configuration, click [Modify] in the corresponding port column to enter the port configuration interface.
4. Select or fill in the configuration items that need to be modified and click [Apply]. There will be prompts if the configuration item is filled in incorrectly.

Item	Description	Notes
Port	Port name, selected modified port	
Learning	Functional configuration of port learning, configured via radio buttons. ON: The Port Learning Ability is on. IS3000 / IS2000 series range is 1-8192; OFF: Closes the Port Learning Ability. Note: The default is Enable with value 8192.	

Remarks: The number of address learning is shared by all ports

3.5.4 Base Configuration-FDB Table- FDB Table

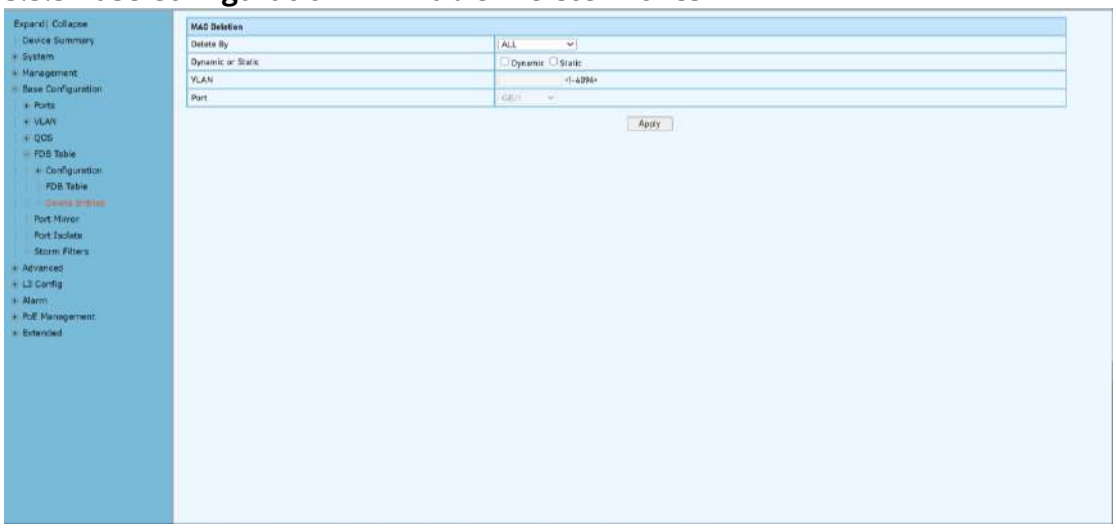
The FDB (forwarding database) table is used by a Layer 2 device (switch/bridge) to store the MAC addresses that have been learned and which ports that MAC address was learned on. The MAC addresses are learned through transparent bridging on switches and dedicated bridges.



Configuration Steps

1. Select [Base Configuration / FDB Table / FDB Table] to enter [FDB Table] interface.
2. On the FDB Table interface, you can view the FDB Table information.
3. If delete a forwarding entry, select the corresponding forwarding entry or select it all and click [Delete] to delete the entry.

3.5.5 Base Configuration-FDB Table- Delete Entries



Configuration Steps

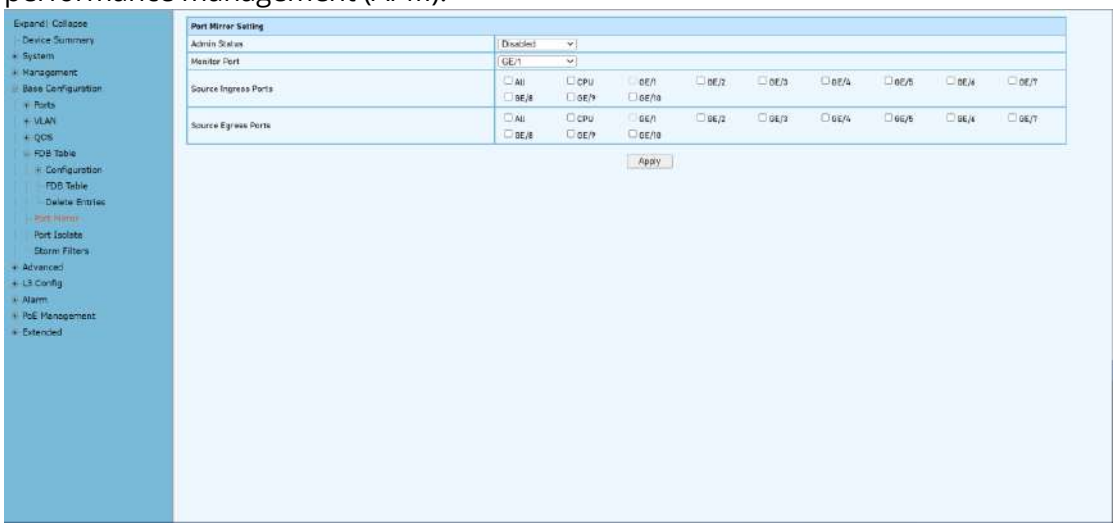
1. Select [Base Configuration / FDB Table / Delete] to enter the [Delete] interface.
2. If delete related entries in the FDB Table in batches, select the corresponding remove condition in the MAC address deletion column, and then click [Apply].

Item	Description	Notes
Delete By	All: Deletes all FDB Table entries. VLAN: Specifies the VLAN ID to delete FDB Table entries. Port: Specify the port number to delete the FDB	

	Table entries.
Dynamic or static	Dynamic: Delete the dynamic FDB Table entries that have been learned. Static: Delete manually added static FDB Table entries.
VLAN	Delete the forwarding entry of the specified VLAN. The range is 1-4094.
Port	Delete the forwarding entry of the specified port.

3.5.6 Base Configuration-FDB Table- Port Mirror

Port mirroring is used on a network switch to send a copy of network packets seen on one switch port (or an entire VLAN) to a network monitoring connection on another switch port. This is commonly used for network appliances that require monitoring of network traffic such as an intrusion detection system, passive probe or real user monitoring (RUM) technology that is used to support application performance management (APM).



Configuration Steps

1.Select [Base Configuration / Port Mirror] in the navigation bar to enter the [Port Mirror] configuration interface

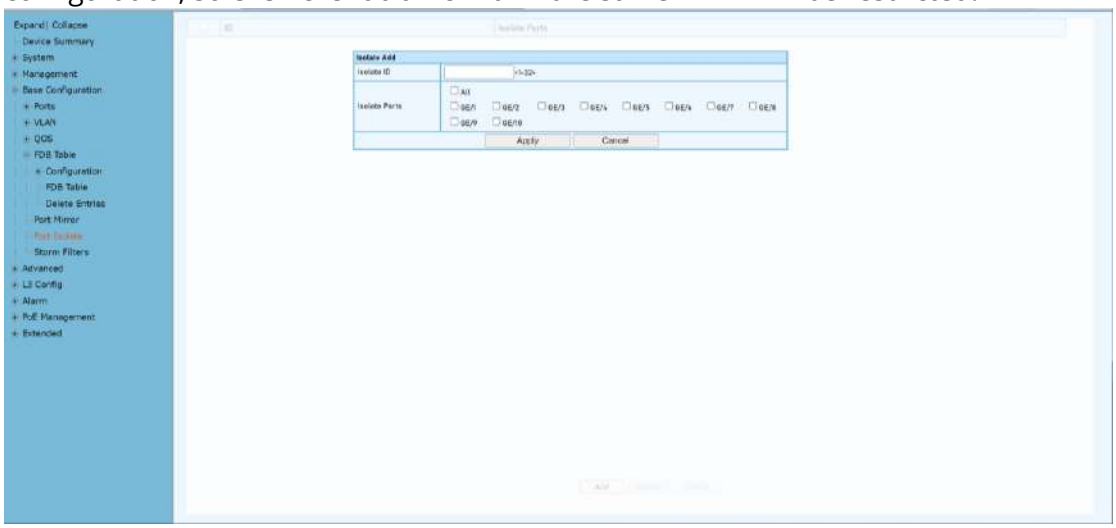
2.Modify the port mirroring configuration information. Pull down and select to disable or enable mirroring, select the mirroring destination port, check the ingress port and egress port, the ingress or egress cannot contain the destination port, and click [apply] to submit the modification

Item	Description	Notes
Admin Status	Select whether to enable port mirroring	
Monitor Port	Select the destination port for port mirroring via drop-down box	
Source Ingress Ports	Select the source port list in the ingress direction. It can be selected with the check button. (The source port list cannot contain the destination port)	

Source Egress Ports	Select the source port list in the egress direction. It can be selected with the check button. (The source port list cannot contain the destination port)

3.5.7 Base Configuration-FDB Table- Port Isolate

Port isolation allows a network administrator to prevent traffic from being sent between specific ports. This can be configured in addition to an existing VLAN configuration, so even client traffic within the same VLAN will be restricted**.**



Configuration Steps

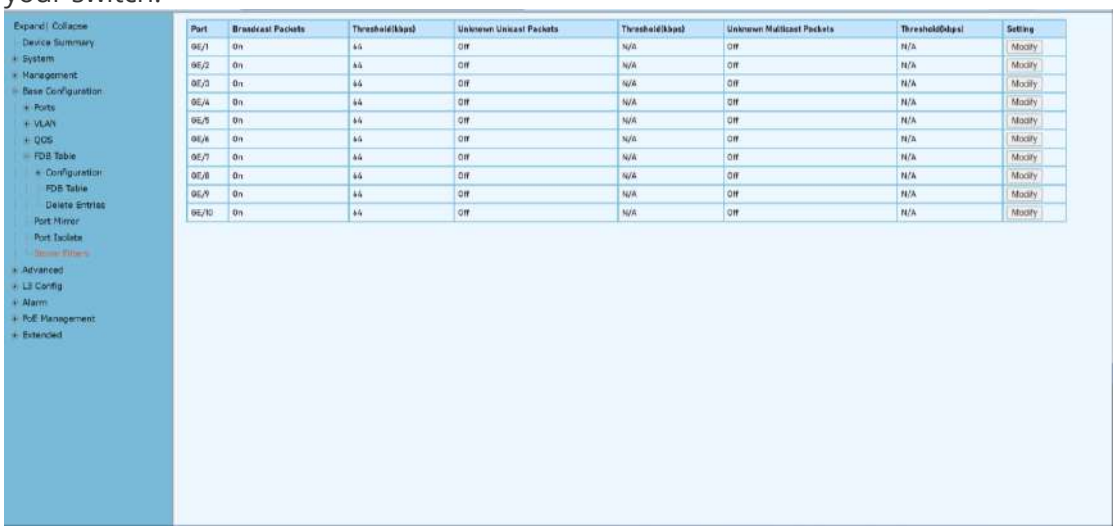
1.Select [Base Configuration / Port Isolate] in the navigation bar to enter the [Port Isolate] configuration interface

2.Modify the port isolate configuration information. Pull down and select to Add or Modify, enter Isolate ID, select a Isolate Ports, and click [apply] to submit the modification.

3.5.8 Base Configuration-FDB Table- Storm Filters

Broadcast filtering helps to prevent a broadcast storm, which is a massive

transmission of broadcast packets being sent by a single port to every port on a local area network (LAN). Forwarded message responses can overload network resources, slow regular network traffic, or cause the network to time out. Broadcast filtering lets you limit the number of broadcast packets that each port sends. When you turn on broadcast filtering, you have the option to set the storm control rate on each port of your switch.



Configuration Steps

1. Select [Base Configuration / Storm Filters] in the navigation bar to enter [Storm Filters] configuration interface.
2. The Storm Filtering interface displays broadcast storm filtering configuration information for each port.
3. To modify the port storm filtering configuration information, click the [Modify] to enter the [Storm Filters] modification interface, as shown in Figure 13.2. Enter valid configuration parameters and click [Apply] to submit the changes. Click [Cancel] to cancel the modification

Item	Description	Notes
Port	Modify the configured port	
Broadcast Packets	**ON**- If you choose to enable, enter the corresponding rate suppression value, <16-1000000>, and enter 16, unit is kbps **OFF**	
Unknown Unicast Packets	**On** - If you choose to enable, enter the corresponding rate suppression value, <16-1000000>, enter 16, unit is kbps **OFF**	
Unknown Multicast Packets	**On** - If you choose to enable, enter the corresponding rate suppression value, <16-1000000>, enter 16, unit is kbps **OFF**	

Chapter 4 Advanced Configurations

This chapter describes the advance configuration in detail, including but not limit to the following:

- ACL
- DHCP snooping
- Multicast
- GMRP
- GVRP
- EPRS

---

4. Advanced Configuration

4.1 Advanced Configuration – Ports – Ports Security

Port security is a layer-2 traffic control feature on Fiberroad Industrial switches. It enables an administrator configure individual switch ports to allow only a specified number of source MAC addresses ingressing the port.

Configuration Steps

1.Select [Advance] in the navigation bar to enter the [Port Security] configuration interface

2.Modify the Port Security configuration information. Pull down and select to disabled or enabled mode, select the action, enter the number of MAC addresses to be secured on a port, and click [apply] to submit the modification.

Item	Description	Notes
Mode	Enable port security on the desired ports. If desired, specify the secure MAC address.	
Action	Trap/Shundown/Trap&Shundown/Drop/Trap&Drop	
MAC 1/MAC 2/MAC 3	You can add MAC address to the list of secure address	

Remarks: If you want to modify the mode, you must enable the port learning ability and set the learning number to 8192.

4.2 Advanced Configuration – ACL

4.2.1 Advanced Configuration – ACL – ACL Group Setting

The Groups for ACLs feature lets you classify users, devices, or protocols into groups and apply those groups to access control lists (ACLs) to create access control policies for those groups.

Configuration Step

1. Select [Advanced / ACL / ACL Group Setting] in the navigation bar to enter the ACL interface.
2. The ACL information will be added in [ACL Group Setting] interface.
3. Add an ACL Group: click [Add] to enter [ACL Group Setting] interface, An ordinal number (0-3999) is assigned to the group. Set a name for the group, not repeatable. Then select the port and bind to the group. It is not workable if port binding not done. Click [Apply] to complete the configuration.
4. Modify an ACL Group Configuration: select an ACL group and click [Modify] to enter the [ACL Group Setting] interface. Fill in the required configuration items, and click [Apply] to complete the configuration.
5. Delete an ACL Group Configuration: select an ACL group and click [Delete] to delete the configuration.

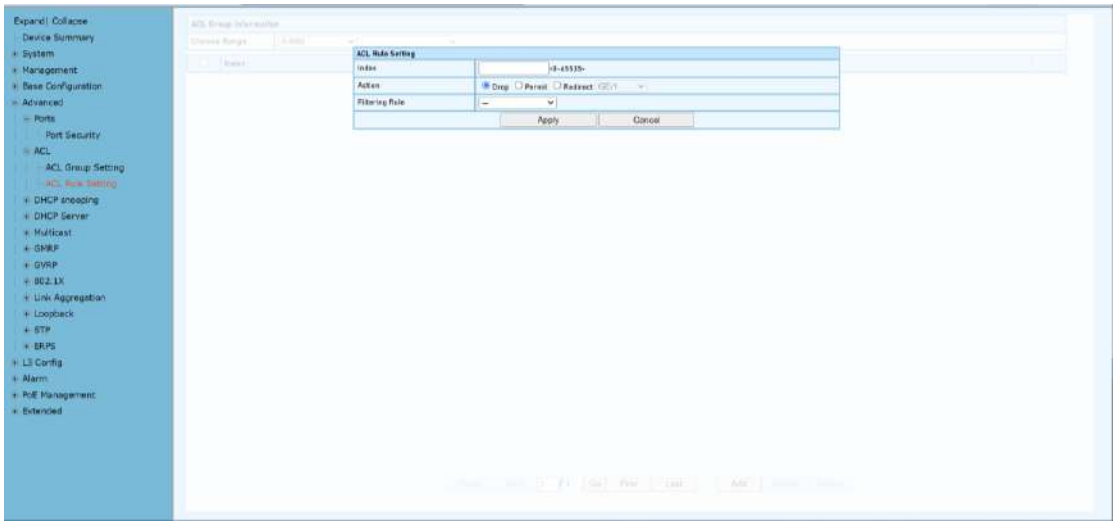
ACL Group Setting	
Index	<0-3999>
Group Name	
Binding Ports	All GE/1 GE/2 GE/3 GE/4 GE/5 GE/6 GE/7 GE/8 GE/9 GE/10 (Leave Binding Ports empty to disable the ACL Group.)
Apply	Cancel

Item	Description	Notes
Index	ACL group index, range <0-3999>, divided into 4 matching groups L2, L3 / L4, Source L2 / L3 / L4, Destination L2 / L3 / L4. The matching items supported by each matching group are as follows: **L2:** Source MAC, Destination MAC, Ethernet type, VLAN, IP protocol, range 0-999. **L3 / L4:** VLAN, Source IP, Destination IP, Source IP port, Destination IP port, IP protocol, range 1000-1999. **Source L2 / L3 / L4:** Source MAC, Ethernet type,	

	VLAN, Source IP, Source IP port, IP protocol, range 2000-2999. **Destination L2 / L3 / L4:** Destination MAC, Ethernet type, VLAN, Destination IP, Destination IP port, IP protocol, range 3000-3999.
Group Name	The Group name must be unique and string format, ASCII code A-Z, a-z,0-9, _, no more than 32 characters.
Binding Ports	An ACL is applied to a certain port or some port, then the bound port ACL becomes effective.

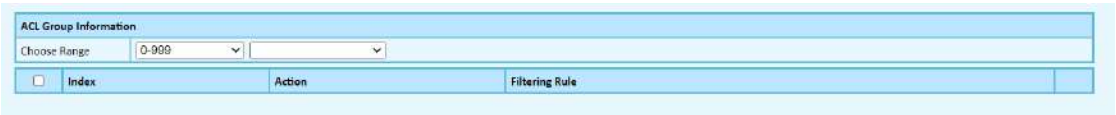
4.2.2 Advanced Configuration – ACL – ACL Rule Setting

ACLs are a collection of permit and deny conditions, called rules, that provide security by blocking unauthorized users and allowing authorized users to access specific resources. ACLs can block any unwarranted attempts to reach network resources.



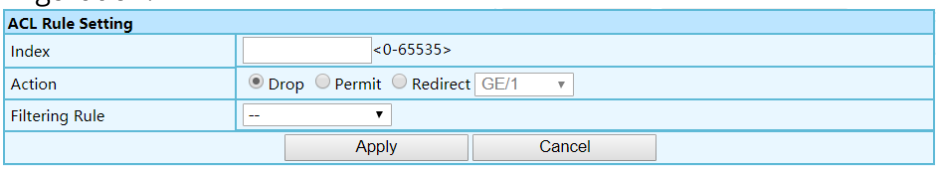
Configuration Step

1. Select [Advanced / ACL / ACL Rule Setting] in the navigation bar to enter the ACL Rule view interface.
2. In Select Range, select the interval of the group in the first drop-down list, and select a specific group within the group interval in second drop-down list. The next two lines show the selected group name and the port that the group binds. The table shows the ACL rules that the group has configured. Click the icon ⊞ in the filter rule bar to expand and view the specific content of the filter rule, the icon changed to be ⊟.

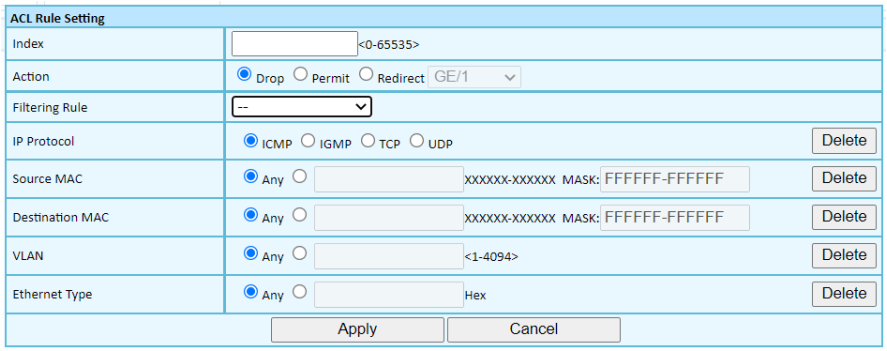


3. Add an ACL Rule: click [Add] to enter the ACL rule setting interface.One of the filtering rules can be selected by selecting different filters via the drop-down list, and then the corresponding filtering items will be automatically generated for users to fill in. You can also remove the filter items by the [Delete] on the right side. Fill in the required configuration items, and click [Apply] to complete the

configuration.



4. Modify an ACL Rule: select an ACL and click 'Modify' to enter the [ACL Rule Setting] interface. Fill in the required configuration items, and click 'Apply' to complete the configuration.
5. Delete an ACL Rule: select an ACL and click 'Delete' to delete the configuration.



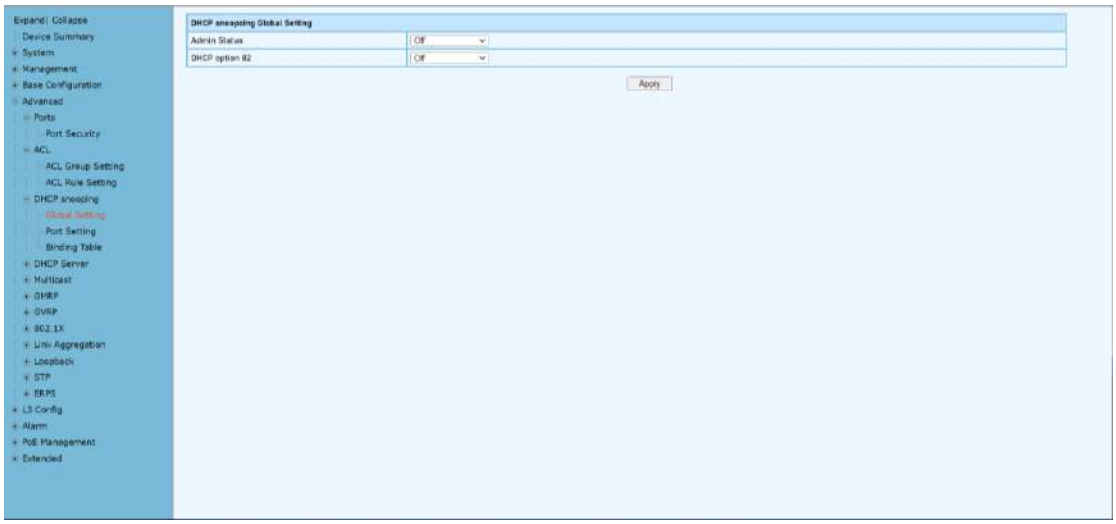
Item	Description	Notes
Index	ACL Rule Index	
Action	When the message conforms to the filter rule, the action includes: Allow Discarded Redirect to the destination port	
Filtering Rule	ACL filtering rules include: Source MAC Destination MAC IP Protocol Ethernet type VLAN The filtering items can be filtered by a range via setting the mask. **Note: When the match mask is 1, it is matched. Not matched at 0**	

Item	Description	Notes
Sources MAC	Format xxxxxx-xxxxxx, support the mask, default mask ffffff-ffffff	
Destination MAC	Format xxxxxx-xxxxxx, support the mask, default mask ffffff-ffffff	
IP Protocol	Only supports TCP, UDP, ICMP, IGMP currently	
Ethernet Type	Hexadecimal format, support mask, default mask FFFF	
VLAN	<1-4094>	

4.3 Advanced Configuration – DHCP snooping

4.3.1 Advanced Configuration – DHCP snooping – Global Setting

DHCP snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers.

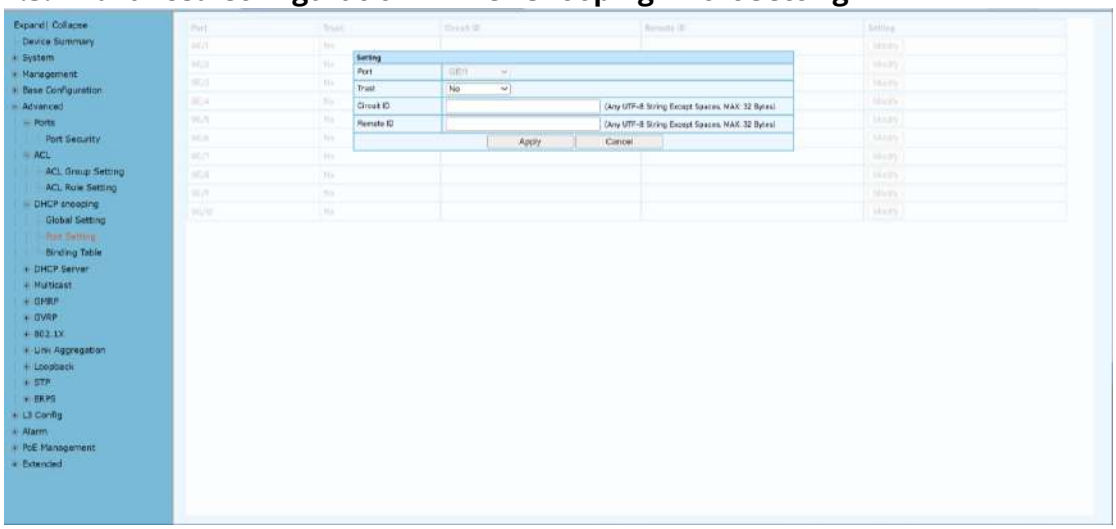


Configuration Steps

1. Select [Advanced / DHCP Snooping / Global Setting] in the navigation bar to enter the [Global Setting] interface of DHCP snooping.
2. The global configuration information can be viewed in of DHCP snooping [Global Setting] interface.
3. To modify the global configuration of DHCP snooping in the DHCP snooping global configuration box, click [Apply].

Item	Description	Notes
Admin Status	ON: Enable DHCP Snooping Global OFF: Disable DHCP Snooping Global	Default: OFF
DHCP option 82	ON: Enable DHCP Snooping Global OFF: Disable DHCP Snooping Global	Default: OFF

4.3.2 Advanced Configuration – DHCP snooping – Port Setting



Configuration Steps

1. Select [Advanced / DHCP Snooping / Port Setting] in the navigation bar to enter the DHCP snooping [Port Setting] interface.
2. The port configuration can be viewed in the DHCP snooping [Port Setting] interface.
3. To modify the DHCP snooping configuration for a port, click the [modify] to enter the port configuration interface, as shown in figure 17.2.
4. Select or fill in the configuration items that need to be modified, and click [Apply] to make effective. There will be prompts if the configuration items are incorrectly filled.

Item	Description	Notes
Port	The name of information	
Trust	Yes: Set as trust port No: Set as untrust port	
Circuit ID	Default by global agent circuit ID	
Remote ID	Default by global agent remote ID	

4.3.3 Advanced Configuration – DHCP snooping – Binding Table

Configuration Steps

1.Select [Advanced / DHCP Snooping / Binding Table] in the navigation bar to enter the DHCP snooping [Binding Table] interface.

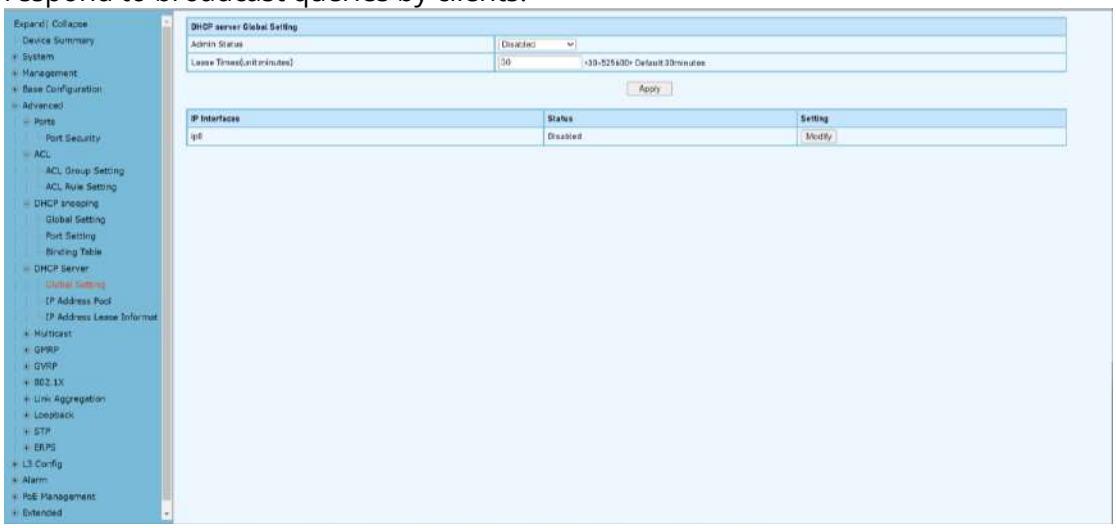
2.All bind list information can be viewed in the DHCP snooping [Binding Table] interface.

3.Click [Refresh] to update all DHCP snooping bind list information.

4.4 Advanced Configuration – DHCP Server

4.4.1 Advanced Configuration – DHCP Server – Global Setting

A DHCP Server is a network server that automatically provides and assigns IP address, default gateways and other network parameters to client devices. It relies on the standard protocol know as Dynamic Host configuration protocol or DHCP to respond to broadcast queries by clients.



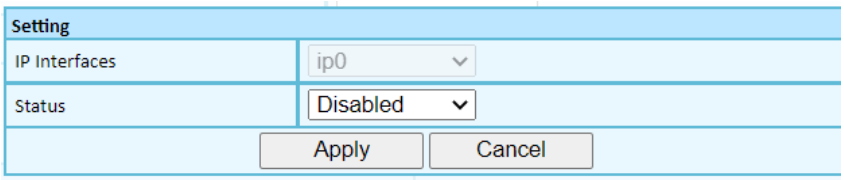
Configuration Steps

1.Select [Advanced / DHCP Server / Global] in the navigation bar to enter the DHCP Server[Global Setting] interface.

2.The DHCP server global setting admin status can be enabled/disable , and enter the lease times.

Remarks: 1. This DHCP-assigned IP address is not permanent and expires in about 24 hours.

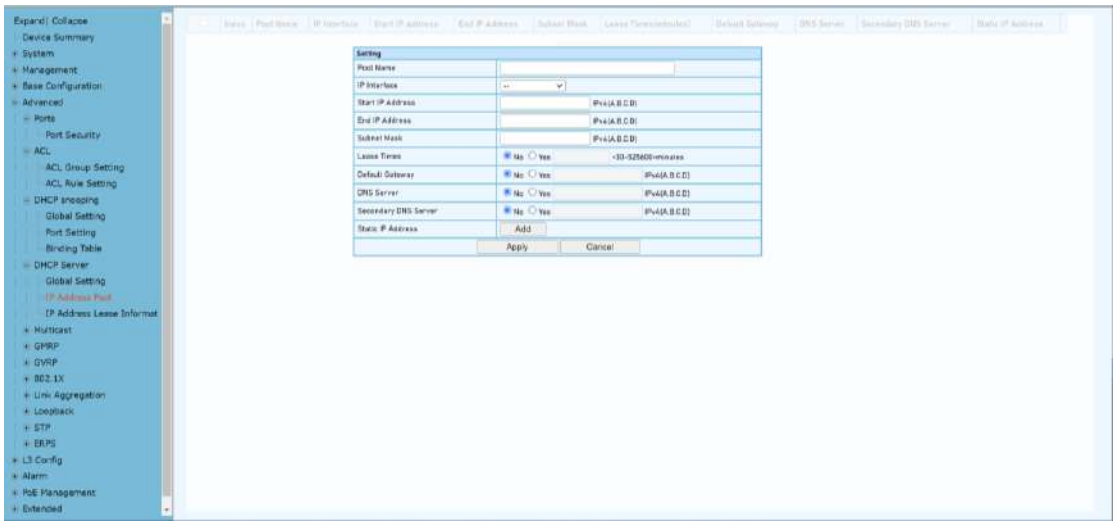
3, Click [Modify] to modify IP interface individually.



Item	Description	Notes
Admin Status	Enabled / Disabled DHCP server global setting	Default: Disabled
Lease time	<30-525600>	Default:30minutes
Status	Enabled / Disabled IP interface individually	Default:30minutes

4.4.2 Advanced Configuration – DHCP Server – IP Address Pool

Each DHCP address pool has a group of assignable IP addresses and network configuration parameters. The DHCP server selects IP addresses and other parameters from the address pool and assigns them to the DHCP clients.



Configuration Steps

1.Select [Advanced / DHCP Server / IP Address Pool] in the navigation bar to enter the DHCP Server[IP Address Pool] interface.

2. All IP Address Pool information can be viewed in the DHCP Server [IP Address Pool] interface.

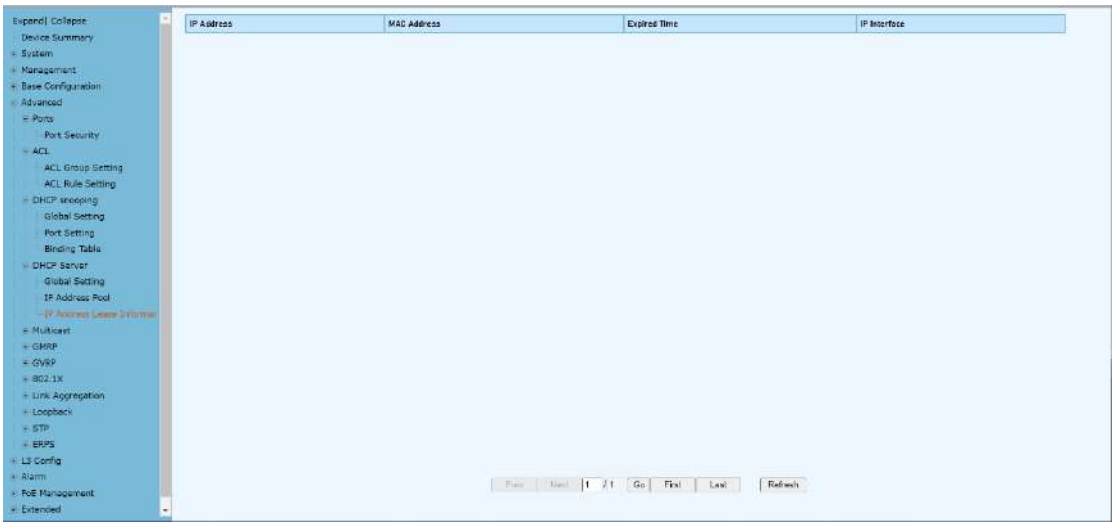
3, Click [Add] to add IP address pool individually. Click [Apply] to complete the configuration.

Item	Description	Notes
Pool Name	The name information of IP address pool	Default: None
IP Interface	Select a needed IP interface	Default: None
Start IP Address	Start IP Address in the IP address pool	Default: None
End IP Address	End IP Address in the IP address pool	Default: None
Subnet Mask	Subnet Mask of IP address	Default: None
Lease Times	No Yes: <30-525600> minutes	Default: None
Default Gateway	No Yes IPv4(A.B.C.D)	Default: None
DNS Server	No Yes IPv4(A.B.C.D)	Default: None
Secondary DNS Server	No Yes IPv4(A.B.C.D)	Default: None
Static IP Address	Add Static IP Address as needed	Default: None

4.4.3 Advanced Configuration – DHCP Server – IP Address Lease Information

Configuration Steps

1.Select [Advanced / DHCP Server / IP Address Lease Information] in the navigation bar to enter the DHCP Server [IP Address Lease Information] interface.



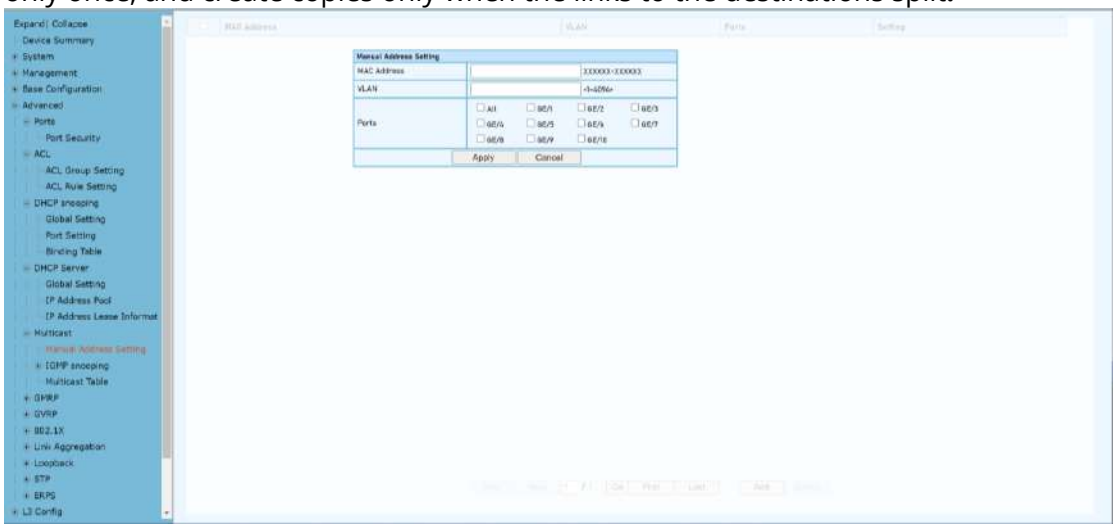
2. All IP Address Lease Information can be viewed in the DHCP Server [IP Address Lease Information] interface.

3, Click [Refresh] to refresh the list of the information.

4.5 Advanced Configuration – Multicast

4.5.1 Advanced Configuration – Multicast – Manual Address Setting

Multicast is the delivery of information to a group of destinations simultaneously, using the most efficient strategy to deliver messages over each link of the network only once, and create copies only when the links to the destinations split**.**



Configuration Steps

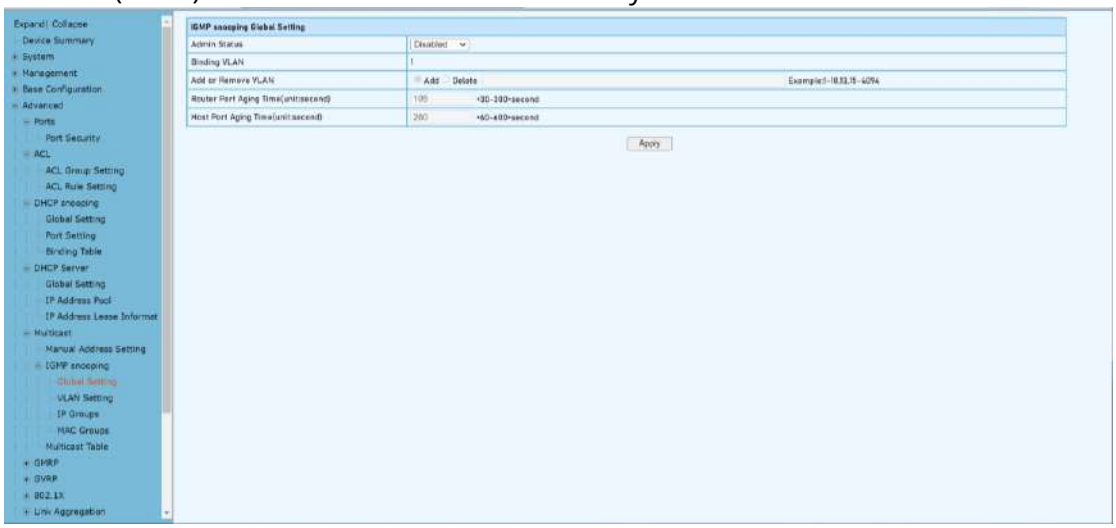
1.Select [Advanced / Multicast /Manual Address Setting] in the navigation bar to enter the Multicast [Manual Address Setting] interface.

2. All manual address can be viewed in the Multicast [Manual Address Setting] interface.

3, Click [Add] to manual add MAC address and VLAN for corresponding ports.4, Click [Apply] to complete the configurations

4.5.2 Advanced Configuration – Multicast – IGMP snooping Global Setting

IGMP snooping is the process of listening to Internet Group Management Protocol(IGMP) network traffic to control delivery of IP multicasts.



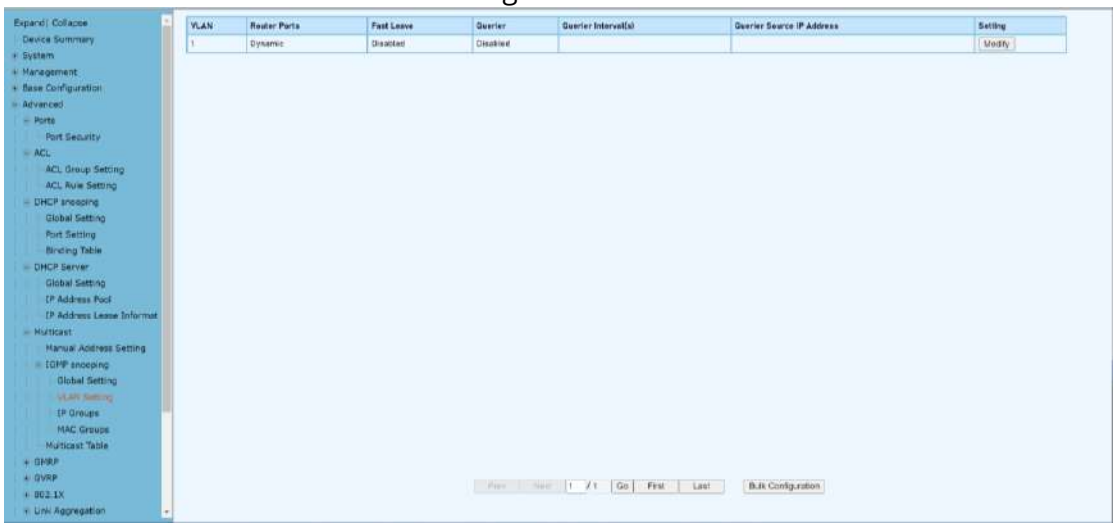
Configuration Steps

1. Select [Advanced / Multicast / IGMP snooping / Global Setting] in the navigation bar to enter the [Global Setting].
2. You can view the global configuration of IGMP snooping on the IGMP snooping global interface.
3. If you need to modify the global configuration of IGMP snooping, you can modify the corresponding configuration in the configuration box, and then click [Apply].

Item	Description	Notes
Admin Status	Enabled: Enable the IGMP snooping function Disabled: Disable IGMP snooping function	Default: Disabled
Blinding VLAN	List of VLANs to be bound	
Add or Remove VLAN	Select the operation for the VLAN and enter the list of VLANs to add or remove: **Add**: Add a VLAN. The format is as follows: 1-10,13,15-4094; **Delete**: Delete the VLAN. The format is as follows: 1-10,13,15-4094.	
Route Port Aging Time	Valid aging time of routed ports, range 30-300. The default is 105. The unit is seconds.	
Host Port Aging Time	Effective host port aging time, range 60-600. The default is 260.	Unit: Second

4.5.3 Advanced Configuration – Multicast – IGMP snooping VLAN setting

To run the IGMP Snooping querier on a VLAN, you have to enable it globally and on the VLAN. To enable IGMP snooping on a specific VLAN, use the IP IGMP snooping VLAN enable command in switch configuration mode.

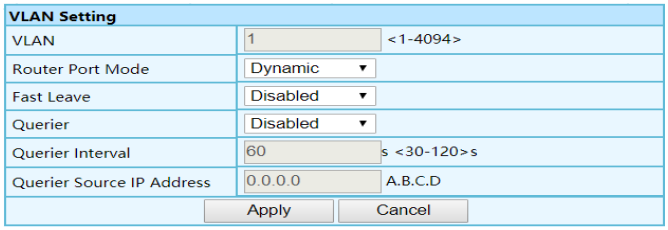


Configuration Steps

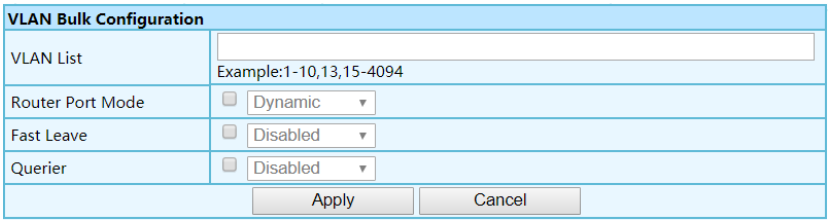
1. Select [Advanced / IGMP Snooping / VLAN Settings] to enter the VLAN Settings

2. The IGMP snooping [VLAN Settings] interface displays all the VLAN configuration information of IGMP Snooping.

3. Modify individual bound VLAN configuration information. After entering the [VLAN Settings] interface, click the [Modify] to enter the modification interface, as shown in Figure 12.2. Enter valid configuration parameters and click [Apply] to submit the modification. Click [Cancel] to abandon the modification.



4. Bulk VLAN configuration information in batches. After entering the [VLAN Setting], click the [Bulk Configuration] at the bottom of the page to enter the [VLAN Bulk Configuration], as shown in Figure 12.3. Enter valid configuration parameters and click [Apply] to submit the modification. Click [Cancel] to abandon the modification.



Item	Description	Notes
VLAN	VLAN being configured	
RouterPort Mode	Select the mode of the routed port in this VLAN. Use the drop-down box to modify it. **Dynamic** **Static** - If you choose the static routing port mode, you still need to select specific routing ports. It can be selected with the check button.	
Fast Leave Mode	Select whether to enable the quick leave mode under this VLAN. Use the drop-down box to modify it. **Disabled** **Enabled**	
Querier	Select whether to enable the querier function in this VLAN. Use the drop-down box to modify it. **Disabled** **Enable** - If the querier is enabled, you need to set the corresponding querier interval and query source IP address.	
Query Interval	The query interval of the querier is 30-120 seconds.	
Queryer Source IP Address	Set the source IP address of the query message sent by the querier. The valid unicast address is “192.168.1.11”. "0.0.0.0" is also available	

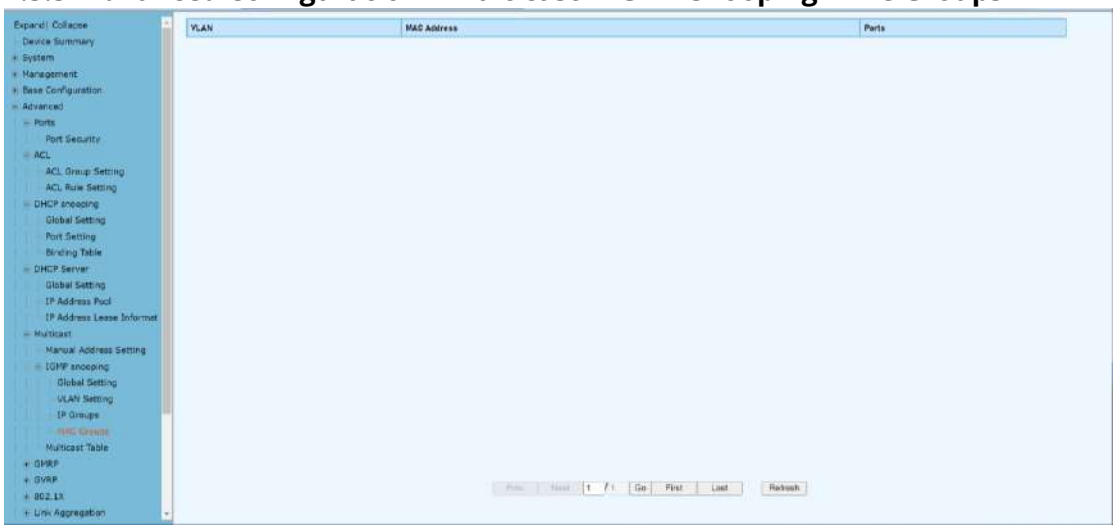
4.5.4 Advanced Configuration – Multicast – IGMP snooping IP Groups

Configuration Steps

Select [Advanced / IGMP snooping / IP Groups] in the navigation bar to enter the IP Group interface.

The IGMP snooping [IP group] interface displays the IP group information maintained by IGMP Snooping and can be refreshed by clicking the [Refresh].

4.5.5 Advanced Configuration – Multicast – IGMP snooping MAC Groups



Configuration Steps

1. Select [Advanced / IGMP Snooping / MAC Groups] in the navigation bar to enter the MAC Group interface
2. The IGMP snooping [MAC Group] interface displays the MAC group information maintained by IGMP Snooping. Click the Refresh button to refresh.

4.5.6 Advanced Configuration – Multicast – IGMP snooping Multicast Table

Configuration Steps

1. Select [Advanced / IGMP Snooping / Multicast Table] in the navigation bar to enter the Multicast Table interface
2. The IGMP snooping [Multicast Table] interface displays the Multicast Table information maintained by IGMP Snooping. Click the Refresh button to refresh.

4.6 Advanced Configuration – GMRP

4.6.1 Advanced Configuration – GMRP– GMRP Setting

GARP Multicast Registration Protocol (GMRP) is a Generic Attribute Registration Protocol (GARP) application that provides a constrained multicast flooding facility similar to IGMP snooping. GMRP and GARP are industry-standard protocols defined by the IEEE 802.1

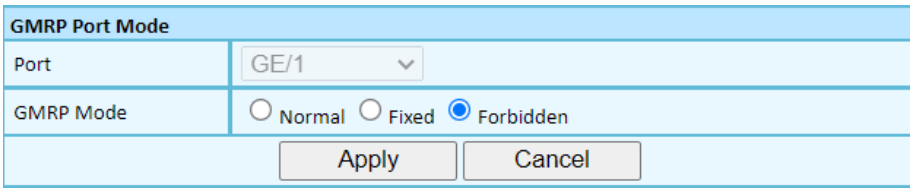
Configuration steps

1. Select [GMRP / GMRP Setting] in the navigation bar to enter the GMRP configuration interface.
2. You can view the global configuration of GMRP in the [GMRP Global Settings] interface
3. If you need to modify the global configuration of GMRP, modify the corresponding configuration in the GMRP global configuration box, and then click <Apply>.

Item	Description	Notes
Admin Status	GMRP global enable switch. **Enabled**: Enable GMRP function; **Disabled:** Disable the GMRP function.	Default: Disabled
Hold Time	Hold timer period, the range is 100-32760 (ms), the default value is 100ms;	≤2
Join Time	Join timer period, the range is 100-32760 (ms), the default value is 200ms;	≤2
Leave Time	Leave timer period, the range is 100-32760 (ms), the default value is 600ms	Leave Time ≤ Leave All Time
Leave All Time	Leave all timer period, the range is 100-32760 (ms), the default value is 10000ms;	Leave Time ≤ Leave All Time

GMRP Port Mode Configurations,

1.If you need to modify the Port Mode of GMRP, Click [modify] to select GMRP Mode as Normal , Fixed, Forbidden

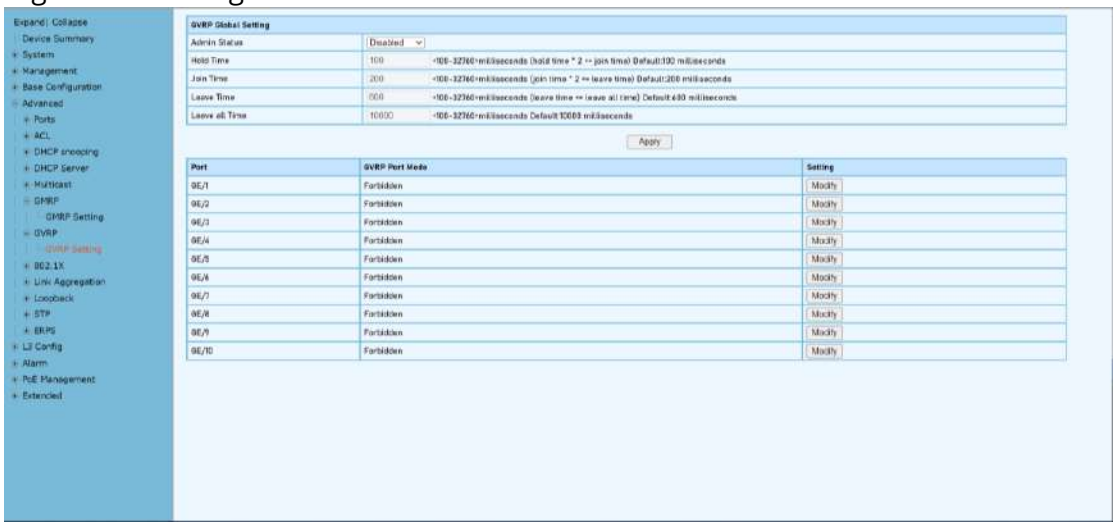


Item	Description	Notes
Port	Port name of information	
GMRP Mode	Normal, Fixed, Forbidden	Default: Forbidden

4.7 Advanced Configuration – GVRP

4.7.1 Advanced Configuration – GVRP – GVRP Setting

Same as GMRP, GVRP (GARP VLAN Registration Protocol) is a VLAN registration protocol based on GARP (Generic Attribute Registration Protocol), which is used to register and deregister VLAN attributes



Configuration Steps

1.Select [GVRP/GVRP configuration] from the navigation bar to enter the GVRP configuration interface.

2.The global configuration of GVRP can be viewed in the [GVRP global Settings] interface,

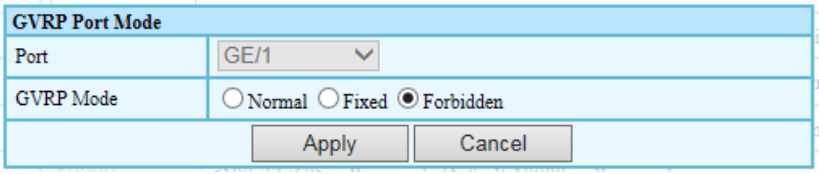
3.To modify the GVRP global configuration, modify the corresponding configuration in the GVRP global configuration box, and then click < apply >.

Item	Description	Notes
Admin Status	GVRP global enable switch. Enabled: Enable GVRP function; Disabled: Disable the GVRP function.	DEFAULT: DISABLED
Hold Time	Hold timer period, the range is 100-32760 (ms), the default value is 100ms;	≤2
Join Time	Join timer period, the range is 100-32760 (ms), the default value is 200ms;	≤2
Leave Time	Leave timer period, the range is 100-32760	LEAVE TIME ≤

	(ms), the default value is 600ms	LEAVE ALL TIME
Leave All Time	Leave all timer period, the range is 100-32760 (ms), the default value is 10000ms;	LEAVE TIME ≤ LEAVE ALL TIME

GVRP Port Mode Configurations,

1.If you need to modify the Port Mode of GVRP, Click [modify] to select GVRP Mode as Normal , Fixed,



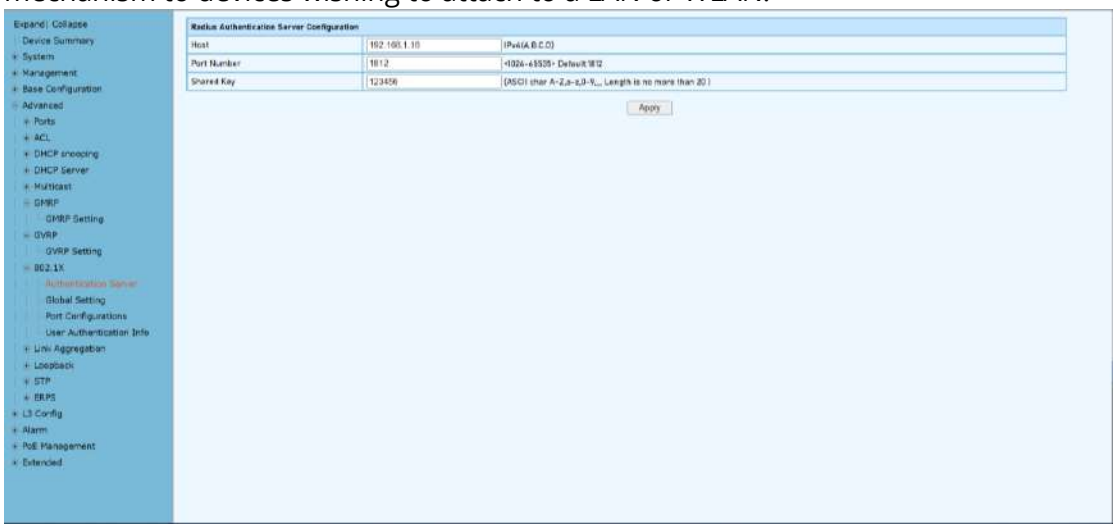
Forbidden

Item	Description	Notes
Port	Port name of information	
GVRP Mode	Normal, Fixed, Forbidden	Default: Forbidden

4.8 Advanced Configuration – 802.1X

4.8.1 Advanced Configuration – 802.1X – Authentication Server

IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.



Configuration Steps

1. Select [Advanced / 802.1X / Authentication Server] in the navigation bar to enter Radius Authentication Server Configuration.
2. Check the configuration information in the interface
3. To apply the Authentication Server configuration, click [Apply] in the Authentication Server configuration box.

Item	Description	Notes
Host	The IP of Radius Authenticated Server, IPv4 and Dotted decimal format	
Port Number	The port of Radius Authenticated Server, range<1-65535>, default with 1812	Default:1812
Shared Key	Must be consistent with Radius server, otherwise it can not pass authentication. String format, only contain letters, numbers, underscores, and the length cannot be more than 20 byte	

4.8.2 Advanced Configuration – 802.1X – Global Setting

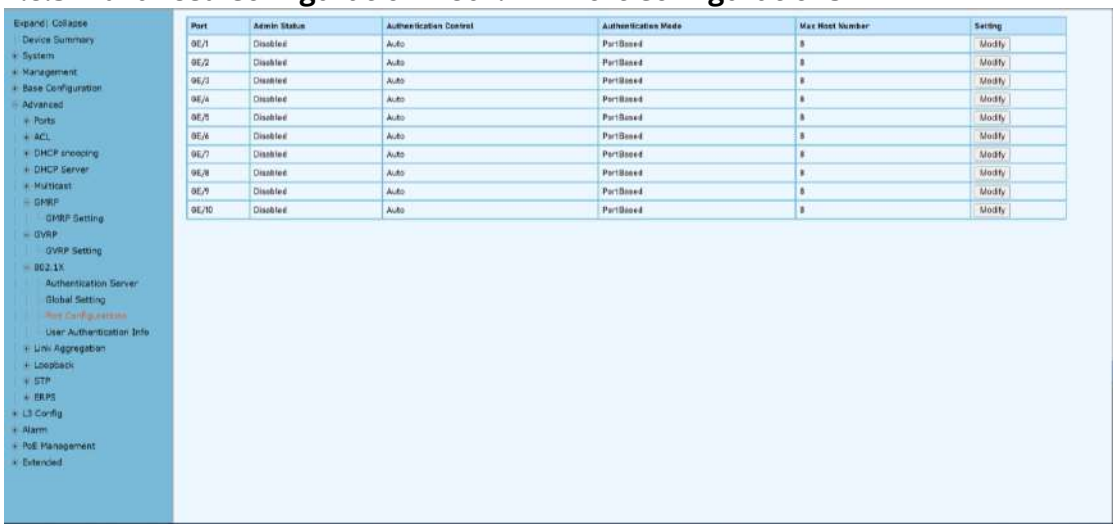
Configuration Steps

1. Select [Advanced / 802.1X / Global Setting] in the navigation bar to enter the [Global Setting] interface.
2. The global configuration information can be viewed in the interface.
3. To modify the global configuration in the Global Configuration box, click [Apply].

Item	Description	Notes
Admin Status	Disabled: Disabled Global 802.1X Enabled: Enabled Global 802.1X	Default: Disabled
Reatuthentication	Disabled: Disabled re-authentication Enabled: Enabled re-authentication	Default: Disabled
Quiet Function	Disabled: Disabled quiet function Enabled: Enabled quiet function	Default: Disabled
Authentication Method	EAP/PAP/CHAP	
Tx Period (Unit:Second)	1-120	Default: 30
Supplicant Timeout (Unit: Second)	1-120	Default: 30
Server Timeout (Unit:Second)	1-120	Default: 30
ReAuthentication Period	60-7200	Default:

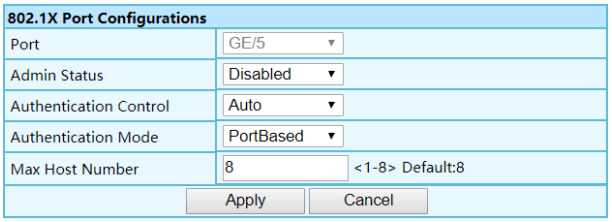
(Unit:Second)		3600
Quiet Period (Unit:Second)	10-3600	Default: 60

4.8.3 Advanced Configuration – 802.1X – Port Configurations



Configuration Steps

1. Select [Advanced / 802.1X / Port Configurations] in the navigation bar to enter the [Port Configurations] interface.
2. On the [Port Configurations] interface, you can view the configuration information of each port, the current 802.1X configuration information of each port is displayed.
3. To modify the configuration of a port, simply click the [Edit] in corresponding entry to enter modification interface, as shown in Figure 10.4. Modify the corresponding configuration item, click the [Apply] to complete the modification, and click the [Cancel] to cancel the modification.

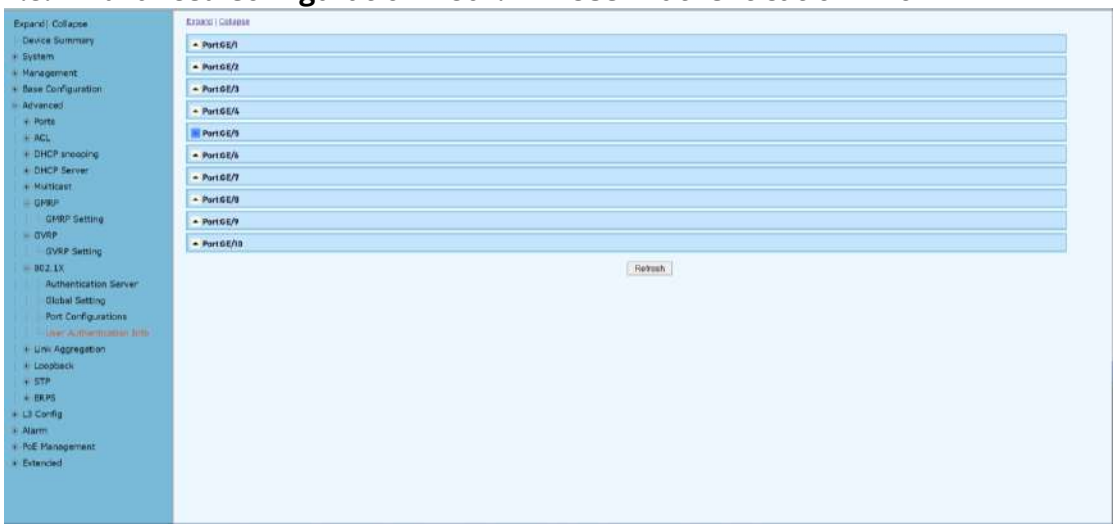


Remarks: When the 802.1X port is configured to authentication mode, all authenticated users will go offline and re-authentication is required to access the network.

Item	Description	Notes
Port	Selected port configurations	
Admin Status	Enabled: Enabled port 802.1X Disabled: Disabled port 802.1X	Default: Disabled
Authentication Control	Auto: You cannot access the network before authentication. You can access the network after passing the authentication. Forced-Authentication: Always have access to the network	

	Forced-Unauthentication: Always cannot access the network	
Authentication Mode	PortBased: After a user is authenticated, all users can access the network. MacBased: All users need to be authenticated individually to access the network.	
Max Host Number	There is maximum number of authenticated hosts supported by the port. Authentication will fail if this number is exceeded.	Default: 8

4.8.4 Advanced Configuration – 802.1X – User Authentication Info



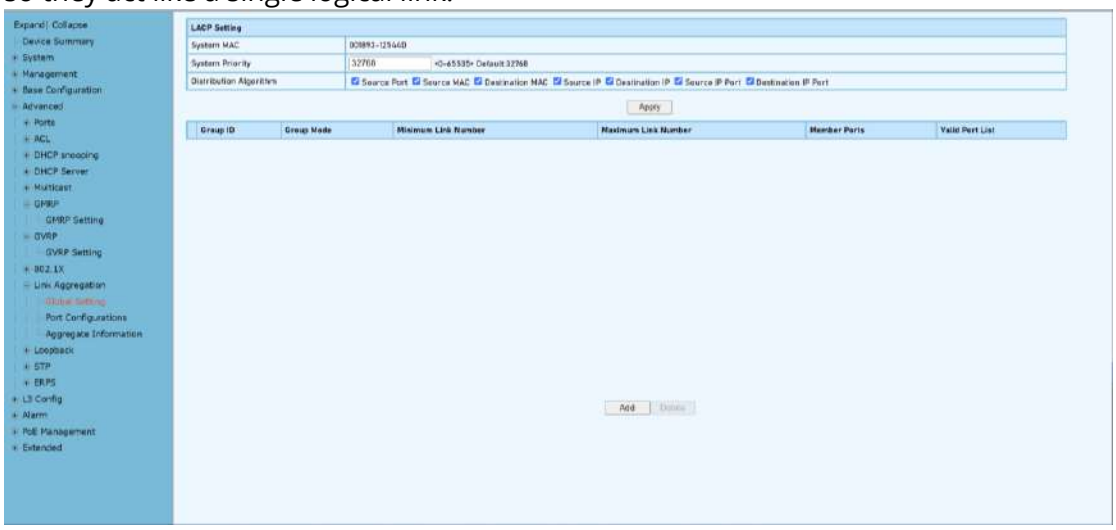
Configuration Steps

1. Select [Advanced / 802.1X / User Authentication Information] in the navigation bar to enter the [User Authentication Information] interface.
2. Click [Expand] in the upper left corner to expand the user authentication information for all ports, and click [Close] to close the user authentication information for all ports. Click the ⊞icon to expand the user authentication information for the corresponding port, and click the ⊟icon to close the user authentication information for the corresponding port.
3. The authentication information of the user can be viewed on this interface: user name, client MAC address, and the time the authentication passed.
4. Click [Refresh] to refresh the current user authentication information.

4.9 Advanced Configuration – Link Aggregation

4.9.1 Advanced Configuration – Link Aggregation – Global Setting

Link aggregation is a way of bundling a bunch of individual (Ethernet) links together so they act like a single logical link.



Configuration Steps

1.Select [Advanced / Link Aggregation / Global Setting] in the navigation bar to enter the [Link Aggregation / Global Setting] interface.

2.The link aggregation global configuration can be viewed in the link aggregation global setting interface.

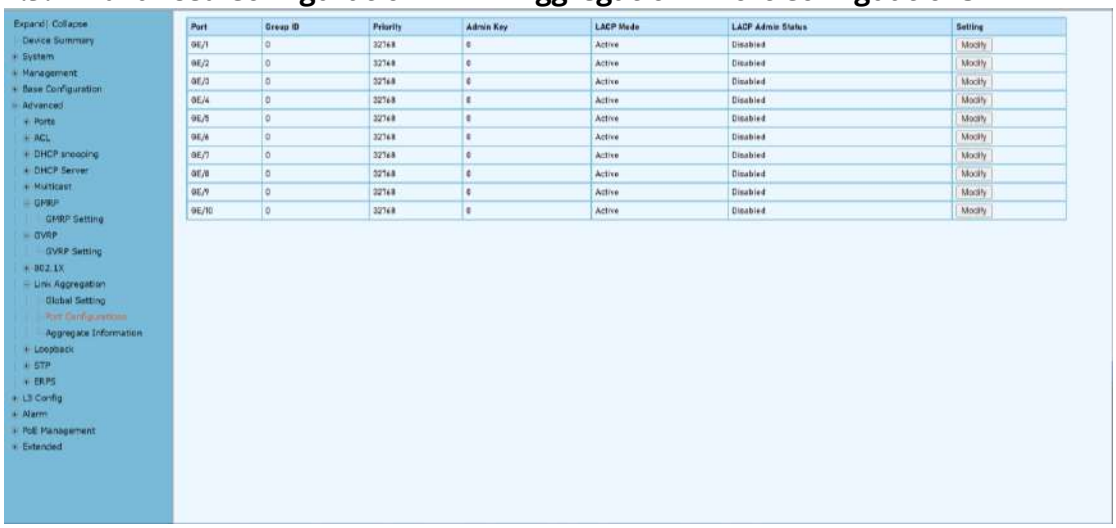
3.To modify the global configuration of link aggregation, modify the corresponding configuration in the LACP (Link Aggregation Control Protocol) configuration box, and then click [Apply]

4.If you want to add an aggregation group, click [set], as shown in figure 14.2. click [Apply].

Item	Description	Notes
System MAC		
System Priority	Set the link aggregation system priority, range 0-65535, the smaller the better.	Default: 32768
Distribution Algorithm	The system supports one or more to compute the load ports according to the source port, source MAC, destination MAC, source IP, destination IP, source IP port and destination IP	
Group ID	Aggregation Group ID information	
Group Mode	Set Aggregation Group Mode Manual: Manual mode, the port of the aggregation group member is manually configured and the port LACP protocol is closed. Static: Static mode, the port of the aggregation group member is manually configured and the port LACP protocol is on.	

Minimum Port	The active ports minimum number of aggregation group configuration, ranging <0-8>, and the value cannot exceed the maximum number of links.
Maximum Port	The active ports maximum number of aggregation group configuration, ranging <0-8>, and the value cannot be less than the minimum number of links.
Member Port List	Member port of aggregation group configuration

4.9.2 Advanced Configuration – Link Aggregation – Port Configuations



Configuration Steps

1. Select [Advanced / Link Aggregation / Port Configurations] in the navigation bar to enter the link aggregation [Port Configurations] interface.
2. In the link aggregation [Port Configurations]interface, you can view the link aggregation related configuration of the port.
3. If the link aggregation configuration of the port needs to be modified, click the [Modify] to enter the port configuration interface.
4. Select or fill in the configuration items that need to be modified, and click [Apply] to make effective. If the configuration items are incorrectly filled, there will be corresponding prompts.

Item	Description	Notes
Port	Name of port	
Group ID	The Port ID of aggregation group	
Priority	Port link aggregation priority, range <0-65535>	Default:32768
Admin Key	Enter a value to configure the LACP actor admin key that is used while port participates in dynamic aggregation selection. Rang:<0-65535>	Default: 0

LACP Mode	Port master-slave mode in LACP protocol **Active**: Active mode, the port send protocol messages automatically when LACP protocol enabled. **Passive**: Passive mode, the port will not send protocol messages automatically, but only send when received protocol messages.	Default: Active
LACP Admin Status	Enabled: Enabled LACP on port Disabled: Disabled LACP on port	Default: Disabled

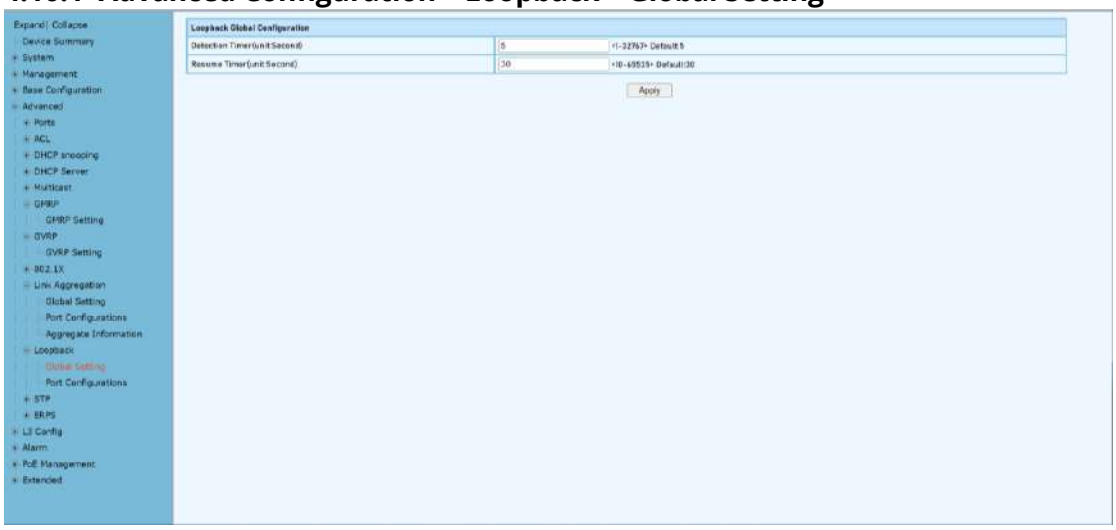
4.9.3 Advanced Configuration – Link Aggregation – Aggregation Information

Configuration Steps

1. Select [Advanced / Link Aggregation / Aggregate Information]in the navigation bar to enter the [Link Aggregation / Aggregation Information]interface.
2. In the link aggregation [Aggregate Information] interface, all port link aggregation related information can be viewed.
3. Click [Refresh] to see the latest aggregation information for each port.

4.10 Advanced Configuration – Loopback

4.10.1 Advanced Configuration – Loopback – Global Setting

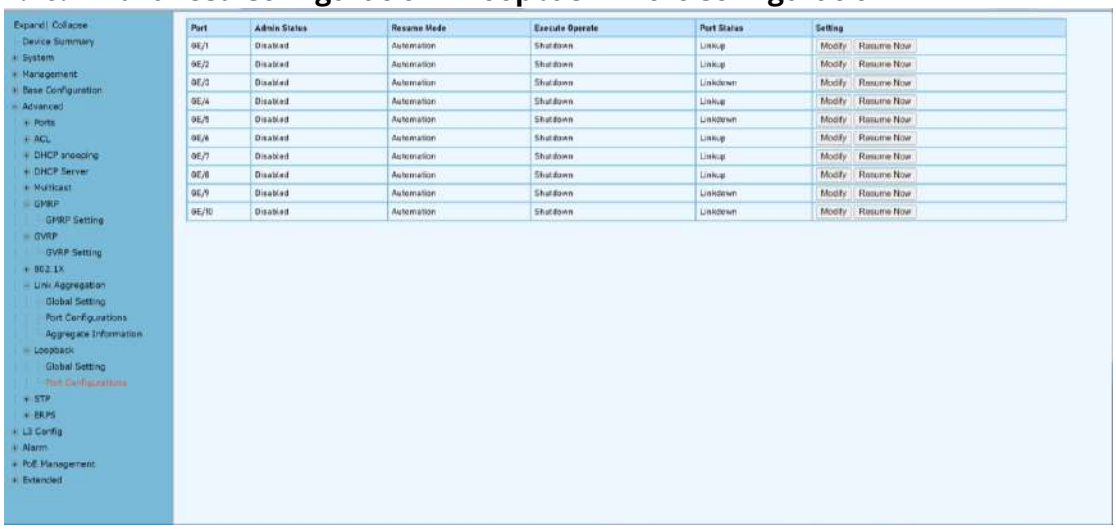


Configuration Steps

1. Select [Advanced / Loopback / Global Setting] in the navigation bar to enter [Global Setting] interface.
2. In the global configuration interface, you can view the global configuration information.
3. To modify the global configuration, modify the corresponding configuration in the Global Configuration box and click [Apply], as shown in Figure 11.1

Item	Description	Notes
Detection Timer	Loop detection packet sending interval, range<1-32767>	Default: 5sec
Resume Timer	Port auto resume period, range<10-65535>, must be less than 2x detection timer	

4.10.2 Advanced Configuration – Loopback – Port Configuration



Configuration Steps

1. Select [Advanced / Loop Detection / Port Configuration] in the navigation bar to enter the Port Configuration interface.
2. On the Port Configuration page, you can see the loop detection configuration information and running status of all the ports.
3. To modify the configuration of a port, simply click the [Edit] on the right side of the corresponding entry to enter the modification interface. Modify the corresponding configuration item, click the [Apply] to complete the modification, and click the [Cancel] to cancel the modification.

Port	Admin Status	Resume Mode	Execute Operate	Port Status	Setting
GE/1	Disabled	Atuomation	Shutdown	Linkdown	Modify Resume Now
GE/2	Disabled	Atuomation	Shutdown	Linkdown	Modify Resume Now
GE/3	Disabled	Atuomation	Shutdown	Linkdown	Modify Resume Now
GE/4	Disabled	Atuomation	Shutdown	Linkdown	Modify Resume Now
GE/5	Disabled	Atuomation	Shutdown	Linkdown	Modify Resume Now
GE/6	Disabled	Atuomation	Shutdown	Linkdown	Modify Resume Now
GE/7	Disabled	Atuomation	Shutdown	Linkdown	Modify Resume Now
GE/8	Disabled	Atuomation	Shutdown	Linkup	Modify Resume Now
GE/9	Disabled	Atuomation	Shutdown	Linkdown	Modify Resume Now
GE/10	Disabled	Atuomation	Shutdown	Linkdown	Modify Resume Now

4. After a loop occurs on a port and the port is shut down or blocked by a specified action, if you want to restore it immediately, you can click the [Restore Now] on the right side of the corresponding entry.

LoopBack Port Configurations	
Port	GE/7
Admin Status	Disabled
Resume Mode	Atuomation
Execute Operate	Shutdown
Apply	Cancel

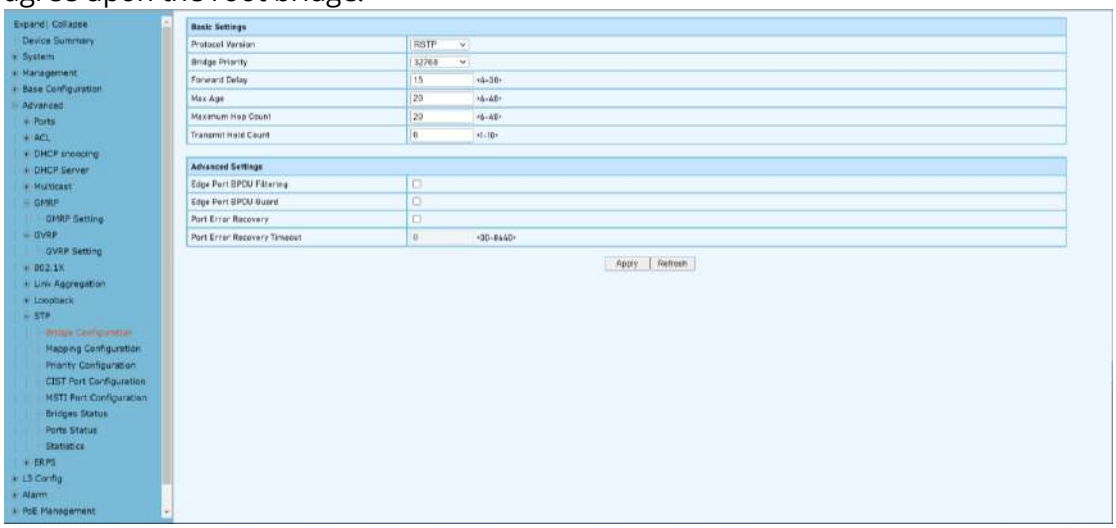
Item	Description	Notes
Port	Selected Port	
Admin Status	Disabled: Disabled loop detection Enabled: Enabled loop detection	Default: Disabled

Resume Mode	Automatic: After the loop occurs, the port is closed or blocked, and the port automatically recovers. Manual: After a loop occurs, the port is closed or blocked, need to manually restore the port.
Execute Operate	Shutdown: After the loop occurs, the port is shutdown Blocked: After a loop occurs, the port is blocked

4.11 Advanced Configuration – STP

4.11.1 Advanced – STP – Bridge Configuration

The Spanning Tree Protocol (STP) is responsible for identifying links in the network and shutting down the redundant ones, preventing possible network loops. In order to do so, all switches in the network exchange BPDU messages between them to agree upon the root bridge.



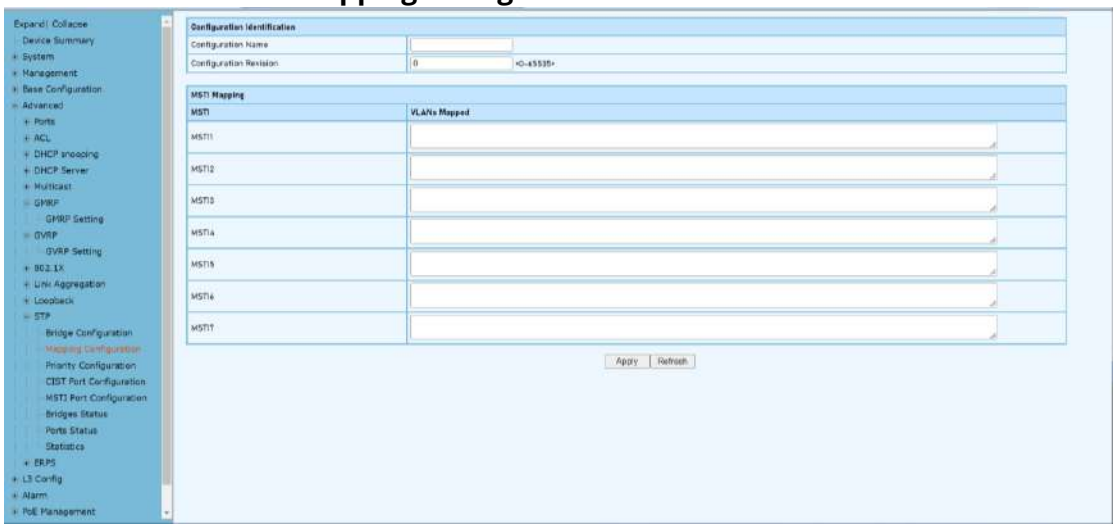
Configuration Steps

1. Select [Advanced / STP / Bridge Configuration] in the navigation bar to enter the STP[Bridge Configuration] interface.
2.The STP Bridge Configuration can be viewed in the [Bridge Configuration] interface.
3. To modify the configuration, you can enter the values that need to be configured directly in corresponding configuration item.

Item	Description	Notes
STP Mode	STP/RSTP/MSTP	
Bridge Priority	STP System priority,Range<0-61440>, the step must be 4096	Default: 32768
Forward Delay	Delay when port switch between disabled / listening / learning / forwarding, Range<4-30>	Default:15sec
Max Age	The maximum survival time of the STP protocol packet received by the bridge. If no new protocol packets received at this time, the packet will be discarded. Range<6-40>	Default: 20second
Maximum Hop	Determines the transmission range of bpdu.	Default:

Count	The range of hops is 6-40.	20
Transmit Hold Count	Count the number of sending hops. The count range is 1-10.	Default: 6 per sec
Edge Port BPDU Filtering	BPDU filtering will prevent the switch from sending BPDUs to the host on a port with the edge port feature enabled.	Default: Disabled
Edge Port BPDU Guard	BPDU guards prevent bridging loops by enabling ports with edge port characteristics to enter the err-disable state when receiving BPDUs	
Port Error Recovery	Enable the recovery function for the port in the err-disable state. If checked, it is enabled. By default, if it is not checked, it is disabled.	
Port Error Recovery Timeout	Restart this port after timeout.	

4.11.2 Advanced-STP-Mapping Configuration

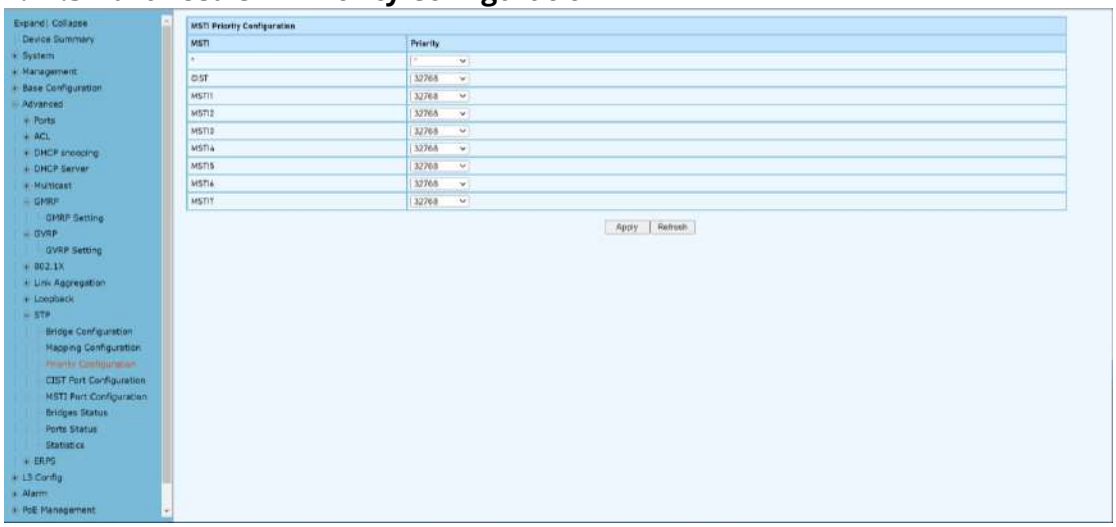


Configuration Steps

1. Select [Advanced / STP / Mapping Configurations] in the navigation bar to enter the STP [Mapping Configuration] interface.
2. The STP Mapping configuration information can be viewed in the [Mapping Configurations] interface.
3. To modify the mapping configuration, you can enter configuration item on the right side of the corresponding ccolumn .

Item	Description	Notes
Port	Port Name	
Configuraiton Name	MAC address identifier	
Configuration Revision	The modification range is 0-65535	Default:0
VLANs Mapped	Use commas to separate, the VLAN range is 1-4096, such as 2-5, 7, 9, etc	

4.11.3 Advanced-STP-Priority Configuration



Configuration Steps

1. Select [Advanced / STP / Priority Configurations] in the navigation bar to enter the STP [Priority Configuration] interface.
2. The STP Priority configuration information can be viewed in the [Priority Configurations] interface.
3. To modify the priority configuration, you can enter configuration item on the right side of the corresponding column .

Item	Description	Notes
Priority	The size of the bridge priority determines whether the device can be selected as the root of the spanning tree. The bridge priority ranges from 0 to 61440	Default:32768

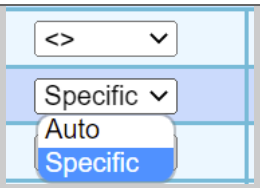
4.11.4 Advanced-STP-CIST Port Configuraion

Configuration Steps

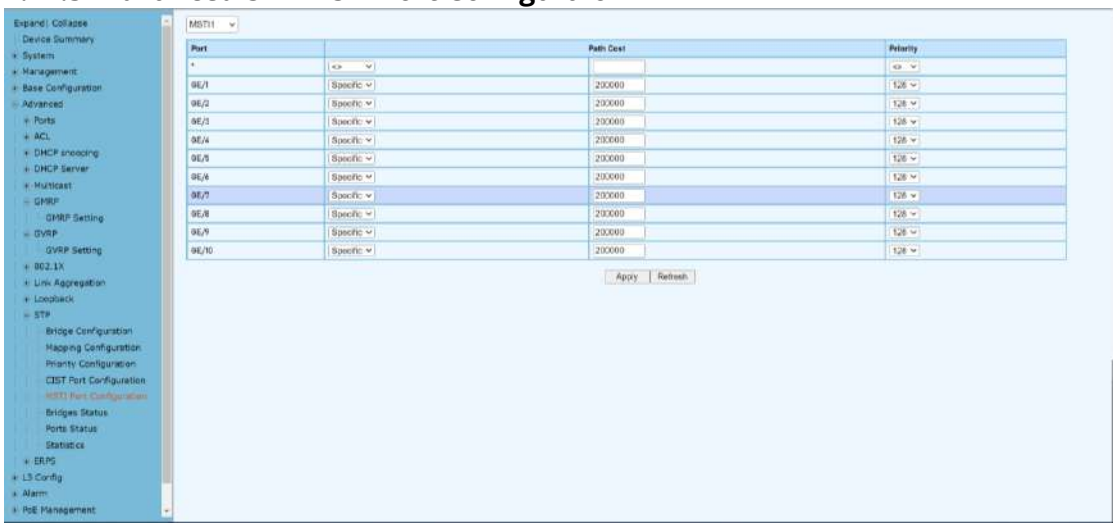
1. Select [Advanced / STP / CIST Port Configuraion] in the navigation bar to enter the STP [CIST Port Configuraion] interface.
2. The STP CIST Port Configuraion can be viewed in the [CIST Port Configuraion]

interface.

3. To modify the CIST Port Configuraion, you can enter configuration item on the corresponding column .

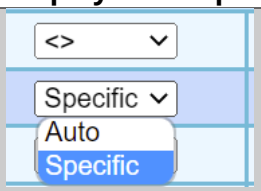
Item	Description	Notes
Port	Display switch port number	
STP Enabled	The checked end means the port stp function is enabled. If it is not checked, it is disabled.	Default:Disabled
Path Cost	 Auto: Auto Negotiation Specific: Manual Setting	Default:Auto
Priority	When the port priority is changed, STP will recalculate the role of the port and perform state migration. The value of the port priority can only be a multiple of 16. The configuration range is 0-240.	Default:128
Admin Edge	Non-Edge/Edge	Default: Non-Edge
Auto Edge	If it is selected, automatic edge port identification is enabled. If it is not selected, automatic edge port identification is disabled. By default, automatic edge port identification is enabled	
Role	If it is selected, the role is enabled. If it is not selected, the role is disabled. By default, the role is disabled	
TCN	The check end indicates TCN. If the check end is not selected, TCN is disabled.	Default:Disabled
BPDU Guard	The BPDU Guard enables an edge port to enter the Err-disable state when receiving BPDUs to prevents bridge loops. The BPDU filter prevents the switch from sending BPDUs to hosts on an edge port. This function is disabled by default	
Point-to-Point	**Force True**: Indicates point-to-point link. If the port is in full-duplex mode, the link type is point-to-point link. **Force False:** Shared link. If the link is running in half-duplex mode, the link type is shared. **Auto:** Indicates that the port automatically establishes a link. The default port automatically establishes a link. Nowadays, switches are generally of point-to-point link type	

4.11.5 Advanced-STP-MSTI Port Configuraion

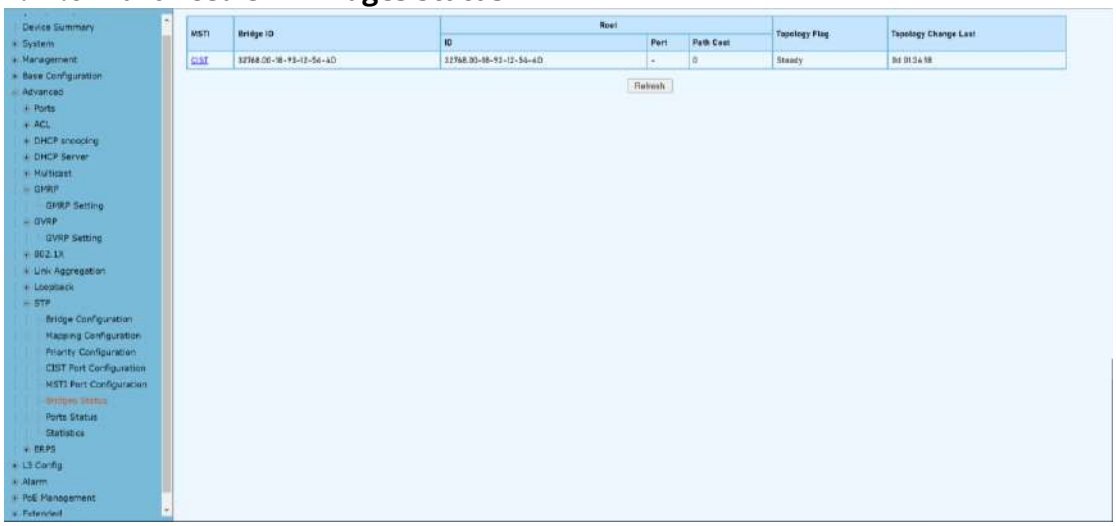


Configuration Steps

1. Select [Advanced / STP / MSTI Port Configuraion] in the navigation bar to enter the STP [MSTI Port Configuraion] interface.
2. The STP MSTI Port Configuraion can be viewed in the [MSTI Port Configuraion] interface.
3. To modify the MSTI Port Configuraion, you can enter configuration item on the corresponding column .

Port	Display switch port number	
Path Cost	 Auto: Auto Negotiation Specific: Manual Setting	
Priority	When the port priority is changed, STP will recalculate the role of the port and perform state migration. The value of the port priority can only be a multiple of 16. The configuration range is 0-240.	Default:128

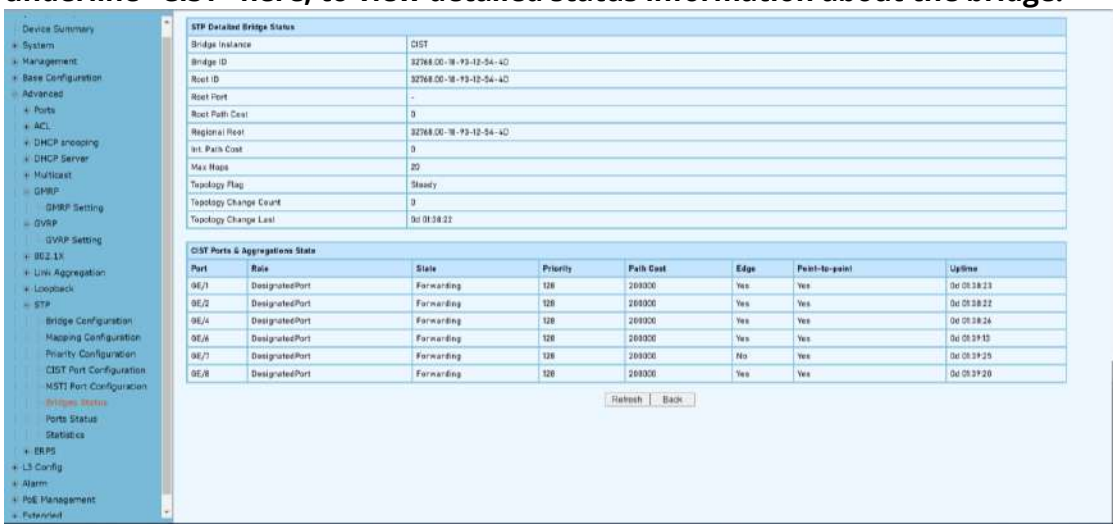
4.11.6 Advanced-STP-Bridges Status



Configuration Steps

1. Select [Advanced / STP / Bridges Status] in the navigation bar and enter the STP [Bridges Status] interface.
2. The Bridges Statuscan be viewed in the [Bridges Status] interface
3. Click [Refresh] to show the latest running information.

Click the name of the MSTI column, for example, the blue text with the underline "CIST" here, to view detailed status information about the bridge.



4.11.7 Advanced-STP-Ports Status

Configuration Steps

1. Select [Advanced / STP / Ports Status] in the navigation bar and enter the STP [Ports Status] interface.
2. The Bridges Statuscan be viewed in the [Ports Status] interface
3. Click [Refresh] to show the latest running information.

4.11.8 Advanced Configuration – Statistics

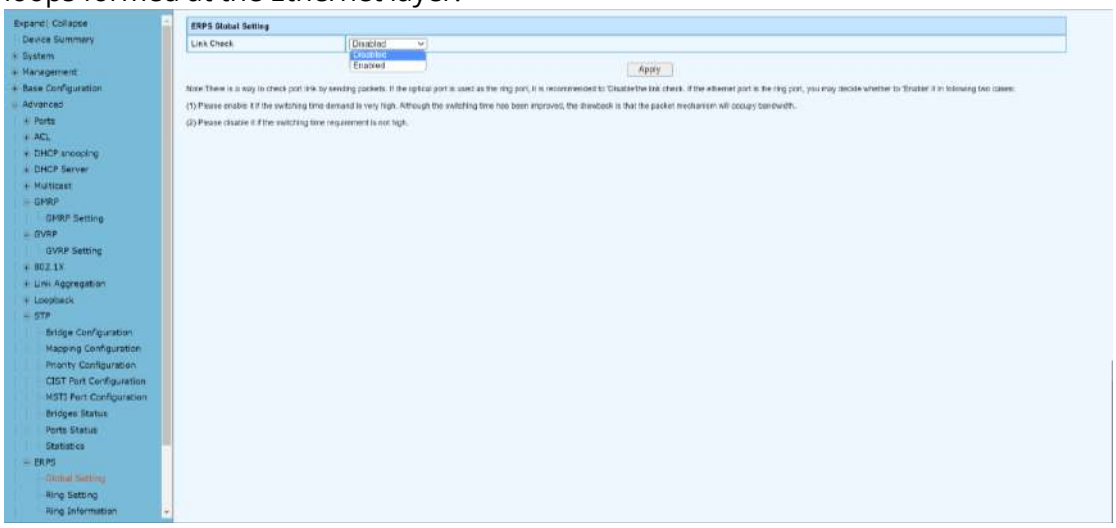
Configuration Step

1. Select [Advanced / STP / Statistics] in the navigation bar and enter the STP [Statistics] interface.
2. The STP current running information can be viewed in the [Statistics] interface
3. Click [Refresh] to show the latest running information.

4.12 Advanced Configuration – ERPS

4.12.1 Advanced Configuration – Global Setting

Ethernet Ring Protection Switching, or ERPS, is an effort at ITU-T under G. 8032 Recommendation to provide sub-50ms protection and recovery switching for Ethernet traffic in a ring topology and at the same time ensuring that there are no loops formed at the Ethernet layer.



Configuration Step

1.Select [Advanced / ERPS / Global Setting] in the navigation bar and enter the ERPS [Global Setting] interface

Remarks: 1, There is a way to check port link by sending packets. If the optical port is used as the ring port, it is recommended to 'Disable' the link check. If the ethernet port is the ring port, you may decide whether to 'enable' it in the following two cases:
(1) Please enable it if the switch time demand is very high. Although the switching time has been improved, the drawback is that the packet mechanism will occupy bandwidth.
(2) Please disable it if the switching time requirement is not high.

4.12.2 Advanced Configuration – ERPS - Ring Setting

Configuration Step

1. Select [Advanced / ERPS / Ring Setting] in the navigation bar and enter the ERPS [Ring Setting] interface

Item	Description	Notes
Ring ID	Ring Adding ID <1-255>	
Ring Type	Major-ring / Sub-ring	
Node Type	**Transfer:** Forward both service packets and protocol packets **rpl-owner:** Responsible for blocking traffic over the RPL so that no loops are formed in the Ethernet traffic. There can be only one RPL owner in a ring. **rpl-neighbour:** An Ethernet ring node adjacent to the RPL. It is responsible for blocking its end of the RPL under normal conditions. This node type is optional and prevents RPL usage when protected.	
Protocol VLAN	Adding ring ERPS protocol VLAN	
East Port	A Ring port created on this node	
West Port	Another ring port created on the node	
RPL Port	*Port on an RPL Link **East Port** **West Port**	
Belong Major Ring		
Virtual Channel		
WTR Timer	<1-12> minutes, Default: 1 minutes, Step 1 minutes	
Guard Timer	<10-2000>milliseconds Default:500 milliseconds, Step is 10 milliseconds	
HoldOff Timer	<0-10000>milliseconds Default:0 milliseconds, Step is 100 milliseconds	

4.12.3 Advanced Configuration – ERPS - Ring Information

Configuration Step

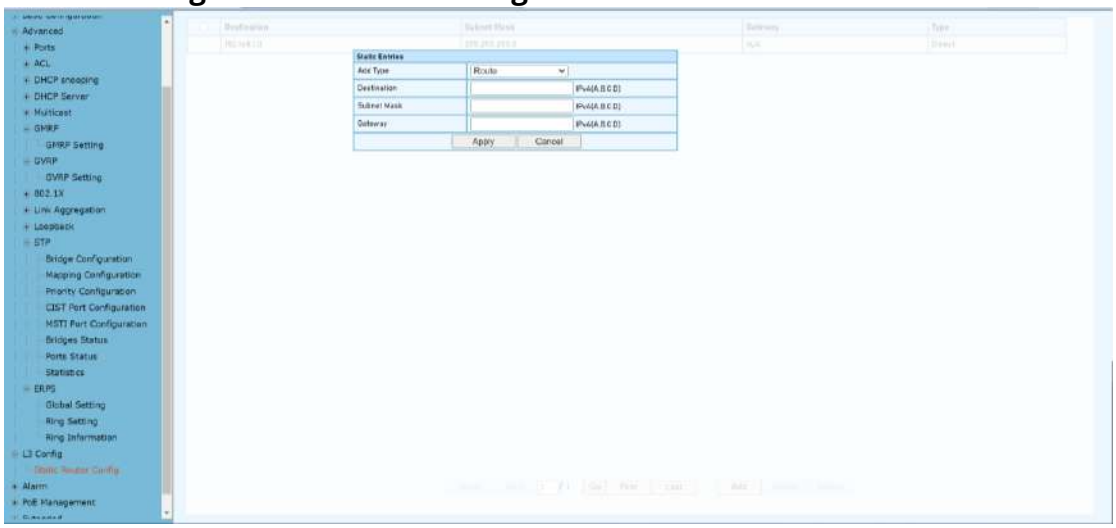
1. Select [Advanced / ERPS / Ring Informations] in the navigation bar to enter the interface of ERPS [Ring Network Information].
2. The ERPS current running information can be viewed in the [Ring Informations] interface.
3. Click [Refresh] to show the latest running information.

Expand | Collapse

Ring ID:1					
Ring Type	major-ring	Node Type	transfer	Protocol Vlan	1
Revertive	revertive	FSM State	protection	Virtual Channel	with
East Port	GE/1/blocking	West Port	GE/2/blocking	Belong Major ring	N/A
Guard Timer	500milliseconds	HoldOff Timer	0milliseconds	WTB Timer	5000milliseconds
WTR Timer	1minutes	Force Switch	Disabled	Manual Switch	Disabled

Refresh

4.13 L3 Config – Static Router Config



Configuration Step

1. Select [Advanced / L3 Config] in the navigation bar to enter the interface of Static Router Config.
2. The Static Router Configuration can be viewed in the [Static Router Config]

interface.
3. Click [Add] to add additional Static Enrties .

4.14 Advanced Configuration – Alarm

4.14.1 Advanced Configuration – Alarm –Relay Setting

Configuration Step

1. Select [Advanced / Alarm / Relay Setting] in the navigation bar to enter the interface of Alarm [Relay Setting].
2. The Alarm Event, Admin Status, Link Status and Alarm Status can be viewed in the [Relay Setting] interface
3 Select [Disabled/Enabled] of admin Status, Click[Apply] to submit the admin status.
4. Click [Refresh] to show the latest running information.

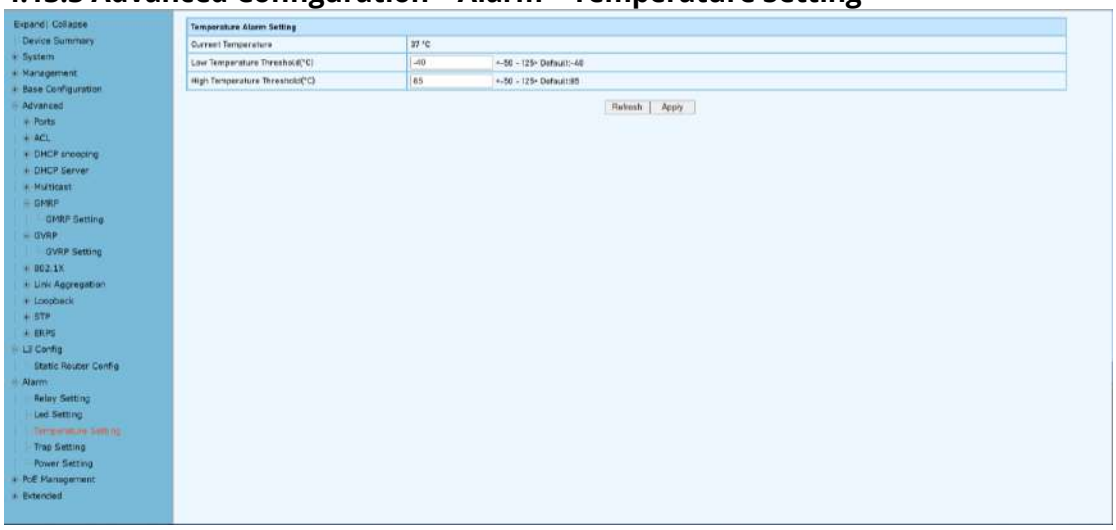
4.13.2 Advanced Configuration – Alarm – Led Setting

Configuration Step

1. Select [Advanced / Alarm / Led Setting] in the navigation bar to enter the interface of Alarm [Led Setting].
2. The Alarm Event, Admin Status, Link Status and Alarm Status can be viewed in the [Led Setting] interface

3 Select [Disabled/Enabled] of admin Status, Click[Apply] to submit the admin status.
4 Click [Refresh] to show the latest running information.

4.13.3 Advanced Configuration – Alarm – Temperature Setting



Configuration Step

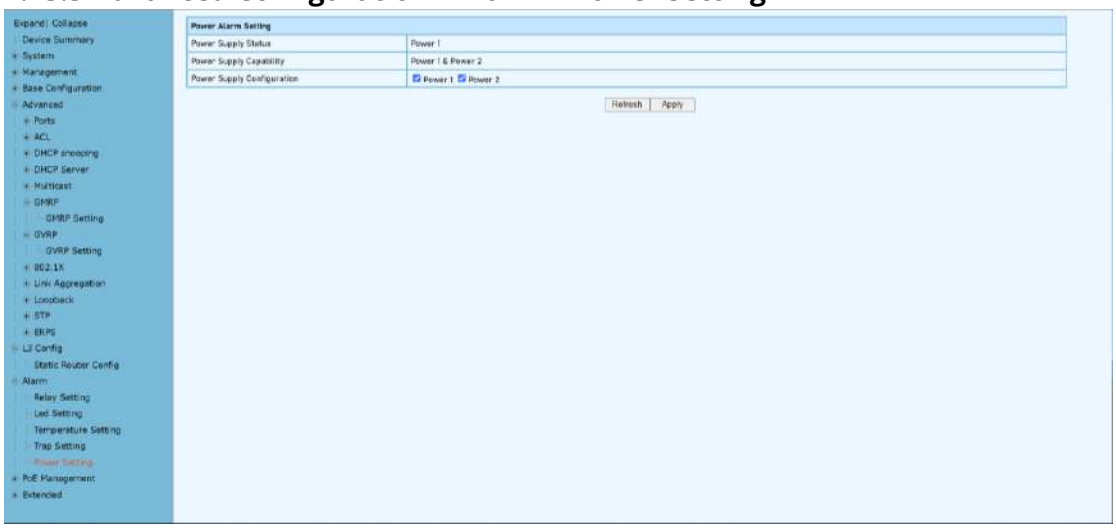
1. Select [Advanced / Alarm /Temperature Setting] in the navigation bar to enter the interface of Alarm [Temperature].
2. The current temperature and temperature setting can be viewed in the [Temperature Setting] interface
3 Enter required temperature value at the Low / High Temperature Threshold(℃), Click[Apply] to submit the modification.
4. Click [Refresh] to show the latest information.

4.13.4 Advanced Configuration – Alarm – Trap Setting

Configuration Step

1. Select [Advanced / Alarm / Trap Setting] in the navigation bar to enter the interface of Alarm [Trap Setting].
2. The Alarm Event, Admin Status, Link Status and Alarm Status can be viewed in the [Trap Setting] interface
3 Select [Disabled/Enabled] of admin Status, Click[Apply] to submit the admin status.
4 Click [Refresh] to show the latest running information.

4.13.5 Advanced Configuration – Alarm – Power Setting

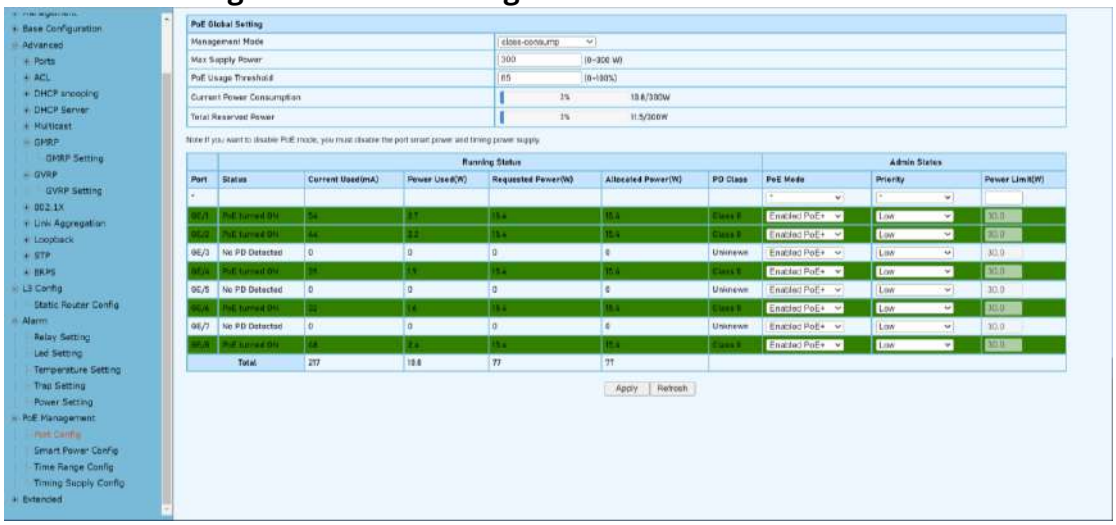


Configuration Step

1. Select [Advanced / Alarm / Power Setting] in the navigation bar to enter the interface of Alarm [Power Setting].

4.15 PoE Management

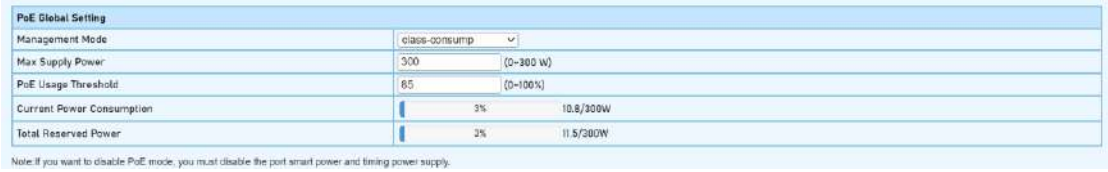
4.15.1 PoE Management – Port Configuration



Configuration Step

1. Select [PoE Management/Port Configuration] in the navigation bar to enter the interface of [Port Configuration].

2. The PoE Port Status and configuration can be viewed in the [Port Configuration] interface.



PoE Global Setting	
Management Mode	class-consump
Max Supply Power	300 (0~300 W)
PoE Usage Threshold	85 (0~100%)
Current Power Consumption	3% 10.8/300W
Total Reserved Power	3% 11.5/300W

Note:If you want to disable PoE mode, you must disable the port smart power and timing power supply.

Item	Description
Management Mode	1) Class-reserved 2) Class-consump 3) Allocated-reserved 4) Allocated-consump **Class**: The corresponding power is allocated according to PD grading, as shown in the figure below: [table below] **Allocated**: A power value is directly assigned to PD regardless of the PD level, and this power value can be set. If PoE+ is enabled, the maximum power is 15.4W. If PoE+ is enabled, The maximum power is 30.0W. **Reserved**: Calculate the total power of the system according to the power allocated to PD. **Consump**: The total system is calculated according to the current power consumed by PD.
PoE Usage Threshold	When the power consumed exceeds this threshold, the interface will display red if the corresponding PoE Max lights will be lightened.
Current Power Consumption	The sum of the power consumption of all PDs as a percentage of the total maximum output power.
Total Reserved Power	Power allocated to PD as a percentage of total power

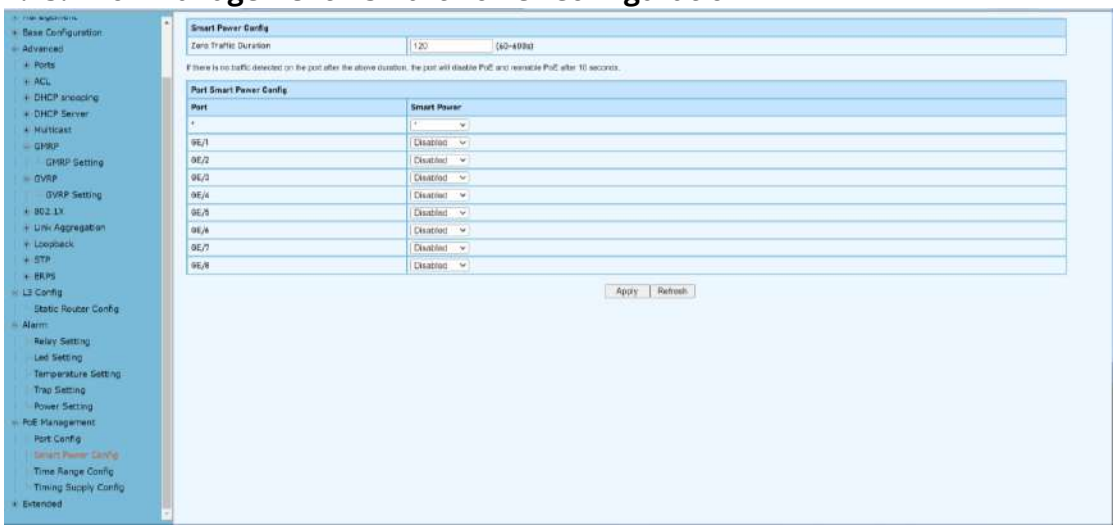
	Class 0	Class 1	Class 2	Class 4	Class 4
Watts	15.4W	4.0W	7.0W	15.4W	30.0W

	Running Status						Admin Status		
Port	Status	Current Used(mA)	Power Used(W)	Requested Power(W)	Allocated Power(W)	PD Class	PoE Mode	Priority	Power Limit(W)
*							*	*	
GE/1	PoE turned ON	54	2.7	15.4	15.4	Class 0	Enabled PoE+	Low	30.0
GE/2	PoE turned ON	44	2.2	15.4	15.4	Class 0	Enabled PoE+	Low	30.0
GE/3	No PD Detected	0	0	0	0	Unknown	Enabled PoE+	Low	30.0
GE/4	PoE turned ON	38	1.9	15.4	15.4	Class 0	Enabled PoE+	Low	30.0
GE/5	No PD Detected	0	0	0	0	Unknown	Enabled PoE+	Low	30.0
GE/6	PoE turned ON	32	1.6	15.4	15.4	Class 0	Enabled PoE+	Low	30.0
GE/7	No PD Detected	0	0	0	0	Unknown	Enabled PoE+	Low	30.0
GE/8	PoE turned ON	48	2.4	15.4	15.4	Class 0	Enabled PoE+	Low	30.0
Total		217	10.8	77	77				

Item	Description
Running Status	Port/Current Used(mA)/Power Used(W)/Requested Power(W)/Allocated Power(W)/PD Class（Class0-4）
Admin Status	**PoE Mode**:(Disable/Enabled PoE/Enabled PoE+) **Priority**: Low(Default), High and Critical When the power consumed by the PD device is greater than the total power that the PSE can provide, it is a means to ensure that key devices can supply power preferentially. When the power supply of the

	PSE equipment is insufficient, if different terminals When the port priorities are the same, the priority is sorted according to the port number, and the port with the smaller port number is given priority to ensure the power supply.
	Power Limit(W):The maximum output power of the port. This value only takes effect when the management mode is Allocated.

4.15.2 PoE Management – Smart Power Configuration



Configuration Step

1. Select [PoE Management/Smart Power Configuration] in the navigation bar to enter the interface of [Smart Power Configuration].
2. The smart power configuration can be viewed in the [Smart Power Configuration] interface.

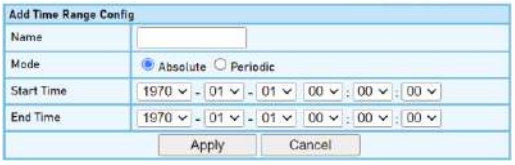
Item	Description
Zero Traffic Duration	If there is no traffic detected on the port after the above duration(Zero Traffic Durtation), the port will disable PoE and reenable PoE after 10 seconds. **Configurable Duration：60-600s**
Smart Power	Disabled/Enable (Default: Disbled)

4.15.3 PoE Management – Time Range and Time Supply Configuration

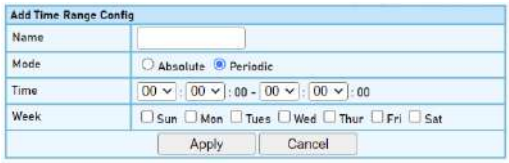
Configuration Step

1. Select [PoE Management/Time Range and Timing Supply Configuration] in the navigation bar to enter the interface of [Time Range and Timing Supply Configuration].
2. The smart poe schedule can be configurate with [Time Range and Timing Supply Configuration] interface.

PoE Schedule Configuraion Step



1. **Enter the name of Time Range**
2. **Select Mode [Absolute / Periodic]**
3. **When selected Absolute mode, also select start time and end time**



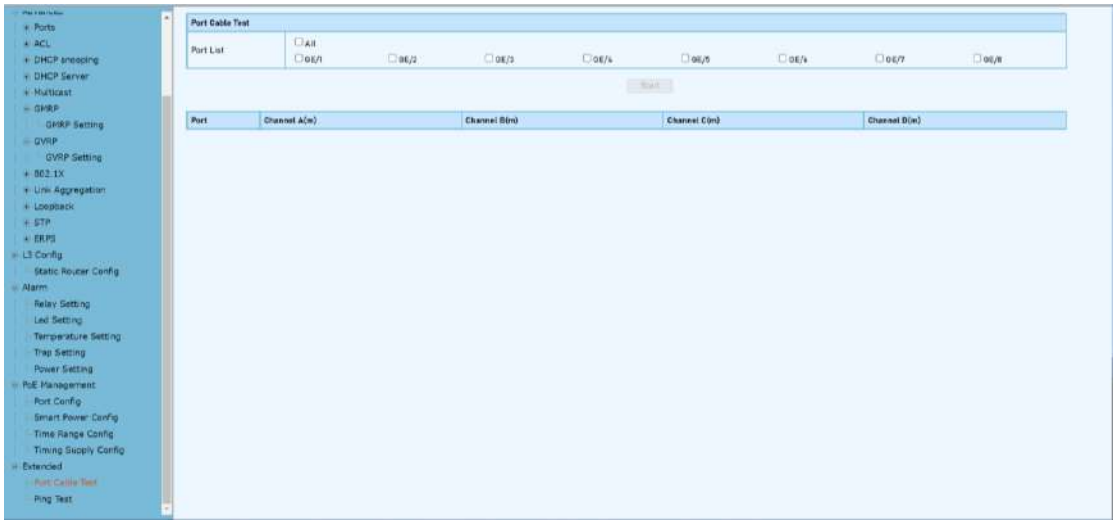
4. **When selected Periodic mode, also select time and week.**

Note: This time is the system time used, so it is best to enable the SNTP client of the switch to synchronize the system time.

4.16 Extended

4.16.1 Extended – Port Cable Setting

You can check the status of copper cables using the time domain reflectometer (TDR). The TDR detects a cable fault by sending a signal through the cable and reading the signal that is reflected back to it. All or part of the signal can be reflected back by any number of cable defects or by the end of the cable itself.

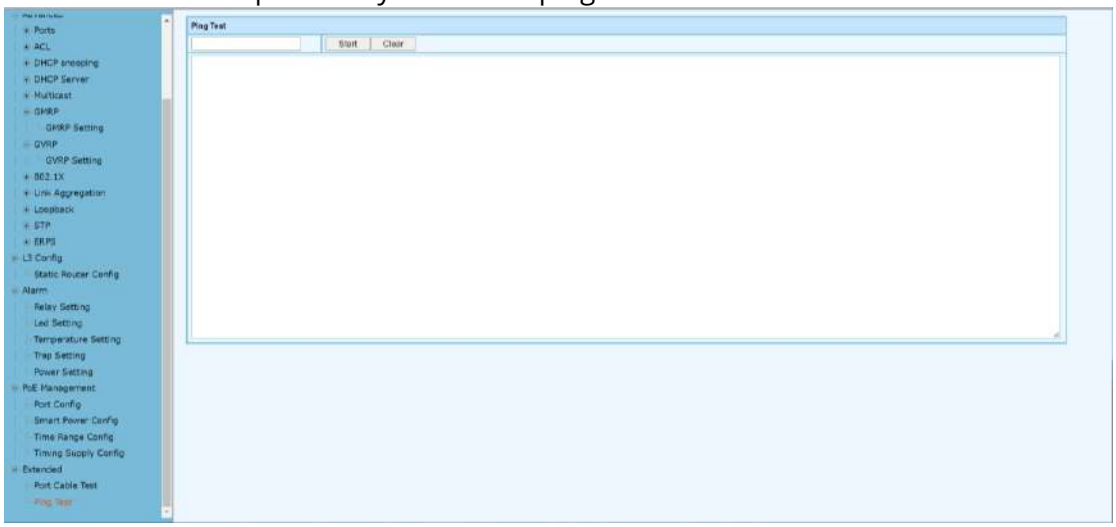


Configuration Step

1. Select [Advanced / Extended /Port Cable Test] in the navigation bar to enter the interface of [Port Cable Test]
2. The Port Cable Setting and Result can be viewed in the [Port Cable Test] interface
3 Select needed test port at the port list ,Click[Start] to submit the testing.

4.16.2 Extended – Ping Test

The easiest way to ping a specific port is to use the telnet command followed by the IP address and the port that you want to ping.



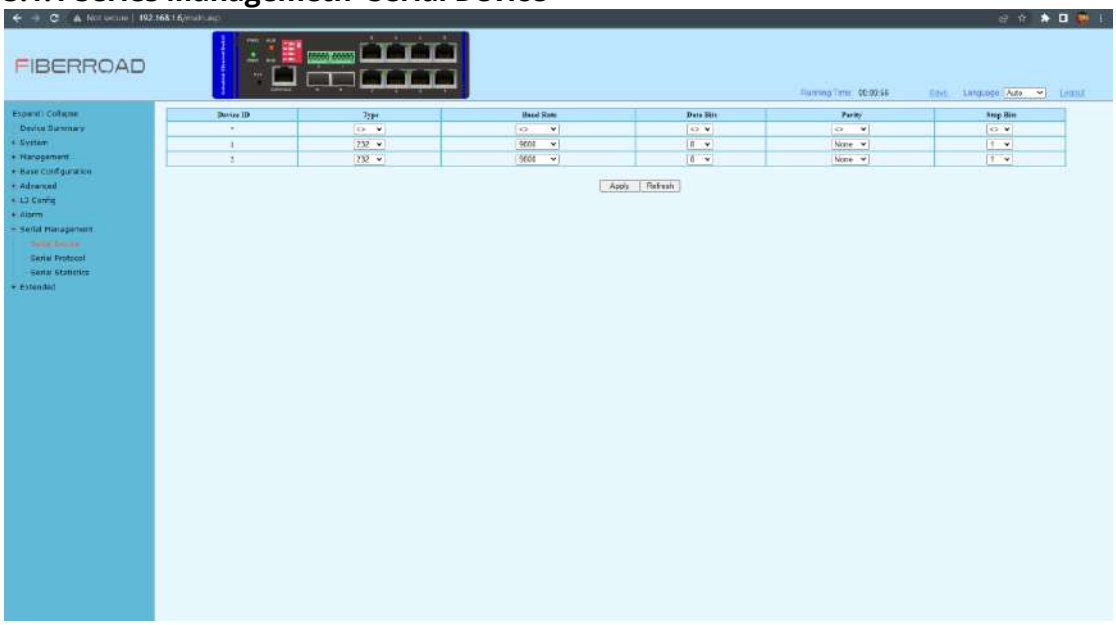
Configuration Steps

1. Select [Advanced / Extended /Ping Test] in the navigation bar to enter the interface of [Ping Test].
2. The ping test configuration and process can be viewed in the [Ping Test] interface
3 Enter destination address, Click[Start] to submit the ping test, all the command can be viewed at the below blank.
4. Click [clean] to clean all of the command at the blank..

5 Extension

5.1 Series Management

5.1.1 Series Managemetn- Serial Device

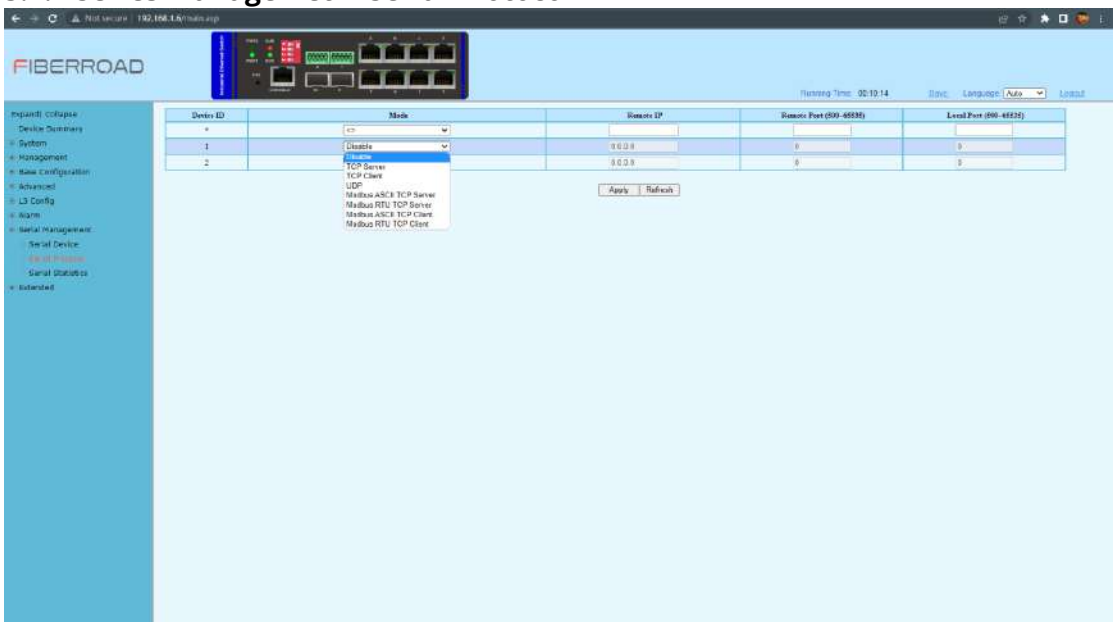


Configuration Steps

1. Select [Serial Management /Serial Device] in the navigation bar to enter the interface of Serial Management [Serial Device].
2. The serial ports configuration can be viewed in the [Serial Device] interface
3. Select required Type, Baud Rate, Data Bits, Parity, Stop Bits , Click[Apply] to submit the modification.
4. Click [Refresh] to show the latest information

Item	Description
Type	Type of serial ports **<232/422/485>**
Baud Rate	To make two devices compatible with each other baud rate is mentioned in the serial communication so that the transmission becomes easy and error free. **<2400-115200>**
Data Bits	The data bits transferred through a serial port might represent device commands, sensor readings, error messages, and so on. <5-8>
Parity	Parity is a method of detecting errors in transmission. When parity is used with a serial port, an extra data bit is sent with each data character, arranged so that the number of 1 bits in each character, including the parity bit, is always odd or always even. **<None/Odd/Even>**
Stop Bits	The stop bit is used to signal the end of a frame. The data is contained in the data bits and the parity bit is an extra bit that is often used to detect transmission errors. **<1/2>**

5.1.2 Series Managemetn- Serial Protocol



Configuration Steps

1. Select [Serial Management /Serial Protocol] in the navigation bar to enter the interface of Serial Management [Serial Protocol].
2. The serial ports protocol can be viewed in the [Serial Protocol] interface
3 Select required Mode, Remote IP, Remote Port, Local Port Click[Apply] to submit the modification.
5. Click [Refresh] to show the latest information.

Item	Description
Mode	**Disable** **TCP Server:** Stream the serial communication through TCP/IP protocol **TCP Client:** TCP Client will connect to server to realize data transmission between the serial port device and server. **UDP:** In UDP Mode, you can unicast or multiunicast data from a serial device to one or multiple host computers. **Modbus ASCII TCP Server** **Modbus RTU TCP Server** **Modbus ASCII TCP Client** **Modbus RTU TCP Client**
Remote IP	**As needed**
Remote Port	**<500-65535>**
Local Port	**<500-65535>**

NOTE: The original Modbus specification included two possible transmission modes: ASCII and RTU. Modbus RTU mode is the most common implementation, using binary coding and CRC error-checking. Modbus ASCII messages (though somewhat more readable because they use ASCII characters) is less efficient and uses less effective LRC error checking. ASCII mode uses ASCII characters to begin and end messages whereas RTU uses time gaps (3.5 character times) of silence for framing.

The two modes are incompatible so a device configured for ASCII mode cannot communicate with one using RTU. Modbus ASCII messages require twice as many bytes to transmit the same content as a Modbus RTU message

5.1.3 Series Managemetn- Serial Statistics

Configuration Steps

1. Select [Serial Management /Serial Statistic] in the navigation bar to enter the interface of Serial Management [Serial Statistics].
2. The serial ports setatistics can be viewed in the [Serial Protocol] interface.
3. Click [Clear All] to restart the staticstics .
4. Click [Refresh] to show the update statistics information.

The information in this document is subject to change without notice. Fiberroad has made all effects to ensure the accuracy of the information, but all information in this document does not constitute any kind of warranty. If you have any questions please feel free to contact to us.

Fiberroad Technology Co., Limited
www.fiberroad.com
Sales Support: sales@fiberroad.com
Technical Support: support@fiberroad.com
Service Support: service@fiberroad.com