



SMART INDUSTRIAL ETHERNET SWITCH

Web GUI User Manual

Ver. 3.0.0



About This Manual

Introduction

This document chapter includes an introduction to the Fiberroad Industrial Ethernet products family,

Conventions

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

Figures and Screen Captures

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

Copyright©2021 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, 2021

Version number: 3.0.0

CONTENTS

Revision History	7
Chapter 1 System Configurations	8
1. About Web-GUI Management.....	8
1.1 Preparing for Web Management	8
1.2 Device Summary	9
1.3 System-Administrations.....	9
1.3.2 System - Online Users.....	10
1.3.3 Management Setting.....	10
1.4 System - Router Table	11
1.4.1 System – Router Table – Static Entries	11
1.4.2 Router Table – Route Table	11
1.5 System Log	12
1.5.1 System Log – Setting.....	12
1.5.2 System Log – View.....	14
1.6 Configurations.....	15
1.6.1 Configurations - View.....	15
1.6.2 Configurations – Import	15
1.6.3 Configurations – Export.....	16
1.6.4 Configurations – Restore Factory Default.....	16
1.6.5 Configurations – Date & Time	17
1.6.6 Configurations – Device Status	18
1.6.7 Configurations – ARP Table	19
1.6.8 Configurations – Software Upgrade	19
1.6.9 Configurations – Reboot.....	20
Chapter 2 Management Configurations	21
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.....	29
2.3.1 Management – LLDP - Global Setting.....	29
2.3.2 Management – LLDP – Port Configurations.....	30
Chapter 3 Base Configuration	32
3 Base Configuration	32
3.1.1 Base Configuration-Port-Status And Setting.....	32
3.1.2 Base Configuration-Port-Statistics.....	34
3.1.3 Base Configuration-Port-SFP Information	35
3.1.4 Base Configuration-Port-SFP Detail Information.....	36
3.1.5 Base Configuration-Port-Traffic	36
3.2 Base Configuration - VLAN.....	37
3.2.1 Base Configuration-VLAN-Basic Setting	37
3.2.2 Base Configuration-VLAN-Port Setting.....	38
3.2.3 Base Configuration-VLAN-Double VLAN	40
3.3 Base Configuration-QoS	40
3.3.1 Base Configuration-QoS- Mapping -802.1p Priority.....	40
3.3.2 Base Configuration-QoS- Mapping – DSCP Priority.....	41
3.3.3 Base Configuration-QoS- Mapping – Local Priority	42
3.4 Base Configuration-QoS- Ports.....	43
3.4.1 Base Configuration-QoS- Ports-Port Priority	43
3.4.2 Base Configuration-QoS- Ports-Rate Limitation	44
3.5 Base Configuration-FDB Table.....	45
3.5.1 Base Configuration-FDB Table- Configuration – Aging Setting	45
3.5.2 Base Configuration-FDB Table- Configuration – Static Mac Entry	46
3.5.3 Base Configuration-FDB Table- Configuration – Port Learning Ability	47
3.5.4 Base Configuration-FDB Table- FDB Table.....	48
3.5.5 Base Configuration-FDB Table- Delete Entries	49
3.5.6 Base Configuration-FDB Table- Port Mirror	50
3.5.7 Base Configuration-FDB Table- Port Isolate	51
3.5.8 Base Configuration-FDB Table- Storm Filters	51
Chapter 4 Advanced Configurations.....	53
4. Advanced Configuration.....	53

4.1 Advanced Configuration – Ports – Ports Security	53
4.2 Advanced Configuration – ACL	54
4.2.1 Advanced Configuration – ACL – ACL Group Setting.....	54
4.2.2 Advanced Configuration – ACL – ACL Rule Setting	56
4.3 Advanced Configuration – DHCP snooping	58
4.3.1 Advanced Configuration – DHCP snooping – Global Setting.....	58
4.3.2 Advanced Configuration – DHCP snooping – Port Setting.....	59
4.3.3 Advanced Configuration – DHCP snooping – Binding Table	60
4.4 Advanced Configuration – DHCP Server	60
4.4.1 Advanced Configuration – DHCP Server – Global Setting.....	60
4.4.2 Advanced Configuration – DHCP Server – IP Address Pool	61
4.4.3 Advanced Configuration – DHCP Server – IP Address Lease Information	62
4.5 Advanced Configuration – Multicast	63
4.5.1 Advanced Configuration – Multicast – Manual Address Setting	63
4.5.2 Advanced Configuration – Multicast – IGMP snooping Global Setting	64
4.5.3 Advanced Configuration – Multicast – IGMP snooping VLAN setting ...	65
4.5.4 Advanced Configuration – Multicast – IGMP snooping IP Groups	67
4.5.5 Advanced Configuration – Multicast – IGMP snooping MAC Groups ..	67
4.5.6 Advanced Configuration – Multicast – IGMP snooping Multicast Table	68
4.6 Advanced Configuration – GMRP	68
4.6.1 Advanced Configuration – GMRP– GMRP Setting.....	68
4.7 Advanced Configuration – GVRP.....	70
4.7.1 Advanced Configuration – GVRP – GVRP Setting.....	70
4.8 Advanced Configuration – 802.1X	71
4.8.1 Advanced Configuration – 802.1X – Authentication Server	71
4.8.2 Advanced Configuration – 802.1X – Global Setting	72
4.8.3 Advanced Configuration – 802.1X – Port Configurations.....	73
4.8.4 Advanced Configuration – 802.1X – User Authentication Info	75
4.9 Advanced Configuration – Link Aggregation	76
4.9.1 Advanced Configuration – Link Aggregation – Global Setting	76
4.9.2 Advanced Configuration – Link Aggregation – Port Configurations	77

4.9.3 Advanced Configuration – Link Aggregation – Aggregation Information	78
4.10 Advanced Configuration – Loopback	79
4.10.1 Advanced Configuration – Loopback – Global Setting	79
4.10.2 Advanced Configuration – Loopback – Port Configuration	80
4.11 Advanced Configuration – STP	81
4.11.1 Advanced Configuration – Global Setting	81
4.11.2 Advanced Configuration – Port Configuration	82
4.11.3 Advanced Configuration – STP Information	84
4.11.3 Advanced Configuration – STP Information	84
4.12 Advanced Configuration – ERPS	85
4.12.1 Advanced Configuration – Global Setting	85
4.12.2 Advanced Configuration – ERPS - Ring Setting	86
4.12.3 Advanced Configuration – ERPS - Ring Information.....	87
4.13 Advanced Configuration – Alarm.....	88
4.13.1 Advanced Configuration – Alarm – Relay Setting	88
4.13.2 Advanced Configuration – Alarm – Led Setting	88
4.13.3 Advanced Configuration – Alarm – Temperature Setting.....	89
4.13.4 Advanced Configuration – Alarm – Trap Setting	90
4.13.5 Advanced Configuration – Alarm – Power Setting.....	90
4.14 Advanced Configuration – Extended.....	91
4.14.1 Advanced Configuration – Extended – Port Cable Setting.....	91
4.14.2 Advanced Configuration – Extended – Ping Test.....	92

Revision History

Version	Date	Author	Reasons of Change	Section(s) Affected
1.0	2017/12/04		Initial Release	All
2.0	2018/05/18		SNMPv3, EEE	SNMP, Basic Configuration
2.1	2018/10/20		Definition of name	All
3.0	2020/11/1		ERPS Ring Setting	ERPS



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 industrial switch on the network and make sure that any one of the PCs on the network can connect with the industrial switch through the web browser.

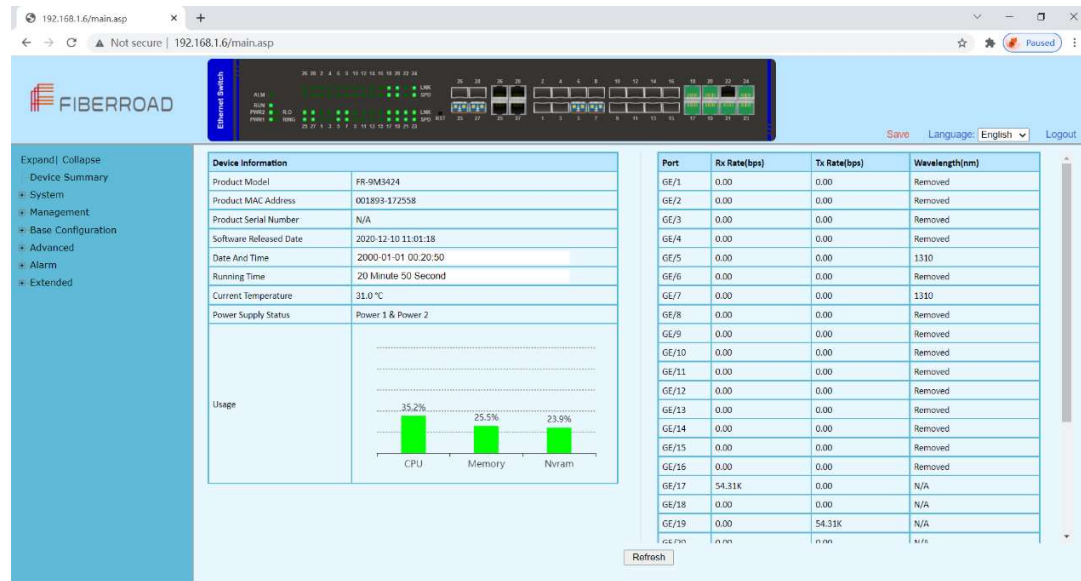
The industrial switch default value of IP, subnet mask, username and password are listed as below:

- ❖ 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.



1.3 System-Administrations

Add Users and its level, status and description.

The screenshot shows the FiberRoad web interface for a device at 192.168.1.6. The left sidebar contains navigation links: Expand/Collapse, Device Summary, System, Management, Base Configuration, Advanced, Alarm, and Extended. The main content area is divided into two sections:

- System-Administrations:** A table showing existing users.
- Add User:** A dialog box for adding a new user.

The 'Add User' dialog box contains the following fields:

- Name:
- Password:
- Confirm Password:
- Level:
- Status:
- Description:

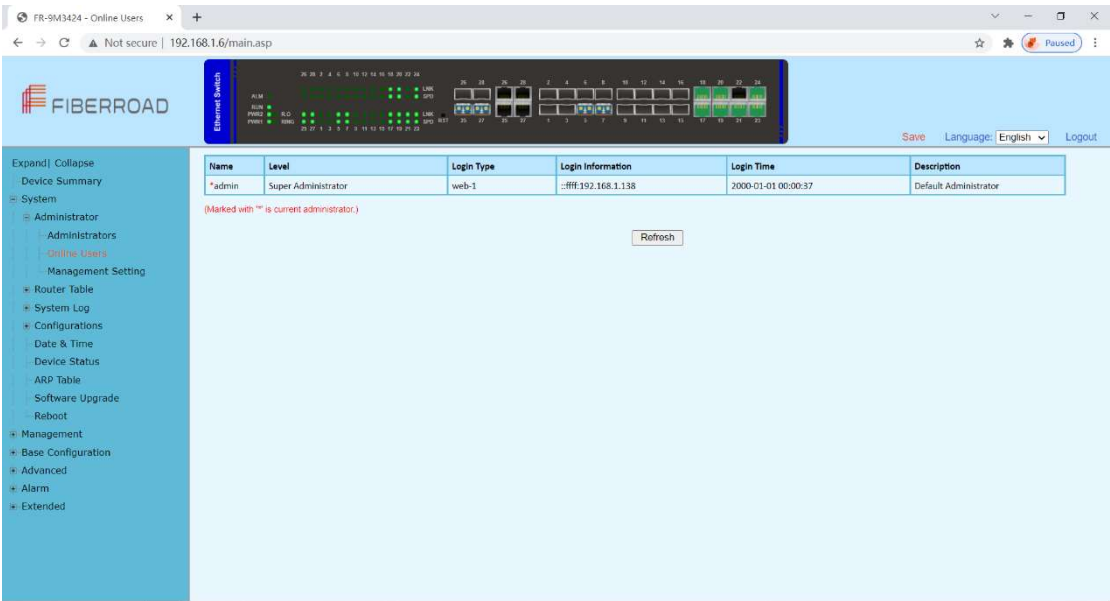
The 'Add User' button is highlighted in blue.

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

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

1.3.2 System - Online Users

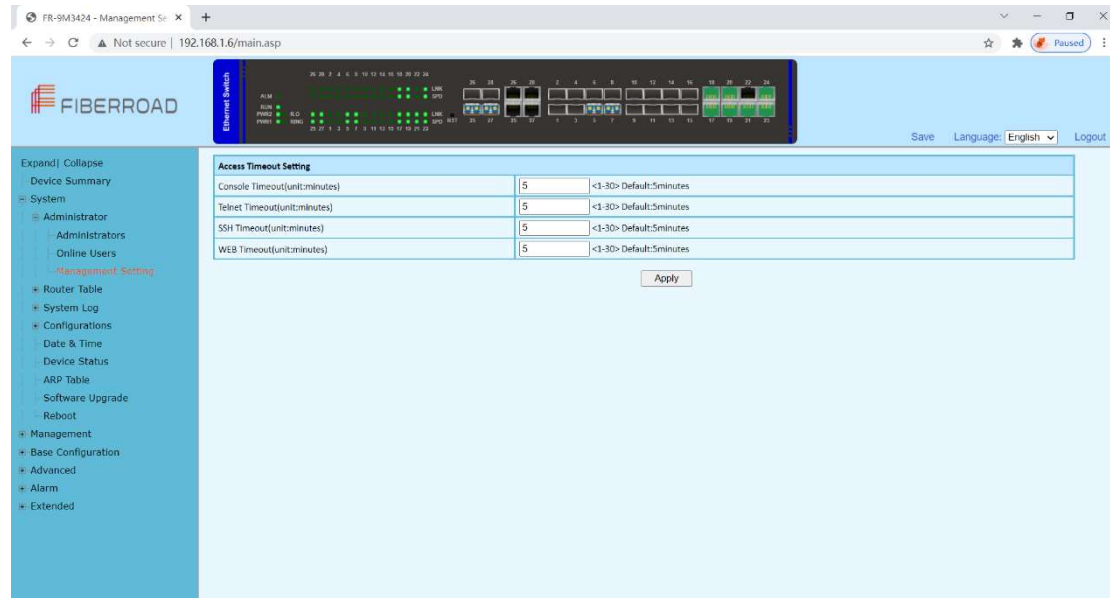
Overview online users information



Remarks: 1, Only super administrator have this privilege.

1.3.3 Management Setting

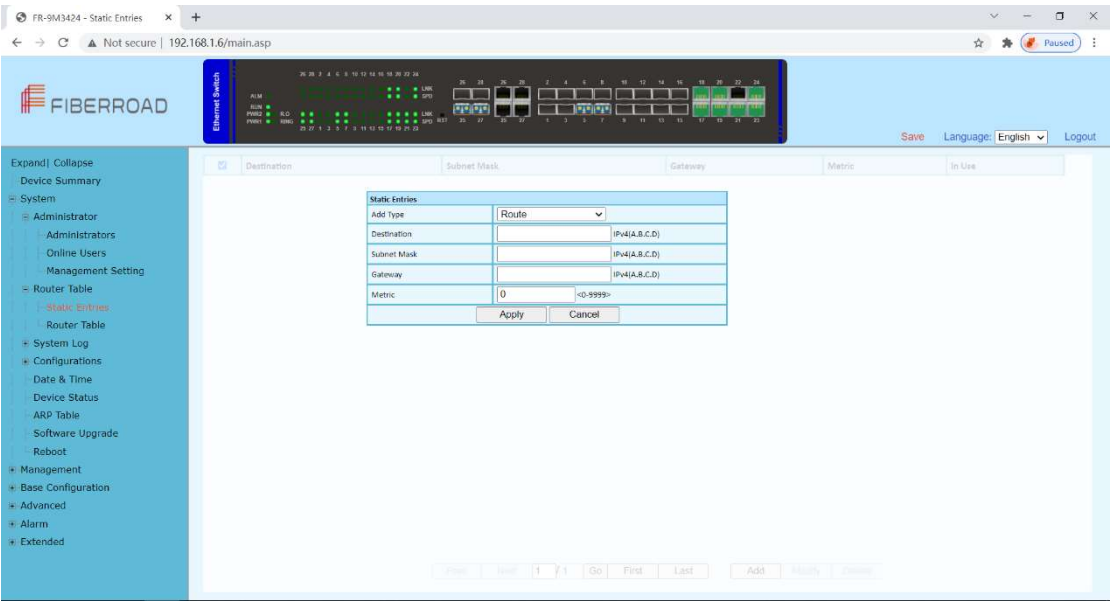
Access Timeout Setting



	Item	Description	Notes
	Consolt Timeout	1-30	Default:5 minutes
	Telnet Timeout	1-30	Default:5 minutes
	SSH Timeout	1-30	Default:5 minutes
	WEB Timeout	1-30	Default:5 minutes

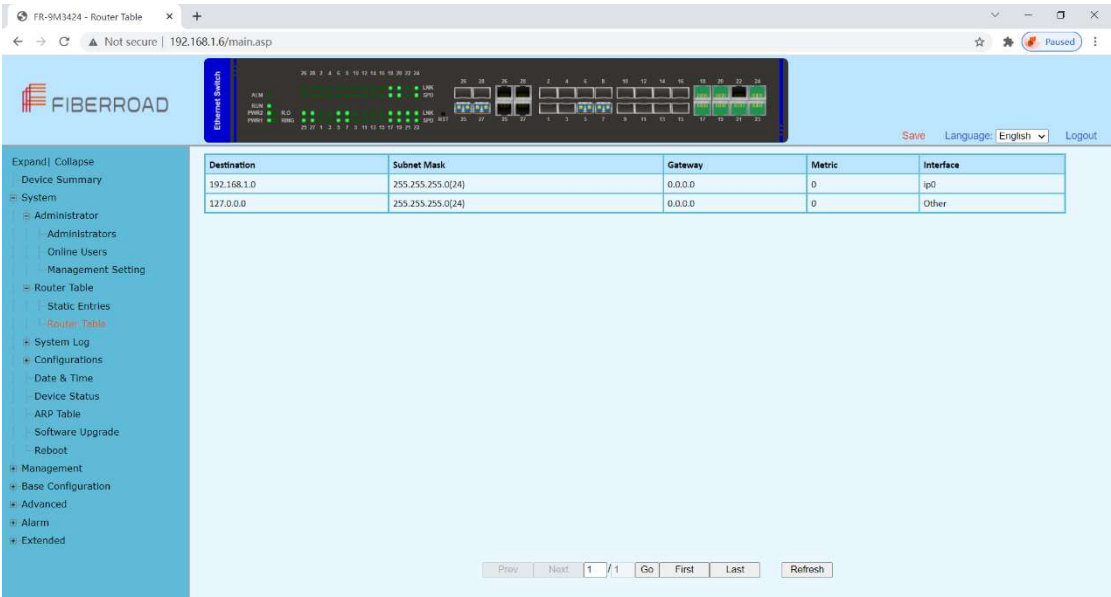
1.4 System - Router Table

1.4.1 System – Router Table – Static Entries



Item	Description	Notes
Add Type	Route/Default Route	
Destination	IPv4(A.B.C.D)	
Subnet Mask	IPv4(A.B.C.D)	
Gateway	IPv4(A.B.C.D)	
Metric	0-9999	

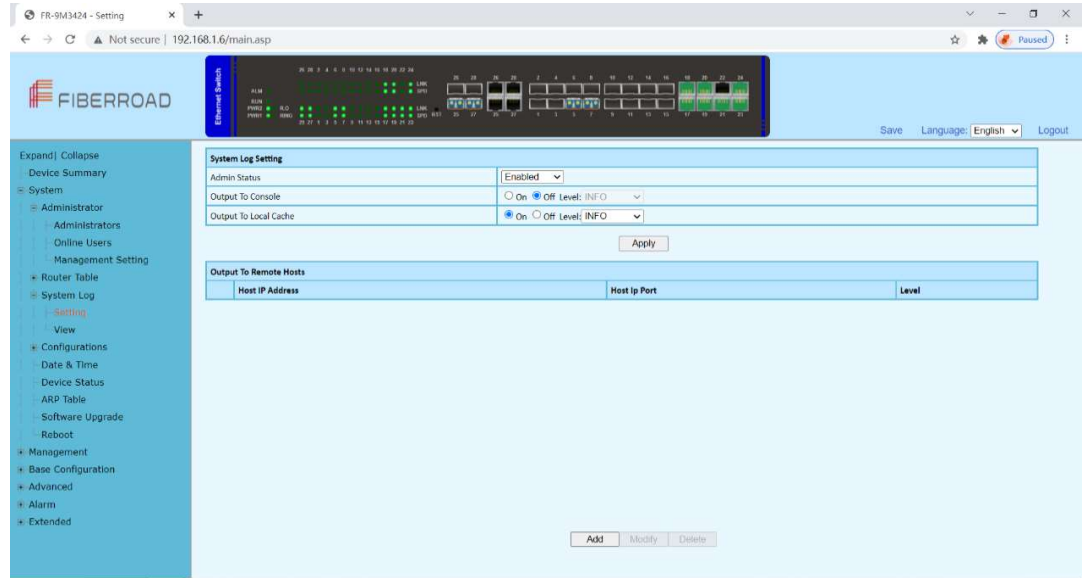
1.4.2 Router Table – Route Table



1.5 System Log

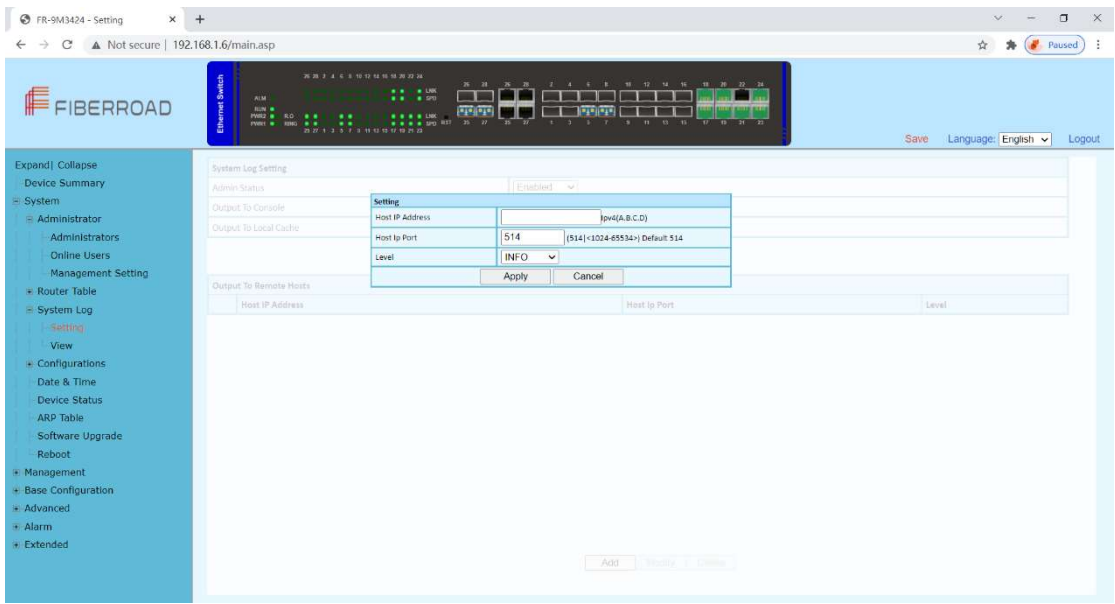
1.5.1 System Log – Setting

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 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	Default: INFO

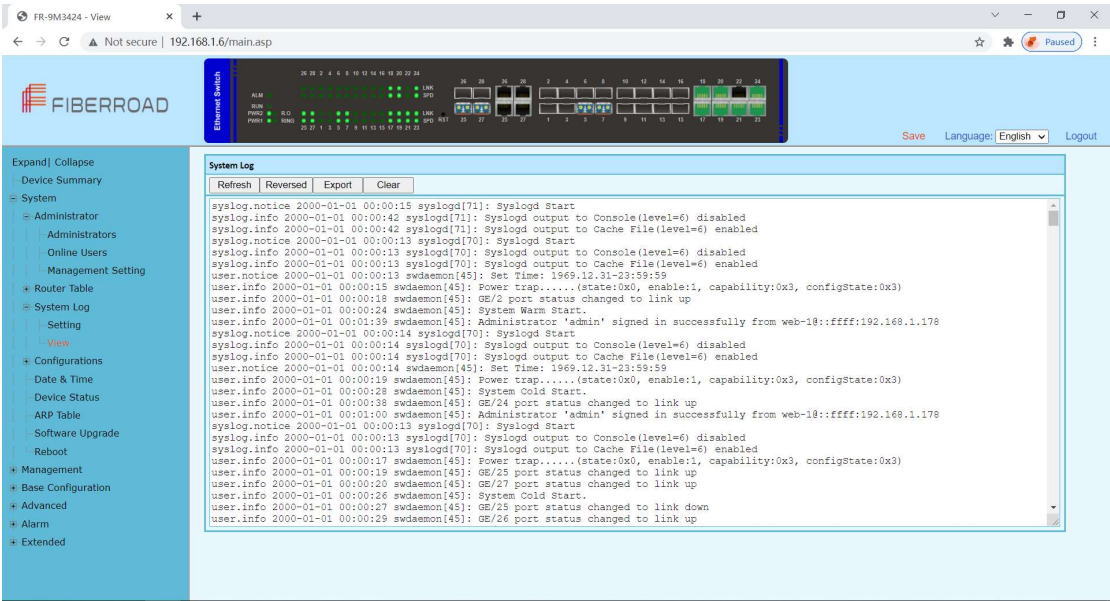
Click the “Add” button, to the output to remote hosts setting.



Item	Description	Notes
Host IP Address	Remote log host IP address	N/A
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 WARNING : Level 4, Warning Status NOTICE : Level 5, normal but important state INFO : Level 6, Notification Event DEBUG : Level 7, debugging information	Default: INFO

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.

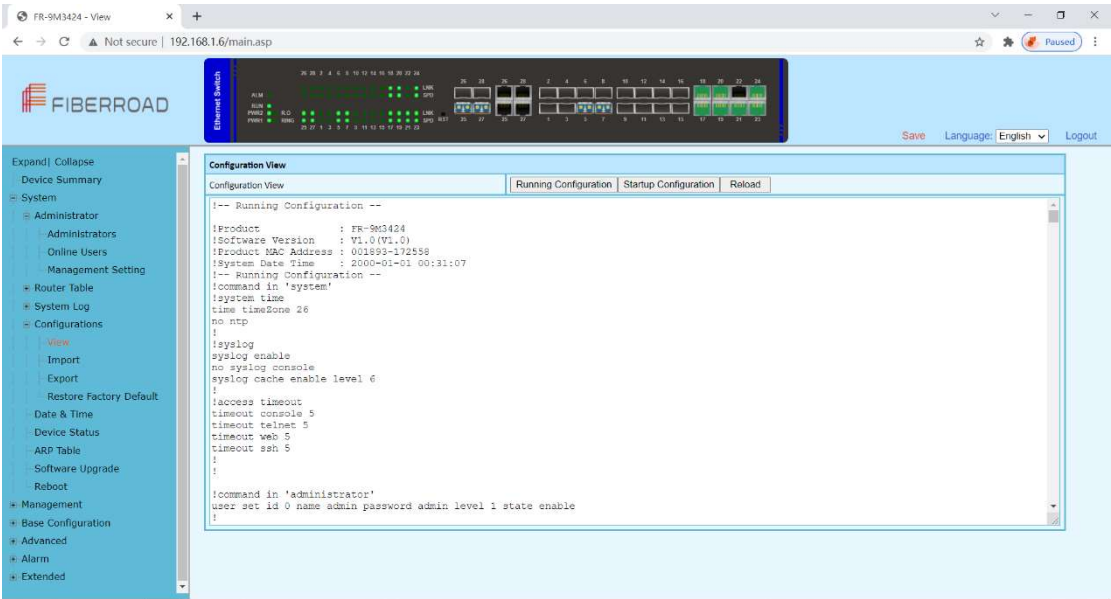
1.5.2 System Log - View



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 the contents of the system log	

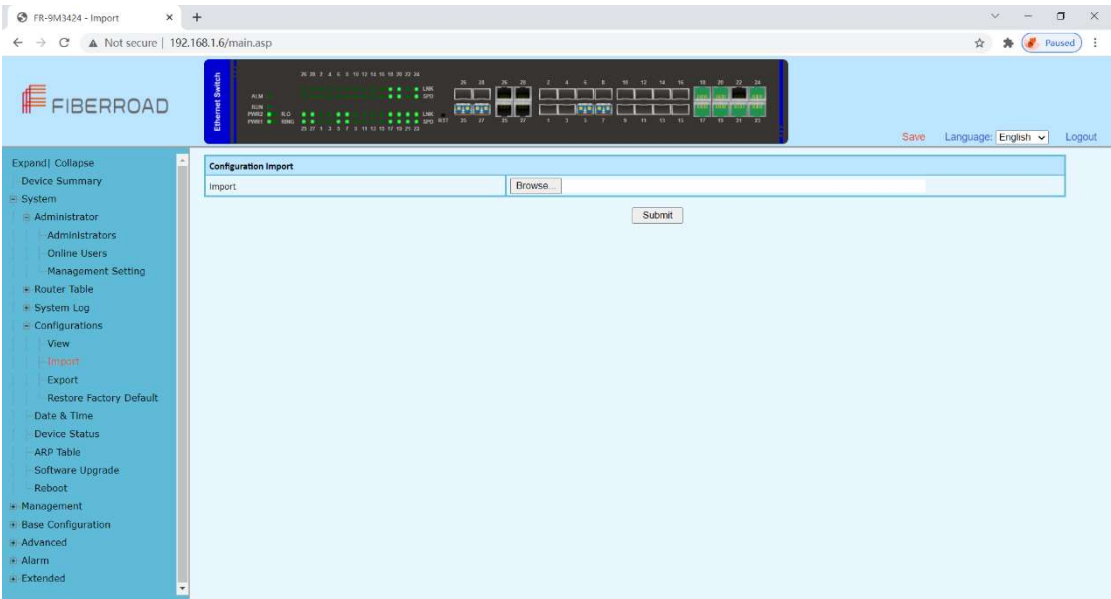
1.6 Configurations

1.6.1 Configurations - View



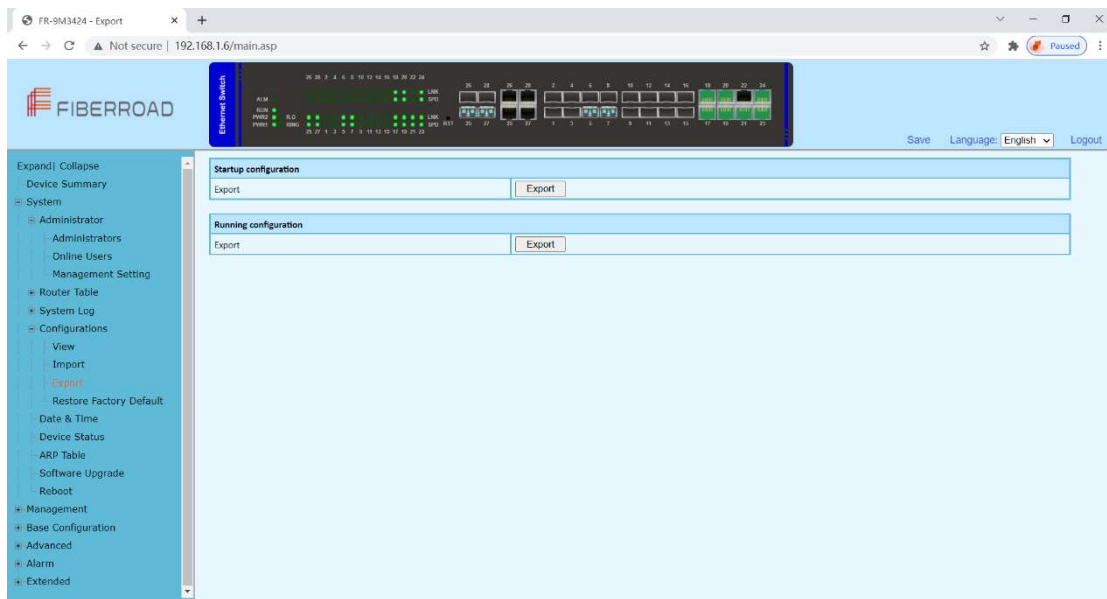
Item	Description	Notes
Running Configuration	Show system running configuration	Text Style
Startup Configuration	Show system startup configuration	Text Style
Reload	Reload the running or startup configuration	

1.6.2 Configurations - Import



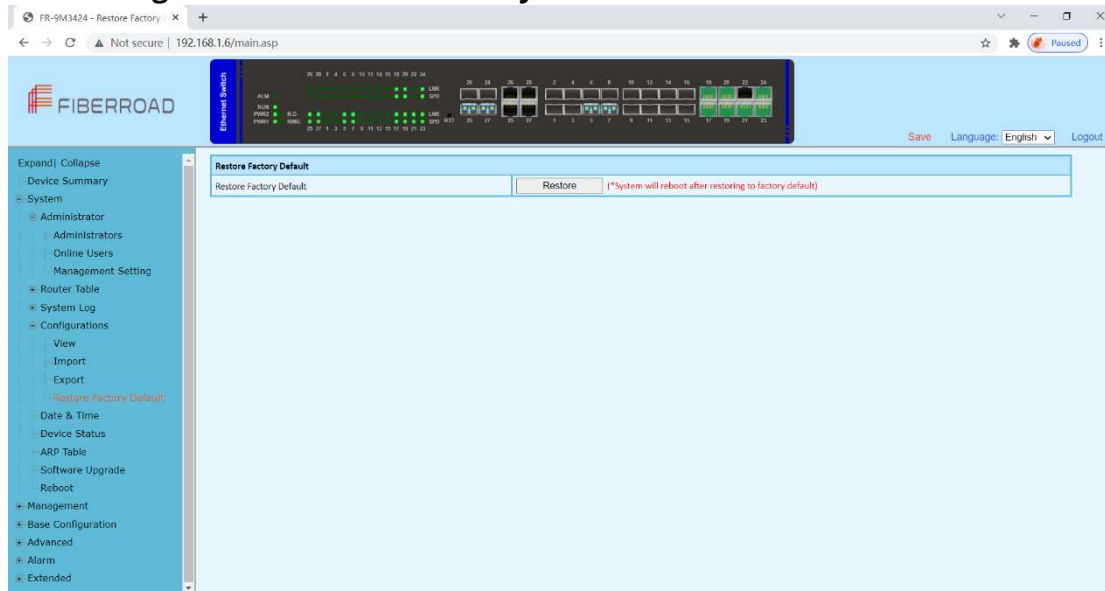
Remarks: 1, In the Configurations [Import] interface, click [Browse], select the configuration file to import, and click [Submit] to start the import.

1.6.3 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.

1.6.4 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.

1.6.5 Configurations – Date & Time

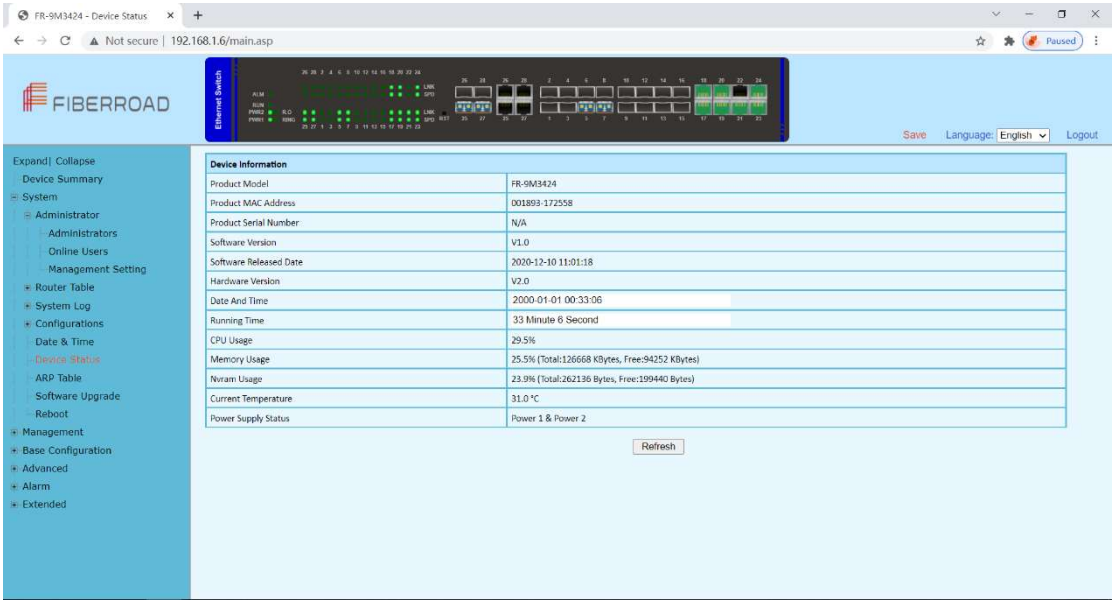
Item	Description	Notes
System Time	Display the actual effective system time.	Read Only
Time Zone	System time zone setting, select any time zone from the drop-down list.	
Manual Set Time	It can be set after the SNTP client is disabled. The year range is 1970-2037. Others are the same as the common settings.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

Item	Description	Notes
Synchronous Mode	Unicast Multicast Broadcast	These three modes are multi-selectable, but at least one must be selected
IP	IP address of 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 mode

Sync now

SNTP client immediate synchronize times

1.6.6 Configurations – Device Status

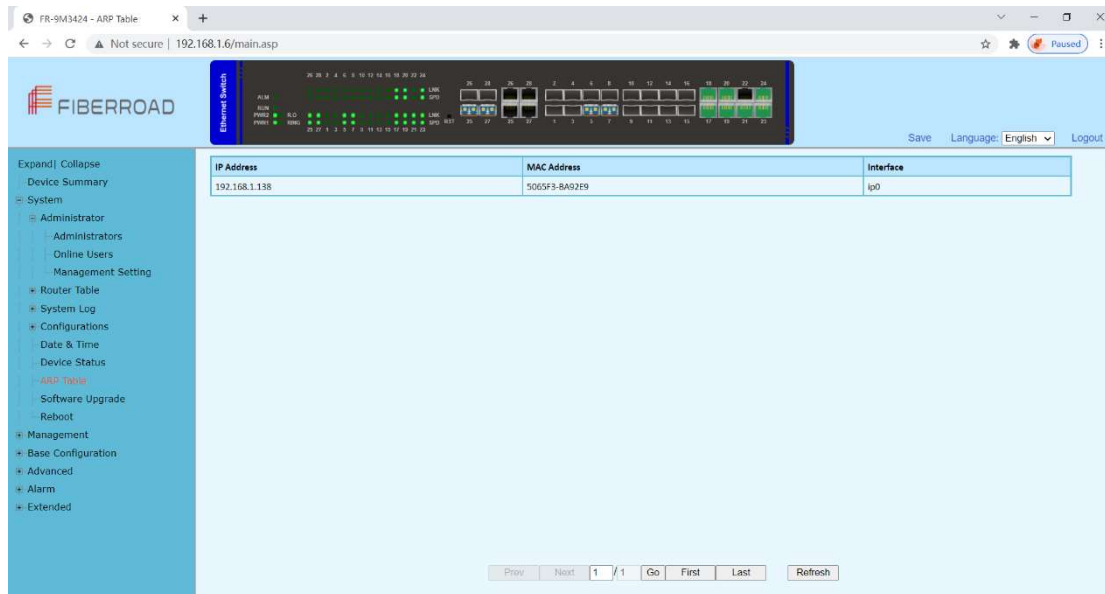


In the [Device Status] interface, the basic information and the operating status information of the device system are displayed.

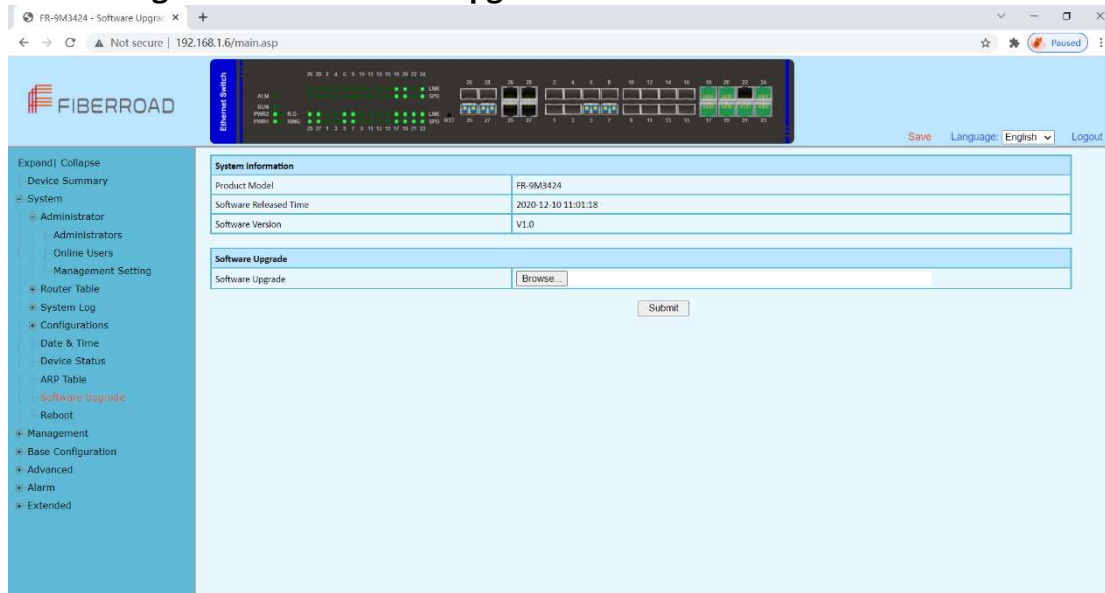
Item	Description	Notes
Product Model	The device mode	Read Only
Product MAC Address	The device MAC address	Read Only
Product Serial Number	The device product serial number	Read Only
Software Version	The software version running on	Read Only
Software Released Date	The time when running the software	Read 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

1.6.7 Configurations – ARP Table

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



1.6.8 Configurations – Software Upgrade



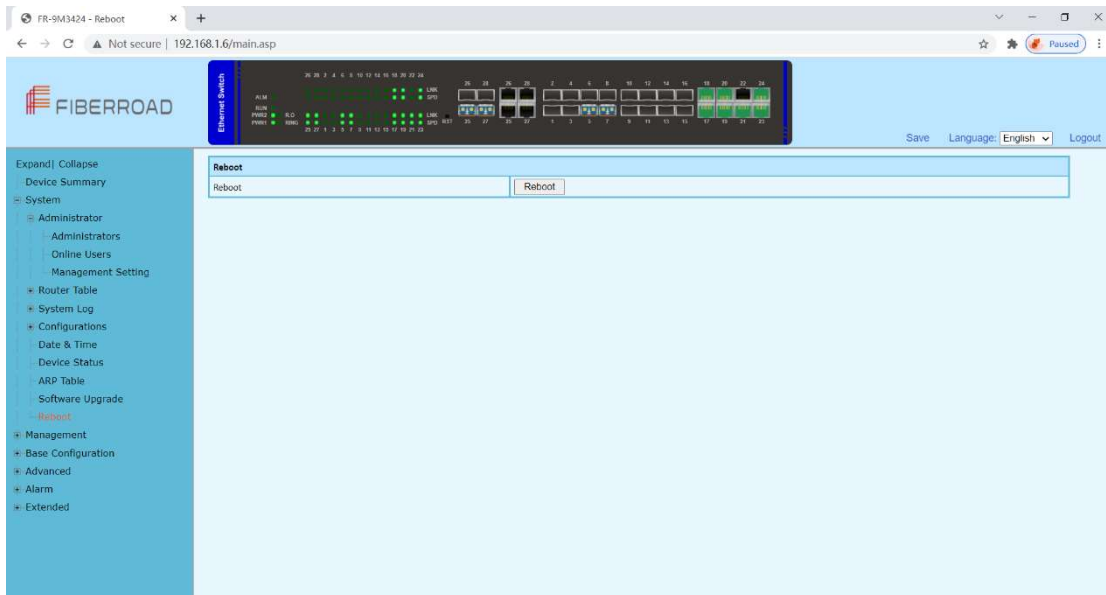
Configuration Step

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.

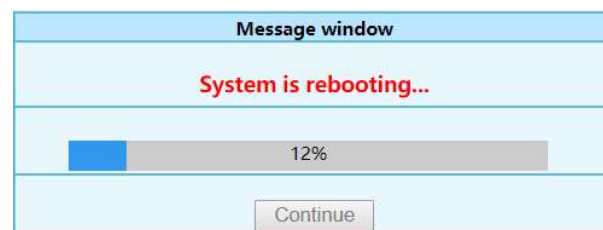
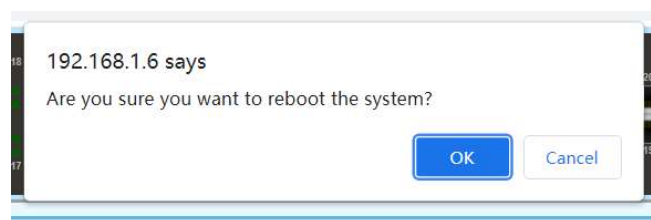
2, During the software upgrade, make sure that the device is powered up until the upgrade is completed.

1.6.9 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

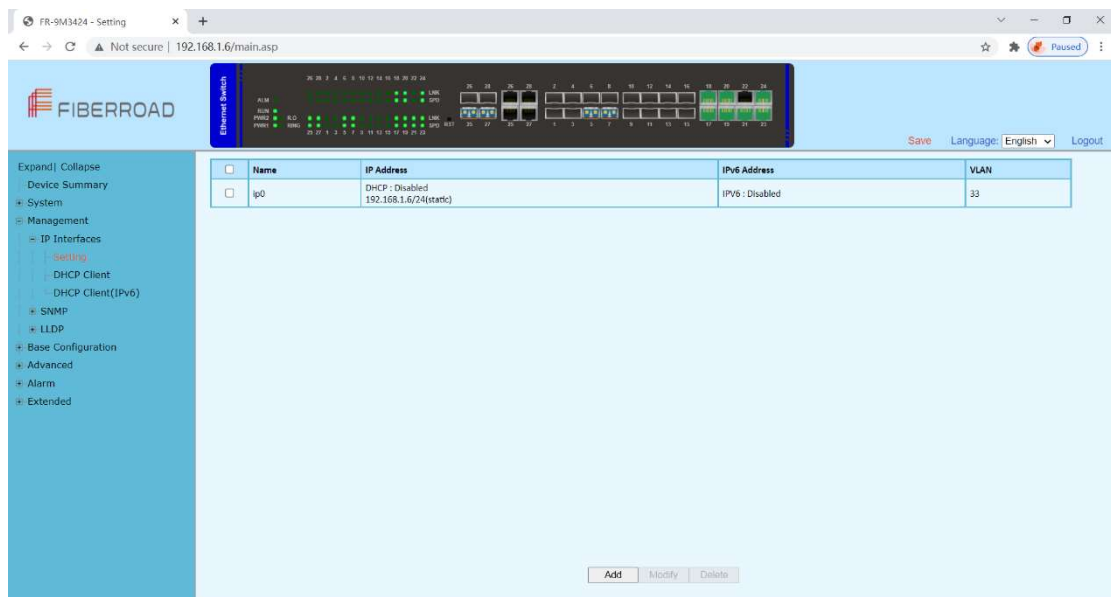
This chapter describes the port configuration in detail, including but not limit to the following:

- ❖ 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	<input type="text"/>	IPv4(A.B.C.D)
Subnet Mask	<input type="text"/>	IPv4(A.B.C.D)
VLAN	<input type="text"/>	<1-4094>
<input type="button" value="Apply"/> <input type="button" value="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>

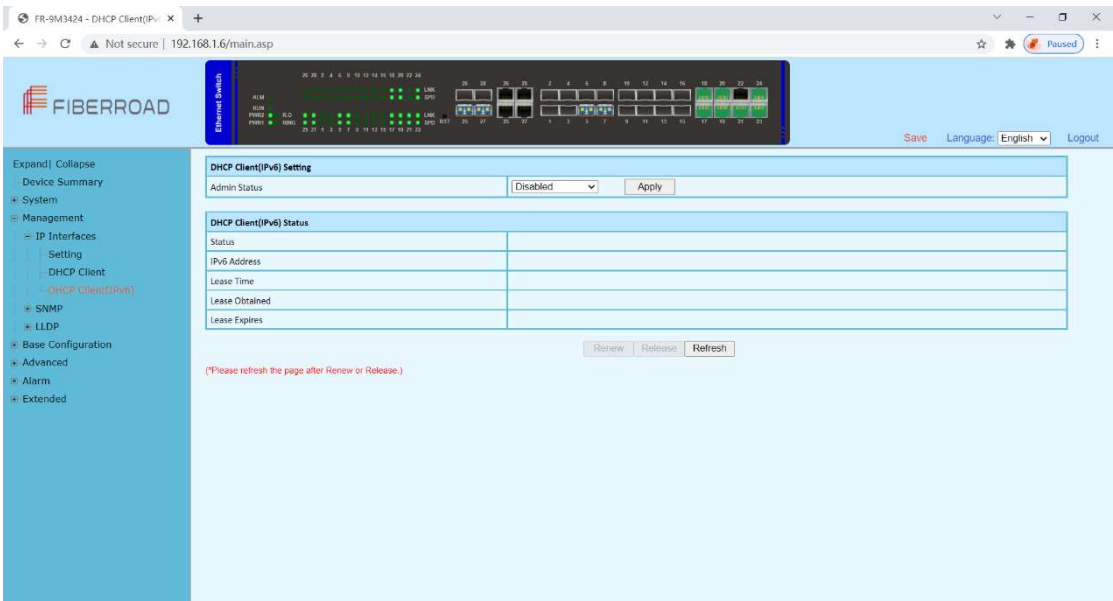
2.1.2 Management – IP Interfaces – DHCP Client

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

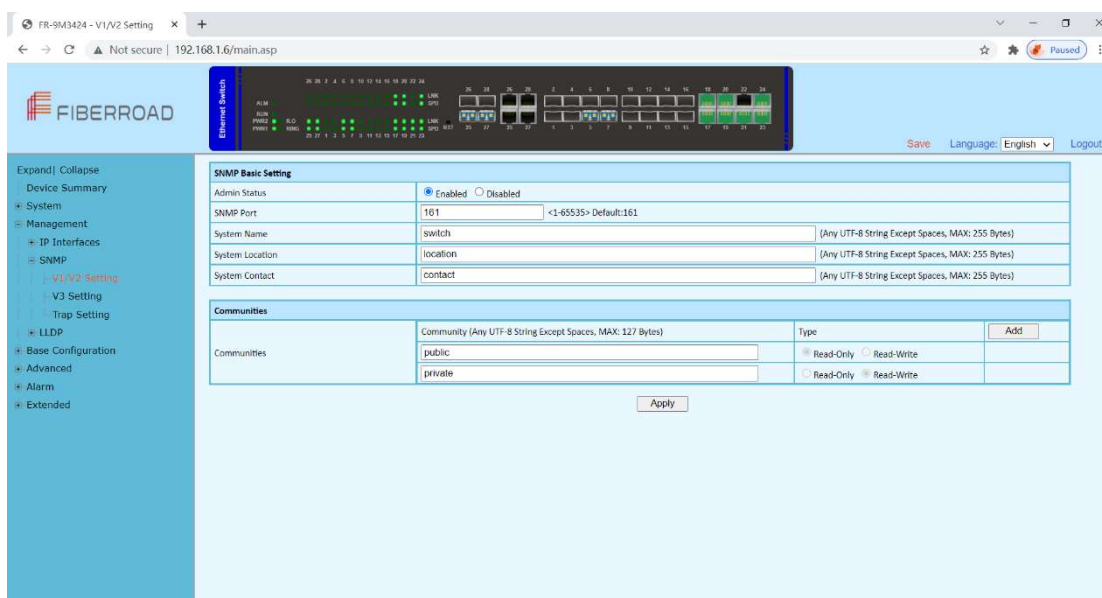
- 1,Select [Management / IP Interface / DHCP Client(IPv6)] in the navigation bar to enter the [DHCP Client(IPv6)] interface.
- 2,In the [DHCP Client(IPv6)] interface, you can view the current configuration information and DHCP client status.

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	

Communities

character other than a space can be entered with a maximum length of 255

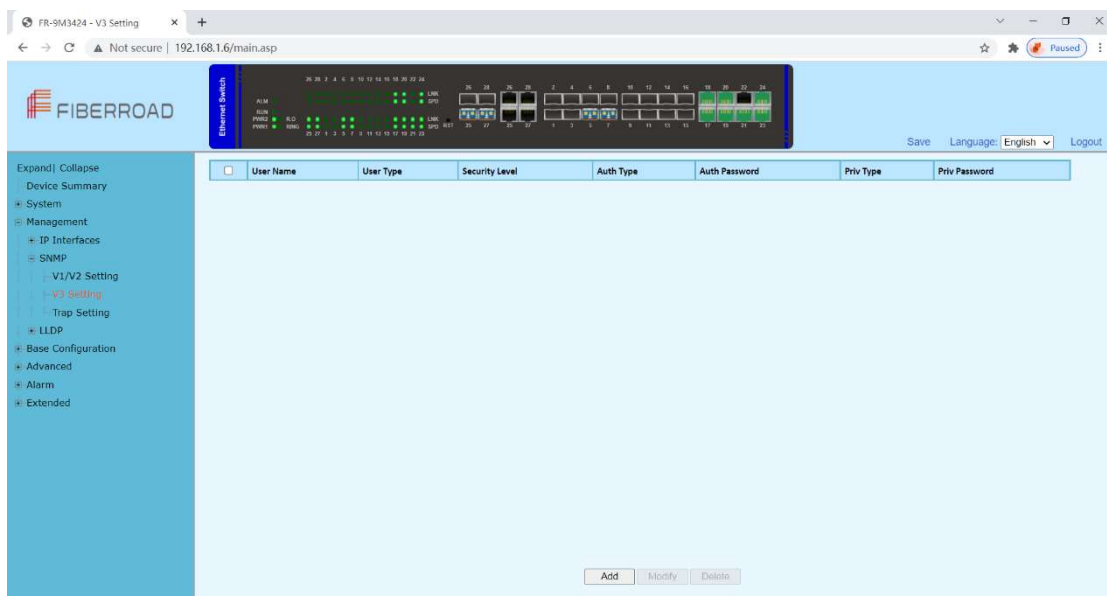
Name: Any legal character other than a space can be entered with a maximum length of 127

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.

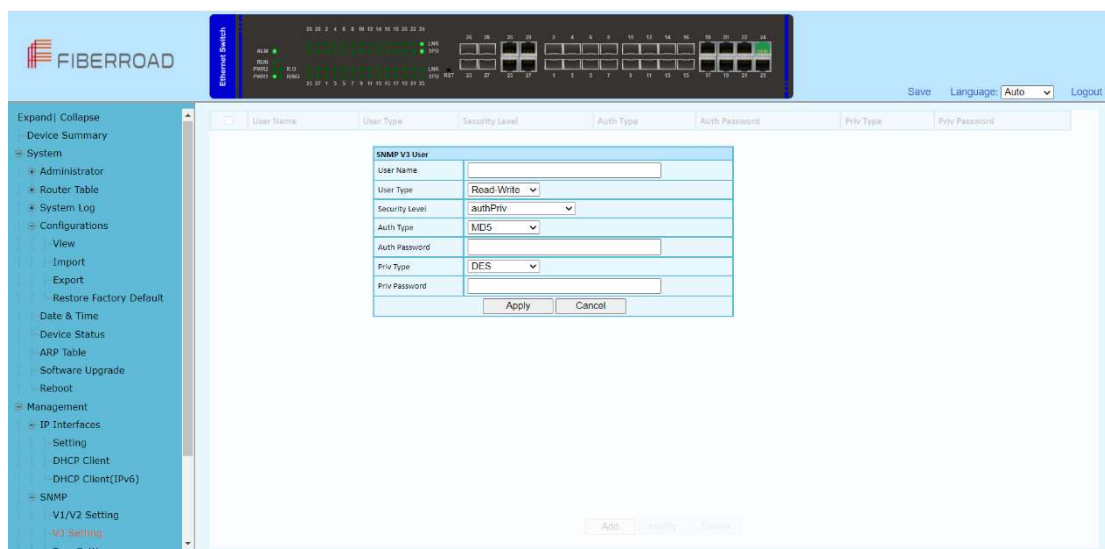


Configuration Steps

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.

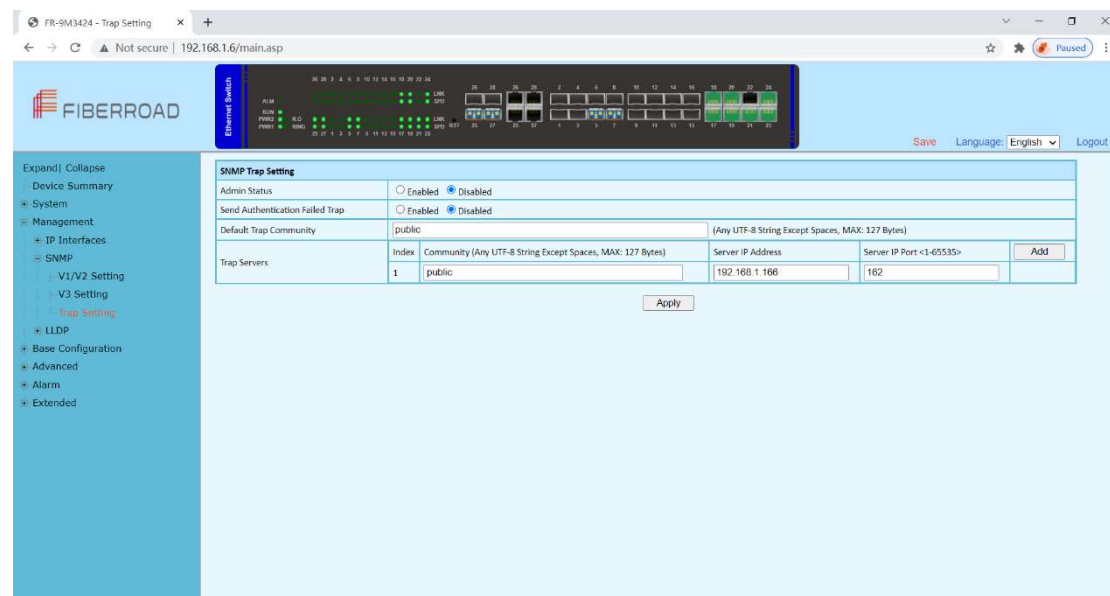


Item	Description	Notes
User Name	As Needed	
User Type	Read-Write/ Read-Only	
Security Level	<p>NoAuthNoPriv:Communication without authentication and privacy.</p> <p>AuthNoPriv:Communication with authentication and without privacy.</p> <p>AuthPriv:Communication with authentication and privacy.</p>	
Auth Type	<p>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.</p> <p>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.</p>	
Auth Password	As Needed	
Priv Type	<p>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</p>	

	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.

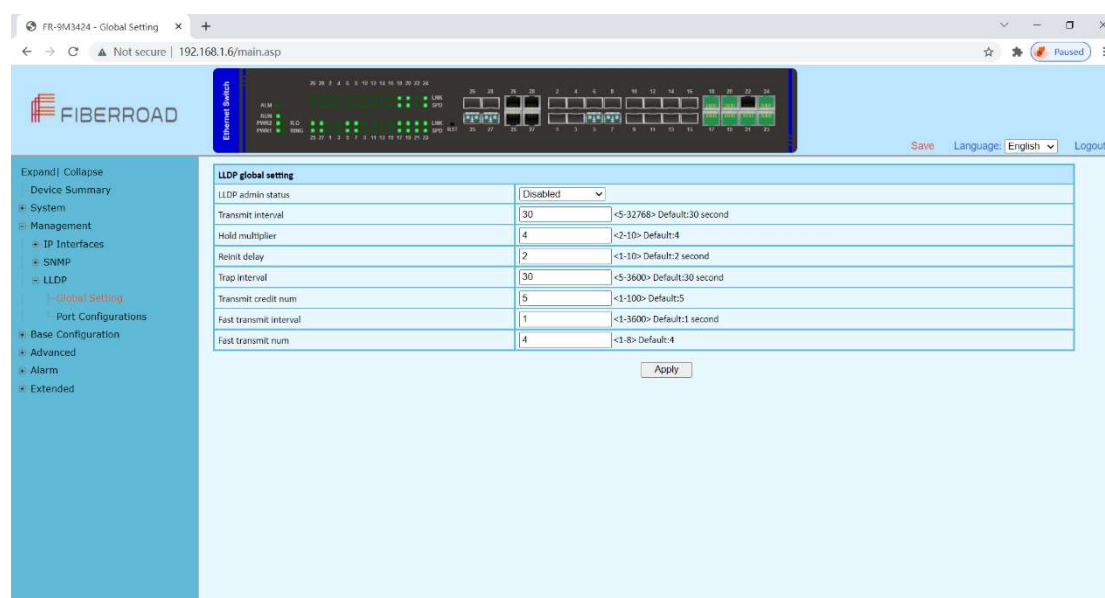
SNMP Trap Setting				
Admin Status	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled			
Send Authentication Failed Trap	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled			
Default Trap Community	<input type="text" value="public"/> (Any UTF-8 String Except Spaces, MAX: 127 Bytes)			
Trap Servers	Index	Community (Any UTF-8 String Except Spaces, MAX: 127 Bytes)	Server IP Address	Server IP Port <1-65535>
	1	<input type="text" value="public"/>	<input type="text" value="192.168.1.166"/>	<input type="text" value="162"/>
<input type="button" value="Add"/>				
<input type="button" value="Apply"/>				

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 Community Characters: Any legal character other than a space can be entered with a maximum length of 127	
Trap Server	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].

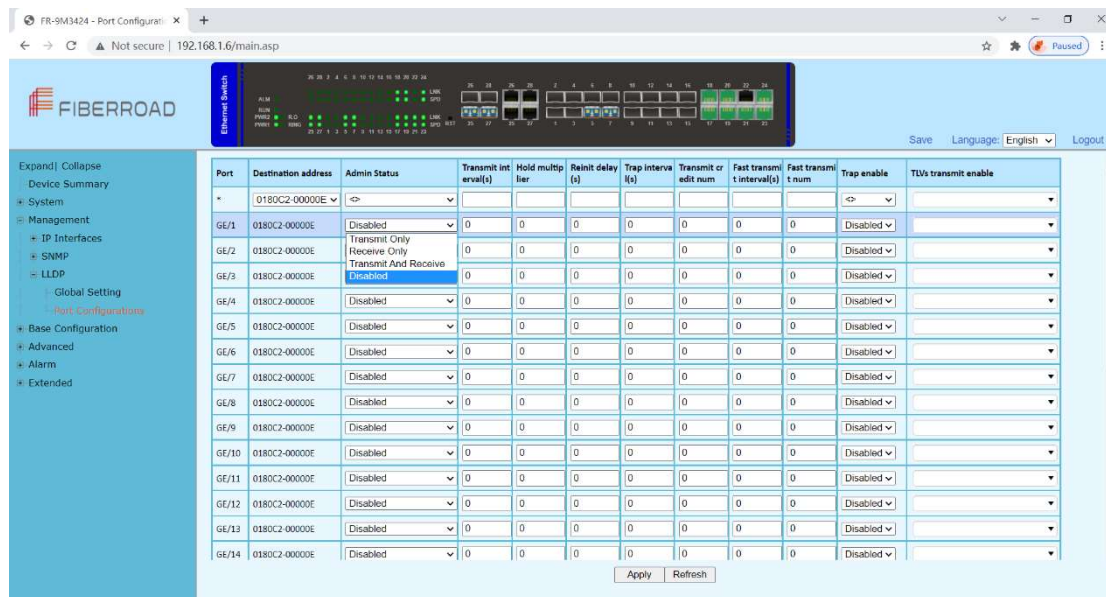
LLDP global setting		
LLDP admin status	Disabled	
Transmit interval	30	<5-32768> Default:30 second
Hold multiplier	4	<2-10> Default:4
Reinit delay	2	<1-10> Default:2 second
Trap interval	30	<5-3600> Default:30 second
Transmit credit num	5	<1-100> Default:5
Fast transmit interval	1	<1-3600> Default:1 second
Fast transmit num	4	<1-8> Default:4

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 interval 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	Default: Disable
	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	
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 interval range 5-3600	
Transmit credit num	Default: Use[Global Setting] Transmit 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

3.1.1 Base Configuration-Port-Status And Setting

Port	Link Status	Port Type	Running Status				Admin Status					
			Speed	Duplex	Rx Rate(bps)	Tx Rate(bps)	Admin Status	Speed	Duplex	Flow Control	EEE	Setting
GE/1	✖	Fiber	10M	Half	0.00	0.00	On	Fiber-Auto	Full	Off	Disabled	Modify
GE/2	✖	Fiber	10M	Half	0.00	0.00	On	Fiber-Auto	Full	Off	Disabled	Modify
GE/3	✖	Fiber	10M	Half	0.00	0.00	On	Fiber-Auto	Full	Off	Disabled	Modify
GE/4	✖	Fiber	10M	Half	0.00	0.00	On	Fiber-Auto	Full	Off	Disabled	Modify
GE/5	✔	Fiber	1000M	Full	0.00	0.00	On	Fiber-Auto	Full	Off	Disabled	Modify
GE/6	✖	Fiber	10M	Half	0.00	0.00	On	Fiber-Auto	Full	Off	Disabled	Modify
GE/7	✔	Fiber	1000M	Full	0.00	0.00	On	Fiber-Auto	Full	Off	Disabled	Modify
GE/8	✖	Fiber	10M	Half	0.00	0.00	On	Fiber-Auto	Full	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
GE/11	✖	Fiber	10M	Half	0.00	0.00	On	Fiber-Auto	Full	Off	Disabled	Modify
GE/12	✖	Fiber	10M	Half	0.00	0.00	On	Fiber-Auto	Full	Off	Disabled	Modify
GE/13	✖	Fiber	10M	Half	0.00	0.00	On	Fiber-Auto	Full	Off	Disabled	Modify
GE/14	✖	Fiber	10M	Half	0.00	0.00	On	Fiber-Auto	Full	Off	Disabled	Modify
GE/15	✖	Fiber	10M	Half	0.00	0.00	On	Fiber-Auto	Full	Off	Disabled	Modify
GE/16	✖	Fiber	10M	Half	0.00	0.00	On	Fiber-Auto	Full	Off	Disabled	Modify
GE/17	✔	Copper	1000M	Full	\$12.00	0.00	On	Auto	Auto	Off	Disabled	Modify



Configuration Steps

1. Select [Base 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.

Setting	
Port	GE/1
Link Status	Link Down
Admin Status	On
Fiber Mode	Fiber-Auto
EEE	Disabled
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

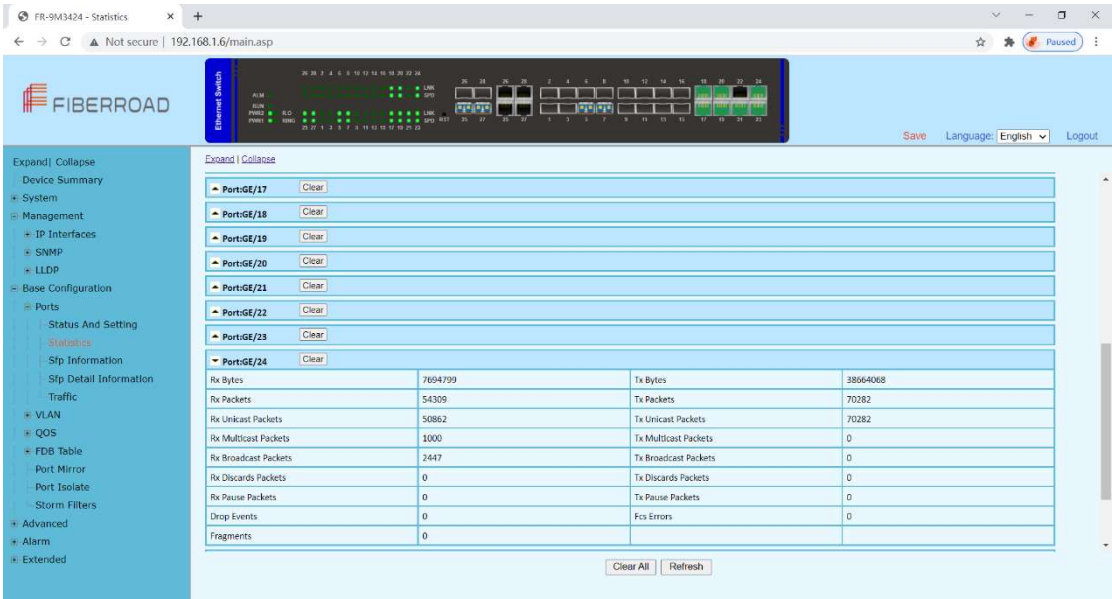
3. If you need to modify the configuration of a port, just click the [Modify] on the right side corresponding entry. to enter the modification interface and modify the corresponding configuration item. Click the [Apply] to complete the modification,

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	Default:
	Fiber-100M	Fiber-Auto
	Fiber-1000M	
EEE	Energy Efficient Ethernet	Default:
	Enabled / Disabled	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-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)	

3.1.3 Base Configuration-Port-SFP Information

Port	Status	Wavelength(nm)	Distance(m)	Bit Rate(MBd)	Ethernet Codes	DDM	Calibrated	Tx Power(dBm)	Rx Power(dBm)	Temperature(°C)	Voltage(V)	Current(mA)
GE/1	Removed	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
GE/2	Removed	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
GE/3	Removed	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
GE/4	Removed	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
GE/5	Inserted	1310	10000	10300	N/A	Supported	Internally	-1.78	-6.57	49.98	3.36	40.00
GE/6	Removed	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
GE/7	Inserted	1310	15000	1300	Fiber-1000M	Supported	Externally	-5.08	-3.26	37.48	3.34	13.16
GE/8	Removed	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
GE/9	Removed	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
GE/10	Removed	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
GE/11	Removed	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
GE/12	Removed	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
GE/13	Removed	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
GE/14	Removed	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
GE/15	Removed	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
GE/16	Removed	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
GE/25	Inserted	1310	20000	1300	Fiber-1000M	Supported	Internally	-6.55	-6.39	35.66	3.38	20.30
GE/26	Removed	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

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(°C)	SFP operating temperature	Unit: °C
Voltage(V)	SFP Voltage	Unit: V
Current(mA)	SFP Current	Unit: mA

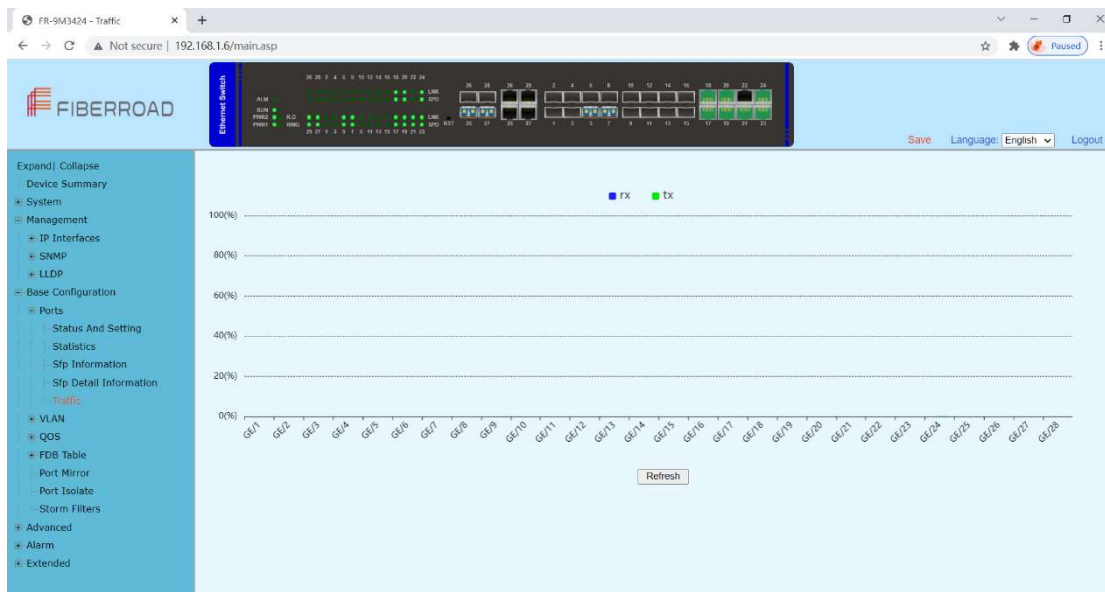
3.1.4 Base Configuration-Port-SFP Detail Information

The screenshot displays the FiberRoad web interface for the FR-9M3424 switch. The left sidebar shows the navigation menu with 'Sfp Detail Information' selected under 'Ports'. The main content area shows the SFP details for Port GE/7. A table lists various parameters:

Parameter	Value	Parameter	Value	Parameter	Value
Status	Inserted	Ethernet Codes	1000BASE-LX	Mode	Single Mode
Wavelength(nm)	1310	Distance(m)	15000	Bit Rate(Mbd)	1300
Vendor Name		OUI	00-00-00	PN	RTXM191-400
Version	3.0	SN	SFP1819461624	Date	2018-12-06
Connector Type	LC	DDM	Supported	Calibrated	Externally
Tx Power(dBm)	-5.08	Rx Power(dBm)	-3.26	Temperature(°C)	37.48
Voltage(V)	3.34	Current(mA)	13.13		

Other ports listed include PortGE/1 through PortGE/6 and PortGE/8 through PortGE/10. A 'Refresh' button is located at the bottom right of the table.

3.1.5 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

Basic Setting	
Created VLAN	1
VLAN List	<input type="text"/> Example:1-10,13,15-4094
	<input checked="" type="radio"/> Add <input type="radio"/> Delete <input type="radio"/> Modify Name: <input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Item	Description	Notes
Choose Range	To search for a VLAN ID	
Search	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

The screenshot shows the 'Port Setting' page in the Fiberroad web interface. The left sidebar contains a navigation menu with the following items: Expand/Collapse, Device Summary, System, Management, IP Interfaces, SNMP, LLDP, Base Configuration, Ports, VLAN, QoS, FDB Table, Port Mirror, Port Isolate, Storm Filters, Advanced, Alarm, and Extended. The main content area displays a table of port settings for various interfaces (GE/1 to GE/16). The table has columns for Port, VLAN Mode, PVID, Tagged VLANs for hybrid / Permitted VLANs for trunk, Untagged VLANs, and Setting. A 'Created VLAN' section at the top shows a list of created VLANs (1,33-46). A 'Refresh' button is located at the bottom right of the table.

Port	VLAN Mode	PVID	Tagged VLANs for hybrid / Permitted VLANs for trunk	Untagged VLANs	Setting
GE/1	Trunk	39	39		Modify
GE/2	Trunk	41	41		Modify
GE/3	Trunk	38	38		Modify
GE/4	Trunk	42	42		Modify
GE/5	Trunk	38	38		Modify
GE/6	Trunk	42	42		Modify
GE/7	Trunk	37	37		Modify
GE/8	Trunk	43	43		Modify
GE/9	Trunk	37	37		Modify
GE/10	Trunk	43	43		Modify
GE/11	Trunk	36	36		Modify
GE/12	Trunk	44	44		Modify
GE/13	Trunk	36	36		Modify
GE/14	Trunk	44	44		Modify
GE/15	Trunk	35	35		Modify
GE/16	Trunk	45	45		Modify

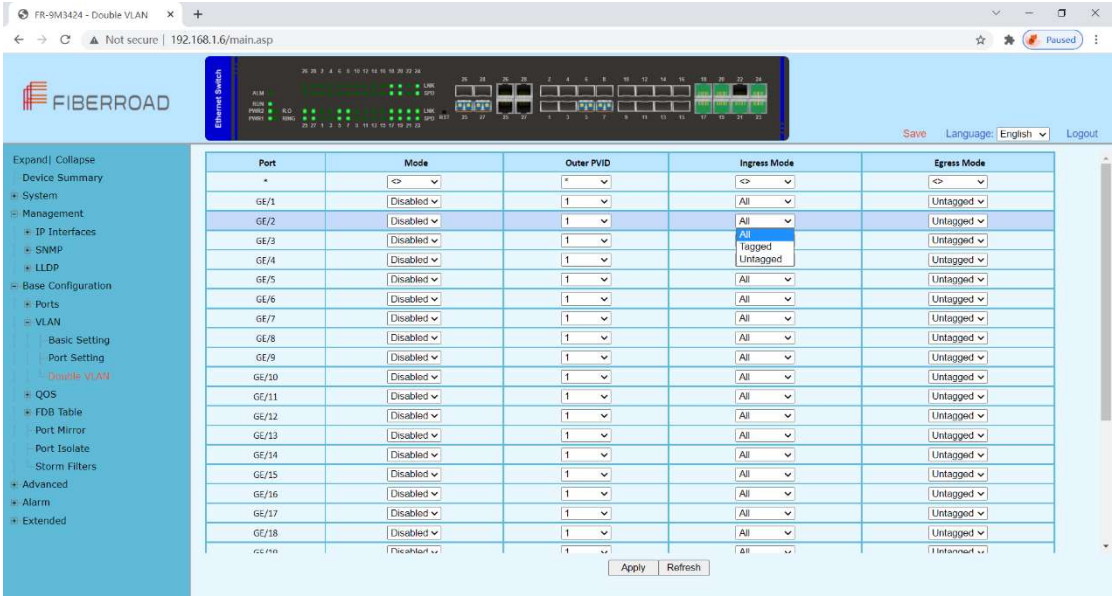
Configuration Steps

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.

Port Setting	
Port	GE/1
VLAN Mode	trunk
PVID	39 <1-4094>
Permitted VLAN	<input type="radio"/> Replace <input type="radio"/> Add <input type="radio"/> Delete <input checked="" type="radio"/> All Created VLAN <input type="text"/> Example:1-10,13,15-4094
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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

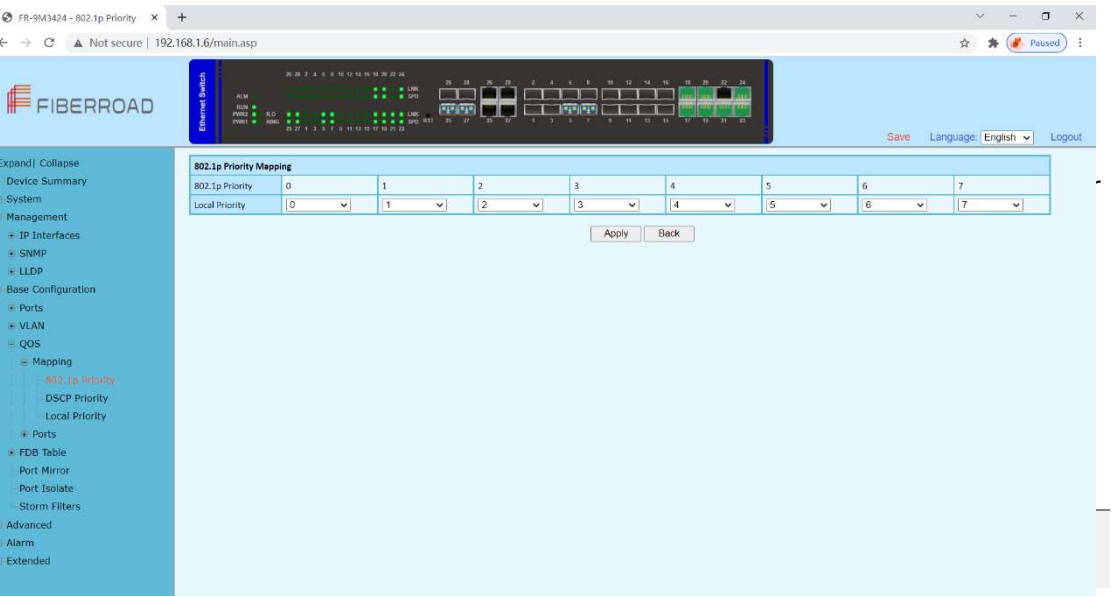


Item	Description	Notes
Port	Port Name Information	Read Only
Mode	Enabled / Disabled	Default: Disabled
Outer PVID	1, 33-46	
Ingress Mode	All / Tagged / Untagged	Default : All
Egress Mode	Tagged / Untagged	Default: Untagged

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.



3.3.2 Base Configuration-QoS- Mapping – DSCP Priority

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

The screenshot shows the 'DSCP Priority Mapping' configuration page in the FiberRoad web interface. The page has a navigation bar on the left with options like System, Management, IP Interfaces, SNMP, LLDP, Base Configuration, Ports, VLAN, QOS, Mapping, 802.1p Priority, DSCP Priority, Local Priority, Ports, FDB Table, Port Mirror, Port Isolate, Storm Filters, Advanced, Alarm, and Extended. The main content area displays a table for mapping DSCP priorities to local priorities. The table has columns for DSCP Priority and Local Priority, with rows for each DSCP priority value from 0 to 47. The 'Local Priority' column contains a dropdown menu for each DSCP priority. The 'Apply' and 'Back' buttons are located at the bottom right of the table.

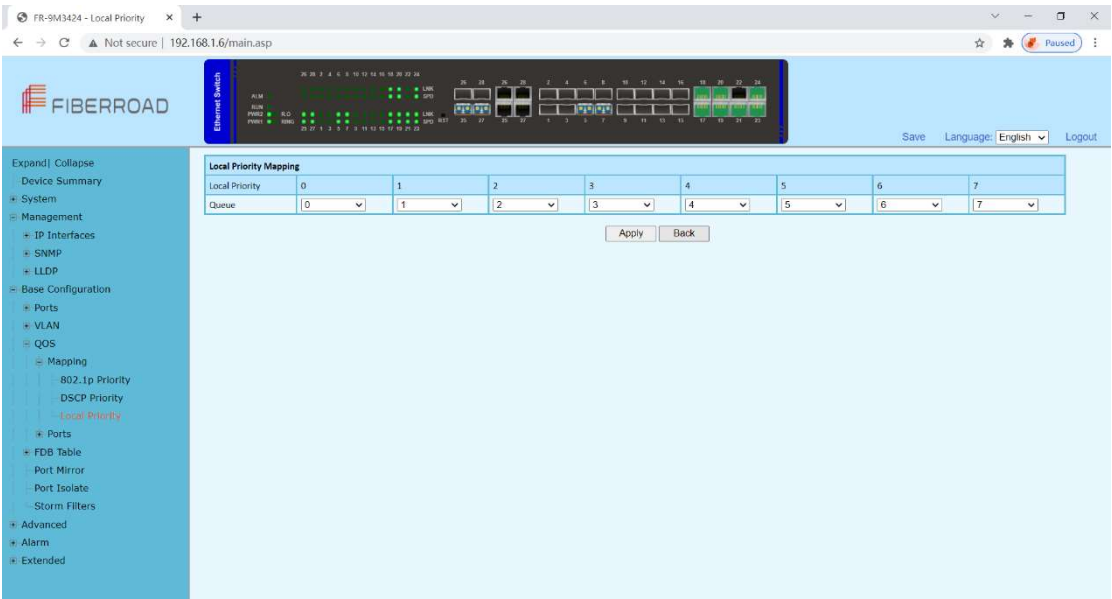
DSCP Priority	0	1	2	3	4	5	6	7
Local Priority	0	0	0	0	0	0	0	0
DSCP Priority	8	9	10	11	12	13	14	15
Local Priority	1	1	1	1	1	1	1	1
DSCP Priority	16	17	18	19	20	21	22	23
Local Priority	2	2	2	2	2	2	2	2
DSCP Priority	24	25	26	27	28	29	30	31
Local Priority	3	3	3	3	3	3	3	3
DSCP Priority	32	33	34	35	36	37	38	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

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.



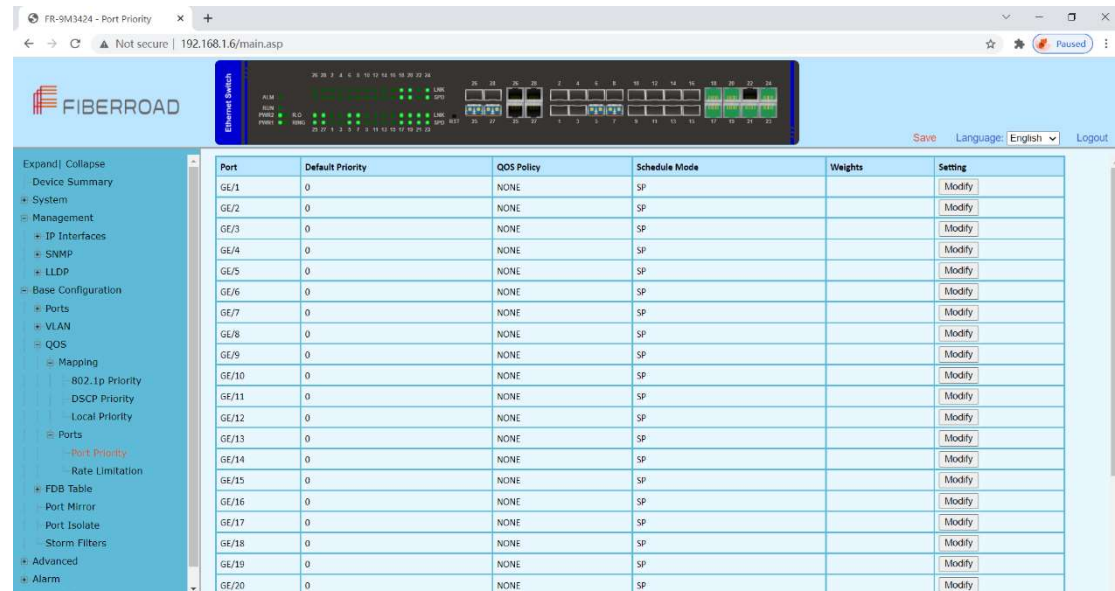
1. Select [Base Configuration / QOS / Mapping / Local Priority] in the navigation bar to enter the QOS Local Mapping.
2. You can view the mapping from the local priority to the egress queue on the QOS [Local Priority] interface.
3. To modify the mapping relationship, click [Modify] and select the mapped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

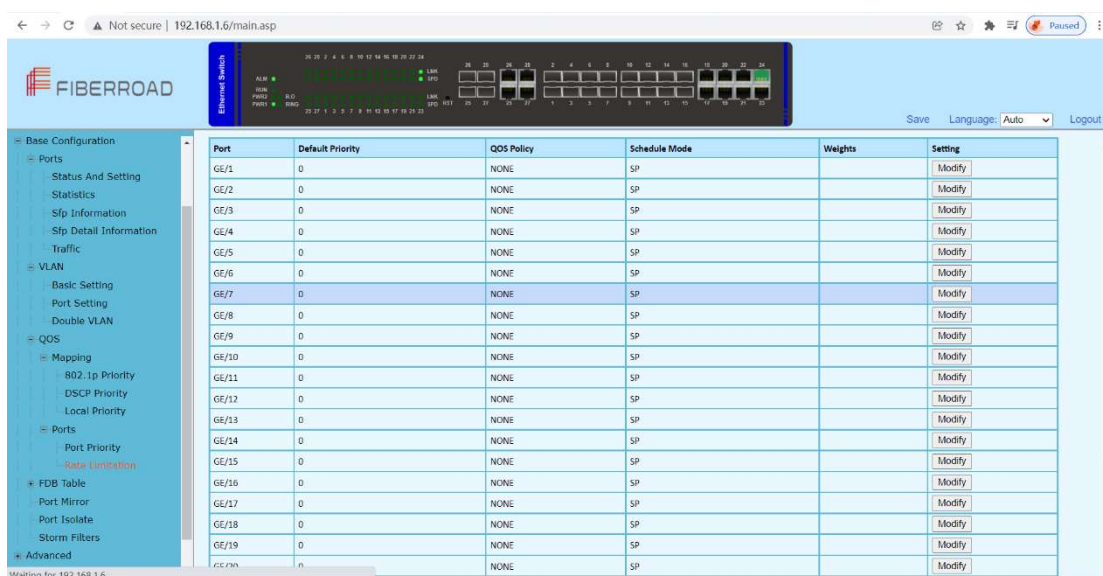
1. Select [Base Configuration / QoS / Ports / Port Priority] in the navigation bar to enter the QoS [Port Priority] interface.
2. The QoS related configuration of the port can be viewed on the QoS [Port Priority] interface.
3. To modify the QoS configuration of a port, click [Modify] on the corresponding 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.

Port Priority	
Port	GE/2 ▼
Default Priority	0 <0-7>
QoS Policy	NONE ▼
Schedule Mode	SP ▼
Weights	1 .3 .5 .7 .11 .25 .31 .44 <1-127>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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 Mode	SP: Strict Priority scheduling strategy 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.

Rate Limitation

Port

GE/5

Ingress Rate Limitation

☐ On ☒ Off

<16-1000000>kbps

Egress Rate Limitation

☐ On ☒ Off

<16-1000000>kbps

Apply

Cancel

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

FIBERROAD

20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1030 1031 1032 1033 1034 1035 1036 1037 1038 1039 1040 1041 1042 1043 1044 1045 1046 1047 1048 1049 1050 1051 1052 1053 1054 1055 1056 1057 1058 1059 1060 1061 1062 1063 1064 1065 1066 1067 1068 1069 1070 1071 1072 1073 1074 1075 1076 1077 1078 1079 1080 1081 1082 1083 1084 1085 1086 1087 1088 1089 1090 1091 1092 1093 1094 1095 1096 1097 1098 1099 1100 1101 1102 1103 1104 1105 1106 1107 1108 1109 1110 1111 1112 1113 1114 1115 1116 1117 1118 1119 1120 1121 1122 1123 1124 1125 1126 1127 1128 1129 1130 1131 1132 1133 1134 1135 1136 1137 1138 1139 1140 1141 1142 1143 1144 1145 1146 1147 1148 1149 1150 1151 1152 1153 1154 1155 1156 1157 1158 1159 1160 1161 1162 1163 1164 1165 1166 1167 1168 1169 1170 1171 1172 1173 1174 1175 1176 1177 1178 1179 1180 1181 1182 1183 1184 1185 1186 1187 1188 1189 1190 1191 1192 1193 1194 1195 1196 1197 1198 1199 1200 1201 1202 1203 1204 1205 1206 1207 1208 1209 1210 1211 1212 1213 1214 1215 1216 1217 1218 1219 1220 1221 1222 1223 1224 1225 1226 1227 1228 1229 1230 1231 1232 1233 1234 1235 1236 1237 1238 1239 1240 1241 1242 1243 1244 1245 1246 1247 1248 1249 1250 1251 1252 1253 1254 1255 1256 1257 1258 1259 1260 1261 1262 1263 1264 1265 1266 1267 1268 1269 1270 1271 1272 1273 1274 1275 1276 1277 1278 1279 1280 1281 1282 1283 1284 1285 1286 1287 1288 1289 1290 1291 1292 1293 1294 1295 1296 1297 1298 1299 1300 1301 1302 1303 1304 1305 1306 1307 1308 1309 1310 1311 1312 1313 1314 1315 1316 1317 1318 1319 1320 1321 1322 1323 1324 1325 1326 1327 1328 1329 1330 1331 1332 1333 1334 1335 1336 1337 1338 1339 1340 1341 1342 1343 1344 1345 1346 1347 1348 1349 1350 1351 1352 1353 1354 1355 1356 1357 1358 1359 1360 1361 1362 1363 1364 1365 1366 1367 1368 1369 1370 1371 1372 1373 1374 1375 1376 1377 1378 1379 1380 1381 1382 1383 1384 1385 1386 1387 1388 1389 1390 1391 1392 1393 1394 1395 1396 1397 1398 1399 1400 1401 1402 1403 1404 1405 1406 1407 1408 1409 1410 1411 1412 1413 1414 1415 1416 1417 1418 1419 1420 1421 1422 1423 1424 1425 1426 1427 1428 1429 1430 1431 1432 1433 1434 1435 1436 1437 1438 1439 1440 1441 1442 1443 1444 1445 1446 1447 1448 1449 1450 1451 1452 1453 1454 1455 1456 1457 1458 1459 1460 1461 1462 1463 1464 1465 1466 1467 1468 1469 1470 1471 1472 1473 1474 1475 1476 1477 1478 1479 1480 1481 1482 1483 1484 1485 1486 1487 1488 1489 1490 1491 1492 1493 1494 1495 1496 1497 1498 1499 1500 1501 1502 1503 1504 1505 1506 1507 1508 1509 1510 1511 1512 1513 1514 1515 1516 1517 1518 1519 1520 1521 1522 1523 1524 1525 1526 1527 1528 1529 1530 1531 1532 1533 1534 1535 1536 1537 1538 1539 1540 1541 1542 1543 1544 1545 1546 1547 1548 1549 1550 1551 1552 1553 1554 1555 1556 1557 1558 1559 1560 1561 1562 1563 1564 1565 1566 1567 1568 1569 1570 1571 1572 1573 1574 1575 1576 1577 1578 1579 1580 1581 1582 1583 1584 1585 1586 1587 1588 1589 1590 1591 1592 1593 1594 1595 1596 1597 1598 1599 1600 1601 1602 1603 1604 1605 1606 1607 1608 1609 1610 1611 1612 1613 1614 1615 1616 1617 1618 1619 1620 1621 1622 1623 1624 1625 1626 1627 1628 1629 1630 1631 1632 1633 1634 1635 1636 1637 1638 1639 1640 1641 1642 1643 1644 1645 1646 1647 1648 1649 1650 1651 1652 1653 1654 1655 1656 1657 1658 1659 1660 1661 1662 1663 1664 1665 1666 1667 1668 1669 1670 1671 1672 1673 1674 1675 1676 1677 1678 1679 1680 1681 1682 1683 1684 1685 1686 1687 1688 1689 1690 1691 1692 1693 1694 1695 1696 1697 1698 1699 1700 1701 1702 1703 1704 1705 1706 1707 1708 1709 1710 1711 1712 1713 1714 1715 1716 1717 1718 1719 1720 1721 1722 1723 1724 1725 1726 1727 1728 1729 1730 1731 1732 1733 1734 1735 1736 1737 1738 1739 1740 1741 1742 1743 1744 1745 1746 1747 1748 1749 1750 1751 1752 1753 1754 1755 1756 1757 1758 1759 1760 1761 1762 1763 1764 1765 1766 1767 1768 1769 1770 1771 1772 1773 1774 1775 1776 1777 1778 1779 1780 1781 1782 1783 1784 1785 1786 1787 1788 1789 1790 1791 1792 1793 1794 1795 1796 1797 1798 1799 1800 1801 1802 1803 1804 1805 1806 1807 1808 1809 1810 1811 1812 1813 1814 1815 1816 1817 1818 1819 1820 1821 1822 1823 1824 1825 1826 1827 1828 1829 1830 1831 1832 1833 1834 1835 1836 1837 1838 1839 1840 1841 1842 1843 1844 1845 1846 1847 1848 1849 1850 1851 1852 1853 1854 1855 1856 1857 1858 1859 1860 1861 1862 1863 1864 1865 1866 1867 1868 1869 1870 1871 1872 1873 1874 1875 1876 1877 1878 1879 1880 1881 1882 1883 1884 1885 1886 1887 1888 1889 1890 1891 1892 1893 1894 1895 1896 1897 1898 1899 1900 1901 1902 1903 1904 1905 1906 1907 1908 1909 1910 1911 1912 1913 1914 1915 1916 1917 1918 1919 1920 1921 1922 1923 1924 1925 1926 1927 1928 1929 1930 1931 1932 1933 1934 1935 1936 1937 1938 1939 1940 1941 1942 1943 1944 1945 1946 1947 1948 1949 1950 1951 1952 1953 1954 1955 1956 1957 1958 1959 1960 1961 1962 1963 1964 1965 1966 1967 1968 1969 1970 1971 1972 1973 1974 1975 1976 1977 1978 1979 1980 1981 1982 1983 1984 1985 1986 1987 1988 1989 1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025 2026 2027 2028 2029 2030 2031 2032 2033 2034 2035 2036 2037 2038 2039 2040 2041 2042 2043 2044 2045 2046 2047 2048 2049 2050 2051 2052 2053 2054 2055 2056 2057 2058 2059 2060 2061 2062 2063 2064 2065 2066 2067 2068 2069 2070 2071 2072 2073 2074 2075 2076 2077 2078 2079 2080 2081 2082 2083 2084 2085 2086 2087 2088 2089 2090 2091 2092 2093 2094 2095 2096 2097 2098 2099 2100 2101 2102 2103 2104 2105 2106 2107 2108 2109 2110 2111 2112 2113 2114 2115 2116 2117 2118 2119 2120 2121 2122 2123 2124 2125 2126 2127 2128 2129 2130 2131 2132 2133 2134 2135 2136 2137 2138 2139 2140 2141 2142 2143 2144 2145 2146 2147 2148 2149 2150 2151 2152 2153 2154 2155 2156 2157 2158 2159 2160 2161 2162 2163 2164 2165 2166 2167 2168 2169 2170 2171 2172 2173 2174 2175 2176 2177 2178 2179 2180 2181 2182 2183 2184 2185 2186 2187 2188 2189 2190 2191 2192 2193 2194 2195 2196 2197 2198 2199 2200 2201 2202 2203 2204 2205 2206 2207 2208 2209 2210 2211 2212 2213 2214 2215 2216 2217 2218 2219 2220 2221 2222 2223 2224 2225 2226 2227 2228 2229 2230 2231 2232 2233 2234 2235 2236 2237 2238 2239 2240 2241 2242 2243 2244 2245 2246 2247 2248 2249 2250 2251 2252 2253 2254 2255 2256 2257 2258 2259 2260 2261 2262 2263 2264 2265 2266 2267 2268 2269 2270 2271 2272 2273 2274 2275 2276 2277 2278 2279 2280 2281 2282 2283 2284 2285 2286 2287 2288 2289 2290 2291 2292 2293 2294 2295 2296 2297 2298 2299 2300 2301 2302 2303 2304 2305 2306 2307 2308 2309 2310 2311 2312 2313 2314 2315 2316 2317 2318 2319 2320 2321 2322 2323 2324 2325 2326 2327 2328 2329 2330 2331 2332 2333 2334 2335 2336 2337 2338 2339 2340 2341 2342 2343 2344 2345 2346 2347 2348 2349 2350 2351 2352 2353 2354 2355 2356 2357 2358 2359 2360 2361 2362 2363 2364 2365 2366 2367 2368 2369 2370 2371 2372 2373 2374 2375 2376 2377 2378 2379 2380 2381 2382 2383 2384 2385 2386 2387 2388 2389 2390 2391 2392 2393 2394 2395 2396 2397 2398 2399 2400 2401 2402 2403 2404 2405 2406 2407 2408 2409 2410 2411 2412 2413 2414 2415 2416 2417 2418 2419 2420 2421 2422 2423 2424 2425 2426 2427 2428 2429 2430 2431 2432 2433 2434 2435 2436 2437 2438 2439 2440 2441 2442 2443 2444 2445 2446 2447 2448 2449 2450 2451 2452 2453 2454 2455 2456 2457 2458 2459 2460 2461 2462 2463 2464 2465 2466 2467 2468 2469 2470 2471 2472 2473 2474 2475 2476 2477 2478 2479 2480 2481 2482 2483 2484 2485 2486 2487 2488 2489 2490 2491 2492 2493 2494 2495 2496 2497 2498 2499 2500 2501 2502 2503 2504 2505 2506 2507 2508 2509 2510 2511 2512 2513 2514 2515 2516 2517 2518 2519 2520 2521 2522 2523 2524 2525 2526 2527 2528 2529 2530 2531 2532 2533 2534 2535 2536 2537 2538 2539 2540 2541 2542 2543 2544 2545 2546 2547 2548 2549 2550 2551 2552 2553 2554 2555 2556 2557 2558 2559 2560 2561 2562 2563 2564 2565 2

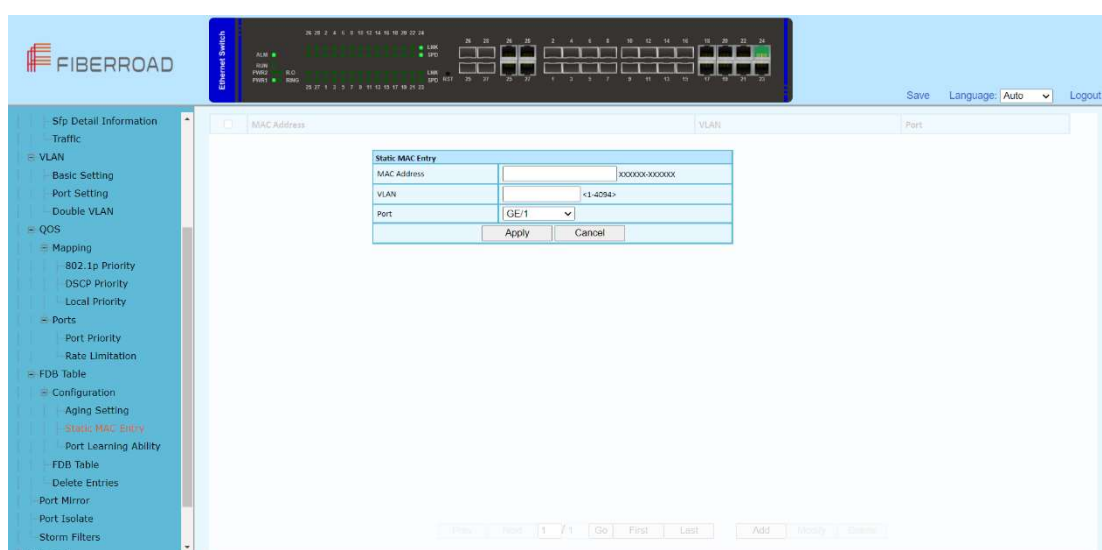
[Aging Time] interface.

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

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



Configuration Steps

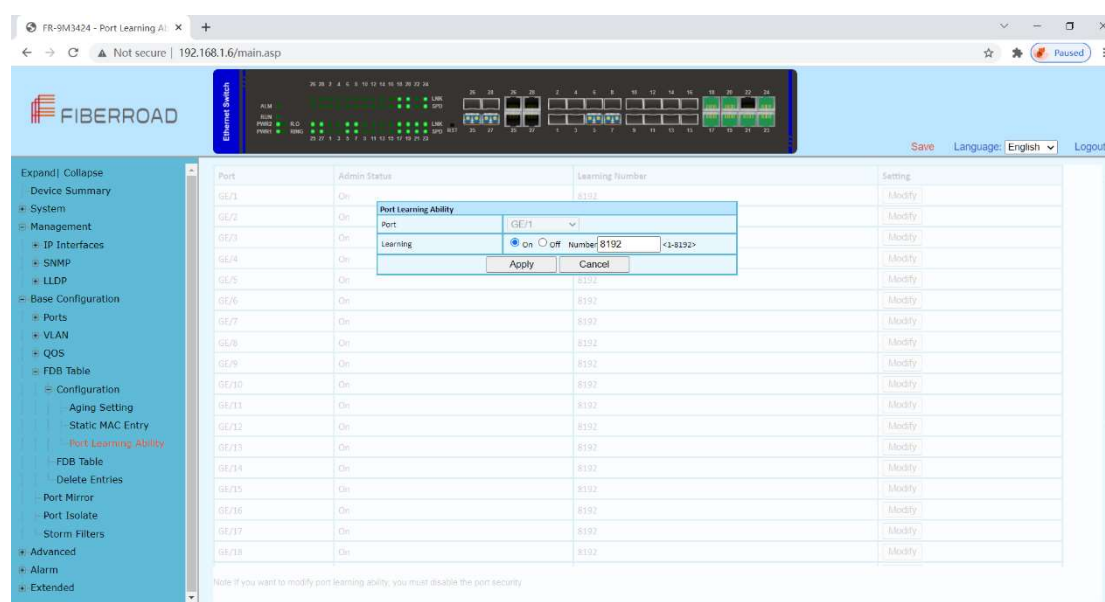
1. Select [Base Configuration / FDB Table / Configuration / Static MAC Entry] to enter the [Static MAC Entry] configuration interface.
2. On FDB Table [Static MAC Entry] interface, you can view the static MAC related configuration information of FDB Table,
3. If add a new static MAC address, click [Add] 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.

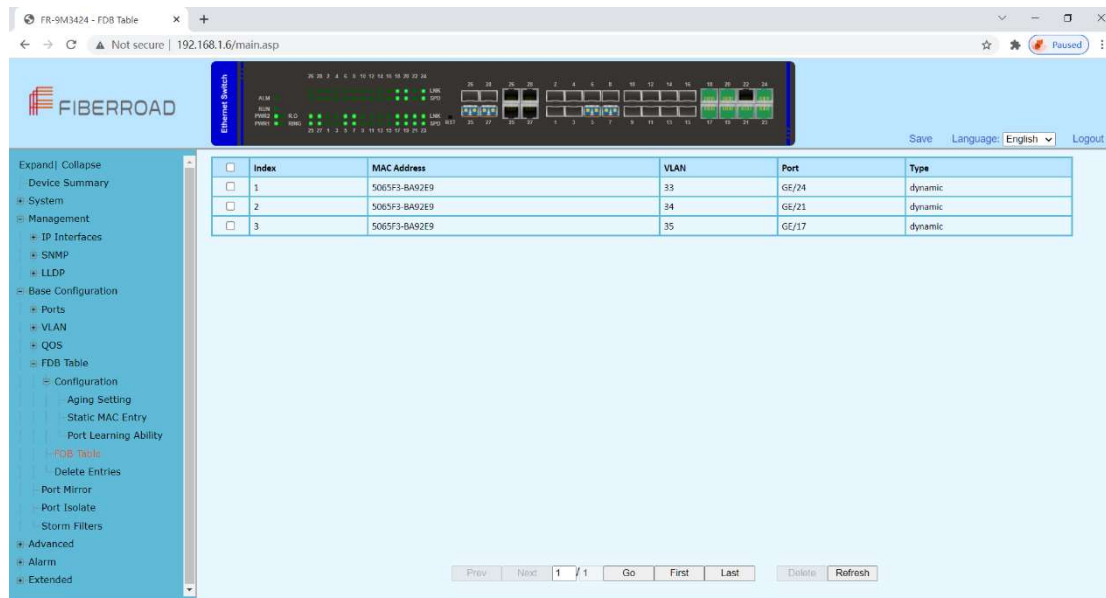
Item	Description	Notes
Port	Port name, selected modified port	
Learning	Functional configuration of port learning, configured via radio buttons. ON: The Port Learning Ability is on. IS3000	

/ 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

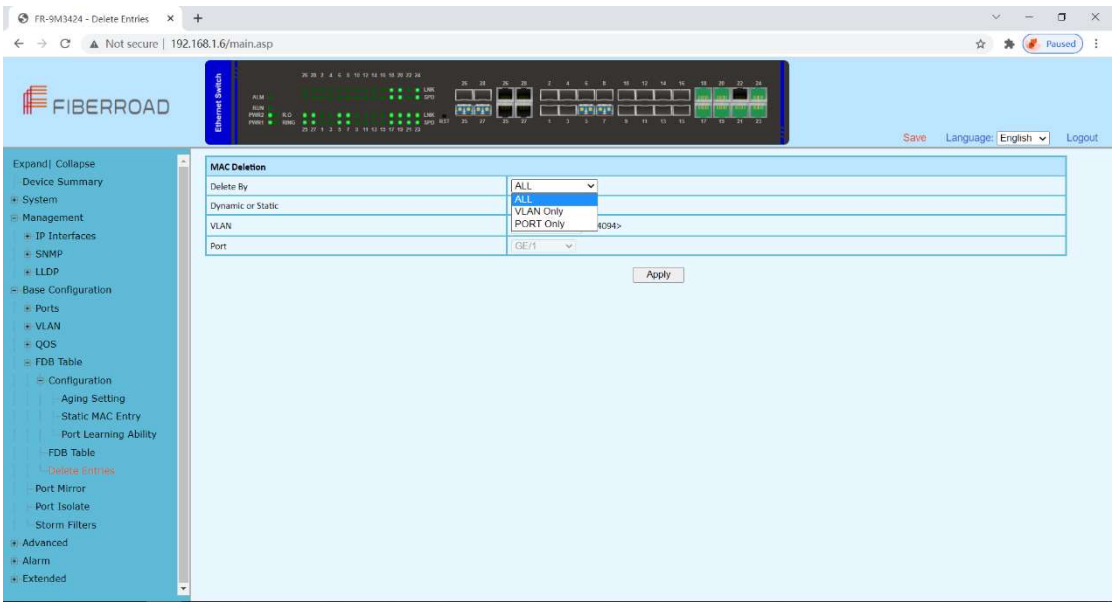
The FDB (forwarding database) table is used by a Layer 2 device (switch/bridge) to store the MAC addresses that have been learned and which ports that MAC address was learned on. The MAC addresses are learned through transparent bridging on switches and dedicated bridges.



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



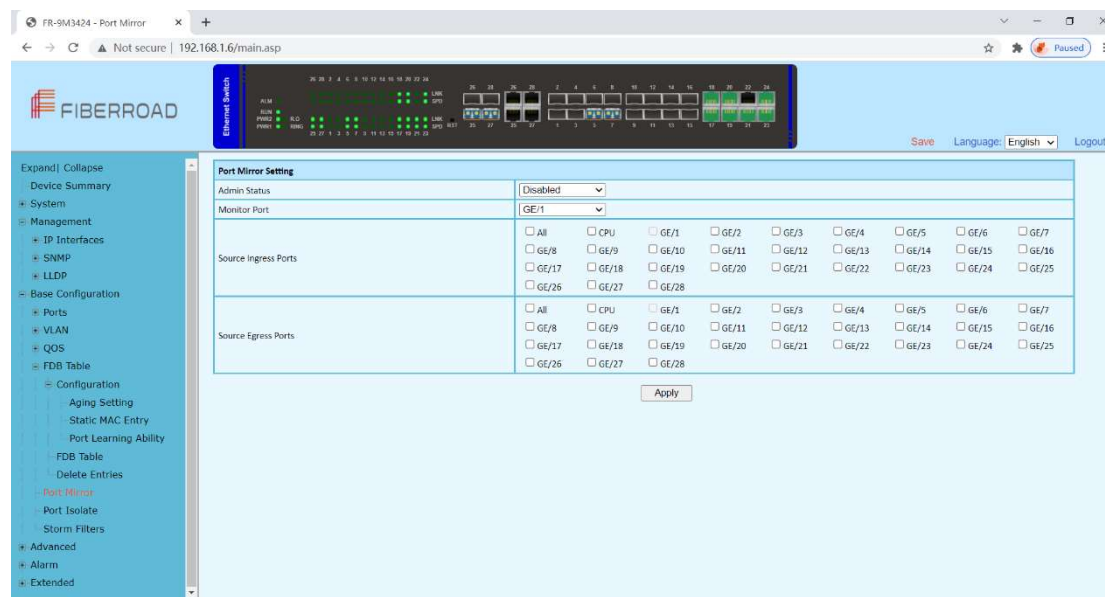
Configuration Steps

- 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).



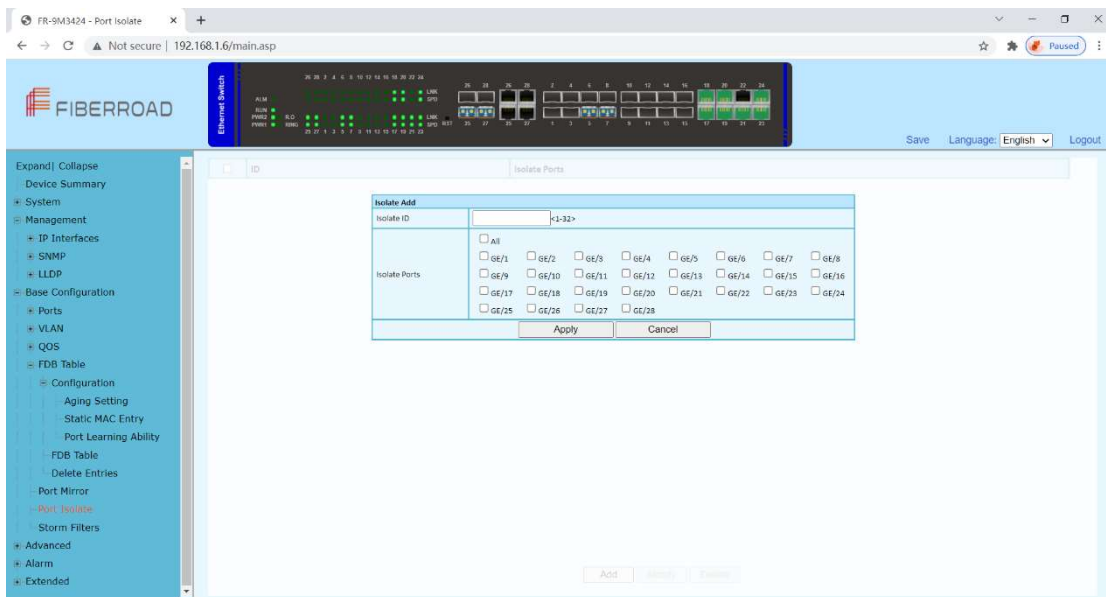
Configuration Steps

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.

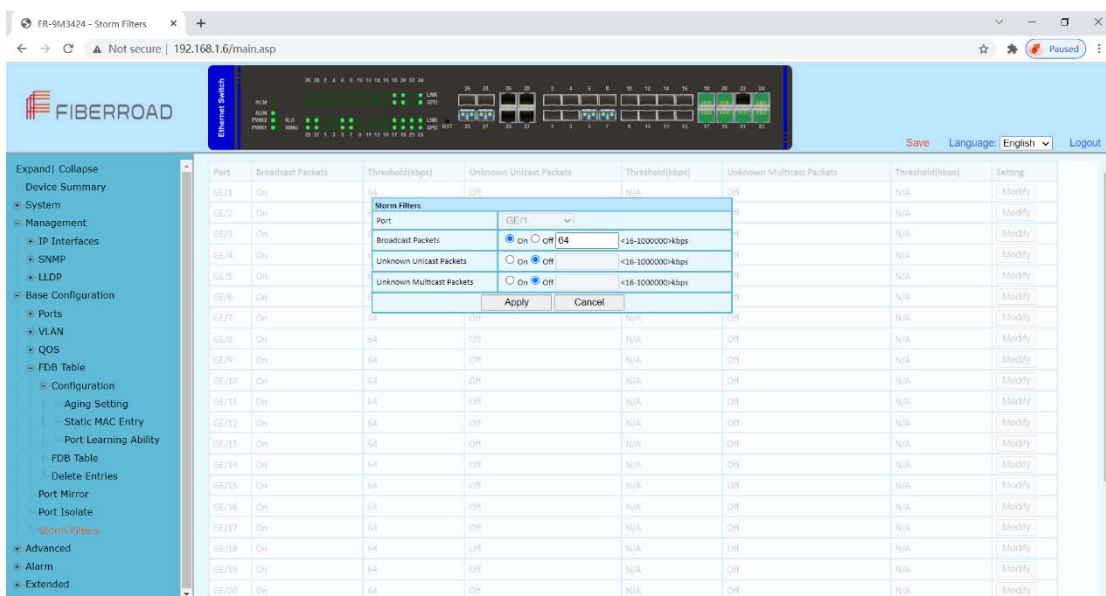


Configuration Steps

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
- ❖ ERPS

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.

Port	Mode	Action	State	MAC 1	MAC 2	MAC 3	Clear
*	<>	<>					Clear
GE/1	Disabled	Trap	Non-Execution	000000-000000	000000-000000	000000-000000	Clear
GE/2	Disabled	Trap	Non-Execution	000000-000000	000000-000000	000000-000000	Clear
GE/3	Disabled	Trap	Non-Execution	000000-000000	000000-000000	000000-000000	Clear
GE/4	Disabled	Trap	Non-Execution	000000-000000	000000-000000	000000-000000	Clear
GE/5	Disabled	Trap	Non-Execution	000000-000000	000000-000000	000000-000000	Clear
GE/6	Disabled	Trap	Non-Execution	000000-000000	000000-000000	000000-000000	Clear
GE/7	Disabled	Trap	Non-Execution	000000-000000	000000-000000	000000-000000	Clear
GE/8	Disabled	Trap	Non-Execution	000000-000000	000000-000000	000000-000000	Clear
GE/9	Disabled	Trap	Non-Execution	000000-000000	000000-000000	000000-000000	Clear
GE/10	Disabled	Trap	Non-Execution	000000-000000	000000-000000	000000-000000	Clear
GE/11	Disabled	Trap	Non-Execution	000000-000000	000000-000000	000000-000000	Clear
GE/12	Disabled	Trap	Non-Execution	000000-000000	000000-000000	000000-000000	Clear
GE/13	Disabled	Trap	Non-Execution	000000-000000	000000-000000	000000-000000	Clear
GE/14	Disabled	Trap	Non-Execution	000000-000000	000000-000000	000000-000000	Clear
GE/15	Disabled	Trap	Non-Execution	000000-000000	000000-000000	000000-000000	Clear
GE/16	Disabled	Trap	Non-Execution	000000-000000	000000-000000	000000-000000	Clear

Apply Refresh

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

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.

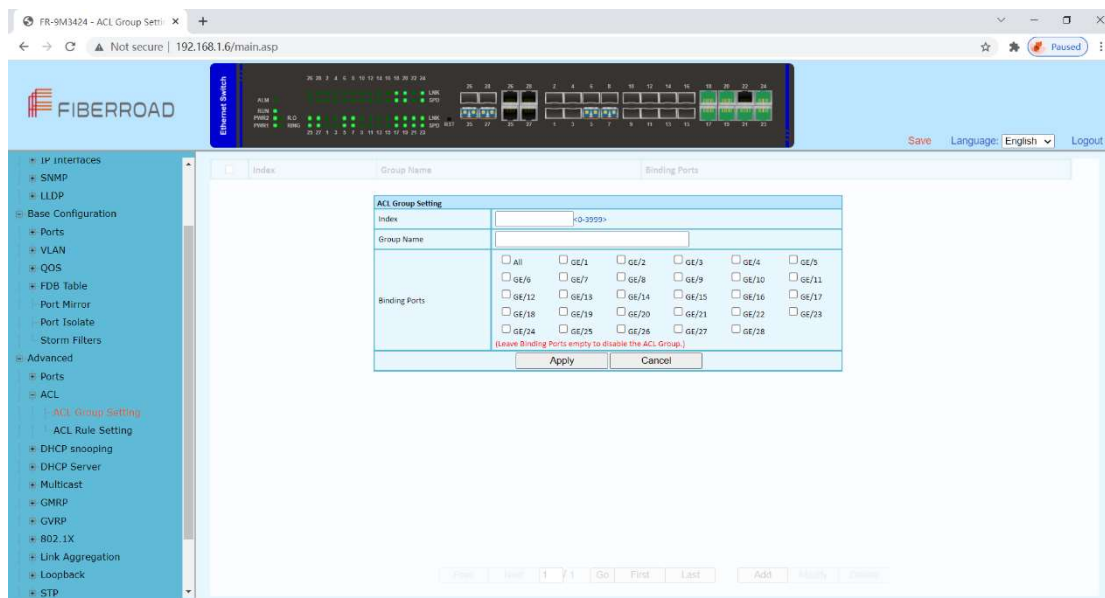
<i>Item</i>	<i>Description</i>	<i>Notes</i>
Mode	Enable port security on the desired ports. If desired, specify the secure MAC address.	
Action	Trap/Shutdown/Trap&Shutdown/Drop/Trap&Drop	
MAC 1/MAC 2/MAC 3	You can add MAC address to the list of secure address	

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.)

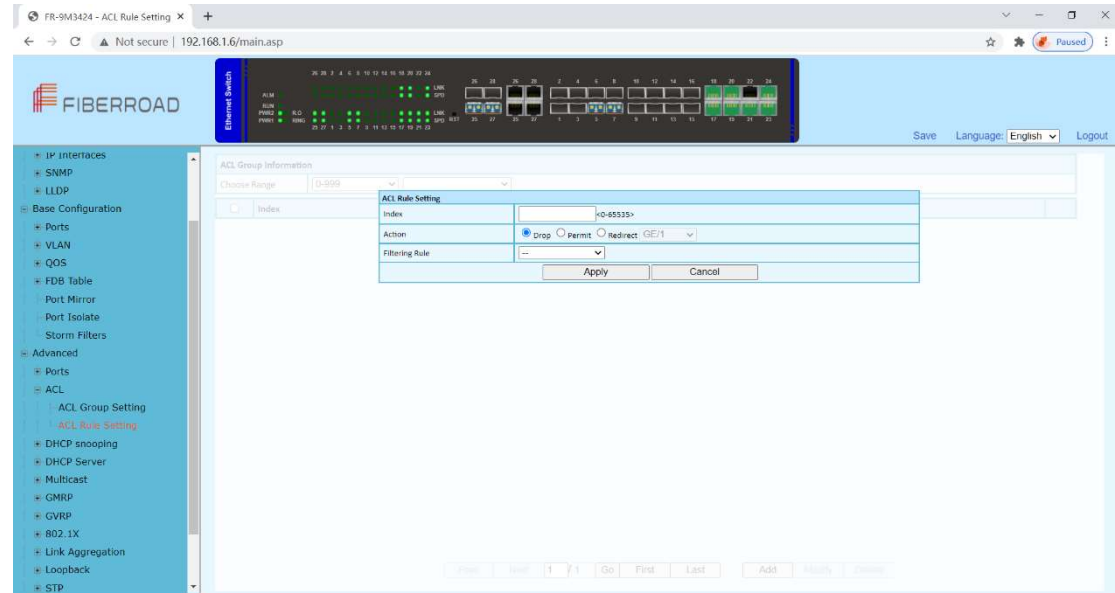
Apply

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.	

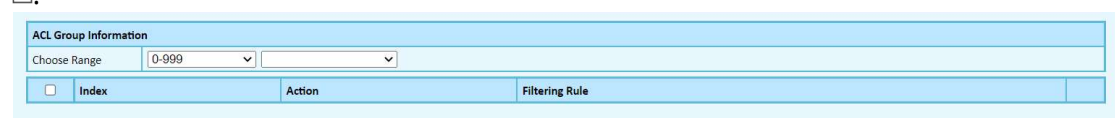
4.2.2 Advanced Configuration – ACL – ACL Rule Setting

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.

ACL Rule Setting	
Index	<0-65535>
Action	<input checked="" type="radio"/> Drop <input type="radio"/> Permit <input type="radio"/> Redirect GE/1
Filtering Rule	--
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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.

ACL Rule Setting

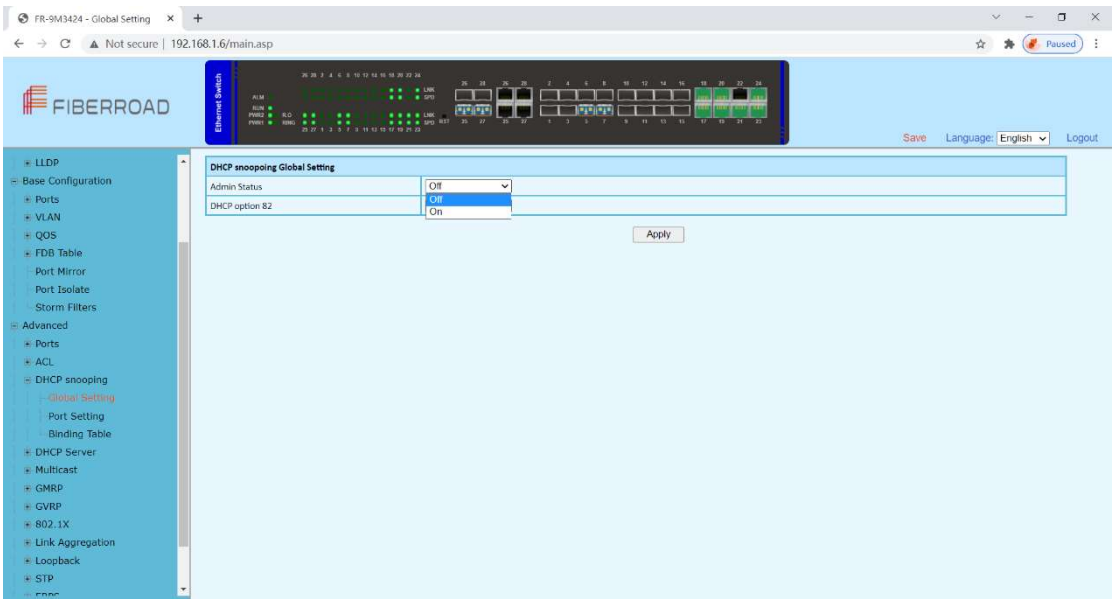
Index	<input type="text" value=""/>	<0-65535>
Action	<input checked="" type="radio"/> Drop <input type="radio"/> Permit <input type="radio"/> Redirect <input type="text" value="GE/1"/>	
Filtering Rule	<input type="text" value="--"/>	
IP Protocol	<input checked="" type="radio"/> ICMP <input type="radio"/> IGMP <input type="radio"/> TCP <input type="radio"/> UDP	<input type="button" value="Delete"/>
Source MAC	<input checked="" type="radio"/> Any <input type="radio"/> <input type="text" value=""/>	XXXXXXXX-XXXXXX MASK: FFFFFFFF-FFFFFF <input type="button" value="Delete"/>
Destination MAC	<input checked="" type="radio"/> Any <input type="radio"/> <input type="text" value=""/>	XXXXXXXX-XXXXXX MASK: FFFFFFFF-FFFFFF <input type="button" value="Delete"/>
VLAN	<input checked="" type="radio"/> Any <input type="radio"/> <input type="text" value=""/>	<1-4094> <input type="button" value="Delete"/>
Ethernet Type	<input checked="" type="radio"/> Any <input type="radio"/> <input type="text" value=""/>	Hex <input type="button" value="Delete"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

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.



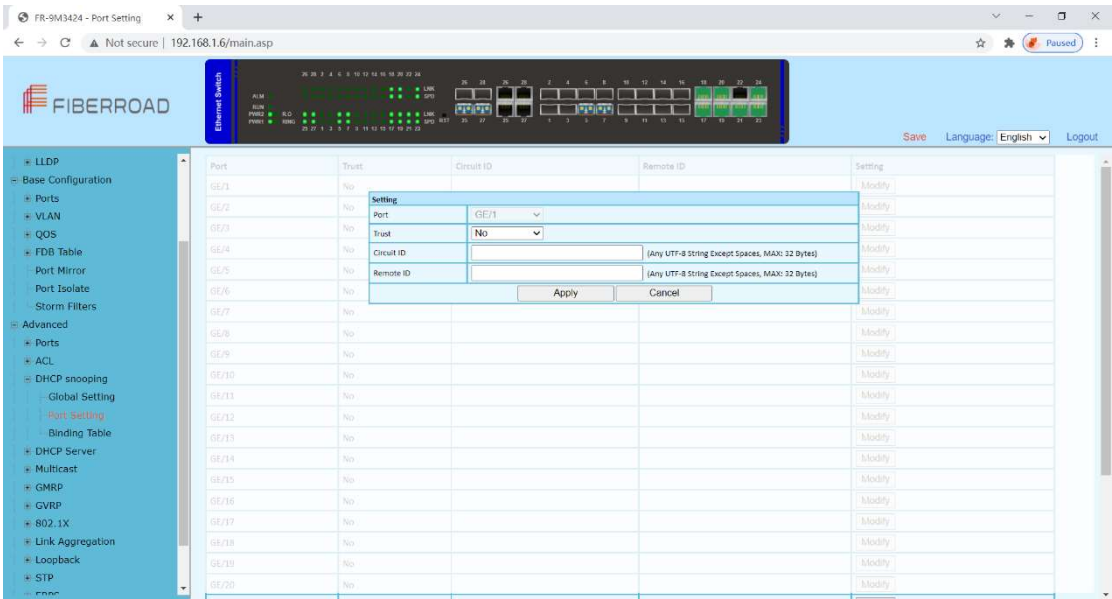
Configuration Steps

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].

DHCP snooping Global Setting	
Admin Status	Off
DHCP option 82	Off
<div>Apply</div>	

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

4.3.2 Advanced Configuration – DHCP snooping – Port Setting

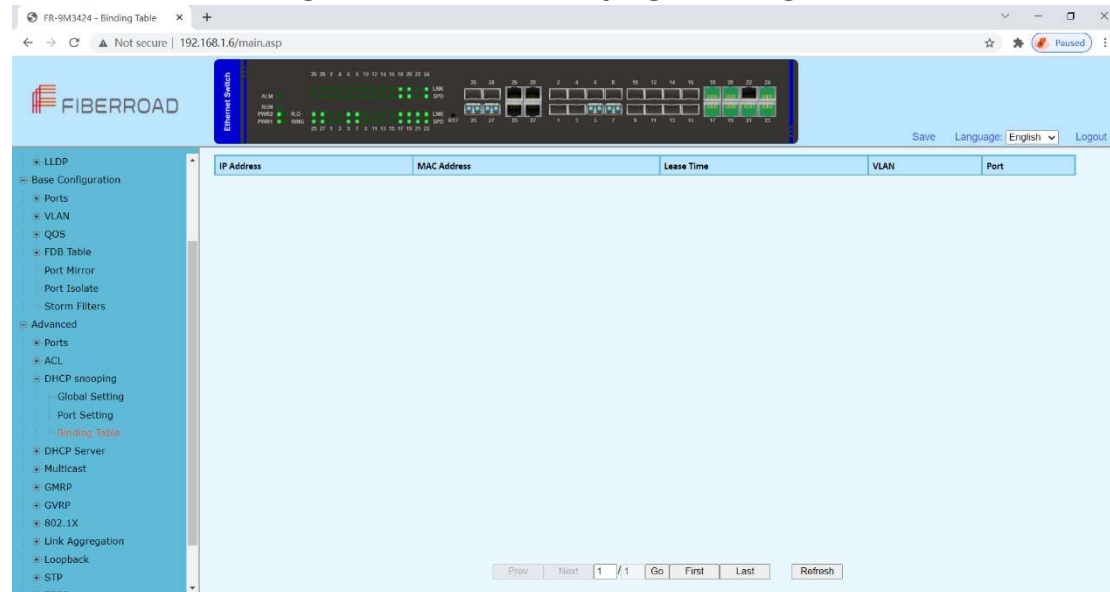


Configuration Steps

- 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



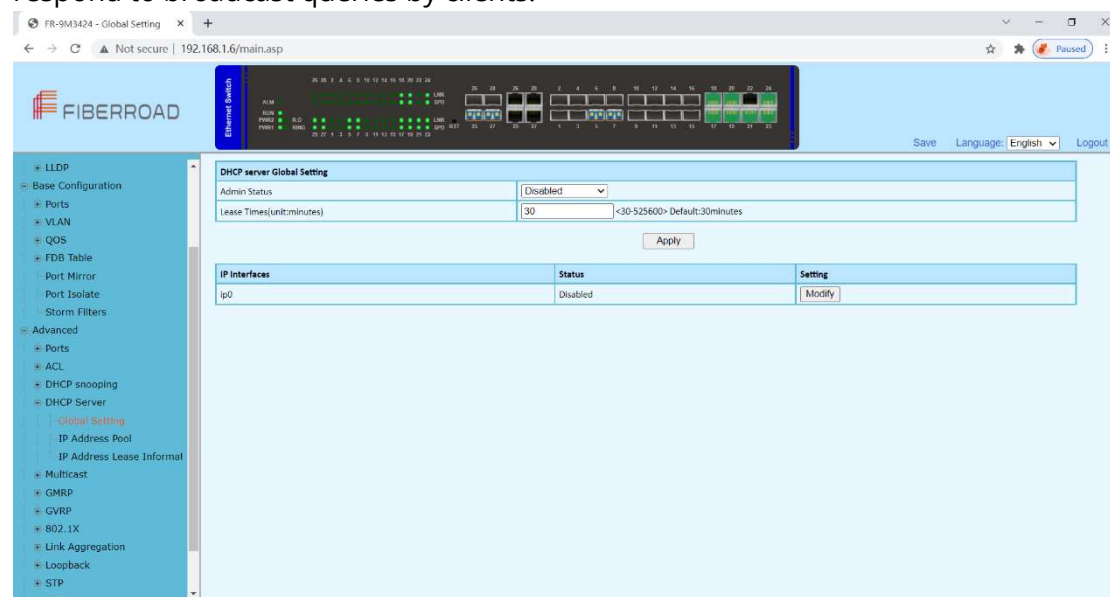
Configuration Steps

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 known 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.

Setting

IP Interfaces

ip0

Status

Disabled

Apply

Cancel

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.

← → ↻ ⚠ Not secure | 192.168.1.6/main.asp

FIBERROAD

Ethernet Switch

Save

Language: Auto

Logout

Expand | Collapse

Device Summary

System

Management

Base Configuration

Advanced

- Ports
 - Port Security
- ACL
 - ACL Group Setting
 - ACL Rule Setting
- DHCP snooping
 - Global Setting
 - Port Setting
 - Binding Table
- DHCP Server
 - Global Setting
 - IP Address Pool
 - IP Address Lease Information
- Multicast
- GMRP
- GVRP
- 802.1X
- Link Aggregation

Index

Pool Name

IP Interface

Start IP Address

End IP Address

Subnet Mask

Lease Times(minutes)

Default Gateway

DNS Server

Secondary DNS Server

Static IP Address

Setting

Pool Name

IP Interface

--

Start IP Address

(IPv4(A.B.C.D))

End IP Address

(IPv4(A.B.C.D))

Subnet Mask

(IPv4(A.B.C.D))

Lease Times

No

Yes

<30-525600>minutes

Default Gateway

No

Yes

(IPv4(A.B.C.D))

DNS Server

No

Yes

(IPv4(A.B.C.D))

Secondary DNS Server

No

Yes

(IPv4(A.B.C.D))

Static IP Address

Add

IP:

MAC:

Delete

Apply

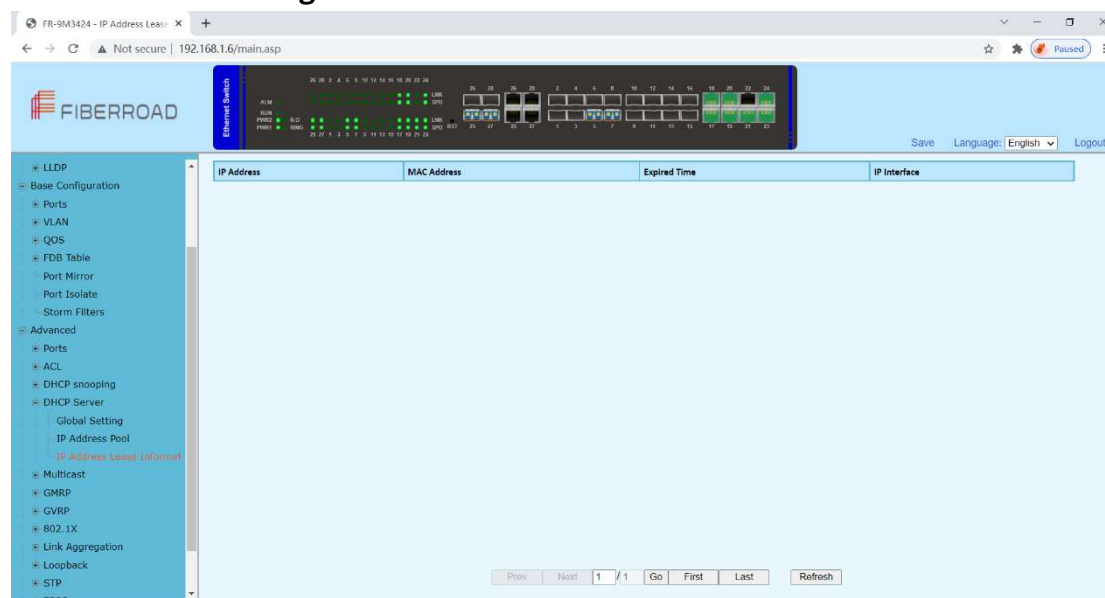
Cancel

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.

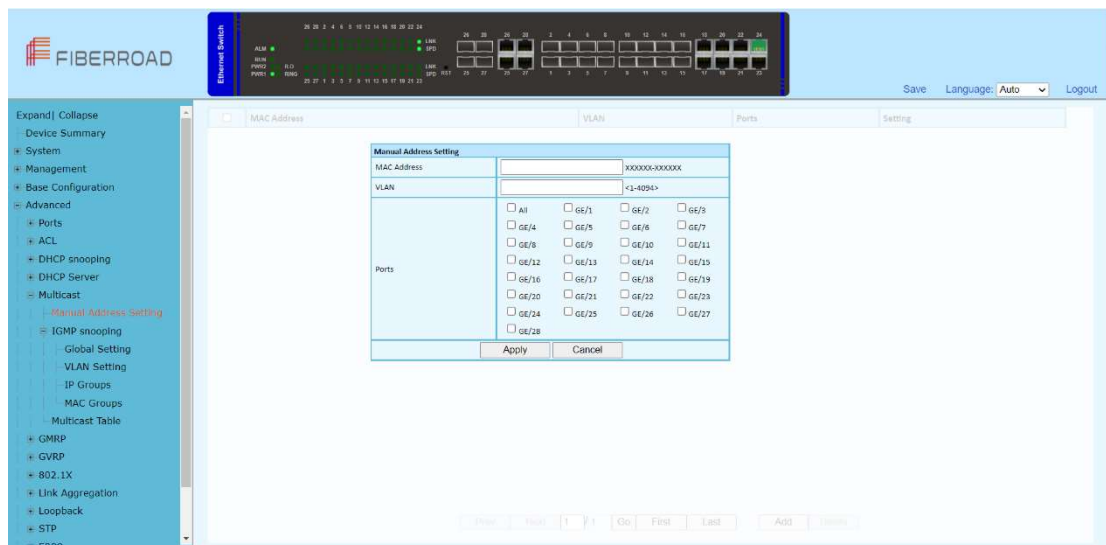
Lease Information] interface.

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.

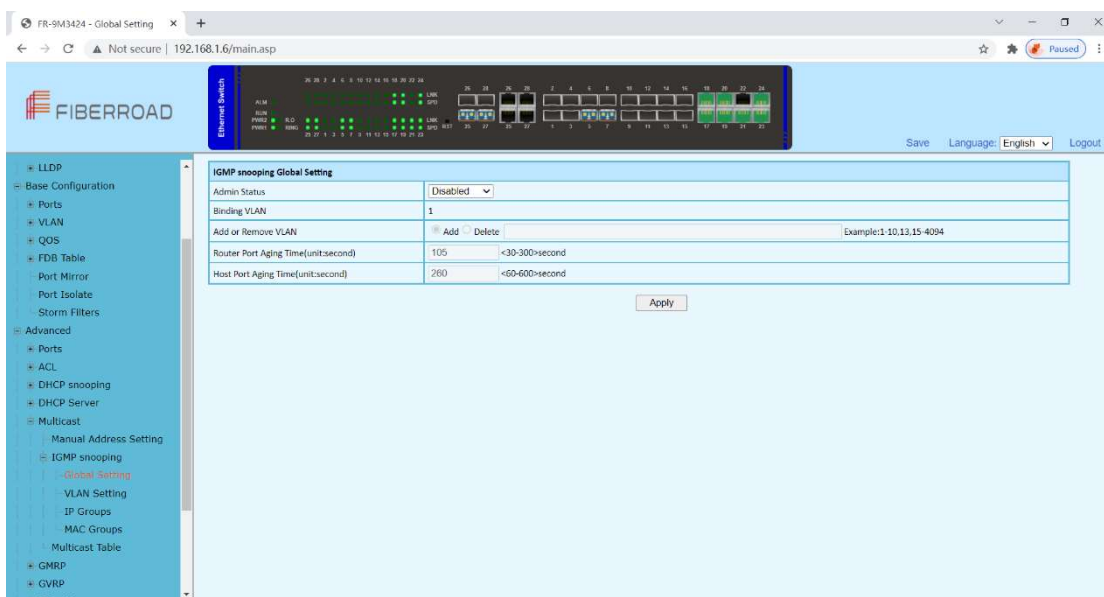


Configuration Steps

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.



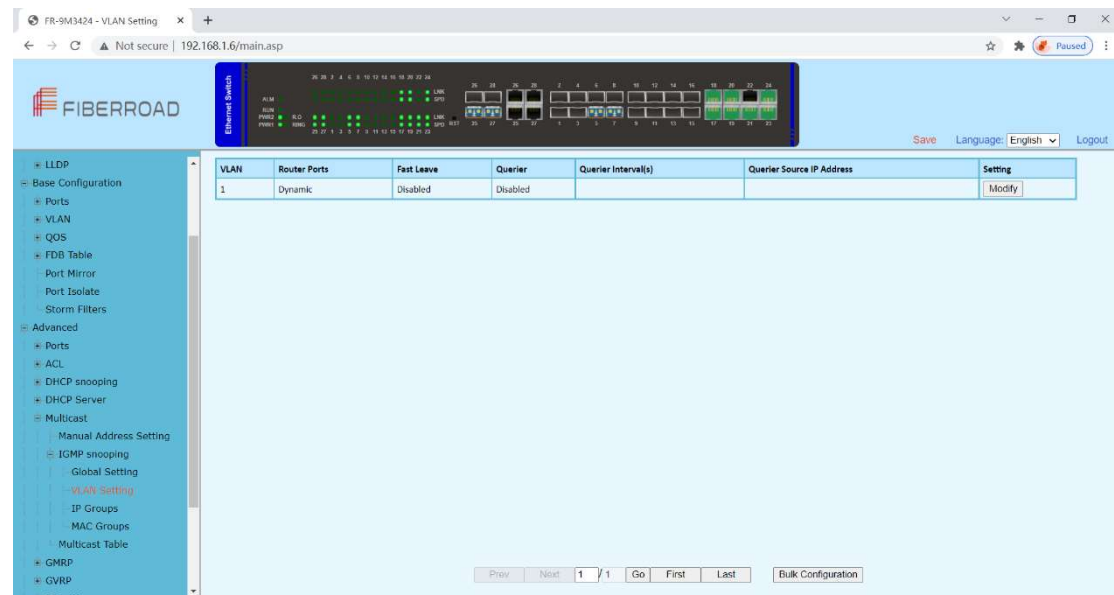
Configuration Steps

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

VLAN	Router Ports	Fast Leave	Querier	Querier Interval(s)	Querier Source IP Address	Setting
1	Dynamic	Disabled	Disabled			Modify

Prev Next 1 / 1 Go Home Tail Bulk Configuration

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.

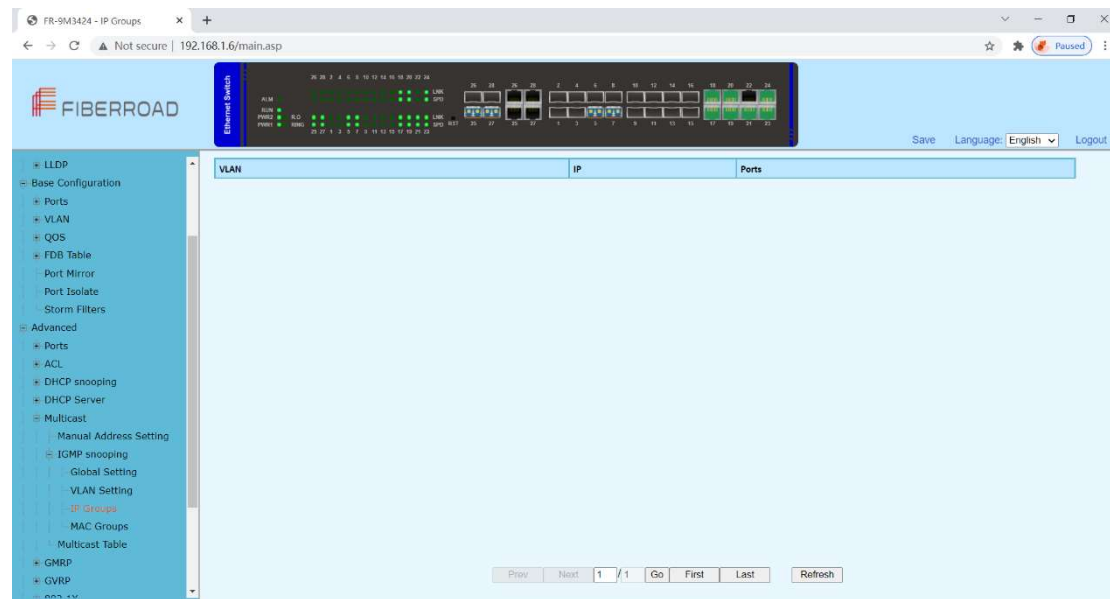
VLAN Setting	
VLAN	1 <1-4094>
Router Port Mode	Dynamic
Fast Leave	Disabled
Querier	Disabled
Querier Interval	60 s <30-120>s
Querier Source IP Address	0.0.0.0 A.B.C.D
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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.

VLAN Bulk Configuration	
VLAN List	<input type="text"/> Example:1-10,13,15-4094
Router Port Mode	<input type="checkbox"/> Dynamic
Fast Leave	<input type="checkbox"/> Disabled
Querier	<input type="checkbox"/> Disabled
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Item	Description	Notes
VLAN	VLAN being configured	
Router Port Mode	<p>Select the mode of the routed port in this VLAN. Use the drop-down box to modify it.</p> <p>Dynamic</p> <p>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.</p>	
Fast Leave Mode	<p>Select whether to enable the quick leave mode under this VLAN. Use the drop-down box to modify it.</p> <p>Disabled</p> <p>Enabled</p>	
Querier	<p>Select whether to enable the querier function in this VLAN. Use the drop-down box to modify it.</p> <p>Disabled</p> <p>Enable - If the querier is enabled, you need to set the corresponding querier interval and query source IP address.</p>	
Query Interval	The query interval of the querier is 30-120 seconds.	
Querier 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

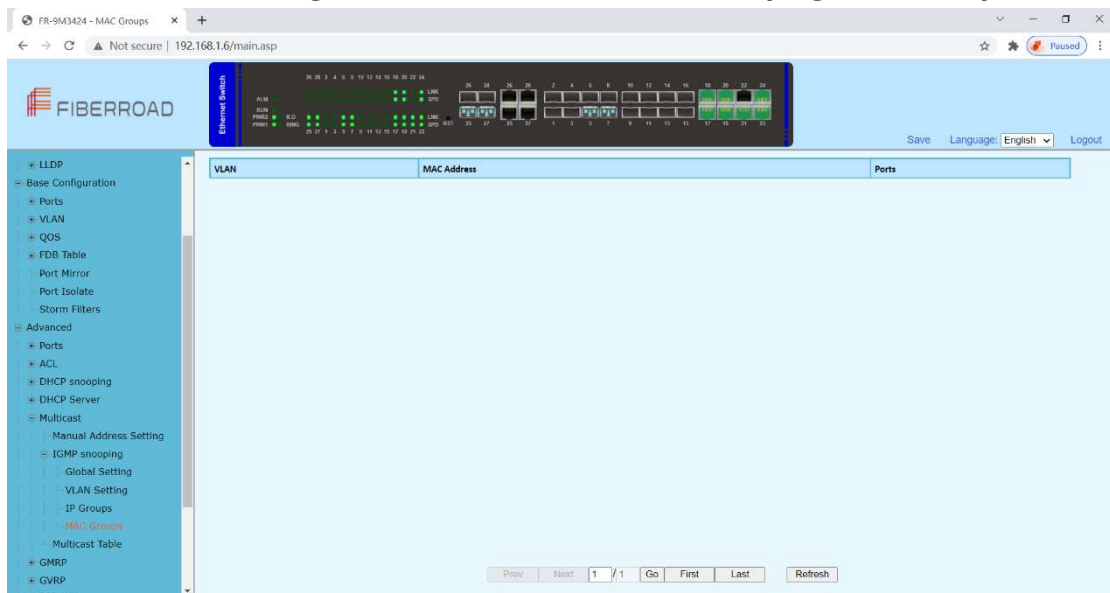


Configuration Steps

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].

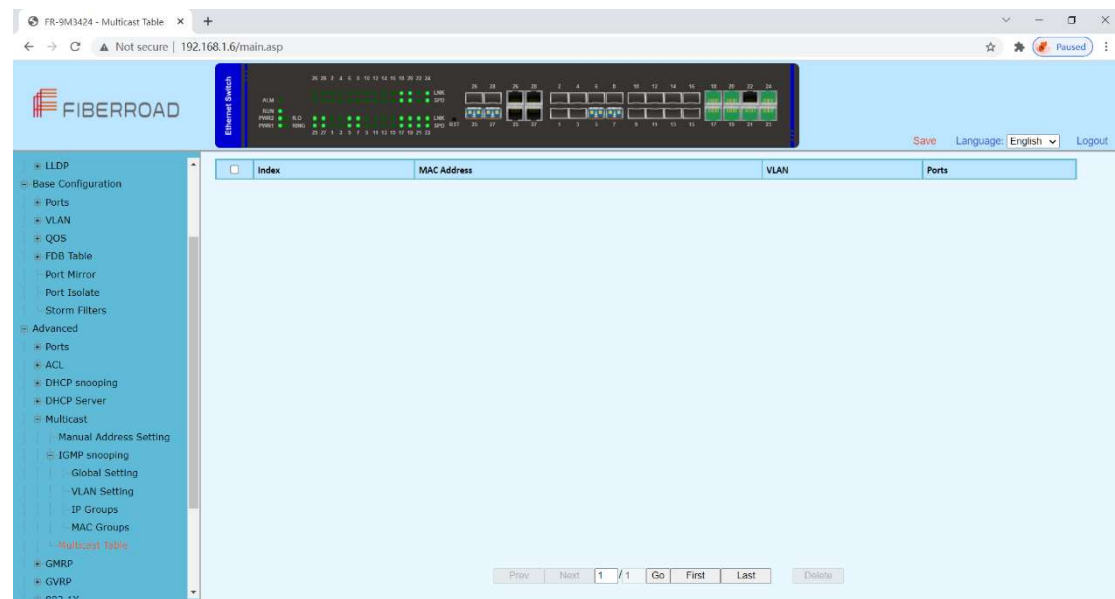
4.5.5 Advanced Configuration – Multicast – IGMP snooping MAC Groups



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



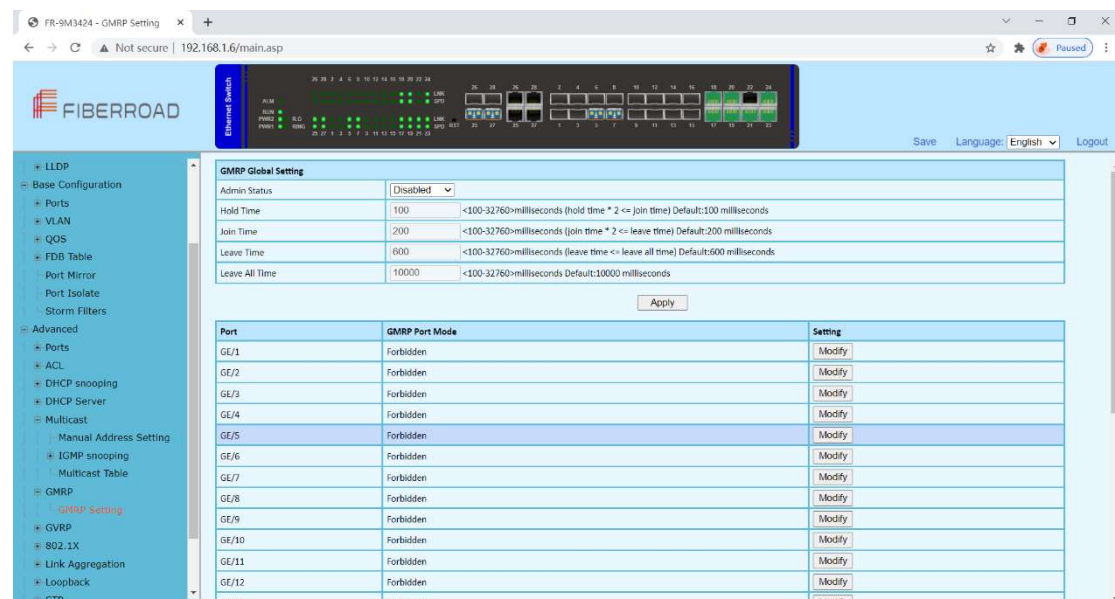
Configuration Steps

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

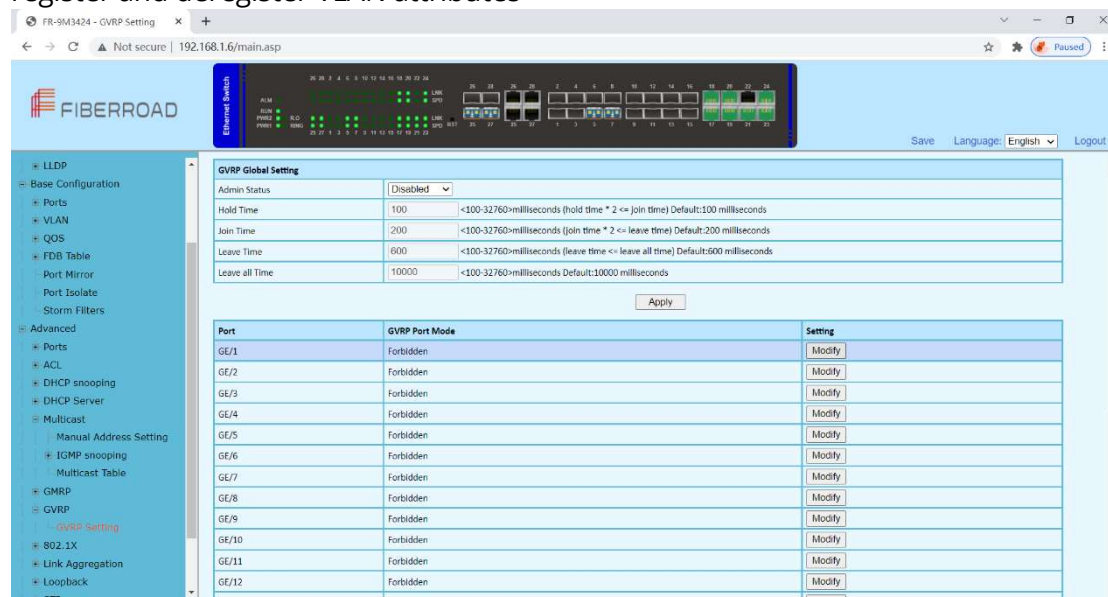
GMRP Port Mode	
Port	GE/1
GMRP Mode	<input type="radio"/> Normal <input type="radio"/> Fixed <input checked="" type="radio"/> Forbidden
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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 (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

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.

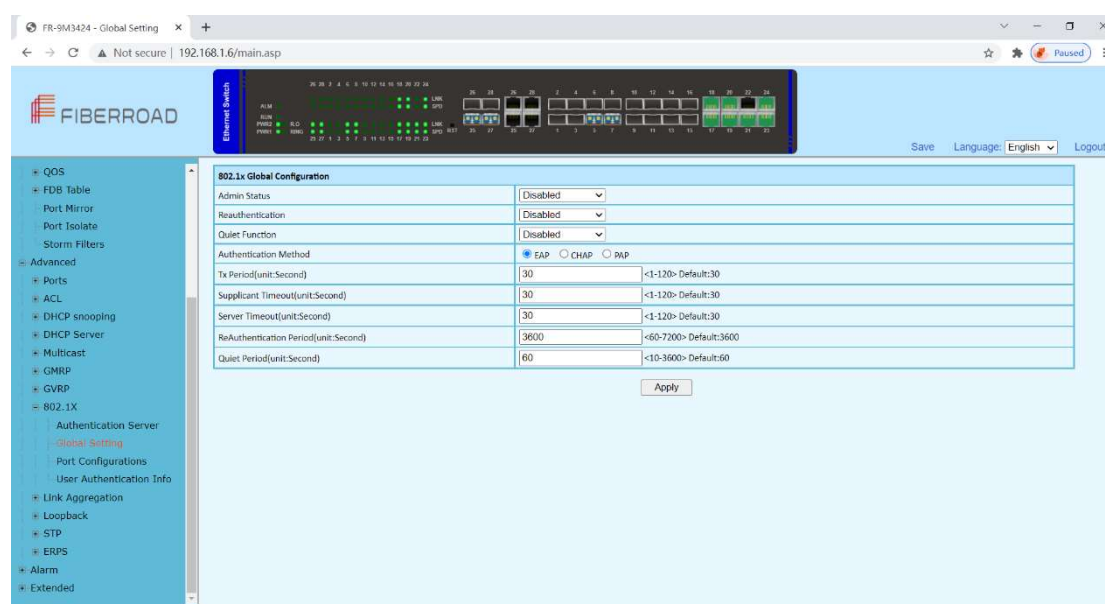
Configuration Steps

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,	Default:1812

Shared Key

range<1-65535>, default with 1812
 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	1-120	Default: 30

TIMEOUT (UNIT: SECOND)		
SERVER TIMEOUT (UNIT:SECOND)	1-120	Default: 30
REAUTHENTICATION PERIOD (UNIT:SECOND)	60-7200	Default: 3600
QUIET PERIOD (UNIT:SECOND)	10-3600	Default: 60

4.8.3 Advanced Configuration – 802.1X – Port Configurations

Port	Admin Status	Authentication Control	Authentication Mode	Max Host Number	Setting
GE/1	Disabled	Auto	PortBased	8	Modify
GE/2	Disabled	Auto	PortBased	8	Modify
GE/3	Disabled	Auto	PortBased	8	Modify
GE/4	Disabled	Auto	PortBased	8	Modify
GE/5	Disabled	Auto	PortBased	8	Modify
GE/6	Disabled	Auto	PortBased	8	Modify
GE/7	Disabled	Auto	PortBased	8	Modify
GE/8	Disabled	Auto	PortBased	8	Modify
GE/9	Disabled	Auto	PortBased	8	Modify
GE/10	Disabled	Auto	PortBased	8	Modify
GE/11	Disabled	Auto	PortBased	8	Modify
GE/12	Disabled	Auto	PortBased	8	Modify
GE/13	Disabled	Auto	PortBased	8	Modify
GE/14	Disabled	Auto	PortBased	8	Modify
GE/15	Disabled	Auto	PortBased	8	Modify
GE/16	Disabled	Auto	PortBased	8	Modify
GE/17	Disabled	Auto	PortBased	8	Modify
GE/18	Disabled	Auto	PortBased	8	Modify
GE/19	Disabled	Auto	PortBased	8	Modify
GE/20	Disabled	Auto	PortBased	8	Modify

Configuration Steps

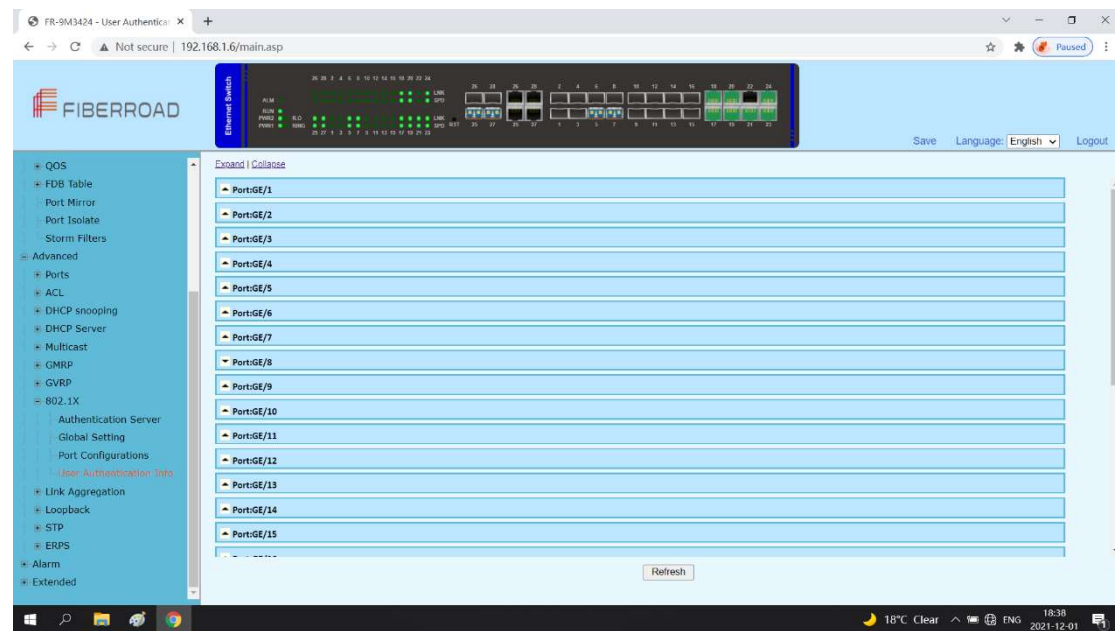
1. Select [Advanced / 802.1X / Port Configurations] in the navigation bar to enter the [Port Configurations] interface.
2. On the [Port Configurations] interface, you can view the configuration information of each port, the current 802.1X configuration information of each port is displayed.
3. To modify 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.

802.1X Port Configurations	
Port	GE/5
Admin Status	Disabled
Authentication Control	Auto
Authentication Mode	PortBased
Max Host Number	8 <1-8> Default:8
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	



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



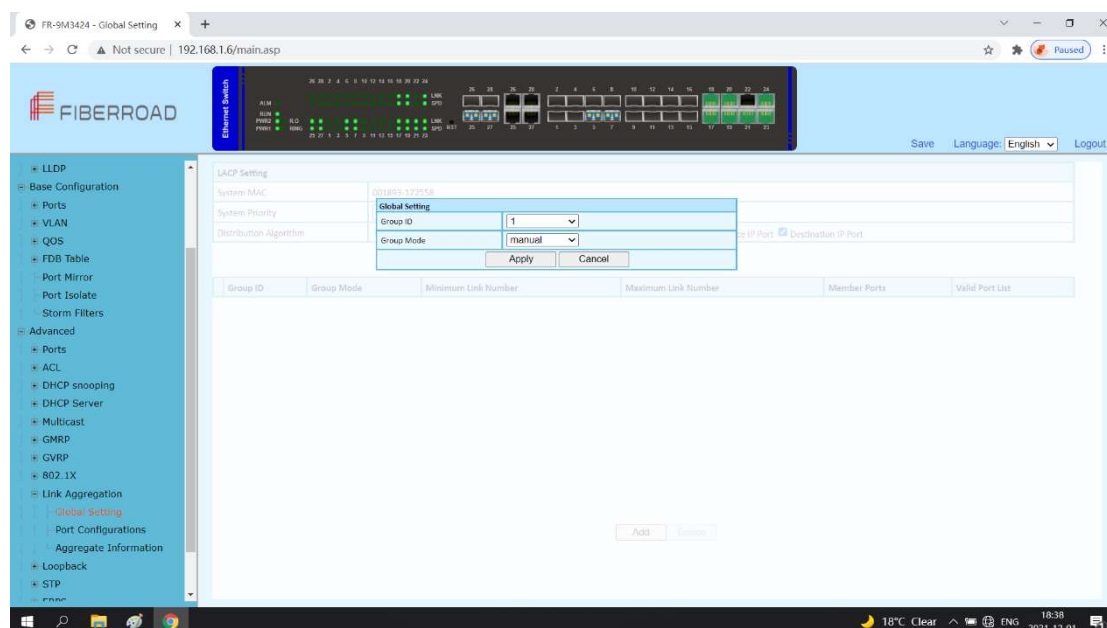
Configuration Steps

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	

Minimum Port

closed.

Static: Static mode, the port of the aggregation group member is manually configured and the port LACP protocol is on.

The active ports minimum number of aggregation group configuration, ranging <0-8>, and the value cannot exceed the maximum number of links.

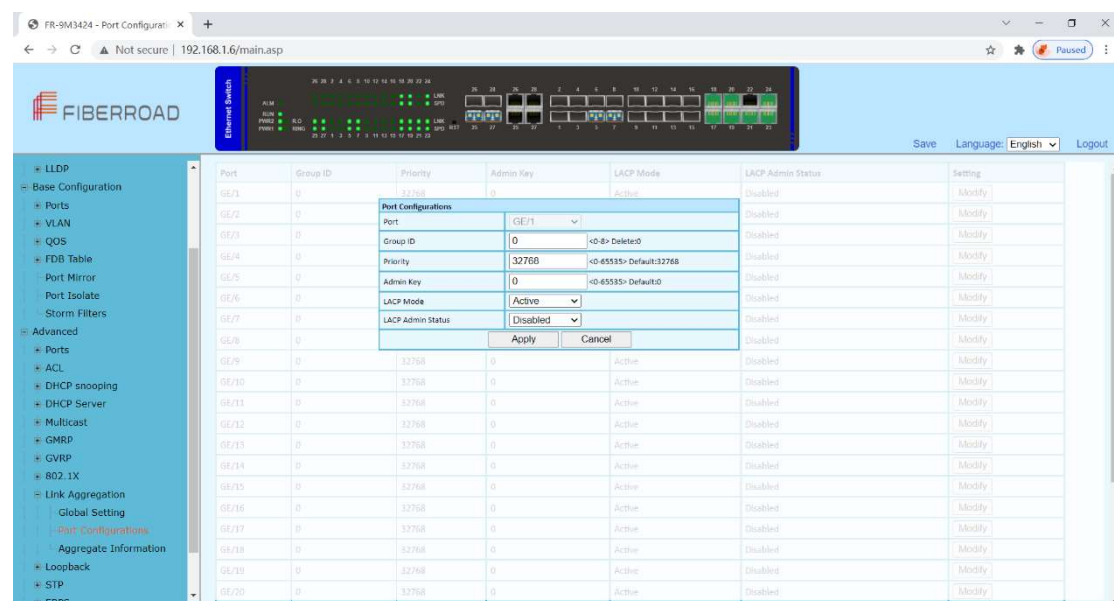
Maximum Port

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 Configurations

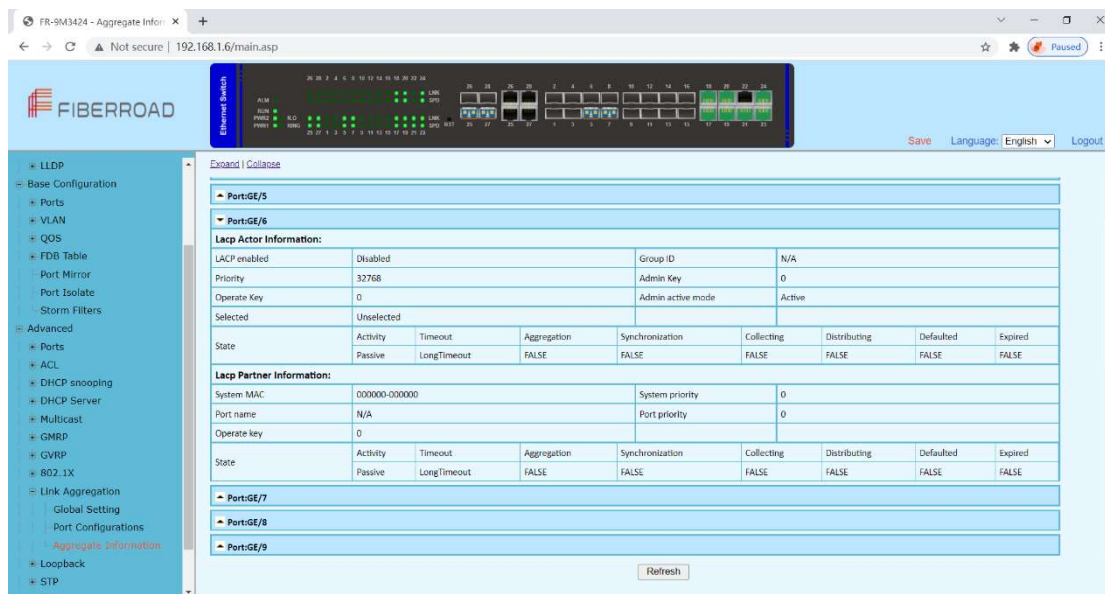


Configuration Steps

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

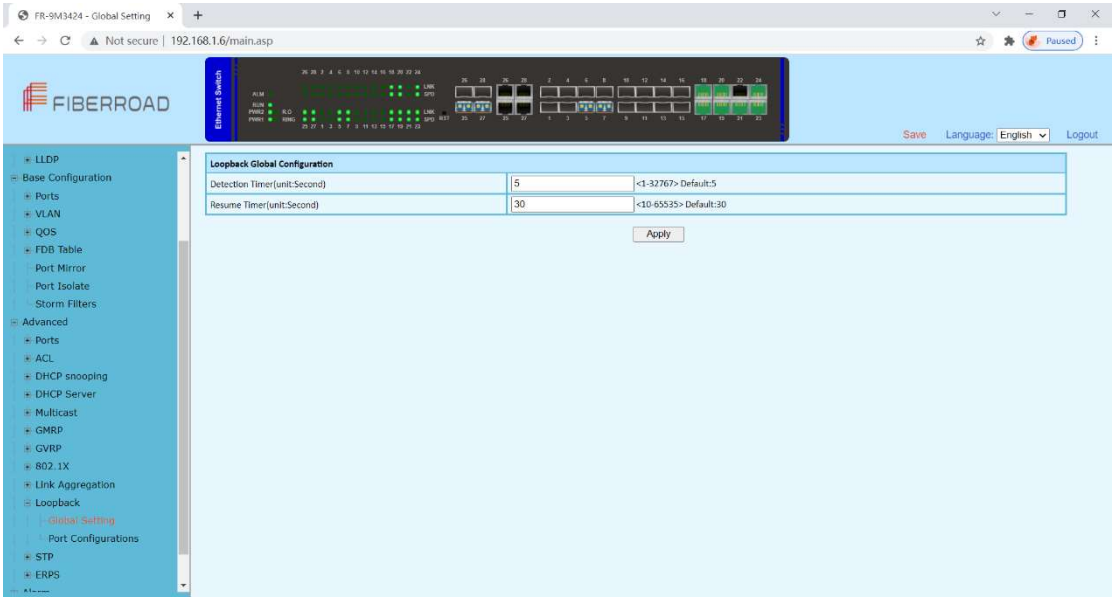


Configuration Steps

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

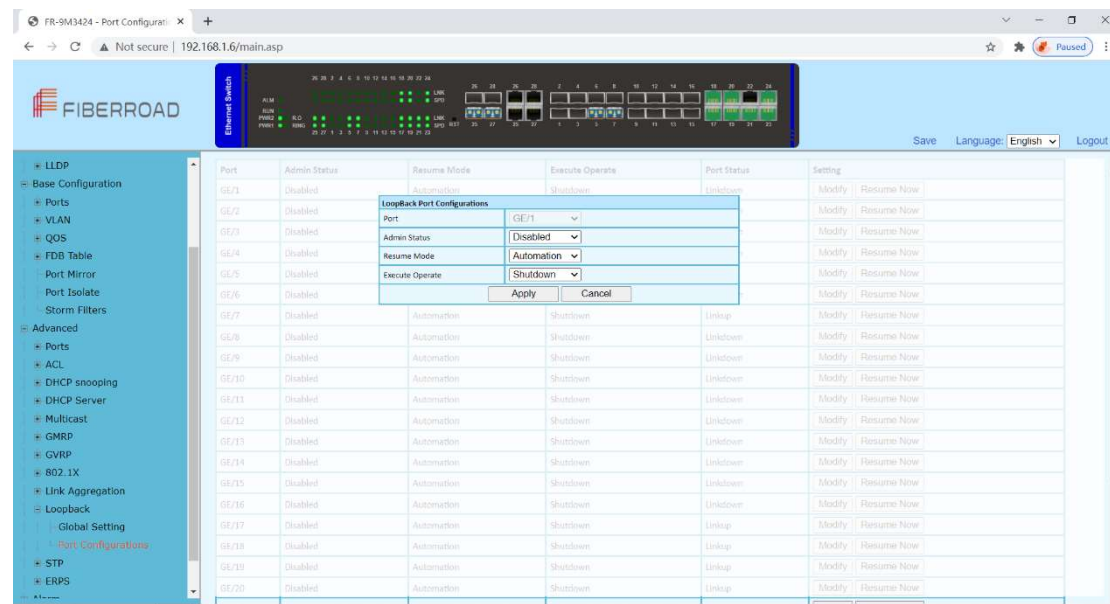


Configuration Steps

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	Automation	Shutdown	Linkdown	Modify Resume Now
GE/2	Disabled	Automation	Shutdown	Linkdown	Modify Resume Now
GE/3	Disabled	Automation	Shutdown	Linkdown	Modify Resume Now
GE/4	Disabled	Automation	Shutdown	Linkdown	Modify Resume Now
GE/5	Disabled	Automation	Shutdown	Linkdown	Modify Resume Now
GE/6	Disabled	Automation	Shutdown	Linkdown	Modify Resume Now
GE/7	Disabled	Automation	Shutdown	Linkdown	Modify Resume Now
GE/8	Disabled	Automation	Shutdown	Linkup	Modify Resume Now
GE/9	Disabled	Automation	Shutdown	Linkdown	Modify Resume Now
GE/10	Disabled	Automation	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.

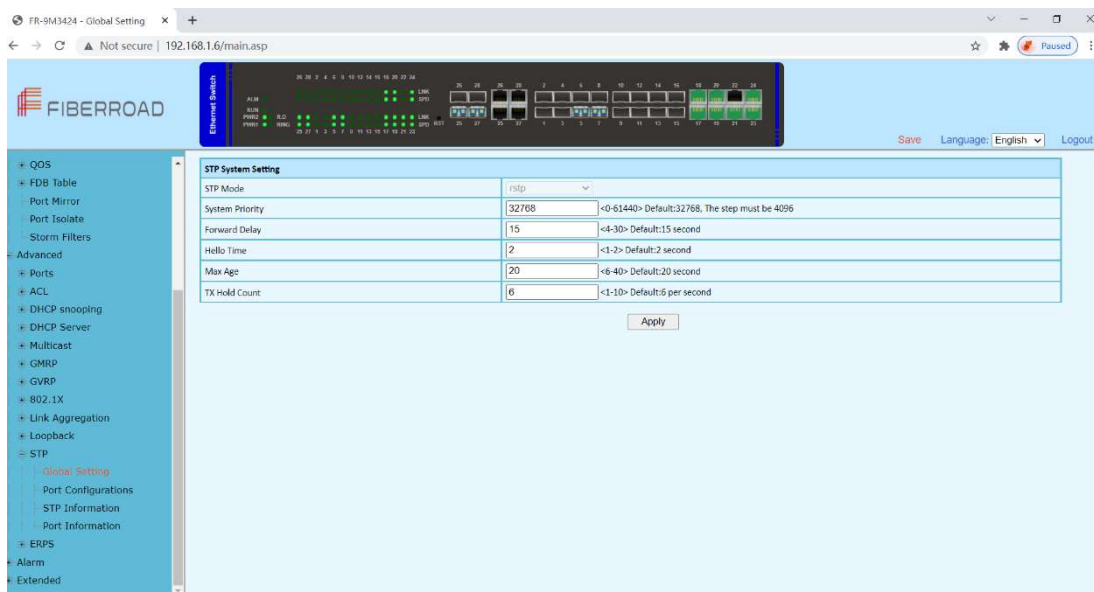
LoopBack Port Configurations	
Port	GE/7
Admin Status	Disabled
Resume Mode	Automation
Execute Operate	Shutdown
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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 Configuration – Global Setting

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 / Global Setting] in the navigation bar to enter the STP[Global Setting] interface.
2. The STP global setting information can be viewed in the [Global Setting] 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	Support RSTP, Compatible with STP	
System 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
Hello Time	The time interval sent by STP protocol message in stable state, Range<1-2>	Default: 2sec
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
TX Hold Count	The maximum number of STP protocol packets sent by Port per second. Range<1-10>	Default: 6 per sec

4.11.2 Advanced Configuration – Port Configuration

The screenshot shows the FiberRoad web interface for STP Port Configuration. The main content area contains a table with the following data:

Port	STP Admin Status	Priority	Path Cost Mode	Path Cost
GE/1	Disabled	128	Auto	0
GE/2	Disabled	128	Auto	0
GE/3	Disabled	128	Auto	0
GE/4	Disabled	128	Auto	0
GE/5	Disabled	128	Auto	0
GE/6	Disabled	128	Auto	0
GE/7	Disabled	128	Auto	0
GE/8	Disabled	128	Auto	0
GE/9	Disabled	128	Auto	0
GE/10	Disabled	128	Auto	0
GE/11	Disabled	128	Auto	0
GE/12	Disabled	128	Auto	0
GE/13	Disabled	128	Auto	0
GE/14	Disabled	128	Auto	0
GE/15	Disabled	128	Auto	0
GE/16	Disabled	128	Auto	0
GE/17	Disabled	128	Auto	0

The interface includes a left sidebar with a navigation menu, a top status bar, and a bottom 'Apply' button.

Configuration Steps

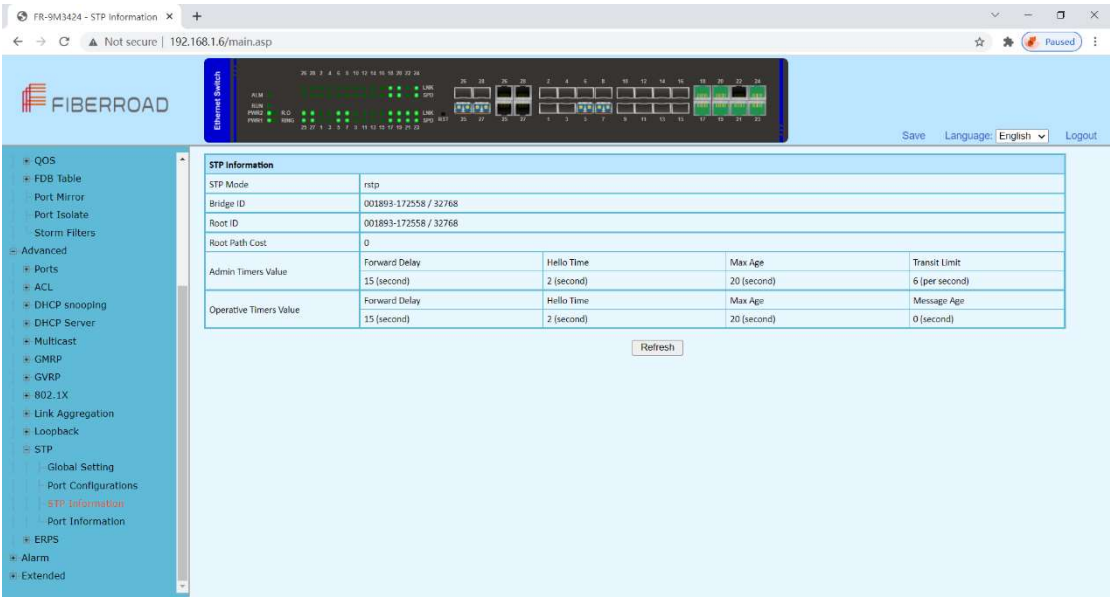
1. Select [Advanced / STP / Port Configurations] in the navigation bar to enter the STP [Port Configurations] interface.
2. The STP port configuration information can be viewed in the [Port Configurations] interface.
3. To modify the port configuration, you can click [Modify] on the right side of the corresponding port to enter the port configuration interface of the STP.

Item	Description	Notes
Port	Port Name	
STP Admin Status	Enabled / Disabled	Default: Disabled
Priority	Every switch taking part in spanning tree has a bridge priority. The switch with the lowest priority becomes the root bridge. If there's a tie, then the switch with the lowest bridge ID number wins. The ID number is typically derived from a MAC address on the switch.	
Path Cost Mode	The calculation of STP port path overhead, [Auto] or [Managed]	Default: Auto
Path Cost	Path cost - The path cost is the metric STP uses to calculate the shortest path to elect root port to reach the root-bridge .	

Remarks: The STP BPDU message requires a certain Path overhead for each Root port. The Path overhead of each bridge is cumulative, and this value is called Root Path Cost. The path overhead is different corresponding to the root ports of different rates, as shown in the following table:

Port Rate	Path Cost
10Mbps	2,000,000
100Mbps	200,000
1000Mbps	20,000

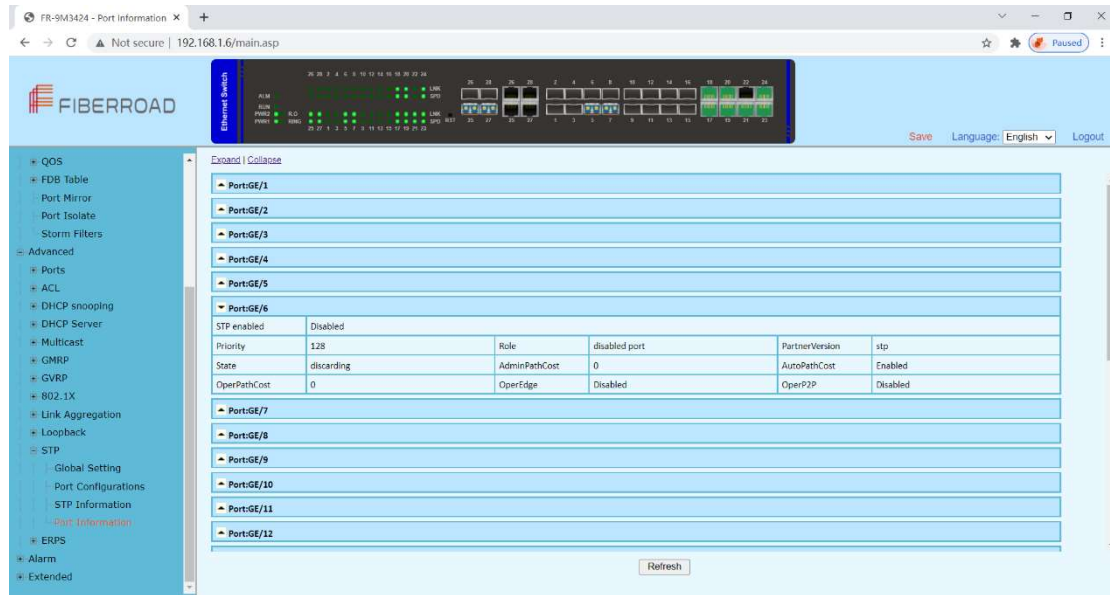
4.11.3 Advanced Configuration – STP Information



Configuration Step

1. Select [Advanced / STP / STP Informations] in the navigation bar and enter the STP [STP informations] interface.
2. The STP current running information can be viewed in the [STP informations] interface, as shown in figure 7.3
3. Click [Refresh] to show the latest running information.

4.11.3 Advanced Configuration – STP Information



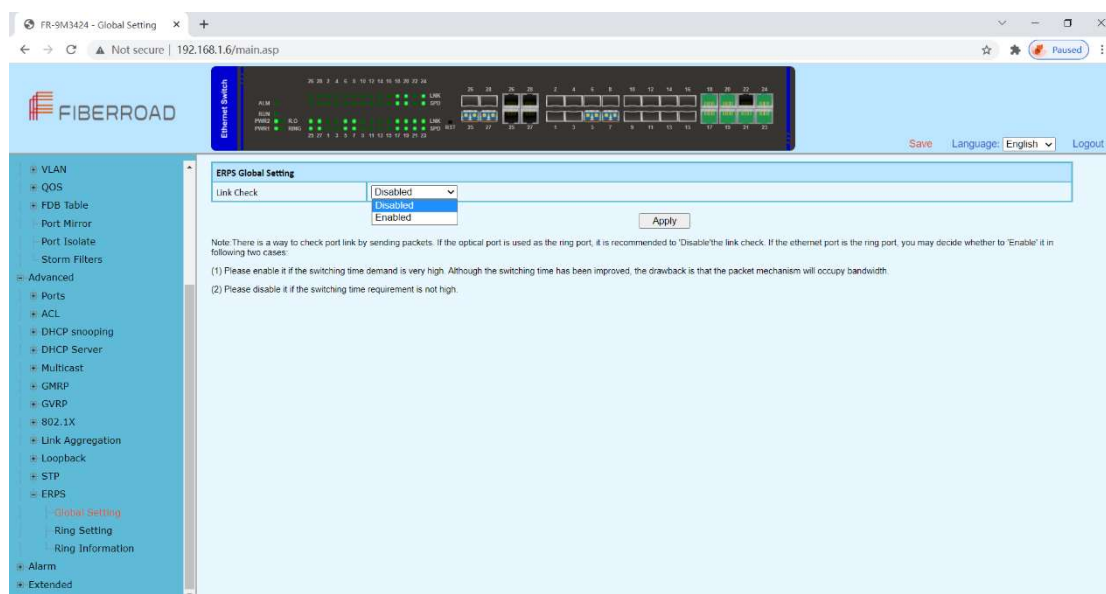
Configuration Step

1. Select [Advanced / STP / Port Information] in the navigation bar and enter the STP [Port information] interface.
2. The STP current running information can be viewed in the [Port Information] interface, as shown in figure 7.4
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.

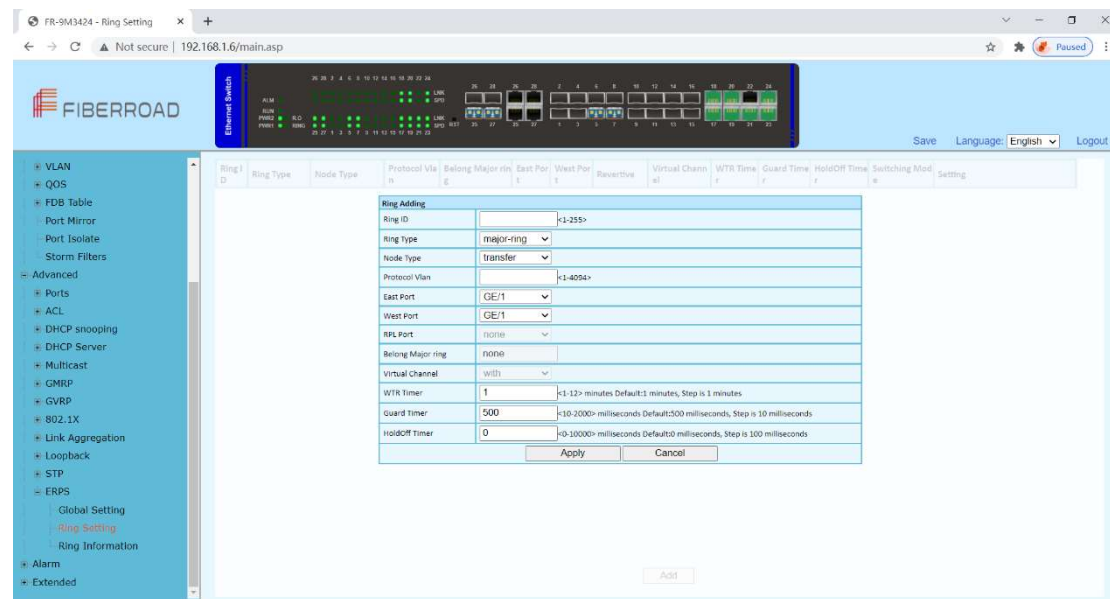


Configuration Step

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



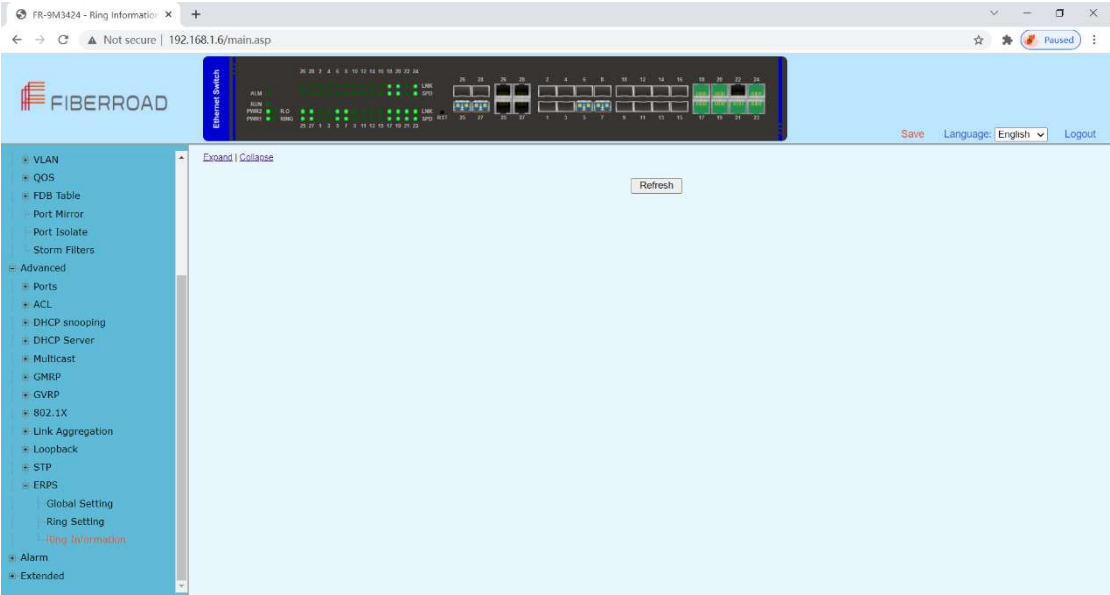
Configuration Step

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	<p>Transfer: Forward both service packets and protocol packets</p> <p>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.</p> <p>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.</p>	
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	
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



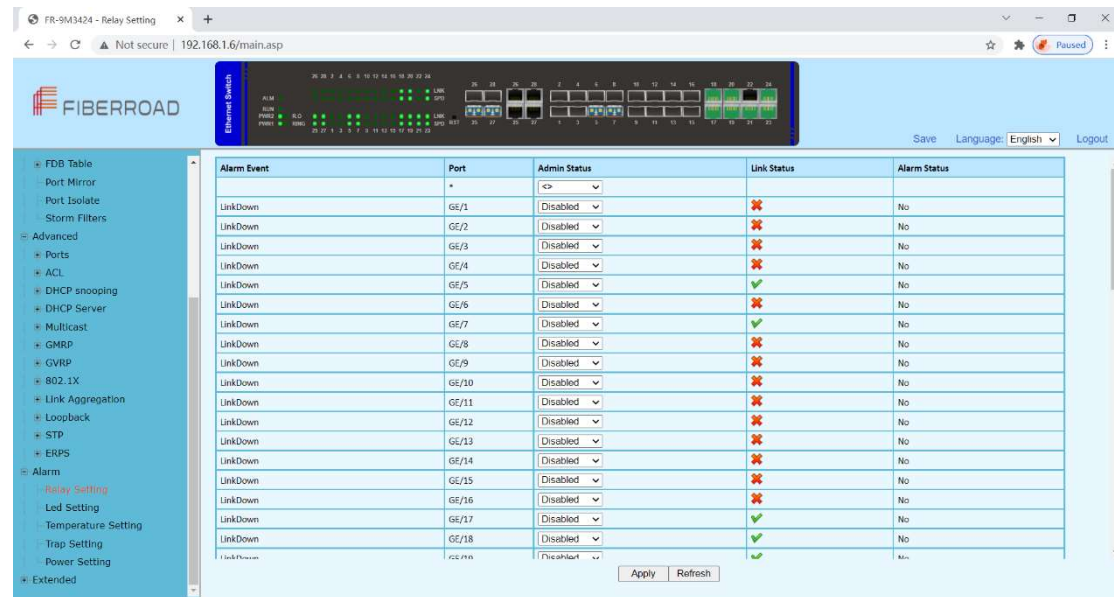
Configuration Step

- 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, as shown in figure 8.5.
- 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 Advanced Configuration – Alarm

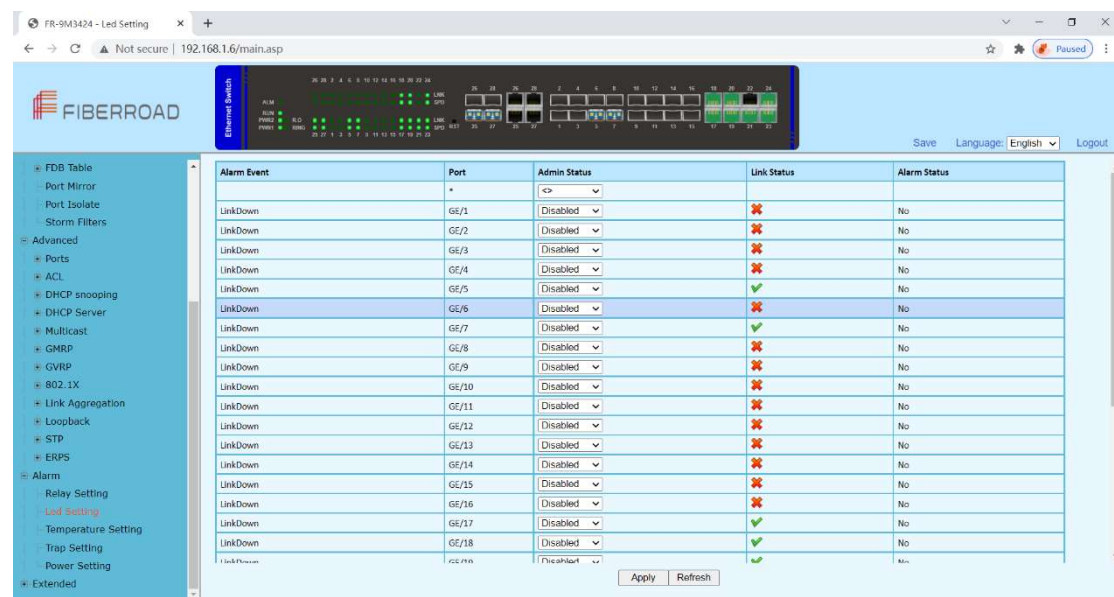
4.13.1 Advanced Configuration – Alarm – Relay Setting



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.

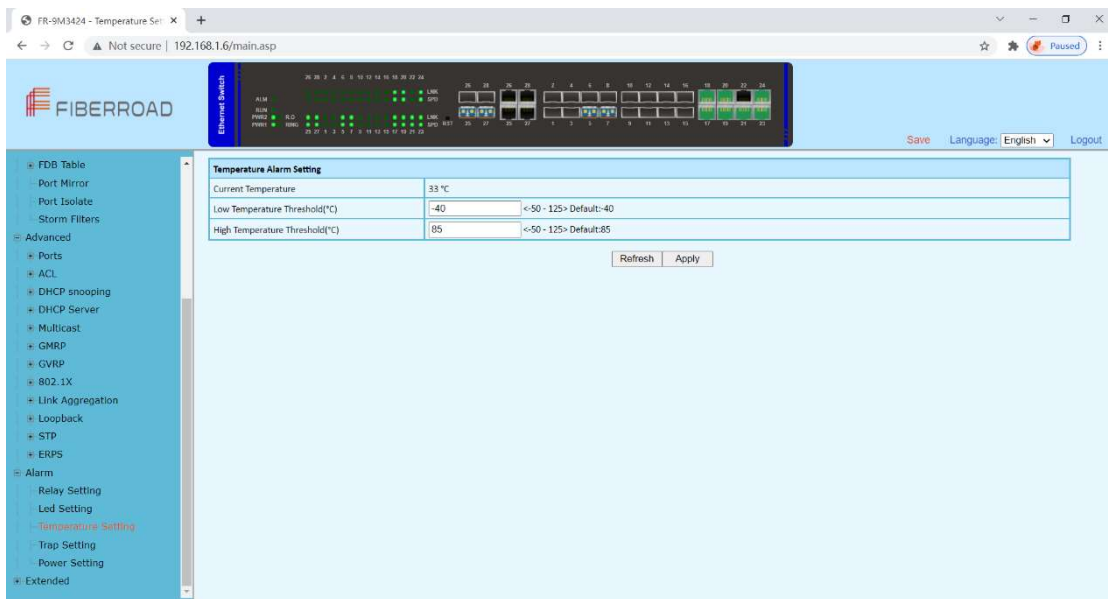
4.13.2 Advanced Configuration – Alarm – Led Setting



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.

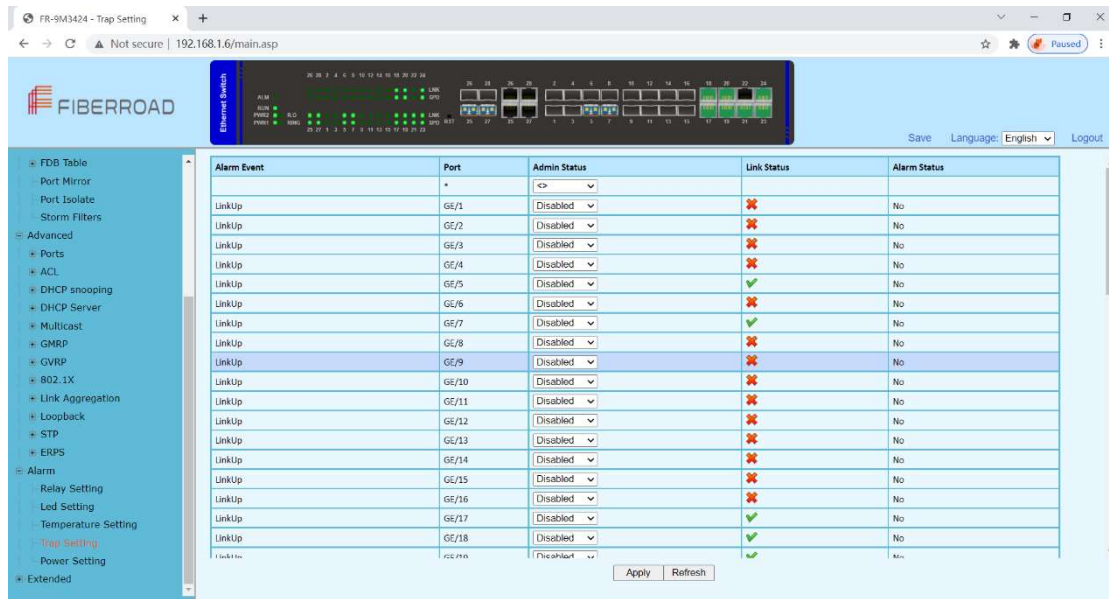
4.13.3 Advanced Configuration – Alarm – Temperature Setting



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(°C), Click[Apply] to submit the modification.
4. Click [Refresh] to show the latest information.

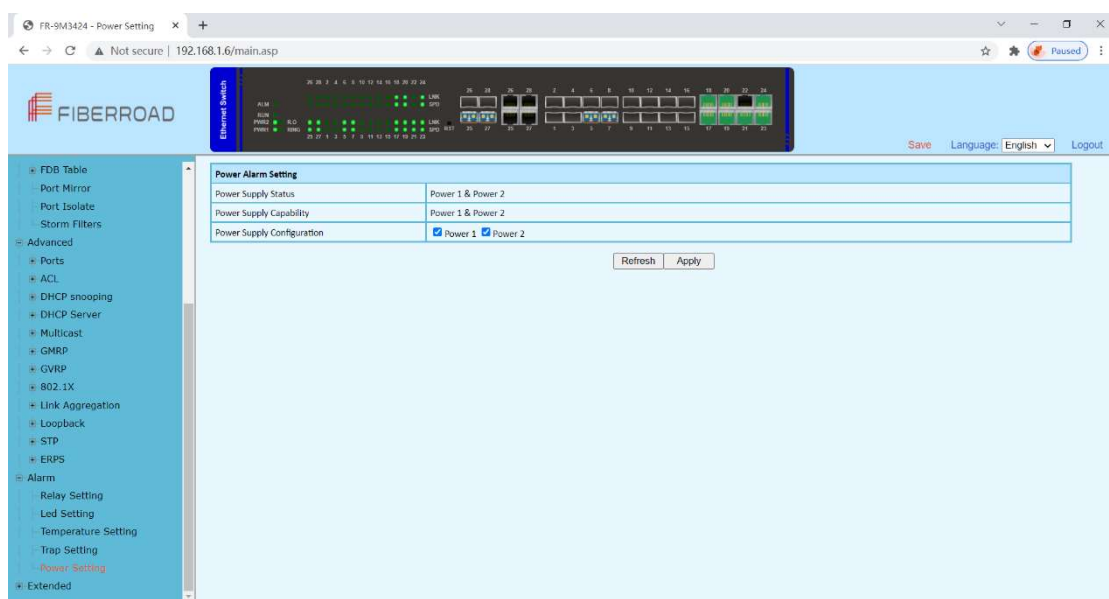
4.13.4 Advanced Configuration – Alarm – Trap Setting



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



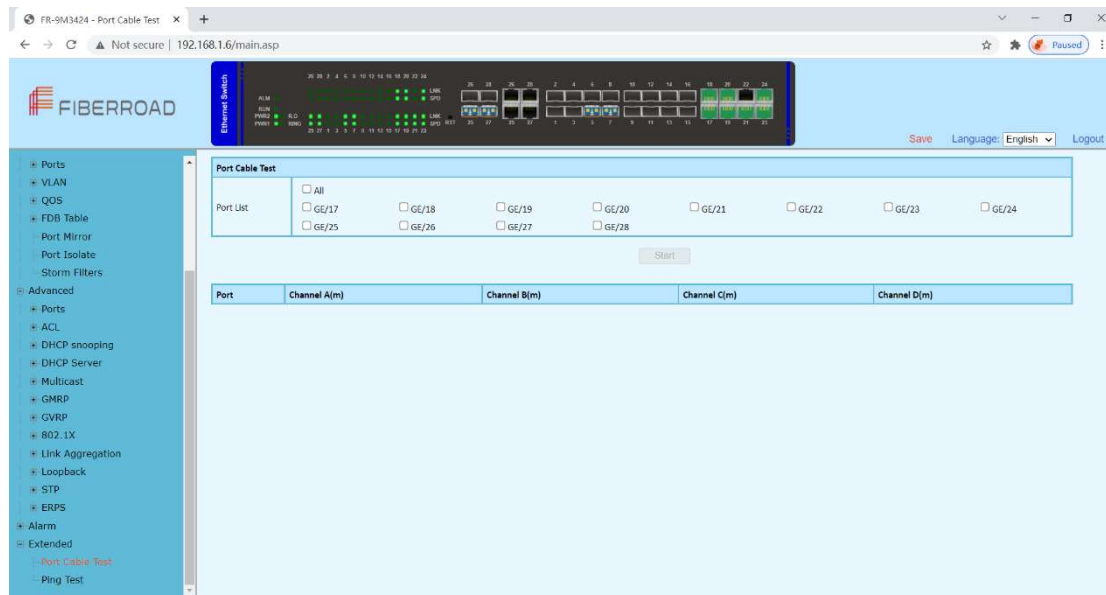
Configuration Steps

1. Select [Advanced / Alarm /Power Setting] in the navigation bar to enter the interface of Alarm [Power Supply].
2. The power Alarm Setting can be viewed in the [Power Setting] interface
- 3 Select required power supply configuration ,Click[Apply] to submit the modification.
4. Click [Refresh] to show the latest information.

4.14 Advanced Configuration – Extended

4.14.1 Advanced Configuration – 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.

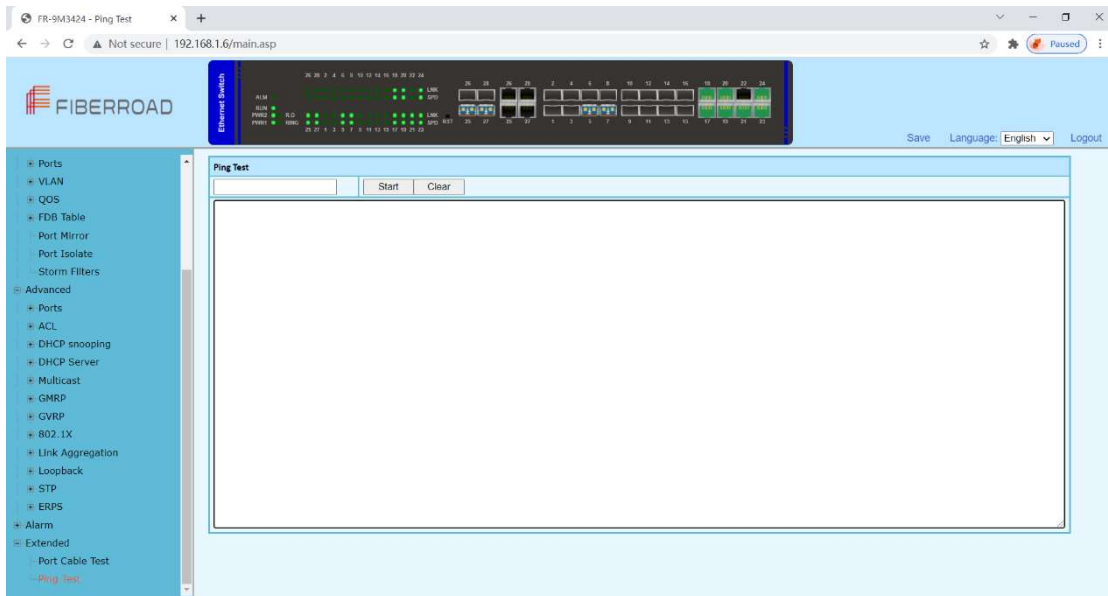


Configuration Step

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.

4.14.2 Advanced Configuration – 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..

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., Ltd

www.fiberroad.com

Sales Support: sales@fiberroad.com

Technical Support: tech@fiberroad.com

Service Support: service@fiberroad.com

