



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.....	39
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.....	41
3.3.2 Base Configuration-QoS- Mapping – DSCP Priority.....	42
3.3.3 Base Configuration-QoS- Mapping – Local Priority	43
3.4 Base Configuration-QoS- Ports.....	44
3.4.1 Base Configuration-QoS- Ports-Port Priority	44
3.4.2 Base Configuration-QoS- Ports-Rate Limitation	45
3.5 Base Configuration-FDB Table.....	46
3.5.1 Base Configuration-FDB Table- Configuration – Aging Setting	46
3.5.2 Base Configuration-FDB Table- Configuration – Static Mac Entry	47
3.5.3 Base Configuration-FDB Table- Configuration – Port Learning Ability	48
3.5.4 Base Configuration-FDB Table- FDB Table.....	49
3.5.5 Base Configuration-FDB Table- Delete Entries	50
3.5.6 Base Configuration-FDB Table- Port Mirror	51
3.5.7 Base Configuration-FDB Table- Port Isolate	52
3.5.8 Base Configuration-FDB Table- Storm Filters	53
Chapter 4 Advanced Configurations	54
4. Advanced Configuration.....	54

4.1 Advanced Configuration – Ports – Ports Security	54
4.2 Advanced Configuration – ACL	55
4.2.1 Advanced Configuration – ACL – ACL Group Setting.....	55
4.2.2 Advanced Configuration – ACL – ACL Rule Setting.....	57
4.3 Advanced Configuration – DHCP snooping	59
4.3.1 Advanced Configuration – DHCP snooping – Global Setting.....	59
4.3.2 Advanced Configuration – DHCP snooping – Port Setting.....	60
4.3.3 Advanced Configuration – DHCP snooping – Binding Table	61
4.4 Advanced Configuration – DHCP Server	61
4.4.1 Advanced Configuration – DHCP Server – Global Setting.....	61
4.4.2 Advanced Configuration – DHCP Server – IP Address Pool	62
4.4.3 Advanced Configuration – DHCP Server – IP Address Lease Information	63
4.5 Advanced Configuration – Multicast	64
4.5.1 Advanced Configuration – Multicast – Manual Address Setting	64
4.5.2 Advanced Configuration – Multicast – IGMP snooping Global Setting	65
4.5.3 Advanced Configuration – Multicast – IGMP snooping VLAN setting ...	66
4.5.4 Advanced Configuration – Multicast – IGMP snooping IP Groups	68
4.5.5 Advanced Configuration – Multicast – IGMP snooping MAC Groups ..	68
4.5.6 Advanced Configuration – Multicast – IGMP snooping Multicast Table	69
4.6 Advanced Configuration – GMRP	70
4.6.1 Advanced Configuration – GMRP– GMRP Setting.....	70
4.7 Advanced Configuration – GVRP.....	71
4.7.1 Advanced Configuration – GVRP – GVRP Setting.....	71
4.8 Advanced Configuration – 802.1X	73
4.8.1 Advanced Configuration – 802.1X – Authentication Server	73
4.8.2 Advanced Configuration – 802.1X – Global Setting.....	74
4.8.3 Advanced Configuration – 802.1X – Port Configurations.....	75
4.8.4 Advanced Configuration – 802.1X – User Authentication Info	76
4.9 Advanced Configuration – Link Aggregation	77
4.9.1 Advanced Configuration – Link Aggregation – Global Setting.....	77
4.9.2 Advanced Configuration – Link Aggregation – Port Configurations	78

4.9.3 Advanced Configuration – Link Aggregation – Aggregation Information	79
4.10 Advanced Configuration – Loopback	80
4.10.1 Advanced Configuration – Loopback – Global Setting	80
4.10.2 Advanced Configuration – Loopback – Port Configuration	81
4.11 Advanced Configuration – STP	82
4.11.1 Advanced Configuration – Global Setting	82
4.11.2 Advanced Configuration – Port Configuration	83
4.11.3 Advanced Configuration – STP Information	84
4.11.3 Advanced Configuration – STP Information	85
4.12 Advanced Configuration – ERPS	86
4.12.1 Advanced Configuration – Global Setting	86
4.12.2 Advanced Configuration – ERPS - Ring Setting	87
4.12.3 Advanced Configuration – ERPS - Ring Information.....	88
4.13 Advanced Configuration – Alarm.....	89
4.13.1 Advanced Configuration – Alarm – Relay Setting	89
4.13.2 Advanced Configuration – Alarm – Led Setting	89
4.13.3 Advanced Configuration – Alarm – Temperature Setting.....	90
4.13.4 Advanced Configuration – Alarm – Trap Setting	91
4.13.5 Advanced Configuration – Alarm – Power Setting.....	92
4.14 Serial Management.....	92
4.14.1 Serial Management – Serial Device	92
4.14.2 Serial Management – Serial Protocol	94
4.14.3 Serial Management – Serial Statistics.....	95
4.15 Advanced Configuration – Extended.....	96
4.15.1 Advanced Configuration – Extended – Port Cable Setting.....	96
4.15.2 Advanced Configuration – Extended – Ping Test.....	97

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.

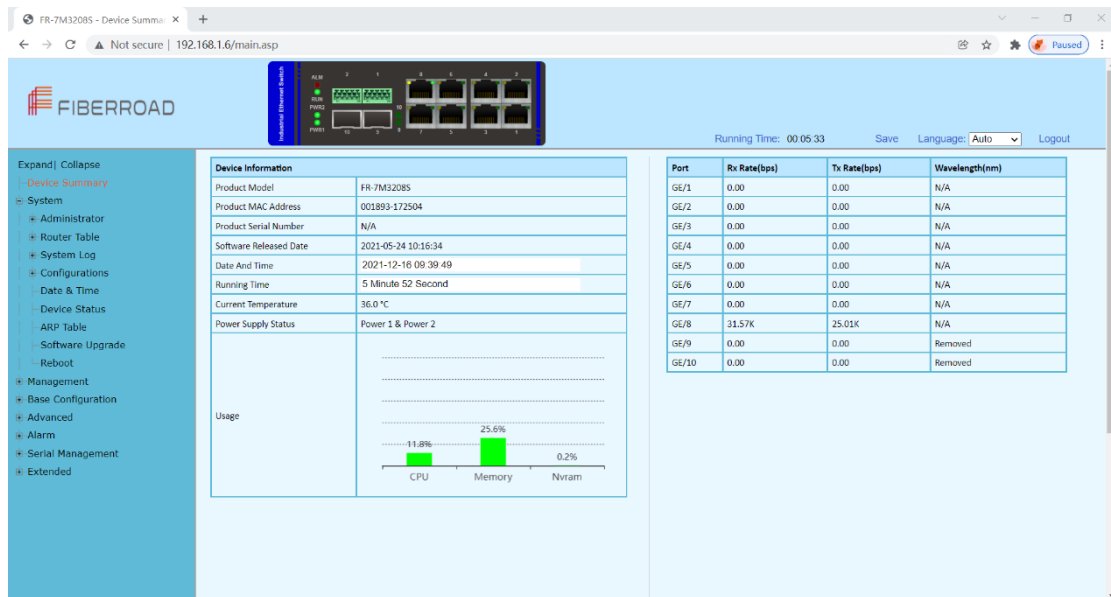
The industrial switch default value of IP, subnet mask, username and password are listed as below:

- ❖ 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 displays the 'Administrators' page. It features a table of existing users and an 'Add User' dialog box. The table lists the Name, Password, Status, Level, and Description for each user. The 'Add User' dialog box allows for adding a new user with fields for Name, Password, Confirm Password, Level, Status, and Description. The 'Level' dropdown menu is currently set to 'Guest User'.

Name	Password	Status	Level	Description
*admin	admin	✓	Super Administrator	Default Administrator

Item	Description	Notes
Name/Password/ConfirmPassword	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.

Name	Level	Login Type	Login Information	Login Time	Description
*admin	Super Administrator	web-1	::ffff:192.168.1.138	2021-12-16 09:34:49	Default Administrator

(Marked with * is current administrator)

Refresh

1.3.3 Management Setting

Access Timeout Setting

Login Way Setting	Timeout	Default
Console Timeout	5	<1-30> Default:5minutes
Telnet	☒ Enabled ☐ Disabled Timeout: 5	<1-30> Default:5minutes
SSH	☒ Enabled ☐ Disabled Timeout: 5	<1-30> Default:5minutes
WEB	☒ Enabled ☐ Disabled Timeout: 5	<1-30> Default:5minutes

Refresh Apply

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

FR-7M32085 - Static Entries

Not secure | 192.168.1.6/main.asp

Running Time: 00:07:07 Save Language: Auto Logout

Expand | Collapse

Device Summary

System

- Administrator
 - Administrators
 - Online Users
 - Management Setting
- Router Table
 - Static Entries
 - Router Table
- System Log
- Configurations
 - Date & Time
 - Device Status
 - ARP Table
 - Software Upgrade
 - Reboot
- Management
 - Base Configuration
 - Advanced
 - Alarm
 - Serial Management
 - Extended

Destination Subnet Mask Gateway Metric In Use

Static Entries

Add Type	Route
Destination	IPv4(A.B.C.D)
Subnet Mask	IPv4(A.B.C.D)
Gateway	IPv4(A.B.C.D)
Metric	0 <0-9999>
Apply Cancel	

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

FR-7M32085 - Router Table

Not secure | 192.168.1.6/main.asp

Running Time: 00:07:25 Save Language: Auto Logout

Expand | Collapse

Device Summary

System

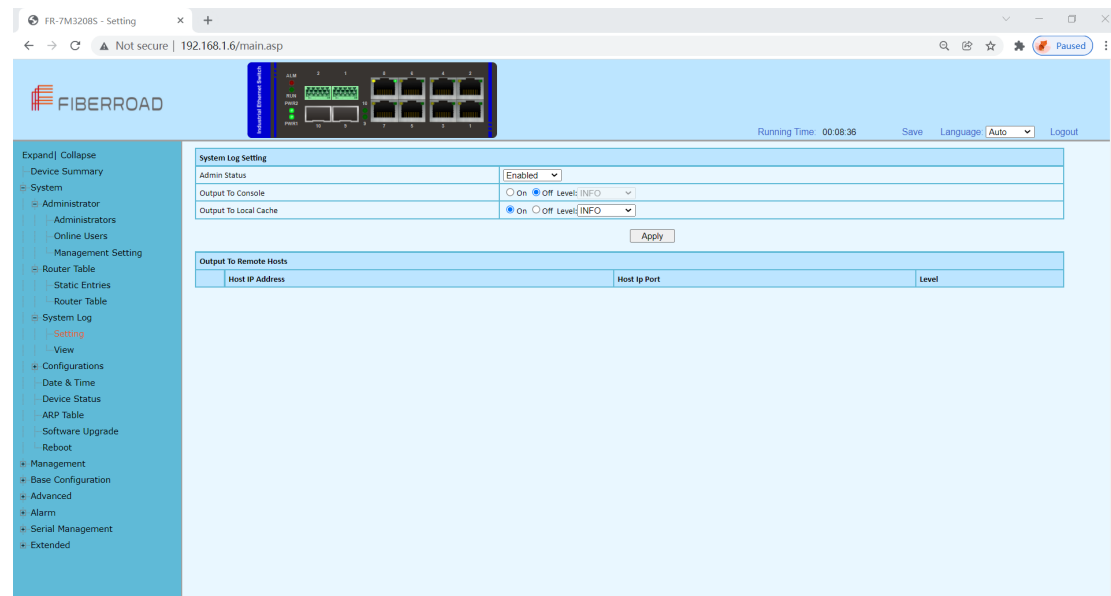
- Administrator
 - Administrators
 - Online Users
 - Management Setting
- Router Table
 - Static Entries
 - Router Table
- System Log
- Configurations
 - Date & Time
 - Device Status
 - ARP Table
 - Software Upgrade
 - Reboot
- Management
 - Base Configuration
 - Advanced
 - Alarm
 - Serial Management
 - Extended

Destination	Subnet Mask	Gateway	Metric	Interface
192.168.1.0	255.255.255.0(24)	0.0.0.0	0	ip0
127.0.0.0	255.255.255.0(24)	0.0.0.0	0	Other

1.5 System Log

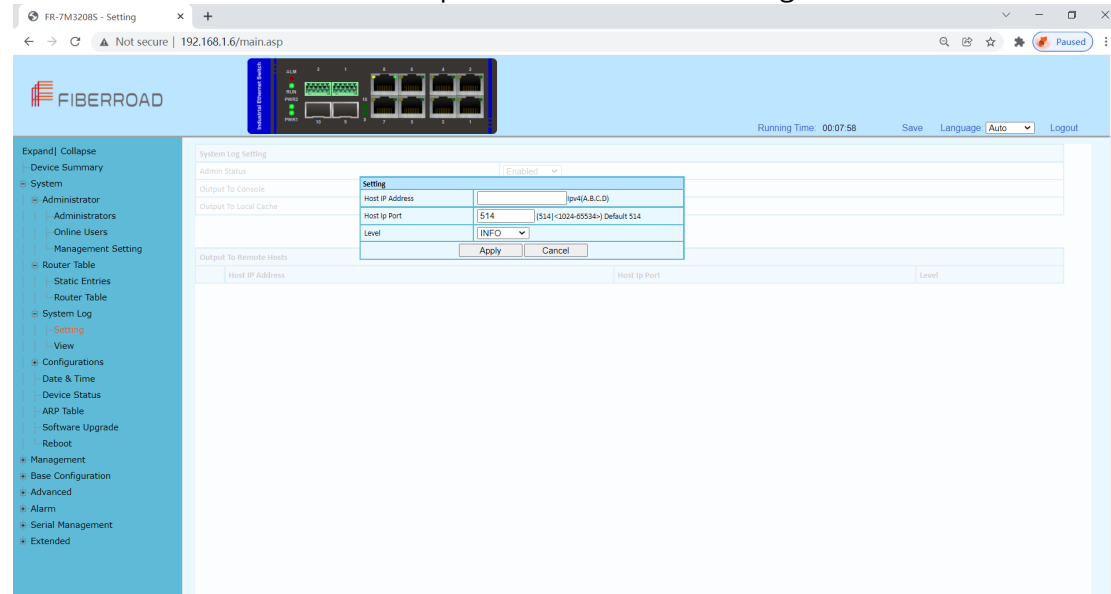
1.5.1 System Log – Setting

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	Default: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

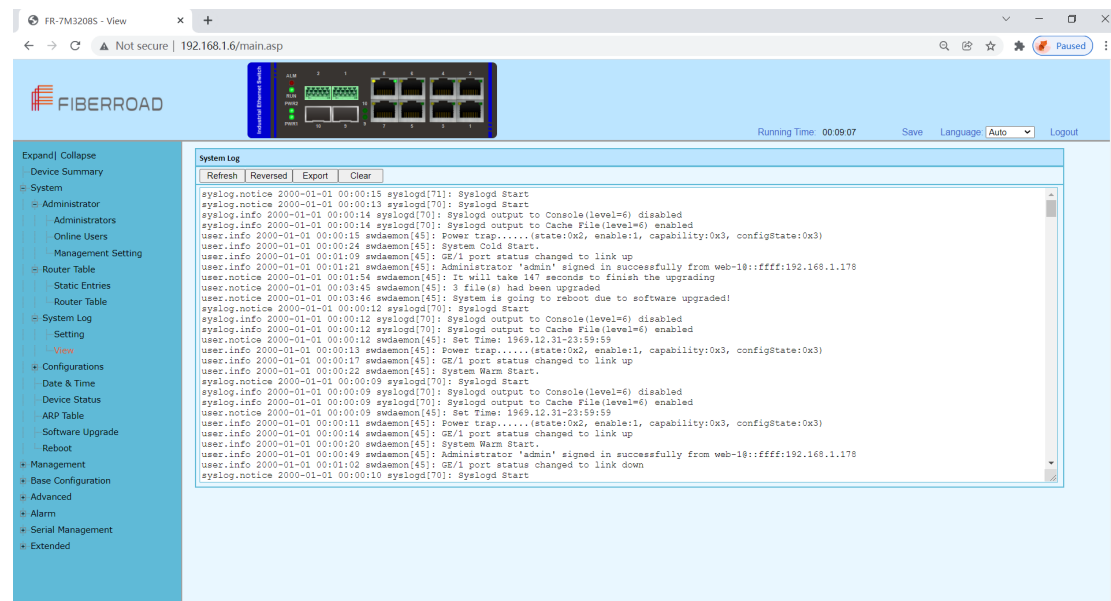
Click the “Add” button, to the output to remote hosts setting.



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.

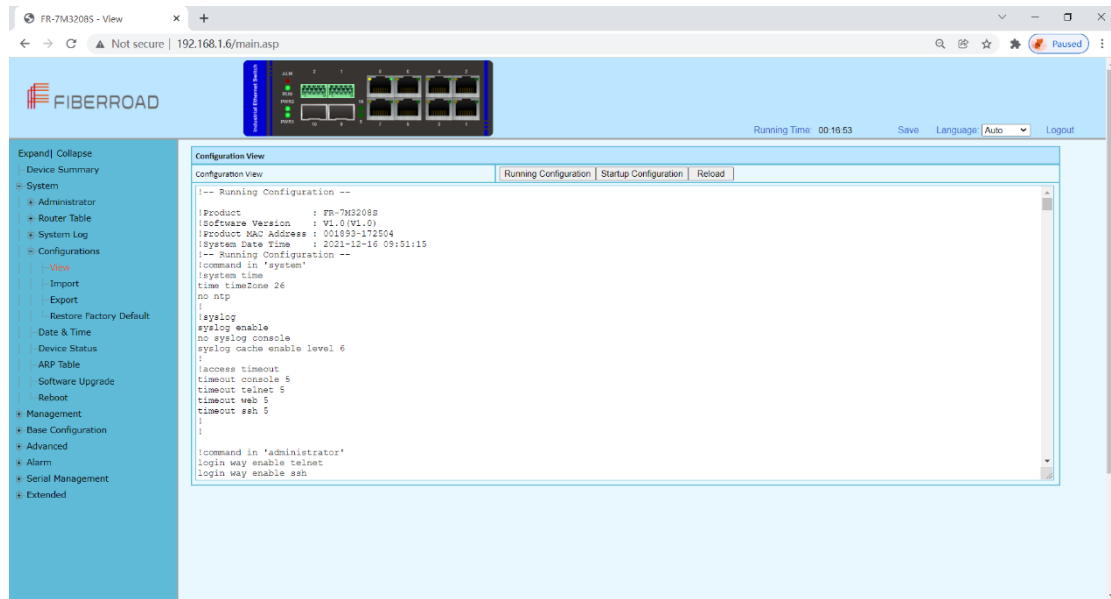
1.5.2 System Log - View



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	

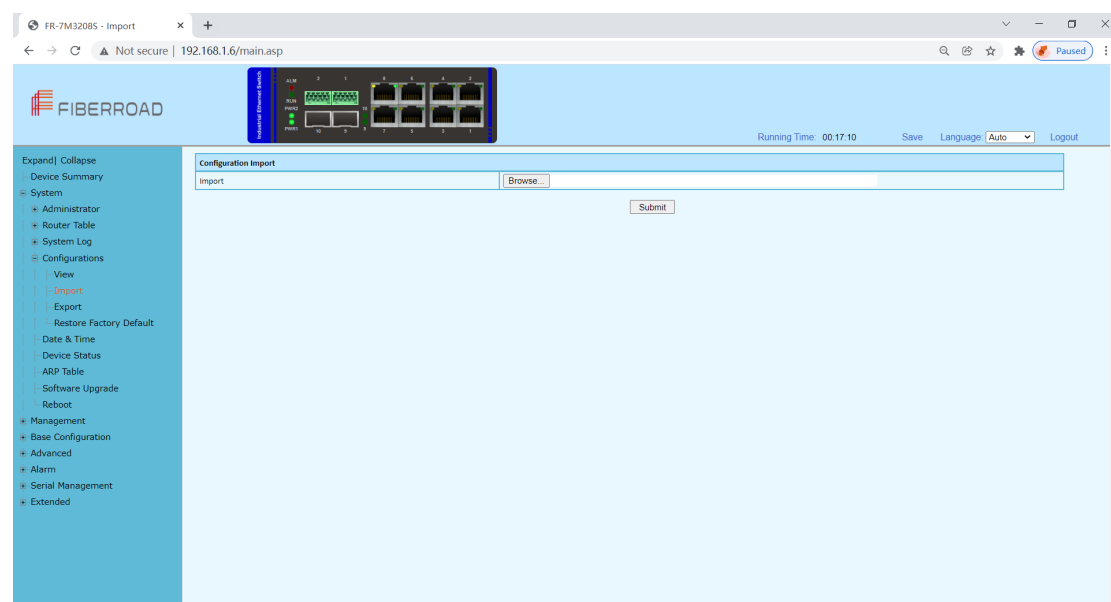
1.6 Configurations

1.6.1 Configurations – View



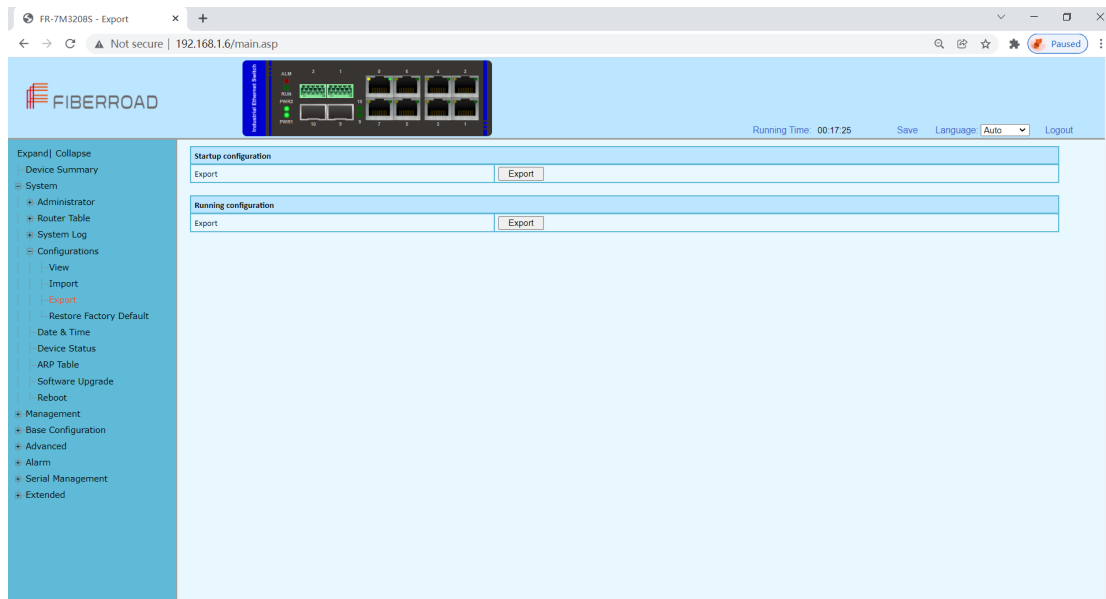
Item	Description	Notes
Running Configuration	Show system running configuration	Text Style
Startup Configuration	Show system startup configuration	Text Style
Reload	Reload the running or startup configuration	

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

The screenshot shows the 'Date & Time' configuration page in the FiberRoad FR-7M3208S web interface. The page has a sidebar menu on the left with options like 'System', 'Router Table', 'System Log', 'Configurations', and 'Management'. The main content area displays the following configuration fields:

- System Time:** 2021-12-16 09:52:18
- Time Zone:** ((GMT+8:00) Beijing, Perth, Singapore, Hong Kong)
- Manual Set Time:** 2021-12-16 09:52:18
- SNTP Client:** Disabled

Buttons for 'Refresh' and 'Apply' are located at the bottom right of the configuration area.

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

The screenshot shows the 'Date & Time' configuration page with the 'SNTP Client' set to 'Enabled'. Below the 'SNTP Client' dropdown, there are checkboxes for 'Unicast', 'Multicast', and 'Broadcast'. The 'Unicast' checkbox is checked, and the IP address is set to 8.8.8.8. The interval is set to 1440 minutes. There is a 'Sync now' button.

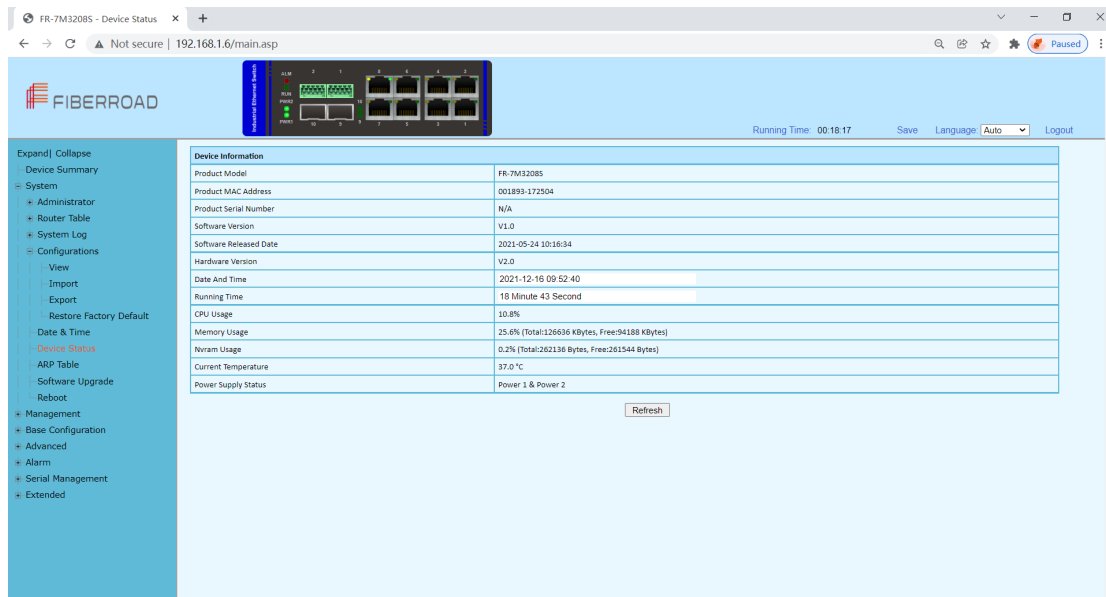
Item	Description	Notes
Synchronous Mode	Unicast Multicast Broadcast	These three modes are multi-selectable, but at least one must be selected
IP	IP address of SNTP, Default IP address 8.8.8.8; Interval range 10-43200, and default value 1440	Only for unicast mode
Interval	SNTP client time synchronization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

Sync now

SNTP client immediate synchronize times

mode

1.6.6 Configurations – Device Status

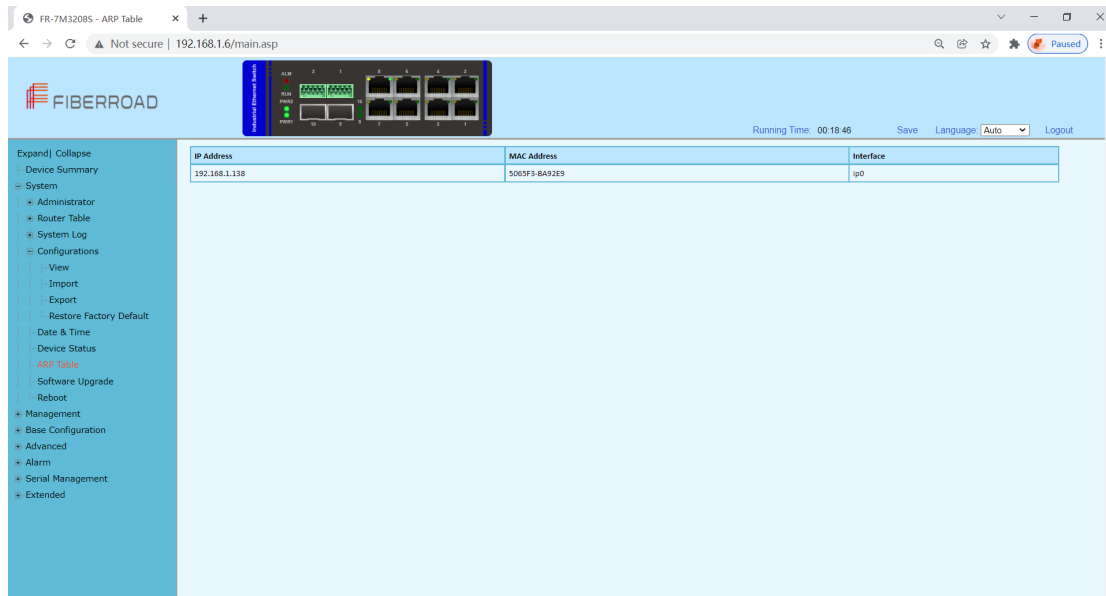


In the [Device Status] interface, the basic information and the operating status information of the device system are displayed.

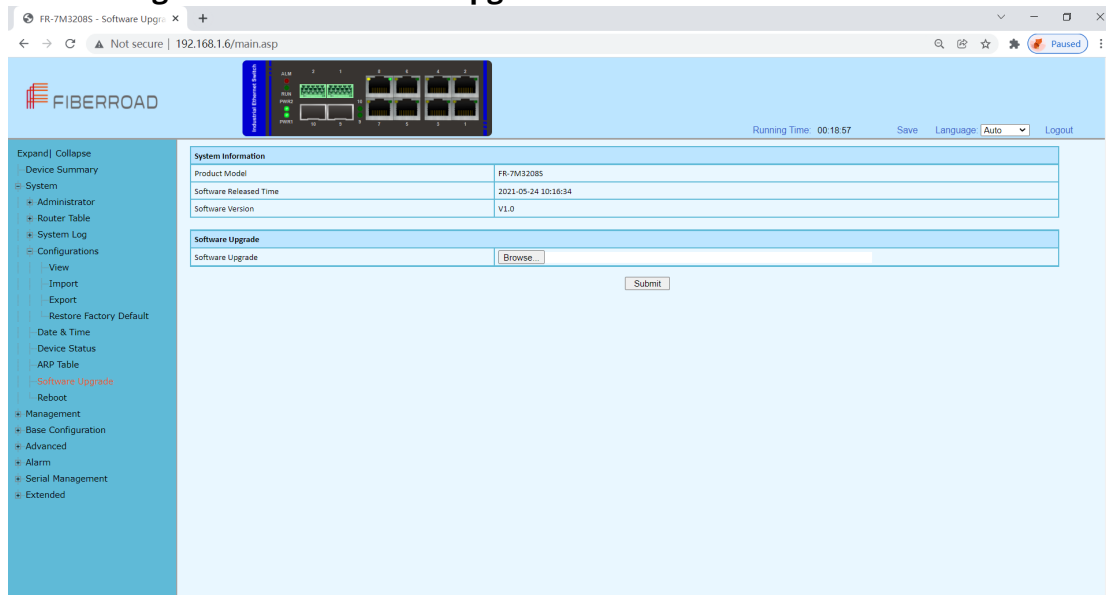
Item	Description	Notes
Product Model	The device mode	Read Only
Product MAC Address	The device MAC address	Read Only
Product Serial Number	The device product serial number	Read Only
Software Version	The software version running on	Read Only
Software Released Date	The time when running the software	Read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

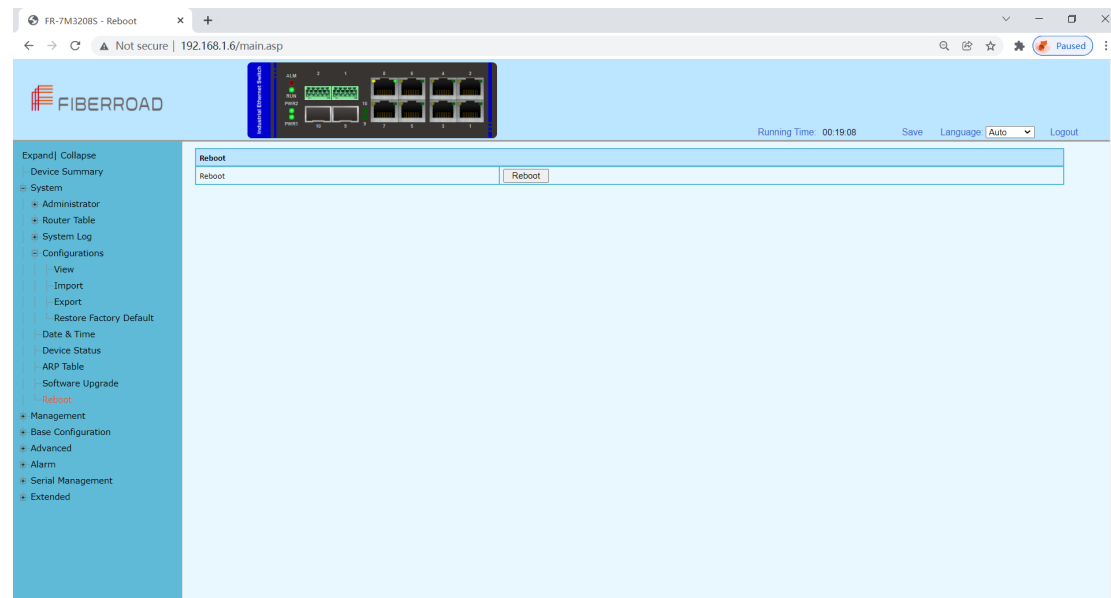


Configuration Step

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.

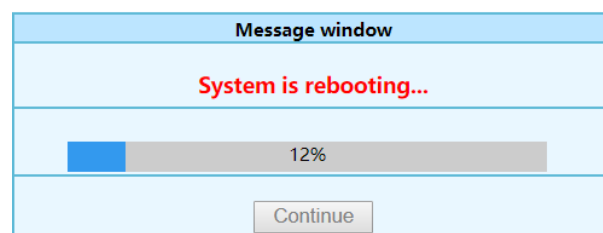
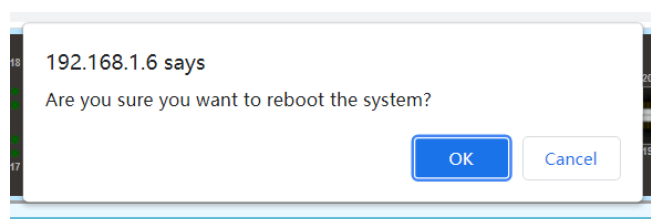
2, During the software upgrade, make sure that the device is powered up until the upgrade is completed.

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.





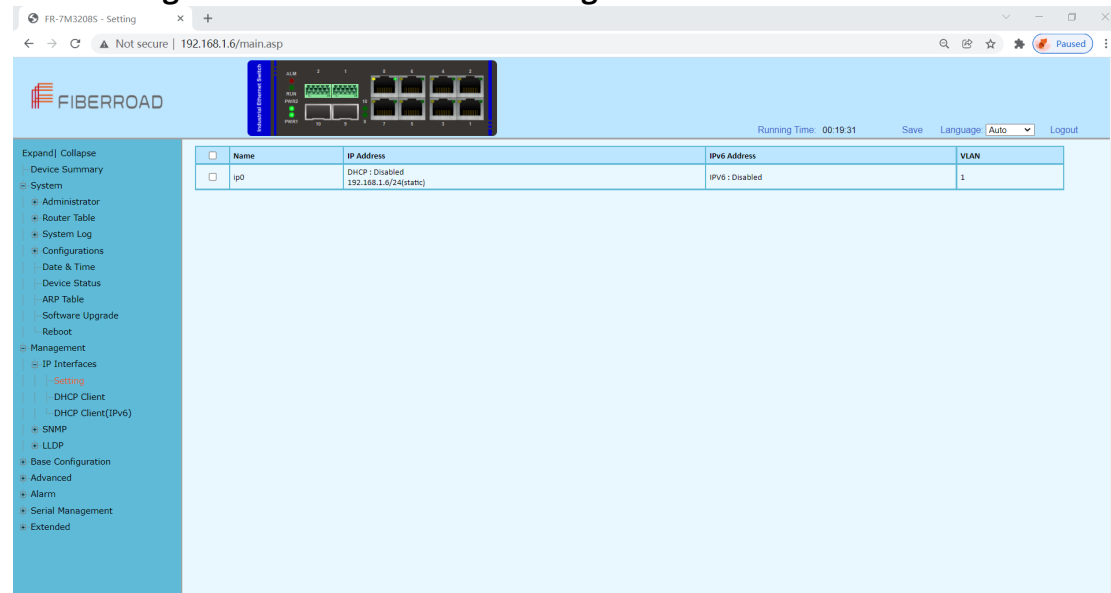
Chapter 2 Management Configurations

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		IPv4(A.B.C.D)
Subnet Mask		IPv4(A.B.C.D)
VLAN		<1-4094>
Apply Cancel		

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

2.1.2 Management – IP Interfaces – DHCP Client

The screenshot shows the Fiberroad web interface for the DHCP Client configuration. The left sidebar contains a navigation menu with options like 'Expand/Collapse', 'Device Summary', 'System', 'Administrator', 'Router Table', 'System Log', 'Configurations', 'Date & Time', 'Device Status', 'ARP Table', 'Software Upgrade', 'Reboot', 'Management', 'IP Interfaces', 'Setting', 'DHCP Client', 'DHCP Client(IPv6)', 'SNMP', 'LLDP', 'Base Configuration', 'Advanced', 'Alarm', 'Serial Management', and 'Extended'. The main content area is titled 'DHCP Client Setting' and includes a dropdown for 'Admin Status' (currently 'Disabled') and an 'Apply' button. Below this is the 'DHCP Client Status' section, which displays a table with columns for Status, IP Address, Subnet Mask, Lease Time, Lease Obtained, and Lease Expires. At the bottom of this section are buttons for 'Renew', 'Release', and 'Refresh'. A red note at the bottom of the status section reads: '(Please refresh the page after Renew or Release.)'

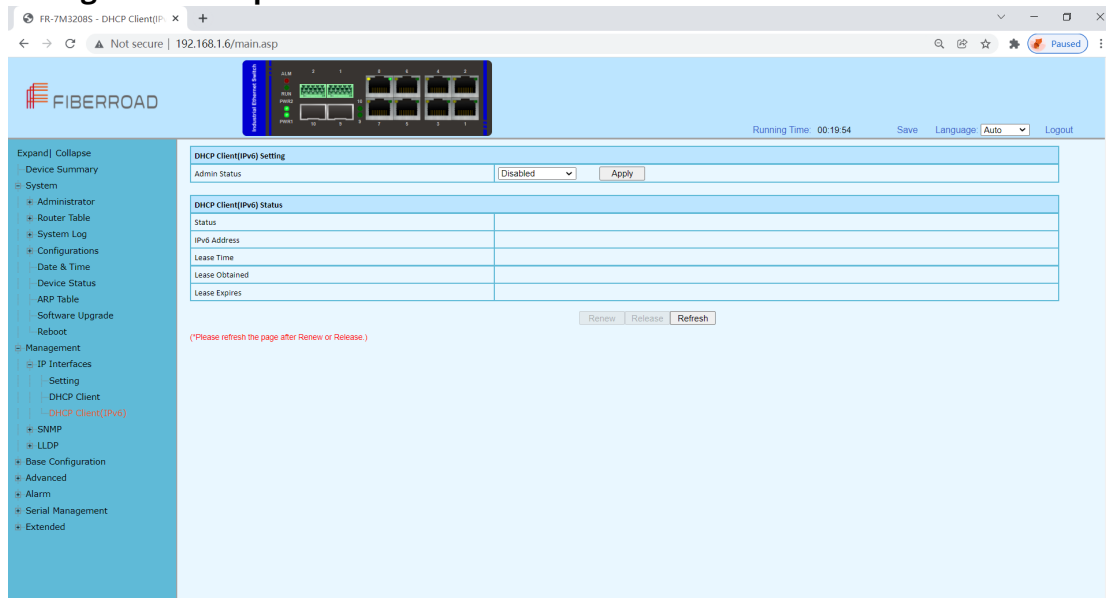
Configuration Step

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

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

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

2.1.3 Management – IP Interfaces – DHCP Client(IPv6) Configuration Steps



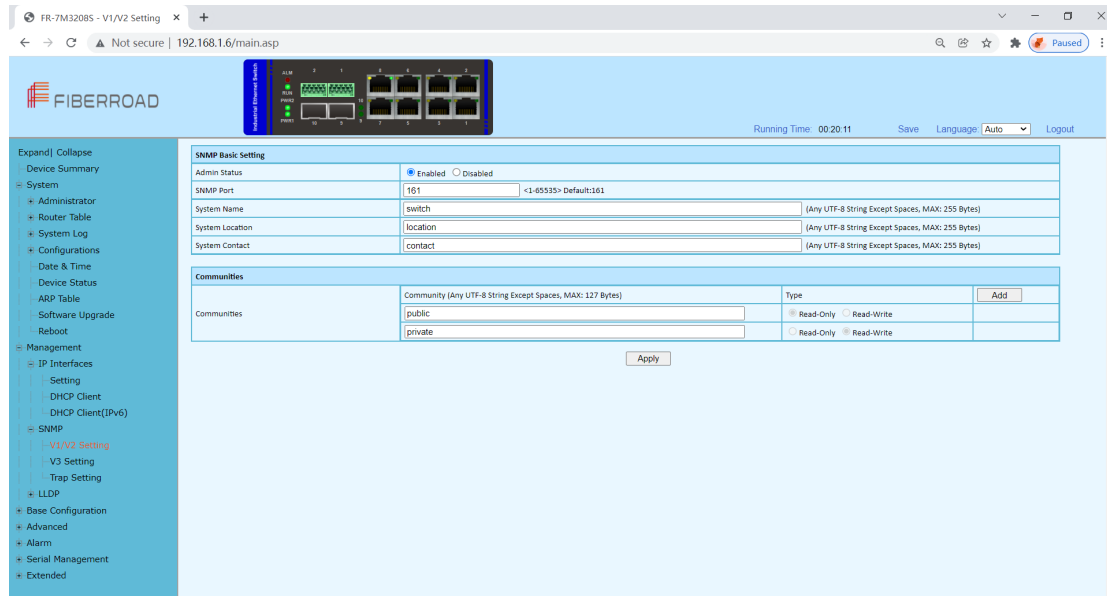
- 1, Select [Management / IP Interface / DHCP Client(IPv6)] in the navigation bar to enter the [DHCP Client(IPv6)] interface.
- 2, In the [DHCP Client(IPv6)] interface, you can view the current configuration information and DHCP client status.

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

2.2 Management – SNMP

2.2.1 Management -SNMP - v1/v2 setting

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



Configuration Steps

1. Select [Management / SNMP / V1/V2 Setting] in the navigation bar to enter the SNMP interface.
2. You can view the Base Setting of SNMP in the [SNMP Base Setting] interface.
3. To modify the Base Configuration, modify the corresponding configuration in the configuration box, and then click [Apply] to make effective.
4. If you want to add a group word, click [Add] and a group word is added to set the group word name and type. The system supports up to eight group characters, with the first and second being the default, so you can add up to six more. Click [Apply] to make effective.
5. To delete a group word, click [Delete] on the right corresponding entry (the first and second are the system default, cannot be deleted), and click [Apply] to make effective.

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

Communities

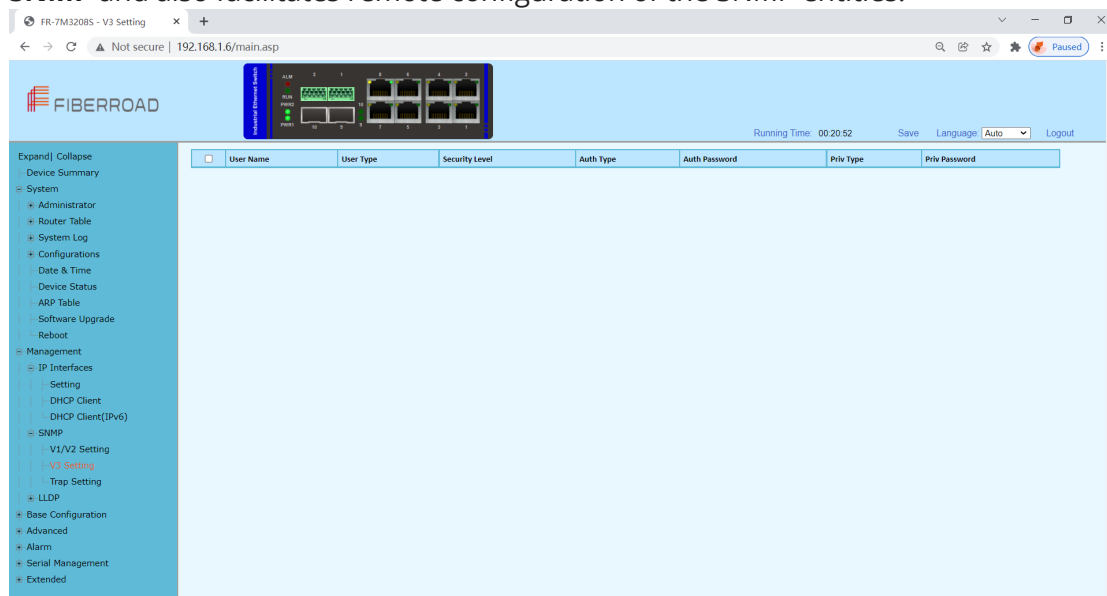
Name: Any legal character other than a space can be entered with a maximum length of 127

Type: Read and write

Note: The system supports a maximum of 8 group characters and requires at least two group characters. The default two group characters can only change the group name, cannot change the type or delete. Click [Add] to add a group character, add a group character can change the name and type, and delete.

2.2.2 Management – SNMP – v3 setting

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



Configuration Steps

1. Select [Management / SNMP V3 Setting] in the navigation bar to enter the SNMP interface.
2. You can view the Base Setting of SNMP in the [SNMP Base Setting] interface.
3. To modify the Base Configuration, modify the corresponding configuration in the configuration box, and then click [Apply] to make effective.
4. If you want to add a group word, click [Add] and a group word is added to set the group word name and type. The system supports up to eight group characters, with the first and second being the default, so you can add up to six more. Click [Apply] to make effective.
5. To delete a group word, click [Delete] on the right corresponding entry (the first and second are the system default, cannot be deleted), and click [Apply] to make effective.

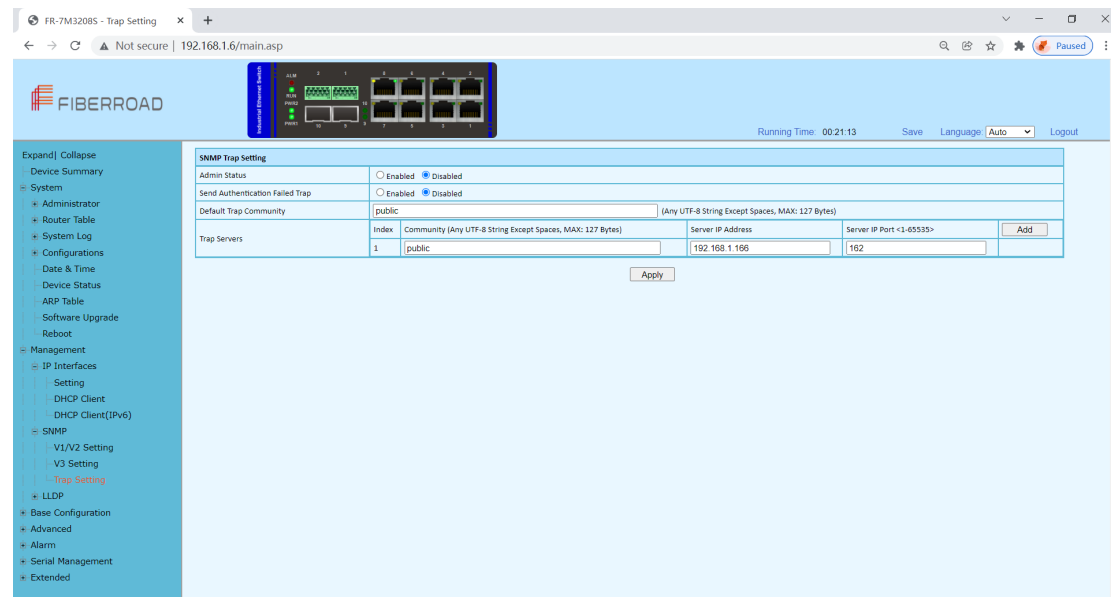
Item	Description	Notes
User Name	As Needed	
User Type	Read-Write/ Read-Only	
Security Level	NoAuthNoPriv:Communication without authentication and privacy. AuthNoPriv:Communication with authentication an witout privacy. AuthRriv:Communication with authentication and privacy. NoAuthNoPriv can't support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

Priv Password

As Needed

2.2.3 Management – SNMP – Trap Setting

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



Configuration Steps

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

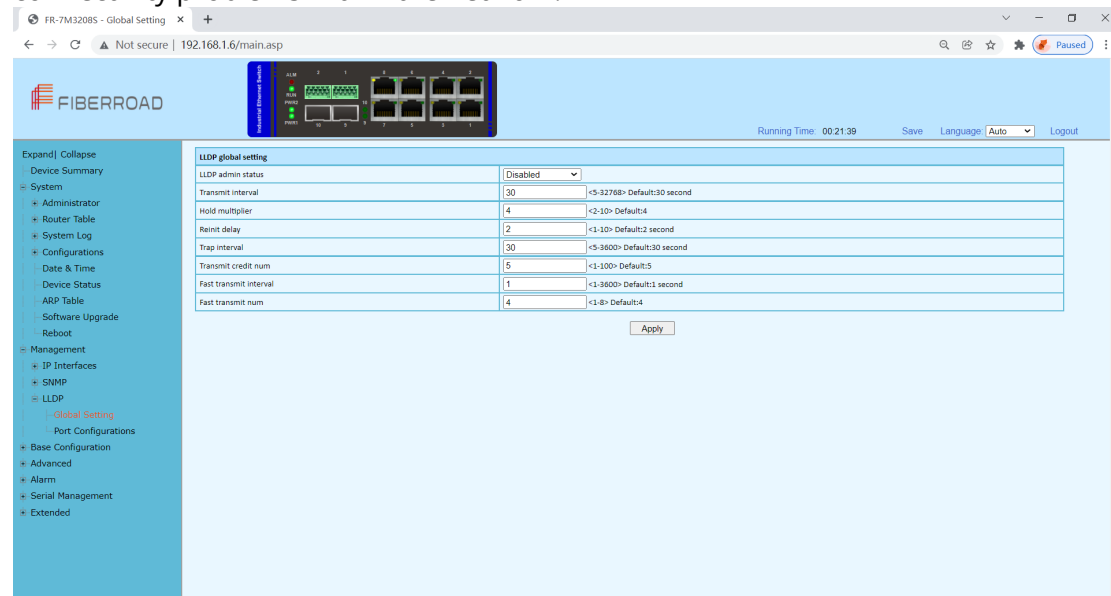
SNMP Trap Setting				
Admin Status	☐ Enabled ☒ Disabled			
Send Authentication Failed Trap	☐ Enabled ☒ Disabled			
Default Trap Community	public (Any UTF-8 String Except Spaces, MAX: 127 Bytes)			
Trap Servers	Index	Community (Any UTF-8 String Except Spaces, MAX: 127 Bytes)	Server IP Address	Server IP Port <1-65535> Add
	1	public	192.168.1.166	162
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 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	
Trap Server	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

Port	Destination address	Admin Status	Transmit interval (s)	Hold multiple	Reinit delay (s)	Trap interval (s)	Transmit credit num	Fast transmit interval (s)	Fast transmit num	Trap enable	TLVs transmit enable
*	0180C2-00000E	<>								<>	
GE/1	0180C2-00000E	Disabled	0	0	0	0	0	0	0	Disabled	
GE/2	0180C2-00000E	Disabled	0	0	0	0	0	0	0	Disabled	
GE/3	0180C2-00000E	Disabled	0	0	0	0	0	0	0	Disabled	
GE/4	0180C2-00000E	Disabled	0	0	0	0	0	0	0	Disabled	
GE/5	0180C2-00000E	Disabled	0	0	0	0	0	0	0	Disabled	
GE/6	0180C2-00000E	Disabled	0	0	0	0	0	0	0	Disabled	
GE/7	0180C2-00000E	Disabled	0	0	0	0	0	0	0	Disabled	
GE/8	0180C2-00000E	Disabled	0	0	0	0	0	0	0	Disabled	
GE/9	0180C2-00000E	Disabled	0	0	0	0	0	0	0	Disabled	
GE/10	0180C2-00000E	Disabled	0	0	0	0	0	0	0	Disabled	

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 Configuration Steps

Port	Link Status	Port Type	Running Status				Admin Status	Admin Status				Setting
			Speed	Duplex	Rx Rate(bps)	Tx Rate(bps)		Speed	Duplex	Flow Control	EEE	
GE/1	✗	Copper	10M	Half	0.00	0.00	On	Auto	Auto	Off	Disabled	Modify
GE/2	✗	Copper	10M	Half	0.00	0.00	On	Auto	Auto	Off	Disabled	Modify
GE/3	✗	Copper	10M	Half	0.00	0.00	On	Auto	Auto	Off	Disabled	Modify
GE/4	✗	Copper	10M	Half	0.00	0.00	On	Auto	Auto	Off	Disabled	Modify
GE/5	✗	Copper	10M	Half	0.00	0.00	On	Auto	Auto	Off	Disabled	Modify
GE/6	✗	Copper	10M	Half	0.00	0.00	On	Auto	Auto	Off	Disabled	Modify
GE/7	✗	Copper	10M	Half	0.00	0.00	On	Auto	Auto	Off	Disabled	Modify
GE/8	✓	Copper	1000M	Full	23.44K	20.32K	On	Auto	Auto	Off	Disabled	Modify
GE/9	✗	Fiber	10M	Half	0.00	0.00	On	Fiber-Auto	Full	Off	Disabled	Modify
GE/10	✗	Fiber	10M	Half	0.00	0.00	On	Fiber-Auto	Full	Off	Disabled	Modify

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
Apply 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,

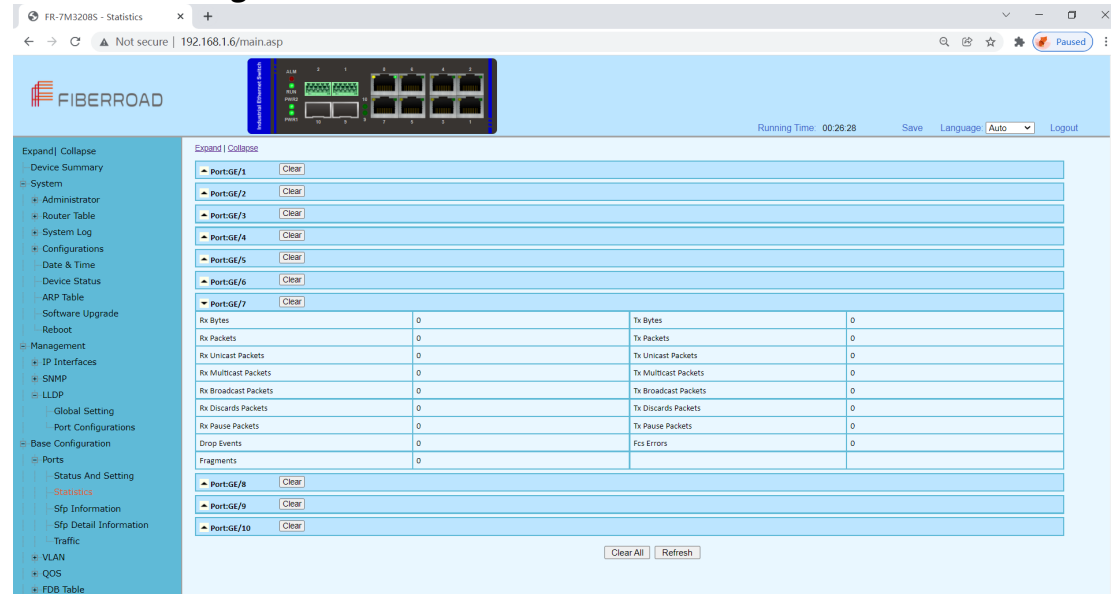
and click the [Cancel] to cancel the modification.

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 Enabled / Disabled	Default: Disabled

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

3.1.2 Base Configuration-Port-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/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

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
Crrent(mA)	SFP Current	Unit: mA

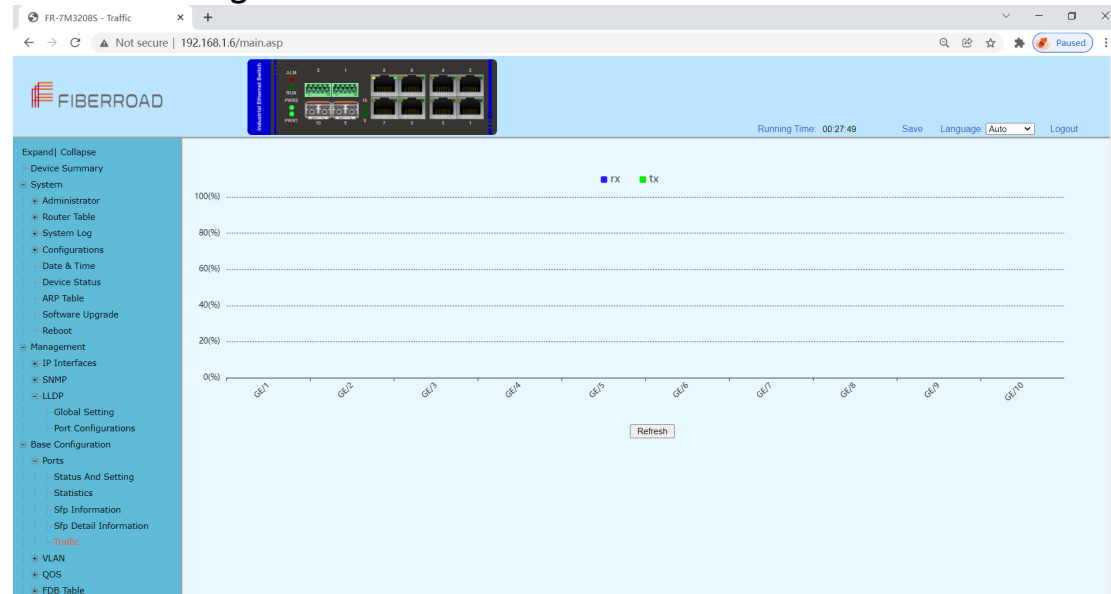
3.1.4 Base Configuration-Port-SFP Detail Information

The screenshot displays the FIBERROAD web interface for a device (FR-7M32085) at IP 192.168.1.6. The left sidebar shows a navigation menu with options like System, Management, and Base Configuration. The main content area is titled 'Port-GE/9' and shows detailed SFP information for Port GE/10.

Port-GE/10					
Status	Inserted	Ethernet Codes	1000BASE-LX	Mode	Single Mode
Wavelength(nm)	1310	Distance(m)	20000	Bit Rate(MBd)	1300
Vendor Name	OEM	OUI	00-00-00	PN	SFP
Version	000	SN	HW35207001557	Date	2020-07-04
Connector Type	LC	DDM	Supported	Calibrated	Internally
Tx Power(dBm)	-7.06	Rx Power(dBm)	-inf	Temperature(°C)	17.96
Voltage(V)	3.32	Current(mA)	8.20		

Refresh

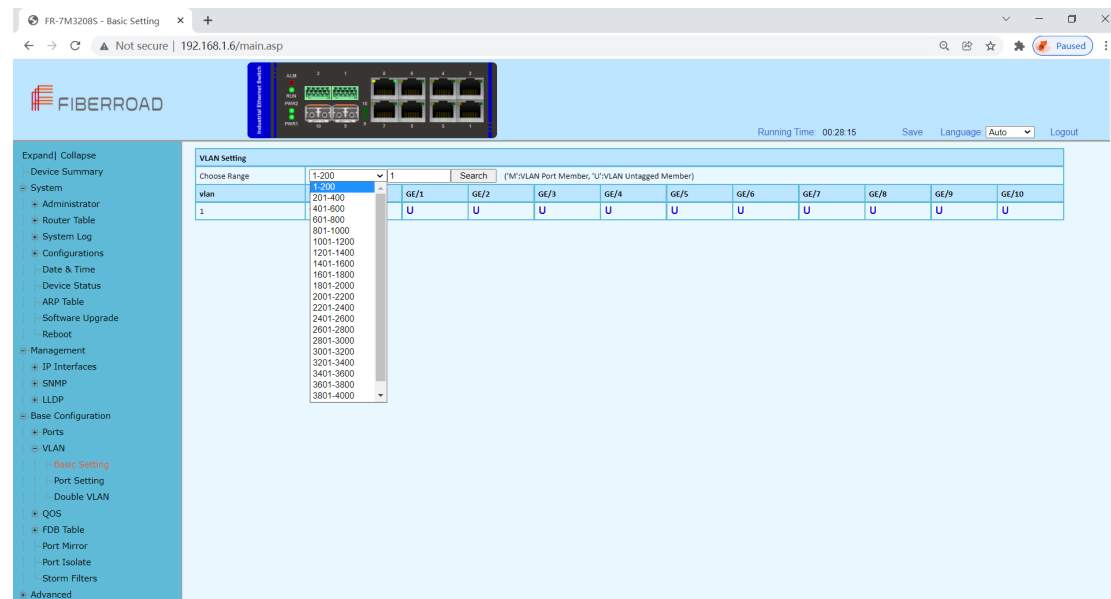
3.1.5 Base Configuration-Port-Traffic



Remarks: Real-time traffic statistics of each ports.

3.2 Base Configuration - VLAN

3.2.1 Base Configuration-VLAN-Basic Setting



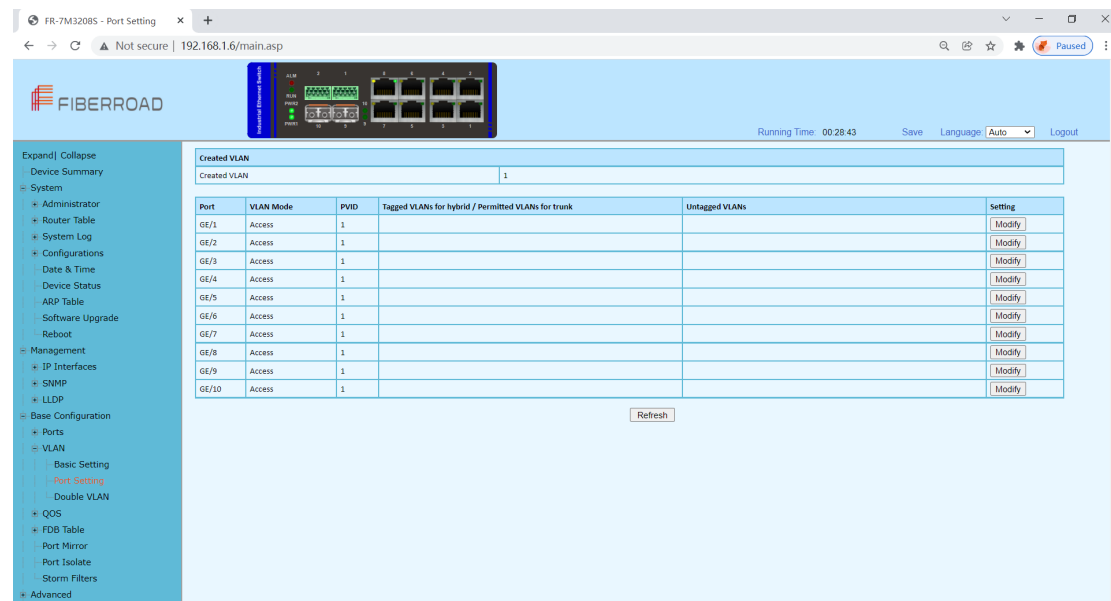
Configuration Steps

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	 Example:1-10,13,15-4094
	☒ Add ☐ Delete ☐ Modify Name:
Apply 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



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	☐ Replace ☐ Add ☐ Delete ☒ All Created VLAN
Example:1-10,13,15-4094	
Apply 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

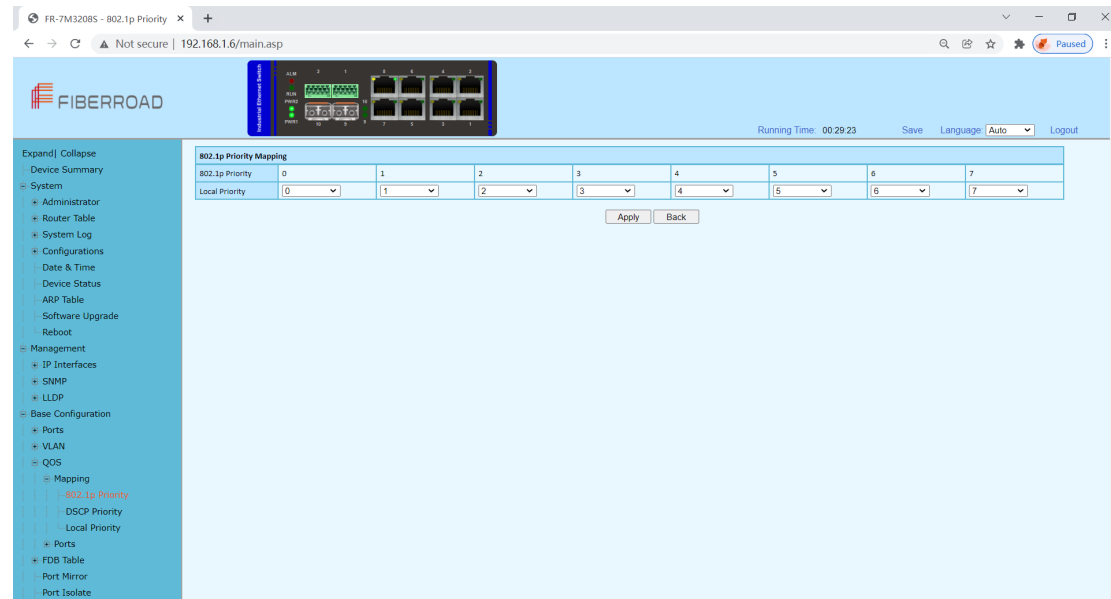
Port	Mode	Outer PVID	Ingress Mode	Egress Mode
*	<>	*	<>	<>
GE/1	Disabled	1	All	Untagged
GE/2	Disabled	1	All	Untagged
GE/3	Disabled	1	All	Untagged
GE/4	Disabled	1	All	Untagged
GE/5	Disabled	1	All	Untagged
GE/6	Disabled	1	All	Untagged
GE/7	Disabled	1	All	Untagged
GE/8	Disabled	1	All	Untagged
GE/9	Disabled	1	All	Untagged
GE/10	Disabled	1	All	Untagged

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.

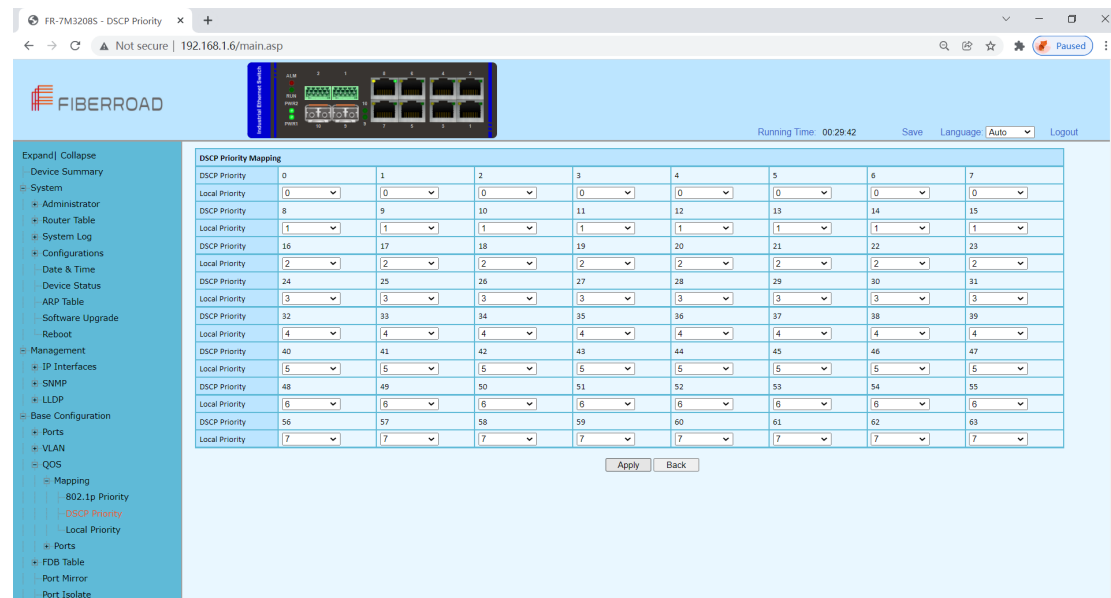


1. Select [Base Configuration / QoS / Mapping / 802.1p Priority] in the navigation bar to enter the QoS [802.1p Priority] interface.
2. On the QoS [802.1p Priority] interface, you can view the mapping from 802.1p priorities to local priorities.
3. To modify the mapping relationship, click [Modify] and select the mapped local priority for the corresponding 802.1p priority in drop-down list box.

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

3.3.2 Base Configuration-QoS- Mapping – DSCP Priority

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

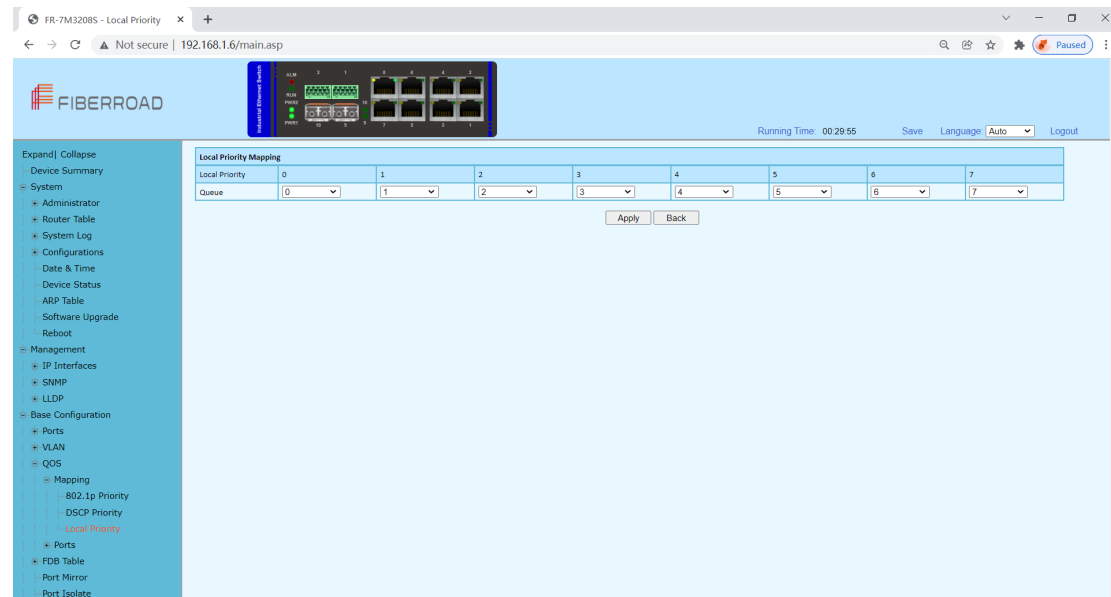


1. Select [Base Configuration / QOS / Mapping / DSCP Priority] in the navigation bar to enter the QOS DSCP Priority Mapping interface.
2. On the QOS [DSCP Priority] interface, you can view the mapping from DSCP priorities to local priorities.
3. To modify the mapping relationship, click [Modify] and 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.



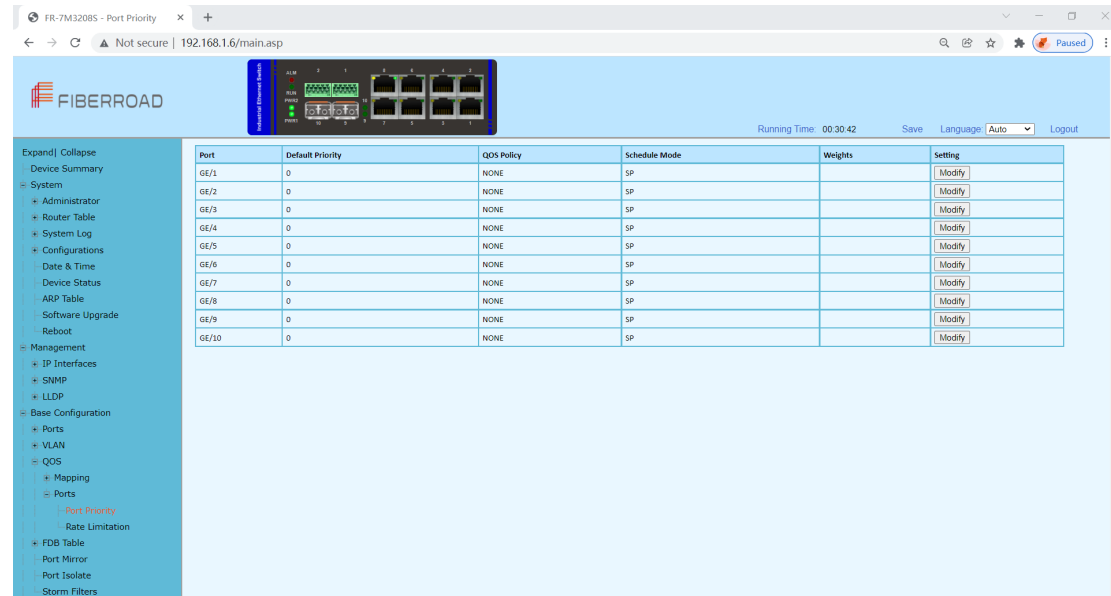
1. Select [Base Configuration / QoS / Mapping / Local Priority] in the navigation bar to enter the QoS Local Mapping.
2. You can view the mapping from the local priority to the egress queue on the QoS [Local Priority] interface.
3. To modify the mapping relationship, click [Modify] and select the mapped 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>
Apply 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 SP: Strict Priority scheduling strategy	
Scheduling Mode	WRR: Weighted Round Robin scheduling strategy WFQ: Weighted Fair Queue scheduling strategy	
Weights	If the selected scheduling mode is WRR or WFQ, you need to configure the weight of each queue, total 8 queues. To set 8 weights, the weight of all queues must be 127.	

3.4.2 Base Configuration-QoS- Ports-Rate Limitation

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

Port	Ingress Rate Limitation	Rate(kbps)	Egress Rate Limitation	Rate(kbps)	Setting
GE/1	OFF	N/A	OFF	N/A	Modify
GE/2	OFF	N/A	OFF	N/A	Modify
GE/3	OFF	N/A	OFF	N/A	Modify
GE/4	OFF	N/A	OFF	N/A	Modify
GE/5	OFF	N/A	OFF	N/A	Modify
GE/6	OFF	N/A	OFF	N/A	Modify
GE/7	OFF	N/A	OFF	N/A	Modify
GE/8	OFF	N/A	OFF	N/A	Modify
GE/9	OFF	N/A	OFF	N/A	Modify
GE/10	OFF	N/A	OFF	N/A	Modify

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

The screenshot shows the Fiberroad web interface for configuring the Aging Setting. The sidebar on the left contains a tree view with the following structure:

- Expand/Collapse
 - Device Summary
 - System
 - Administrator
 - Router Table
 - System Log
 - Configurations
 - Date & Time
 - Device Status
 - ARP Table
 - Software Upgrade
 - Reboot
 - Management
 - IP Interfaces
 - SNMP
 - LLDP
 - Base Configuration
 - Ports
 - VLAN
 - QOS
 - Mapping
 - Ports
 - Port Priority
 - Rate Limitation
 - FDB Table
 - Configuration
 - Aging Setting (selected)
 - Static MAC Entry

The main configuration area for Aging Setting includes the following fields:

- Aging Time(unit:second): ☒ On ☐ Off 300 <1-86400> Default:300second
- Fast Aging Time: Enabled

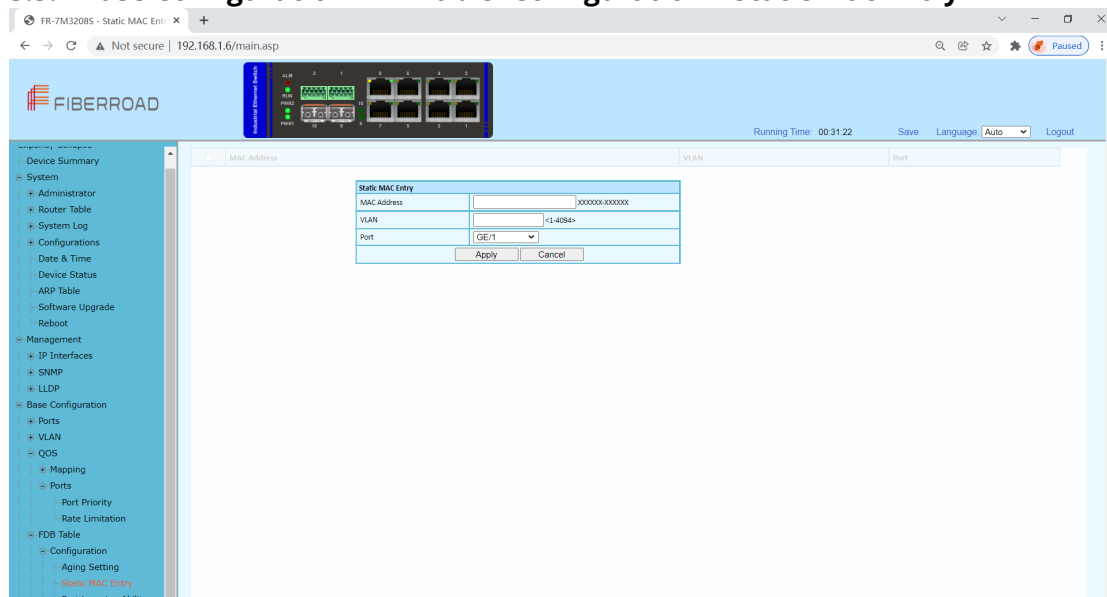
An button is located at the bottom right of the configuration area.

Configuration Steps

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

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

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



Configuration Steps

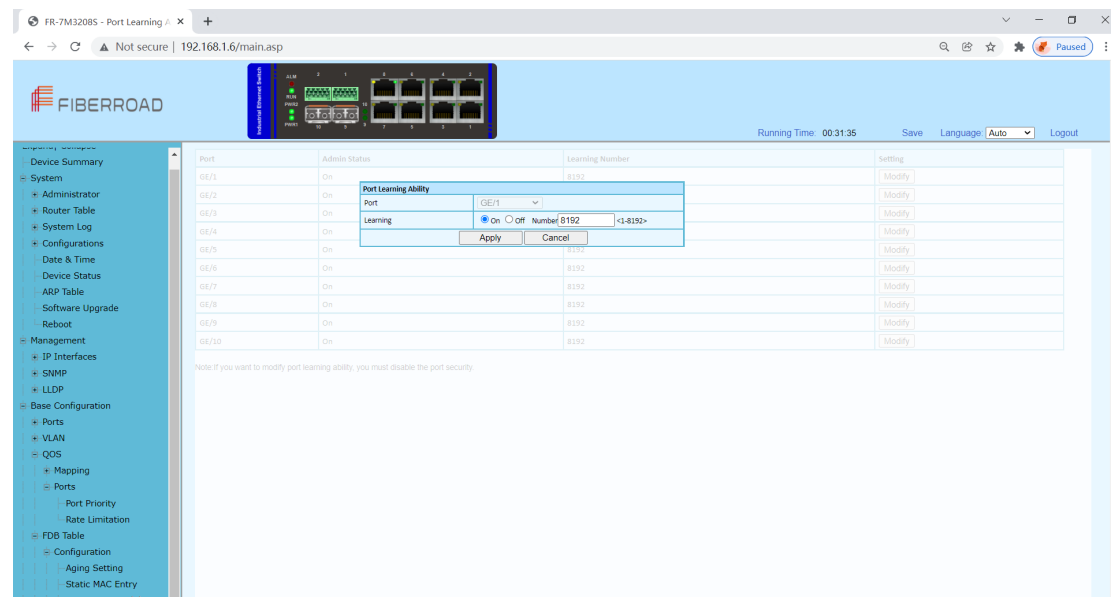
1. Select [Base Configuration / FDB Table / Configuration / Static MAC Entry] to enter the [Static MAC Entry] configuration interface.
2. On FDB Table [Static MAC Entry] interface, you can view the static MAC related configuration information of FDB Table,
3. If add a new static MAC address, click [Add]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

configuration item, click [Apply] to complete the modification. There will be prompts if the configuration item is filled in incorrectly.

5. If delete a static MAC, select the corresponding static MAC and click [Delete] to delete the static MAC.

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

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



Configuration Steps

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

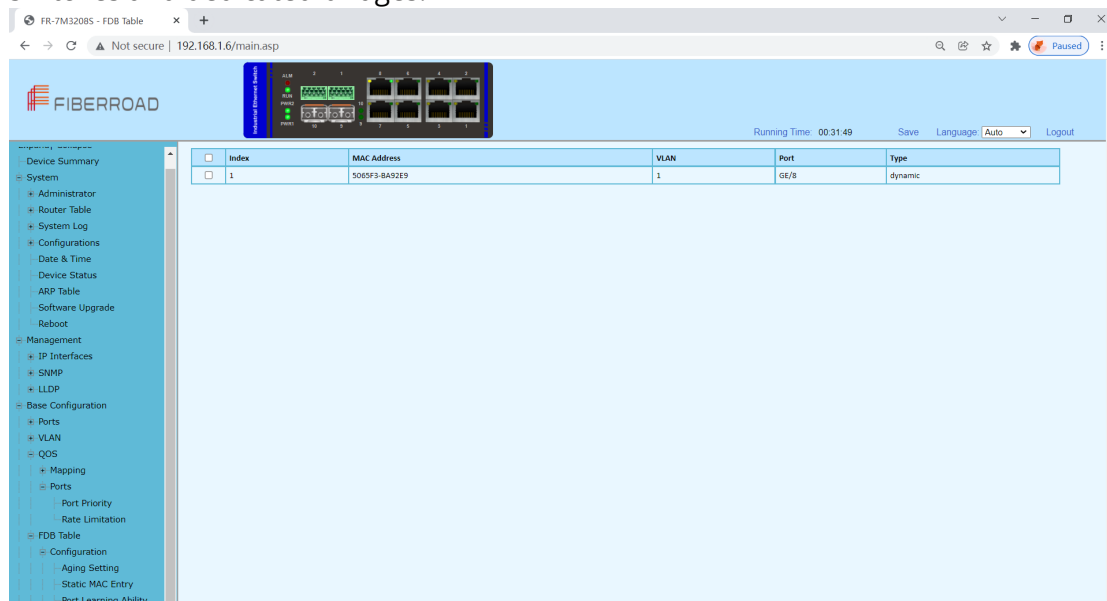
Item	Description	Notes
Port	Port name, selected modified port	
Learning	Functional configuration of port learning, configured via radio buttons. ON: The Port Learning Ability is on. IS3000 / IS2000 series range is 1-8192; OFF: Closes the Port Learning Ability.	

Note: The default is Enable with value 8192.

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

3.5.4 Base Configuration-FDB Table- FDB Table

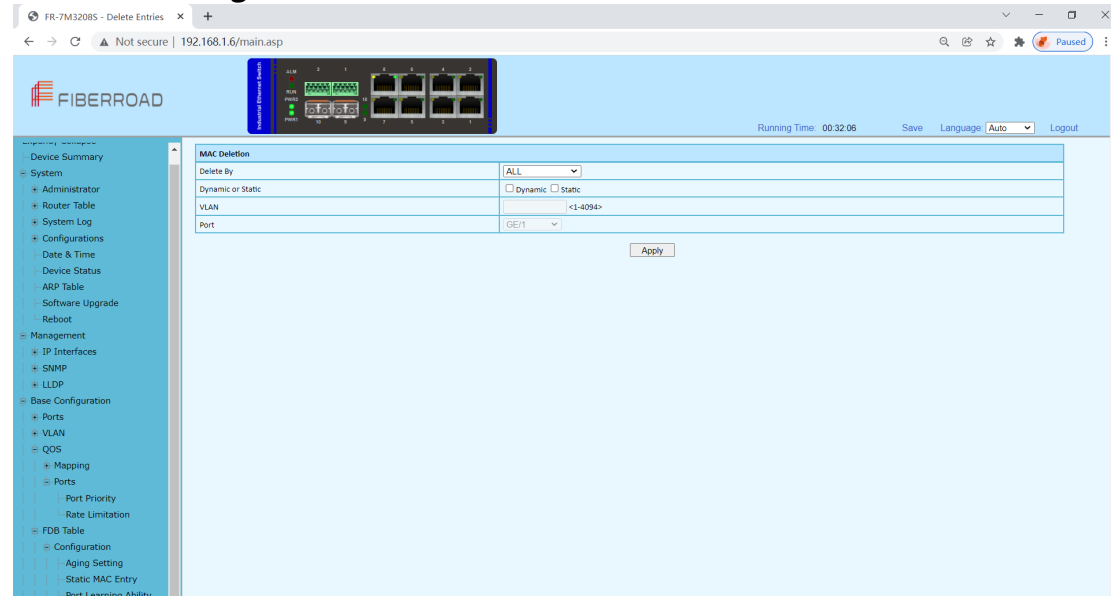
The FDB (forwarding database) table is used by a Layer 2 device (switch/bridge) to store the MAC addresses that have been learned and which ports that MAC address was learned on. The MAC addresses are learned through transparent bridging on switches and dedicated bridges.



Configuration Steps

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

3.5.5 Base Configuration-FDB Table- Delete Entries



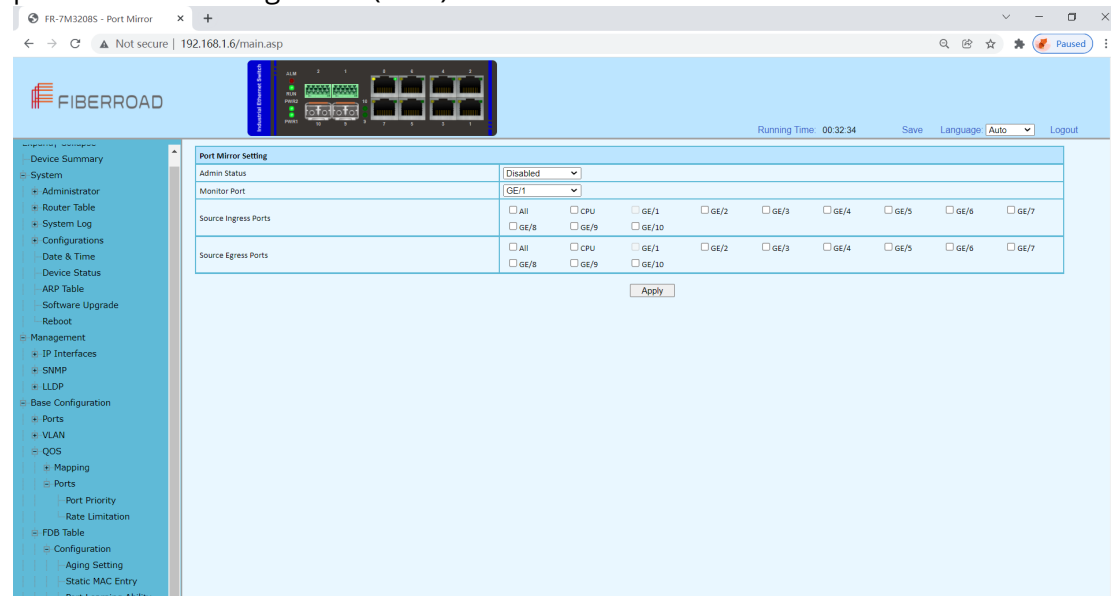
Configuration Steps

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

Item	Description	Notes
Delete By	All: Deletes all FDB Table entries. VLAN: Specifies the VLAN ID to delete FDB Table entries. Port: Specify the port number to delete the FDB Table entries.	
Dynamic or static	Dynamic: Delete the dynamic FDB Table entries that have been learned. Static: Delete manually added static FDB Table entries.	
VLAN	Delete the forwarding entry of the specified VLAN. The range is 1-4094.	
Port	Delete the forwarding entry of the specified port.	

3.5.6 Base Configuration-FDB Table- Port Mirror

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



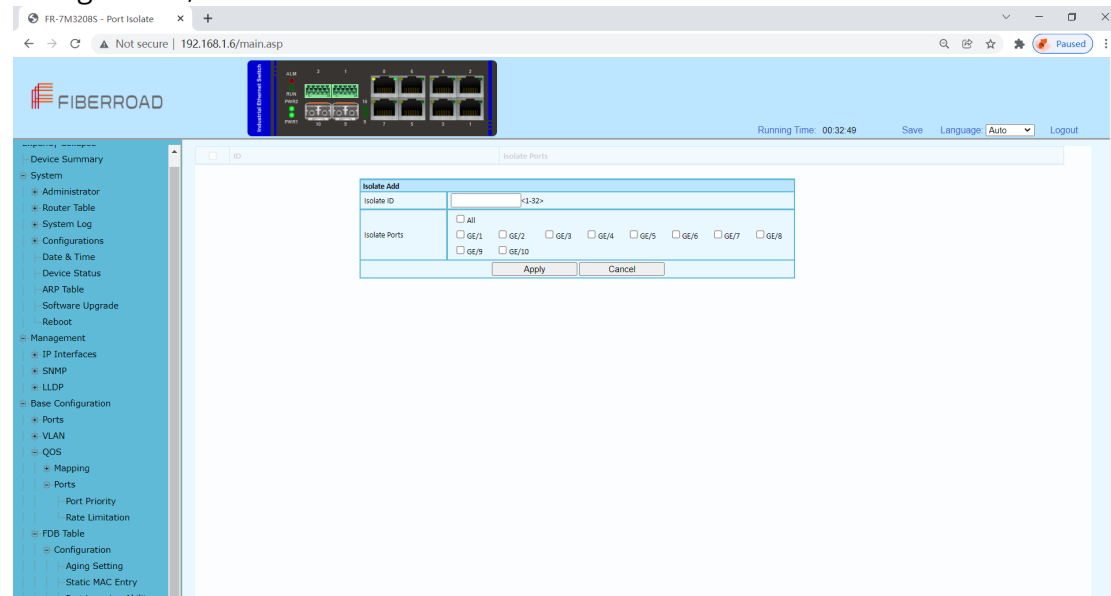
Configuration Steps

1. Select [Base Configuration / Port Mirror] in the navigation bar to enter the [Port Mirror] configuration interface
2. Modify the port mirroring configuration information. Pull down and select to disable or enable mirroring, select the mirroring destination port, check the ingress port and egress port, the ingress or egress cannot contain the destination port, and click [apply] to submit the modification

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

3.5.7 Base Configuration-FDB Table- Port Isolate

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

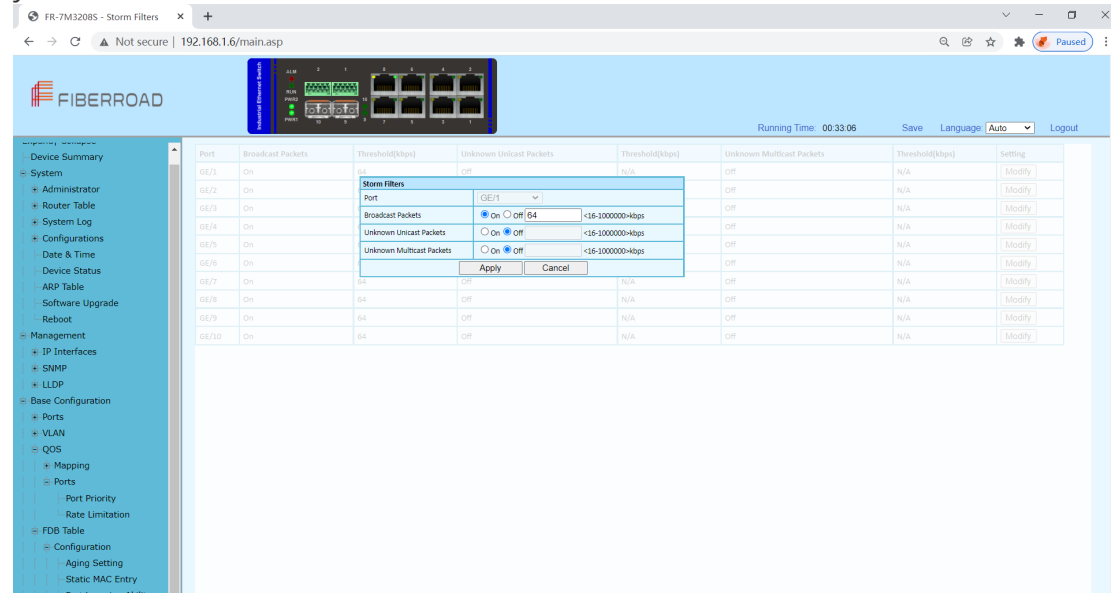


Configuration Steps

1. Select [Base Configuration / Port Isolate] in the navigation bar to enter the [Port Isolate] configuration interface
2. Modify the port isolate configuration information. Pull down and select to Add or Modify, enter Isolate ID, select a Isolate Ports, and click [apply] to submit the modification.

3.5.8 Base Configuration-FDB Table- Storm Filters

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



Configuration Steps

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

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



Chapter 4 Advanced Configurations

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

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

4. Advanced Configuration

4.1 Advanced Configuration – Ports – Ports Security

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

Port	Mode	Action	State	MAC 1	MAC 2	MAC 3	Clear
GE1/1	Disabled	Trap	Non-Execution	000000-000000	000000-000000	000000-000000	Clear
GE1/2	Disabled	Trap	Non-Execution	000000-000000	000000-000000	000000-000000	Clear
GE1/3	Disabled	Trap	Non-Execution	000000-000000	000000-000000	000000-000000	Clear
GE1/4	Disabled	Trap	Non-Execution	000000-000000	000000-000000	000000-000000	Clear
GE1/5	Disabled	Trap	Non-Execution	000000-000000	000000-000000	000000-000000	Clear
GE1/6	Disabled	Trap	Non-Execution	000000-000000	000000-000000	000000-000000	Clear
GE1/7	Disabled	Trap	Non-Execution	000000-000000	000000-000000	000000-000000	Clear
GE1/8	Disabled	Trap	Non-Execution	000000-000000	000000-000000	000000-000000	Clear
GE1/9	Disabled	Trap	Non-Execution	000000-000000	000000-000000	000000-000000	Clear
GE1/10	Disabled	Trap	Non-Execution	000000-000000	000000-000000	000000-000000	Clear

Note: If you want to modify the mode, you must enable the port learning ability and set the learning number to 0192.

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.

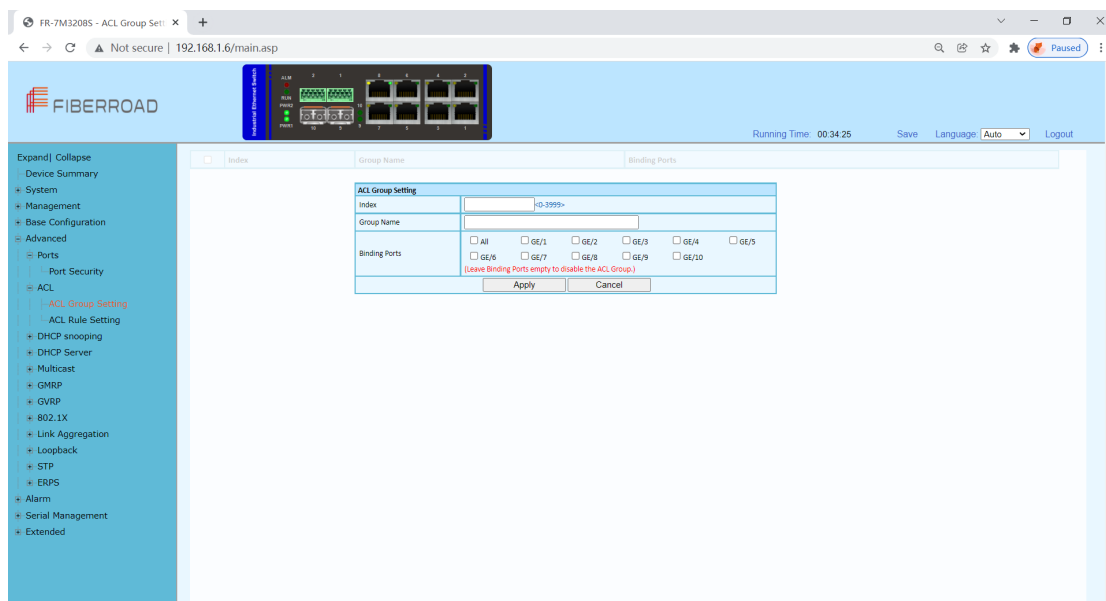
<i>Item</i>	<i>Description</i>	<i>Notes</i>
Mode	Enable port security on the desired ports. If desired, specify the secure MAC address.	
Action	Trap/Shutdown/Trap&Shutdown/Drop/Trap&Drop	
MAC 1/MAC 2/MAC 3	You can add MAC address to the list of secure address	

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

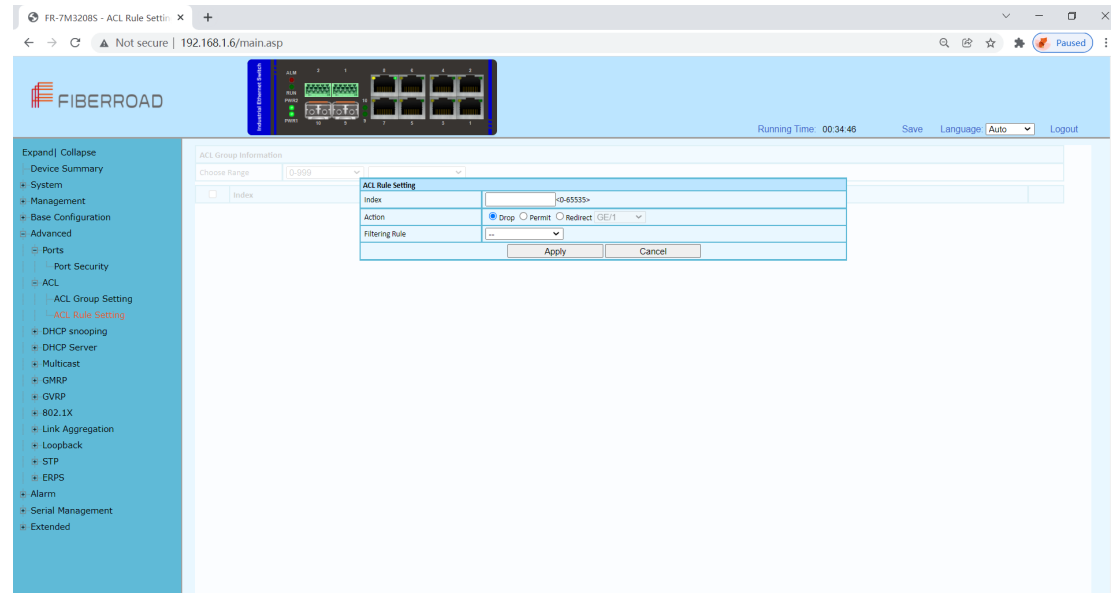
1. Select [Advanced / ACL / ACL Group Setting] in the navigation bar to enter the ACL interface.
2. The ACL information will be added in [ACL Group Setting] interface.
3. Add an ACL Group: click [Add] to enter [ACL Group Setting] interface, An ordinal number (0-3999) is assigned to the group. Set a name 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	☒ Drop ☐ Permit ☐ Redirect GE/1
Filtering Rule	--
Apply 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.

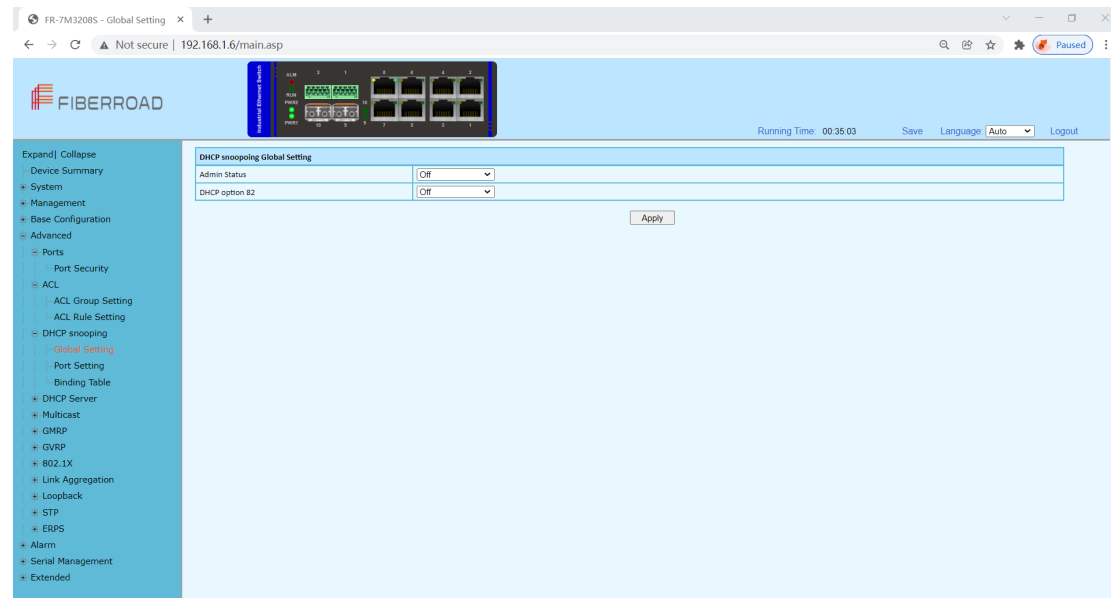
ACL Rule Setting	
Index	<0-65535>
Action	☒ Drop ☐ Permit ☐ Redirect GE/1
Filtering Rule	--
IP Protocol	☒ ICMP ☐ IGMP ☐ TCP ☐ UDP Delete
Source MAC	☒ Any ☐ xxxxxx-xxxxxx MASK: FFFFFF-FFFFFF Delete
Destination MAC	☒ Any ☐ xxxxxx-xxxxxx MASK: FFFFFF-FFFFFF Delete
VLAN	☒ Any ☐ <1-4094> Delete
Ethernet Type	☒ Any ☐ Hex Delete
Apply 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.



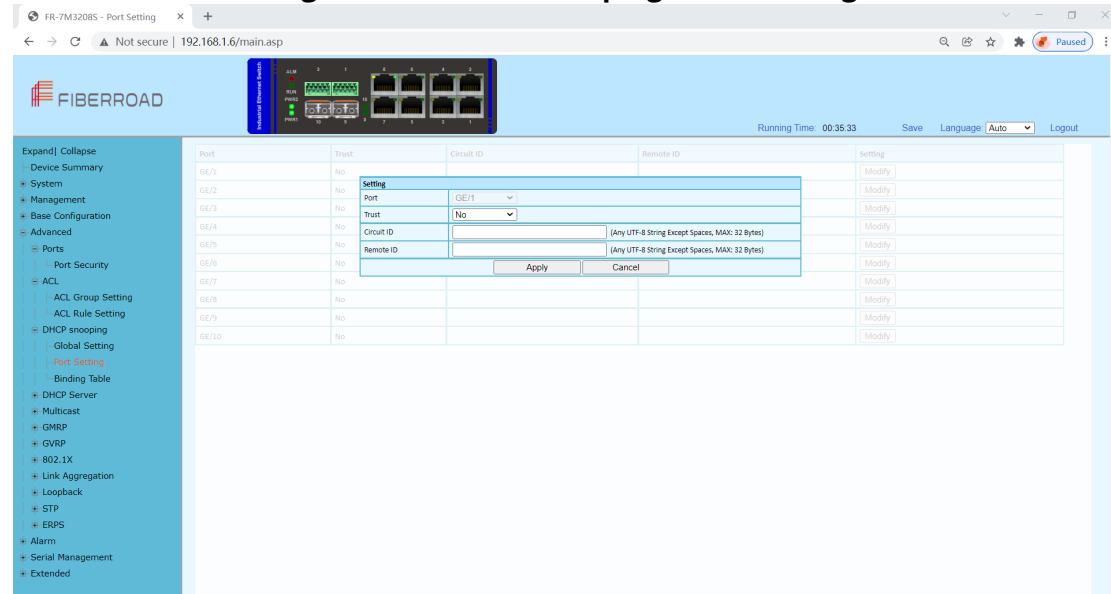
Configuration Steps

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
Apply	

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

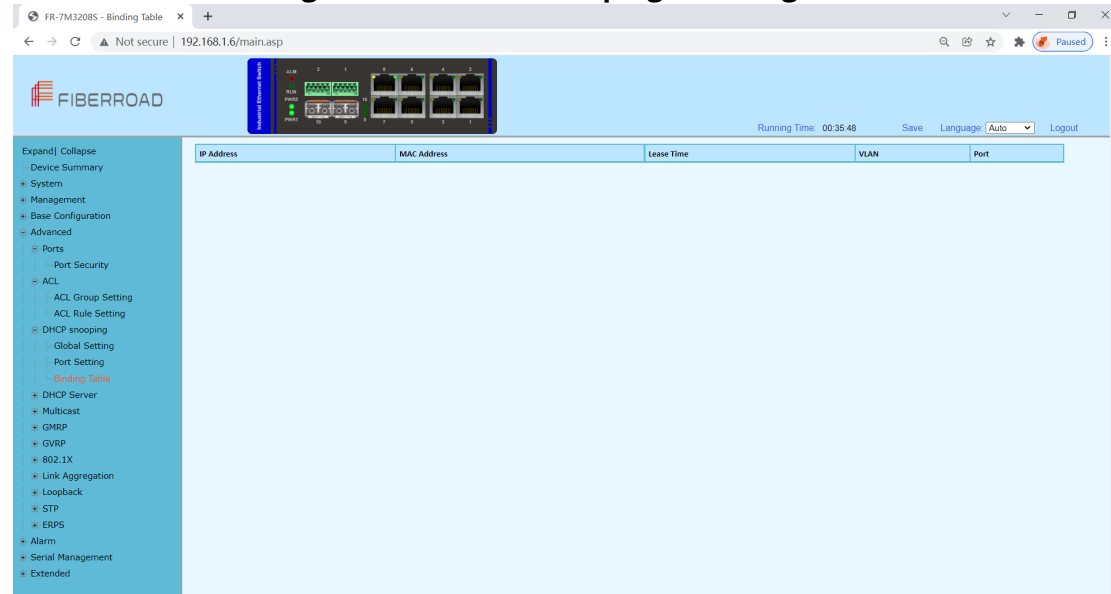


Configuration Steps

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



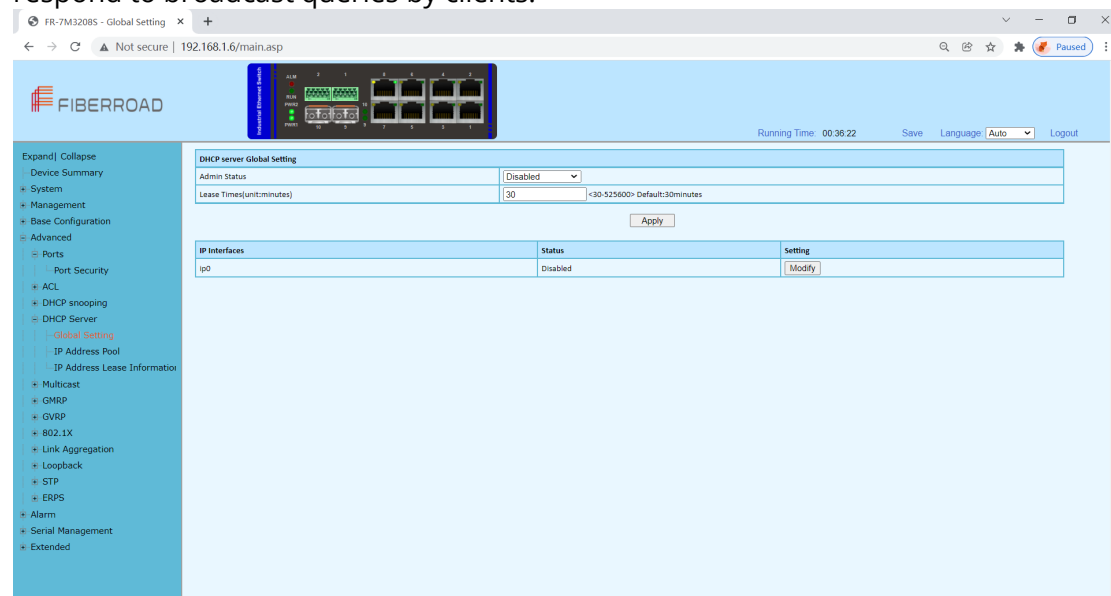
Configuration Steps

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.

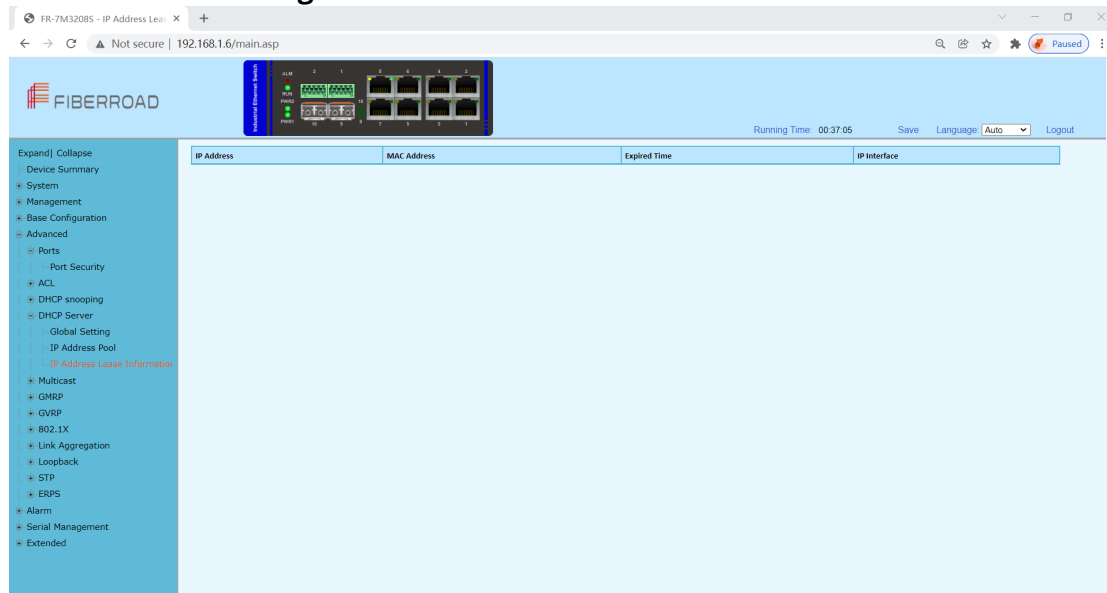
The screenshot shows the FiberRoad DHCP Server configuration interface. The left sidebar contains a navigation tree with options like 'Expand/Collapse', 'Device Summary', 'System', 'Management', 'Base Configuration', and 'Advanced'. The 'Advanced' section is expanded, showing 'Ports', 'Port Security', 'ACL', 'DHCP snooping', 'DHCP Server', 'Global Setting', 'IP Address Pool', and 'IP Address Lease Information'. The 'IP Address Pool' option is selected. The main content area displays the 'IP Address Pool' configuration form. The form has a 'Setting' tab and a table with columns: Pool Name, IP Interface, Start IP Address, End IP Address, Subnet Mask, Lease Times, Default Gateway, DNS Server, Secondary DNS Server, and Static IP Address. The 'Lease Times' field is set to '<30-525600-minutes'. The 'Default Gateway', 'DNS Server', and 'Secondary DNS Server' fields are set to 'IPV4(A.B.C.D)'. The 'Static IP Address' field has an 'Add' button. The form includes 'Apply' and 'Cancel' buttons at the bottom.

Configuration Steps

1. Select [Advanced / DHCP Server / IP Address Pool] in the navigation bar to enter the DHCP Server [IP Address Pool] interface.
2. All IP Address Pool information can be viewed in the DHCP Server [IP Address Pool] interface.
3. Click [Add] to add IP address pool individually. Click [Apply] to complete the configuration.

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

4.4.3 Advanced Configuration – DHCP Server – IP Address Lease Information



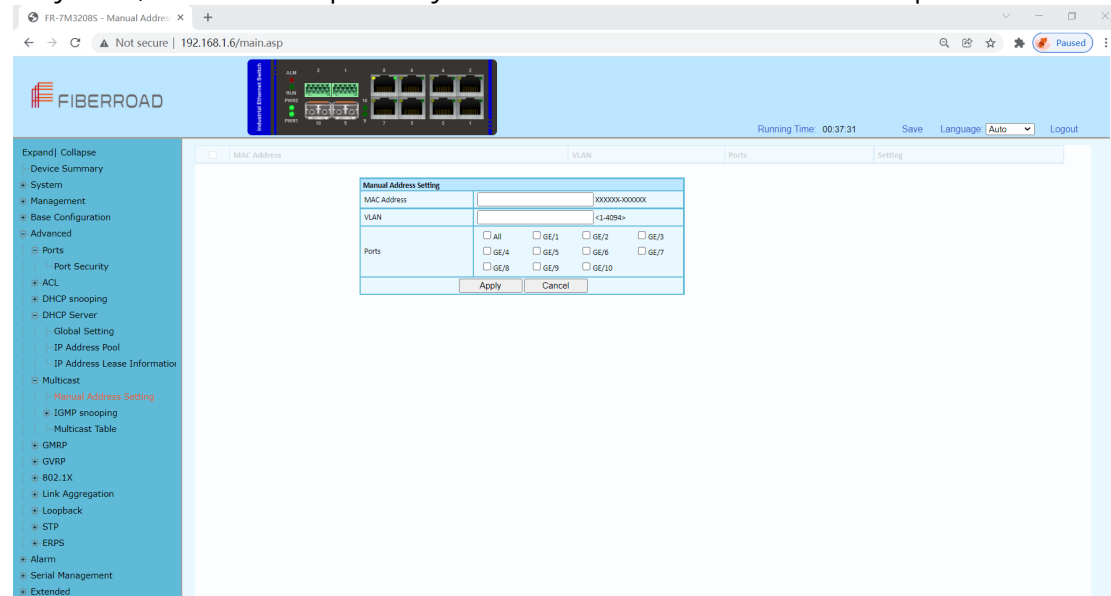
Configuration Steps

1. Select [Advanced / DHCP Server / IP Address Lease Information] in the navigation bar to enter the DHCP Server [IP Address Lease Information] interface.
2. All IP Address Lease Information can be viewed in the DHCP Server [IP Address Lease Information] interface.
3. Click [Refresh] to refresh the list of the information.

4.5 Advanced Configuration – Multicast

4.5.1 Advanced Configuration – Multicast – Manual Address Setting

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

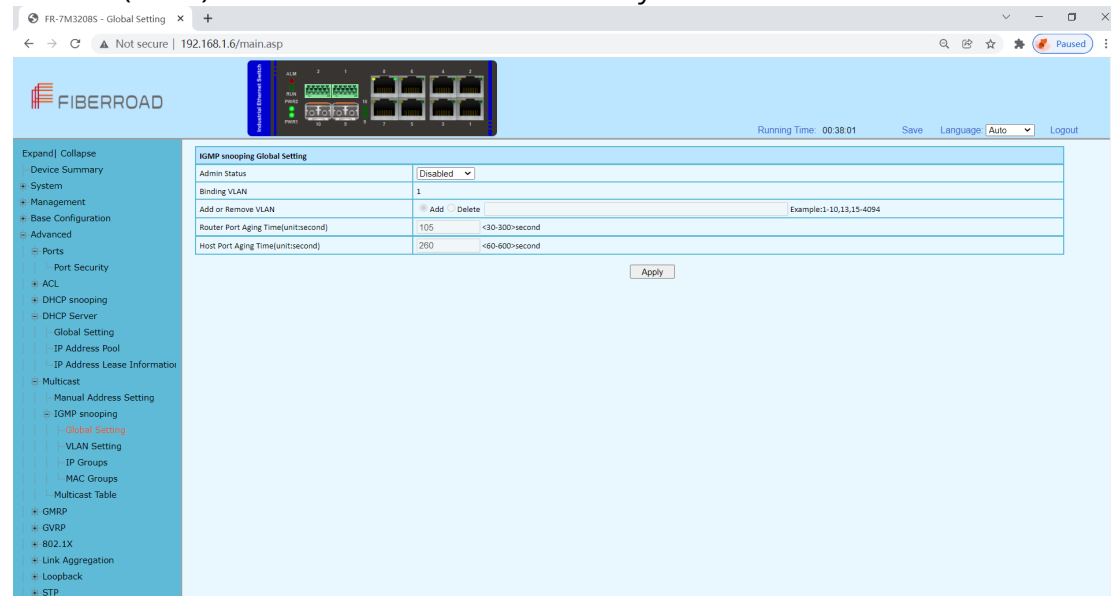


Configuration Steps

1. Select [Advanced / Multicast / Manual Address Setting] in the navigation bar to enter the Multicast [Manual Address Setting] interface.
2. All manual address can be viewed in the Multicast [Manual Address Setting] interface.
3. Click [Add] to manual add MAC address and VLAN for corresponding ports.
4. Click [Apply] to complete the configurations.

4.5.2 Advanced Configuration – Multicast – IGMP snooping Global Setting

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



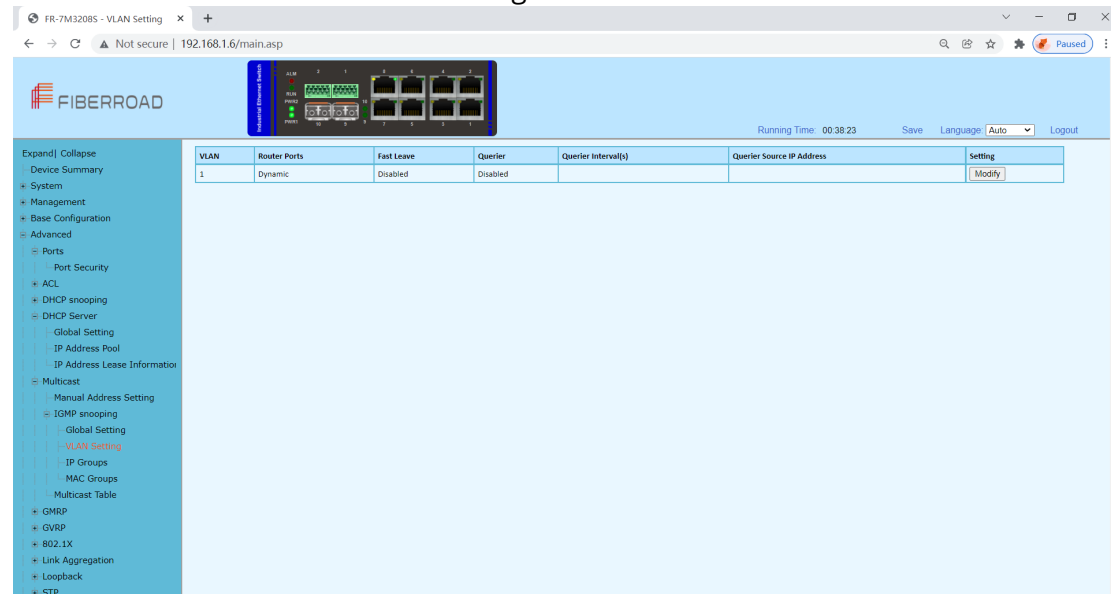
Configuration Steps

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

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

4.5.3 Advanced Configuration – Multicast – IGMP snooping VLAN setting

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



Configuration Steps

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

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.

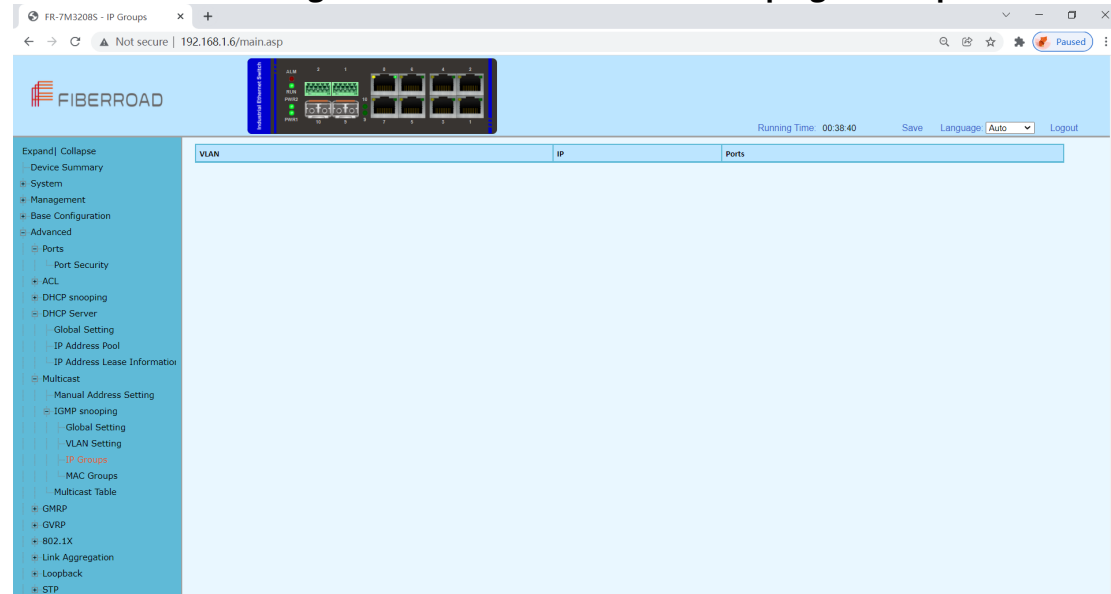
VLAN Setting	
VLAN	1 <1-4094>
Router Port Mode	Dynamic
Fast Leave	Disabled
Querier	Disabled
Querier Interval	60 s <30-120> s
Querier Source IP Address	0.0.0.0 A.B.C.D
Apply Cancel	

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	Example:1-10,13,15-4094
Router Port Mode	☐ Dynamic
Fast Leave	☐ Disabled
Querier	☐ Disabled
Apply Cancel	

Item	Description	Notes
VLAN	VLAN being configured	
	Select the mode of the routed port in this VLAN. Use the drop-down box to modify it.	
Router Port Mode	Dynamic Static - If you choose the static routing port mode, you still need to select specific routing ports. It can be selected with the check button.	
Fast Leave Mode	Select whether to enable the quick leave mode under this VLAN. Use the drop-down box to modify it. Disabled Enabled	
Querier	Select whether to enable the querier function in this VLAN. Use the drop-down box to modify it. Disabled Enable - If the querier is enabled, you need to set the corresponding querier interval and query source IP address.	
Query Interval	The query interval of the querier is 30-120 seconds.	
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

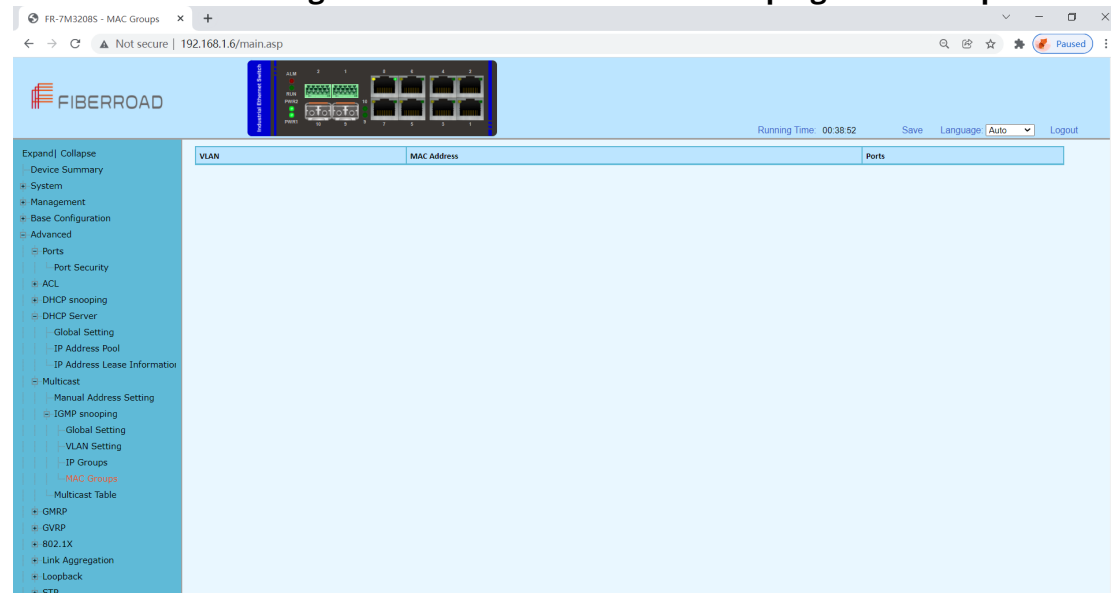


Configuration Steps

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].

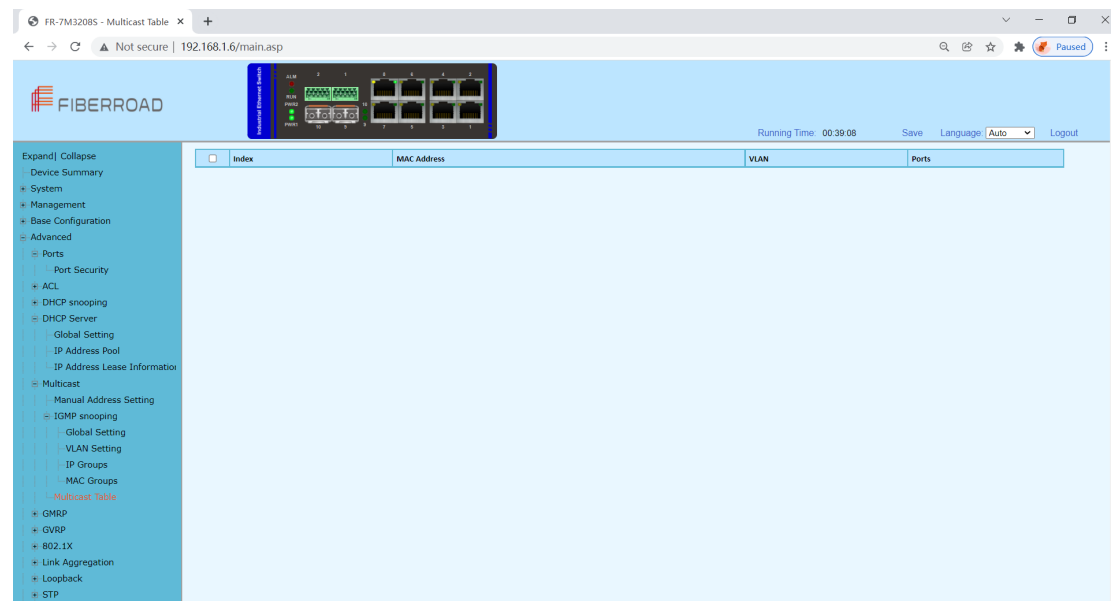
4.5.5 Advanced Configuration – Multicast – IGMP snooping MAC Groups



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



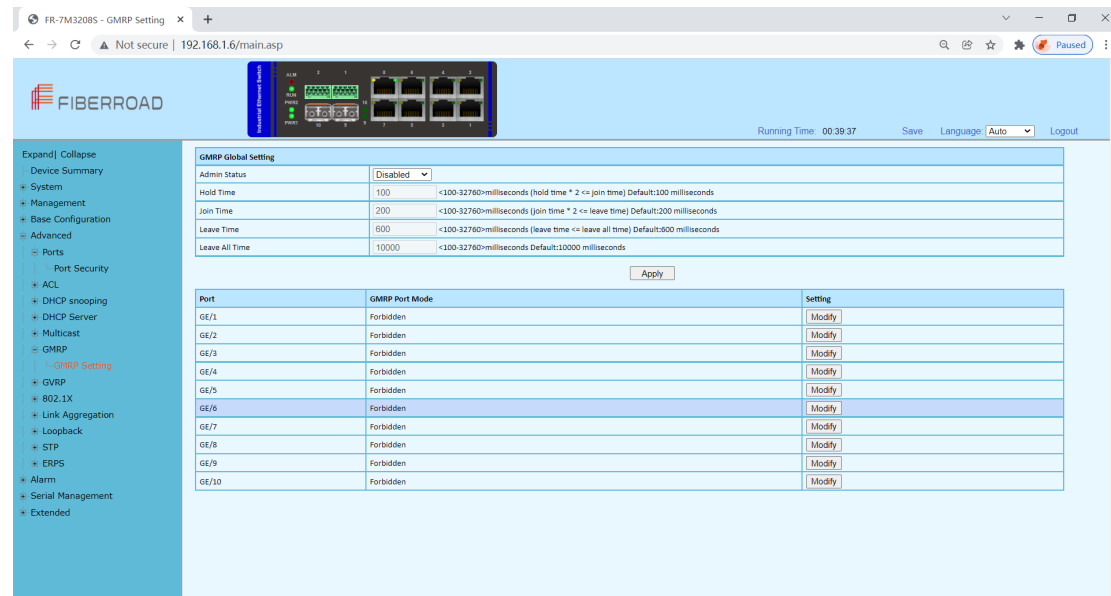
Configuration Steps

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	☐ Normal ☐ Fixed ☒ Forbidden
Apply 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

The screenshot shows the GVRP configuration interface for a FiberRoad switch. The top section is titled 'GVRP Global Setting' and includes fields for Admin Status (Disabled), Hold Time (100), Join Time (200), Leave Time (600), and Leave all Time (10000). Below this is a table for 'GVRP Port Mode' configurations for ports GE/1 through GE/10. Each port is currently set to 'Forbidden' mode, and there is a 'Modify' button for each entry.

Port	GVRP Port Mode	Setting
GE/1	Forbidden	Modify
GE/2	Forbidden	Modify
GE/3	Forbidden	Modify
GE/4	Forbidden	Modify
GE/5	Forbidden	Modify
GE/6	Forbidden	Modify
GE/7	Forbidden	Modify
GE/8	Forbidden	Modify
GE/9	Forbidden	Modify
GE/10	Forbidden	Modify

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

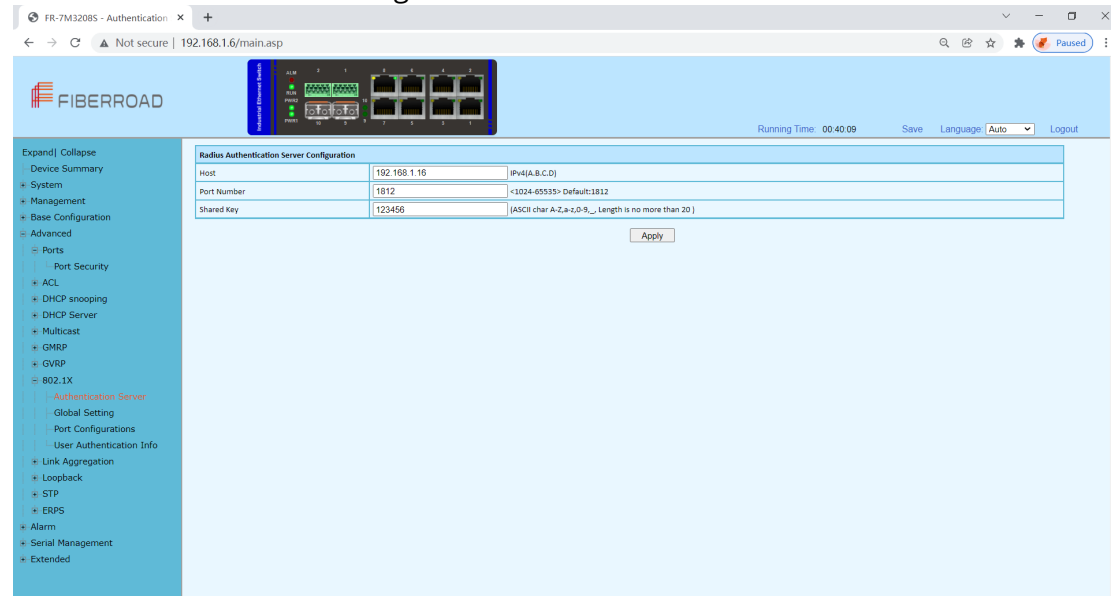
GVRP Port Mode	
Port	GE/1
GVRP Mode	☐ Normal ☐ Fixed ☒ Forbidden
Apply Cancel	

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

4.8 Advanced Configuration – 802.1X

4.8.1 Advanced Configuration – 802.1X – Authentication Server

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

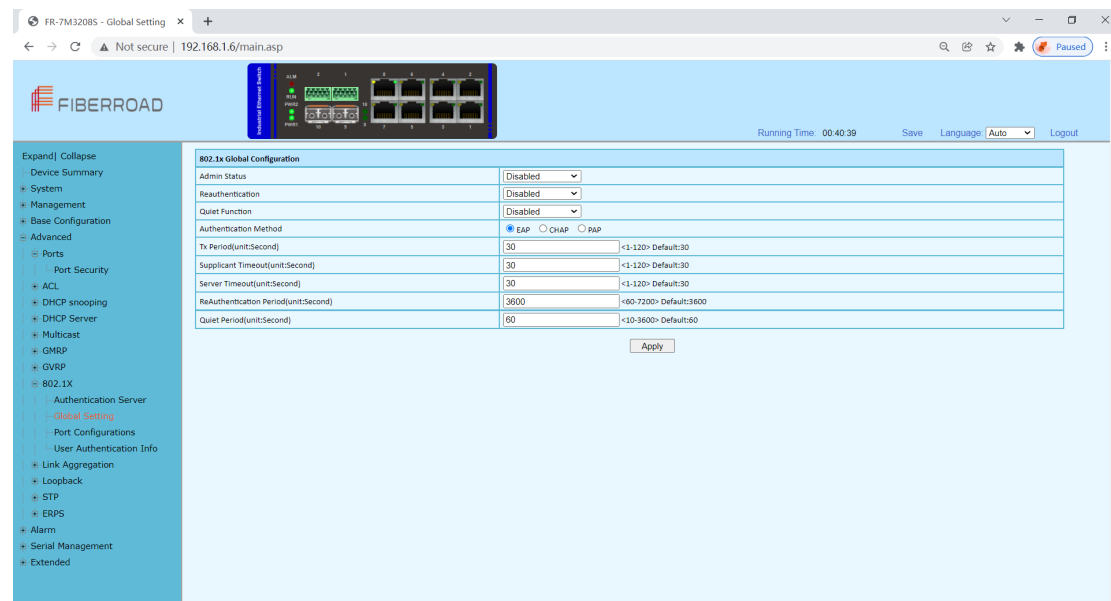


Configuration Steps

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

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

4.8.2 Advanced Configuration – 802.1X – Global Setting

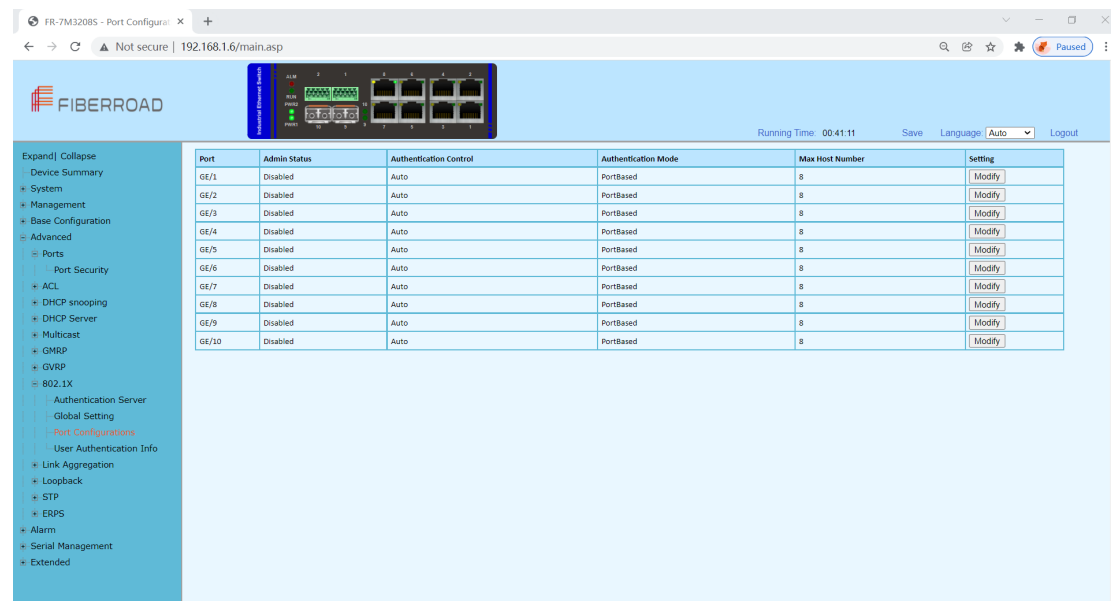


Configuration Steps

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

ITEM	DESCRIPTION	NOTES
ADMIN STATUS	Disabled: Disabled Global 802.1X Enabled: Enabled Global 802.1X	Default: Disabled
REATUTHENTICATION	Disabled: Disabled re-authentication Enabled: Enabled re-authentication	Default: Disabled
QUIET FUNCTION	Disabled: Disabled quiet function Enabled: Enabled quiet function	Default: Disabled
AUTHENTICATION METHOD	EAP/PAP/CHAP	
TX PERIOD (UNIT: SECOND)	1-120	Default: 30
SUPPLICANT TIMEOUT (UNIT: SECOND)	1-120	Default: 30
SERVER TIMEOUT (UNIT:SECOND)	1-120	Default: 30
REAUTHENTICATION PERIOD (UNIT:SECOND)	60-7200	Default: 3600
QUIET PERIOD (UNIT:SECOND)	10-3600	Default: 60

4.8.3 Advanced Configuration – 802.1X – Port Configurations



Configuration Steps

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

802.1X Port Configurations	
Port	GE/5 ▼
Admin Status	Disabled ▼
Authentication Control	Auto ▼
Authentication Mode	PortBased ▼
Max Host Number	8 <1-8> Default:8
Apply 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.

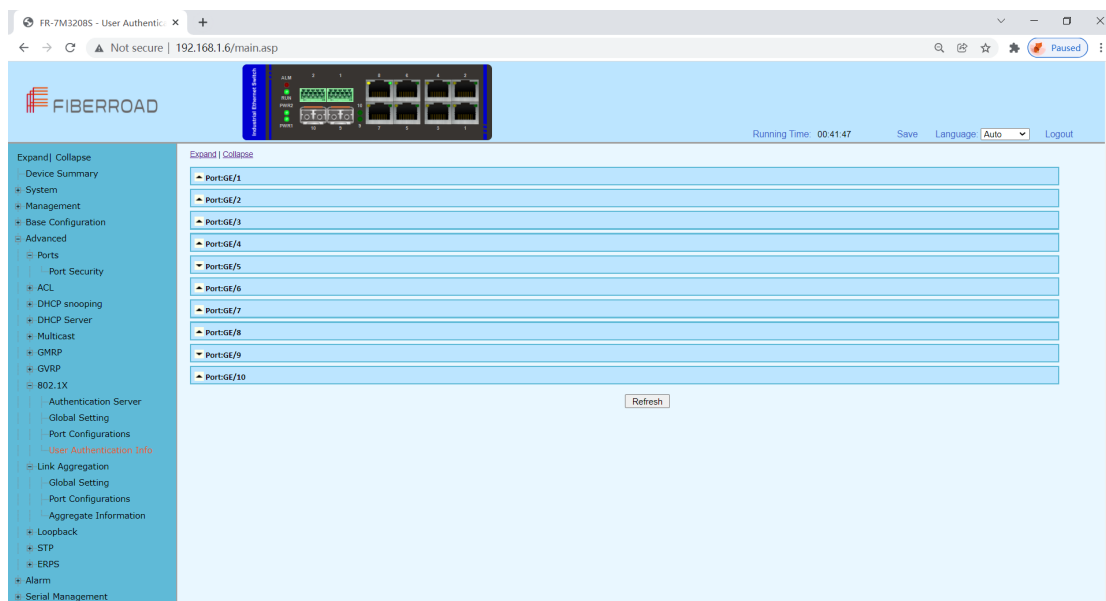
MacBased: All users need to be authenticated individually to access the network.

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



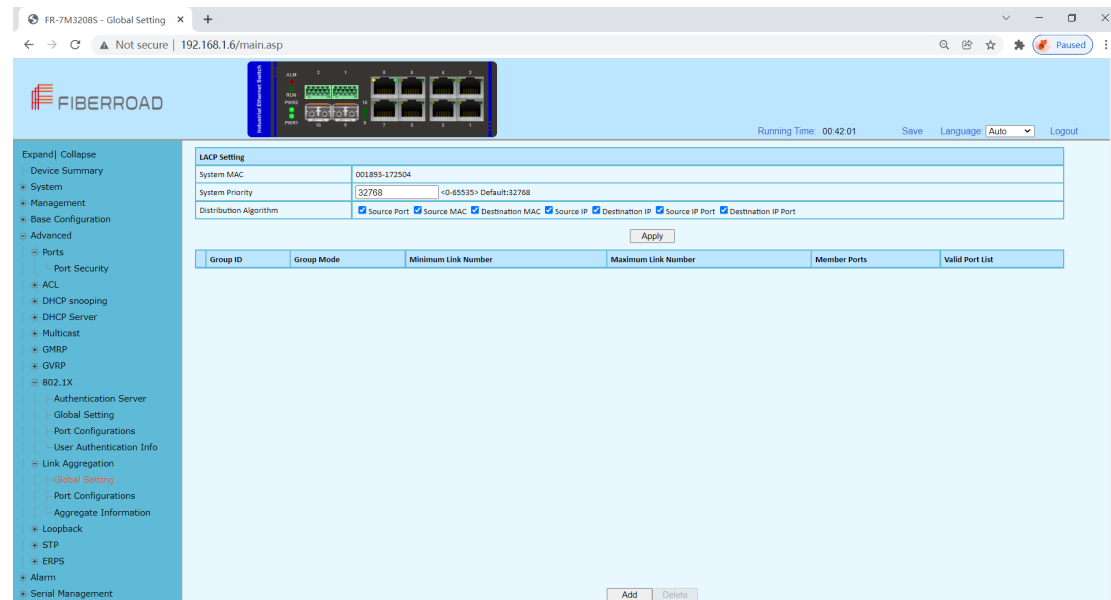
Configuration Steps

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 closed. Static: Static mode, the port of the	

Minimum Port

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

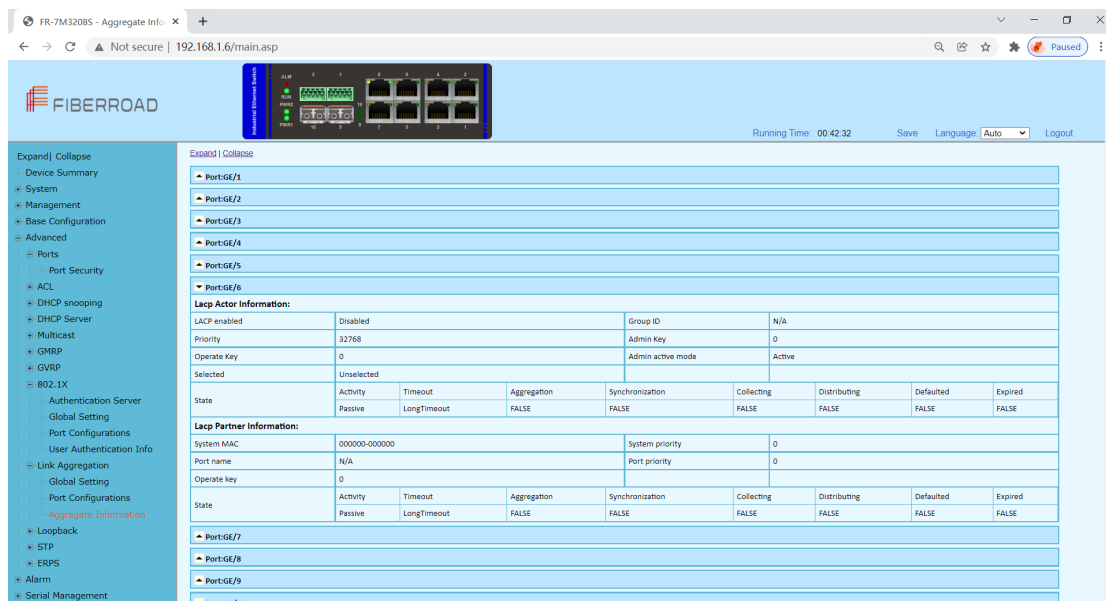
Port	Group ID	Priority	Admin Key	LACP Mode	LACP Admin Status	Setting
GE/1	0	32768	0	Active	Disabled	Modify
GE/2	0	32768	0	Active	Disabled	Modify
GE/3	0	32768	0	Active	Disabled	Modify
GE/4	0	32768	0	Active	Disabled	Modify
GE/5	0	32768	0	Active	Disabled	Modify
GE/6	0	32768	0	Active	Disabled	Modify
GE/7	0	32768	0	Active	Disabled	Modify
GE/8	0	32768	0	Active	Disabled	Modify
GE/9	0	32768	0	Active	Disabled	Modify
GE/10	0	32768	0	Active	Disabled	Modify

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 Group ID	Name of port 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

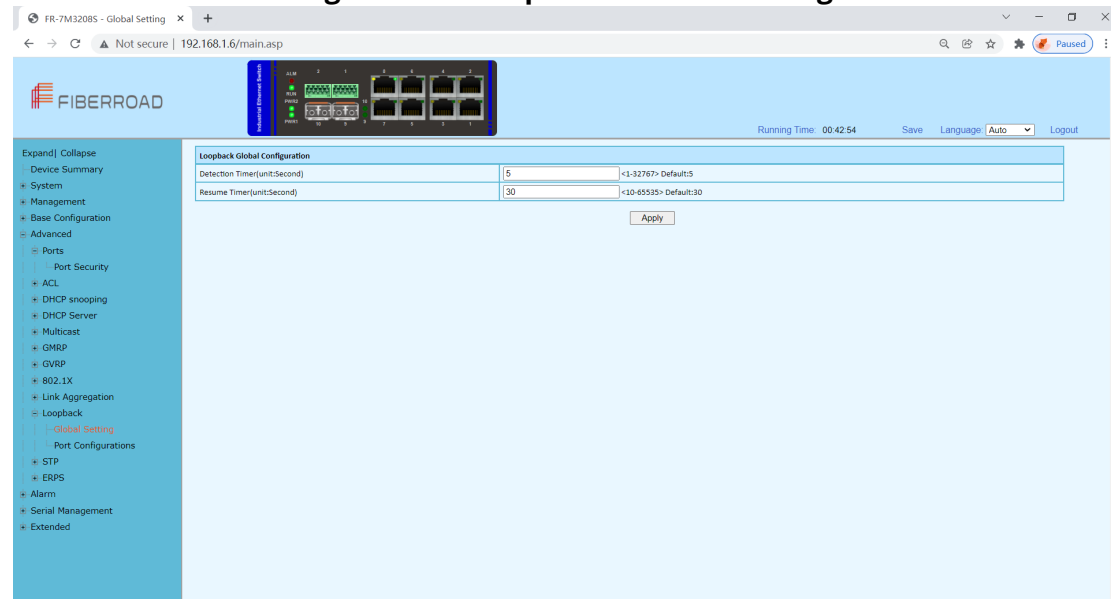


Configuration Steps

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

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

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.

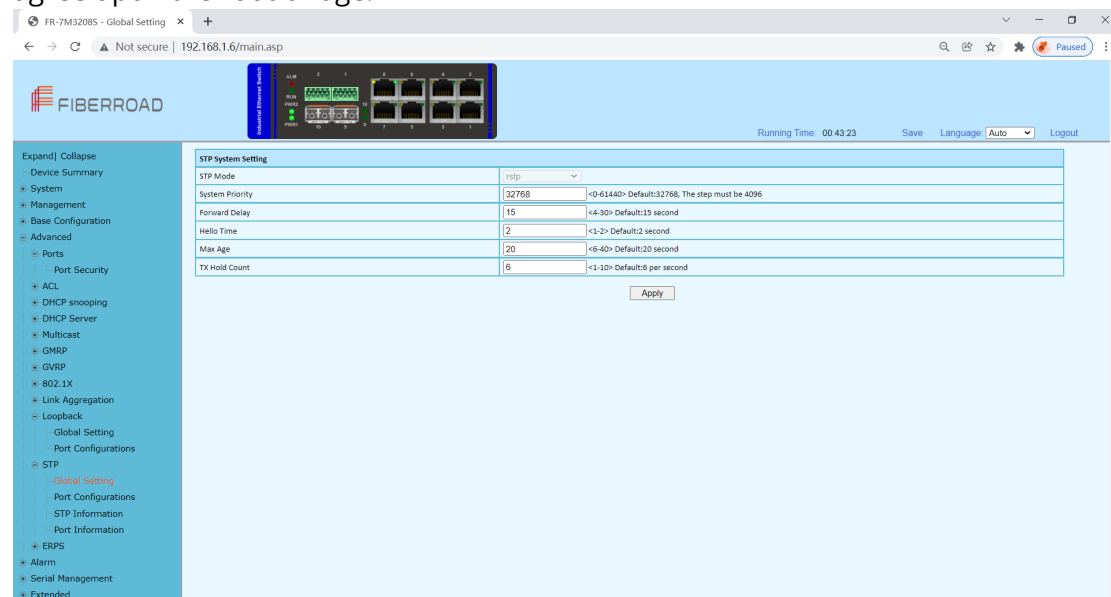
LoopBack Port Configurations	
Port	GE/7 ▼
Admin Status	Disabled ▼
Resume Mode	Automation ▼
Execute Operate	Shutdown ▼
Apply Cancel	

Item Port	Description	Notes
Admin Status	Selected Port	
	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.

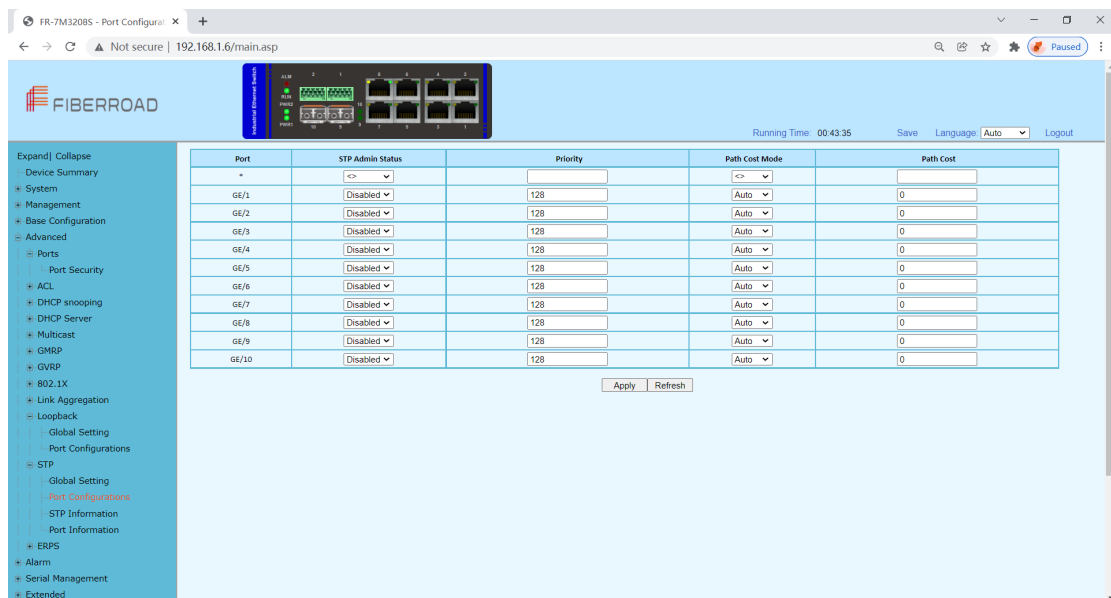


Configuration Steps

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



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

The screenshot shows the Fiberroad web interface for STP Information configuration. The main content area displays the following information:

- STP Mode:** rstp
- Bridge ID:** 001899-172504 / 32768
- Root ID:** 001899-172504 / 32768
- Root Path Cost:** 0

Below this, there are two tables for timer configurations:

Admin Timers Value	Forward Delay	Hello Time	Max Age	Transit Limit
15 (second)	2 (second)	20 (second)	6 (per second)	

Operative Timers Value	Forward Delay	Hello Time	Max Age	Message Age
15 (second)	2 (second)	20 (second)	0 (second)	

A "Refresh" button is located below the Operative Timers table.

The left sidebar contains a navigation menu with the following items:

- Expand/Collapse
- Device Summary
- System
- Management
- Base Configuration
- Advanced
 - Ports
 - Port Security
 - ACL
 - DHCP snooping
 - DHCP Server
 - Multicast
 - GMP
 - GVRP
 - 802.1X
 - Link Aggregation
 - Loopback
 - Global Setting
 - Port Configurations
 - STP
 - Global Setting
 - Port Configurations
 - STP Information
 - Port Information
 - ERPS
 - Alarm
 - Serial Management
 - Extended

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

The screenshot shows the FIBERROAD web interface. The left sidebar contains a navigation menu with categories like System, Management, Base Configuration, Advanced, ACL, DHCP snooping, DHCP Server, Multicast, GMRP, GVRP, 802.1X, Link Aggregation, Loopback, Global Setting, Port Configurations, STP, Global Setting, Port Configurations, STP Information (highlighted), ERPS, Alarm, Serial Management, and Extended. The main content area displays the STP configuration for PortGE/6. It includes a table with the following data:

STP enabled	Disabled	Priority	128	Role	disabled port	PartnerVersion	stp
State	discarding	AdminPathCost	0	AutoPathCost	Enabled		
OperPathCost	0	OperEdge	Disabled	OperP2P	Disabled		

Below the table, there is a 'Refresh' button. The interface also shows a 'Running Time' of 00:44:18 and a 'Save' button.

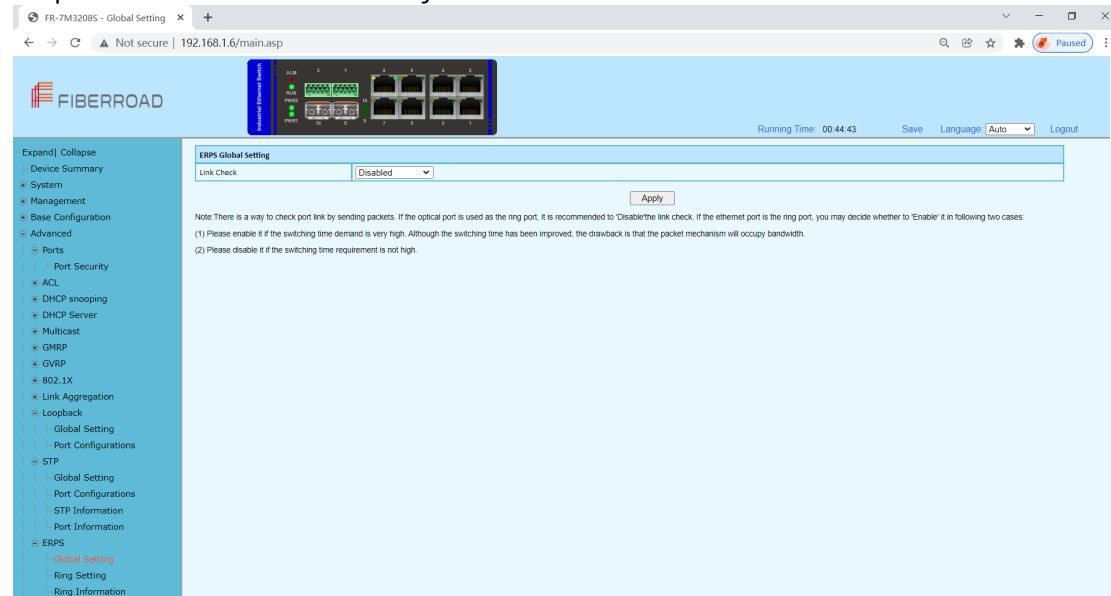
Configuration Step

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.

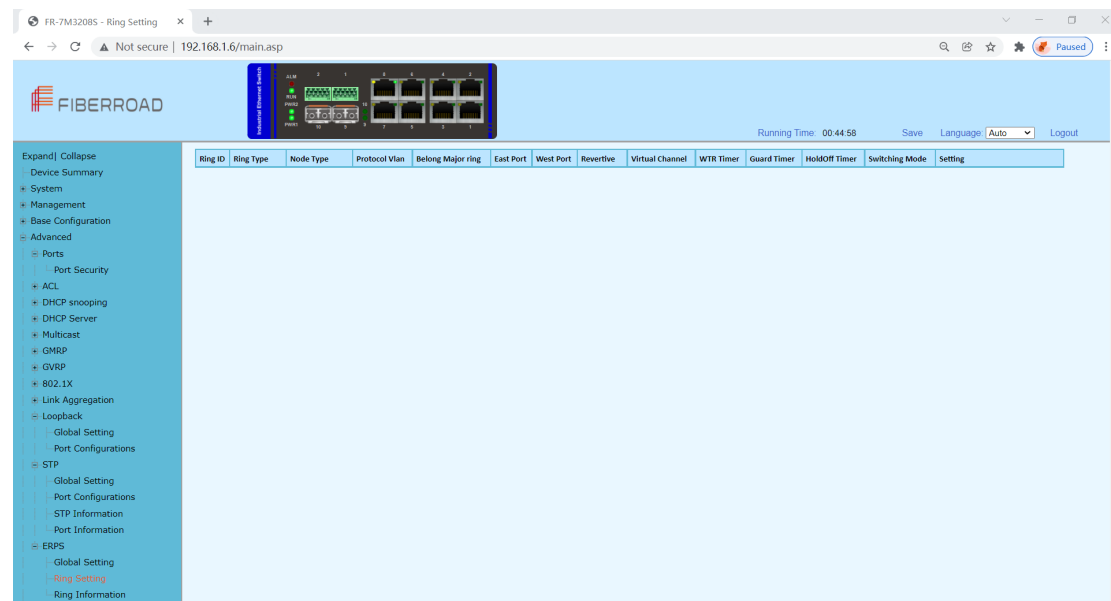


Configuration Step

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



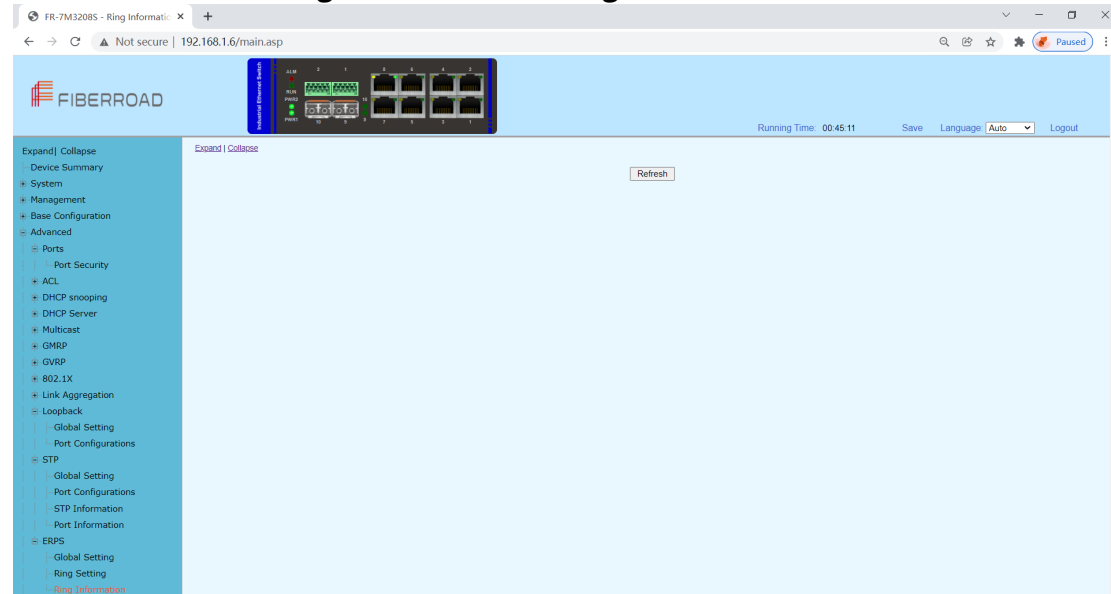
Configuration Step

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	Transfer: Forward both service packets and protocol packets rpl-owner: Responsible for blocking traffic over the RPL so that no loops are formed in the Ethernet traffic. There can be only one RPL owner in a ring. rpl-neighbour: An Ethernet ring node adjacent to the RPL. It is responsible for blocking its end of the RPL under normal conditions. This node type is optional and prevents RPL usage when protected.	
Protocol VLAN	Adding ring ERPS protocol VLAN	
East Port	A Ring port created on this node	
West Port	Another ring port created on the node	
RPL Port	*Port on an RPL Link	
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

Alarm Event	Port	Admin Status	Link Status	Alarm Status
LinkDown	GE/1	Disabled	No	No
LinkDown	GE/2	Disabled	No	No
LinkDown	GE/3	Disabled	No	No
LinkDown	GE/4	Disabled	No	No
LinkDown	GE/5	Disabled	No	No
LinkDown	GE/6	Disabled	No	No
LinkDown	GE/7	Disabled	No	No
LinkDown	GE/8	Disabled	No	No
LinkDown	GE/9	Disabled	No	No
LinkDown	GE/10	Disabled	No	No
Power Supply	N/A	Enabled	N/A	No
Low Temperature	N/A	Enabled	N/A	No
High Temperature	N/A	Enabled	N/A	No

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

Alarm Event	Port	Admin Status	Link Status	Alarm Status
LinkDown	GE/1	Disabled	No	No
LinkDown	GE/2	Disabled	No	No
LinkDown	GE/3	Disabled	No	No
LinkDown	GE/4	Disabled	No	No
LinkDown	GE/5	Disabled	No	No
LinkDown	GE/6	Disabled	No	No
LinkDown	GE/7	Disabled	No	No
LinkDown	GE/8	Disabled	No	No
LinkDown	GE/9	Disabled	No	No
LinkDown	GE/10	Disabled	No	No
Power Supply	N/A	Enabled	N/A	No
Low Temperature	N/A	Enabled	N/A	No
High Temperature	N/A	Enabled	N/A	No

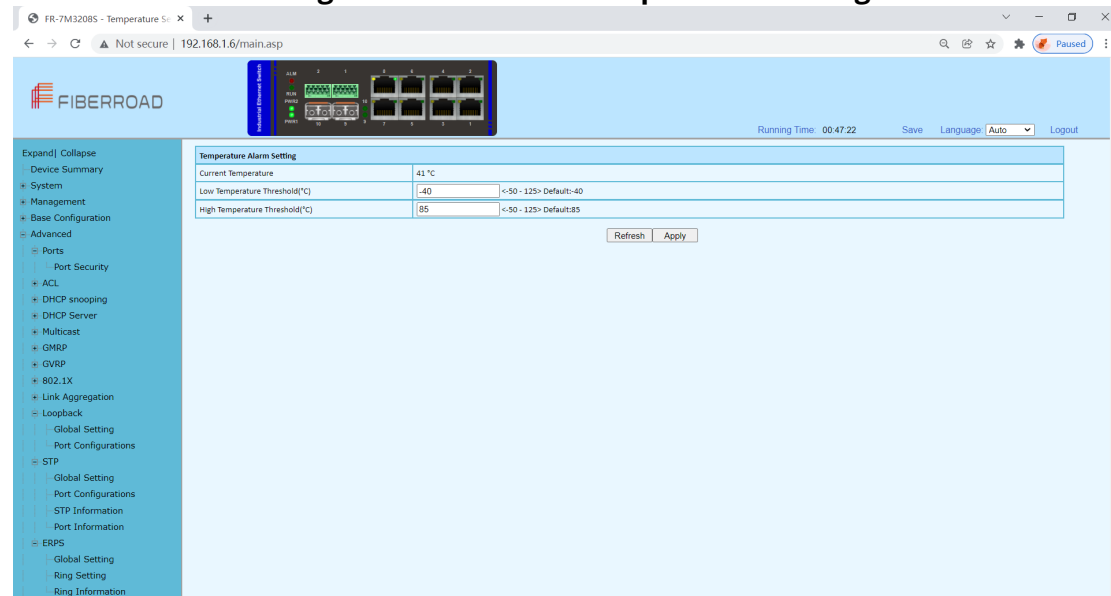
Configuration Step

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

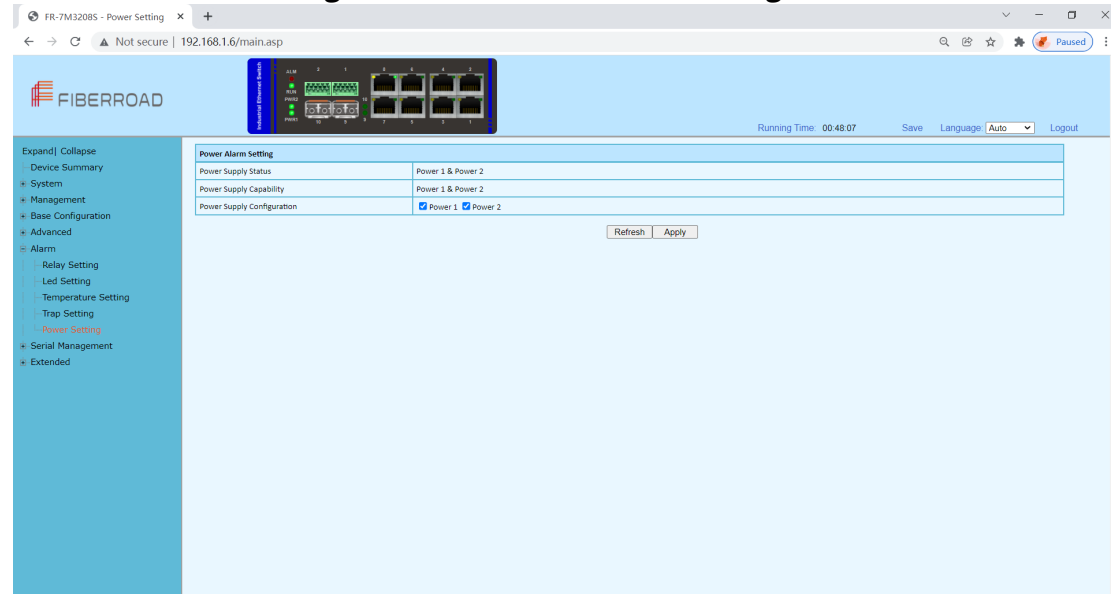
The screenshot shows the FIBERROAD web interface for the 'Trap Setting' configuration. The left sidebar contains a navigation menu with options like 'Expand/Collapse', 'Device Summary', 'System', 'Management', 'Base Configuration', 'Advanced', 'Alarm', 'Relay Setting', 'Led Setting', 'Temperature Setting', 'Trap Setting' (highlighted), 'Power Setting', 'Serial Management', and 'Extended'. The main content area displays a table with the following columns: Alarm Event, Port, Admin Status, Link Status, and Alarm Status. The table lists various events and their corresponding ports and statuses.

Alarm Event	Port	Admin Status	Link Status	Alarm Status
LinkUp	GE/1	Disabled	✗	No
LinkUp	GE/2	Disabled	✗	No
LinkUp	GE/3	Disabled	✗	No
LinkUp	GE/4	Disabled	✗	No
LinkUp	GE/5	Disabled	✗	No
LinkUp	GE/6	Disabled	✗	No
LinkUp	GE/7	Disabled	✗	No
LinkUp	GE/8	Disabled	✓	No
LinkUp	GE/9	Disabled	✗	No
LinkUp	GE/10	Disabled	✗	No
LinkDown	GE/1	Disabled	✗	No
LinkDown	GE/2	Disabled	✗	No
LinkDown	GE/3	Disabled	✗	No
LinkDown	GE/4	Disabled	✗	No
LinkDown	GE/5	Disabled	✗	No
LinkDown	GE/6	Disabled	✗	No
LinkDown	GE/7	Disabled	✗	No
LinkDown	GE/8	Disabled	✓	No
LinkDown	GE/9	Disabled	✗	No
LinkDown	GE/10	Disabled	✗	No
Power Supply	N/A	Enabled	N/A	No
Low Temperature	N/A	Enabled	N/A	No
High Temperature	N/A	Enabled	N/A	No

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

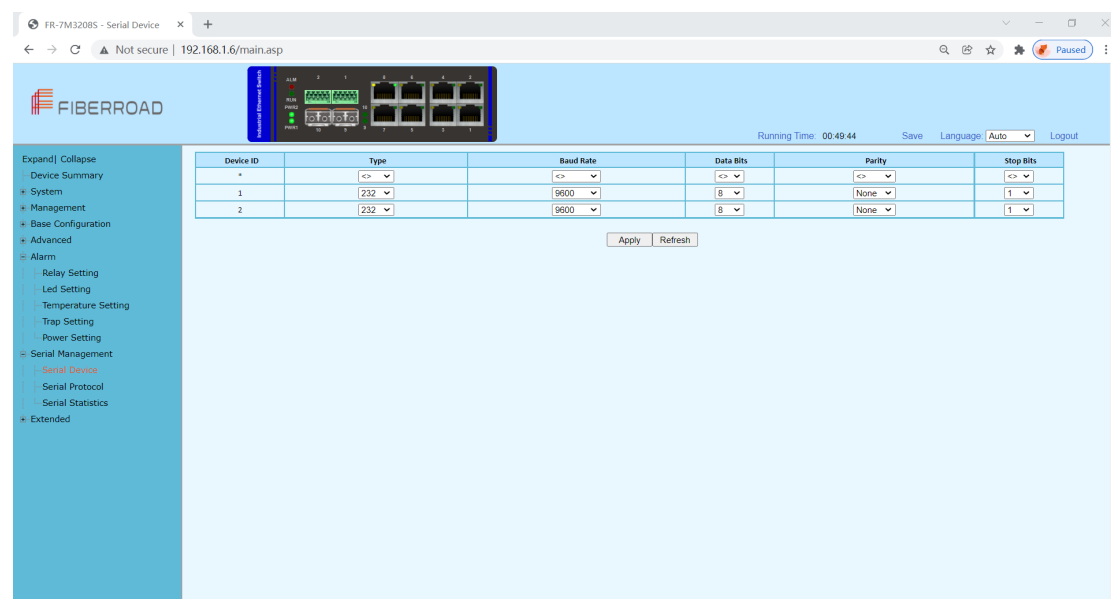


Configuration Steps

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 Serial Management

4.14.1 Serial Management – Serial Device

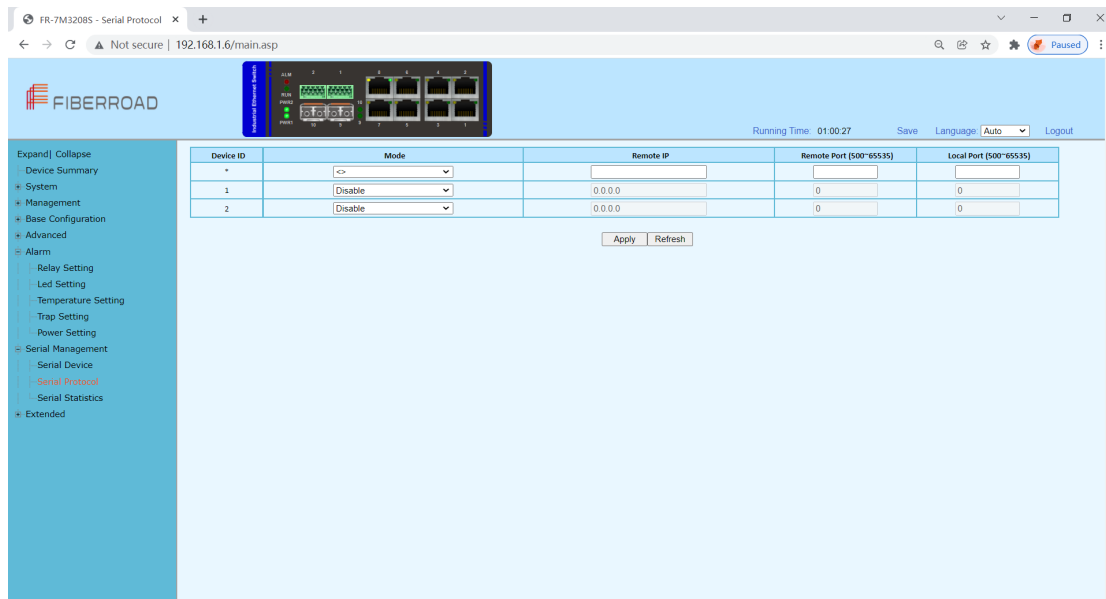


Configuration Steps

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

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

4.14.2 Serial Management – Serial Protocol



Configuration Steps

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

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

Notes: The original Modbus specification included two possible transmission modes: ASCII and RTU. Modbus RTU mode is the most common implementation, using binary coding and CRC error-checking. Modbus ASCII messages (though somewhat more readable because they use ASCII characters) is less efficient and uses less

effective LRC error checking. ASCII mode uses ASCII characters to begin and end messages whereas RTU uses time gaps (3.5 character times) of silence for framing. The two modes are incompatible so a device configured for ASCII mode cannot communicate with one using RTU. Modbus ASCII messages require twice as many bytes to transmit the same content as a Modbus RTU message.

4.14.3 Serial Management – Serial Statistics

The screenshot shows the FIBERROAD FR-7M320B5 Serial Statistics web interface. The browser address bar shows the URL 192.168.1.6/main.asp. The interface has a blue header with the FIBERROAD logo and a navigation menu on the left. The main content area displays statistics for two serial ports, Serial 1 and Serial 2. Each port has a 'Clear' button and a table showing Rx Bytes, Rx Packets, Tx Bytes, and Tx Packets, all currently at 0. At the bottom, there are 'Clear All' and 'Refresh' buttons. The top of the interface shows the device name, a 'Paused' status, and a 'Running Time' of 01:27:39.

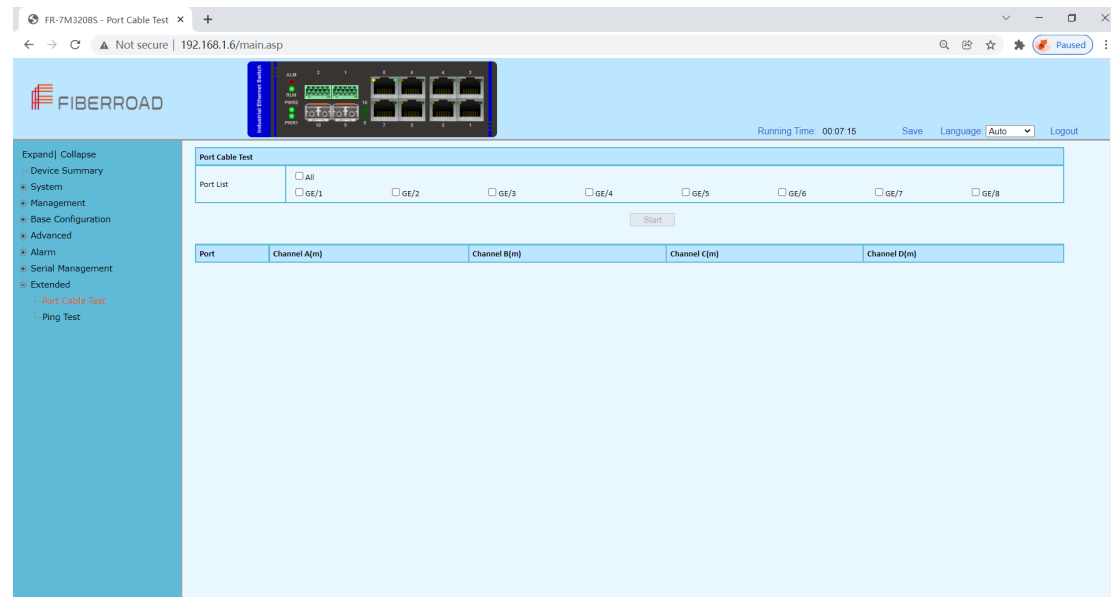
Configuration Steps

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

4.15 Advanced Configuration – Extended

4.15.1 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.

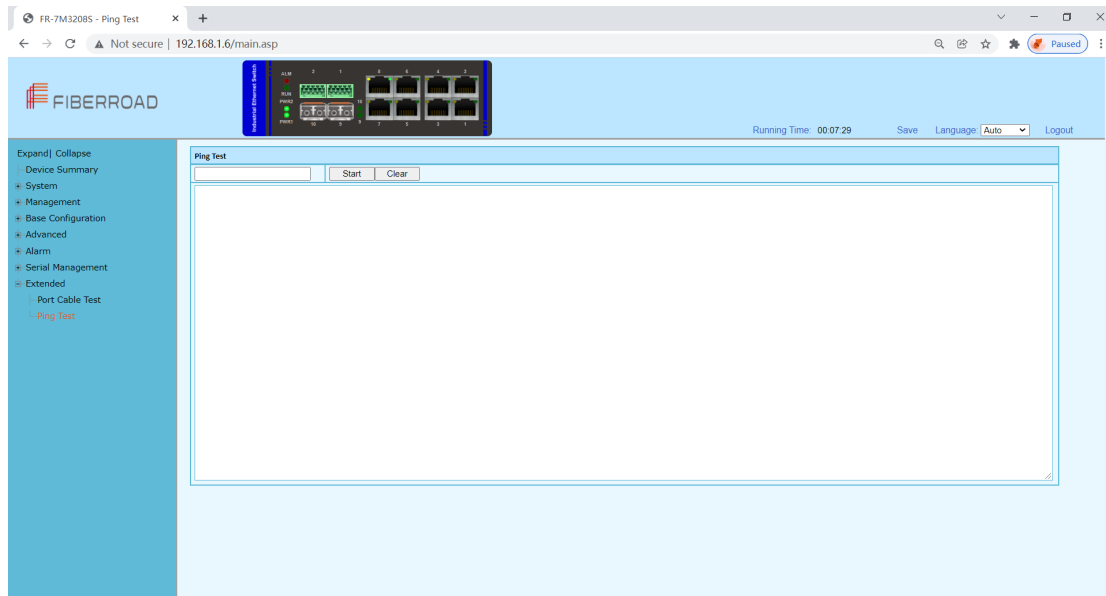


Configuration Step

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.

4.15.2 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

