FIBERROAD®

WEB SMART PLUS Series

WebGUI Management User Manual

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.

Jan 01, 2025

CONTENTS

Revision History

Version	Date	Author	Reasons of Change	Section(s) Affected
1.0	2025/1/2		Initial Release	All

Chapter 1 System Configurations

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

- System Information
- IP Setting
- User Account
- Port Setting

---

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

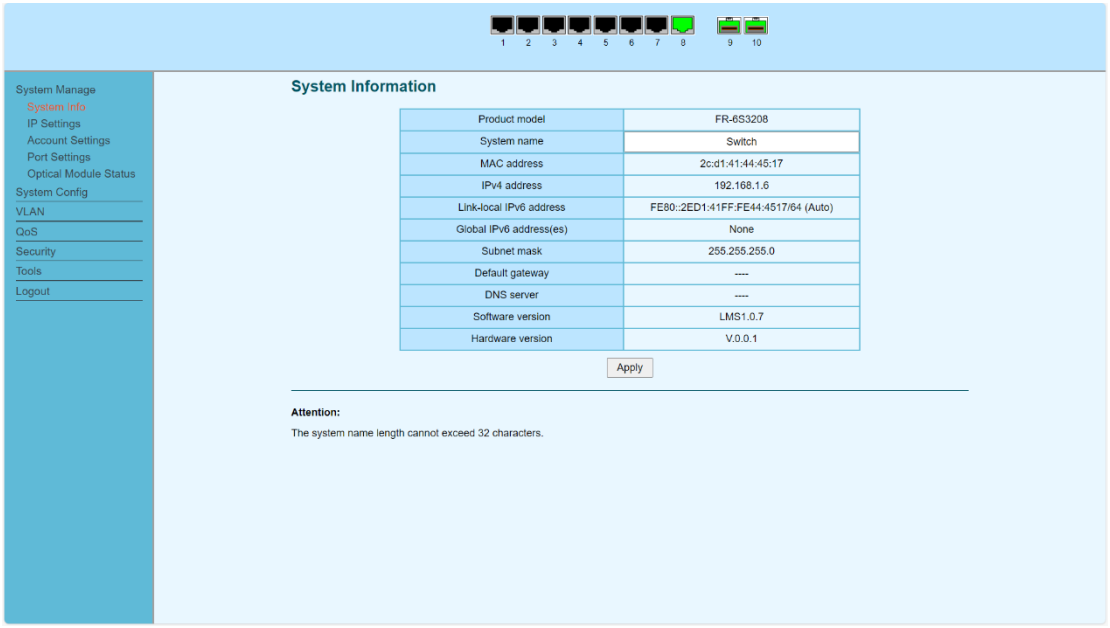
Before using the web management, install the industrial switch on the network and make sure that any one of the PCs on the network can connect with the industrial switch through the web browser.
The industrial switch default value of IP, subnet mask, username and password are listed as below:

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

1.2 System Manage

1.2.1 System Information

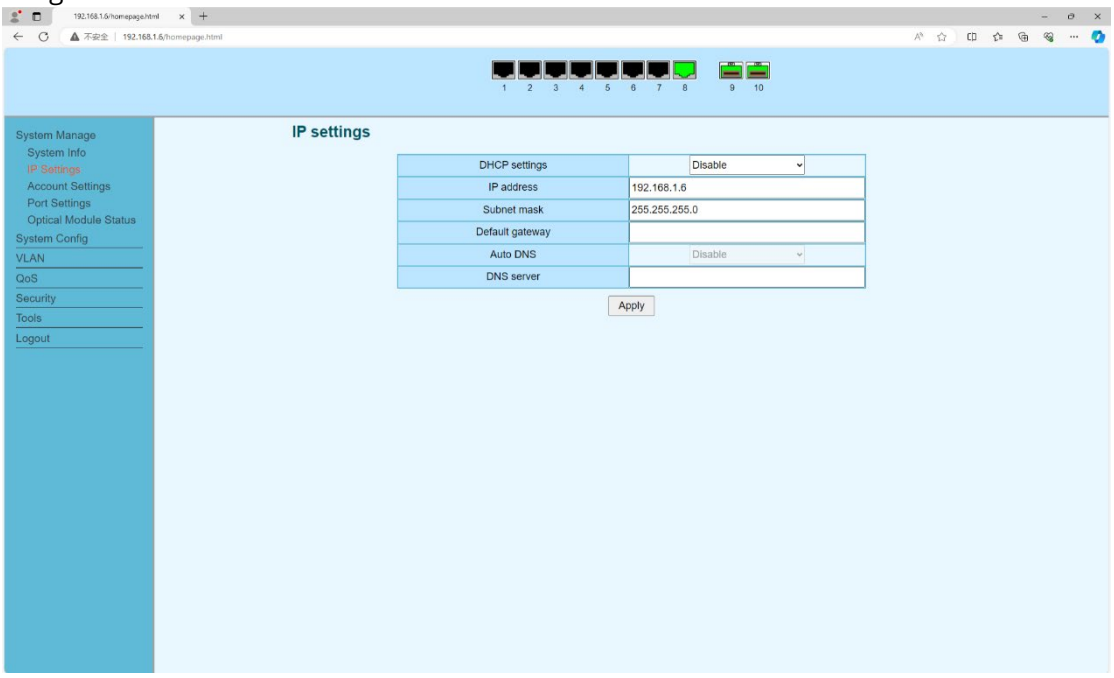
Overview the system information, including the System Name, MAC address, IPv4 address, Link-local IPv6 address,software version, Hardware version, etc.



Item	Description	Notes
System name	Default: Switch	The system name length cannot exceed 32 characters

1.2.2 System Manage-IP Settings

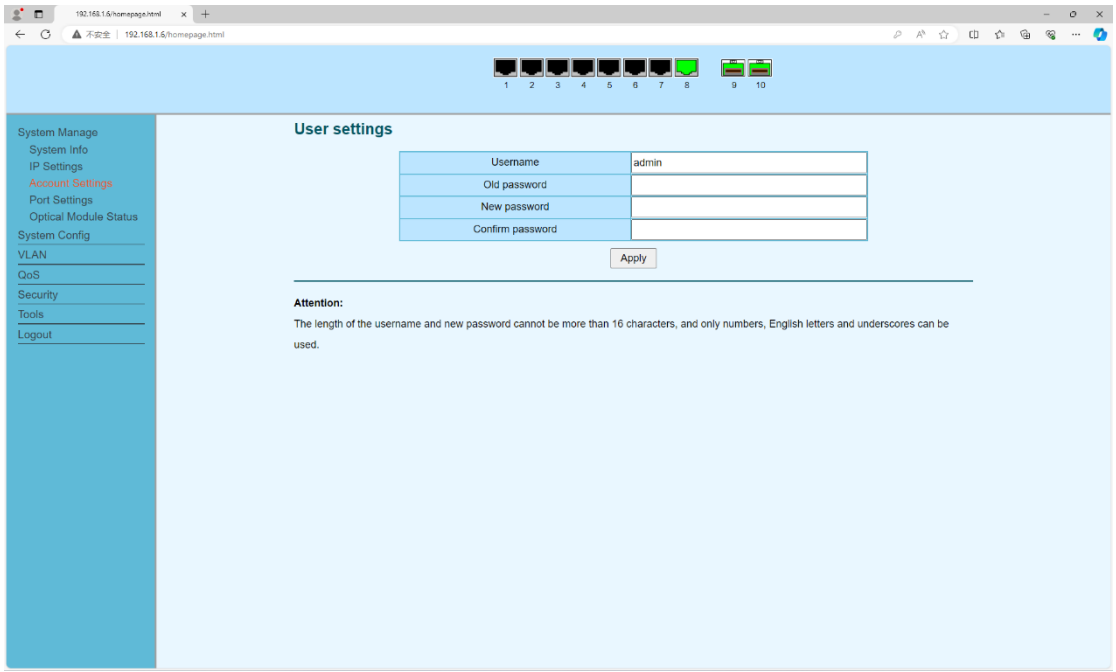
The IP setting is used to configure DHCP settings, IP address,Subnet mask, Default gateway and DNS server. The device supports Static IP address and DHCP automatically assigns IP address.



Item	Description	Notes
DHCP	Enable/Disable Default: Disable	When enabled, enable the DHC client to obtain the dynamic IP address. When disabled, use the configured static IP address.
IP Address	Default:192.168.1.6	Static IP Address
Subnet Mask	Default:255.255.255.0	Static IP subnet mask
Gateway	Default: N/A	Gateway Adress
Auto DNS	Default: Disablt	Automatically updates Domain Name System (DNS) records, typically for dynamic IP addresses.
DNS Server	Default: N/A	After enabling DHCP, the IP address is obtained from the host's address.

1.2.3 System Manage – Account Settings

The account setting is used to configure user name and password

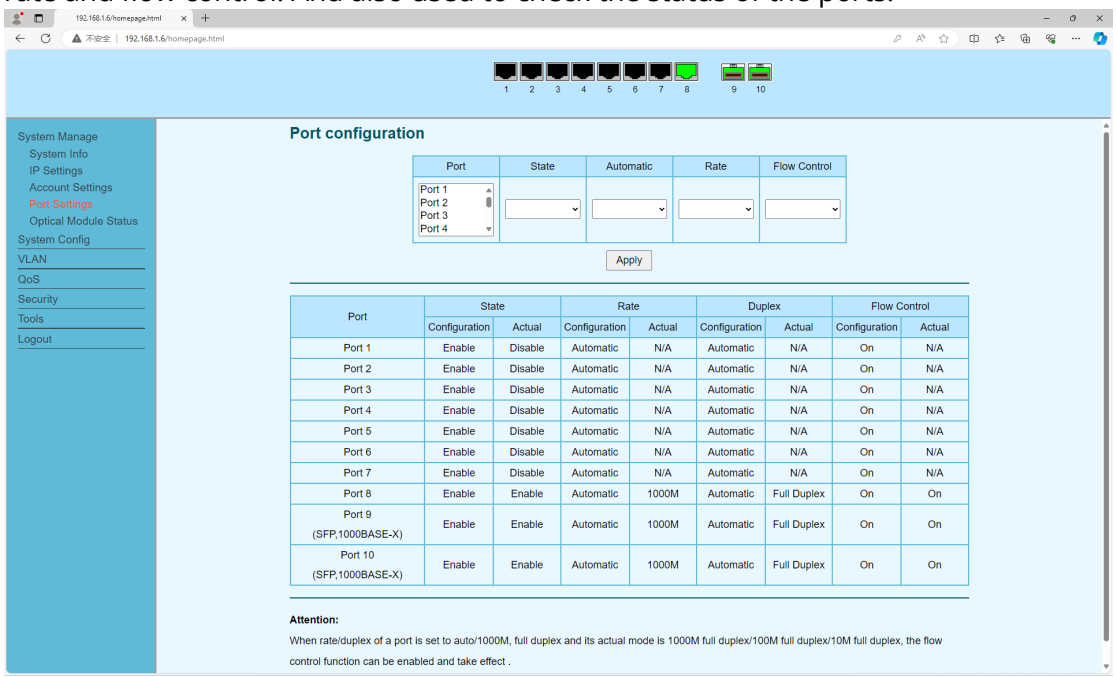


Item	Description	Notes
Username	Default: admin	The length of the username and new password cannot ne more that 16 characters, and only numbers, english letters and

	underscores can be used.
Old password	Default: admin
New password	
Confirm password	

1.2.4 System Manage-Port configuration

The port configuration is used to configure the specific port state,automatic and data rate and flow control. And also used to check the status of the ports.



Item	Description	Notes
Port	Port 1 to 10	
State	Enable/Diable Default: Enable	
Automatic	Automatic Rate matching Default: Enable	
Rate	When Automatic enabling, the rate does not to configure. When Automatic disabling, the rate option to be: 10M half/full duplex 100M half/full duplex 1000M half/full duplex	
Flow control	Enable/Disable Default: Enable	Prevent data loss and congestion

1.2.5 System Manage-Optical Module States

The Optical Module Stats is used to show the SFP Module operating status, such as Temperature, Tx Power(mW), Rx Power(mW) and Loss of Signal.

Chapter 2 System Configurations

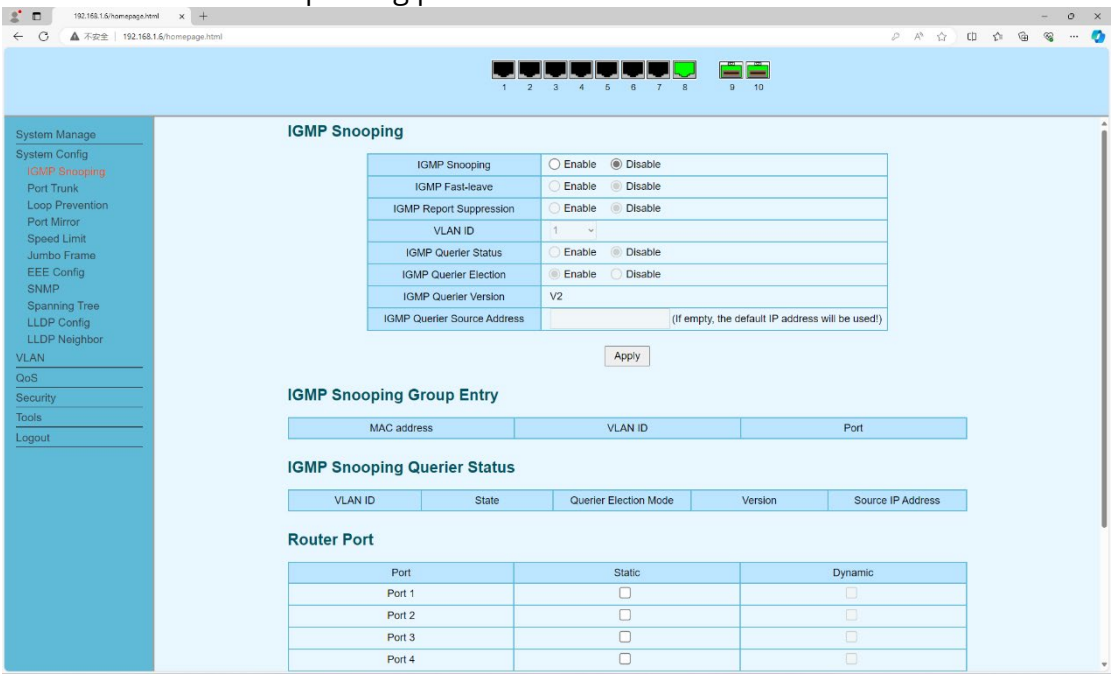
This chapter describes the System configuration in detail, including but not limit to the following:

- IGMP Snooping
- Loop Prevention
- Spanning Tree
- LLDP Configuration

2. System Configuration

2.1 System Configuration-IGMP Snooping

IGMP Snooping is a feature in network switches that optimizes the delivery of multicast traffic. It allows the switch to intelligently forward multicast packets only to devices that are interested in receiving them, reducing unnecessary network traffic and improving performance.

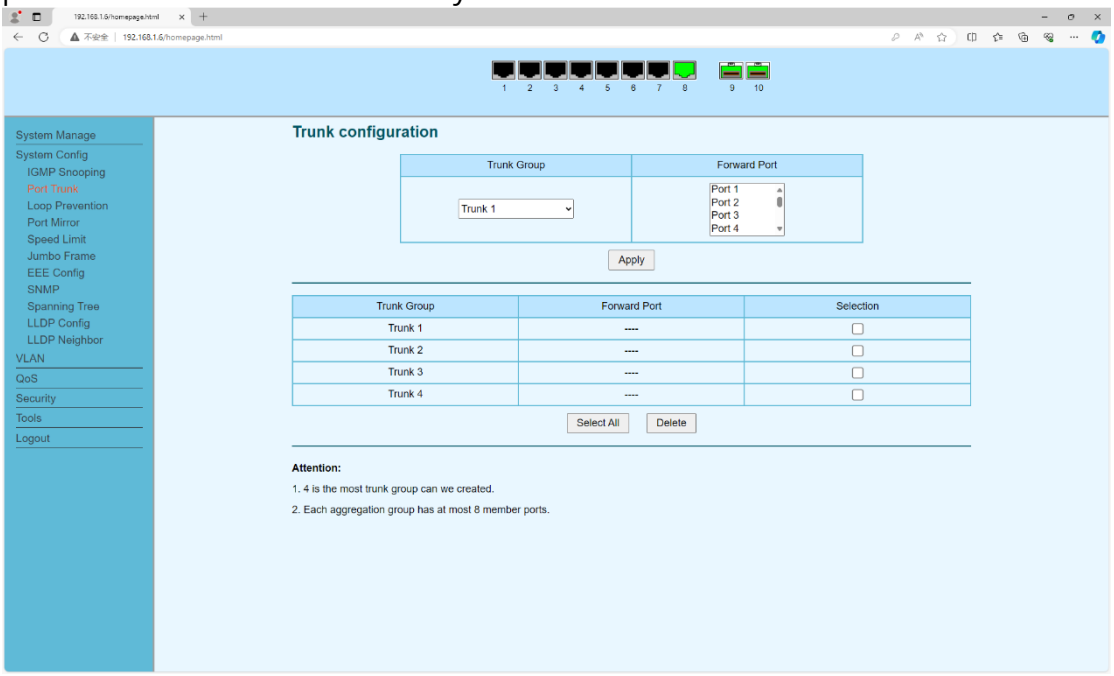


Item	Description	Notes
IGMP Snooping	Enable/Disable	Default: Disable
IGMP Fast-leave	Enable/Disable	Default: Disable Notification control is achieved through IGMP Leave messages. By default, the switch will immediately leave the multicast group upon receiving the Leave message and stop forwarding multicast

		traffic to this port (note: when enabled, it may increase the processing burden on the switch in large-scale networks)
IGMP Report Suppression	Enable/Disable	Default: Disable IGMP Report suppression is a network optimization mechanism that reduces unnecessary IGMP report messages in the network, suppresses duplicate IGMP reports, lowers network load, and improves efficiency. It is mainly applicable when multiple hosts join the same multicast group and send the same IGMP report messages.
VLAN ID		
IGMP Querier Status	Enable/Disable	Default: Disable After enabling, you can check that the query group messages are sent regularly to 224.0.0.1 to query whether any hosts on the subnet need to receive any multicast messages.
IGMP Querier Election	Enable/Disable	Default: Disable
IGMP Querier Version	V2	
IGMP Querier Source Address		When the queryer status is enabled, the source address will be displayed here.

2.2 System Configuration-Port Trunk

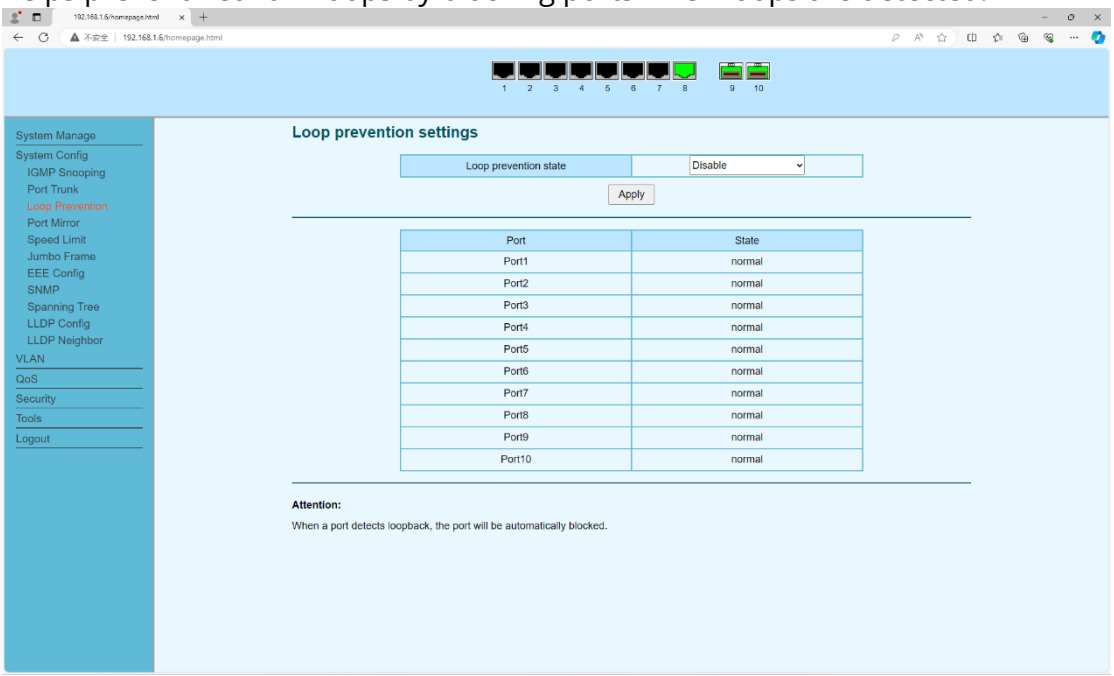
Port Trunk is a technology that combines multiple physical ports into a single logical link through software configuration. It is mainly used to increase the bandwidth between switches and network nodes, providing higher transmission performance and link redundancy.



Item	Description	Notes
Trunk Group	Trunk 1,2,3,4	Supports up to 4 trunk groups
Forward Port	Select the corresponding physical port. At least two ports need to be involved. When making the selection, please hold down the 'Ctrl' key on the keyboard for multiple selection operations.	Each aggregation group has at most 8 member ports
Selection-Delete	Check the corresponding trunk groups that need to be deleted, and then click the "Delete" button.	

2.3 System Configuration-Loop Prevention

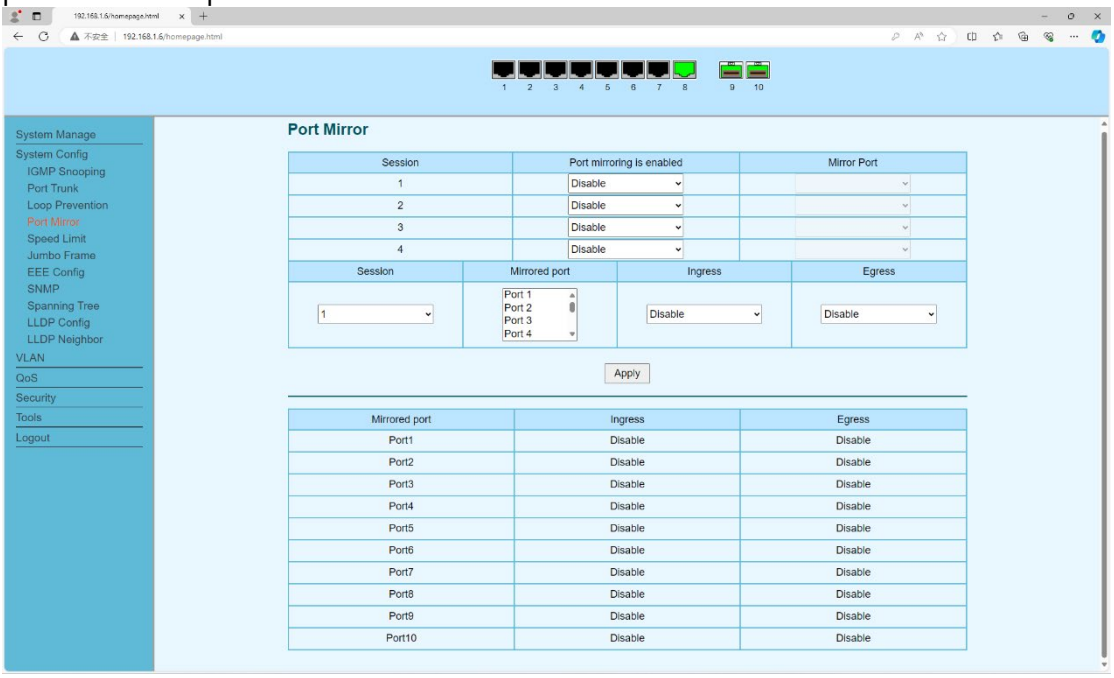
Loop prevention, also known as loopguard, is a feature in Layer 2 switching that helps prevent network loops by blocking ports when loops are detected.



Item	Description	Notes
Loop prevention state	Enable/Disable	Default:Disable To enable the loopback protection state, the RSTP function of the device needs to be disabled. After enabling the loop prevention function, the switch will continuously send broadcast messages to the corresponding port for detection. Once the corresponding device receives the loopback information, it will automatically block the loopback port.

2.4 System Configuration-Port Mirror

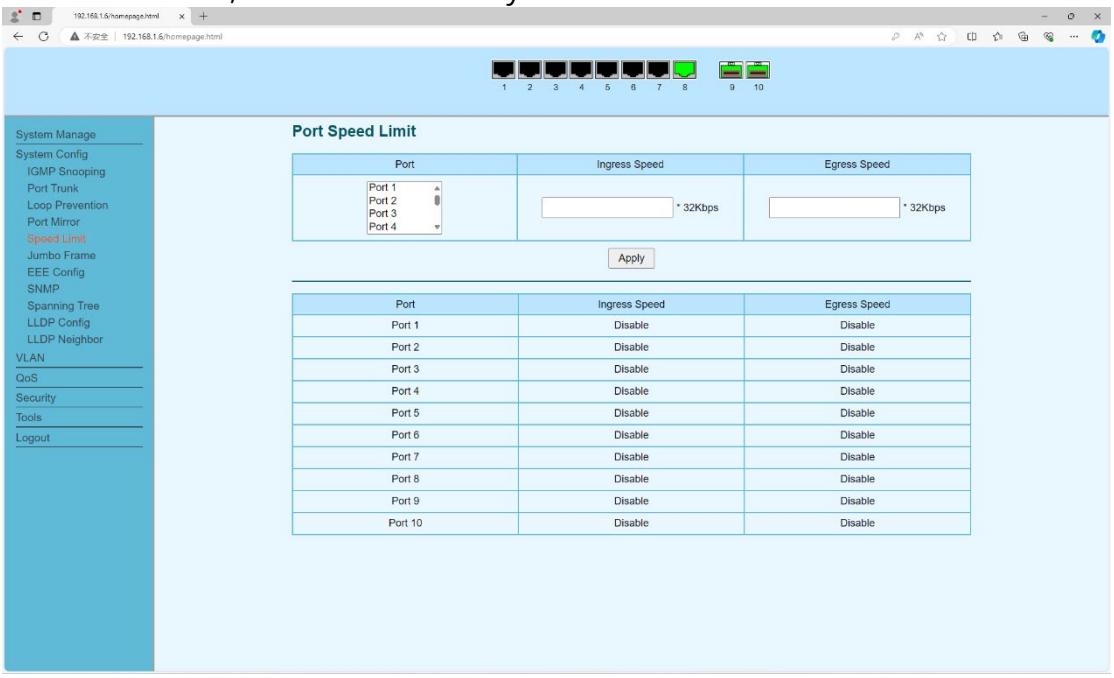
Port mirroring is a network function that duplicates traffic from one or more source ports or VLANs and forwards it to a designated destination port, also known as a monitoring port or analyzer port. This mirrored traffic can then be analyzed by network monitoring tools for troubleshooting, security analysis, or performance optimization.



Item	Description	Notes
Session		This device supports a maximum of 4 sets of mirrored ports.
Port Mirroring is enabled	Enable or disable the corresponding functions for the mirror session	
Mirror Port	Select the mirror port. Each mirror session can only have one mirror port.	
Mirrored Port	Select the mirrored ports. You can choose multiple ports. Use the 'Ctrl' key for multiple selections.	
Ingress	The ingress data of the mirrored port	
Egress	The egress data of the mirrored port	

2.5 System Configuration-Speed Limit

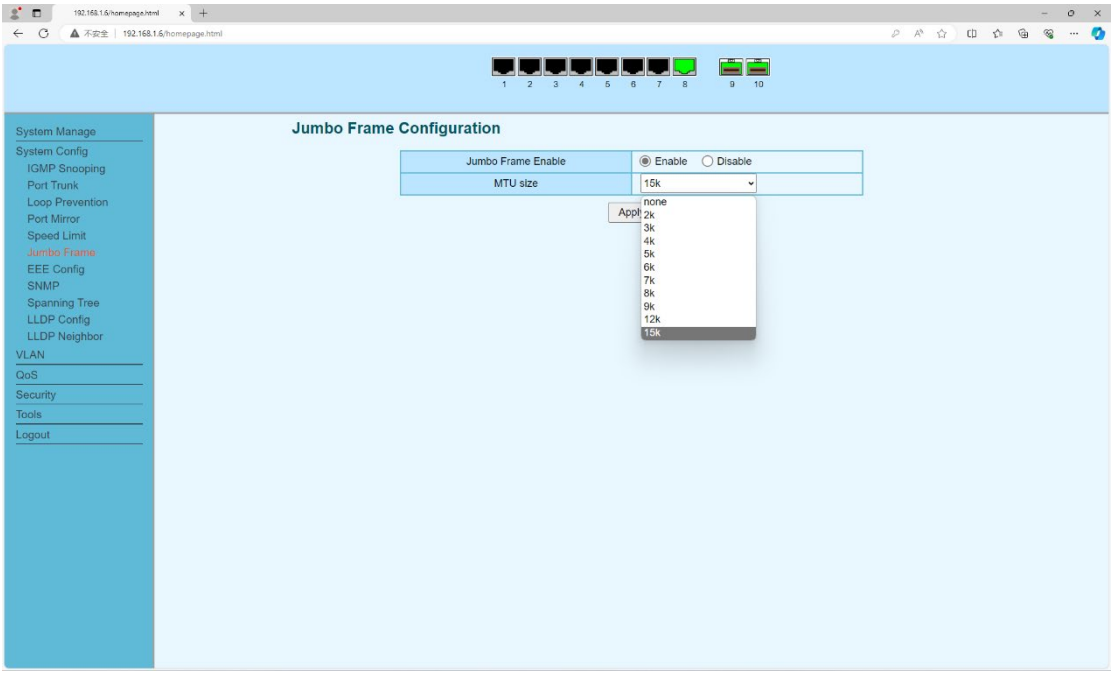
The port speed limit function mainly restricts the transmission speed of the port. It is used to balance network bandwidth, prevent malicious attacks, protect server resources, etc. It can effectively control the network traffic.



Item	Description	Notes
Port	Select the corresponding ports that require speed limit. You can use 'Ctrl' + the port number to select them in batches.	
Ingress Speed	Minimum 1*32kbps, maximum 10000*32kbps	
Egress Speed	Minimum 1*32kbps, maximum 10000*32kbps	

2.6 System Configuration-Jumbo Frame

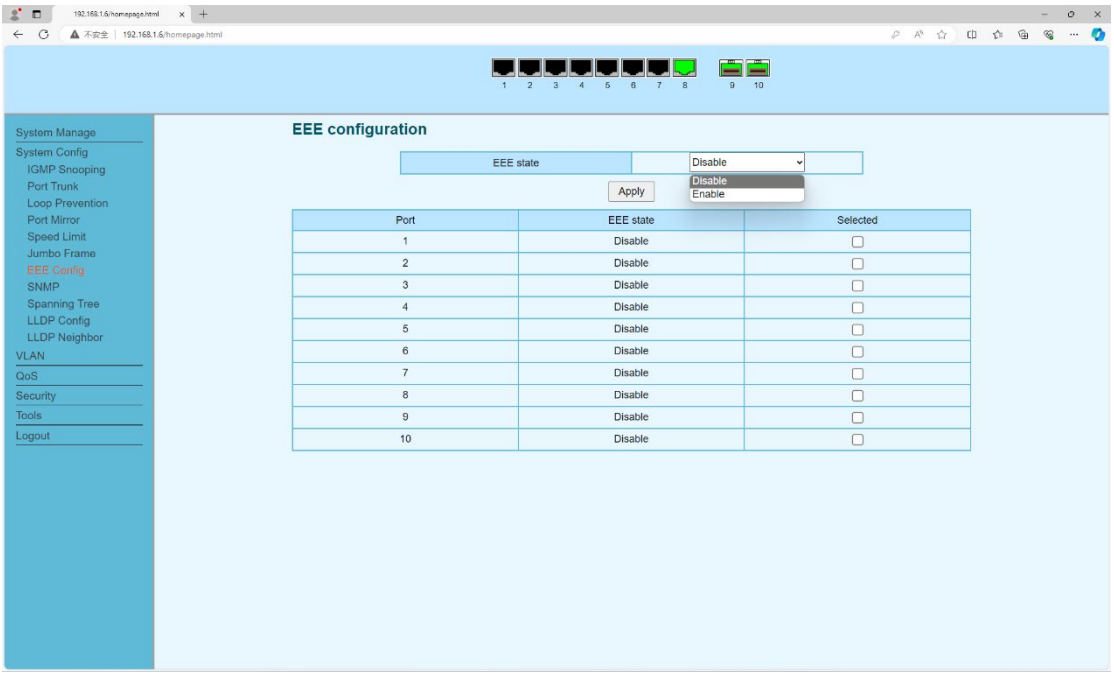
Jumbo frames are Ethernet frames that exceed the standard Maximum Transmission Unit (MTU) of 1500 bytes. They offer the potential to improve network performance by reducing the number of frames transmitted, leading to lower CPU load and potentially higher data throughput, especially in high-bandwidth environments like data centers.



Item	Description	Notes
Jumbo Frame Enable	Enable/Disable Default:Disable	Generally, the application of Jumbo frames requires that all devices on the link enable Jumbo frame mode and maintain the same MTU value; otherwise, it may lead to performance degradation or packet loss.
MTU size	Maximum 15K	

2.7 System Configuration-EEE Configuration

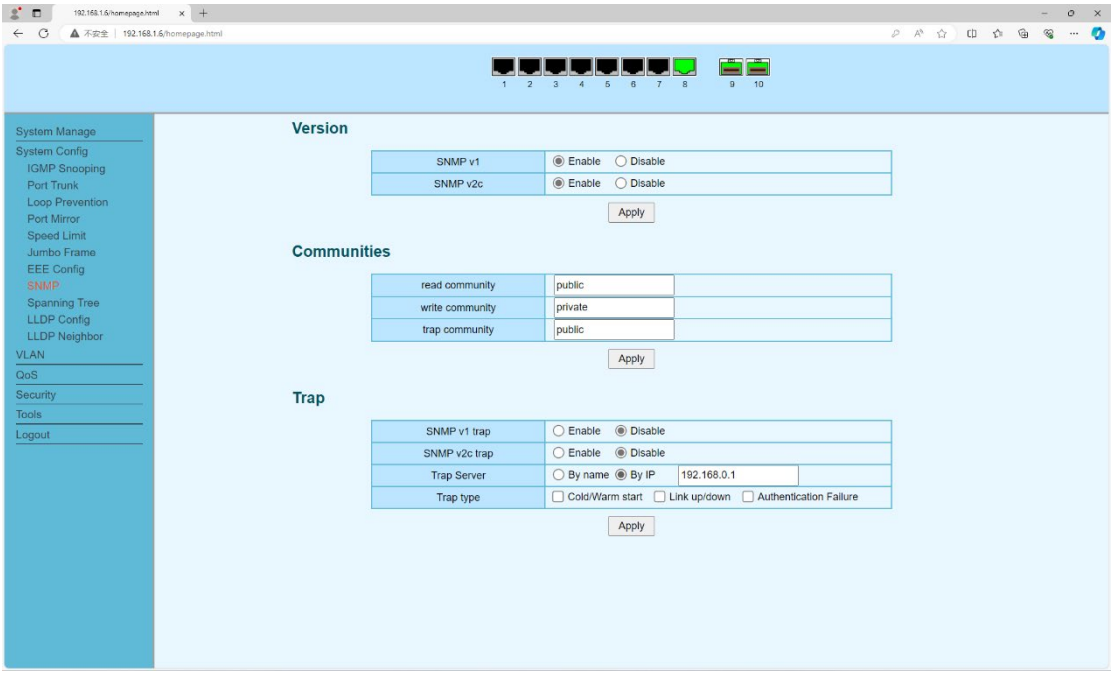
EEE (Energy Efficient Ethernet) is an IEEE 802.3az standard designed to reduce power consumption in Ethernet networks during idle periods. It's enabled at the interface level, and its configuration involves enabling it for the desired electrical interface.



Item	Description	Notes
EEE State	Enable/Disable	Default:Disable
Selected	Select the port and enable the EEE	

2.8 System Configuration-SNMP

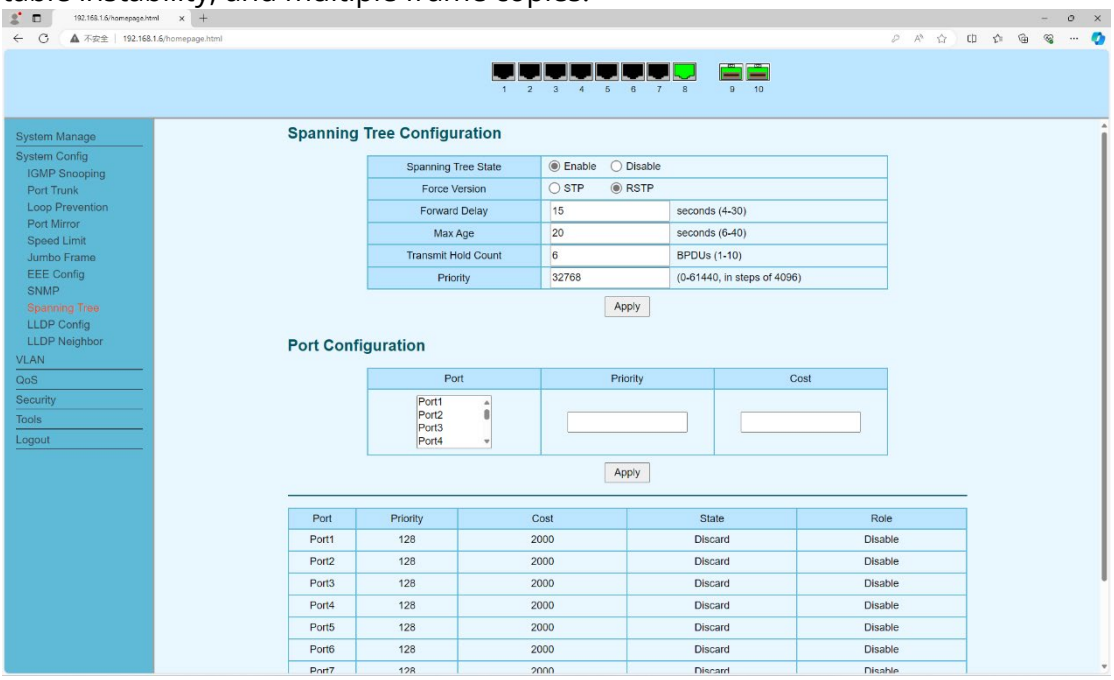
SNMP stands for Simple Network Management Protocol. It's an Internet Standard protocol used for managing and monitoring network-connected devices in IP networks.



Item	Description	Notes
Version	SNMPv1:Enable/Disable SNMPv2:Enable/Disable	
Communities	read community: public write community:private trap community:public	The authentication string used to verify the legitimacy of SNMP Trap messages can ensure that the trap messages are sent by trusted devices to the NMS management site.
Trap	SNMPv1 trap: Enable/Disable SNMPv2c trap: Enable/Disable Trap Server: By name or By IP Trap type: Cold/Warm start Link up/down Authentication Failure	

2.9 System Configuration-Spanning Tree Configuration

Spanning Tree Protocol (STP) is a crucial Layer 2 network protocol that prevents loops in a switched network by selectively blocking redundant paths. This ensures a loop-free logical topology, preventing broadcast storms, MAC address table instability, and multiple frame copies.

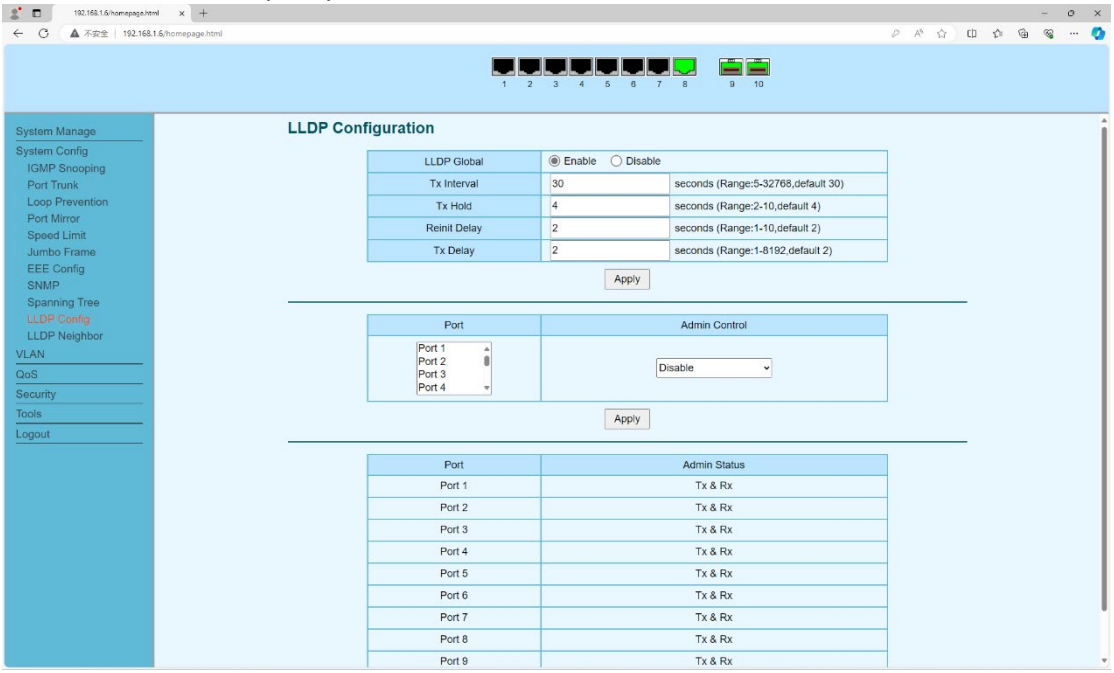


Item	Description	Notes
Spanning Tree State	Enable/Disable	
Force Version	STP/RSTP	
Forward Delay	4-30 seconds	It is a timer for controlling the switching of port states, ensuring that data forwarding is permitted only after the loop has been eliminated.
Max Age	6-40 seconds	The timer unit used to determine whether the configured BPDU message has timed out. It is mainly used for the timeout period of the blocked port. If no BPDU message is received within the specified time, a re-negotiation will occur. Secondly, it controls the network scale and prevents the BPDU message from being forwarded too far.

Transmit hold count	1-10 BPDUs	
Priority	0-61440, in steps of 4096	Default:32768
Port	Port 1 to Port 10	
Priority	Default:128, Priority:16	Port election decision parameters, used to elect the root port or designated port role on the switch. The lower the priority, the higher the priority. By default, the election is generally based on the port number.
Cost	Gigabit is 2000, 10 Gigabit is 200, the bandwidth is automatically calculated and no modification is required.	

2.10 System Configuration-LLDP Configuration

LLDP (Link Layer Discovery Protocol) is an industry-standard, vendor-neutral Layer 2 protocol used by network devices to advertise their identity, capabilities, and other relevant information to directly connected neighboring devices on a local area network (LAN).

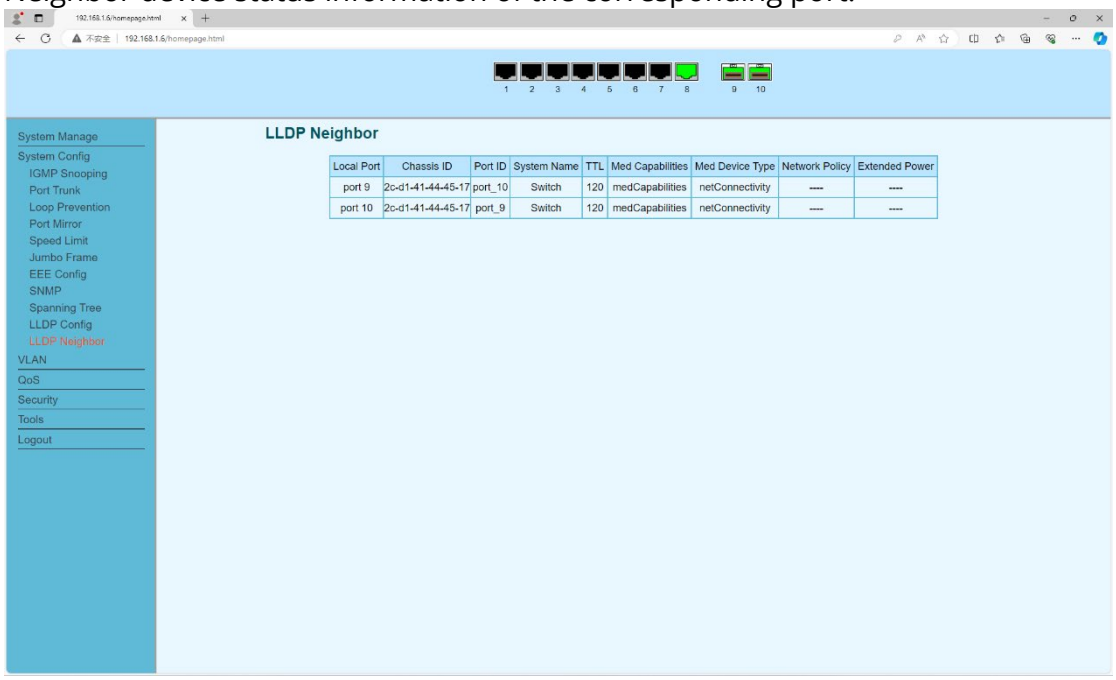


Item	Description	Notes
LLDP Global	Enable/Disable	Default: Enable
Tx Interval	5-32768 seconds	Default:30 second The sending interval time of the LLDPDU message encapsulating TLV

Tx hold	2-10 seconds	Default:4 seconds The duration for which the device information remains valid in the neighboring devices
Reinit Delay	1-10 seconds	Default:2 seconds The delay time from the enabled state to the re-enabled state, to avoid topological connection oscillation of neighboring devices caused by frequent changes in the LLDP protocol state.
Tx Delay	1-8192 seconds	Default: 2 senconds The minimum delay time for sending LLDP messages to neighboring devices when the device status changes frequently
Admin Control		After enabling the LLDP function, all default ports remain in the management and control state, capable of sending and receiving LLDP messages. This configuration allows for the disabling of LLDP sending or receiving functions.

2.11 System Configuration-LLDP Neighbor

Neighbor device status information of the corresponding port.



Chapter 3 VLAN

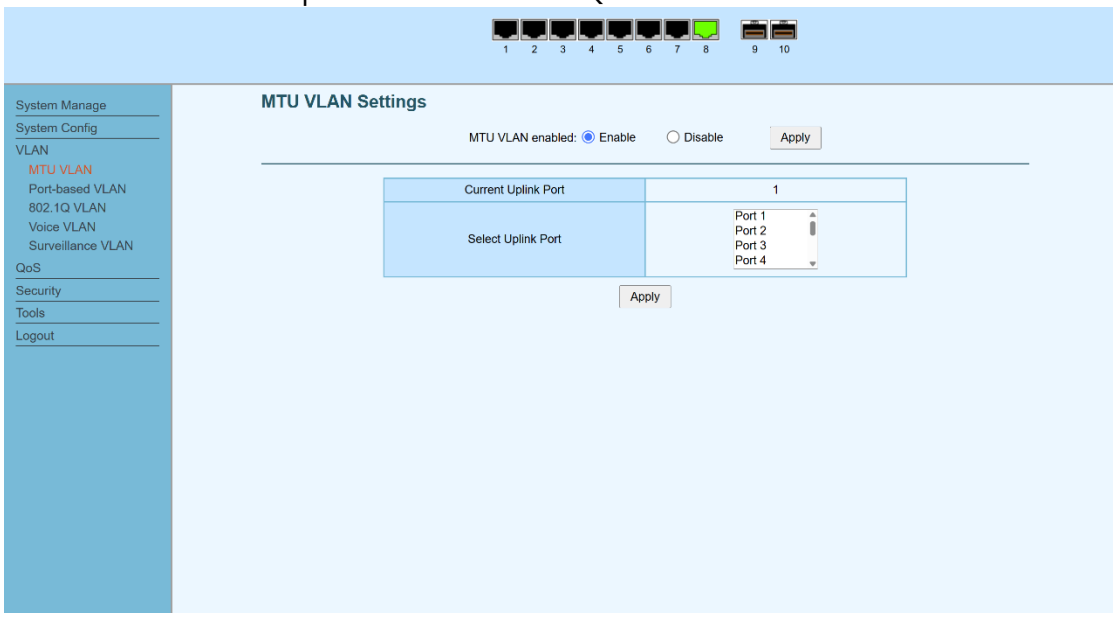
This chapter describes the VLAN functions in detail, including but not limit to the following:

- Port-based VLAN
- 802.1Q VLAN
- Voice VLAN
- Surveillance VLAN

3. VLAN

3.1 VLAN-MTU VLAN Settings

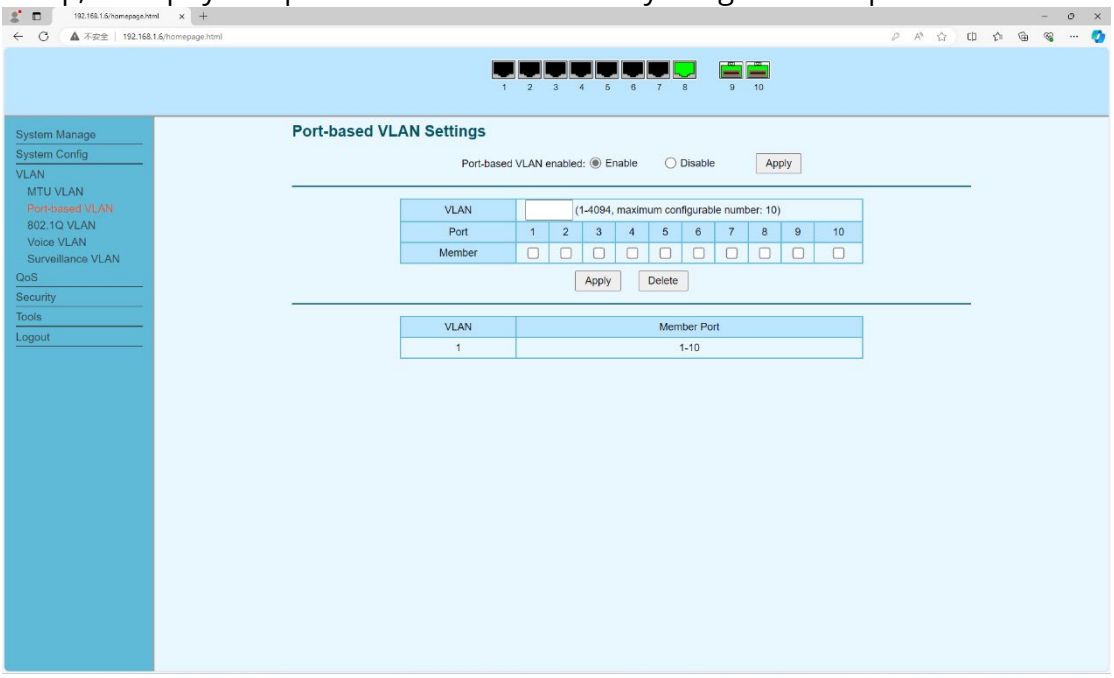
It can be understood as the port isolation function. Set an uplink port. This port can maintain effective communication with all the ports below, but the other ports below are isolated from each other. Note that after enabling the MTU port, the functions such as port VLAN and 802.1Q VLAN are all disabled.



Item	Description	Notes
MTU VLAN	Enable/Disable	Default: Disable
Current Uplink Port	After a port is selected, that port remains in communication with other ports, while the other ports are isolated from each other and do not communicate with one another.	

3.2 VLAN-Port-based VLAN

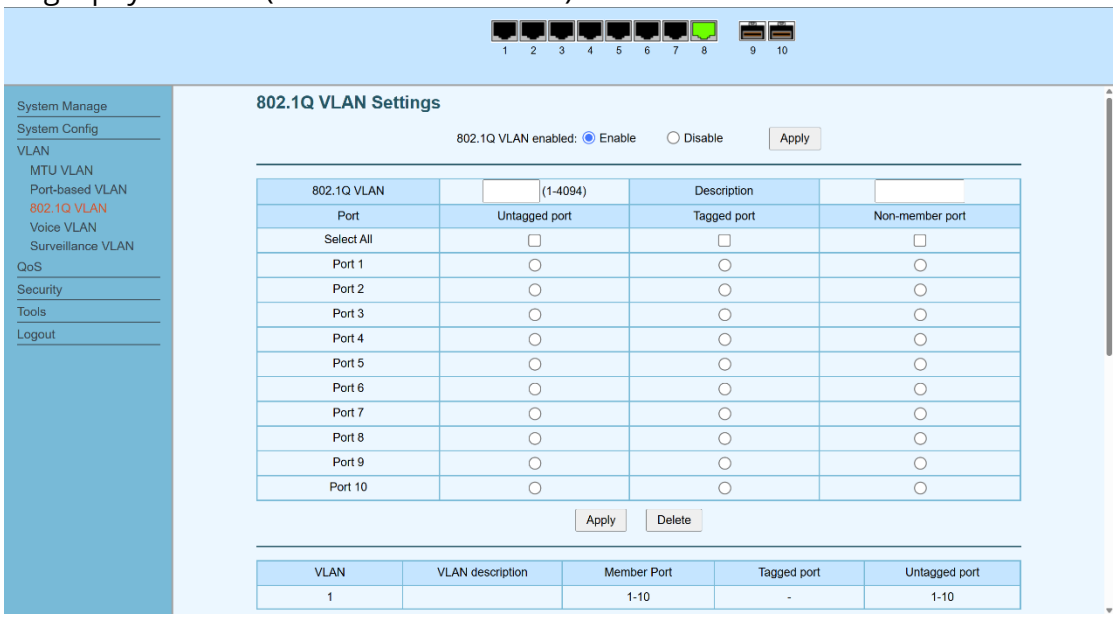
Port-based VLANs are the simplest and most common method for implementing Virtual Local Area Networks (VLANs) on a network switch. In a port-based VLAN setup, each physical port on a switch is statically assigned to a specific VLAN.



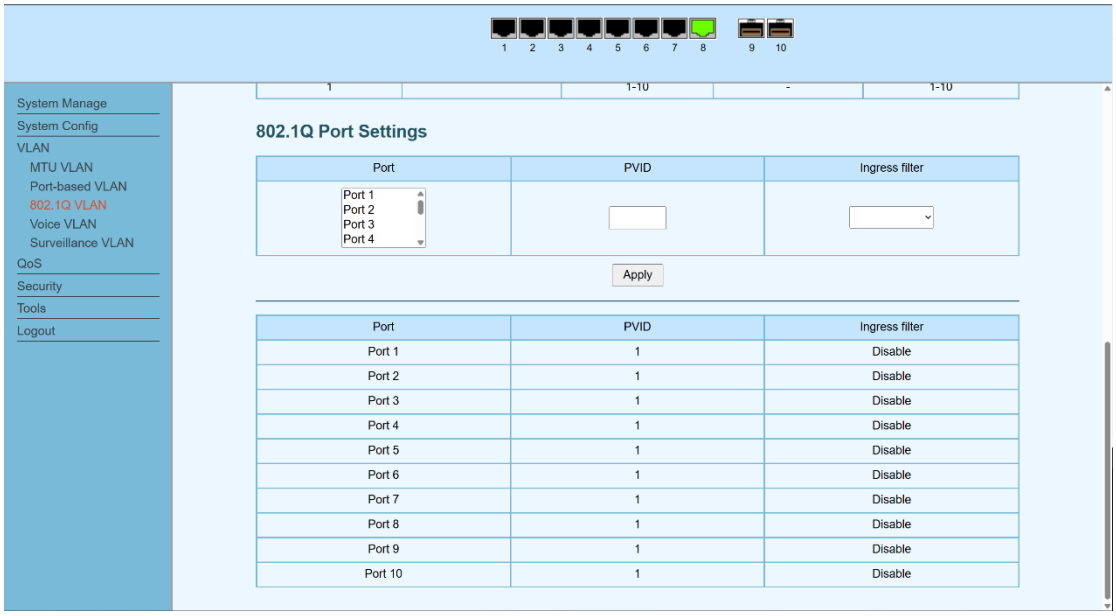
Item	Description	Notes
Port-based VLAN enabled	Enable/Disable	Default: Enable
VLAN	1-4094, maximum configuration number:10	
Member	Select the corresponding ports based on the corresponding VLAN.	

3.3 VLAN-802.1Q VLAN Settings

802.1Q VLAN settings refer to the configuration parameters for implementing VLANs using the IEEE 802.1Q standard, which is the most widely adopted method for VLAN tagging in Ethernet networks. This standard defines how VLAN information is inserted into Ethernet frames to allow multiple VLANs to share a single physical link (known as a trunk link).



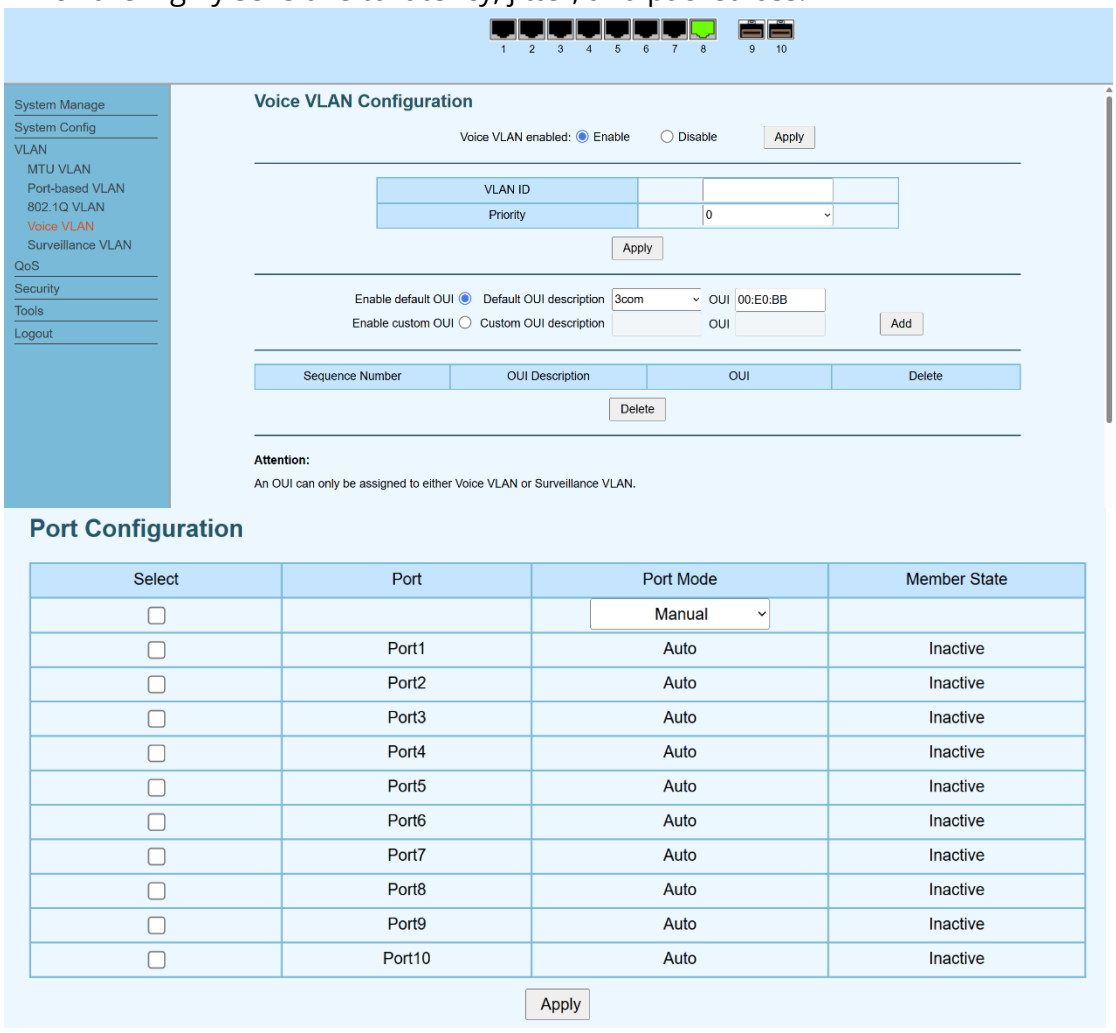
Item	Description	Notes
802.1Q VLAN enabled	Enable/Disable	Default:Disable
802.1Q VLAN ID	1-4094	
Description	Optional	
Port	For the selected port, you can choose Untagged port, Tagged port or non-member port.	



Item	Description	Notes
Port	Select the corresponding port according to the specifications in the 802.1Q VLAN settings.	
PVID	Fill in the corresponding VLAN PVID number according to the rules set in 802.1Q VLAN.	
Ingress Filter	Enable/Disable	

3.4 VLAN-Voice VLAN Configuration

A Voice VLAN is a specialized Virtual Local Area Network (VLAN) specifically dedicated to carrying Voice over IP (VoIP) traffic from IP phones. Its primary purpose is to ensure the Quality of Service (QoS) for voice communications, which are highly sensitive to latency, jitter, and packet loss.

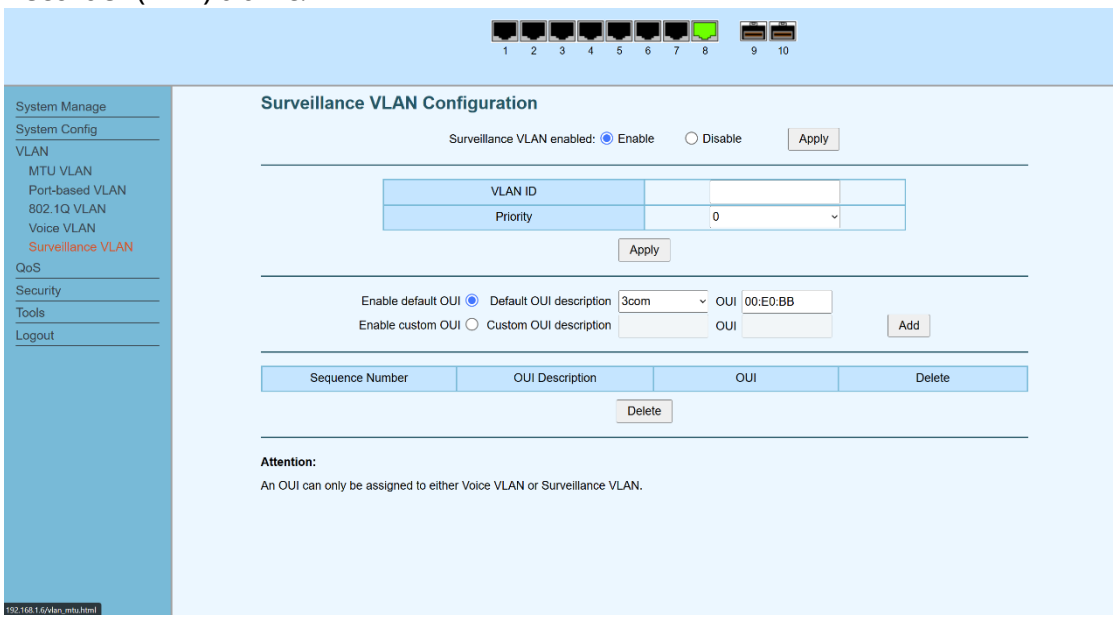


Item	Description	Notes
Voice VLAN enabled	Enable/Disable	Default: Disable
VLAN ID	After determining which VLAN the voice traffic will use based on the 802.1Q VLAN	

	configuration, proceed to fill in the details.
Priority	Different voice VLANs can have different priorities. You can fill in the options as needed. The higher the number, the higher the priority.
OUI	According to the inquiry by the IP phone manufacturer, a fixed unique number can be used and customized.
Port Configuration	After checking the corresponding IP phone port, select either manual or automatic.

3.5 VLAN-Surveillance VLAN Configuration

A Surveillance VLAN (also known as a Video VLAN or sometimes Auto Surveillance VLAN in some vendor implementations) is a dedicated Virtual Local Area Network specifically designed to carry IP camera and Network Video Recorder (NVR) traffic.



Item	Description	Notes
Surveillance VLAN enabled	Enable/Disable	Default: Disable
VLAN ID	After determining which VLAN the video traffic will use based on the 802.1Q VLAN configuration, proceed to fill in the details.	
Priority	Different Surveillance VLANs can have different priorities.	

	You can fill in the options as needed. The higher the number, the higher the priority.
OUI	According to the inquiry by the Video Camera manufacturer, a fixed unique number can be used and customized.

Chapter 4 QoS

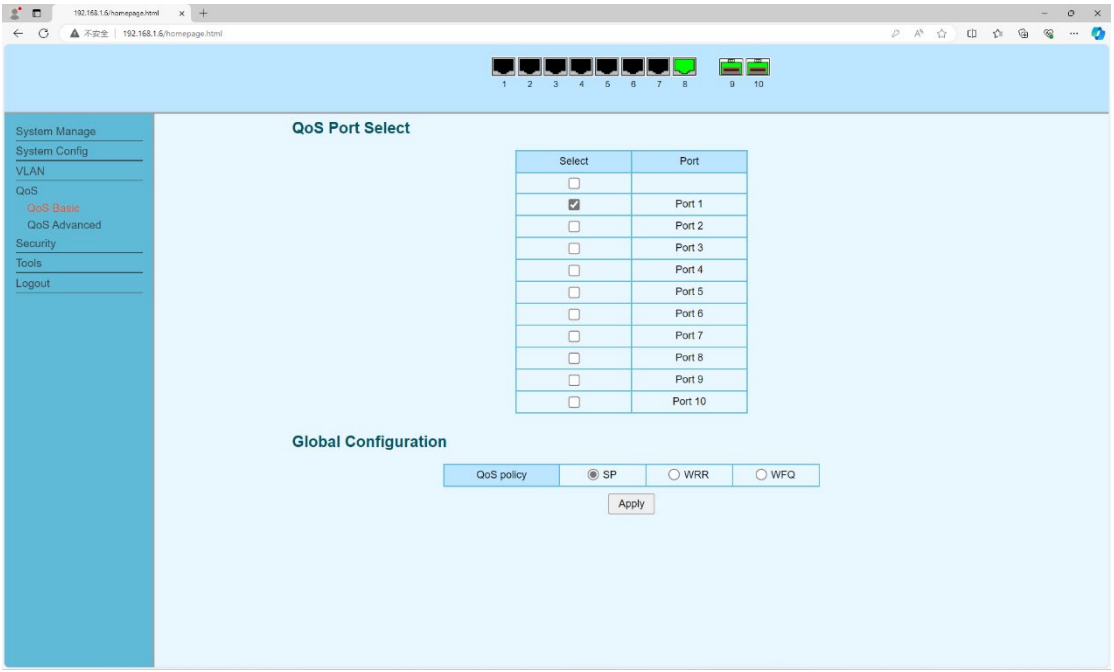
This chapter describes the QoS functions in detail, including but not limit to the following:

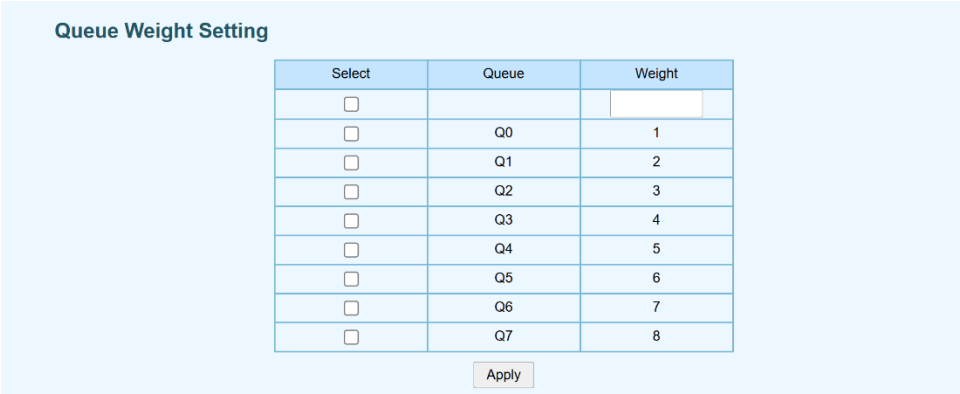
- QoS Basic
- QoS Advanced

4. QoS

4.1 QoS-QoS Basic

QoS (Quality of Service) is a set of technologies and mechanisms used in computer networks to manage and prioritize network traffic, ensuring that critical applications and services receive the necessary bandwidth, low latency, minimal jitter, and reduced packet loss. In essence, QoS allows network administrators to differentiate between various types of traffic and apply different levels of service based on their importance and sensitivity to network conditions.

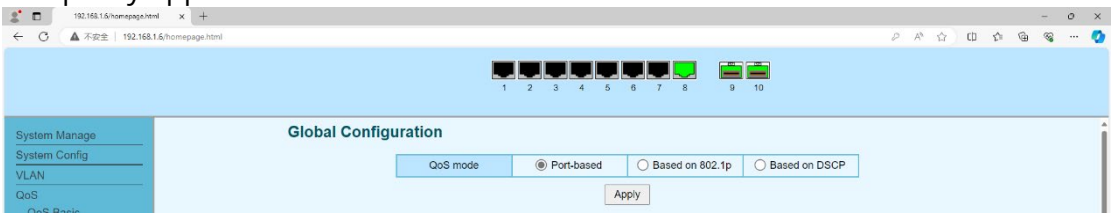


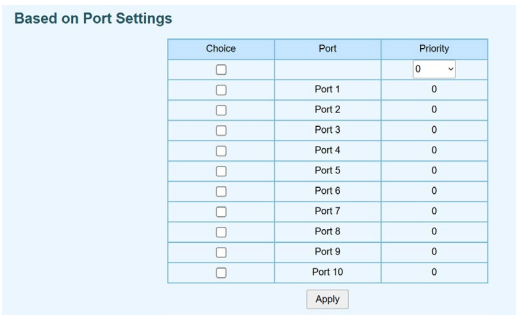


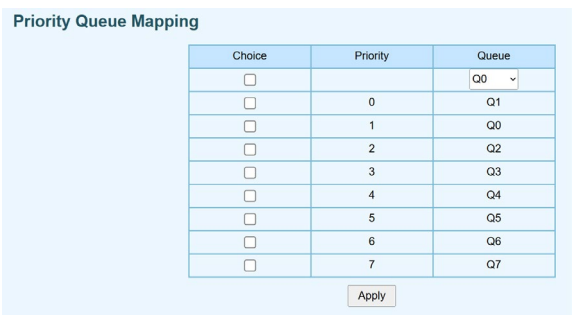
Item	Description	Notes
QoS Port Select	After checking the port, the corresponding QoS policy will be activated.	
QoS Policy	Optional SP absolute priority strategy, or WRR (Weighted Round Robin) or WFQ (Weighted Fair Queueing) priority polling strategy	
Queue Weight Setting	Only effective for WRR or WFQ. Configure the weight ratio of the priority queues.	

4.2 QoS-QoS Advanced

The QoS advanced configuration function is mainly used for the global QoS configuration of the device, including the adoption of three priority methods: port QoS, 802.1p, and DSCP. Among them, the port priority is the default priority method of the device. When the packet does not carry any other priority mark, such as a packet without VLAN Tag, it adopts the port priority. The 802.1p priority is located in the TCI field of the Layer 2 VLAN tag, using 3 bits, with a range of 0-7, and is used to identify the priority of frames in the Layer 2 network. The DSCP priority belongs to the three-layer marking and is located in the TOS field of IPv4 or the Traffic Class field of IPv6, using 6 bits, with a range of 0-63. The use of Differentiated Services Code Point (DSCP) mainly serves for traffic classification and policy application.







Global Configuration

QoS mode	Port-based	Based on 802.1p	Based on DSCP

Apply

Priority Queue Mapping

Choice	Priority	Queue
☐		Q0
☐	0	Q1
☐	1	Q0
☐	2	Q2
☐	3	Q3
☐	4	Q4
☐	5	Q5
☐	6	Q6
☐	7	Q7

Apply

Global Configuration

QoS mode	Port-based	Based on 802.1p	Based on DSCP

Apply

Based on DSCP Settings

Choice	DSCP	Priority
☐		0
☐	0	0
☐	1	0
☐	2	0
☐	3	0
☐	4	0
☐	5	0
☐	6	0
☐	7	0
☐	8	0
☐	9	0
☐	10	0
☐	11	0
☐	12	0
☐	13	0
☐	14	0
☐	15	0
☐	16	0
☐	17	0

Item	Description	Notes
QoS Mode	Port-based Based on 802.1p Based on DSCP	
Based on Port Settings-Priority	Port priority setting	
Priority Queue Mapping	The priority and queue are mapped, and generally no changes are made.	
Based on DSCP setting-priority	Setting priorities in the DSCP mode	

Chapter 5 Security

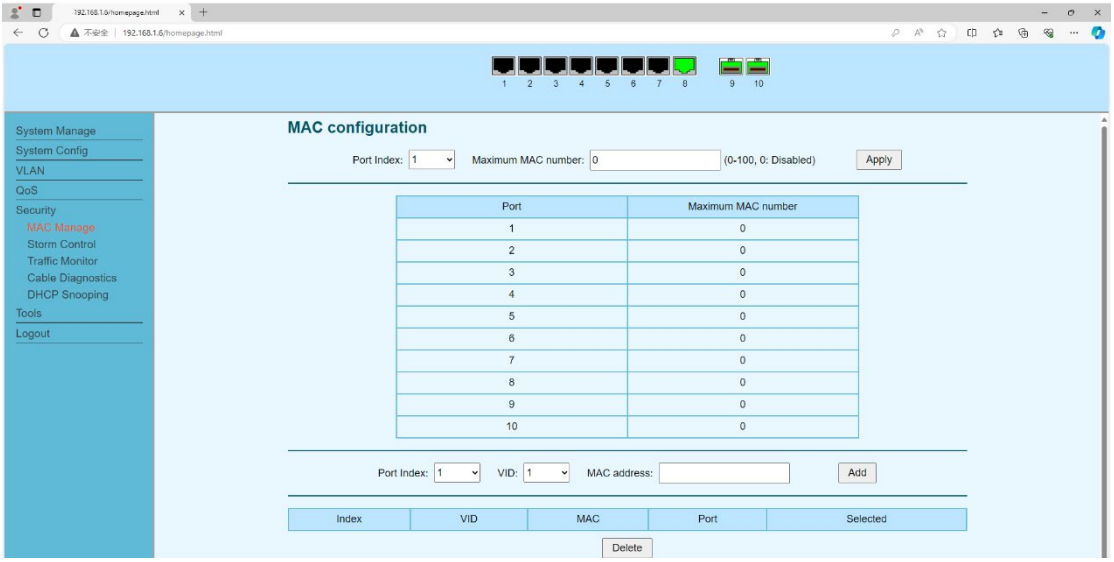
This chapter describes the Security functions in detail, including but not limit to the following:

- MAC Manage
- Storm Control
- DHCP Snooping

5. Security

5.1 Security – MAC Manage

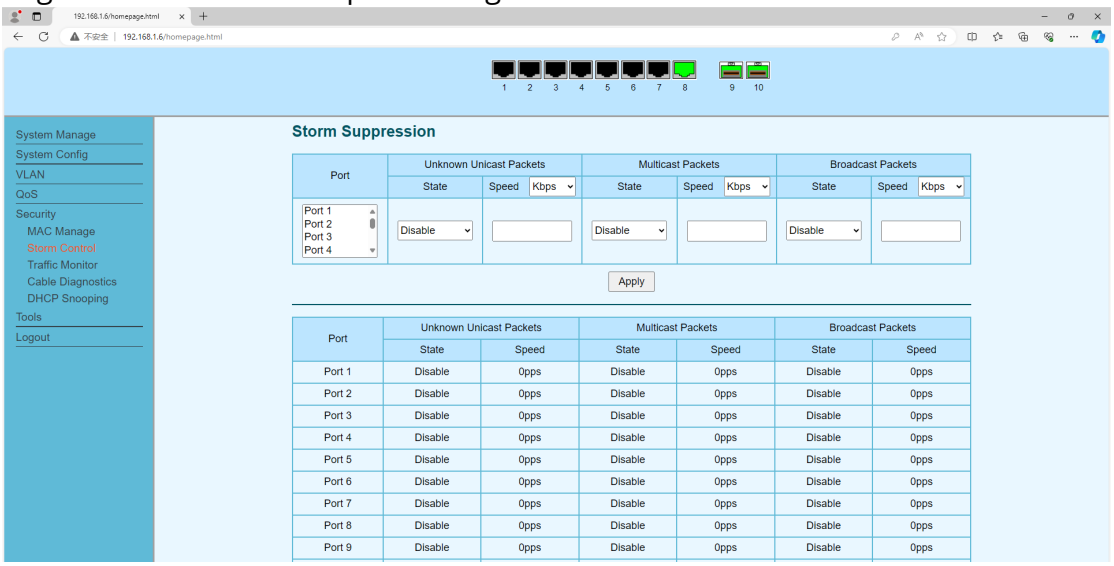
After setting the maximum number of MAC addresses for the corresponding port, the device forwards only the manually bound static MAC addresses. It will only dynamically learn other MAC addresses when the number of bound static MAC addresses is less than the maximum number.



Item	Description	Notes
MAC Configuration	select the corresponding port index to impose a limit on the maximum MAC address learning.	
Port Index, VID, MAC address	Fixed static MAC addresses for corresponding ports can be set and manually added.	

5.2 Security – Storm Control

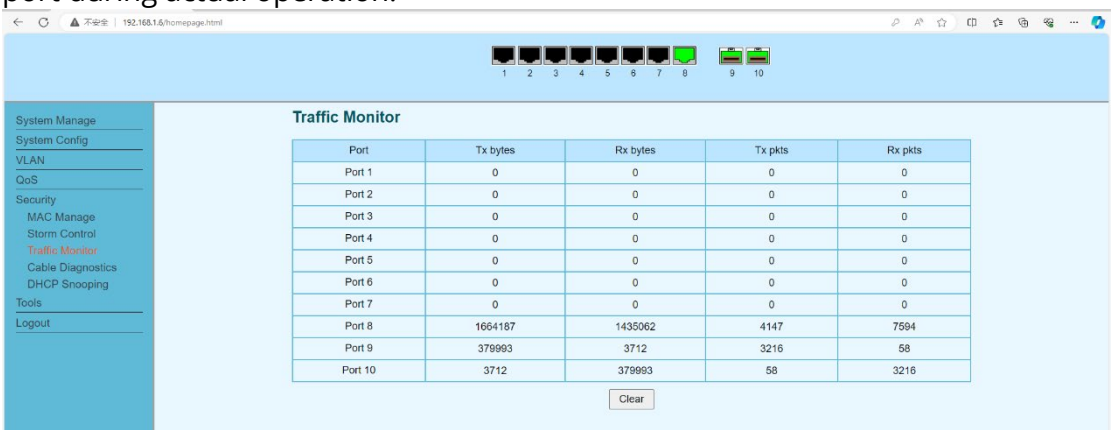
Storm control is a crucial network security and performance feature implemented on network switches to prevent traffic storms. A traffic storm occurs when an excessive amount of a specific type of traffic (broadcast, multicast, or unknown unicast) floods a LAN, consuming excessive bandwidth, overwhelming network devices, and potentially leading to network performance degradation or even complete outages.



Item	Description	Notes
Port	Unknown Unicast Packets Multicast Packets Broadcast Packets	Select the corresponding ports that need to be operated on. Holding down the 'Ctrl' key allows for batch selection.
State	Default:Disable	
Speed	Kbps/pps	

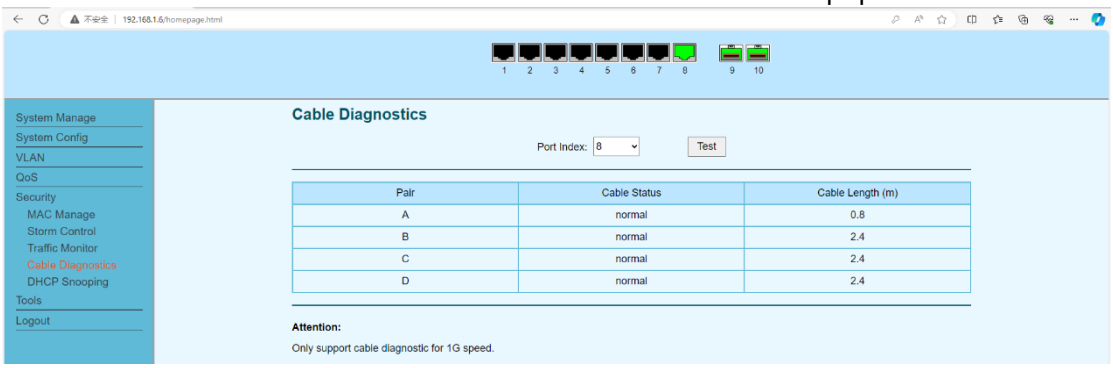
5.3 Security – Traffic Monitor

The traffic monitoring function mainly provides the cumulative values of the number of bytes sent/received and the number of packets sent/received by each port during actual operation.



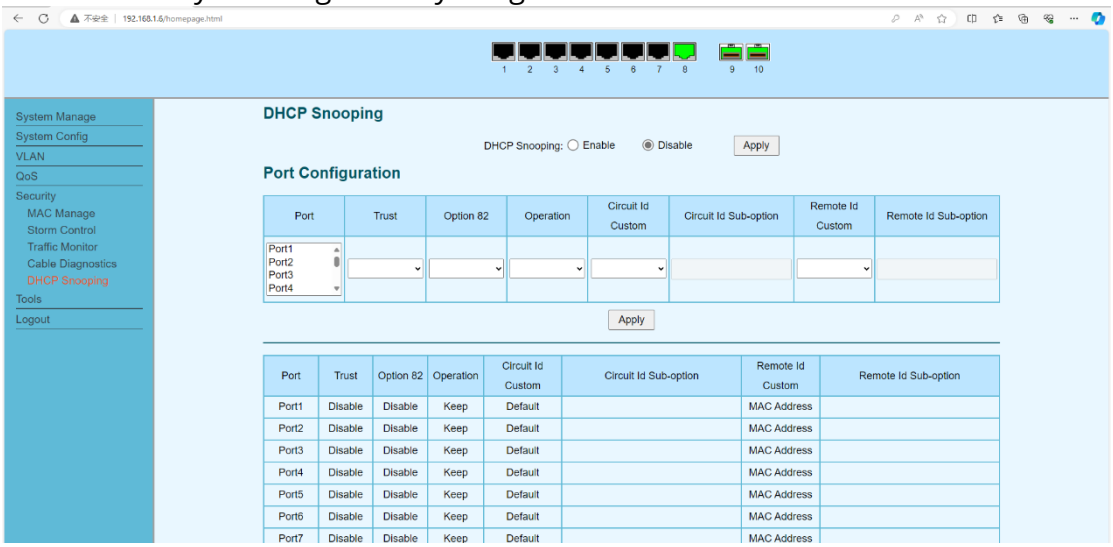
5.4 Security – Cable Diagnostics

Provide the cable status of each electrical interface on the equipment



5.5 Security – DHCP Snooping

DHCP Snooping is a Layer 2 security feature implemented on network switches to protect against unauthorized (rogue) DHCP servers and various DHCP-related attacks. It acts as a firewall for DHCP messages, ensuring that only legitimate DHCP servers can assign IP addresses to clients and that clients only use IP addresses they were legitimately assigned.



Item	Description	Notes
DHCP Snooping	Default: Disable	
Port	Select the corresponding listening port	
Trust	Select the configuration for Snooping port and enable trust.	
Option 82	The enhanced service option is mainly used for the relay proxy function.	

Chapter 6 Tools

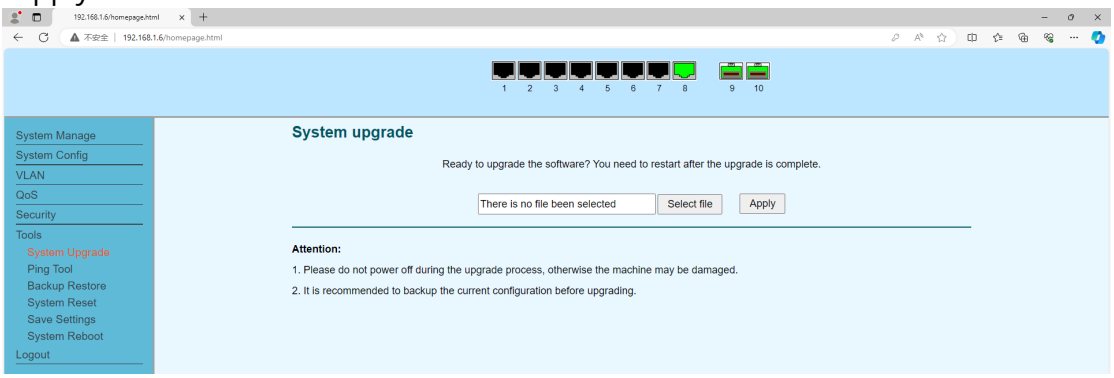
This chapter describes the tools functions in detail, including but not limit to the following:

- System Upgrade
- Ping Tool
- Backup Restore
- System Reset

6. Tools

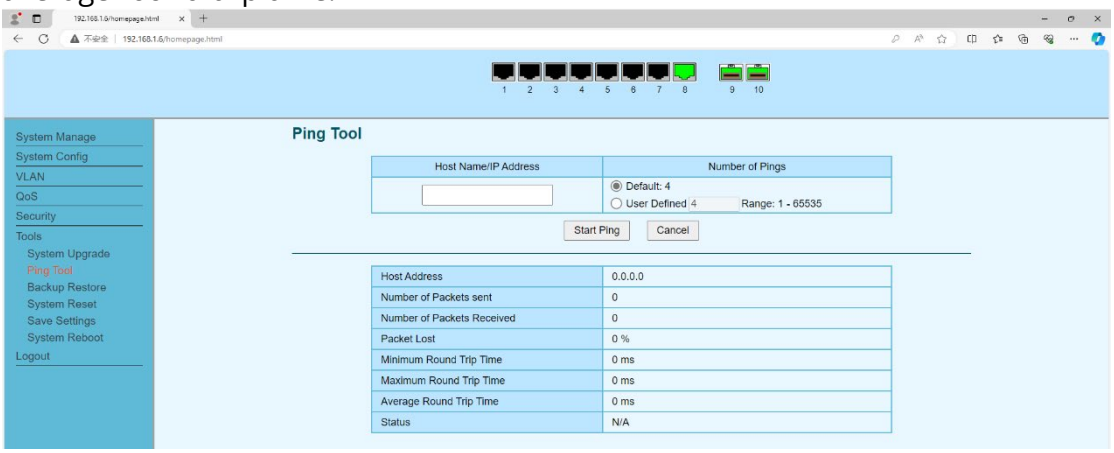
6.1 Tools – System Upgrade

The equipment is equipped with a system upgrade function. When a system upgrade operation is required, please use the correct upgrade file provided by our company to carry out the upgrade. After selecting the file, simply click "Apply".



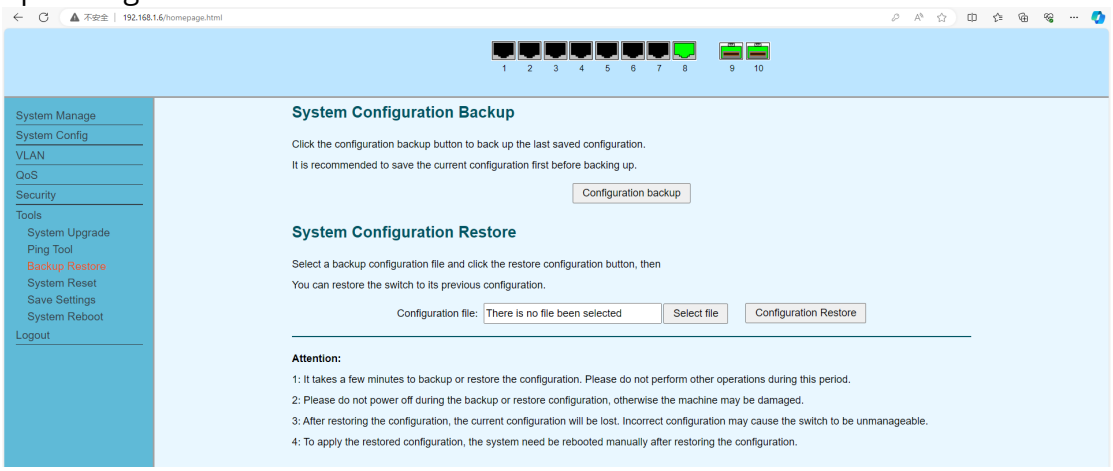
6.2 Tools – Ping Tool

The equipment integrates Ping application commands based on this, and can send request messages and display response message situations via the ICMP protocol to achieve the purpose of testing whether the target site is reachable and obtaining related status information such as connection packet loss rate and average round-trip time.



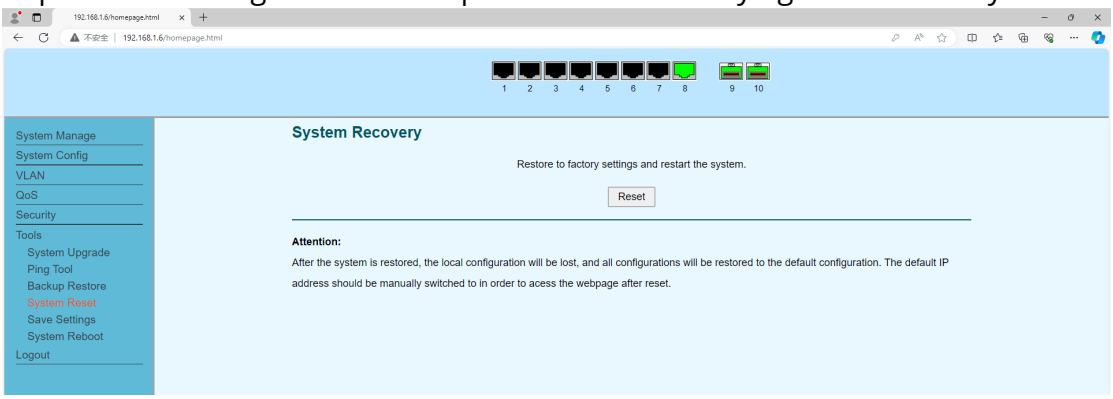
6.3 Tools – Backup Restore

The device provides the functions of downloading configuration files and uploading configuration files. Through these functions, users can perform operations such as saving configurations, modifying configurations and then uploading them.



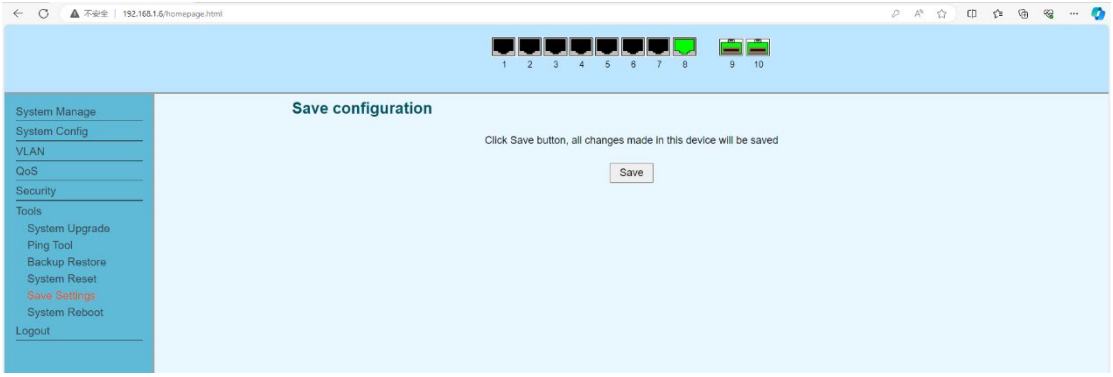
6.4 Tools – System Reset

Restore to factory default configuration operation. Please proceed with caution to avoid any unnecessary configuration loss or other issues. It is recommended to perform a configuration save operation before carrying out the factory reset.



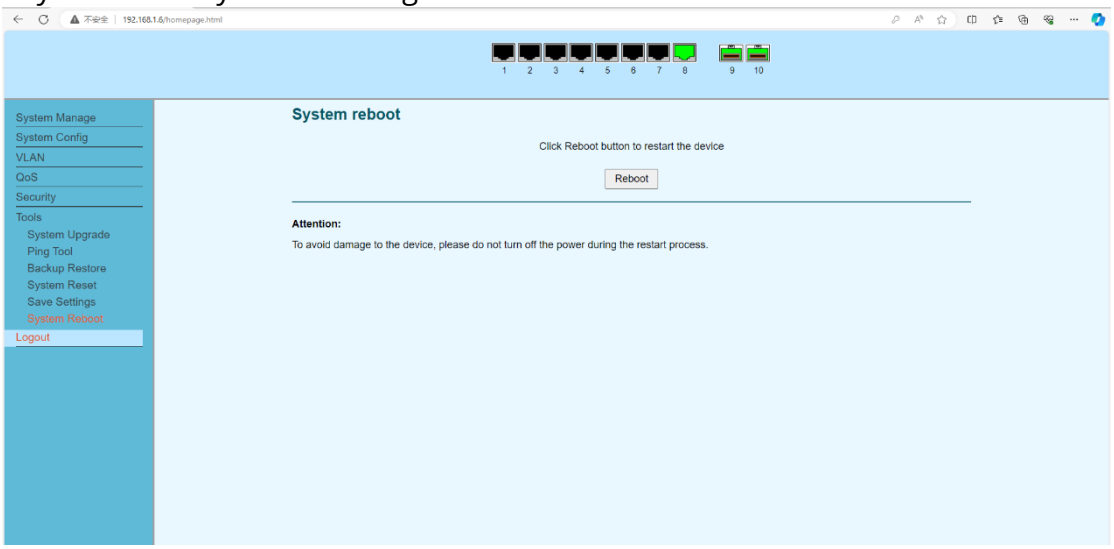
6.5 Tools – Save Settings

All configuration modifications for the functions must be completed before the device is powered off, and a configuration save operation needs to be performed at that time.



6.6 Tools – System Reboot

Device restart function. Please note that before performing the device restart operation, please ensure that the device configuration has been saved to avoid any unnecessary loss of configuration.



Chapter 7 Console

This switch is equipped with a Console interface, which provides simple maintenance and query functions for the switch. It is mainly applied in the following scenarios:If the IP address of the switch is forgotten, it can be queried through the Console port;

As shown in the figure below:

```
Username:admin
Password:******
Login successful. Welcome!

Switch> help
help: Lists all the registered commands
debug: enter debug shell mode
tftp-fw-upgrade <server-ip> <firmware-name>: upgrade image using TFTP
reset: reset system

Switch>
```

```
debug#help
help: Lists all the registered commands
memrl address: read 4 bytes from register or memory at the address
memwl address value: write 4-byte value to register or memory at the address
ip_get: Show IP address
sysmac_get: Show System mac
model_get: Show Model string
```

Item	Description	Notes
Switch>help	List all the configurable commands	
Switch>debug	Debugging commands can offer IP address query and MAC address query functions.	
Switch>tftp-fw-upgrade	system upgrade	
Switch>reset	Soft restart command	
Debug>help	List all the configurable commands	

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