

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.

Copyright©2025 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, 2025

CONTENTS

Revision History	5
Chapter 1 System Configurations	6
1. About Web-GUI Management.....	6
1.1 Preparing for Web Management	6
1.2 System Manage.....	7
1.2.1 System Information	7
1.2.2 System Manage-IP Settings	7
1.2.3 System Manage – Account Settings.....	8
1.2.4 System Manage-Port configuration.....	9
1.2.5 System Manage-Optical Module States	10
Chapter 2 System Configurations	11
2. System Configuration	11
2.1 System Configuration-IGMP Snooping	11
2.2 System Configuration-Port Trunk.....	13
2.3 System Configuration-Loop Prevention.....	14
2.4 System Configuration-Port Mirror.....	15
2.5 System Configuration-Speed Limit.....	16
2.6 System Configuration-Jumbo Frame.....	17
2.7 System Configuration-EEE Configuration	18
2.8 System Configuration-SNMP	19
2.9 System Configuration-Spanning Tree Configuration.....	20
2.10 System Configuration-LLDP Configuration.....	21
2.11 System Configuration-LLDP Neighbor	22
Chapter 3 VLAN.....	23
3. VLAN.....	23
3.1 VLAN-MTU VLAN Settings.....	23
3.2 VLAN-Port-based VLAN.....	24
3.3 VLAN-802.1Q VLAN Settings	25
3.4 VLAN-Voice VLAN Configuration.....	26
.....	26
3.5 VLAN-Surveillance VLAN Configuration	27
Chapter 4 QoS.....	29

4. QoS.....	29
4.1 QoS-QoS Basic.....	29
4.2 QoS-QoS Advanced.....	30
Chapter 5 Security	33
5. Security	33
5.1 Security – MAC Manage.....	33
5.2 Security – Storm Control	34
5.3 Security – Traffic Monitor	34
5.4 Security – Cable Diagnostics	35
5.5 Security – DHCP Snooping	35
Chapter 6 Tools.....	36
6. Tools.....	36
6.1 Tools – System Upgrade.....	36
6.2 Tools – Ping Tool	36
6.3 Tools – Backup Restore	37
6.4 Tools – System Reset	37
6.5 Tools – Save Settings	37
6.6 Tools – System Reboot	38
Chapter 7 Console	38

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.

The screenshot shows the 'System Information' page. At the top, there are 10 port status icons (1-10). On the left is a navigation menu with items like 'System Manage', 'System info', 'IP Settings', 'Account Settings', 'Port Settings', 'Optical Module Status', 'System Config', 'VLAN', 'QoS', 'Security', 'Tools', and 'Logout'. The main content area is titled 'System Information' and contains a table with the following data:

Product model	FR-6S3208
System name	Switch
MAC address	2c:d1:41:44:45:17
IPv4 address	192.168.1.6
Link-local IPv6 address	FE80::2ED1:41FF:FE44:4517/64 (Auto)
Global IPv6 address(es)	None
Subnet mask	255.255.255.0
Default gateway	----
DNS server	----
Software version	LMS1.0.7
Hardware version	V.0.0.1

Below the table is an 'Apply' button. An 'Attention:' section below that states: 'The system name length cannot exceed 32 characters.'

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.

The screenshot shows the 'IP settings' page. At the top, there are 10 port status icons (1-10). On the left is a navigation menu with items like 'System Manage', 'System info', 'IP Settings', 'Account Settings', 'Port Settings', 'Optical Module Status', 'System Config', 'VLAN', 'QoS', 'Security', 'Tools', and 'Logout'. The main content area is titled 'IP settings' and contains a table with the following data:

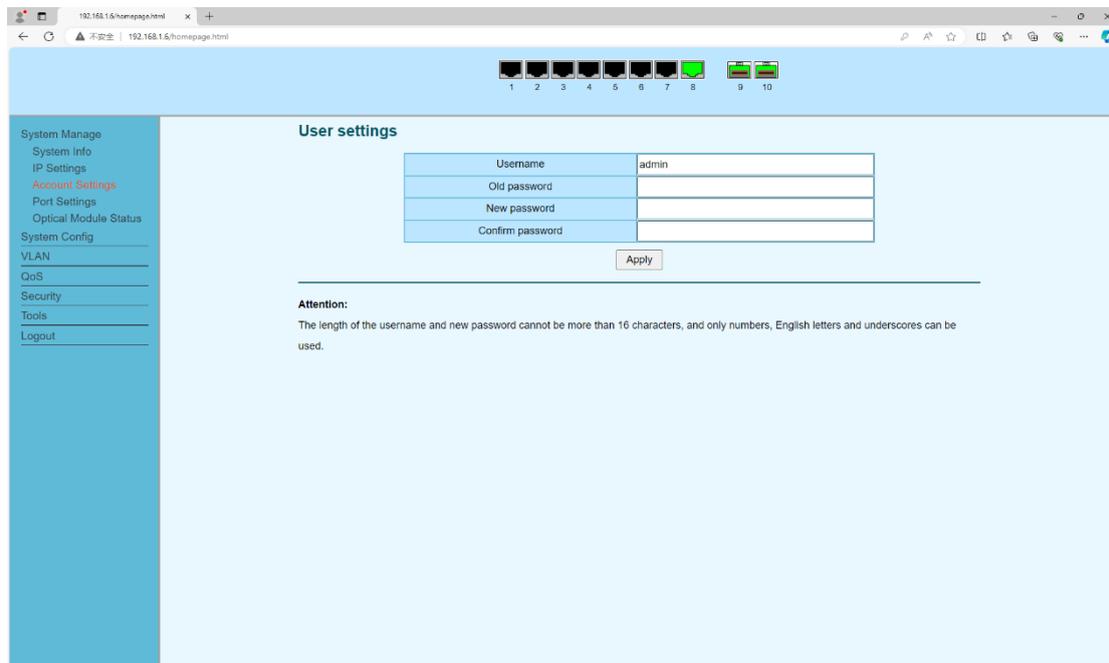
DHCP settings	Disable
IP address	192.168.1.6
Subnet mask	255.255.255.0
Default gateway	
Auto DNS	Disable
DNS server	

Below the table is an 'Apply' button.

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 Address
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 be more than 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.

Port	State		Rate		Duplex		Flow Control	
	Configuration	Actual	Configuration	Actual	Configuration	Actual	Configuration	Actual
Port 1	Enable	Disable	Automatic	N/A	Automatic	N/A	On	N/A
Port 2	Enable	Disable	Automatic	N/A	Automatic	N/A	On	N/A
Port 3	Enable	Disable	Automatic	N/A	Automatic	N/A	On	N/A
Port 4	Enable	Disable	Automatic	N/A	Automatic	N/A	On	N/A
Port 5	Enable	Disable	Automatic	N/A	Automatic	N/A	On	N/A
Port 6	Enable	Disable	Automatic	N/A	Automatic	N/A	On	N/A
Port 7	Enable	Disable	Automatic	N/A	Automatic	N/A	On	N/A
Port 8	Enable	Enable	Automatic	1000M	Automatic	Full Duplex	On	On
Port 9 (SFP,1000BASE-X)	Enable	Enable	Automatic	1000M	Automatic	Full Duplex	On	On
Port 10 (SFP,1000BASE-X)	Enable	Enable	Automatic	1000M	Automatic	Full Duplex	On	On

Attention:
When rate/duplex of a port is set to auto/1000M, full duplex and its actual mode is 1000M full duplex/100M full duplex/10M full duplex, the flow control function can be enabled and take effect.

Item	Description	Notes
Port	Port 1 to 10	
State	Enable/Disable 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.



The screenshot displays a web-based network management interface. At the top, there is a navigation bar with icons for ports 1 through 10. Below this, a sidebar on the left contains a menu with options: System Manage, System Info, IP Settings, Account Settings, Port Settings, Optical Module Status (highlighted in red), System Config, VLAN, QoS, Security, Tools, and Logout. The main content area is titled "Optical Module Status" and contains a table with the following data:

Port	Temperature(°C)	Voltage(V)	Current(mA)	Tx Power(mW)	Rx Power(mW)	Loss of Signal
9	40.79	3.26	20.92	0.25	0.09	False
10	43.46	3.27	23.13	0.25	0.25	False



Chapter 2 System Configurations

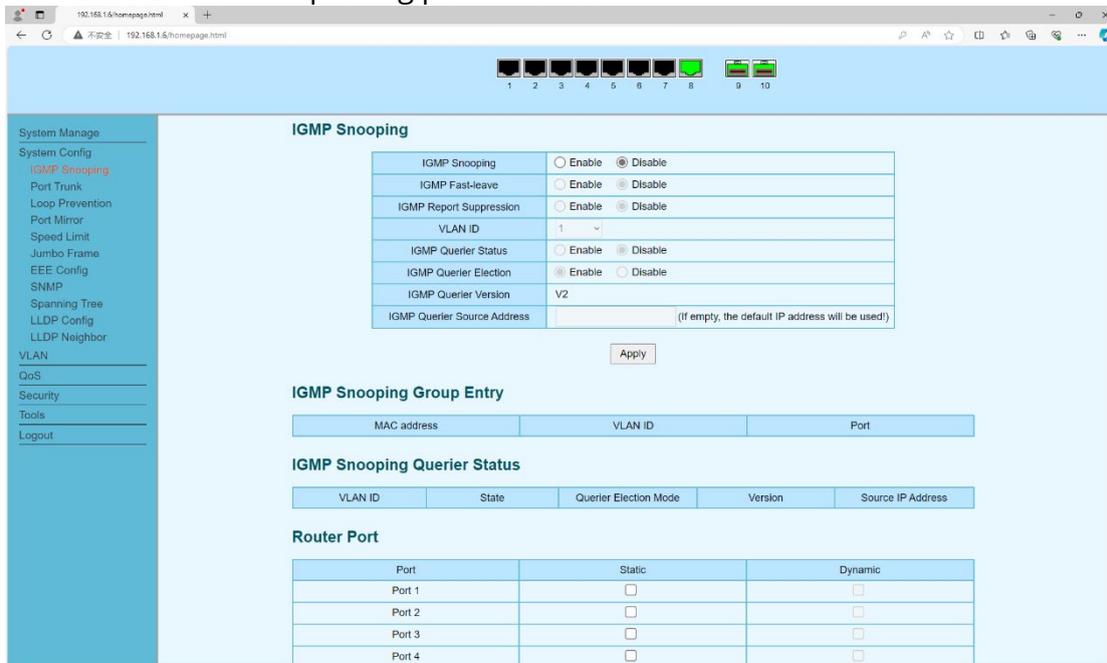
This chapter describes the System configuration in detail, including but not limit to the following:

- ❖ 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 querier 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.

The screenshot shows a web interface for configuring port trunks. At the top, there are 10 port status indicators. The main area is titled 'Trunk configuration'. It features a form with a 'Trunk Group' dropdown (set to 'Trunk 1') and a 'Forward Port' multi-select menu (showing Port 1, Port 2, Port 3, Port 4). An 'Apply' button is below the form. Below the form is a table:

Trunk Group	Forward Port	Selection
Trunk 1	----	<input type="checkbox"/>
Trunk 2	----	<input type="checkbox"/>
Trunk 3	----	<input type="checkbox"/>
Trunk 4	----	<input type="checkbox"/>

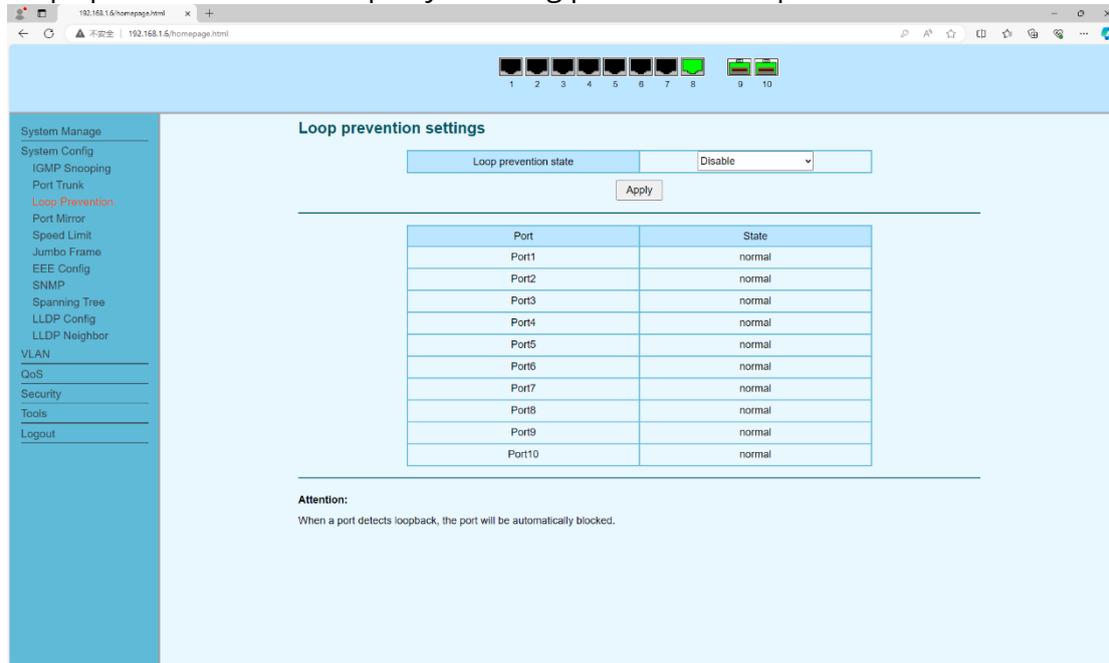
Below the table are 'Select All' and 'Delete' buttons. An 'Attention' section contains the following notes:

1. 4 is the most trunk group can we created.
2. Each aggregation group has at most 8 member ports.

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.



The screenshot shows the 'Loop prevention settings' page. At the top, there is a 'Loop prevention state' dropdown menu currently set to 'Disable' and an 'Apply' button. Below this is a table with two columns: 'Port' and 'State'. The table lists ports from Port1 to Port10, all of which are in a 'normal' state. At the bottom of the page, there is an 'Attention:' section with the text: 'When a port detects loopback, the port will be automatically blocked.'

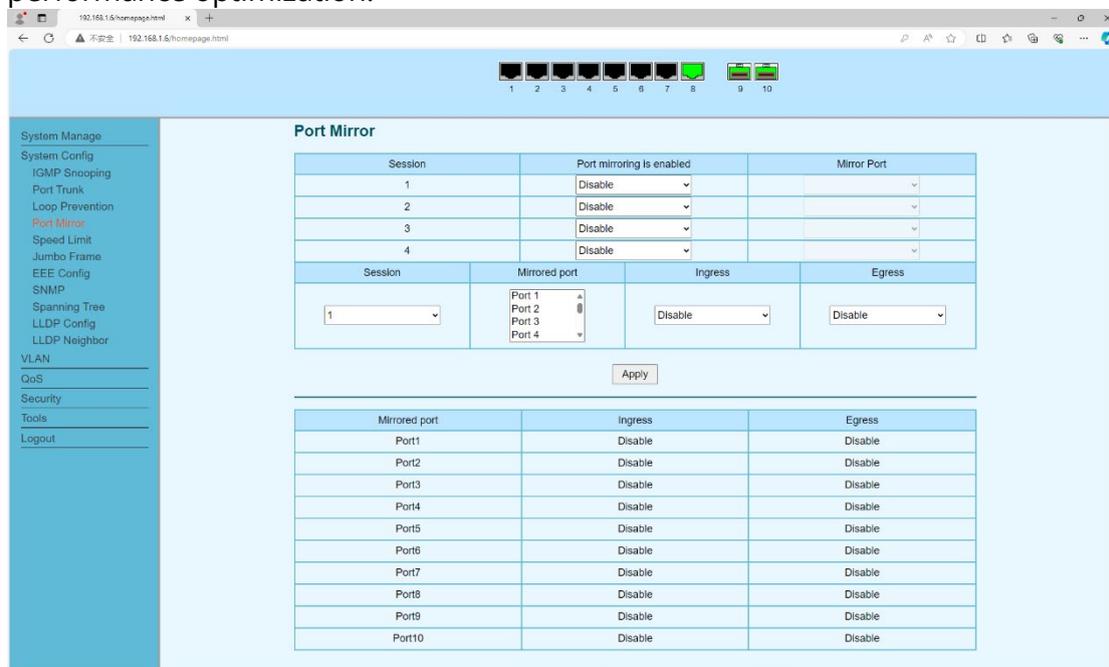
Port	State
Port1	normal
Port2	normal
Port3	normal
Port4	normal
Port5	normal
Port6	normal
Port7	normal
Port8	normal
Port9	normal
Port10	normal

Attention:
When a port detects loopback, the port will be automatically blocked.

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

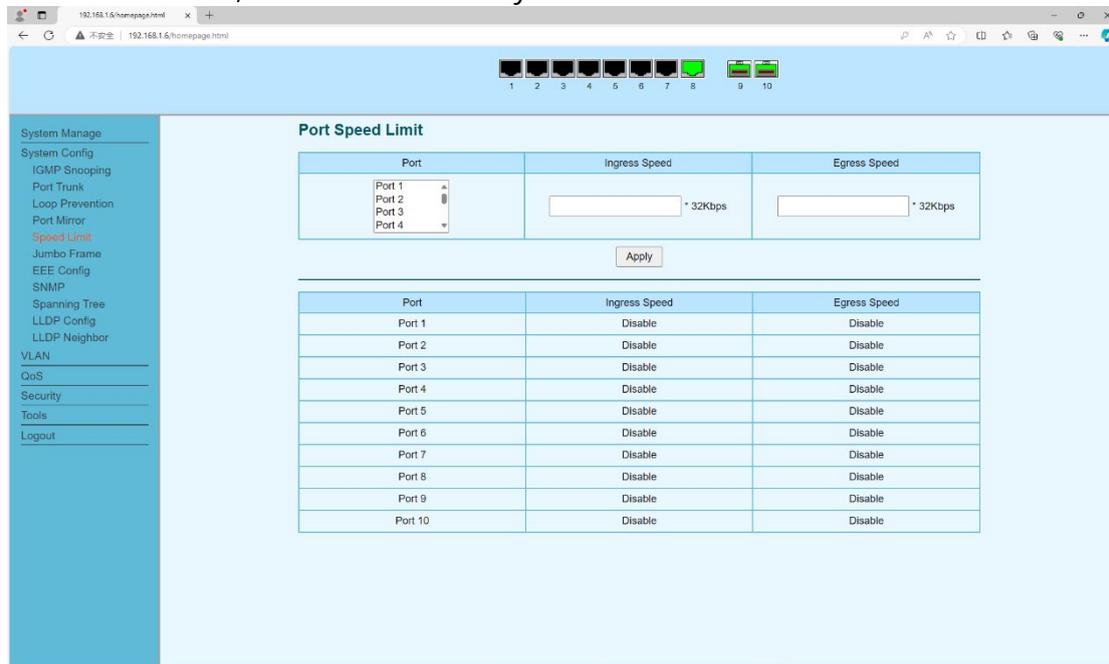
Port mirroring is a network function that duplicates traffic from one or more source ports or VLANs and forwards it to a designated destination port, also known as a monitoring port or analyzer port. This mirrored traffic can then be analyzed by network monitoring tools for troubleshooting, security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

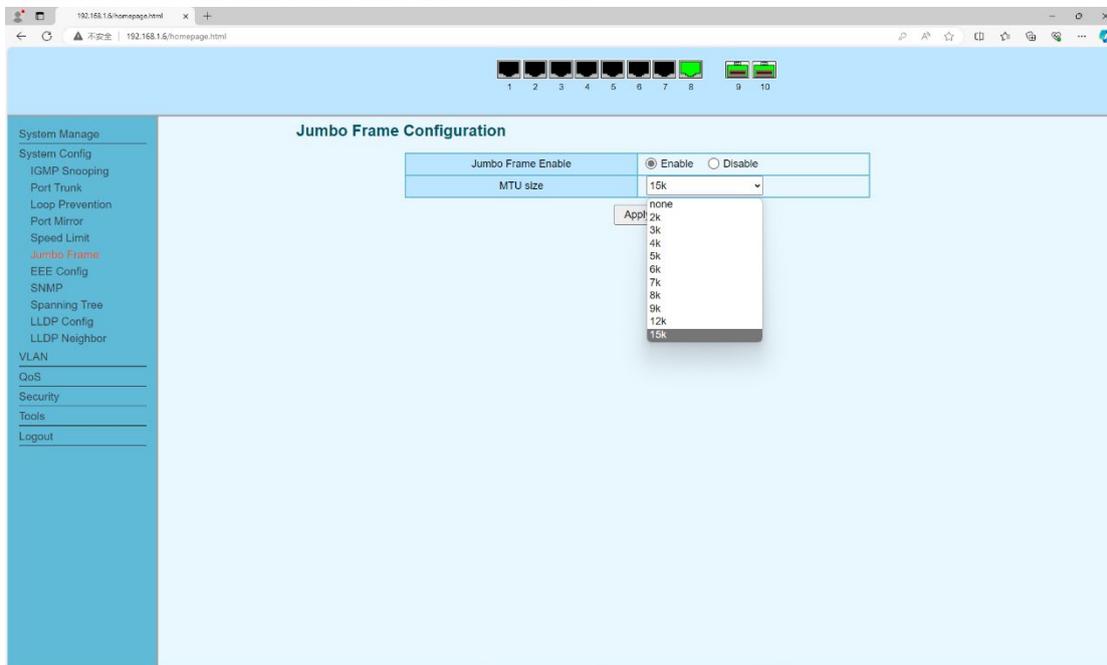
The port speed limit function mainly restricts the transmission speed of the port. It is used to balance network bandwidth, prevent malicious attacks, protect server resources, etc. It can effectively control the network traffic.



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.

The screenshot shows the 'EEE configuration' page in a web browser. At the top, there is a dropdown menu for 'EEE state' currently set to 'Disable', with an 'Apply' button below it. Below this is a table with the following data:

Port	EEE state	Selected
1	Disable	<input type="checkbox"/>
2	Disable	<input type="checkbox"/>
3	Disable	<input type="checkbox"/>
4	Disable	<input type="checkbox"/>
5	Disable	<input type="checkbox"/>
6	Disable	<input type="checkbox"/>
7	Disable	<input type="checkbox"/>
8	Disable	<input type="checkbox"/>
9	Disable	<input type="checkbox"/>
10	Disable	<input type="checkbox"/>

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.

The screenshot shows the SNMP configuration interface. On the left is a navigation menu with options like System Manage, System Config, IGMP Snooping, Port Trunk, Loop Prevention, Port Mirror, Speed Limit, Jumbo Frame, EEE Config, **SNMP**, Spanning Tree, LLDP Config, LLDP Neighbor, VLAN, QoS, Security, Tools, and Logout. The main content area is divided into three sections:

- Version:** Contains two rows. The first row is for 'SNMP v1' with radio buttons for 'Enable' (selected) and 'Disable'. The second row is for 'SNMP v2c' with radio buttons for 'Enable' (selected) and 'Disable'. An 'Apply' button is below.
- Communities:** Contains three rows. The first row is 'read community' with a text input field containing 'public'. The second row is 'write community' with a text input field containing 'private'. The third row is 'trap community' with a text input field containing 'public'. An 'Apply' button is below.
- Trap:** Contains four rows. The first row is 'SNMP v1 trap' with radio buttons for 'Enable' and 'Disable' (selected). The second row is 'SNMP v2c trap' with radio buttons for 'Enable' and 'Disable' (selected). The third row is 'Trap Server' with radio buttons for 'By name' and 'By IP' (selected), and a text input field containing '192.168.0.1'. The fourth row is 'Trap type' with checkboxes for 'Cold/Warm start', 'Link up/down', and 'Authentication Failure'. An 'Apply' button is below.

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.

Spanning Tree Configuration

Spanning Tree State	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Force Version	<input type="radio"/> STP <input checked="" type="radio"/> RSTP	
Forward Delay	15	seconds (4-30)
Max Age	20	seconds (6-40)
Transmit Hold Count	6	BPDUs (1-10)
Priority	32768	(0-61440, in steps of 4096)

Port Configuration

Port	Priority	Cost
Port1		
Port2		
Port3		
Port4		

Port	Priority	Cost	State	Role
Port1	128	2000	Discard	Disable
Port2	128	2000	Discard	Disable
Port3	128	2000	Discard	Disable
Port4	128	2000	Discard	Disable
Port5	128	2000	Discard	Disable
Port6	128	2000	Discard	Disable
Port7	128	2000	Discard	Disable

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).

The screenshot displays the LLDP Configuration page in a web browser. On the left is a navigation menu with options like System Manage, System Config, IGMP Snooping, Port Trunk, Loop Prevention, Port Mirror, Speed Limit, Jumbo Frame, EEE Config, SNMP, Spanning Tree, LLDP Config (selected), LLDP Neighbor, VLAN, QoS, Security, Tools, and Logout. The main content area is titled 'LLDP Configuration' and contains the following sections:

- LLDP Global:** A form with radio buttons for 'Enable' (selected) and 'Disable'. Below are four rows of settings: Tx Interval (30), Tx Hold (4), Reinit Delay (2), and Tx Delay (2). Each row includes a range and default value in parentheses.
- Port Configuration:** A section with a dropdown menu for 'Port' (showing Port 1, 2, 3, 4) and an 'Admin Control' dropdown set to 'Disable'. An 'Apply' button is below.
- Port Status Table:** A table with two columns: 'Port' and 'Admin Status'. It lists ports 1 through 9, all with 'Tx & Rx' status.

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 seconds 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.

The screenshot shows a web browser window displaying the LLDP Neighbor configuration page. The browser address bar shows the URL 192.168.1.6/homepage.html. The page title is "LLDP Neighbor". The main content area contains a table with the following data:

Local Port	Chassis ID	Port ID	System Name	TTL	Med Capabilities	Med Device Type	Network Policy	Extended Power
port 9	2c-d1-41-44-45-17	port_10	Switch	120	medCapabilities	netConnectivity	----	----
port 10	2c-d1-41-44-45-17	port_9	Switch	120	medCapabilities	netConnectivity	----	----

Chapter 3 VLAN

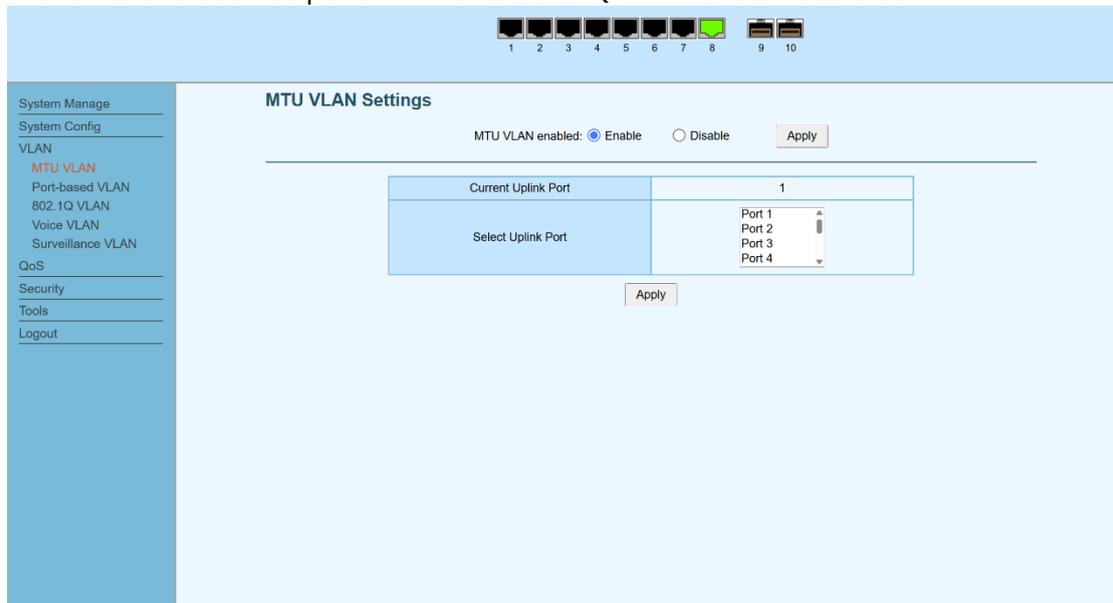
This chapter describes the VLAN functions in detail, including but not limit to the following:

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

3. VLAN

3.1 VLAN-MTU VLAN Settings

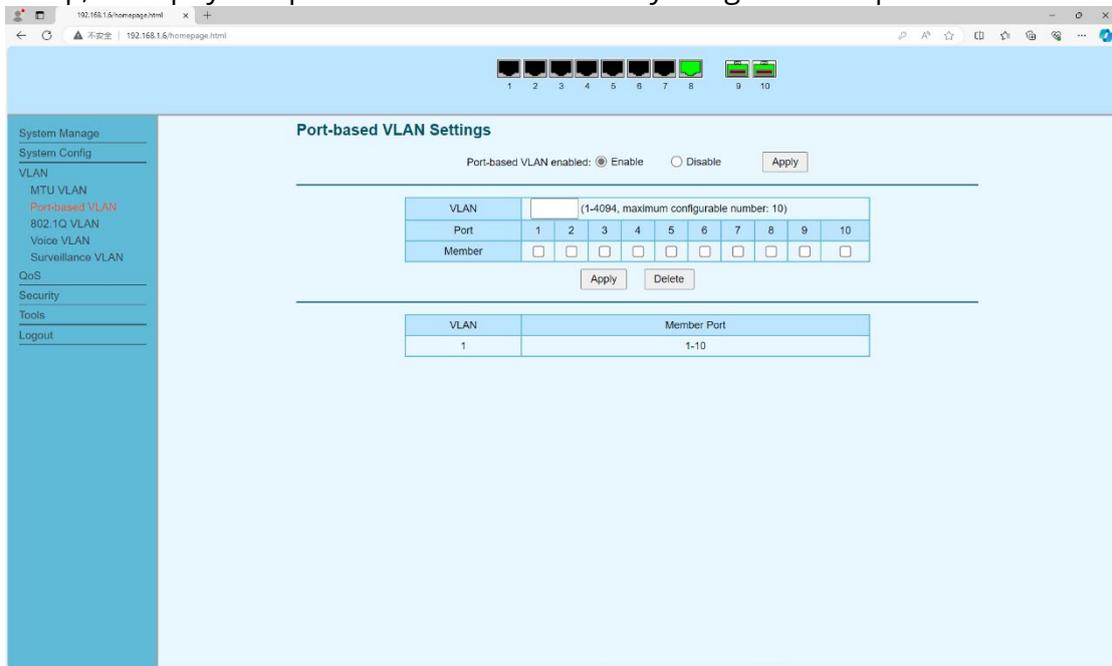
It can be understood as the port isolation function. Set an uplink port. This port can maintain effective communication with all the ports below, but the other ports below are isolated from each other. Note that after enabling the MTU port, the functions such as port VLAN and 802.1Q VLAN are all disabled.



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).

802.1Q VLAN	(1-4094)	Description	
Port	Untagged port	Tagged port	Non-member port
Select All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port 1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Port 2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Port 3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Port 4	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Port 5	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Port 6	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Port 7	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Port 8	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Port 9	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Port 10	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

VLAN	VLAN description	Member Port	Tagged port	Untagged port
1		1-10	-	1-10

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.	

Port	PVID	Ingress filter
Port 1	1	Disable
Port 2	1	Disable
Port 3	1	Disable
Port 4	1	Disable
Port 5	1	Disable
Port 6	1	Disable
Port 7	1	Disable
Port 8	1	Disable
Port 9	1	Disable
Port 10	1	Disable

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.

The screenshot displays the 'Voice VLAN Configuration' page. At the top, there are 10 port status indicators. The configuration includes a 'Voice VLAN enabled' section with 'Enable' selected. Below this is a table for VLAN settings with columns for 'VLAN ID' and 'Priority' (set to 0). There is an 'Apply' button. The 'Enable default OUI' section has 'Default OUI description' selected, with a dropdown for '3com' and 'OUI' '00:E0:BB'. An 'Add' button is present. Below is a table with columns 'Sequence Number', 'OUI Description', 'OUI', and 'Delete', with a 'Delete' button. An 'Attention' note states: 'An OUI can only be assigned to either Voice VLAN or Surveillance VLAN.'

The 'Port Configuration' section contains a table with the following data:

Select	Port	Port Mode	Member State
<input type="checkbox"/>		Manual	
<input type="checkbox"/>	Port1	Auto	Inactive
<input type="checkbox"/>	Port2	Auto	Inactive
<input type="checkbox"/>	Port3	Auto	Inactive
<input type="checkbox"/>	Port4	Auto	Inactive
<input type="checkbox"/>	Port5	Auto	Inactive
<input type="checkbox"/>	Port6	Auto	Inactive
<input type="checkbox"/>	Port7	Auto	Inactive
<input type="checkbox"/>	Port8	Auto	Inactive
<input type="checkbox"/>	Port9	Auto	Inactive
<input type="checkbox"/>	Port10	Auto	Inactive

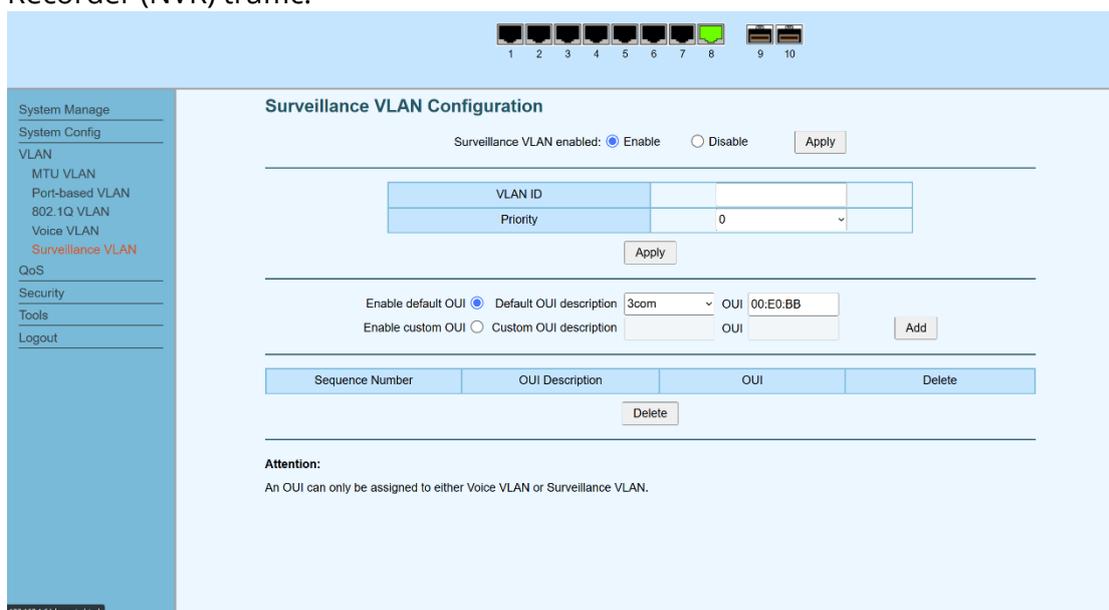
An 'Apply' button is located at the bottom of the Port Configuration section.

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.

The screenshot displays a web-based network management interface. At the top, there is a navigation menu with options: System Manage, System Config, VLAN, QoS (highlighted), QoS Basic, QoS Advanced, Security, Tools, and Logout. The main content area is divided into two sections:

QoS Port Select

Select	Port
<input type="checkbox"/>	Port 1
<input checked="" type="checkbox"/>	Port 2
<input type="checkbox"/>	Port 3
<input type="checkbox"/>	Port 4
<input type="checkbox"/>	Port 5
<input type="checkbox"/>	Port 6
<input type="checkbox"/>	Port 7
<input type="checkbox"/>	Port 8
<input type="checkbox"/>	Port 9
<input type="checkbox"/>	Port 10

Global Configuration

QoS policy: SP WRR WFQ

Apply

Queue Weight Setting

Select	Queue	Weight
<input type="checkbox"/>		<input type="text"/>
<input type="checkbox"/>	Q0	1
<input type="checkbox"/>	Q1	2
<input type="checkbox"/>	Q2	3
<input type="checkbox"/>	Q3	4
<input type="checkbox"/>	Q4	5
<input type="checkbox"/>	Q5	6
<input type="checkbox"/>	Q6	7
<input type="checkbox"/>	Q7	8

Apply

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.

The screenshot displays the QoS configuration interface. At the top, there are 10 port status indicators (1-10). Below them is the 'Global Configuration' section with radio buttons for 'QoS mode': 'Port-based' (selected), 'Based on 802.1p', and 'Based on DSCP'. An 'Apply' button is present.

The 'Based on Port Settings' section contains a table with columns 'Choice', 'Port', and 'Priority'. The 'Priority' column has a dropdown menu set to '0'. The 'Port' column lists Port 1 through Port 10. Each row has a checkbox in the 'Choice' column.

Choice	Port	Priority
<input type="checkbox"/>		0
<input type="checkbox"/>	Port 1	0
<input type="checkbox"/>	Port 2	0
<input type="checkbox"/>	Port 3	0
<input type="checkbox"/>	Port 4	0
<input type="checkbox"/>	Port 5	0
<input type="checkbox"/>	Port 6	0
<input type="checkbox"/>	Port 7	0
<input type="checkbox"/>	Port 8	0
<input type="checkbox"/>	Port 9	0
<input type="checkbox"/>	Port 10	0

An 'Apply' button is located at the bottom of this section.

The 'Priority Queue Mapping' section contains a table with columns 'Choice', 'Priority', and 'Queue'. The 'Queue' column has a dropdown menu set to 'Q0'. The 'Priority' column lists values from 0 to 7. The 'Queue' column lists Q1 through Q7. Each row has a checkbox in the 'Choice' column.

Choice	Priority	Queue
<input type="checkbox"/>		Q0
<input type="checkbox"/>	0	Q1
<input type="checkbox"/>	1	Q0
<input type="checkbox"/>	2	Q2
<input type="checkbox"/>	3	Q3
<input type="checkbox"/>	4	Q4
<input type="checkbox"/>	5	Q5
<input type="checkbox"/>	6	Q6
<input type="checkbox"/>	7	Q7

An 'Apply' button is located at the bottom of this section.

Global Configuration

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

Apply

Priority Queue Mapping

Choice	Priority	Queue
<input type="checkbox"/>		Q0
<input type="checkbox"/>	0	Q1
<input type="checkbox"/>	1	Q0
<input type="checkbox"/>	2	Q2
<input type="checkbox"/>	3	Q3
<input type="checkbox"/>	4	Q4
<input type="checkbox"/>	5	Q5
<input type="checkbox"/>	6	Q6
<input type="checkbox"/>	7	Q7

Apply

Global Configuration

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

Apply

Based on DSCP Settings

Choice	DSCP	Priority
<input type="checkbox"/>		0
<input type="checkbox"/>	0	0
<input type="checkbox"/>	1	0
<input type="checkbox"/>	2	0
<input type="checkbox"/>	3	0
<input type="checkbox"/>	4	0
<input type="checkbox"/>	5	0
<input type="checkbox"/>	6	0
<input type="checkbox"/>	7	0
<input type="checkbox"/>	8	0
<input type="checkbox"/>	9	0
<input type="checkbox"/>	10	0
<input type="checkbox"/>	11	0
<input type="checkbox"/>	12	0
<input type="checkbox"/>	13	0
<input type="checkbox"/>	14	0
<input type="checkbox"/>	15	0
<input type="checkbox"/>	16	0
<input type="checkbox"/>	17	0
<input type="checkbox"/>	18	0
<input type="checkbox"/>	19	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.

The screenshot shows the 'MAC configuration' page in a web browser. At the top, there are icons for ports 1 through 10. Below that, the 'MAC configuration' section has a 'Port Index' dropdown set to 1 and a 'Maximum MAC number' input field set to 0. An 'Apply' button is next to it. A table below shows the configuration for all 10 ports, with 'Maximum MAC number' set to 0 for each. Below the table, there are input fields for 'Port Index' (1), 'VID' (1), and 'MAC address', with an 'Add' button. At the bottom, there is a table with columns 'Index', 'VID', 'MAC', 'Port', and 'Selected', and a 'Delete' button.

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.

Port	Unknown Unicast Packets			Multicast Packets			Broadcast Packets		
	State	Speed	Kbps	State	Speed	Kbps	State	Speed	Kbps
Port 1	Disable			Disable			Disable		
Port 2	Disable			Disable			Disable		
Port 3	Disable			Disable			Disable		
Port 4	Disable			Disable			Disable		
Port 5	Disable			Disable			Disable		
Port 6	Disable			Disable			Disable		
Port 7	Disable			Disable			Disable		
Port 8	Disable			Disable			Disable		
Port 9	Disable			Disable			Disable		
Port 10	Disable			Disable			Disable		

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	

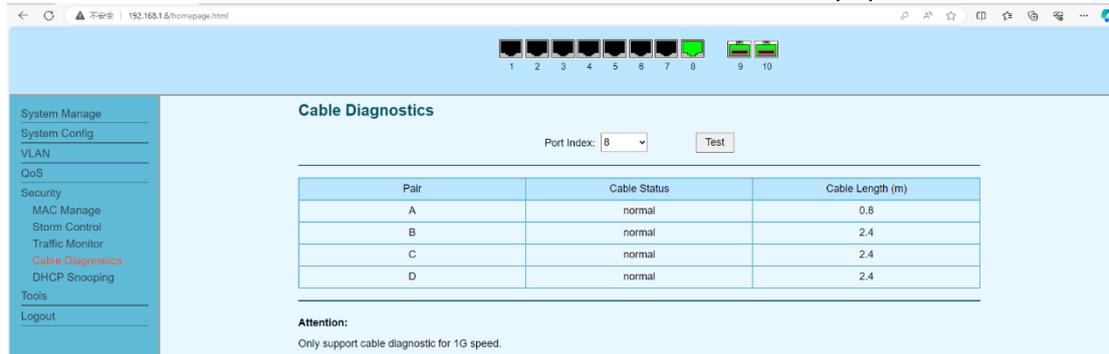
5.3 Security – Traffic Monitor

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.

Port	Tx bytes	Rx bytes	Tx pkts	Rx pkts
Port 1	0	0	0	0
Port 2	0	0	0	0
Port 3	0	0	0	0
Port 4	0	0	0	0
Port 5	0	0	0	0
Port 6	0	0	0	0
Port 7	0	0	0	0
Port 8	1664187	1435062	4147	7594
Port 9	379993	3712	3216	58
Port 10	3712	379993	58	3216

5.4 Security – Cable Diagnostics

Provide the cable status of each electrical interface on the equipment

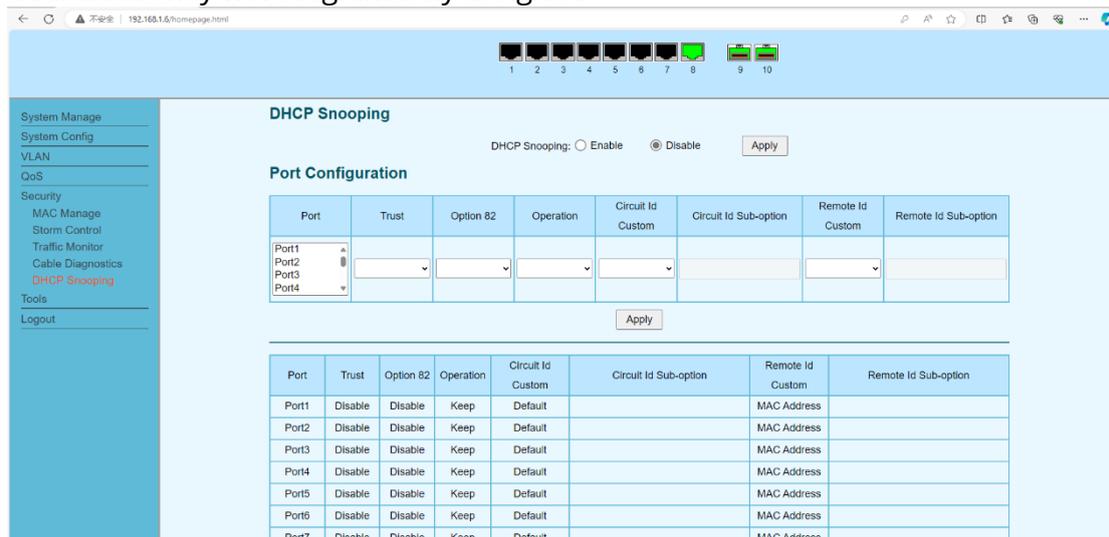


Pair	Cable Status	Cable Length (m)
A	normal	0.8
B	normal	2.4
C	normal	2.4
D	normal	2.4

Attention:
Only support cable diagnostic for 1G speed.

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.



Port	Trust	Option 82	Operation	Circuit Id	Circuit Id Sub-option	Remote Id	Remote Id Sub-option
Port1				Custom		Custom	
Port2							
Port3							
Port4							
Port5	Disable	Disable	Keep	Default		MAC Address	
Port6	Disable	Disable	Keep	Default		MAC Address	
Port7	Disable	Disable	Keep	Default		MAC Address	

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

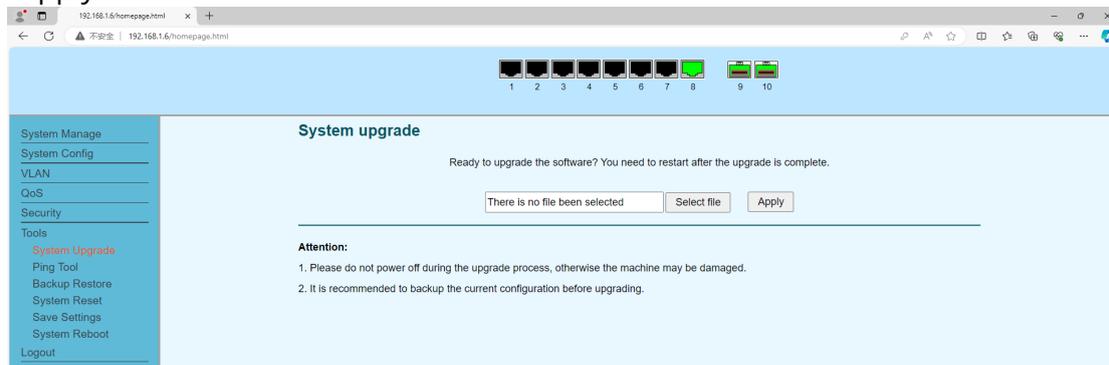
This chapter describes the tools functions in detail, including but not limit to the following:

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

6. Tools

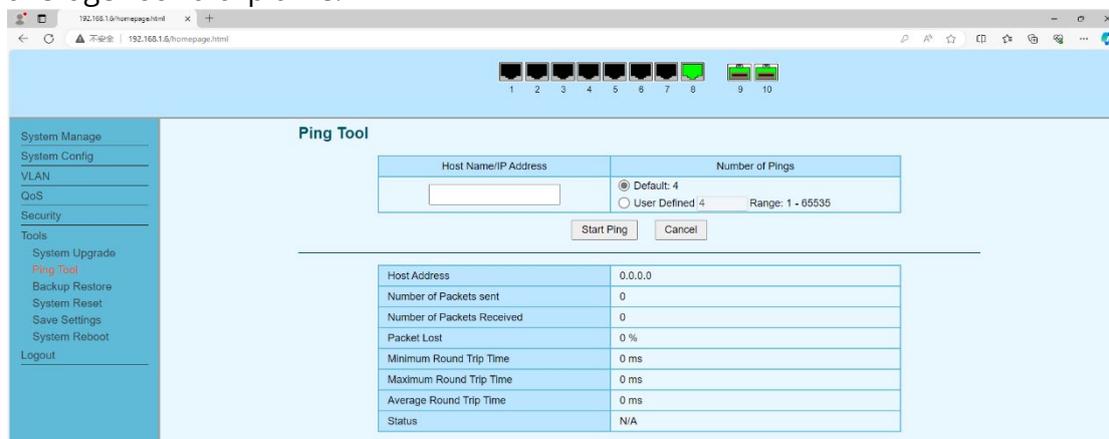
6.1 Tools – System Upgrade

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".



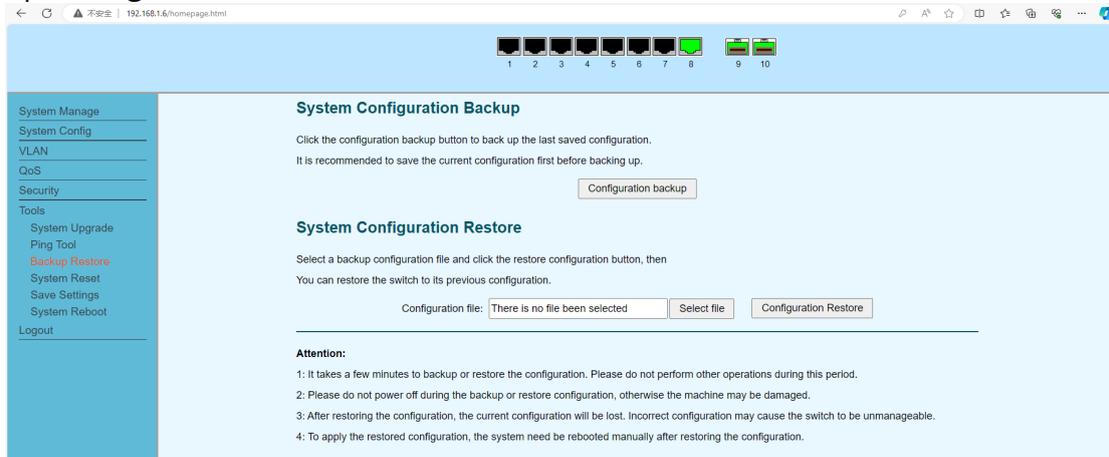
6.2 Tools – Ping Tool

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.



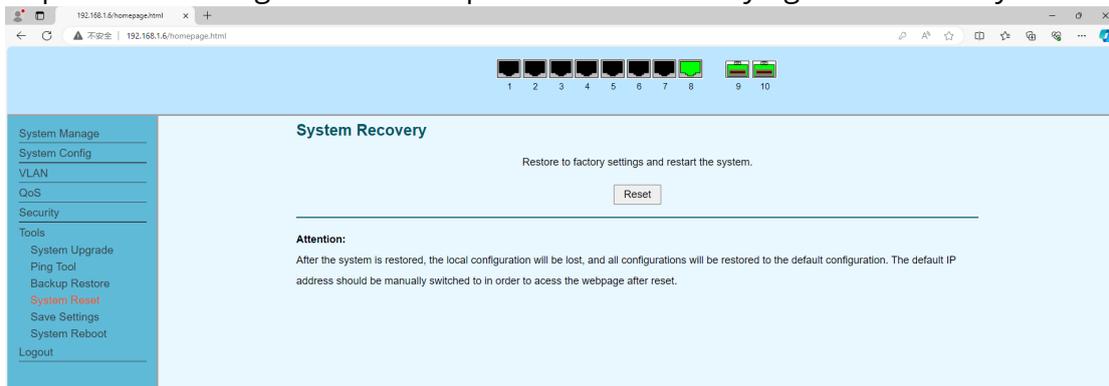
6.3 Tools – Backup Restore

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.



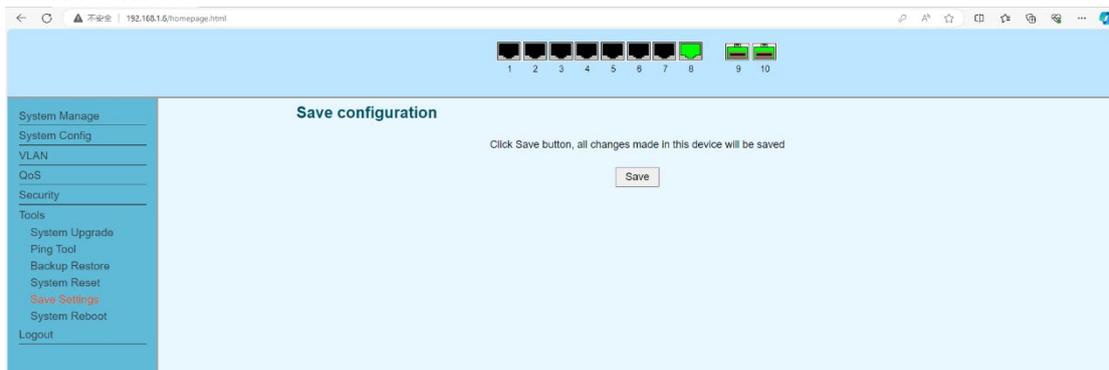
6.4 Tools – System Reset

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.



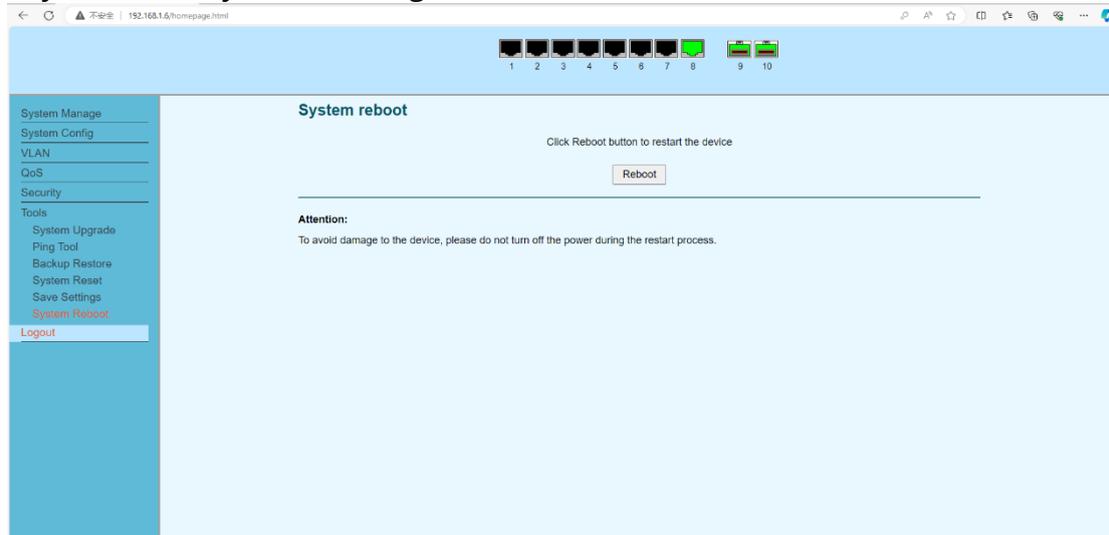
6.5 Tools – Save Settings

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
memr1 address: read 4 bytes from register or memory at the address
memw1 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

