Web Light network Management switch softw are manual

content

Chapter 1 Introduction to the Manual

This manual detailed Web light management switch software function configuration method. Please read this manual carefully before operation.

1.1 Target Audience

The target readers of this manual are those who understand or use the functions of this Web light network management software.

1.2 Manual Conventions

In this manual, the 8-port switch is taken as an example to show the Web interface and software functions.

Use --> symbol to indicate the entry order of the menu, the first function menu --> the second function menu --> the third function menu. Among them, some functions have no two or three function menus.

The <> Angle bracket mark text appearing in the text indicates the name of the button, such as < application >, <apply>.

The special ICONS used in this manual are described as follows:

Instructions	A description of the contents of the operation, with necessary additions and explanations.
 Attention	Remind the matters that should be paid attention to in the operation, improper operation may lead to data loss or equipment damage.

Chapter 2 Introduction to Web Light network Management functions

2.1. Function Introduction

Our new developed Web light network management switch function software, support a variety of models. Provide VLAN, QoS, RSTP, SNMP, POE control, link aggregation and other functions.

Home Page	Support Logo, interface panel, system informationdisplay
System	IP address Settings, port Settings, user accounts
POE	POE power port control
Configuration	VLAN
	QOS
	IGMP
	Link aggregation
	Loop protection
	RSTP
	Port mirroring
	Port isolation
	Bandwidth control
	Giant frame
	MAC constraints
	Green Ethernet
	EEE
	SNMP(V1 only, and some V2 nodes)
Security	MAC address
	Broadcast Storm
Monitoring	Port statistics
	Cable diagnostics
Tools	Firmware upgrade
	Configure backup
	Reset
	Save
	Restart

Note: Only the device with POE power supply has POE function

Chapter 3 Login Web interface

3.1 Login

1. The switch has been powered on and started normally, and any port has been connected to the management PC.

2. The management PC has installed at least one of the following browsers: IE 8.0 or above version, the latest version of Chrome, 360 browser.

The IP address of the management PC has been set to the same network segment as the switch port, that is, 192.168.2.X (X is any integer between 2 and 254), and the subnet mask is 255.255.255.0.

4. In order to ensure a better experience of the Web interface display effect, it is recommended to adjust the resolution of the monitor to 1280×800 pixels or above.

5. Open the browser and enter the default management address of the switch http://192.168.2.1 in the address bar to log in to the switch Web management interface.

6. Switch login page as shown in the following picture, input the user name and password of the switch management account, the factory default value is admin.

FIG. 1 web login interface

7. After successful login, the main page of the web interface shows the following picture.

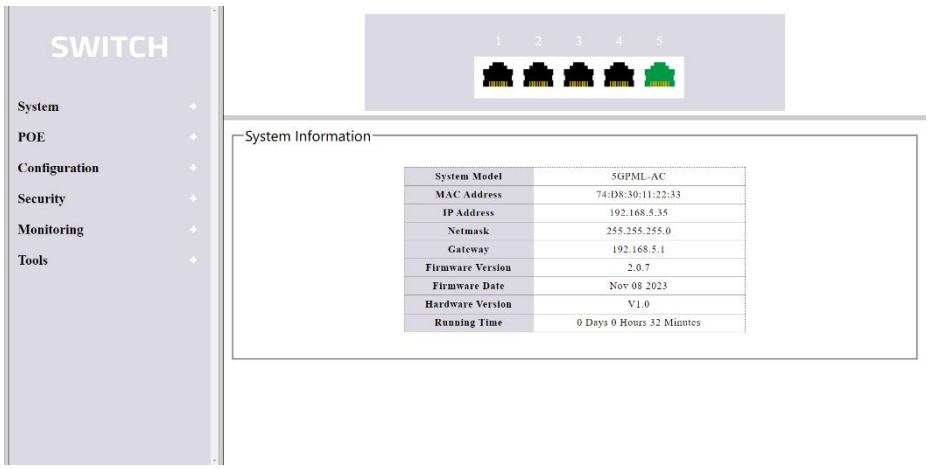


Figure 2 web home page

Left navigation bar, this is neutral software. No Logo is shown. The upper right shows the interface panel of the model. The bottom right is the system basic information.

Chapter IV System

4.1 System Information

You can view your device's system information here, as well as set your device model.

In the navigation bar click: System --> System Information

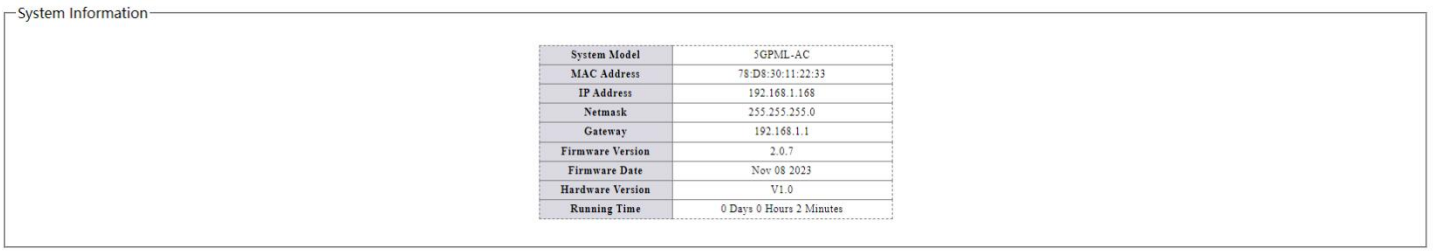


Figure 3 System information

Notes:

Device Model	Display device model
MAC address	Display the MAC address of your device
IP address	Display device management IP address
Subnet mask	Display device subnet mask
Gateway	Display device default gateway
Key version	Display software version
Firmware date	Display the software version date
Hardware version	Display device hardware version
Run time	Display device run time

4.2 IP Settings

Each device in the network has an IP address through which it can log into the management interface to operate the switch. Click the navigation bar: System --> IP Settings

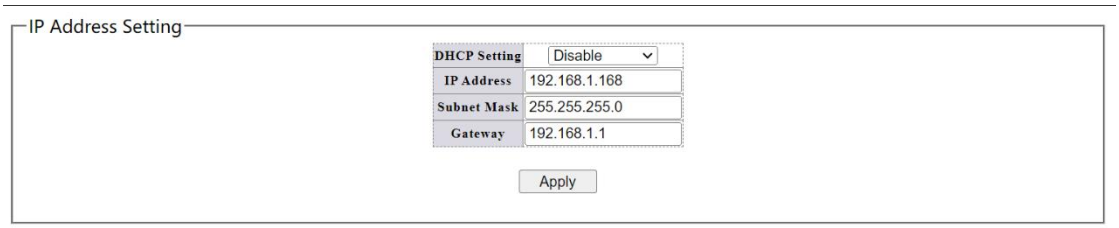


FIG. 4 IP address Settings

Instructions:

DHCP Settings Choose to enable or disable the DHCP feature.

Disable: Select disable, you need to manually enter the IP address, subnet mask and default gateway. Enable: Select Enable, the exchange will get the network parameters from the DHCP server.

IP Address Sets the IP address of the device.

Subnet Mask Sets the subnet mask of the device.

Default Gateway Sets the device's default gateway address.

Click <Apply> System Administration IP, subnet mask, gateway will be modified to the set value.

4.3 User Settings

You can change the username and password you use when you log in here.

Click on the navigation bar: System --> User Account

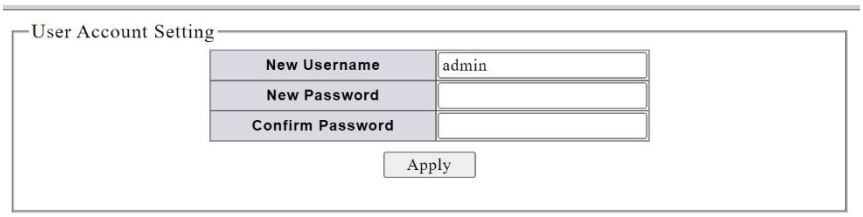


Figure 5 User Account Settings

Instructions:

User Name Set the user name to log into the switch. The username cannot be longer than 16 characters and can only use numbers, English letters, and underscores.

New Password Reset the password used to log in to the switch. The new password cannot be longer than 16 characters and can only use numbers, English letters, and underscores. Make sure you enter the same password twice.

Note: Please refresh the page again after changing the password.

4.4 Port Settings

Port name, status, duplex speed, flow control can be modified here.

Click on the navigation bar: System --> Port Settings

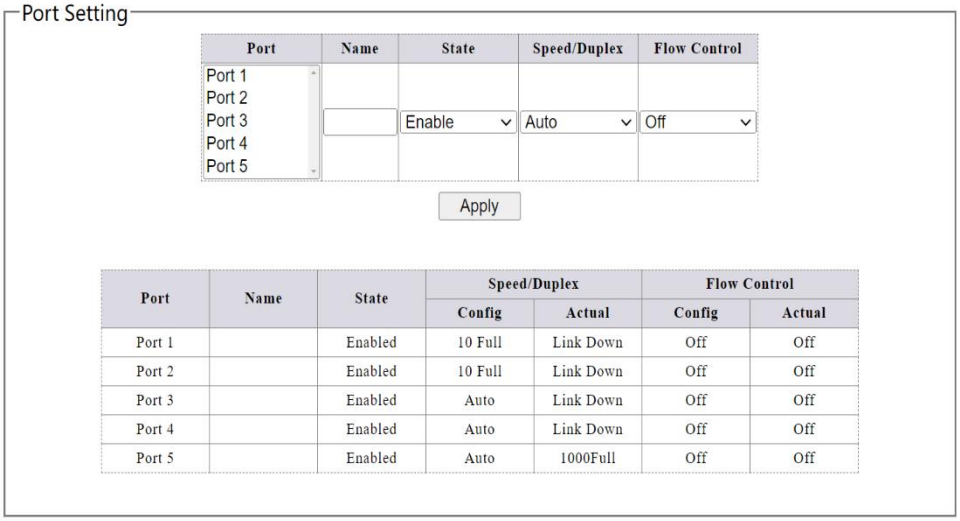


Figure 6 Port Settings

Instructions:

First name sets port aliases.

The port is open and closed. If the port is open, the port can forward packets normally.

Speed/duplex can be selected 10M/Half, 10M/Full, 100M/Half, 100M/Full, automatic. When the mode is selected as auto, the rate and duplex will be determined by negotiation

The flow control function is turned on and off. When the flow control function is turned on, the rate of data packet forwarding on each port can be controlled and adjusted to avoid congestion

After changing the Settings, click the port Settings to refresh the display status

Note: The flow control function will actually be turned on in half duplex mode

Chapter 5 POE

5.1. POE

Shows the total power consumed by the POE port

Click on the navigation bar: POE --> System

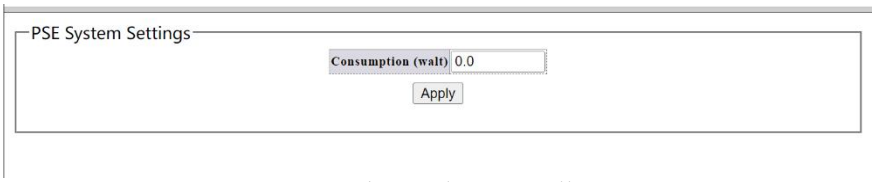


Figure 7 Total power consumed by POE

You can set the PSE port status here (only for devices that support the POE power supply function) by clicking on the navigation bar: POE --> Port[i]

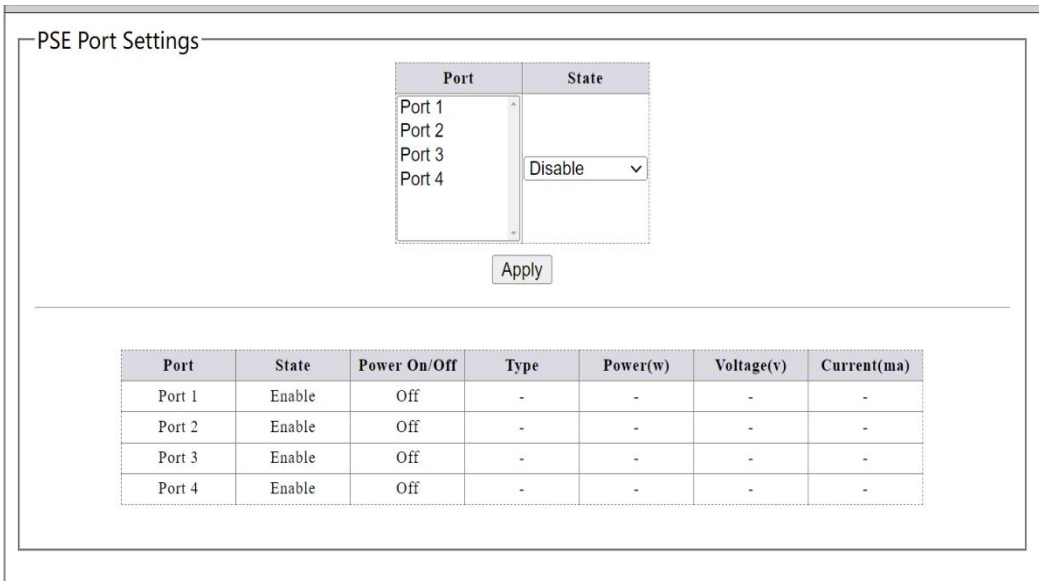


FIG. 8 PSE port Settings

Instructions:

Ports Multiple ports can be selected

State In the open state can be normal power supply. Power on/off display current working state power display port output power voltage display PSE port supply voltage current display PSE port supply current

Chapter VI Configuration

6.1 VLAN

VLAN (Virtual Local Area Network, virtual local area network) is a physical LAN in the logical division of multiple broadcast domains of communication technology, this technology by defining the extension field on the LAN data frame, to the physical network logical division, In order to limit the local area network data frame forwarding range, narrow the broadcast domain. VLAN technology is mainly used in network equipment such as switches, routers and switches.

Click navigation bar: Configuration -> VLAN -> Static VLAN

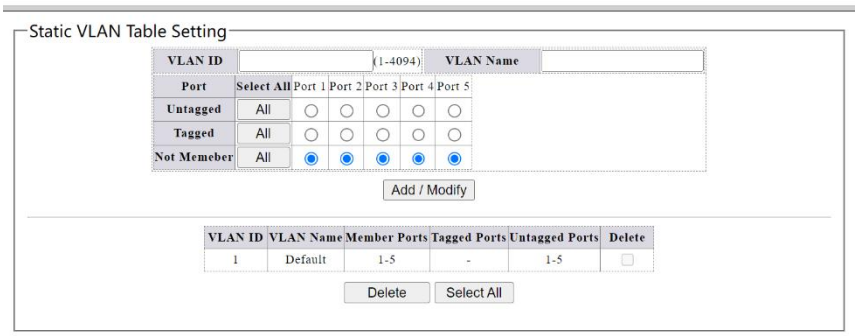


Figure 9 Static V LA N

Click on the navigation bar: Configuration --> VLAN --> VLAN Settings

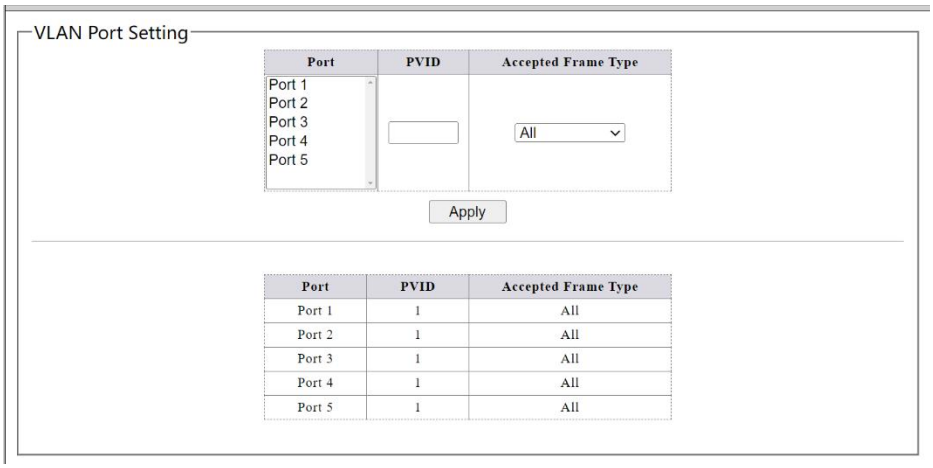


Figure 10 VLAN Settings

Vlans are distinguished by VLAN ids, and all Untagged packets arriving at the port will be tagged by the Tag of the port PVID. Instructions:

You need to set the VLAN ID before setting the port VID

VLAN ID is set for static VLAN, ranging from 1-4094.

Untagged port If Untagged port is selected, the output data frame does not have tag information. If the Tagged port is selected, the output dataframe will have tag information.

If no member port is selected, it means that the port is not a member port of VLAN.

Note: Before deleting a VLAN, it is necessary to set the VID of the port using this VLAN to 1 before deleting this VLAN.

6.1.1Example

Set VLAN10 for ports 1, 2 and 3 of the switch, and VLAN20 for ports 4, 5, 6 and 7 of the switch. Port 8 is added to VLAN10 and VLAN20 respectively as the upper connection port. At the same time, VLAN1 contains all ports. In this way, data packets from ports VLAN10 and VLAN20 can be forwarded to port 8. As shown in the following picture

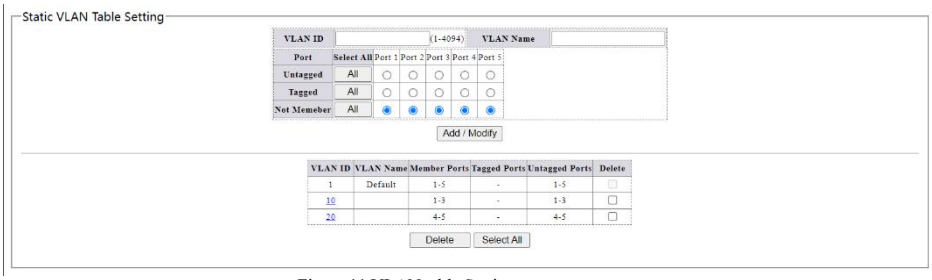


Figure 11 VLAN table Settings

After setting up the VLAN table, you also need to set the port VID. Set the VID on ports 1, 2, and 3 to 10, the VID on ports 4, 5, 6, and 7 to 20, and the VID on port 8 to default 1. This way the data on port 8 will be forwarded to all ports. The result is shown in the following figure

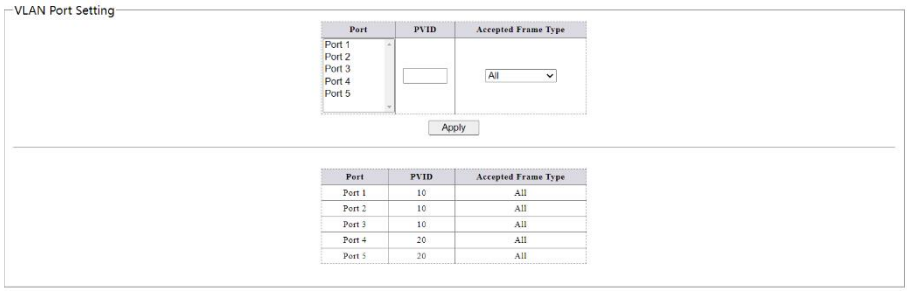


Figure 12 Setting V L A N back port 5/8ping pass

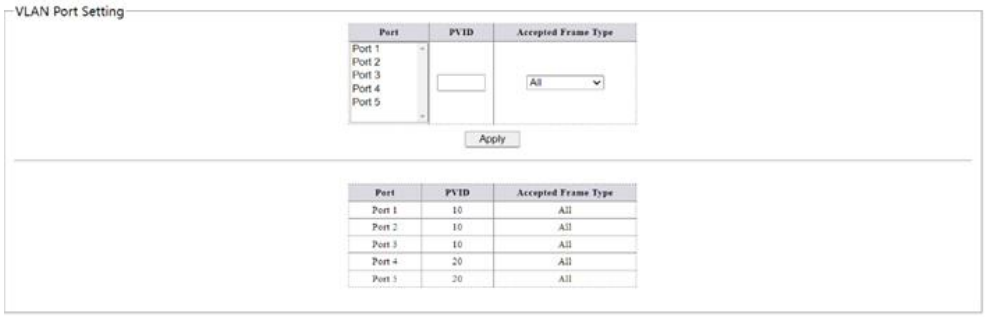


Figure 13 Setting up VLAN back port 2/8ping pass

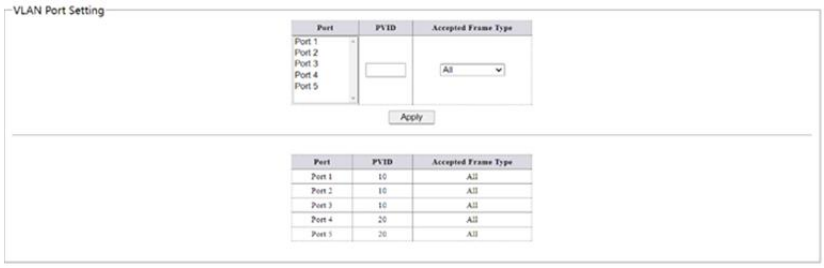


Figure 14 Setting VLAN back port 2/6 ping blocked

Ports 1, 2 and 3 are isolated from ports 4, 5, 6 and 7, and can communicate with upper link port 8.

6.2 QoS

QoS (quality of Service) functions are used to optimize network performance and provide better network service experience. Switches are based on port, 802.1P, DSCP priority mode.

6.2.1 Priority selection

Click on the navigation bar: Configuration > QOS > Priorities

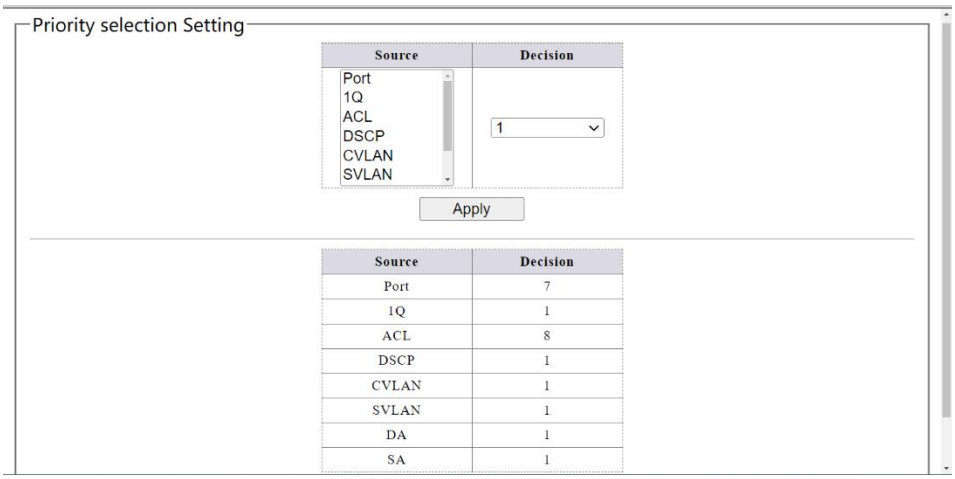


Figure 15 Priority selection Settings

Instructions:

Priority selection sets the priority of the priority source, specifying the transmission queue for the frame based on the highest priority source.

6.2.2 DSCP remap

DSCP gives a recommended definition for the IP DSCP field. IP packets are mapped to eight priorities based on DSCP values (0-63).

Click on the navigation bar: Configure --> QOS --> DSCP Remap

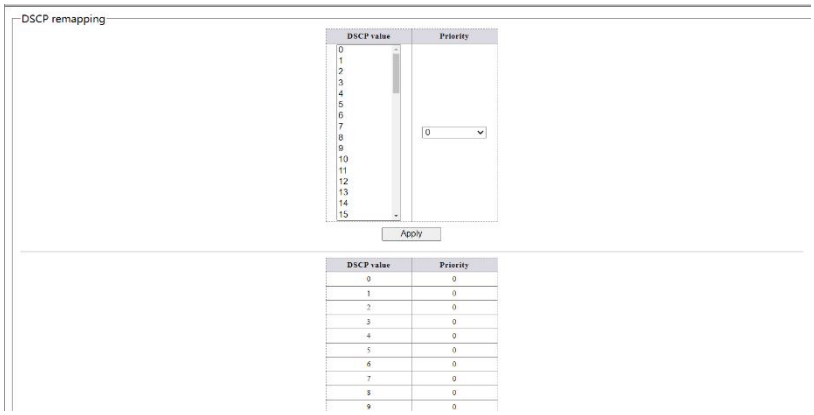


Figure 16 DSCP priority mapping

Note:
Map DSCP values to internal priorities

6.2.3 Priority and queue map

Map different priorities to different queues (4 queues)

Click on the navigation bar: Configure -> QOS -> Priority to Queue

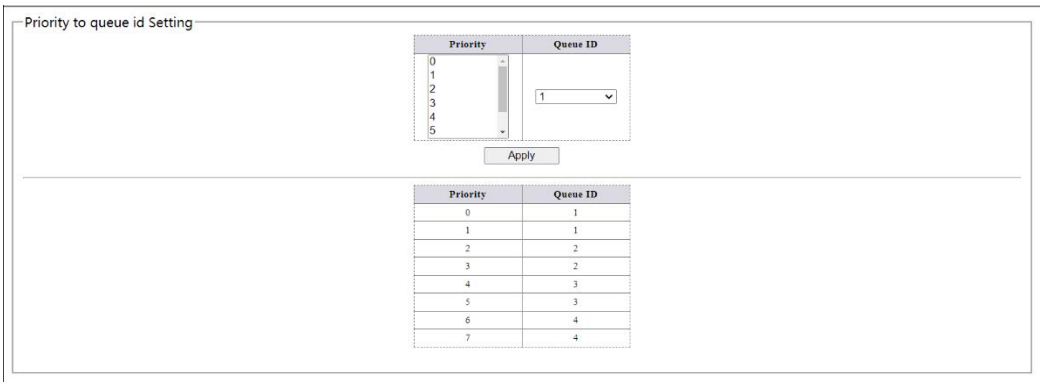


Figure 17 Priority queue mapping

6.2.4 Port priority

These packets are mapped to eight different priority levels based on the incoming port.

Click on the navigation bar: Configuration -> QOS -> Port Priority

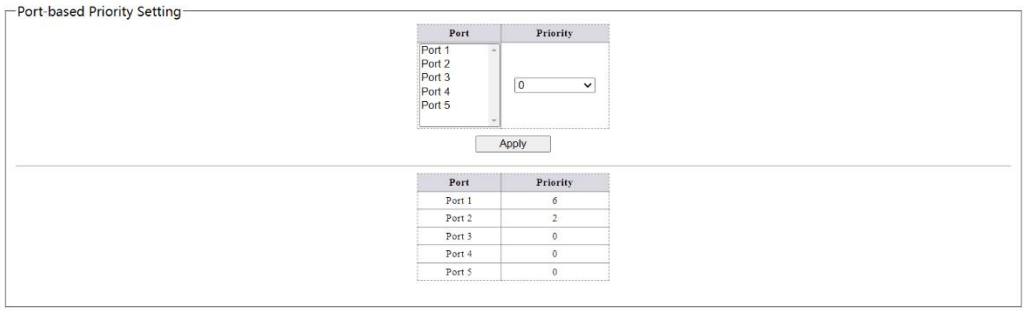


Figure 18 Port priority Settings

6.2.5 Queue weights

Set the queue weights so that different queues get different scheduling priorities.Click on the navigation bar: Configure --> QOS --> Q Queue Weight

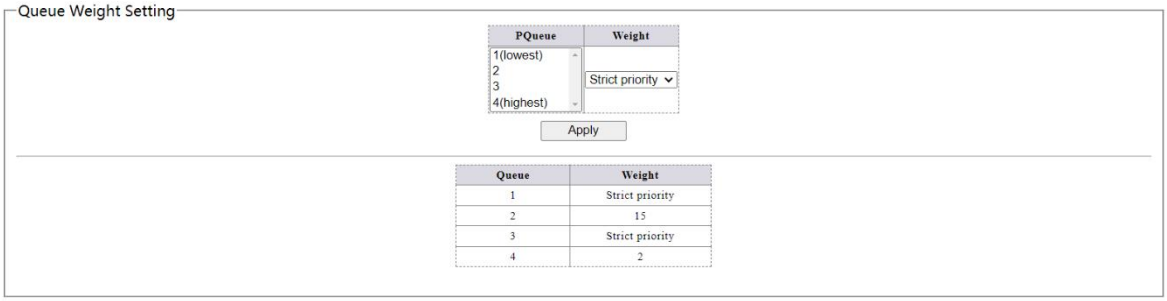


Figure 19 Q queue weights

6.2.6 Example 1

An example of port priority

1 Connect your device with the following topology.

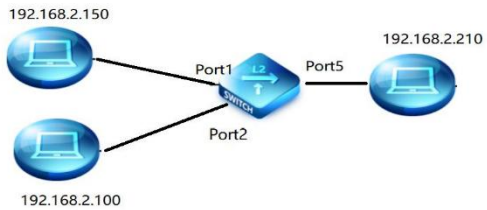


Figure 20 Connection topology

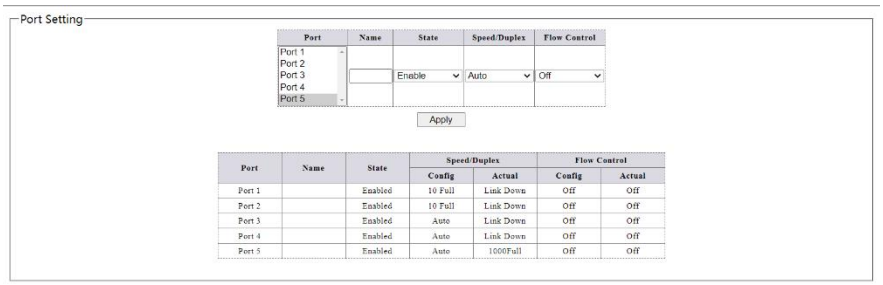


Figure 21 Port 1/2 setup

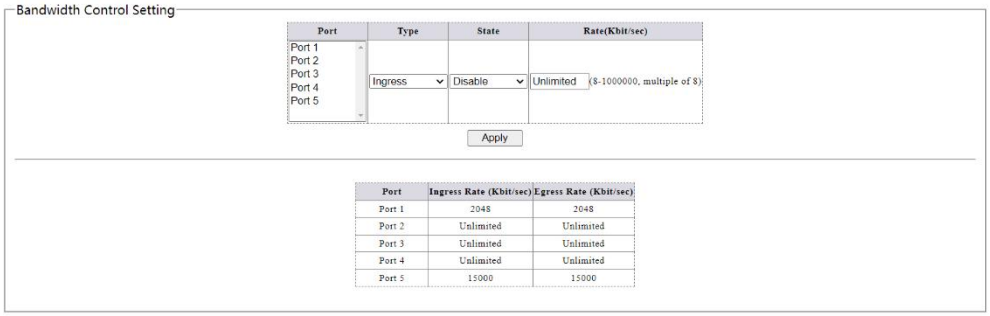


Figure 22 Port 5 speed limit

3 Open the test software and test the sending rate of ports 1 and 2 when the port priority is not set. The sending rate of ports 1 and 2 is constantly changing.

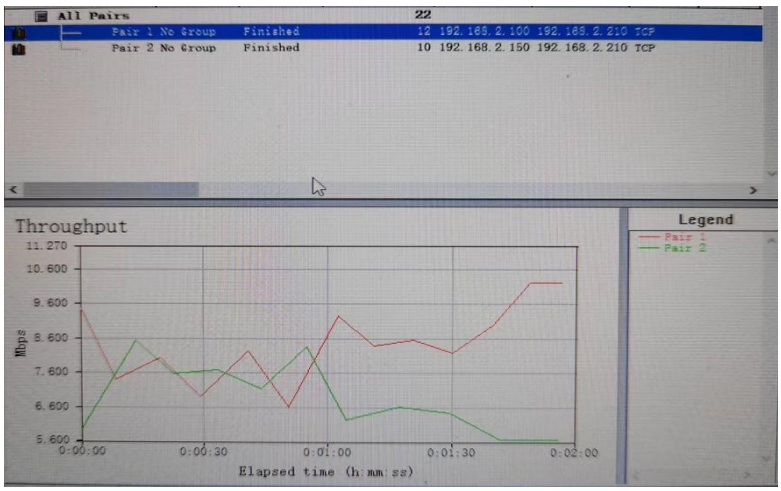


Figure 23 Port 1/2 bandwidth distribution when port priority is not set

4. Set the priority of port 1 to 6 and port 2 to 2.

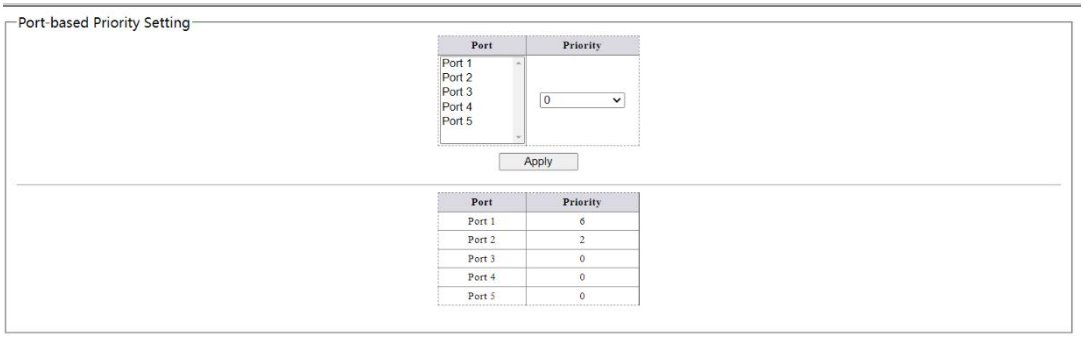


Figure 24 Port priority Settings

4 Open the test software and test the sending rate of ports 1 and 2 after setting the port priority. Port 1 has a rate of nearly 10M bps, and port 2 has a rate of only 5Mbps.

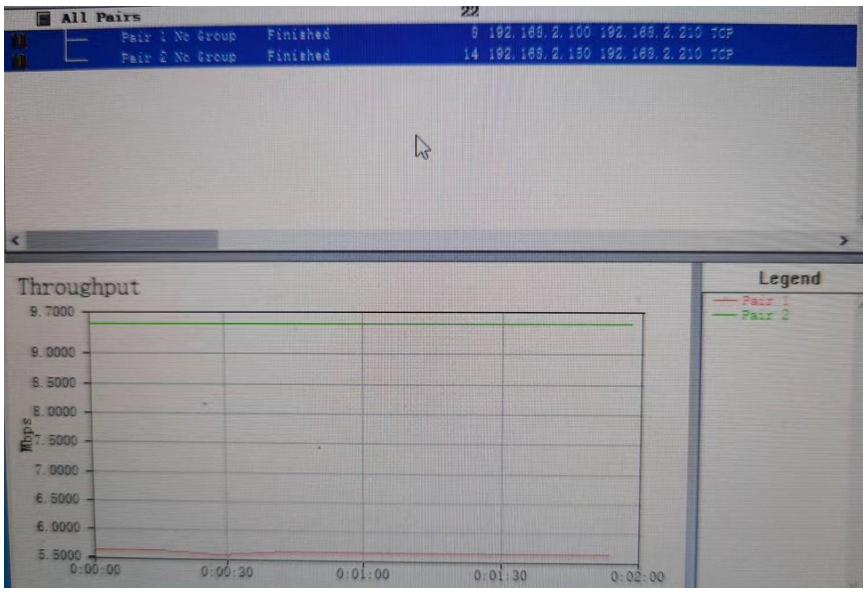


Figure 25 Port bandwidth distribution after setting port priority

6.2.7 Example 2

Queue weight example

Connect to the topology of Example 1, port 1 is connected to the device with IP 192.168.2.100, port 8 is connected to the device with IP 192.168.2.50, and port 5 is connected to the device 192.168.2.210.

2, Set the priority and queue mapping.

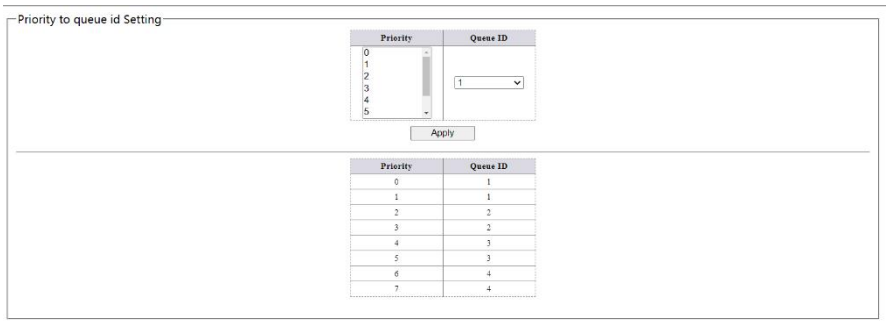


Figure 26 Priority and queue mapping

3, Set port priority

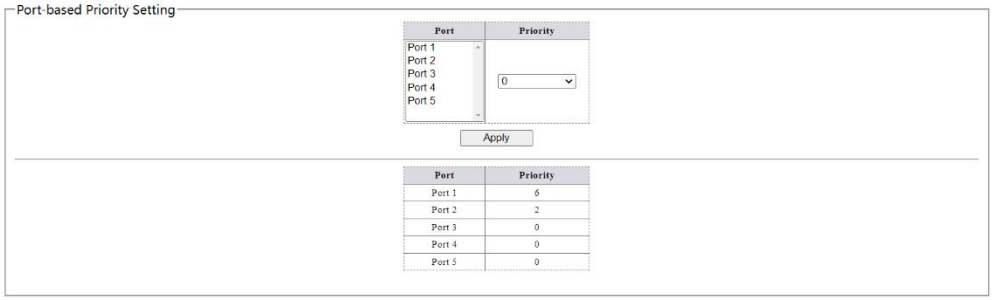


Figure 27 Port priority

4. Queue weight is not set and strict priority is default.

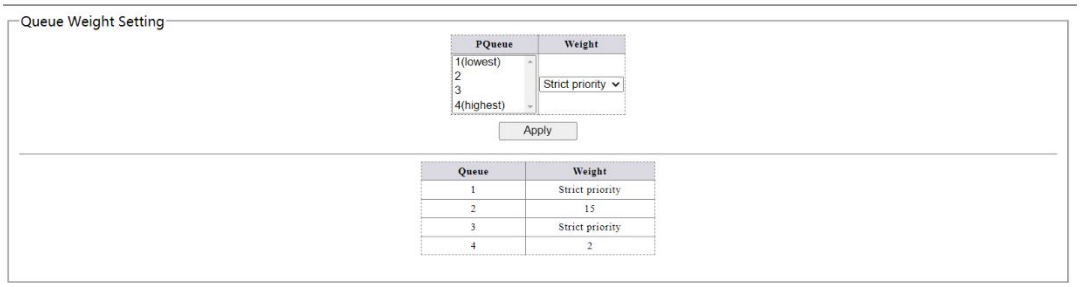


Figure 28 Default strict priority setting

5 Open the test software and hit the flow test. The results are as follows: the sending rate of port 1 is about 980Mbps, and the sending rate of port 8 is about 10Mbps.

FIG. 29 Results without setting the queue weight

5. Modify the queue weight as shown below.

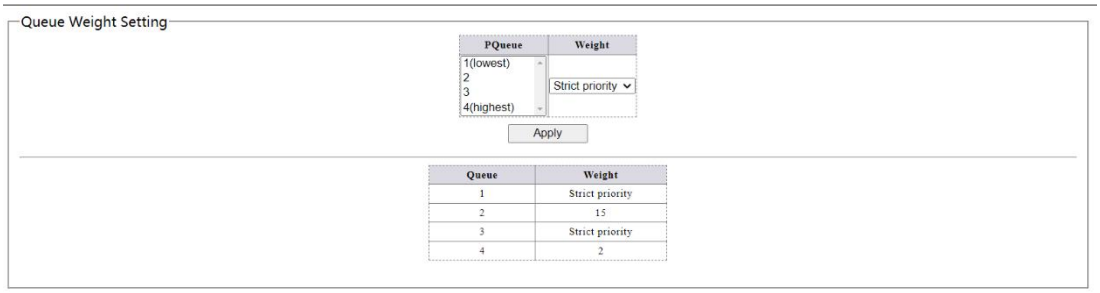
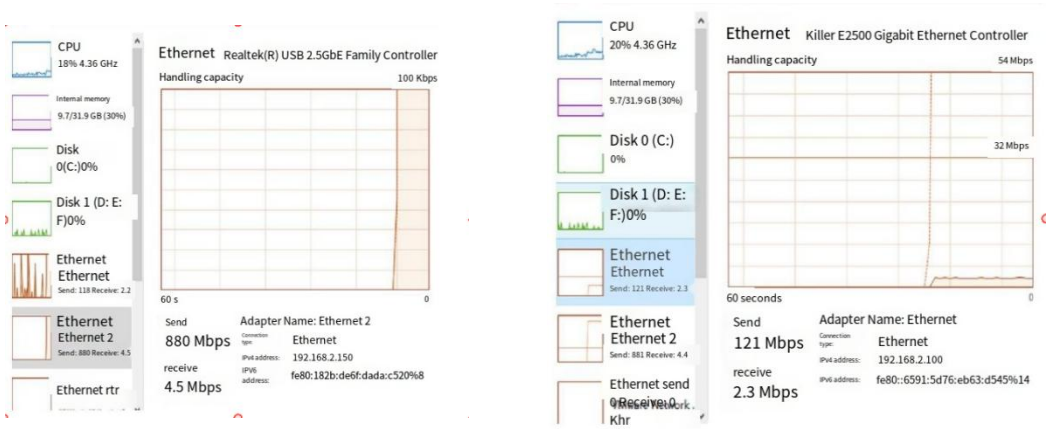


Figure 30 Queue weight Settings

6, Re-test results as shown in the figure below, port 8 sending rate becomes 880Mbps, port 1sending rate becomes 121 Mbps.



Pair 1	No Group	Finished	371	192.168.2.150	192.168.2.210	TCP	High_Performance_Throughput.scr	192.168.2.150	TCP	n/a	192.168.2.210	n/a
Pair 2	No Group	Finished	41	192.168.2.100	192.168.2.210	TCP	High_Performance_Throughput.scr	192.168.2.100	TCP	n/a	192.168.2.210	n/a
Pair 3	No Group	Finished	376	192.168.2.150	192.168.2.210	TCP	High_Performance_Throughput.scr	192.168.2.150	TCP	n/a	192.168.2.210	n/a
Pair 4	No Group	Finished	41	192.168.2.100	192.168.2.210	TCP	High_Performance_Throughput.scr	192.168.2.100	TCP	n/a	192.168.2.210	n/a
Pair 5	No Group	Finished	378	192.168.2.150	192.168.2.210	TCP	High_Performance_Throughput.scr	192.168.2.150	TCP	n/a	192.168.2.210	n/a
Pair 6	No Group	Finished	89	192.168.2.100	192.168.2.210	TCP	High_Performance_Throughput.scr	192.168.2.100	TCP	n/a	192.168.2.210	n/a
Pair 7	No Group	Finished	386	192.168.2.150	192.168.2.210	TCP	High_Performance_Throughput.scr	192.168.2.150	TCP	n/a	192.168.2.210	n/a
Pair 8	No Group	Finished	37	192.168.2.100	192.168.2.210	TCP	High_Performance_Throughput.scr	192.168.2.100	TCP	n/a	192.168.2.210	n/a
Pair 9	No Group	Finished	372	192.168.2.150	192.168.2.210	TCP	High_Performance_Throughput.scr	192.168.2.150	TCP	n/a	192.168.2.210	n/a
Pair 10	No Group	Finished	40	192.168.2.100	192.168.2.210	TCP	High_Performance_Throughput.scr	192.168.2.100	TCP	n/a	192.168.2.210	n/a

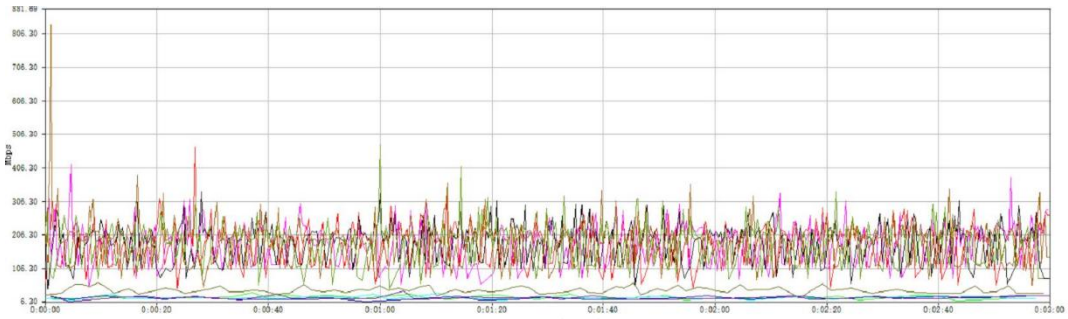


FIG. 31 Test results after setting the queue weight

6.3 IGMP

IGMP is a network multicast protocol used to establish and maintain multicast membership between hosts and multicast routers. IGMP Snooping controls layer 3 multicast groups by listening and analyzing the multicast packets sent between the host and the device. It is beneficial to suppress unnecessary multicast data forwarding in layer 2 networks and save network bandwidth.

Click on the navigation bar: Configuration --> IGMP

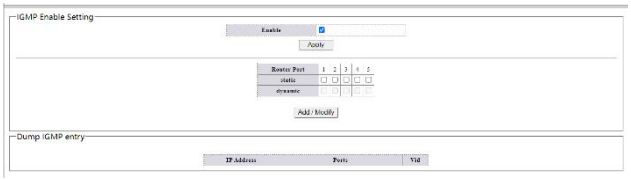


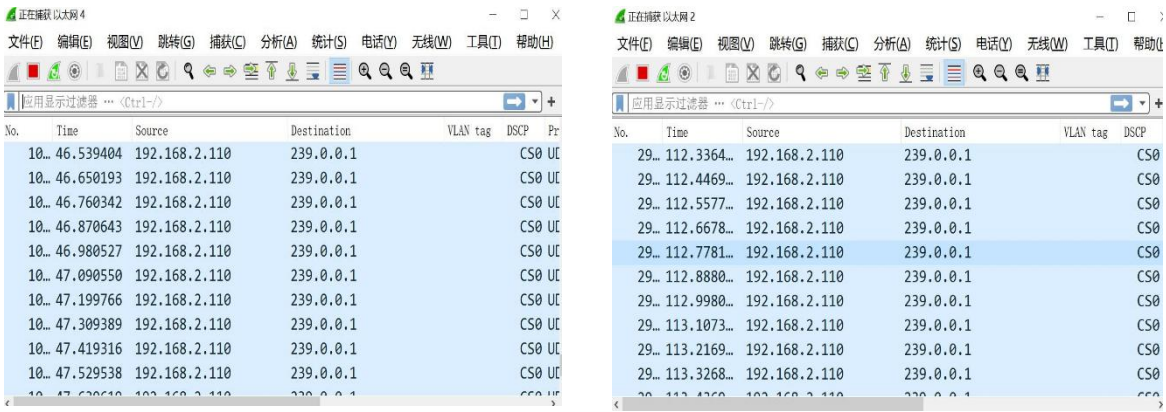
Figure 32 IGMP Settings

Instructions:

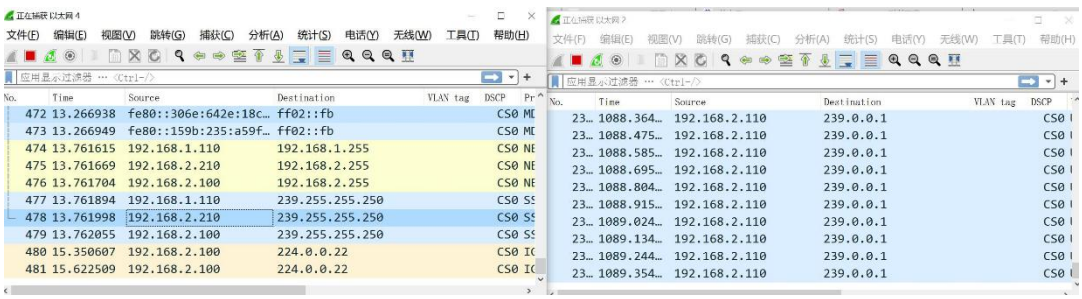
IGMP Enable Settings choose to enable or disable the IGMP listeningfeature.
IP Address View the multicast IP address
Ports View a list of multicast group ports
VID to view the VLAN ID corresponding to the multicast group

6.3.1 Example

Multicast packets are broadcast on the switch when IGMP is not enabled



When IGMP function is turned on, the multicast address table is displayed, and multicast packets are forwarded only on the corresponding multicast member port



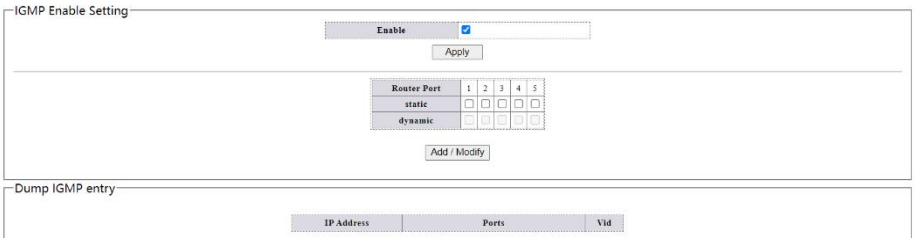


Figure 33 Multicast address table

Description:

IP Address Multicast IP Port

Multicast Port VID VLAN

ID

6.4 Port Aggregation

trunk is a way of bundling a set of physical interfaces together as a logical interface to increase bandwidth and reliability, and the port configuration for the trunk needs to be the same.

You can do this by configuring link aggregation if you have the following requirements:

When two switch devices are connected by a link reliability does not meet the requirements.

Click on the navigation bar: Configuration --> Link Aggregation Settings

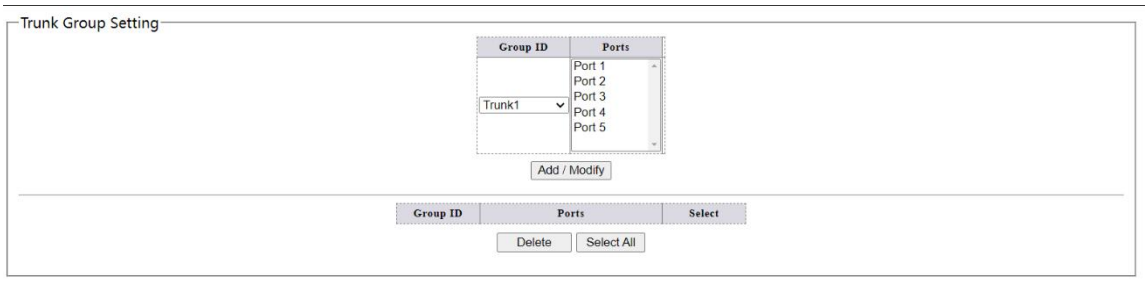


Figure 34 Link aggregation Settings

Note:

Group ID Sink group ID.

Port belongs to the physical port of the aggregation group

Member ports that belong to the same sink group must have a consistent configuration.

Note: trunk 1 supports 1 to 4 ports, trunk 2 supports 5 to 8 ports, and trunk3 (10-port switch) supports 9 to 10 ports

6.4.1 Example

Set up the switch port aggregation function and test the topology as shown below.

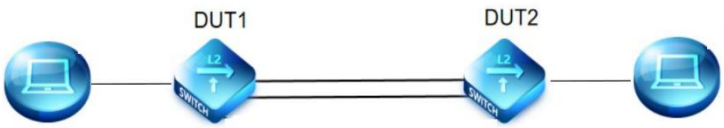


Figure 35 Test topology

1 Set switch 1's ports 7 and 8, adaptively.

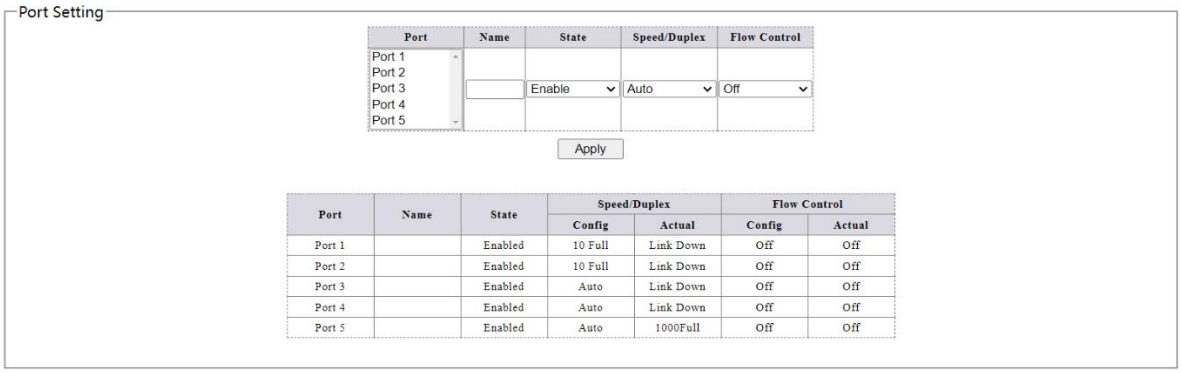


FIG. 36 Port Settings

For the convenience of testing, set the bandwidth of ports 7 and 8 to 10240Kbps

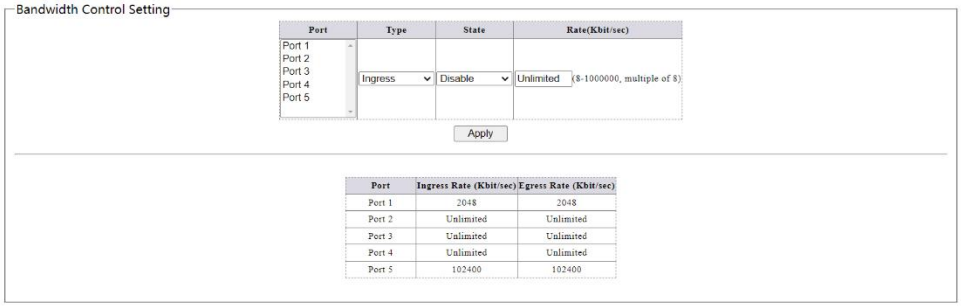


Figure 37 Bandwidth Settings

2. Set ports 7 and 8 as aggregation ports. The other switch is also set.

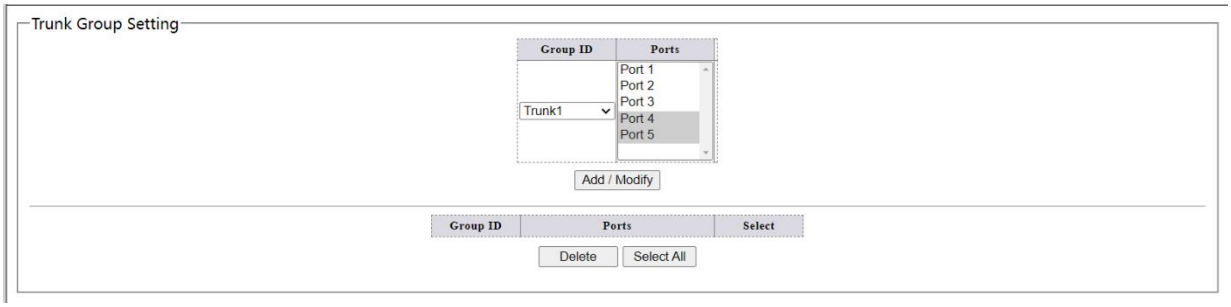


Figure 38 Aggregation Settings

4 Connect the test device according to the test topology.

5. Open the test software to test the flow. First, connect the double network cable to see the rate, disconnect one of the network cables to see the rate change, and then connect the disconnected network cable to see the rate change. The results are shown in the following figure.

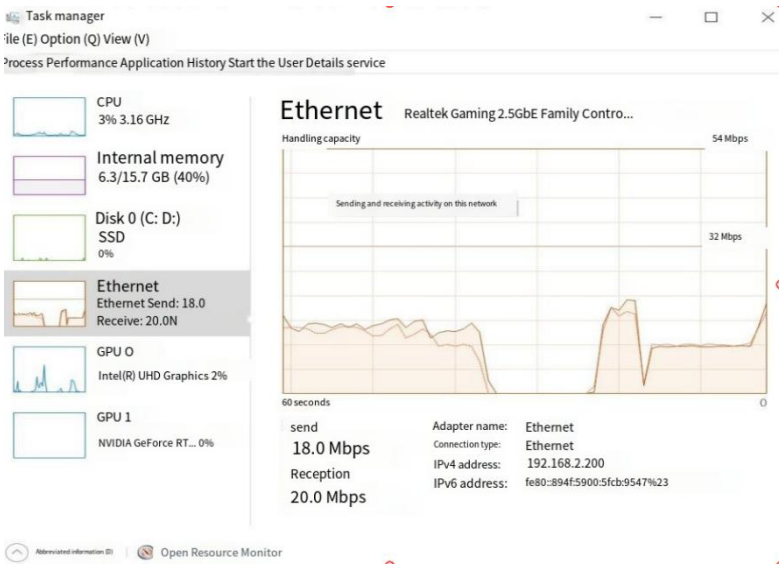


Figure 39 Rate when dual network cable is connected

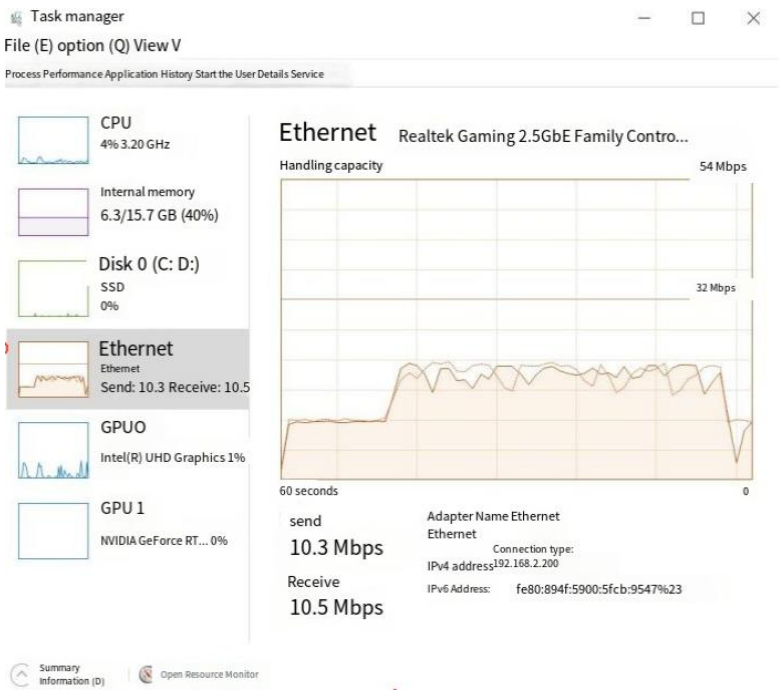


Figure 40 The rate after disconnecting a network cable

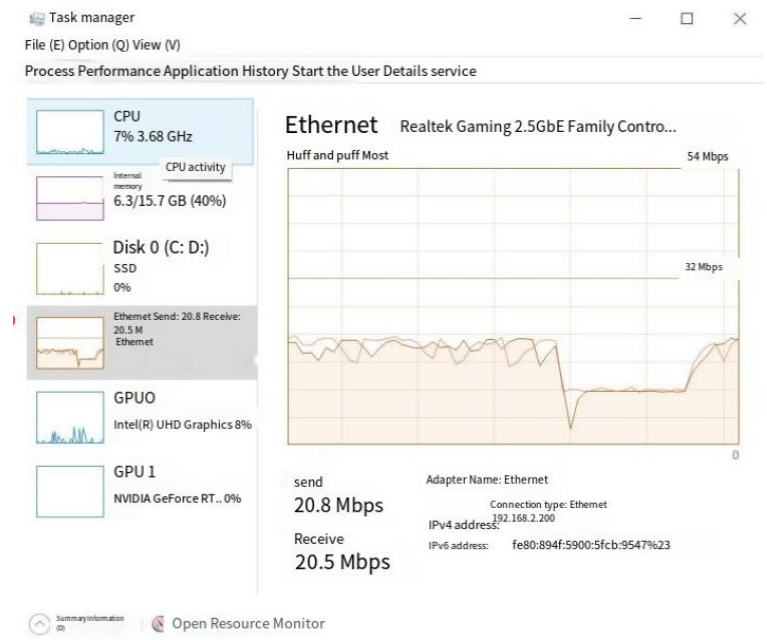


Figure 41 Rate after reconnecting the dual network cable

6. According to the test, when the bandwidth of single port is set to 10Mbps, the use of port aggregation function improves the reliability of the network and increases the bandwidth.

6.5 Loop protection

The loop is the topology of the switch connected to the network to form a ring. The loop will cause a broadcast storm in the internal network, which will consume a lot of CPU and line bandwidth of the switch. In serious cases, it can even cause equipment to crash and the network to be paralyzed.

Click the navigation bar: Configuration -> Loop protection

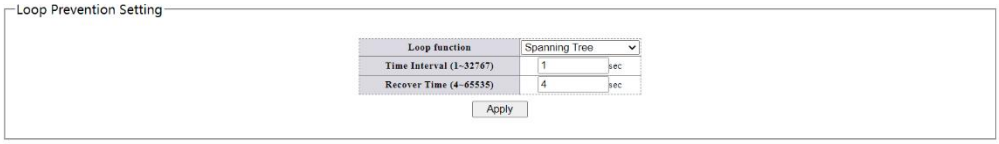


Figure 42 Loop protection Settings

Description:

Time intervals	time monitors the network loop at this time interval
The recovery	When the loop is found, the switch will initiate the processing mechanism, and the port will automatically return to normal after this time.

6.5.1 Example

1. Turn on the switch loop detection function first, connect the ports 3 and 4 to another switch with network cable to form a loop or self-loop, and the following figure appears (because the network is paralyzed due to the loop, it is not necessary to refresh this figure). The corresponding loop port indicator light will flash slowly, and the loop detection cannot prevent the loop, and the switch network will be paralyzed after the loop is formed

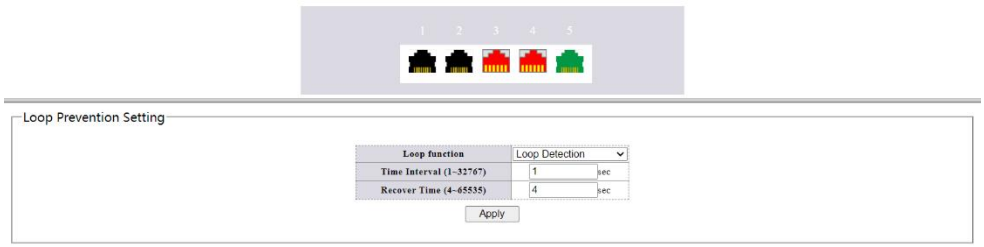


FIG. 43 Loop detection

2. Turn on the switch loop prevention, turn on all port loop prevention, and connect port 3 and 4 to another switch with network cable to form a loop. The management host can still ping 192.168.137.10 equipment.

Figure 44 Enabling loop prevention

6.6 Spanning tree

In order to backup links and improve network reliability, redundant links are usually used in Ethernet switching networks. However, the use of redundant links will generate loops on the switching network, cause broadcast storm and MAC address table instability and other failures, resulting in poor communication quality, and even communication interruption. To solve the loop problem in switching networks, Spanning Tree Protocol (STP) is proposed.

As with the development of the many protocols, Spanning Tree Protocol is updated constantly with the development of the network, from the initial the I EEE 802.1 D defined in STP to Rapid Spanning Tree Protocol defined in IEEE 802.1 W RSTP (Rapid Spanning Tree Protocol), To the latest IEEE 802.1 S defined in the multiple spanning tree protocol MSTP.

Click on the navigation bar: Configuration --> RSTP Global

Configure --> RSTP Port

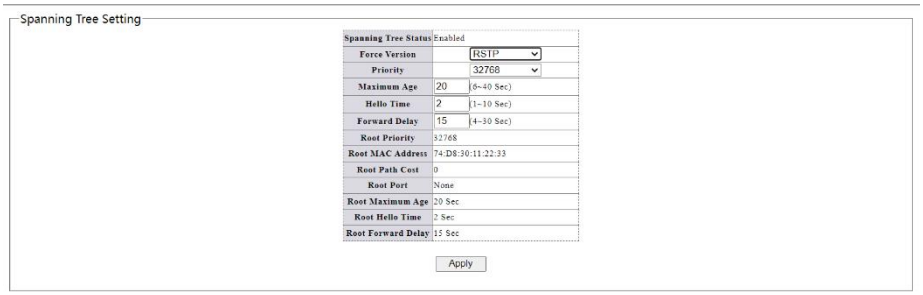


Figure 45 Spanning tree global Settings

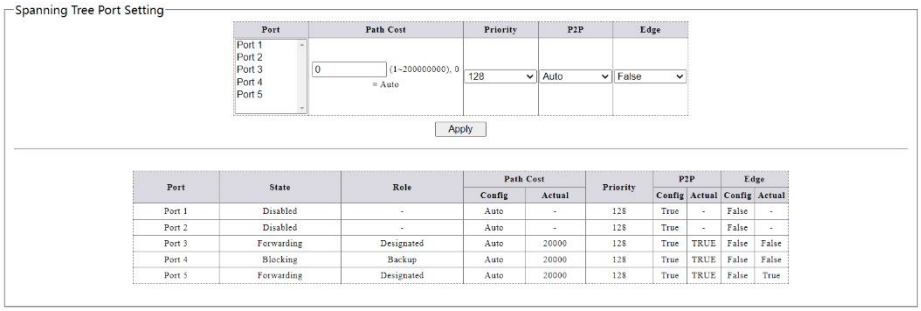


Figure 46 Spanning tree port Settings

Root bridge: First, compare the priority of switches, and the switch with the smaller priority is used as the root bridge switch; If the priority is the same, choose the one with the smaller MAC address as the root bridge switch.

Root port: Select a root port on each non-root bridge switch. First, compare the cost value of the link from the switch port to the root bridge (the smaller the better); If the cost value, is more upside switch bridge ID (priority - > MAC address); If there are two links, the port of the link with the smaller uplink switch port number is elected to be the root port.

Designated port: select a designated port on each link (generally, the interface of the root bridge is the designated port) compare the cost of the root port of the switch at both ends of the link to the root bridge, and the side with the smaller cost becomes the designated port; If the overhead, the more link ID size switches at the ends of the bridge, the bridge ID small become a specified port, become blocked ports on the port.

Blocking port: After the above election is completed, the port on the link that has not been elected becomes the blocking port

6.6.1 sample

1, Click on the navigation bar: Configuration --> Loop Protection to enable the spanning tree.

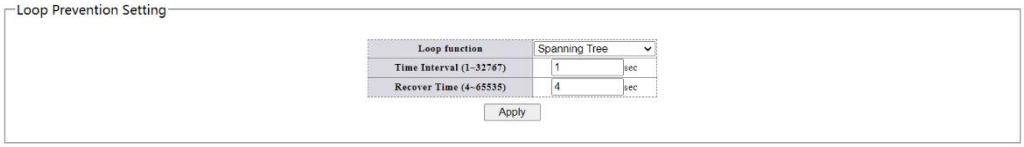


Figure 47 Enabling the spanning tree

2, click on the navigation bar: Configuration --> RSTP Global Set switch priority.

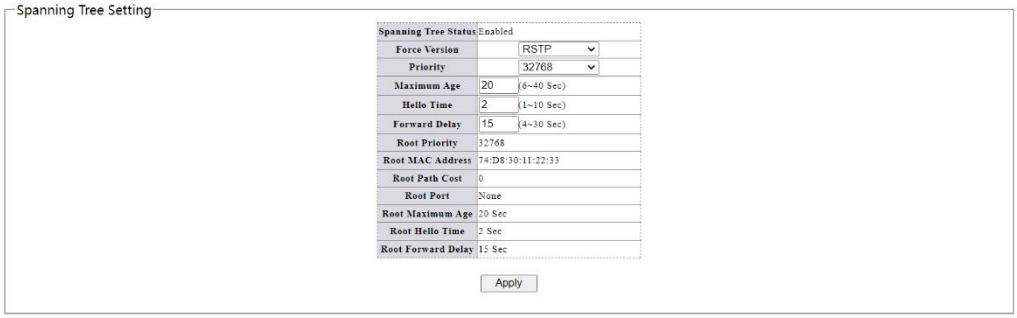


FIG. 48 RSTP global Settings

3, click on the navigation bar: Configuration --> RSTP port set path cost.

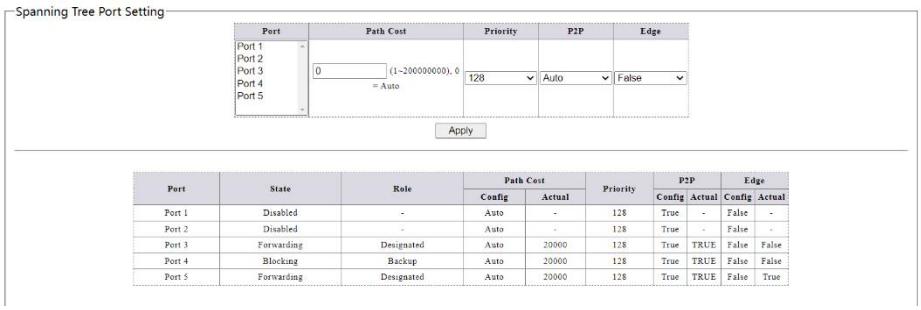


FIG. 49 RSTP port Settings

4, with three switches to form the following diagram topology.

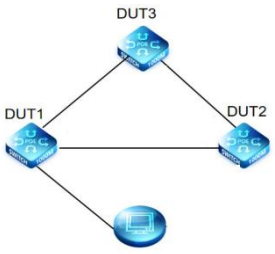


FIG. 50 Test topology

5. After calculation, the switch will automatically elect the root switch, root port, and blocking port.

Spanning Tree Setting

Spanning Tree Status	Enabled	
Force Version		RSTP
Priority		32768
Maximum Age	20	(6~40 Sec)
Hello Time	2	(1~10 Sec)
Forward Delay	15	(4~30 Sec)
Root Priority	32768	
Root MAC Address	74:D8:30:11:22:33	
Root Path Cost	0	
Root Port	None	
Root Maximum Age	20 Sec	
Root Hello Time	2 Sec	
Root Forward Delay	15 Sec	

Apply

Spanning Tree Port Setting

Port	Path Cost	Priority	P2P	Edge
Port 1 Port 2 Port 3 Port 4 Port 5	0 (1~200000000), 0 = Auto	128	Auto	False

Apply

Port	State	Role	Path Cost		Priority	P2P		Edge	
			Config	Actual		Config	Actual	Config	Actual
Port 1	Disabled	-	Auto	-	128	True	-	False	-
Port 2	Disabled	-	Auto	-	128	True	-	False	-
Port 3	Forwarding	Designated	Auto	20000	128	True	TRUE	False	False
Port 4	Blocking	Backup	Auto	20000	128	True	TRUE	False	False
Port 5	Forwarding	Designated	Auto	20000	128	True	TRUE	False	True

FIG. 51 RSTP results

6 Disconnect the root port, change the topology, and the switch reselects the root port.

Port	State	Role	Path Cost		Priority	P2P		Edge	
			Config	Actual		Config	Actual	Config	Actual
Port 1	Disabled	-	Auto	-	128	True	-	False	-
Port 2	Disabled	-	Auto	-	128	True	-	False	-
Port 3	Forwarding	Designated	Auto	20000	128	True	TRUE	False	False
Port 4	Blocking	Backup	Auto	20000	128	True	TRUE	False	False
Port 5	Forwarding	Designated	Auto	20000	128	True	TRUE	False	True

Figure 52 Topology change

6.7 Port mirroring

Port mirroring is to copy the packet of the specified port of the switch to the destination port; The copied port is called the source port, and the copied port is called the destination port. The destination port is connected to data detection devices, and users use these devices to analyze the packets received from the destination port for network monitoring and troubleshooting

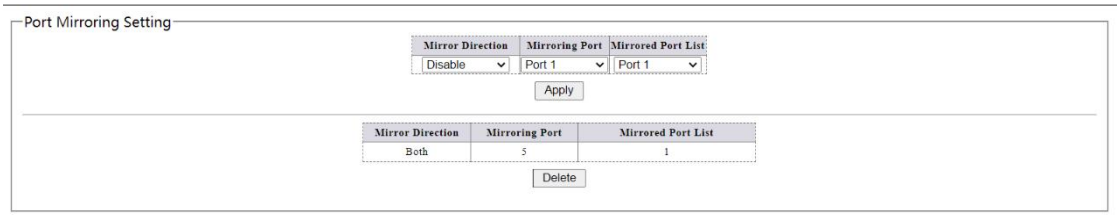


Figure 53 port mirror

Note:

Mirror direction The data flow direction of the mirrored port (incoming, outgoing, bi-directional)

6.7.1 Example

Port 1 is connected to the device with IP address 192.168.137.10, port 5 is connected to the device 192.168.137.251, port 8 is connected to the management host, set port 8 as the monitoring port and port 1 as the monitored port. Use Wireshark to capture packets in the management host. It can be found in Wireshark to grab the ping packet as shown in Figure

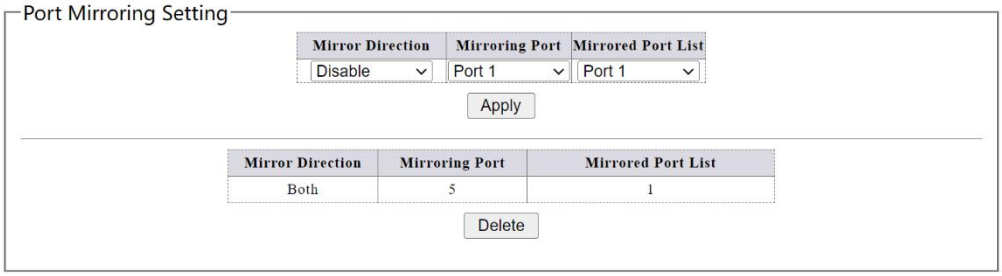


Figure 54 Port mirroring Settings

No.	Time	Source	Destination	VLAN tag	DSCP	Protocol	Length	Info
55…	381.3611…	192.168.137.10	192.168.137.251		CS0	ICMP	74	Echo (ping) reply id=0x0
55…	381.3611…	192.168.137.10	192.168.137.251		CS0	ICMP	74	Echo (ping) reply id=0x0
55…	381.3648…	192.168.137.10	192.168.137.251		CS0	ICMP	74	Echo (ping) reply id=0x0
55…	381.3648…	192.168.137.10	192.168.137.251		CS0	ICMP	74	Echo (ping) reply id=0x0
55…	382.0126…	192.168.137.251	192.168.137.10		CS0	ICMP	74	Echo (ping) request id=0x0
55…	382.0127…	192.168.137.1	192.168.137.251		CS0	ICMP	102	Redirect (Redir
55…	382.0127…	192.168.137.251	192.168.137.10		CS0	ICMP	74	Echo (ping) request id=0x0
55…	382.0128…	192.168.137.251	192.168.137.10		CS0	ICMP	74	Echo (ping) request id=0x0
55…	382.0128…	192.168.137.251	192.168.137.10		CS0	ICMP	74	Echo (ping) request id=0x0
55…	382.0130…	192.168.137.251	192.168.137.10		CS0	ICMP	74	Echo (ping) request id=0x0
55…	382.0130…	192.168.137.251	192.168.137.10		CS0	ICMP	74	Echo (ping) request id=0x0

Figure 55 Wireshark packet capture result

6.8 Port isolation

Click on Navigation bar: Configuration --> Port Isolation

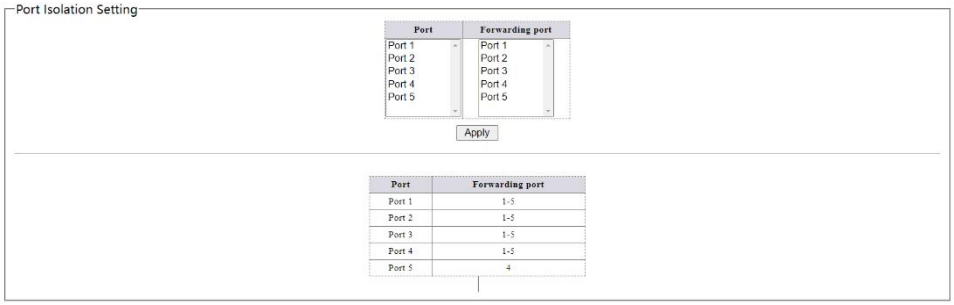


Figure 56 Port Isolation

Instructions:

Port Source port Port isolation
forwarding port

Configure a forwarding port for the source port. Packets received by the source port cannot be forwarded to a port that is not in the forwarding port.

6.8.1 Example

Set port 1 and ports 2 and 3 to forward packets to each other, and port 1 data cannot be forwarded to other ports (ports 4-8). Select port 1 on the web port, and select port 1, 2, and 3 on the port isolation. Ping packet test, 7 ports and 1 port Ping packet is not as shown below.

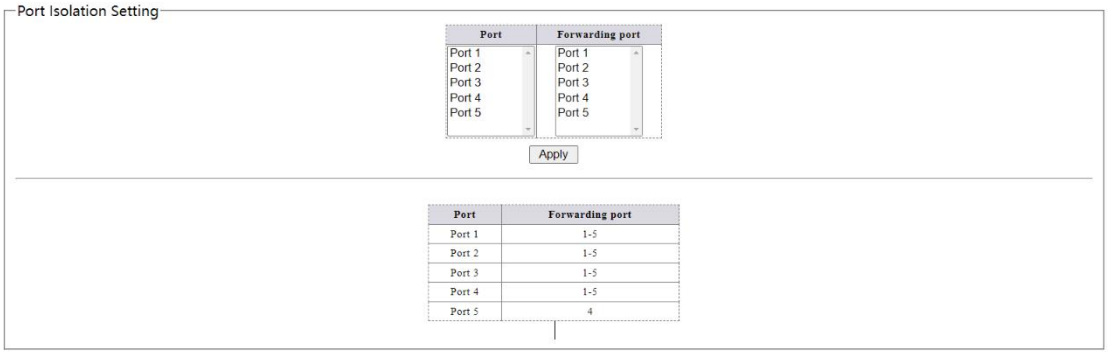


FIG. 57 Results of 7-port ping packet

The 3-port and 1-port ping packets can ping, as shown below.

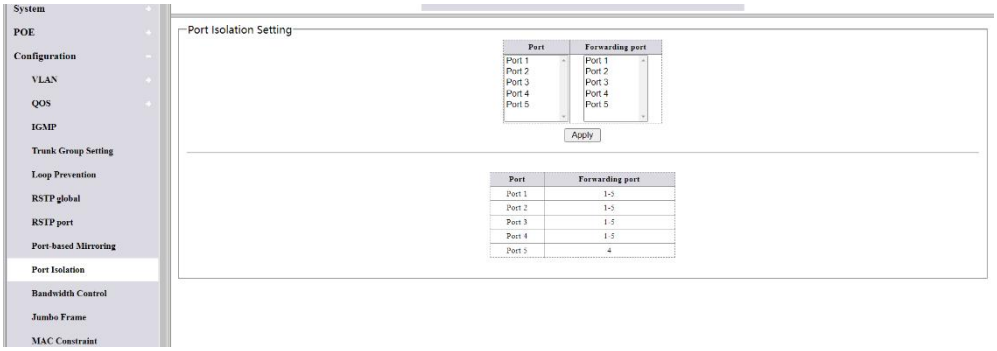


FIG. 58 Result of 3-port ping packet

6.9 Bandwidth Control

To configure port bandwidth is to limit the rate at which the physical interface can send out or receive data in.

Before the traffic is sent out of the interface, the speed limit is configured on the outgoing direction of the interface to control all the outgoing packet traffic. Before the traffic is received from the interface, the speed limit is configured on the incoming direction of the interface to control all the incoming packet traffic. Click on the navigation bar: Configuration --> Bandwidth Control

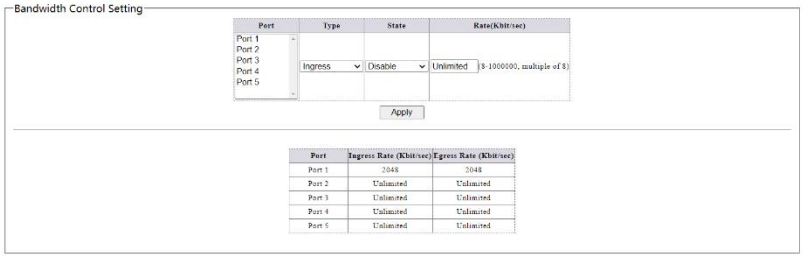


Figure 59 Bandwidth Control

6.9.1 Example

The port 1 ingress rate is limited to 2048kbps, which is set as shown below.

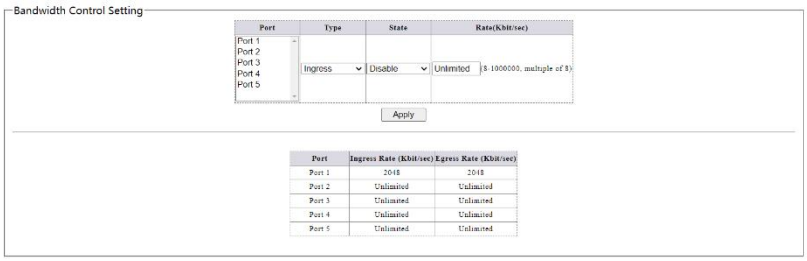


Figure 60 Bandwidth limit Settings

Download the file on the PC connected to port 1, open the task manager and click Ethernet. The receiving rate is 2.1Mbps as shown in the figure below

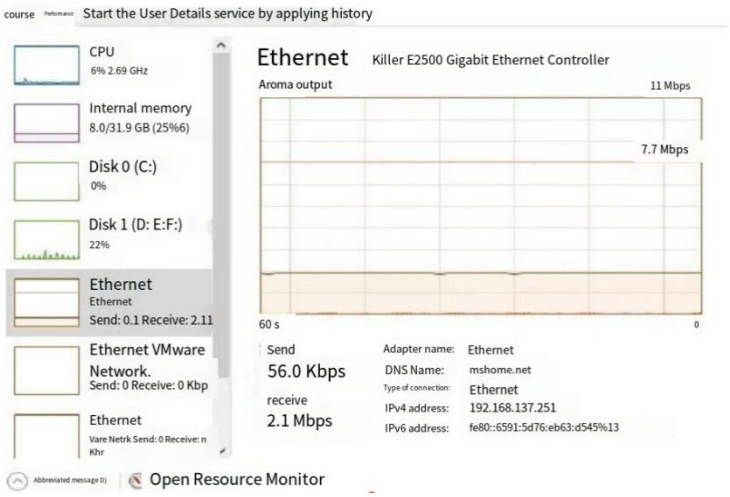


Figure 61 Results of port speed limit

6.10 Jumbo Frame

Configure the maximum packet length the system can forward by clicking on the navigation bar: Configuration > Jumbo Frame

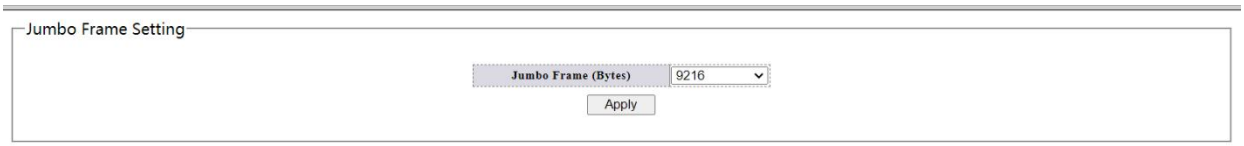


Figure 62 jumbo frame

6.10.1 Example

After enabling jumbo frame, set PC NIC to enable jumbo frame, set ping packet data 8000, no subpacket. Command ping-f 192.168.2.210 -l 8000 -t, catch the giant frame on the PC with IP 192.168.2.210.

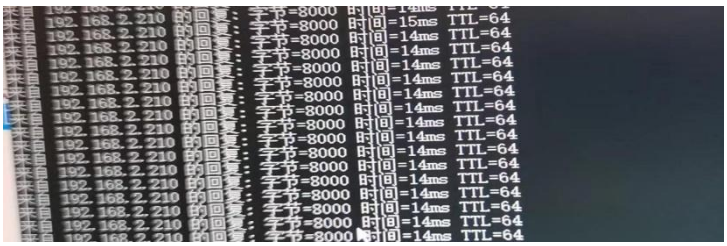


Figure 63 ping jumbo packets

14…	171.5954…	192.168.2.210	192.168.2.100	CS0 ICMP	642	Echo (ping) reply id=0x00
14…	172.6010…	192.168.2.100	192.168.2.210	CS0 ICMP	8042	Echo (ping) request id=0x00

Figure 64 captures data of length 8042

6.11 MAC Constraints

The system supports the port Mac learning limit function. The system learns the source MAC of the user's packet, and when the learned MAC reaches the limit threshold. If the source MAC of the user's packet already exists in the MAC table, the user's packet will continue to be forwarded. If the source MAC of the packet does not exist in the MAC table, the system will process the packet accordingly according to the MAC restriction action. For example, if the action is drop, then the user packet will be dropped at the incoming port.

Click on the navigation bar: Configuration --> Mac Constraints

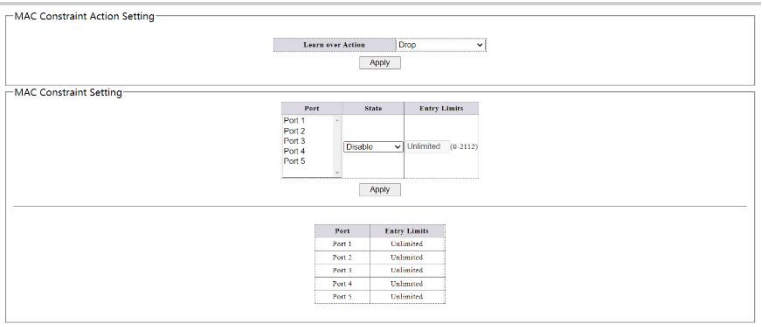


Figure 65 Mac Constraints

6.11.1 Example

mac address information learned by port 2 when there is no MAC address constraint set

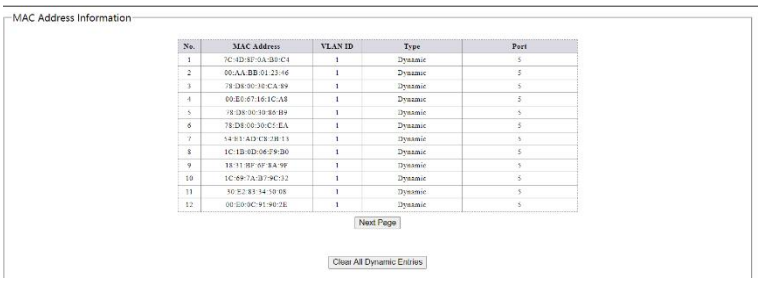


Figure 66 MAC address information for port 2

When the 2-port MAC address limit entry is set to 1, only one mac address information can be learned by port 2

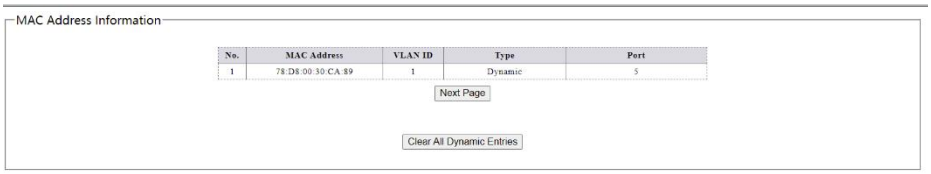


Figure 67 MAC address information for port 2 after restriction

6.12 Green Ethernet

Green Ethernet refers to features that are environmentally friendly and reduce the power consumption of devices. The system provides the connection and dynamic detection of the cable length, as well as the dynamic adjustment of the power required for the detected cable length. High performance and low power consumption. The link d own of the system support port saves power and greatly reduces the power consumption when the network cable is disconnected. When the input signal is detected, it wakes up from the link down power saving and enters the normal mode.

Click on the navigation bar: Configuration --> Green Ethernet

Figure 68 Green Ethernet

6.13 Energy Efficient Ethernet (EEE)

Energy Efficient Ethernet (EEE) supports operating in low-power idle mode. Systems at both ends of the link can disable some functions when the link utilization is low, saving power. Switching off is recommended.

Click on the navigation bar: Configuration --> EEE

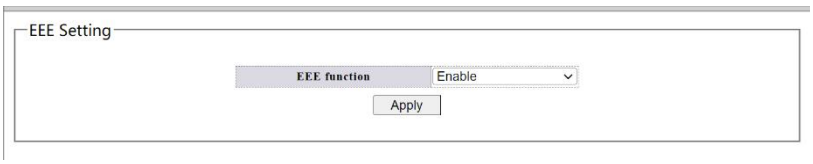


Figure 69 EEE Settings

6.14 SNMP

SNMP is a standard network management protocol widely used in TCP/IP networks. The protocol can support network management systems to monitor whether there is anything that causes management concern in the equipment connected to the network. The basic components of SNMP include NMS (Network Management System), Agent (Agent), Managed Object (object) and MIB (Management Information Base).

Click on the navigation bar: Configuration --> SNMP

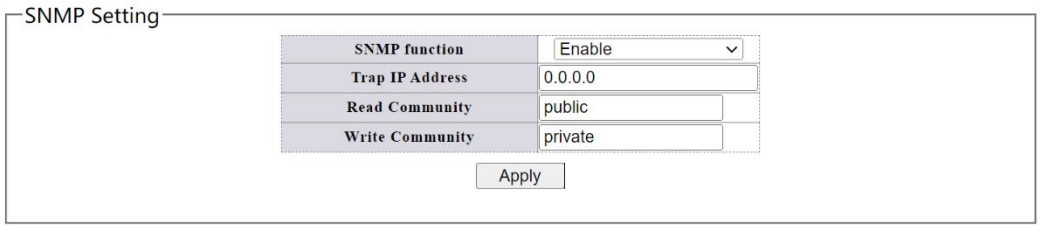


Figure 70 SNMP

6.14.1 Example

1, turn on the SNMP feature

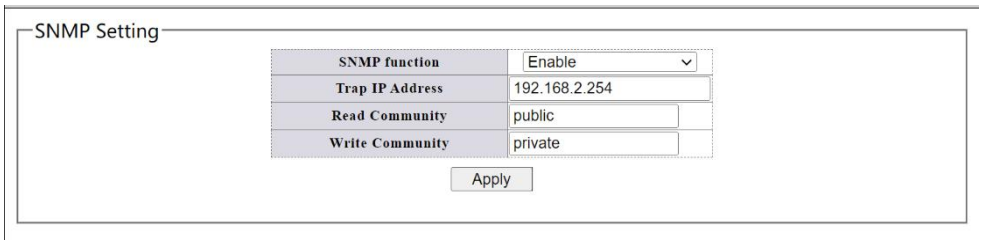


Figure 71 SNMP enabled

2, shut down the management PC, occupying the SNMP service on port 162

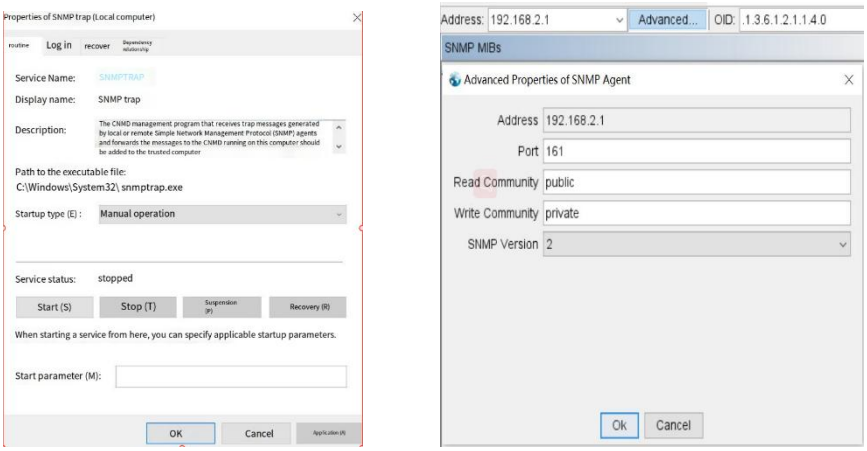


Figure 72 Turn off the SNMP service of the management host and MID Browser Settings

3, open IReasoning MIB Browser software Settings as in the upper right picture.4, click Get Next -> GO in MIB Browser to display the results as shown below

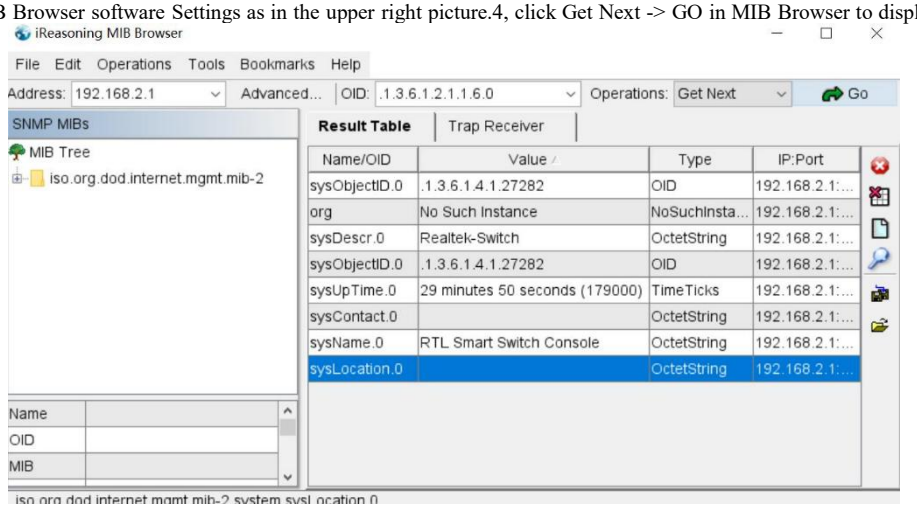


Figure 73 MIB Browser display

5, Select set -> GO in MIB Browser Operations before Get The results are shown below.

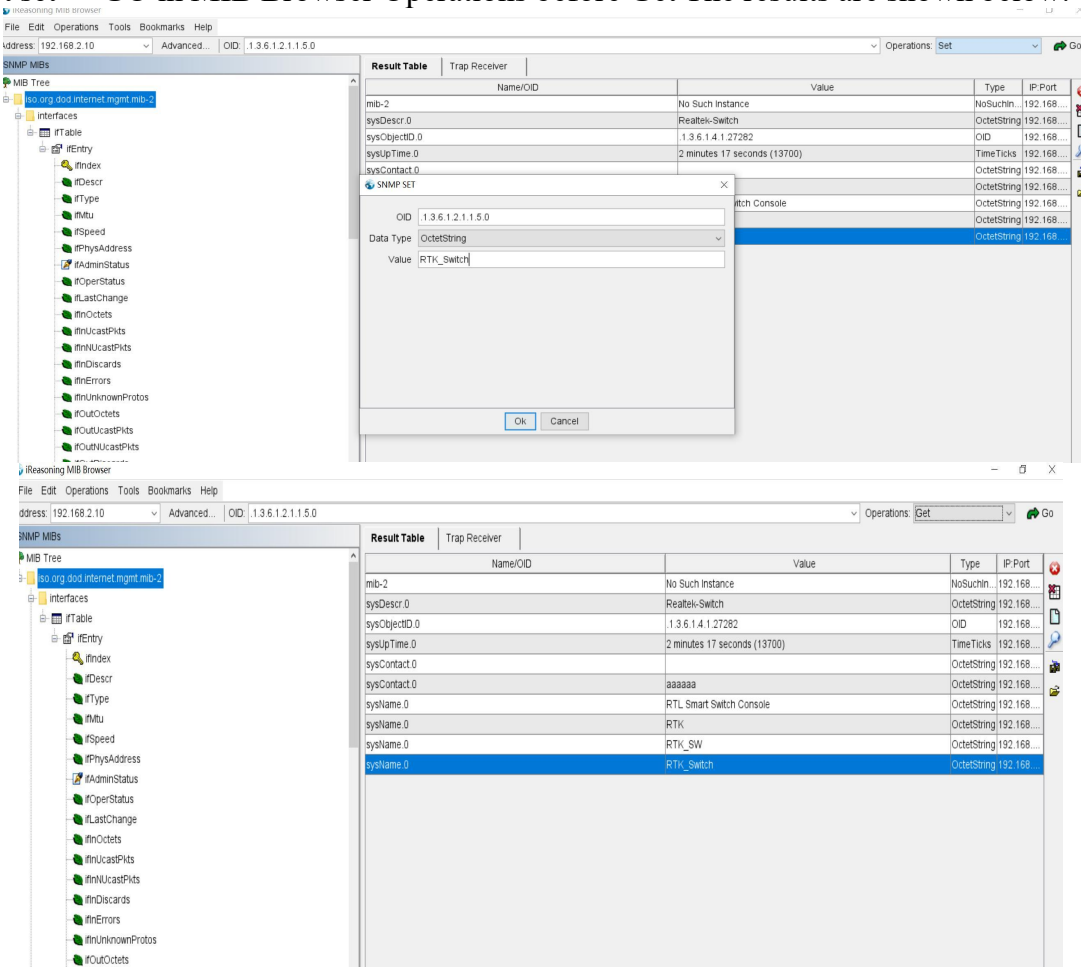


Figure 74 SNMP Trap Set

6, Set the IP address of the management PC to the Trap IP address of the switch configuration, and select the Trap Receiver in the MIB Browser Tools to receive the switch port state change information

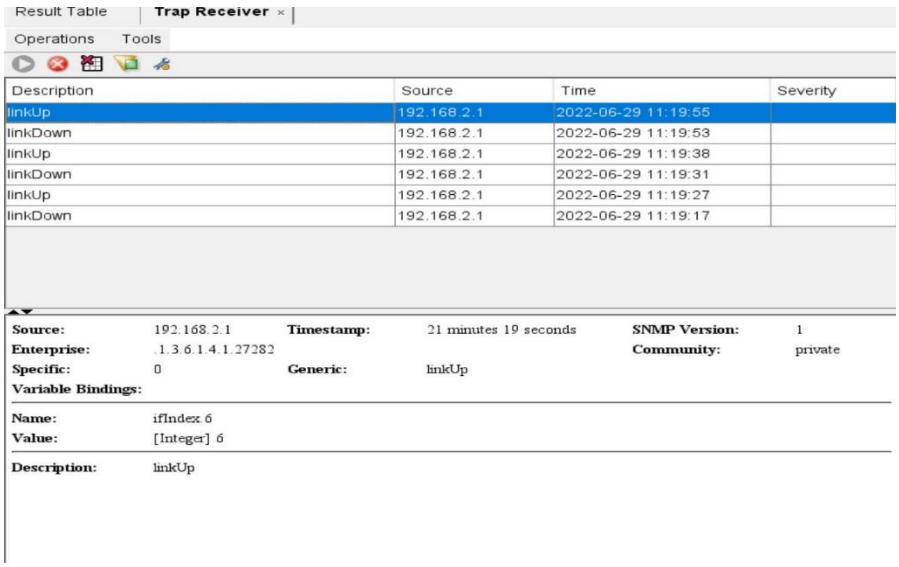


FIG. 75 Trap Receiver

Chapter 7 Safety

7.1 MAC address

MAC Address in English is Media Access Control Address, literally translated as media access control address, Also known as the local area network Address (LAN Address), Ethernet Address (Ethernet Address) or Physical address (physical address), it is an address used to confirm the location of network equipment.

7.1.1 Table of MAC addresses

Click on Navigation bar: Security -> MAC Address -> MAC Table

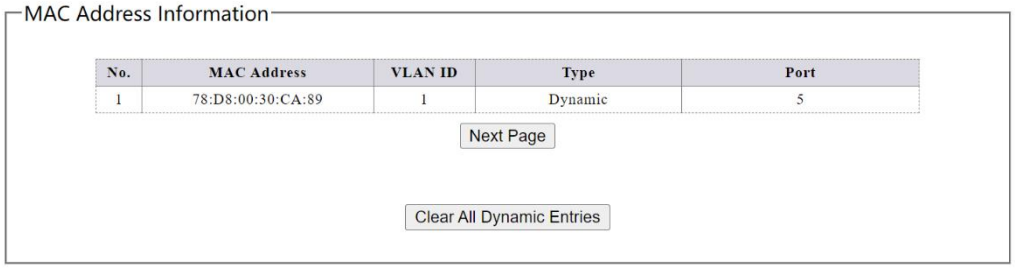


Figure 76 MAC address information

7.1.2MAC Lookup

Go to Security > MAC Address > MAC Lookup

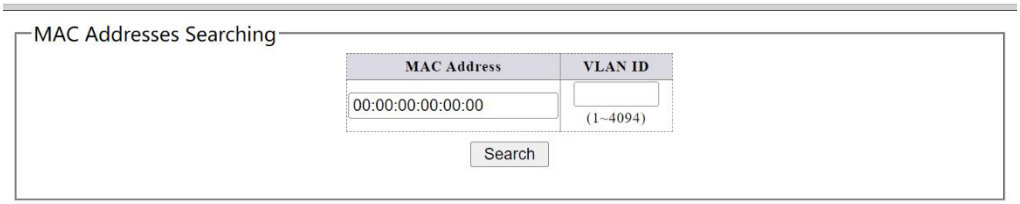


Figure 77 MAC address search

7.1.3 Static MAC

Go to the navigation bar: Security -> MAC Address -> Static MAC

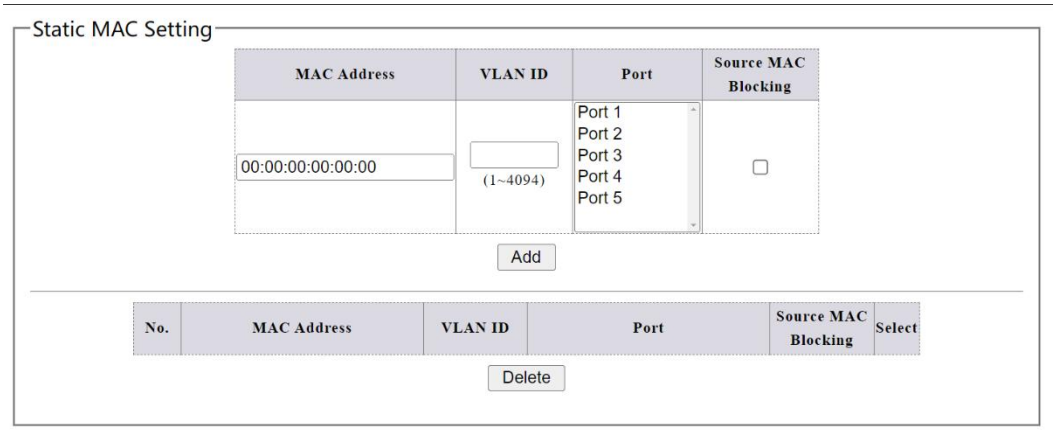


Figure 78 Static MAC

7.2Broadcast Storm

Broadcast storm refers to the rapid increase in the number of broadcast frames on the network because they are constantly forwarded, which affects the normal network communication and seriously reduces the network performance. Broadcast storm can occupy a considerable amount of network bandwidth, resulting in normal data packets can not work properly. Broadcast storm occurs when the broadcast data can not be processed and occupy a large amount of network bandwidth, resulting in normal business can not run, this occurs, resulting in local area network partial or the whole network paralysis

Click on navigation bar: Security -> Broadcast storm

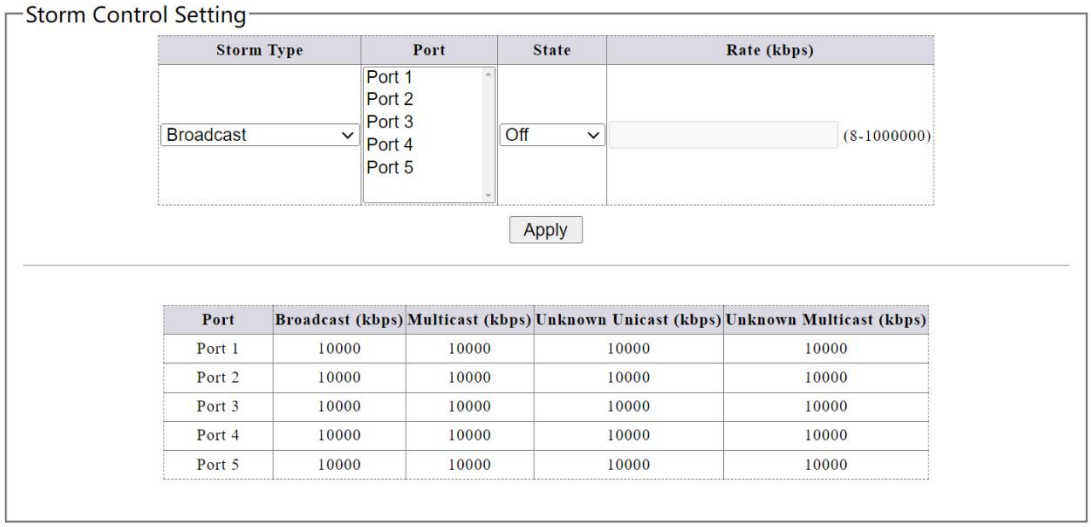


Figure 79 Storm suppression

Caption:

Storm types Broadcast, multicast, Unknown unicast, Unknown multicast

Port Select port, multiple selectable

Status turns broadcast storm suppression on or off

Speed set port broadcast, multicast packet, unknown unicast, unknown multicast bandwidth.

Chapter 8 Monitoring

8.1 Port Statistics

Port statistics shows the traffic information of each port, which is convenient to monitor traffic and analyze network anomalies. Click on the navigation bar: Monitor -> Port Statistics

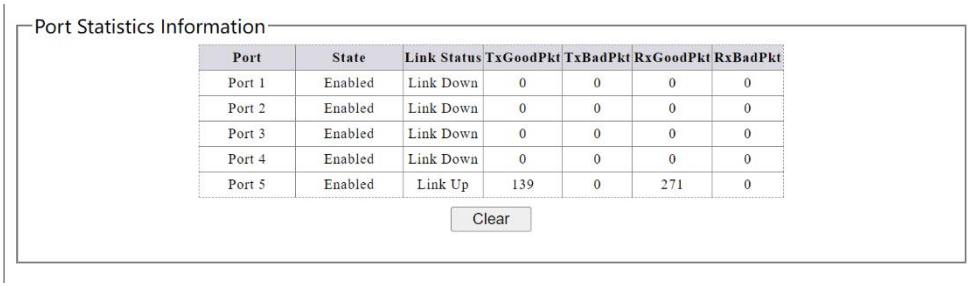


Figure 80 Port statistics

Caption:
Port Port number

Status shows the status of the port. Only when the state is open can the packet be forwarded normally
Receive status port current LINK status

The number of correct packets sent shows the number of correct packets sent by the port

The number of wrong packets sent shows the number of wrong packets sent by the port

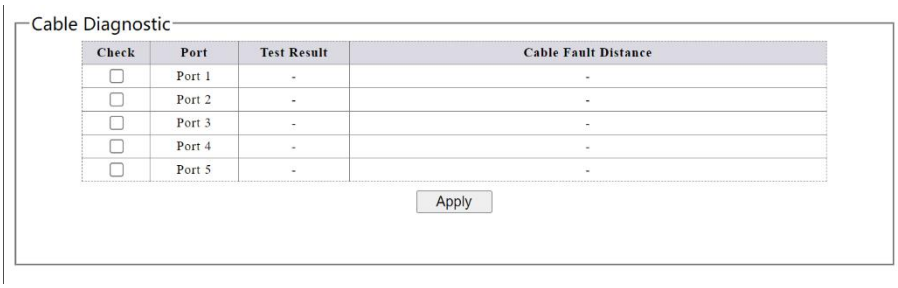
The number of correct packets received shows the number of correct packets received by the port

The number of received incorrect packets shows the number of received incorrect packets at the port

8.2 Cable Diagnostics

When the cable is connected to the switch port, the cable test function can test the cable connection status, the cable length is convenient to diagnose the network fault point, and the results are for reference only.

Click on the navigation bar: Monitoring -> Cable Diagnosis



Instructions:

The port connected to the management host does not support diagnostics.

Chapter 9 Tools

9.1 Firmware Upgrade

You can upgrade the switch's software here.

Click on the navigation bar: Tools -> Firmware Upgrade

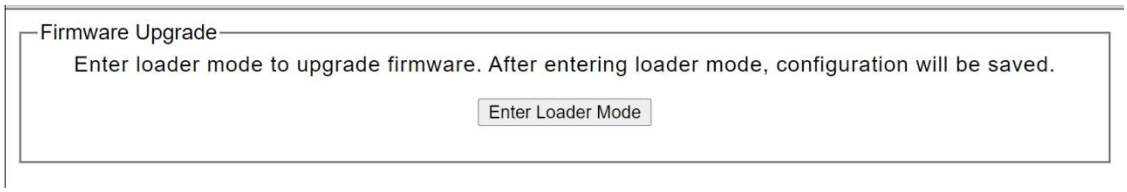


Figure 81 Enter firmware upgrade mode

Click the < Enter loader Mode > button to appear the following picture

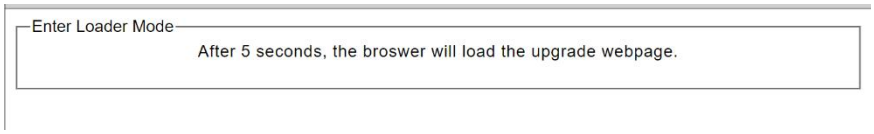


Figure 82 Enter loader mode jump

Finally jump to the firmware upgrade page

Click System --> HTTP Firmware Upgrade in the navigation bar to see the following picture

Figure 83 Firmware Upgrade page

Click the < Select File > button to load the latest firmware file. Click <Upgrade> again to start the upgrade and click < OK > in the pop-up window.

The following image will be displayed after the upgrade is completed.

Figure 84 Upgrade complete

Note:

During the firmware upgrade, please do not power off the device, keep the power stable, and do not refresh the page. You may lose unsaved configuration information when upgrading firmware. Please save configuration before upgrading.

Click System --> Reboot to restart the switch

9.2 Configure backup

You can save the current configuration information here. It is recommended to backup the current configuration information before modifying the configuration and upgrading the software. Click on the navigation bar: Tools -> Configure Backup

Figure 85 Configuring backup and recovery

Backup Settings: Click < Backup > to download the current configuration file locally via your browser.

Restore Settings: Click < Select File > to select the profile and click Upgrade. After that restart the switch to take effect.

9.3 Reset

In addition to hardware restore the factory Settings switch, you can also restore the default Settings on the Web. Go to Tools > Reset in the navigation bar

Figure 86 Restore the default Settings

Click the < Restore Default Settings > button and the exchange will restore all Settings defaults. The current configuration information will be lost. It is recommended that you back up your configuration before restoring the defaults.

The default administrative IP address is 192.168.2.1, and the account name and password are admin.

9.4 Save

Go to Navigation bar: Tools --> Save

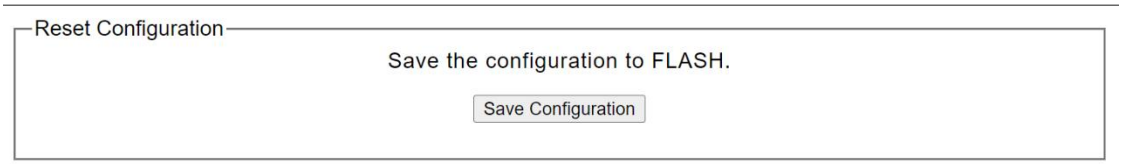


Figure 87 Save configuration to FLASH

It is recommended that after modifying the Settings, save the Settings to FLASH. Otherwise power off or restart the modified Settings will be lost.

9.5 Restart

After clicking Restart, the switch will restart, and it is recommended to save the configuration before restarting to prevent the current modified configuration from being lost. Click on the navigation bar: Tools --> Restart

Figure 88 Restart the switch

Note:
Please do not turn off the power during the restart process, ensure that the power is stable during the restart process, and avoid forced power off.