XikeStor

Simple L2 Managed Switches

User Manual Official Version

This user manual takes SKS3200M-8GPY1XF as an example and is applicable to all Simple L2 Managed Switches (SKS3200M-4GPY2XF,SKS3200M-5GPY1XF, SKS3200-4E2X,SKS3200-5E1X,SKS3200-8E1X,etc.)

XikeStor

Catalogue

XikeStor

1 Preface

1.1 Intended Audience

This manual is intended for installers and system administrators who are responsible for installing, configuring, or maintaining networks. This manual assumes that you understand all of the transport and management protocols used by the network.

This manual also assumes that you are familiar with the terminology, theoretical principles, practical skills, and specific expertise of network devices, protocols, and interfaces related to networking. You must also have experience working with graphical user interfaces, command-line interfaces, simple network management protocols, and Web browsers.

1.2 Book Conventions

This manual uses the following conventions.

GUI conventions	Description
Clarification	The description of the operation content, make necessary additions and explanations.
Note	Remind the operation should pay attention to the matters, improper operation may lead to data loss or equipment damage.

2 Login Web Page

2.1 Logging in Web Management Client

Users can open the Web browser, enter the default address of the switch: http://192.168.10.12, and press the Enter key.

Clarification

Supported browsers: IE9.0 or above, Chrome23.0 or above, Firefox20.0 or above.

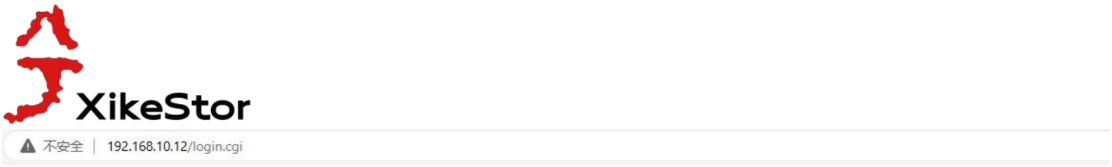
When logging in to the switch, make the IP segment of the PC consistent with that of the switch. Set the IP address of PC to 192.168.10.10 when logging in for the first time.

When logging in for the first time, set the IP address of PC to 192.168.10.x (x stands for 1~254, except 1), and set the subnet mask to 255.255.255.0, but the IP address of PC cannot be the same as that of the switch, that is, it cannot be the same as that of the switch.

However, the IP address of the PC cannot be the same as that of the switch, i.e. it cannot be 192.168.10.12.

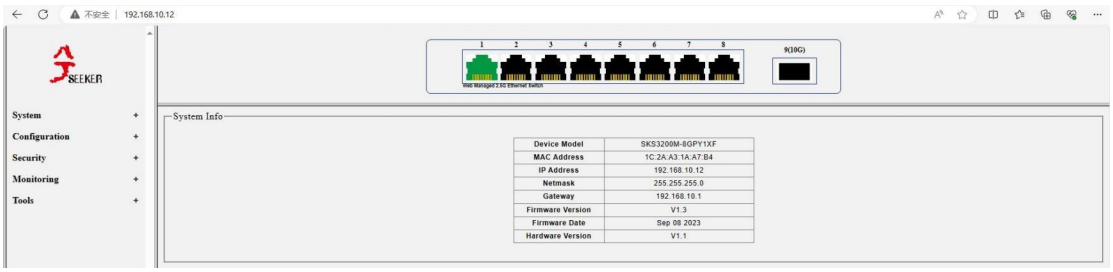
The login window will appear, as shown in the following figure. Enter the default user name: admin and password: admin. click the <Login> button.

Click the <Login> button and you will see the switch system information.



2.2 Client Interface Components

The typical operating interface of the Web Network Management System is described in the following figure.



2.3 Web Interface Navigation Tree

The menus of the Web Network Administrator mainly provide menu items such as System, Configuration, Security, Diagnostics, and Tools. There are submenus under each menu option. The detailed information of the navigation tree is shown below:

Menu	Submenu	Secondary submenu	Description
System	Information		Displays port status and product information.
	IP Setting		Configure to view the management IP address of the current device.
	User Account		Configure to view device user information.
	PortSetting		Configure to view information about all ports on the device.
configure	VLAN	802.1Q VLAN	Configuring View Port PVID VLAN.
		802.1Q VID	Configure the port VID to allow acceptance of frame types.
	QOS	Port to Queue	Configuring View Port Queues.
		Queue Weight	Configuring View Queue Weights.

	Loop	Loop Protocol	Configuration View Loop Detection.
		STP global	Configuring View Spanning Tree Global Information.
		STP port	Configuring to View Spanning Tree Port Information.
	IGMP Snooping		Configuration View IGMP Snooping.
	Trunk Group Setting		Configure to view link aggregation.
	Port-based Mirroring		Configure to view port mirroring.
	Port Isolation		Configuring View Port Isolation.
	Bandwidth Control		Configuring View Port Rate Limiting.
	Jumbo Frame		Configuring View Port Jumbo Frames.
	MAC Constration		Configuring View Port MAC Constraints.
	EEE		Configure to view port EEE power saving status and information.
Security	MAC address	MAC Search	Viewing MAC Address Information.
		Static MAC	Configuring to View Static MAC Information.
	Storm Control		Configure to view storm suppression information.
Monitoring	Port Statistics		View port statistics.
Tools	Firmware Upgrade		Updating and upgrading the software version of the device.
	Configuration Backup		Updating upgrade configuration files.
	Rest		Reset system.
	Save		Save Configuration.
	Reboot		Reboot system.
	Logout		Logout system.

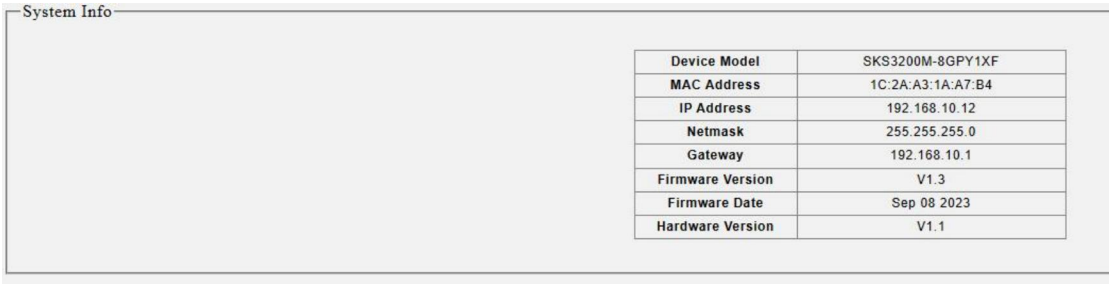
3 System

3.1 System information

Depending on the connected switch, the information of each port on the front panel of the switch and the product information can be displayed very intuitively.

The information displayed includes: product model, version, MAC address, etc. Steps of operation:

Click "System > Information" menu in the navigation tree to enter the system information view interface, as shown in the following figure:



3.2 IP Setting

Configure and view the management IP address of the device.

Steps to Operate:

Click "System > IP Setting" in the navigation tree to enter the IP Settings interface, as shown in the following figure:

The meaning of the interface information is shown in the following table:

Configuration item	Description
DHCP Setting	Enable: Enable DHCP acquisition Disable: De-enable DHCP acquisition
IP address	Managing IP Addresses
Subnet mask	IP address mask
Gateway	Gateway for IP address

3.3 User Account

Users can check and change the current user name and password of the switch.

Procedure:

Click the "System > User Account" menu in the navigation tree to enter the interface, as shown in the following figure:

The meaning of the interface information is shown in the following table:

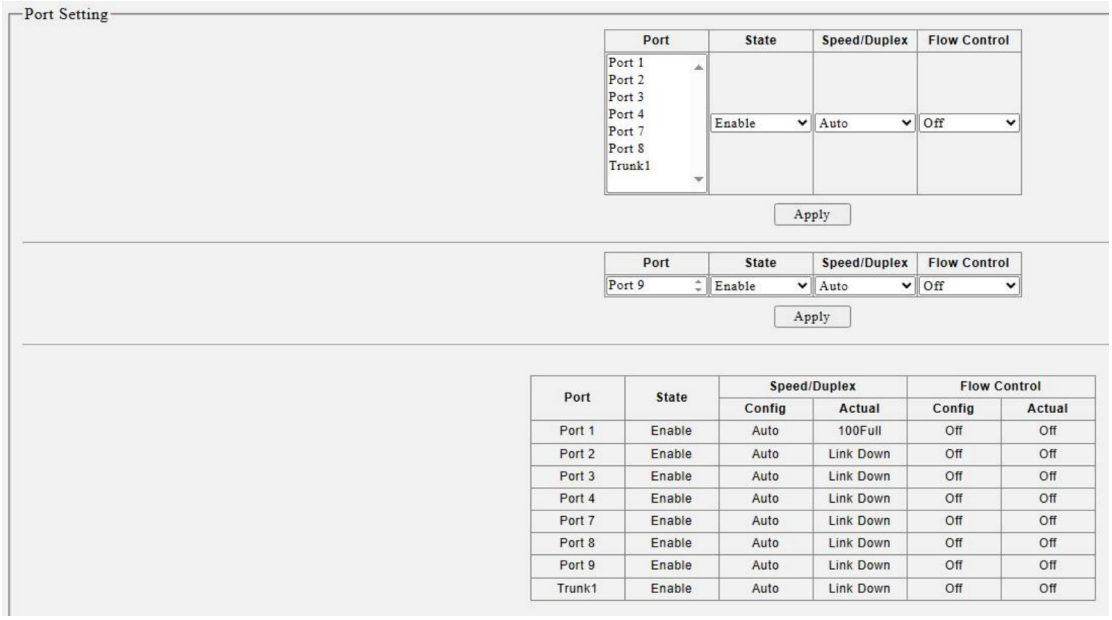
Configuration item	Description
New Username	Account name
New Password	Account password
Confirm Password	Account password re-entry

3.4 Port Setting

Querying and Configuring Ethernet Ports.

Procedure

Click "System > Port Setting" in the navigation tree to enter the interface, as shown in the following figure:



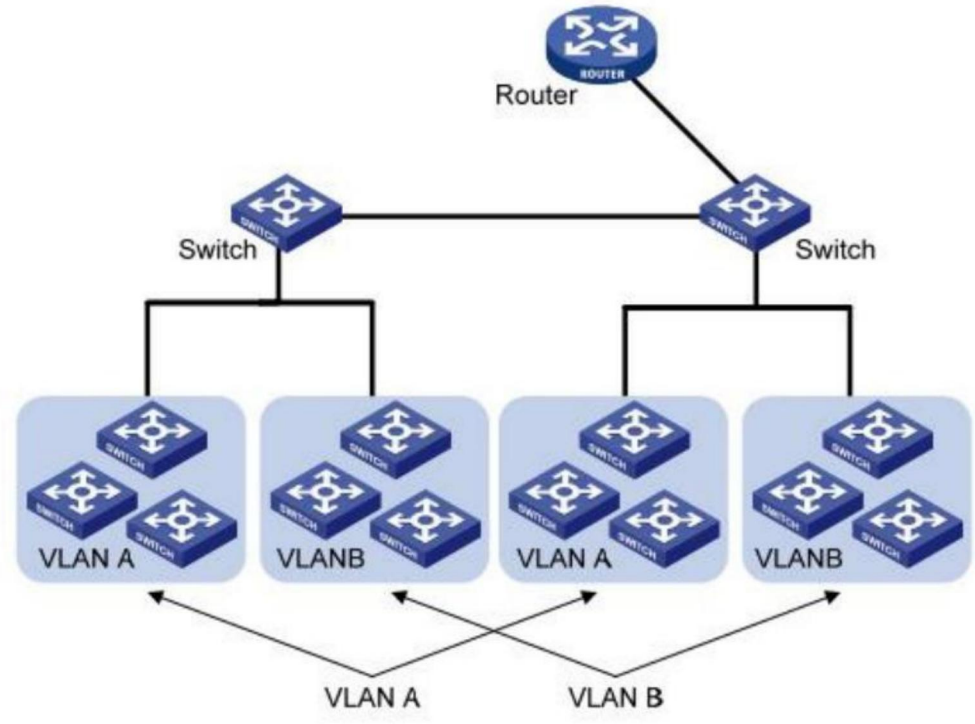
The meaning of the interface information is shown in the following table:

Configuration item	Description
State	Port enable and disable.
Speed/ Duplex	Port speed.
Flow Control	Flow off and on.

4 Configuration

4.1 VLAN

The composition of VLAN is not limited by physical location, so hosts within the same VLAN do not need to be placed in the same physical space. As shown in the figure below, VLAN divides a physical LAN into multiple logical LAN, and each VLAN is a broadcast domain. hosts within a VLAN can interact with each other through traditional Ethernet communication, while hosts within different VLAN need to communicate with each other through network layer devices, such as routers or Layer 3 switches.



VLAN offer the following advantages over traditional Ethernet:

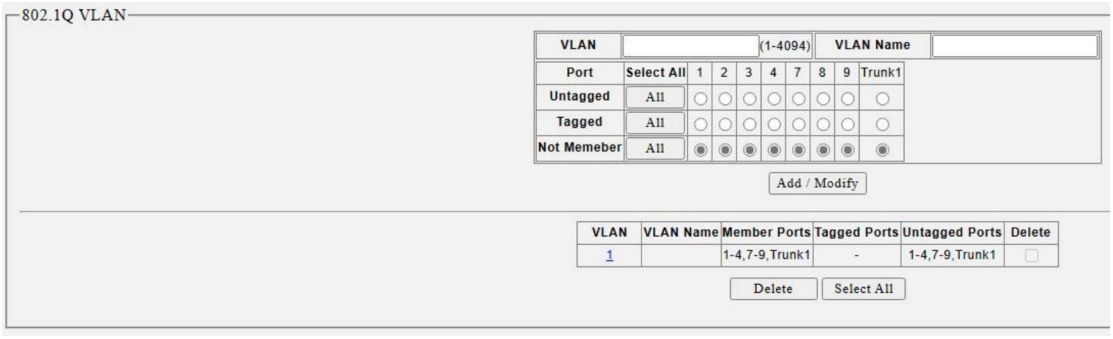
- Controls the scope of broadcast domains: Broadcast messages within the LAN are limited to a VLAN, saving bandwidth and improving network processing power.
- Enhanced LAN security: Since messages are isolated by the broadcast domain delineated by VLAN at the data link layer, hosts within each VLAN cannot communicate directly with each other, and they need to forward the messages at the third layer through network layer devices such as routers or Layer 3 switches.
- Flexible Virtual Workgroup Creation: Using VLAN, virtual workgroups can be created across physical network ranges, allowing users to access the network without changing network configurations when their physical locations move within the virtual workgroup range. This managed switch supports 802.1Q VLAN, port-based VLAN, and in the default configuration, VLANs are in 802. 1QVLAN mode.

4.1.1 802.1Q VLAN

This settings page is functionally equivalent to the Hybrid interface type.

Operational steps:

Click Configuration > VLAN > 802.1Q VLAN menu in the navigation tree to enter the interface as shown below:



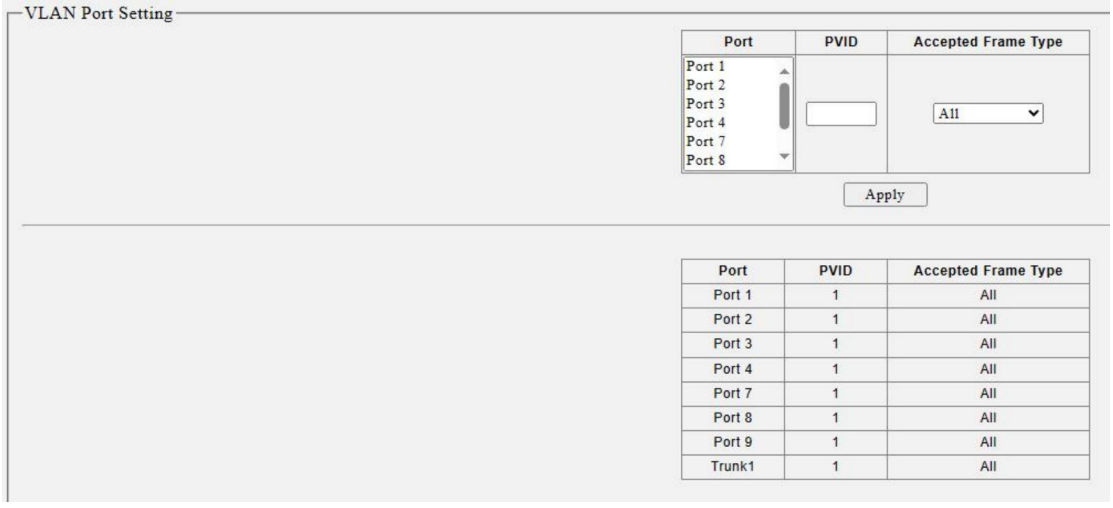
The meaning of the interface information is shown in the following table:

Configuration item	Description
VLAN	Default VLAN for the port.
VLAN Name	VLAN Name Description.

4.1.2 802.1Q VID

Procedure:

Click the "Configuration > VLAN > 802.1Q VID" menu in the navigation tree to enter the interface as shown below:



Configuration item	Description
PVID	VLAN identification of the port.
Accepted Frame Type	All frame types, only packets with tags are accepted, only packets

	without tags are accepted.

4.2 QoS

QoS (Quality of Service) is used to evaluate the ability of a service provider to meet the needs of a customer service, and in the case of the Internet, QoS is used to evaluate the service capability of a network to deliver packets. Since the services provided by the network are varied, they can be evaluated based on different aspects. QoS, as it is commonly referred to, is an assessment of the ability of a service to support core requirements such as bandwidth, delay, delay jitter, and packet loss during packet delivery. Bandwidth, which can also be referred to as throughput, represents the average rate of a service flow over a given period of time, usually in Kbit/s. Latency represents the average time it takes for a service flow to traverse the network. For a device in a network, the need for latency is generally understood in terms of several classes. For example, there are two latency classes, and the priority queue scheduling method enables high-priority services to be served as quickly as possible, while low-priority services have to wait until there are no high-priority services to be served. Delay jitter, which represents the variation in the time it takes for a service flow to traverse the network. Packet loss rate, which indicates the rate at which a service stream is lost during transmission. Due to the high reliability of modern transmission systems, loss of information often occurs when the network becomes congested. The most common scenario is packet loss due to queue overflow. In traditional IP networks, all packets are treated equally without distinction, and each network device processes all packets using a first-in-first-out strategy, and does its best to deliver the packets to their destinations, but does not provide any guarantees for the reliability of the packet delivery, the transmission delay, and other performance.

Network development is rapidly changing, and with the emergence of new applications on IP networks, new requirements are placed on the quality of service of IP networks. For example, delay-sensitive services such as VoIP and video place high demands on the transmission delay of messages. If the delay of message transmission is too long, it will be unacceptable to users. In order to support voice, video, and data services with different service requirements, the network is required to be able to differentiate between different types of services and provide them with appropriate services.

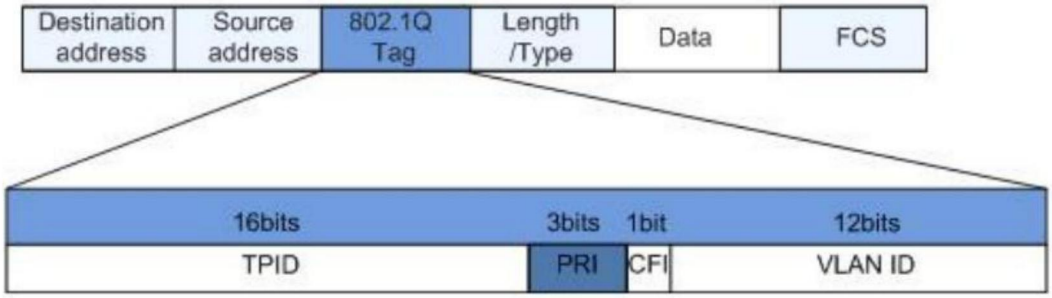
The best effort service of traditional IP networks cannot identify and differentiate the various types of services in the network, and the ability to differentiate between types of services is the prerequisite for providing differentiated services for different services, so the best effort service model of traditional networks can no longer meet the needs of the application. the emergence of QoS technology is dedicated to solving this problem. QoS can regulate network traffic, avoid and manage network congestion, and reduce the packet loss rate. QoS can regulate network traffic to avoid and manage network congestion and reduce packet loss. QoS can regulate network traffic to avoid and manage network congestion and reduce packet loss. It also supports the provision of dedicated bandwidth for users and different quality of service for different services, which improves the service capability of the network.

Different messages use different QoS priorities, for example, VLAN messages use the 802.1p,

or CoS (Class ofService) field, and IP messages use DSCP. in order to maintain the priority of a message as it passes through different networks, you need to configure the mapping of these priority fields at the gateways connecting the different networks.

802.1p priority in VLAN frame header

Typically Layer 2 devices interact with VLAN frames. The PRI field (i.e., 802.1p Priority) in the VLAN frame header, or CoS (Class of Service) field, identifies the quality of service requirements. according to the IEEE 802.1Q definition.802.1p Priority in a VLAN frame.

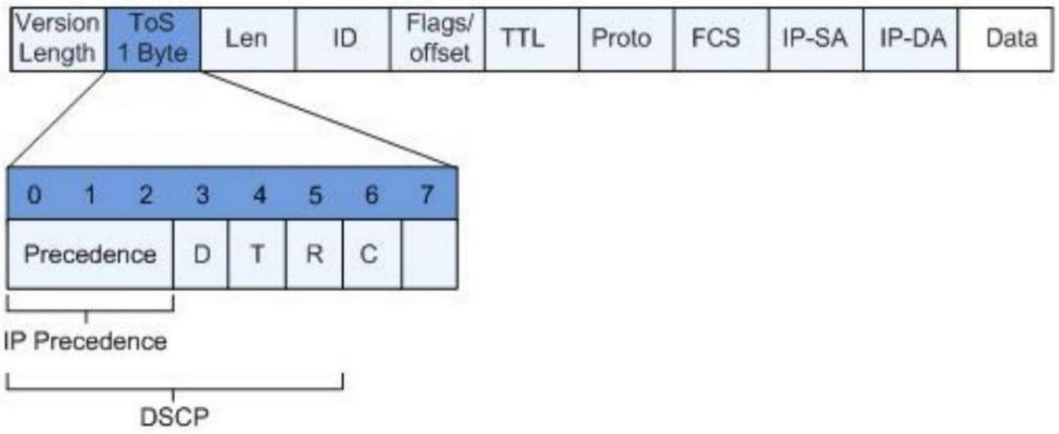


A 3-bit long PRI field is included in the 802.1Q header. The PRI field defines eight service priority CoSs, with values 7, 6, ..., 1, and 0 in descending order of priority.

IP Precedence/DSCP field

According to RFC791, the ToS (Type of Service) field of the IP message header consists of 8 bits, of which the 3-bit Precedence field identifies the priority of the IP message, and the position of Precedence in the message is shown in the figure.

IP Precedence/DSCP field



Bits 0 to 2 represent the Precedence field, which represents the 8 priority levels for message transmission, and the values are 7, 6, ..., 1, and 0 in descending order of priority. The highest priority is 7 or 6, which is often reserved for routing or updating the network control communication, and the user level applications can only use level 0 to 5. In addition to the Precedence field, the ToS field also includes three bits, D, T, and R: D bits represent the delay requirement (Delay, 0 for normal delay, 1 for low delay), T bits represent the throughput (Throughput, 0 for normal throughput, 1 for high throughput), and R bits represent the reliability (Reliability, 0 for normal reliability, 1 for high reliability). R bits represent reliability (Reliability, 0 for normal reliability, 1 for high reliability). bits 6 and 7 in the ToS field are reserved.

RFC1349 redefined the ToS field in IP messages by adding C bits to indicate transmission

overhead (Monetary Cost). Subsequently, the IETF DiffServ Working Group in RFC2474 redefined bits 0-5 in the ToS field of the IPv4 header as DSCP and renamed the ToS field as DS (Differentiated Service) byte.The position of DSCP in the message is shown in the figure above.The first 6 bits (bits 0-5) of the DS field are used as the differentiated service code point DSCP (DS Code Point), and the upper 2 bits (bits 0-5) are used as the differentiated service code point DSCP (DS Code Point). The first 6 bits (bits 0 to 5) of the DS field are used as the Differentiated Service Code Point (DSCP), and the upper 2 bits (bits 6 and 7) are reserved bits. the lower 3 bits (bits 0 to 2) of the DS field are the Class Selector Code Point (CSCP), and the same CSCP value represents a class of DSCPs. the DS node selects the corresponding PHB (Per-Hop Behavior) according to the value of DSCP. The DS node selects the corresponding PHB (Per-Hop Behavior) based on the value of DSCP.

4.2.1 Port to Queue

Sets the processing priority for the different tags of a data frame.

Procedure

Click "Configuration > QOS > Port to Queue" menu in the navigation tree to enter the interface, as shown in the following figure:

The meaning of the interface information is shown in the following table:

Configuration item	Description
Queue	Range 1-8

4.2.2 Queue Weight

The weights are equivalent to SP for strict priority and WRR (Weighted Round-Robin Scheduling Algorithm) for values of 1-15.

Procedure:

Click "Configuration > QOS > Queue Weight" menu in the navigation tree to enter the interface,

as shown in the following figure:

The meaning of the interface information is shown in the following table:

Configuration item	Description
Weight	Defaults to strict priority, with weights ranging from 1-15.

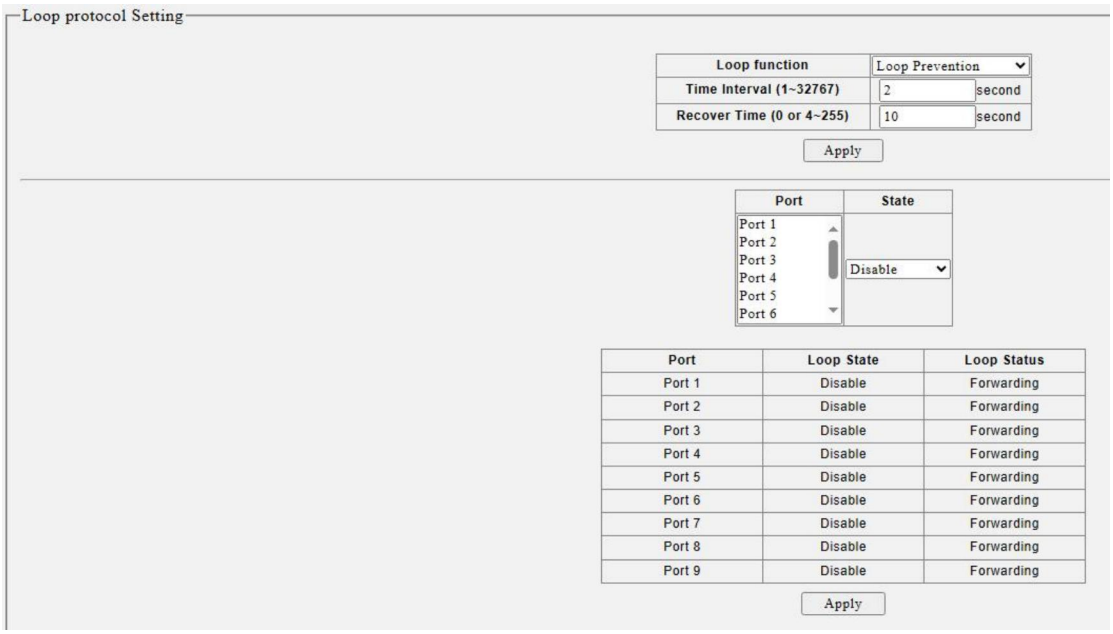
4.3 Loop

4.3.1 Loop Protocol

The device confirms the existence of a loop by sending a loop detection message and detecting whether it returns to the device (it is not required that the receiving and sending ports are the same port). If a port receives a loop detection message from the device, it is recognized that there is a loop on the link where the port is located. When a loop exists in the network, the corresponding port LED will blink to alert the network administrator that a loop exists (the loop will be blocked when Loop Avoidance is enabled).

To do this, click the Configuration > Loop > Loop Detection menu in the navigation tree:

Click "Configuration > Loop Setting > Loop Protocol" in the navigation tree to enter the interface, as shown in the figure below:



The meaning of the interface information is shown in the following table:

Configuration item	Description
Loop Protocol	Shutdown, Loop Detection, Loop Avoidance, Spanning Tree.

4.3.2 STP global

Rapid Spanning Tree Protocol (RSTP) is used to eliminate physical loops at the data link layer in LANs, and its core is the Rapid Spanning Tree algorithm.RSTP is fully backward compatible with STP, and in addition to the functions of avoiding loops and dynamically managing redundant links as in the case of the traditional STP protocol, RSTP greatly shortens the topology convergence time, so that all switching equipment supports RSTP and can be configured to restore stability after a topology change (link UP/DOWN) within seconds in the ideal network topology size. Under the ideal network topology scale, if all switching devices support RSTP protocol and are properly configured, the time to restore stability after a topology change (link UP/DOWN) can be controlled in seconds.The main functions of RSTP can be summarized as follows:

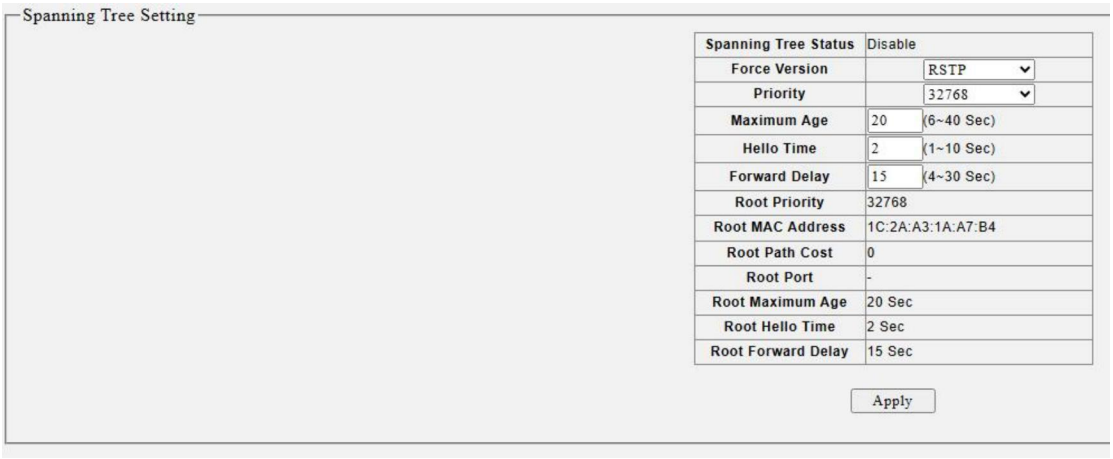
1. Discover and generate an optimal tree topology for the LAN;

2. Discovering topology failures and recovering from them, automatically updating the network topology and enabling backup links while maintaining the optimal tree structure;

To do this, click the Configuration > Loop Protocol > STP Global menu in the navigation tree:

Click "Configuration > Loop Protocol > STP Global" in the navigation tree to enter the interface as

shown below:



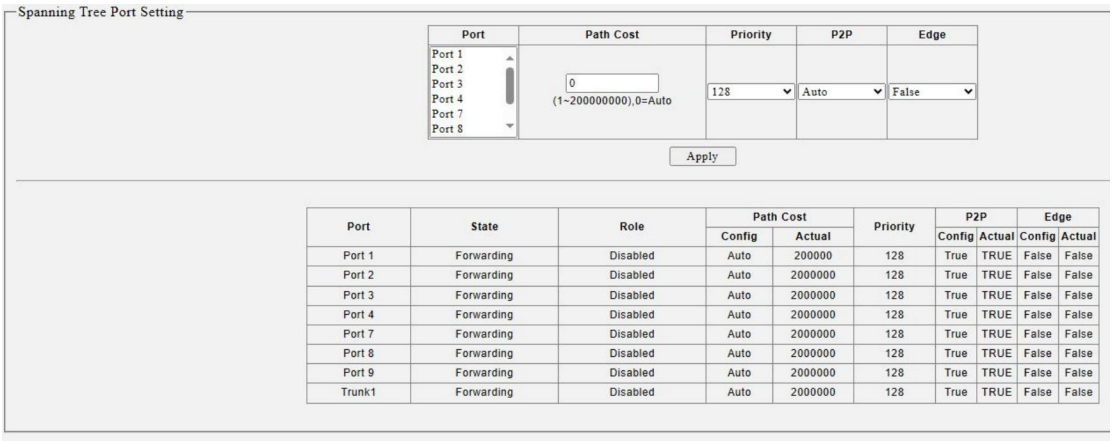
The meaning of the interface information is shown in the following table:

Configuration item	Description
Force Version	Configuration View STP Mode.
Maximum Age	Configure to view maximum aging time.
Hello Time	Configuring View Hello Time.
Forward Delay	Configure to view the forwarding delay time.

4.3.3 STP port

Procedure:

Click "Configuration > Loop Protocol > STP Port" in the navigation tree to enter the interface, as shown in the following figure:



The meaning of the interface information is shown in the following table:

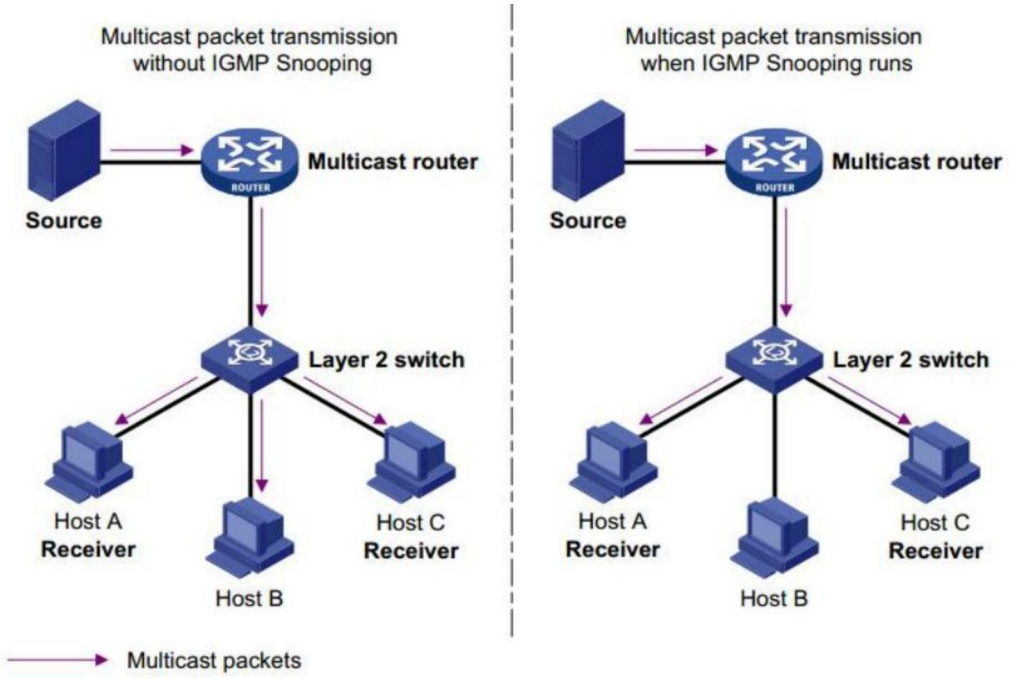
Configuration item	Description
Path Cost	Configuring View Port Path Overhead.
Priority	Configuring View Port Priority.
P2P	Configuration View P2P.
Edge	Configuring View Edge Ports.

4.4 IGMP Snooping

IGMP snooping (Internet Group Management Protocol Snooping) is a multicast constraint mechanism that runs on Layer 2 devices to manage and control multicast groups.

Layer 2 devices running IGMP snooping analyze received IGMP messages to establish a mapping relationship between ports and MAC multicast addresses and forward multicast data according to this mapping relationship.

As shown in the following figure, when a Layer 2 device is not running IGMP snooping, multicast data is broadcast at Layer 2; when a Layer 2 device is running IGMP snooping, the multicast data of a known multicast group is not broadcast at Layer 2, but is multicast to the specified receiver at Layer 2, but the unknown multicast data is still broadcast at Layer 2.



Procedure:

Click the "Configuration > IGMP Snooping" menu in the navigation tree to enter the interface, as shown in the following figure:

The meaning of the interface information is shown in the following table:

Configuration item	Description
Enable	Enable/Disable
Dump IGMP entry	Querying IGMP Group Information.

4.5 Trunk Group Setting

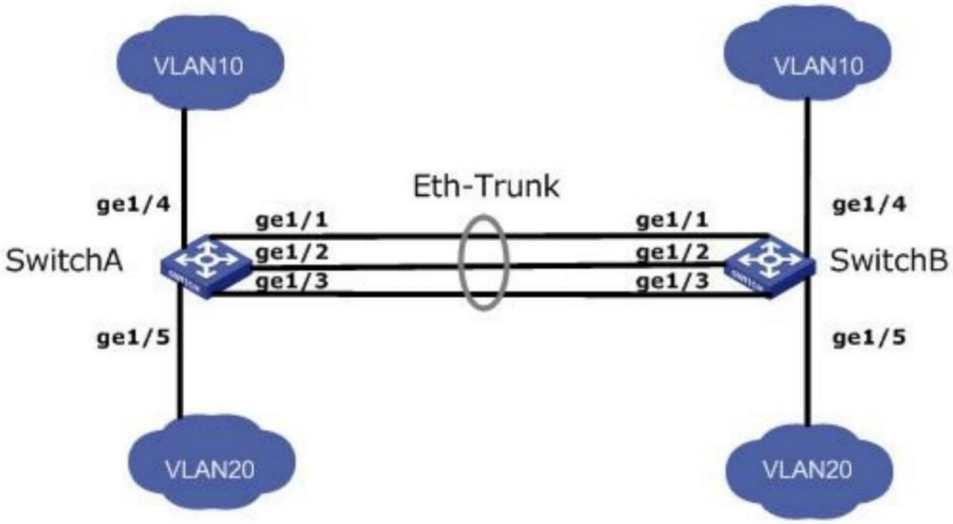
Link Aggregation is a method of bundling a group of physical interfaces together as a logical interface to increase bandwidth and reliability.

Link Aggregation Group LAG (Link Aggregation Group) is a logical link formed by bundling several Ethernet links together, abbreviated as Eth-Trunk.

With the continuous expansion of network scale, users have higher and higher requirements on the bandwidth and reliability of links. In traditional technology, bandwidth is often increased by replacing high-speed interface boards or by replacing equipment that supports high-speed interface boards, but this solution requires high costs and is not flexible enough.

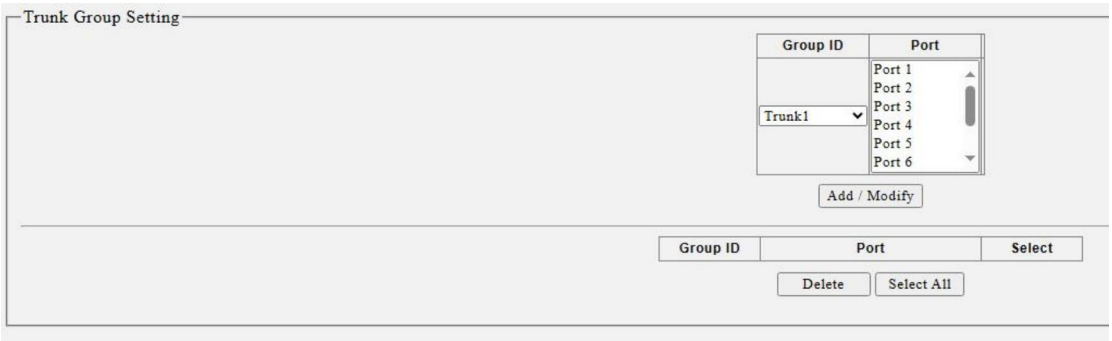
The use of link aggregation technology can realize the purpose of increasing link bandwidth by bundling multiple physical interfaces into one logical interface without hardware upgrade. The backup mechanism of link aggregation can effectively improve reliability, and at the same time, it can also realize the load sharing of traffic on different physical links.

As shown in the figure below, SwitchA and SwitchB are connected to each other by three Ethernet physical links. Bundling these three links together becomes an Eth-Trunk logical link, and the bandwidth of this logical link is equal to the sum of the bandwidths of the original three Ethernet physical links, so as to achieve the purpose of increasing the bandwidth of the link; at the same time, these three Ethernet physical links are backed up by each other, which effectively improves the reliability of the link.



Procedure:

Click "Configuration > Trunk Group Setting" in the navigation tree to enter the interface as shown in the following figure:



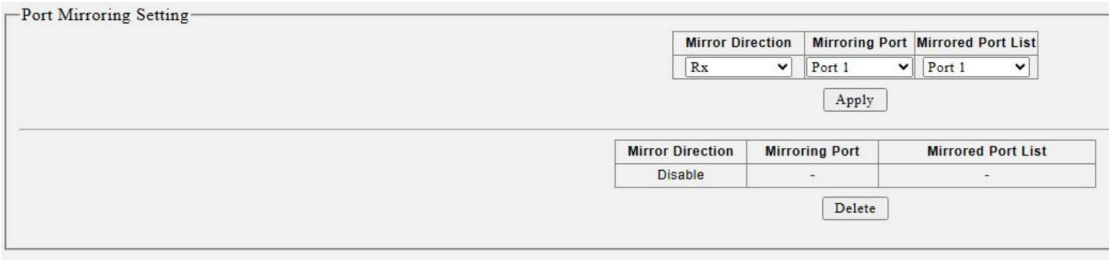
The meaning of the interface information is shown in the following table:

Configuration item	Description
Group ID	Aggregate group IDs, supports up to 2 groups.
Port	Aggregation group member ports, supports up to 4 members.

4.6 Port-based Mirroring

Port mirroring is to copy the messages from the mirrored port of the switch to the monitoring port; the monitoring port usually has access to data inspection devices, which are used by users to analyze the messages received from the mirrored port for network monitoring and troubleshooting.

Click the Configuration > Port Mirroring menu in the navigation tree to enter the interface, as shown in the following figure:



The meaning of the interface information is shown in the following table:

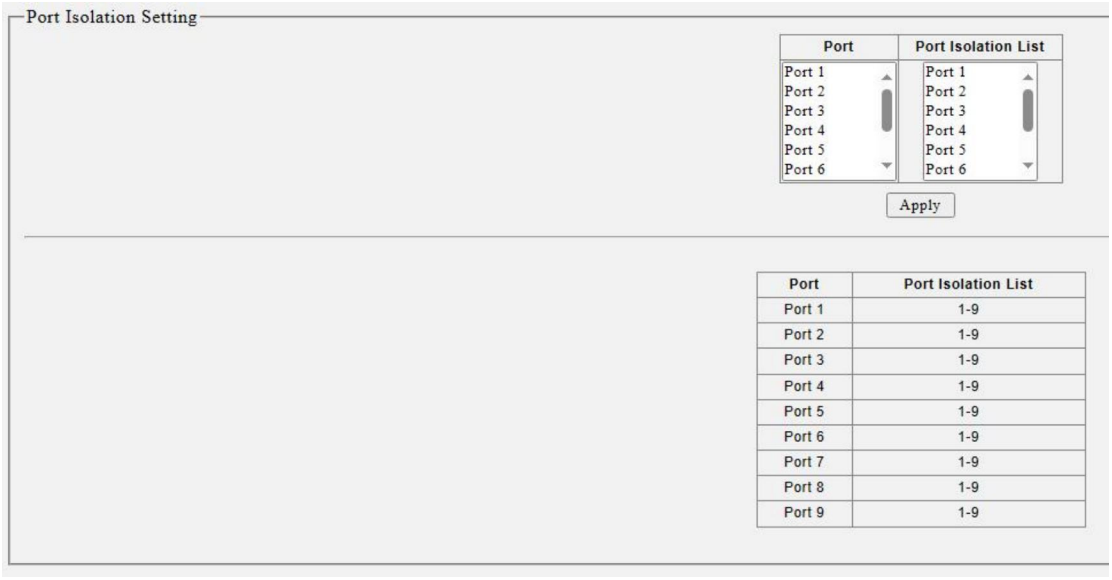
Configuration item	Description
Mirror Direction	Enable or disable port mirroring to support inbound, outbound, and bidirectional.
Mirroring Port	Only one normal physical port can be selected, excluding link aggregation ports and source ports.
Mirrored Port List	Mirror Source Port List.

4.7 Port Isolation

Port traffic sometimes do not need to communicate with each other, but broadcast, multicast and other messages will be flooded to each port, at this time you can use the port isolation

function to achieve port to port message isolation.

Click Configuration > Port Isolation in the navigation tree to enter the interface, as shown in the following figure:



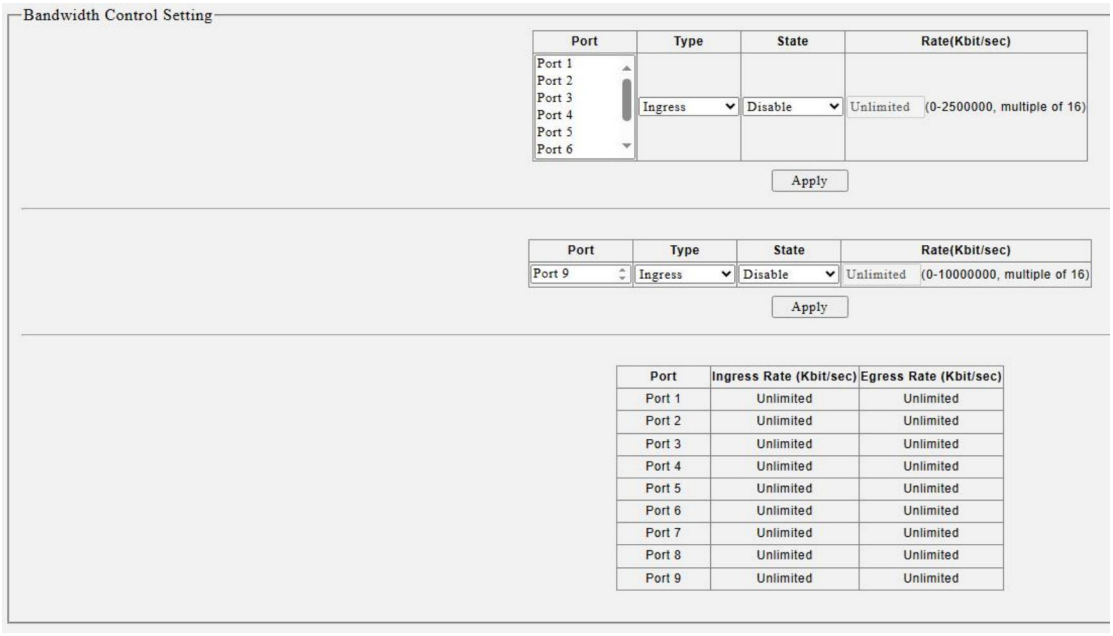
The meaning of the interface information is shown in the following table:

Configuration item	Description
Port	Port list
Port Isolation List	The port to which corresponding port messages are allowed to be forwarded.

4.8 Bandwidth Control

Configuring interface rate limiting is to limit the rate at which a physical interface sends data outward. Configuring rate limiting in the outbound direction of an interface before traffic is sent out of the interface controls all outgoing message traffic.

Click "Configuration > Bandwidth Control" menu in the navigation tree to enter the interface, as shown in the following figure:



The meaning of the interface information is shown in the following table:

Configuration item	Description
Port	Port list
Type	Ingress/Engress
State	Disable/Enable
Rate	Rate limit value, range: 16 to 1,000,000 Kbit

4.9 Jumbo Frame

Sets the maximum MTU of the port.

Click "Configuration > Mega Frames" menu in the navigation tree to enter the interface, as shown in the following figure:

The meaning of the interface information is shown in the following table:

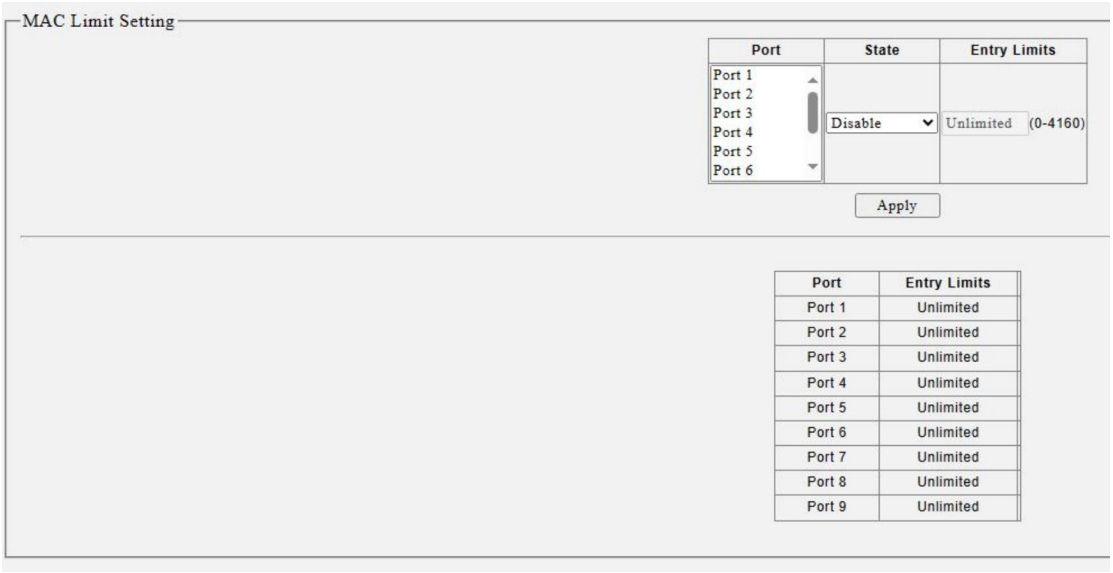
Configuration item	Description
Jumbo Frame Setting	Setting the port MTU

4.10 MAC Constration

The MAC Address Limit function limits the number of MAC addresses that can be learned on each port and stops learning MAC addresses when the limit is exceeded.

Click "Configuration > MAC Constration" menu in the navigation tree to enter the interface, as

shown in the following figure:



The meaning of the interface information is shown in the following table:

Configuration item	Description
State	Disable/Enable
Entry Limits	MAC Learning Limit Values

4.11 EEE

After enabling EEE (Energy Efficient Ethernet), if the interface state is always up and no message is sent or received for a consecutive period of time, the interface automatically enters the low-power mode; when the interface needs to send or receive messages, the interface will automatically return to the normal working mode, so as to achieve the effect of energy saving.

Click the "Configuration > EEE" menu in the navigation tree to enter the interface, as shown in the following figure:

5 Security

5.1 MAC address

The main function of an Ethernet switch is to forward messages at the data link layer, that is, to output the messages to the corresponding ports according to the destination MAC addresses

of the messages. The MAC address forwarding table is a Layer 2 forwarding table containing the correspondence between MAC addresses and forwarding ports, which is the basis for Ethernet switches to realize the fast forwarding of Layer 2 messages.

The table entries in the MAC address forwarding table contain the following information:

- Destination MAC Address
- VLAN ID to which the port belongs
- Forwarding port number on this device
- When forwarding messages, the Ethernet switch takes the following two forwarding methods based on the MAC address table entry information:

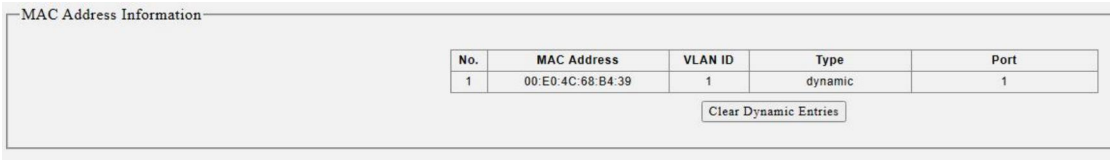
✧ Unicast mode: when the MAC address forwarding table contains a table entry corresponding to the destination MAC address of the message, the switch sends the message directly from the forwarding port in the table entry.

✧ Broadcast Mode: When the switch receives a message whose destination address is all F, or there is no table entry in the MAC address forwarding table that contains the corresponding destination MAC address of the message, the switch will take the broadcast mode to forward the message to all ports except the receiving port.

5.1.1 MAC Search

On this page, you can view the MAC address table information, in order to adapt to the network changes, the MAC address table needs to be updated continuously. the table entries automatically generated in the MAC address table are not valid forever, each table entry has a survival period, the table entries that do not get refreshed before reaching the survival period will be deleted, and this survival period is called the aging time. If a record is refreshed before reaching the survival period, the aging time of the table entry is recalculated.

Click the "Security > MAC Address > MAC Search" menu in the navigation tree to enter the interface, as shown in the following figure:

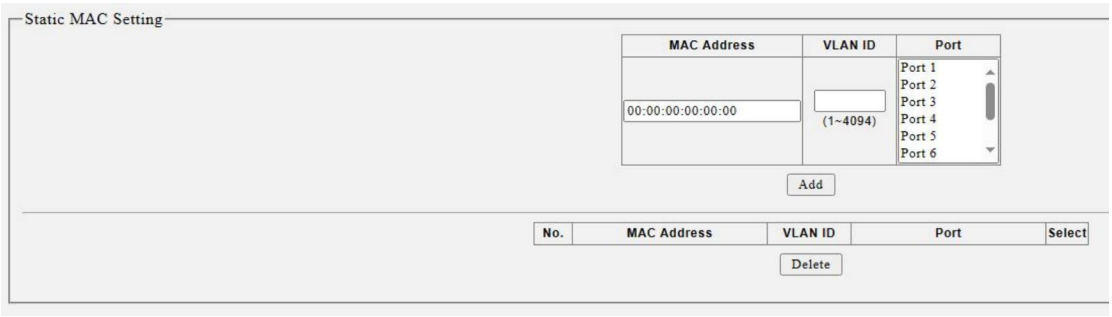


Note: The MAC lookup display wait process can interrupt communication with the device.

5.1.2 Static MAC

Static table entries are manually configured by the user and distributed to each interface board. the table entries do not age. This setting page can also filter source and destination MAC, and the configuration takes effect on all ports.

Click the "Security > MAC Address > Static MAC" menu in the navigation tree to enter the interface, as shown in the following figure:



The meaning of the interface information is shown in the following table:

Configuration item	Description
MAC Address	MAC address e.g.: HH:HH:HH:HH:HH:HH:HH
VLAN ID	Specified VLAN
Port	Static MAC Binding Port List.

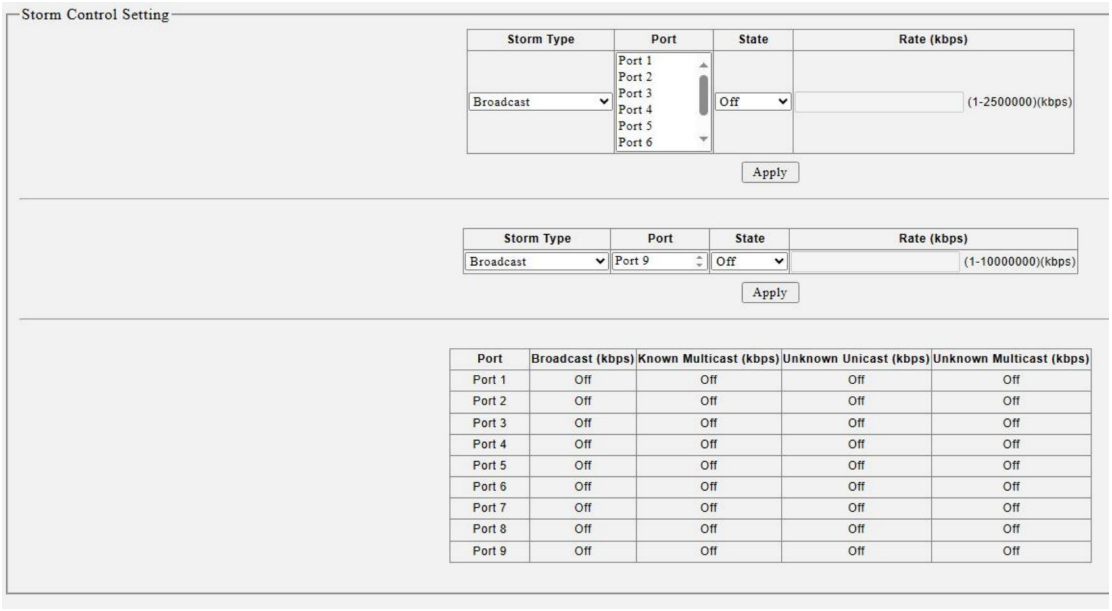
5.2 Storm Control

Storm control prevents broadcast, unknown multicast, and unknown unicast messages from generating broadcast storms in the following forms. The device supports storm control by packet rate for each of these three types of messages under the interface. During a detection interval, the device monitors the average rate of the three types of messages received under the interface and compares it with the configured maximum threshold; when the message rate is greater than the configured maximum threshold, the device performs storm control on the interface and executes the configured storm control actions.

When a Layer 2 Ethernet interface receives a broadcast, multicast, or unknown unicast message, if the device cannot specify the outgoing interface of the message based on the destination MAC address of the message, the device forwards the message to other Layer 2 Ethernet interfaces within the same VLAN (Virtual Local Area Network), which may result in a broadcast storm and reduce the forwarding performance of the device. Introducing the storm suppression feature can control the traffic of these three types of messages and prevent broadcast storms.

Procedure:

Click the "Security > Storm Control" menu in the navigation tree to enter the interface, as shown in the following figure:



The meaning of the interface information is shown in the following table:

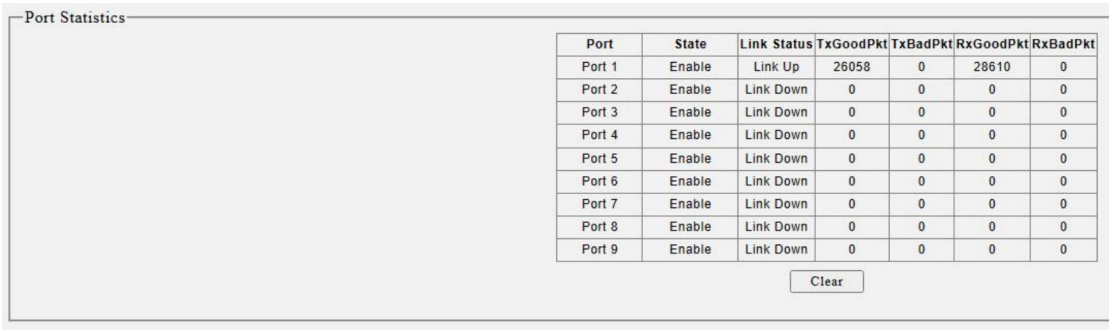
Configuration item	Description
Storm Type	Broadcast, known multicast, unknown unicast, unknown multicast.
Port	Port list
State	Off/on
Rate	Storm Suppression Value.

6 Monitoring

Querying port statistics.

Procedure

Click "Monitor > Port Statistics" in the navigation bar to enter the Port Configuration page:



The meaning of the interface information is shown in the following table:

Configuration item	Description
Port	port list
State	port state
Link Status	port link state
Tx Good Pkt	Number of correct packets sent

Tx Bad Pkt	Number of packets sent in error
Rx Good Pkt	Number of correct packets received
RX Bad Pkt	Number of packets received in error

7 Tools

7.1 Firmware Upgrade

System version firmware upgrade, click upgrade will enter the upgrade mode, jump to the upgrade page and select the firmware online upgrade.

Steps:

Click "Tools > Firmware Upgrade" menu in the navigation tree to enter the interface, as shown in the following figure:

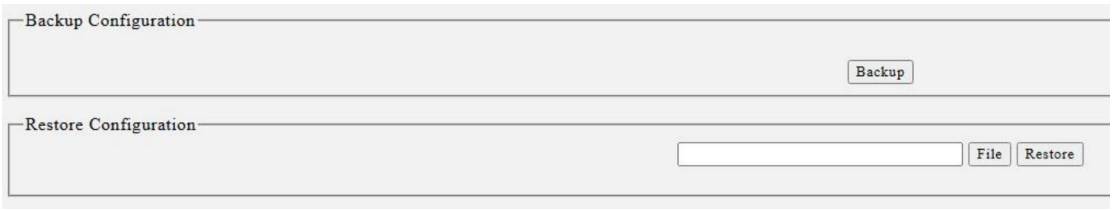
Note: After clicking OK, please do not disconnect the power during the upgrade process, stay on the upgrade page and wait about 1 minute for the upgrade to complete.

7.2 Configuration Backup

Upgrade and backup of system configuration files.

Procedure:

Click "Tools > Configuration Backup" menu in the navigation tree to enter the interface, as shown in the following figure:



The meaning of the interface information is shown in the following table:

Configuration item	Description
Backup	Backup Configuration Files.
Restore	Upload the configuration file.

Note: A reboot is required after uploading the configuration to take effect.

7.3 Rest

The system will be restored to its factory configuration.

Steps:

Click "Tools > Restore Factory" menu in the navigation tree to enter the interface, as shown in the following figure:

7.4 Save

Save Configuration.

Procedure:

Click the "Tools > Save" menu in the navigation tree to enter the interface, as shown below:

7.5 Reboot

Procedure:

Click "Tools > Reboot" menu in the navigation tree to enter the interface, as shown in the following figure:

7.6 Logout

Steps:

Click "Tools > Logout" menu in the navigation tree to exit the configuration interface.