Ethernet Switch WEB User manual

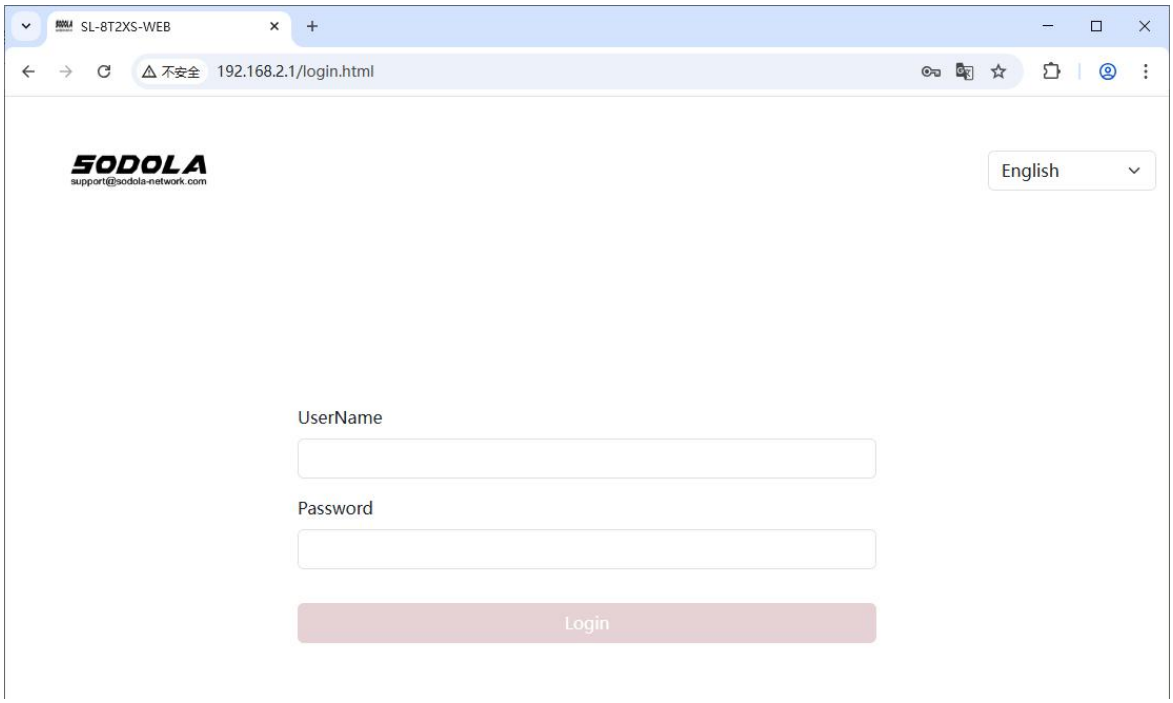
SL-8T2XS-WEB

Table of Contents

Chapter 1 System Functions

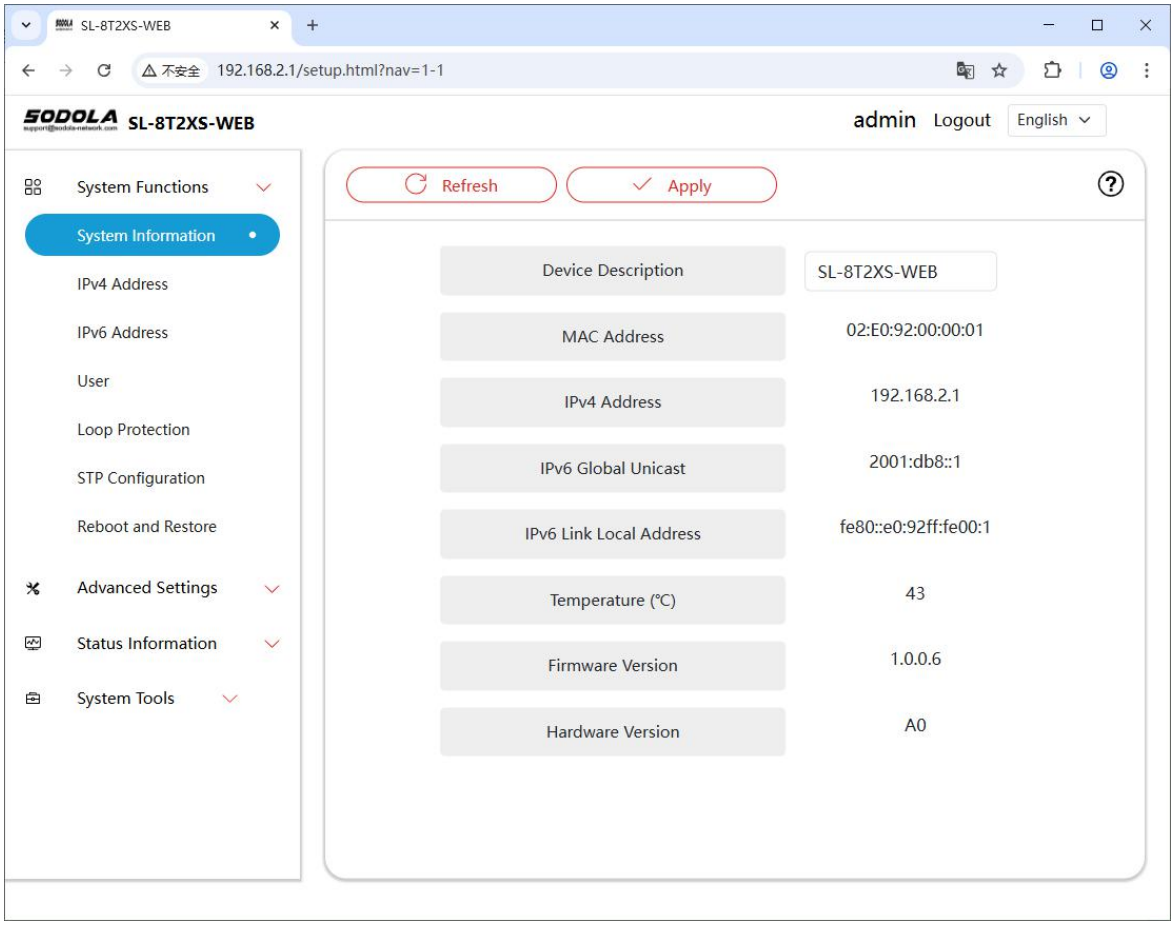
1.1 Logging In to a Switch

When you log in to the switch, ensure that the IP network segment of the PC is the same as that of the switch. At the first login, set the IP address of the PC to 192.168.2.x (x indicates 1 to 254, except 1) and the subnet mask to 255.255.255.0. However, the IP address of the PC cannot be the same as that of the switch, that is, 192.168.2.1. A login window appears, as shown in the following figure. Enter the default user name and password: admin. Click the < Login > button and you will see the switch system information.



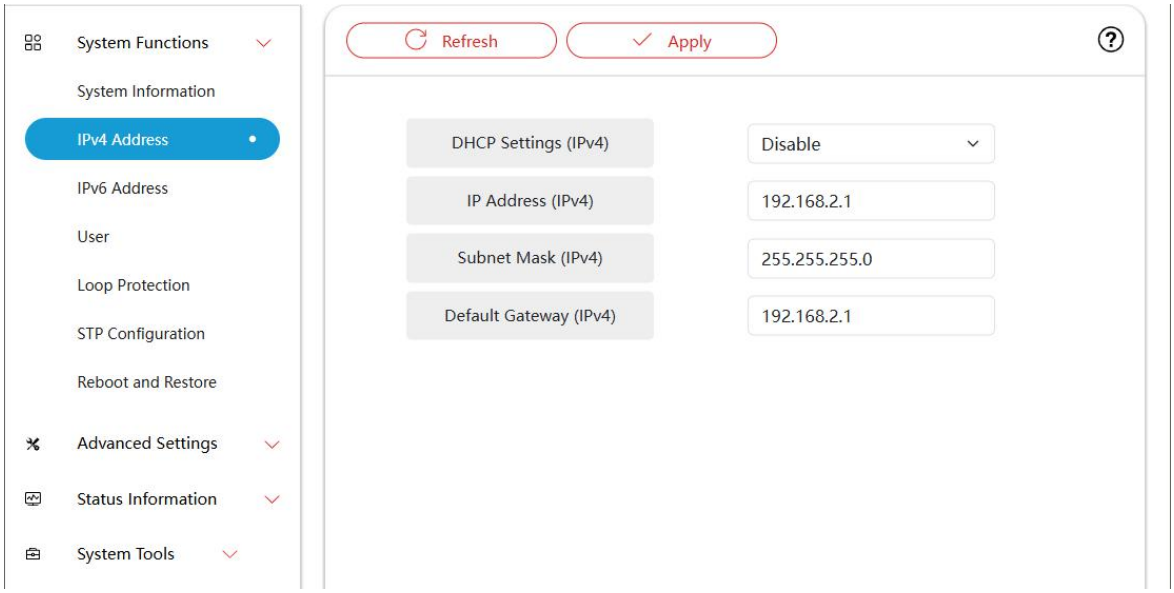
1.2 System Information

1. Click System Function -> System Information
2. The page is used to view the device description, hardware, software, and MAC address.



1.3 IPv4 Address

1. Click System Functions >IPv4 Address.
2. Configure an IPv4 address for logging in to the switch.

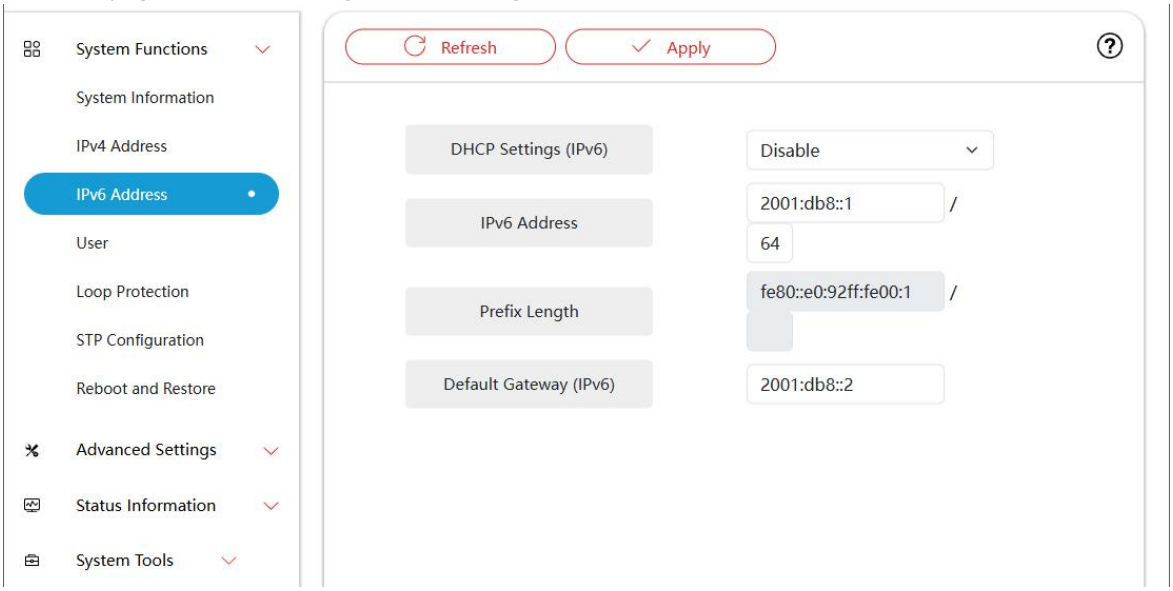


The following table describes the meanings of the interface information.

Configuration item	Instructions
DHCP Settings(IPv4)	Disabled: Access the Internet from a fixed IP address Enable: DHCP Internet access and automatically obtains an IP address for Internet access
IP Address (IPv4)	Management IP address
Subnet Mask(IPv4)	IP address mask
Default Gateway (IPv4)	IP address gateway

1.4 IPv6 Address

1. Click System Function >IPv6 Address. 2.
2. The page is used to configure an IPv6 login address for the switch.

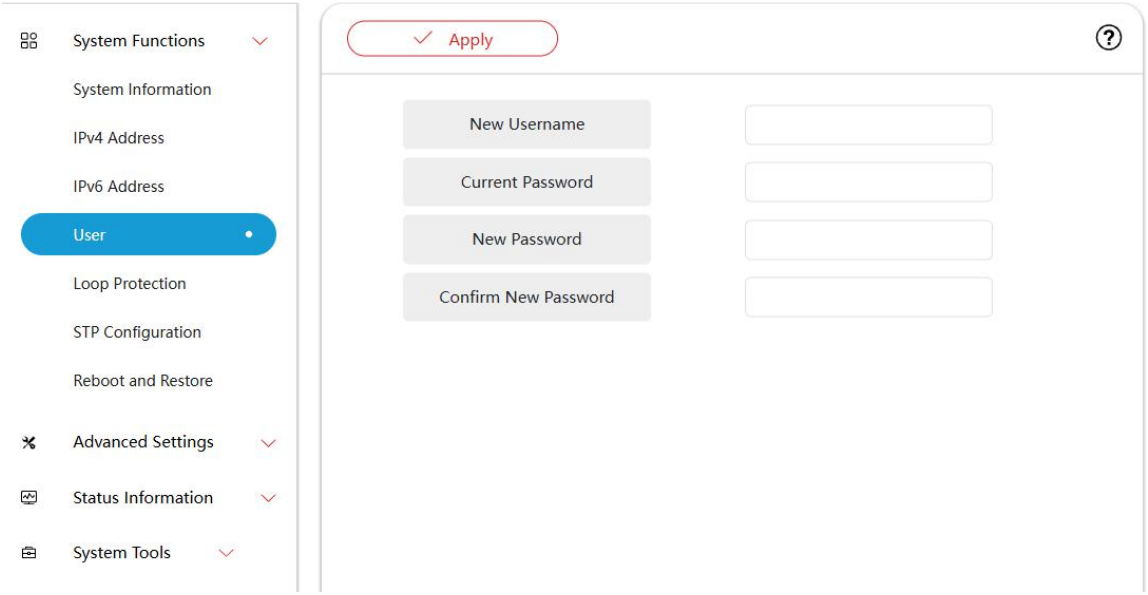


The following table describes the meanings of the interface information.

Configuration item	Instructions
DHCP Settings(IPv6)	Manual: Access the Internet from a fixed IPv6 address Automatic: The DHCP server accesses the Internet and automatically obtains an IP address Automatic configuration: Access the Internet through DHCP and automatically obtain an IP address
IPv6 address	Manage IPv6 addresses
Prefix length	The prefix length of an IPv6 address
Default gateway (IPv6)	Indicates the gateway of an IPv6 address

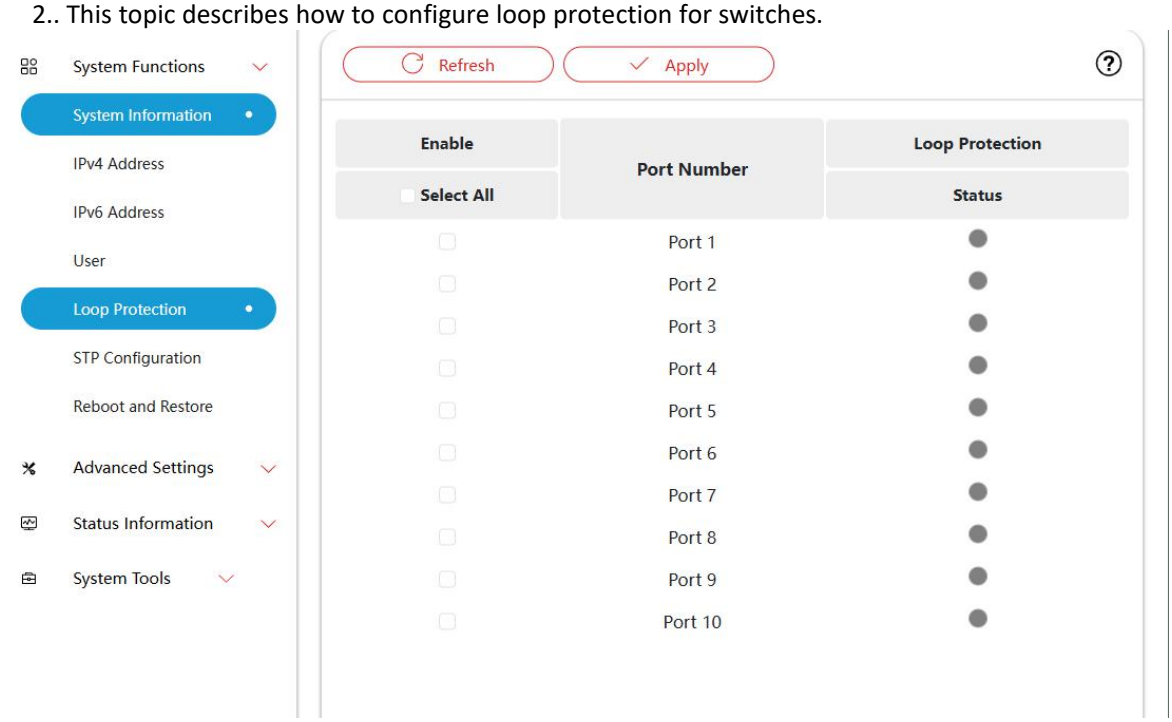
1.5 Users

1. Click System Functions -> Users.
2.. This page is used to configure the user name and password for logging in to the switch.



1.6 Loop Protection

1. Click System Function > Loop Protection.
2.. This topic describes how to configure loop protection for switches.

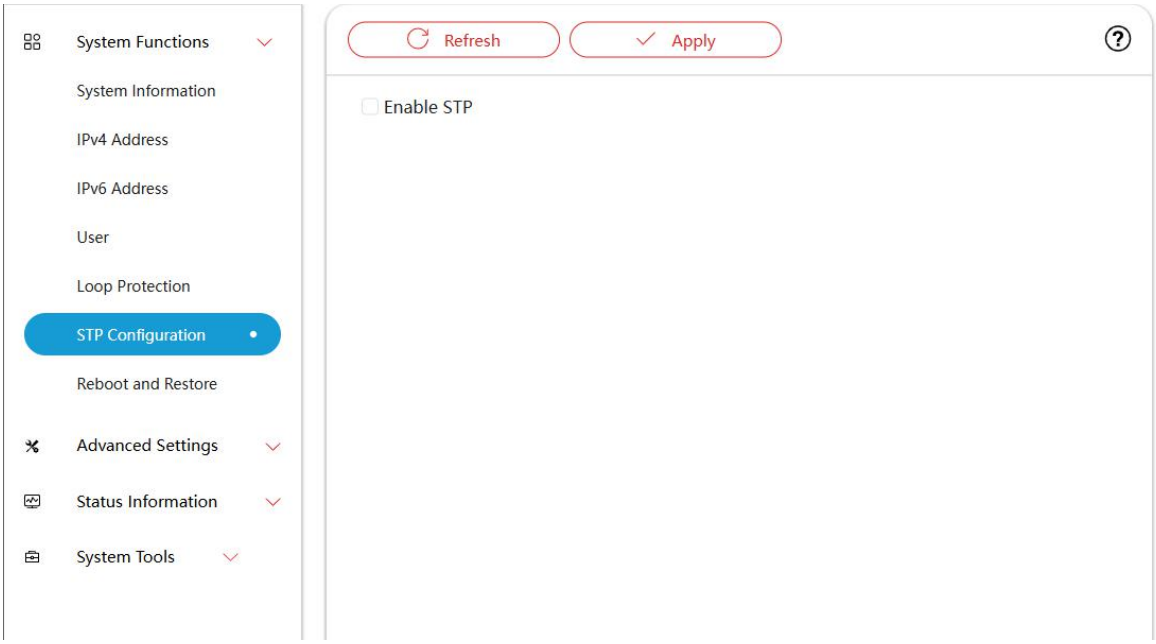


1.7 STP Configuration

Fast Spanning Tree Protocol (RSTP) is used to eliminate the physical loop of data link layer in local area network. RSTP is backward compatible with STP. In addition to the functions of avoiding loops and dynamically managing redundant links like traditional STP, RSTP greatly reduces the topology convergence time. Under the ideal network topology scale, all switch devices support RSTP and are properly configured. The stability recovery time after the topology changes (link UP or DOWN) can be controlled in seconds. The main functions of RSTP can be summarized as follows:

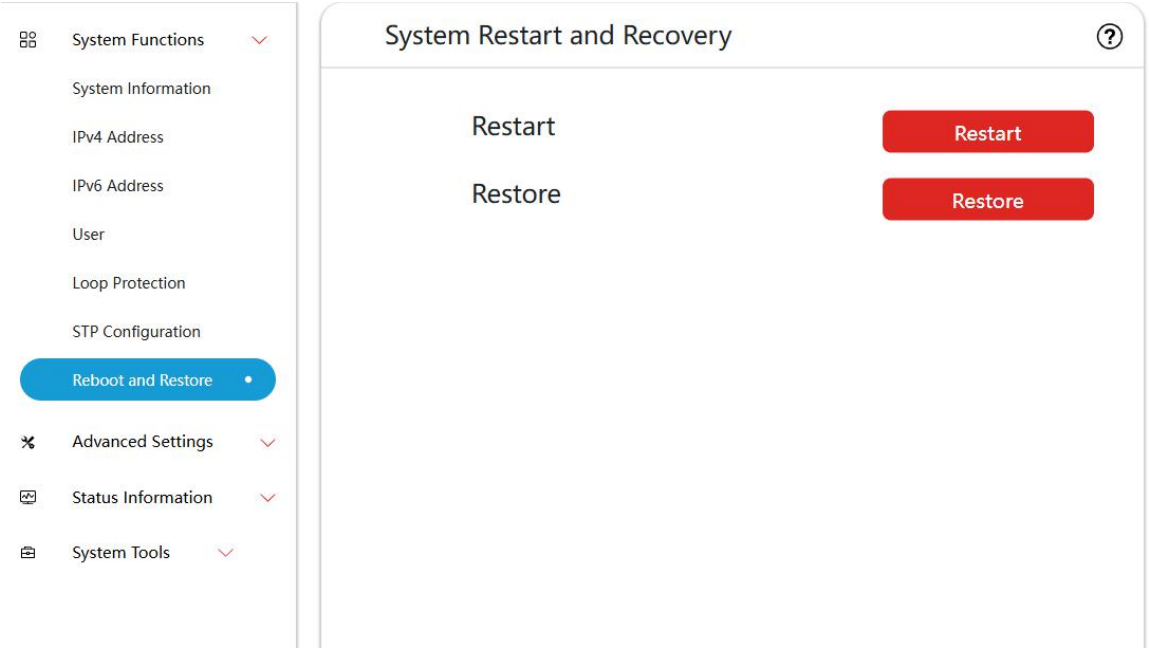
1. Discover and generate an optimal tree topology of LAN;
2. Locate and recover topology faults, automatically update the network topology, enable backup links, and maintain the optimal tree structure.

1. Click System Function > System Time.
2.. This page is used to configure the STP type and edge port of the switch.



1.8 Restart and Recovery

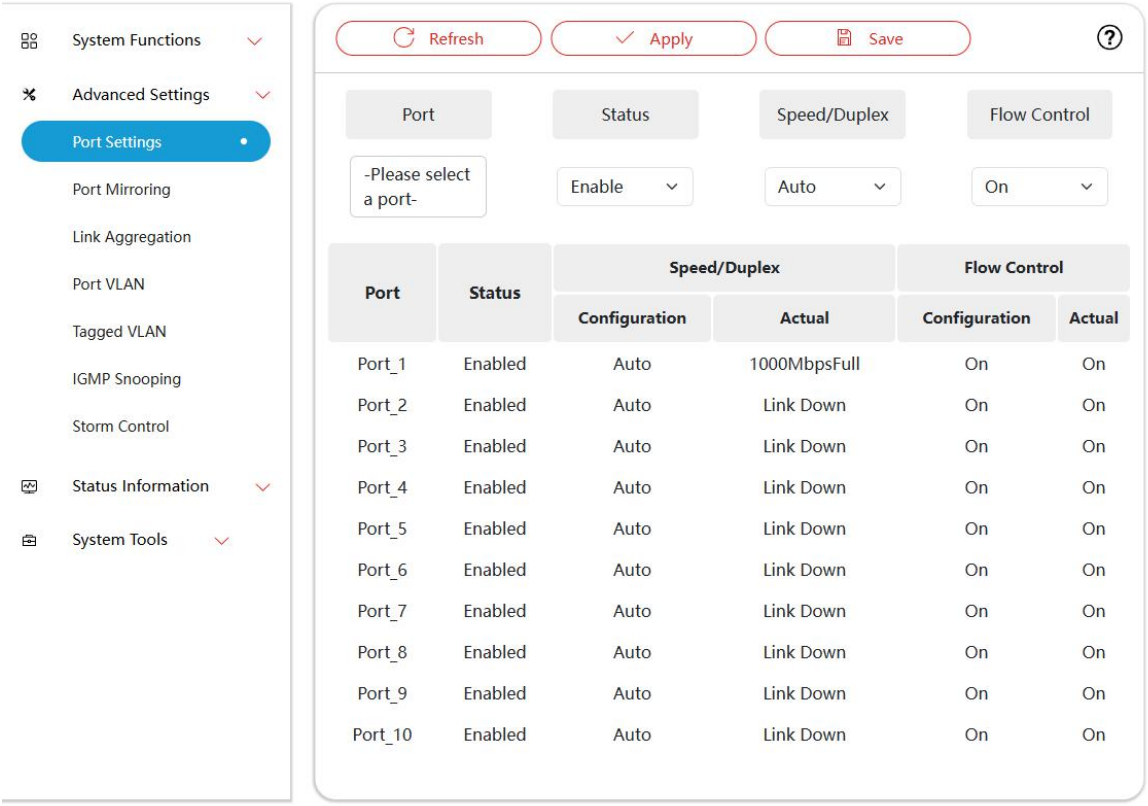
1. Click System Function > Reboot and Restore.
2. The page is used to reset or restart the switch.



Chapter 2 Advanced Settings

2.1 Port Settings

1. Click Advanced Settings -> Port Settings.
2. The page is used to configure switch ports.



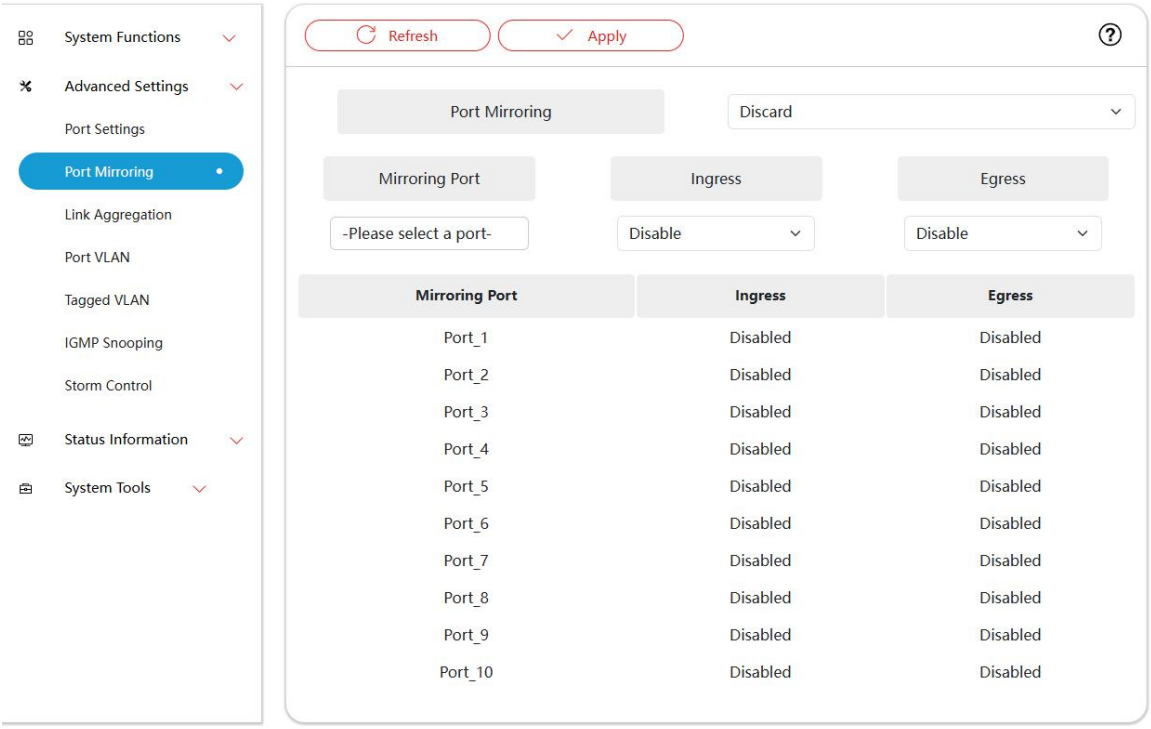
The following table describes the meanings of interface information:

Configuration item	Instructions
Port	Port to be configured
Status	Port switch
Speed/Duplex	Port rate and duplex
Flow Control	Flow control switch

2.2 Port Mirroring

Port mirroring is to copy the packets from the source mirroring port to the destination port. The mirrored destination port is connected to a data detection device. Users can use the device to analyze the packets received by the source mirrored port for network monitoring and troubleshooting.

1. Click Advanced Settings -> Port Mirroring Session.
2. The page is used to configure switch port mirroring. Only one group of mirrors issupported.



The following table describes the meanings of interface information:

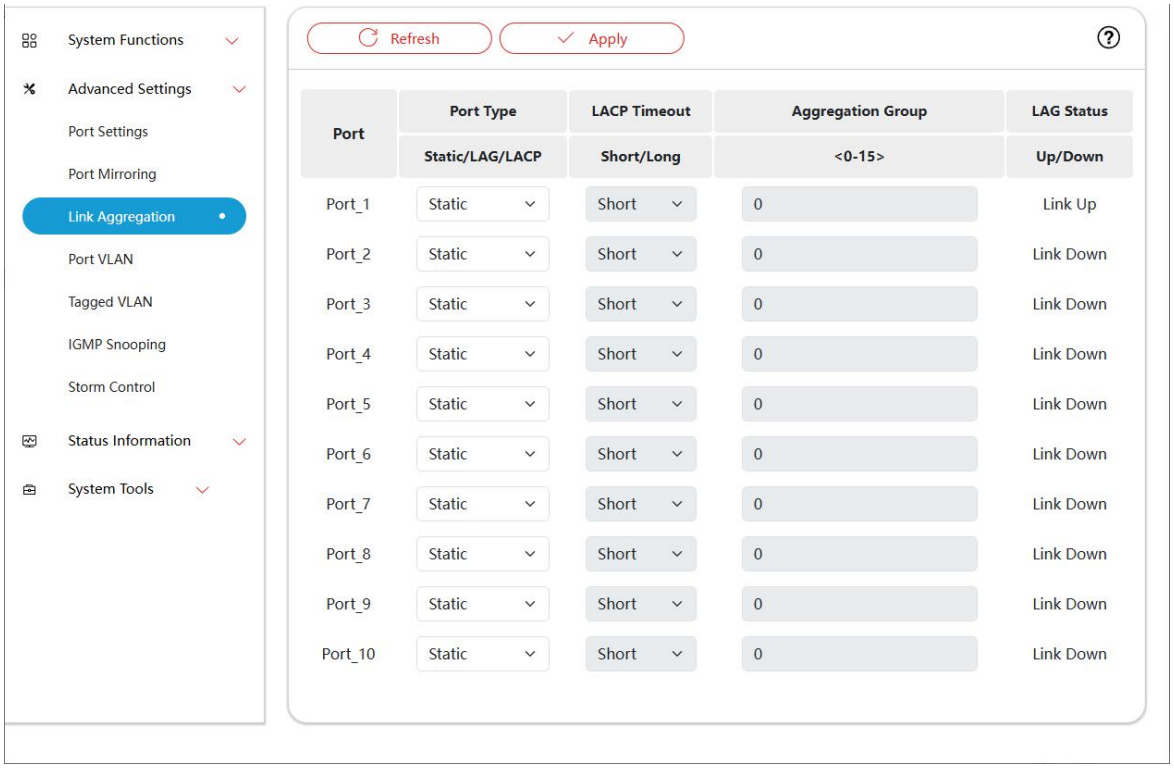
Configuration item	Instructions
Port Mirroring	Select Destination port
Mirroring Port	Select source port
Ingress	The source port import data is enabled or disabled
Egress	The source port egress data is enabled or disabled

2.3 Link Aggregation

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

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

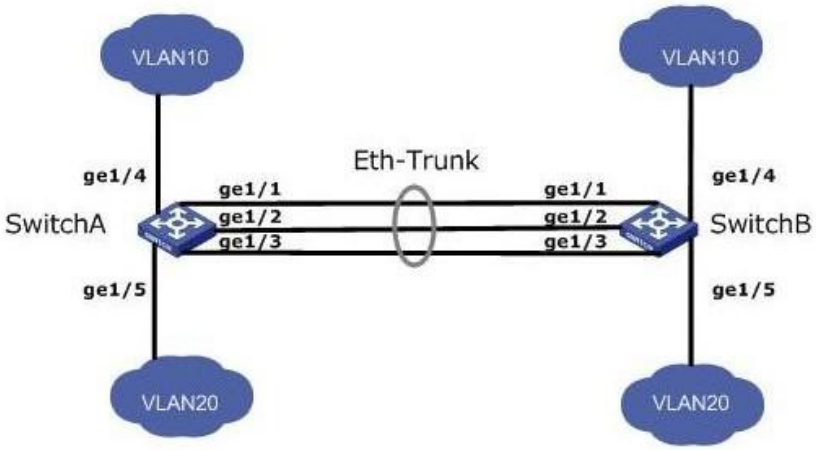
With the continuous expansion of network scale, users have higher and higher requirements for link bandwidth and reliability. In traditional technologies, replacing a high-rate interface board or a device that supports a high-rate interface board is commonly used to increase bandwidth.



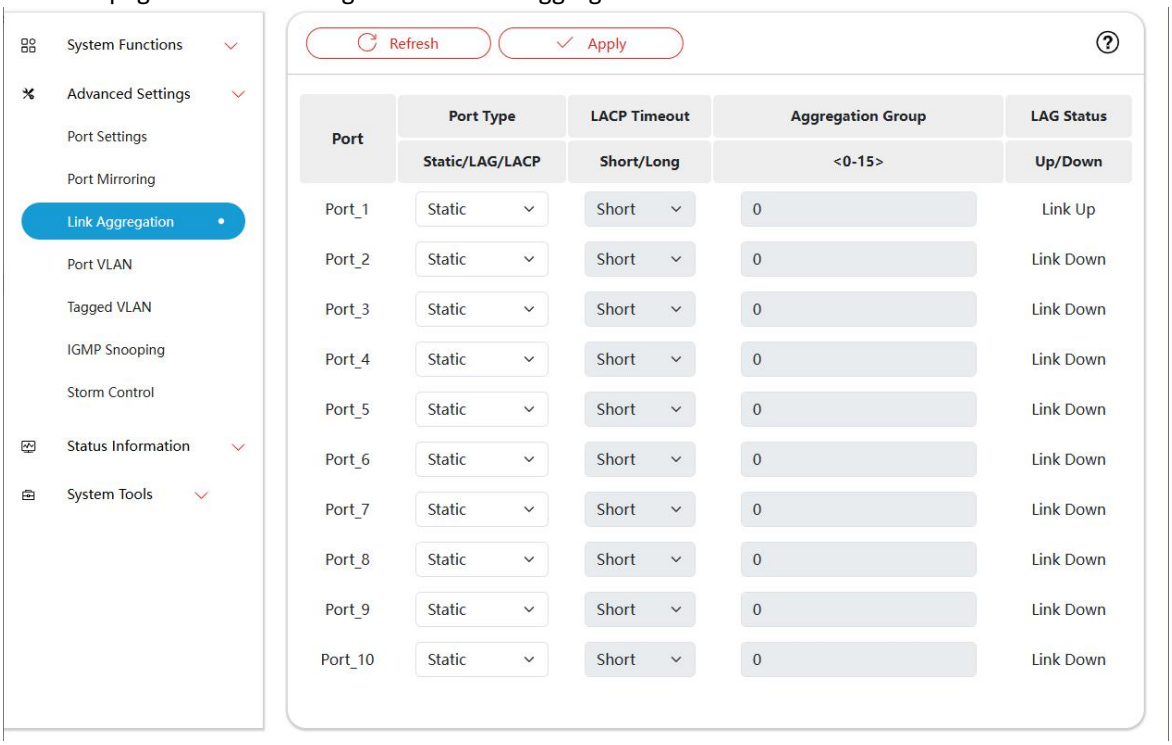
However, this solution requires high cost and is not flexible enough.

The link aggregation technology can increase the link bandwidth by bundling multiple physical interfaces into one logical interface without hardware upgrade. The link aggregation backup mechanism improves reliability and implements load balancing of traffic on different physical links.

As shown in the following figure, SwitchA and SwitchB are connected through three Ethernet physical links. Bundle the three links together to form an Eth-Trunk logical link. The bandwidth of the logical link is equal to the total bandwidth of the original three Ethernet physical links, thereby increasing the bandwidth of the link. At the same time, the three Ethernet physical links back up each other, which effectively improves the reliability of the links.



1. Click Advanced Settings -> Link Aggregation.
2. The page is used to configure switch link aggregation.

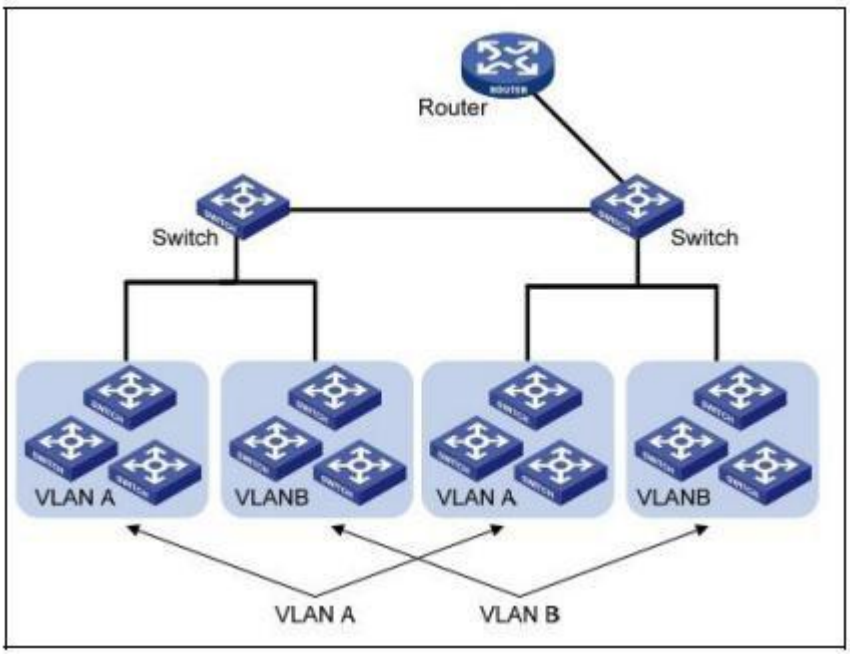


The following table describes the meanings of interface information:

Configuration item	Instructions
Port	Port number
Port Type	The aggregation type can be Static (no aggregation), LAG () Static aggregation or LACP(Dynamic aggregation)
LACP Timeout	The Long timeout period is 90 seconds. The Short timeout period is 3 seconds
Aggregation Group	A maximum of 16 groups are supported
LAG Status	Show connection status

2.4 VLAN

The composition of a VLAN is not limited by physical location, so hosts in the same VLAN do not need to be placed in the same physical space. As shown in the following figure, a VLAN divides a physical LAN into multiple logical Lans. Each VLAN is a broadcast domain. Hosts in a VLAN can exchange packets through traditional Ethernet communication. However, hosts in different vlans can communicate with each other only through network layer devices such as routers or Layer 3 switches.



Compared with traditional Ethernet, VLAN has the following advantages:

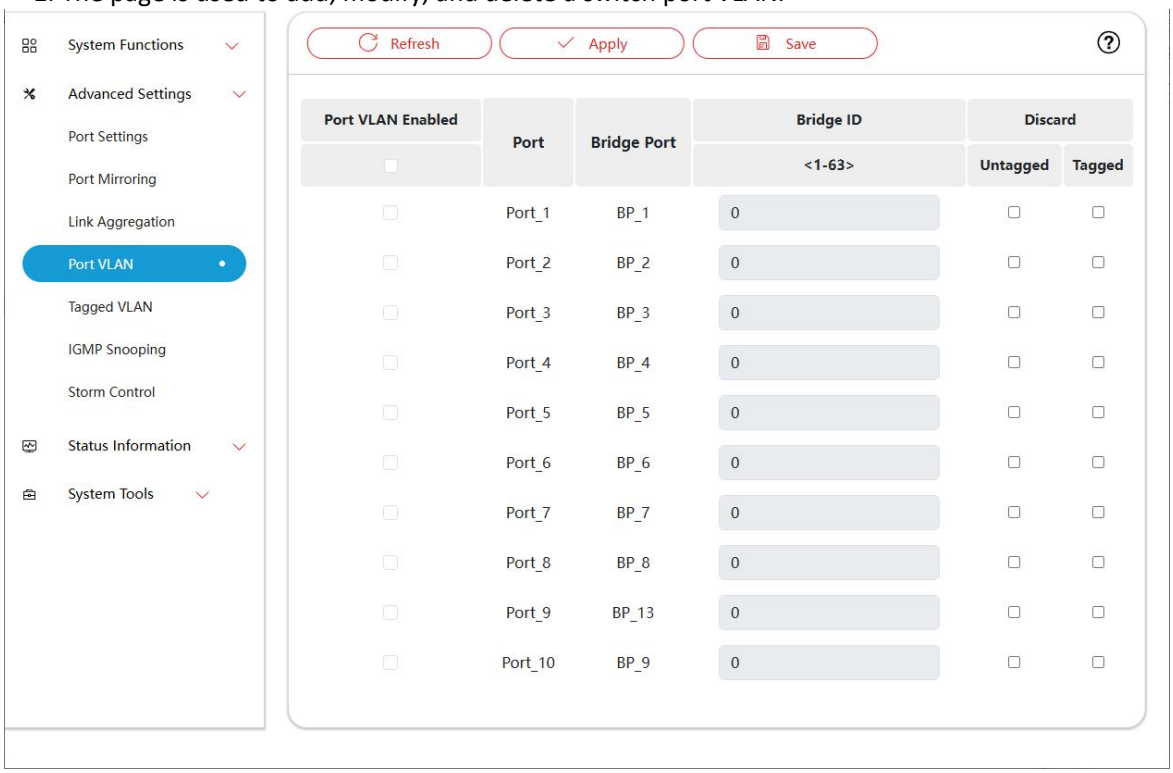
● Control the broadcast domain scope: The broadcast packets on the LAN are restricted to one VLAN, which saves bandwidth and improves the network processing capability.

●enhances LAN security: At the data link layer, packets are isolated by the broadcast domain divided by vlans. Therefore, hosts in each VLAN cannot directly communicate with each other. Therefore, network layer devices, such as routers or Layer-3 switches, forward packets at layer 3.

●Flexible creation of virtual workgroups: You can use vlans to create virtual workgroups across physical networks. When a user moves within the virtual workgroup range, the user can access the network without changing network configuration.

This managed switch supports port-based vlans.

1. Click Advanced Settings ->VLAN.
2. The page is used to add, modify, and delete a switch port VLAN.



The following table describes the meanings of interface information:

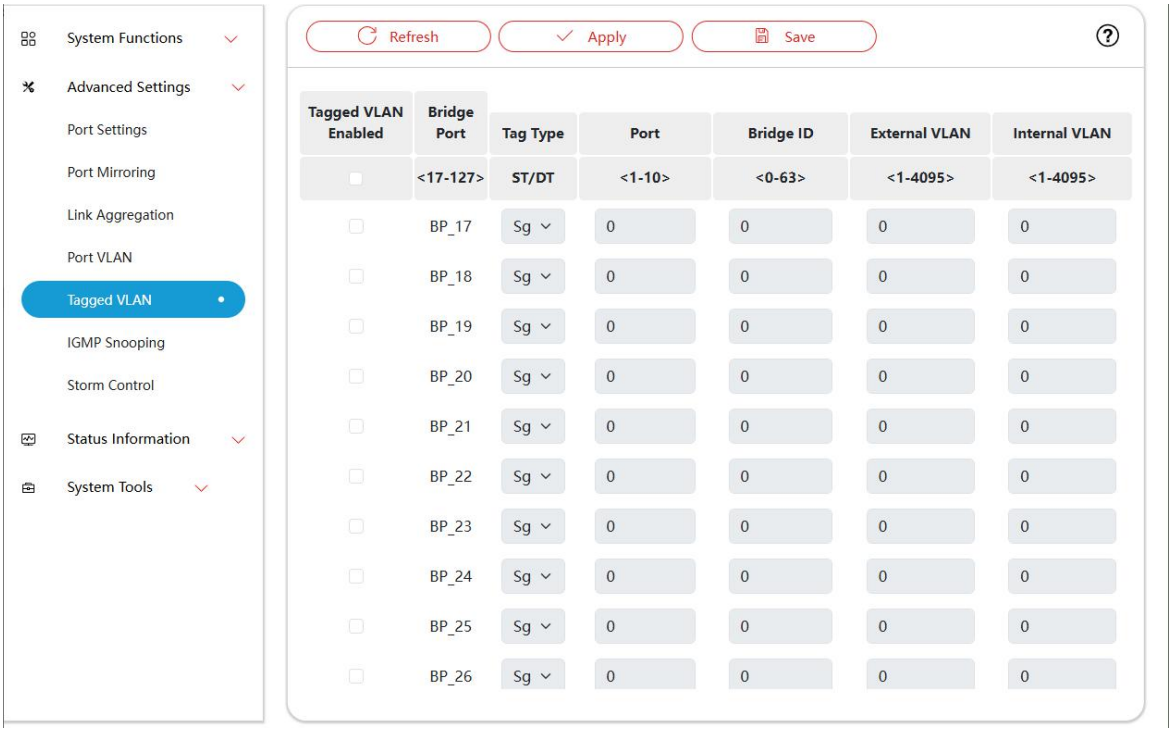
Configuration item	Instructions
Port	Port to be configured
Port Type	Port type Access or Trunk
Access VLAN	VLAN ID of the Access port
Enable VLAN	VLAN ID that is allowed to pass through the Trunk port

2.5 Tagged VLAN

This feature is based on the concept of VLAN tags and provides additional operations when traffic meets the definition of single or dual tags. It then assigns bridge IDs and port numbers as defined in the table. The switch supports up to 128 virtual bridge ports (default is 0 to 16), providing more options for assigning different VLAN tags to bridge IDs and ports.
A single port can be bound to a maximum of 13 virtual bridge ports. A total of 29 virtual bridge ports can be bound.

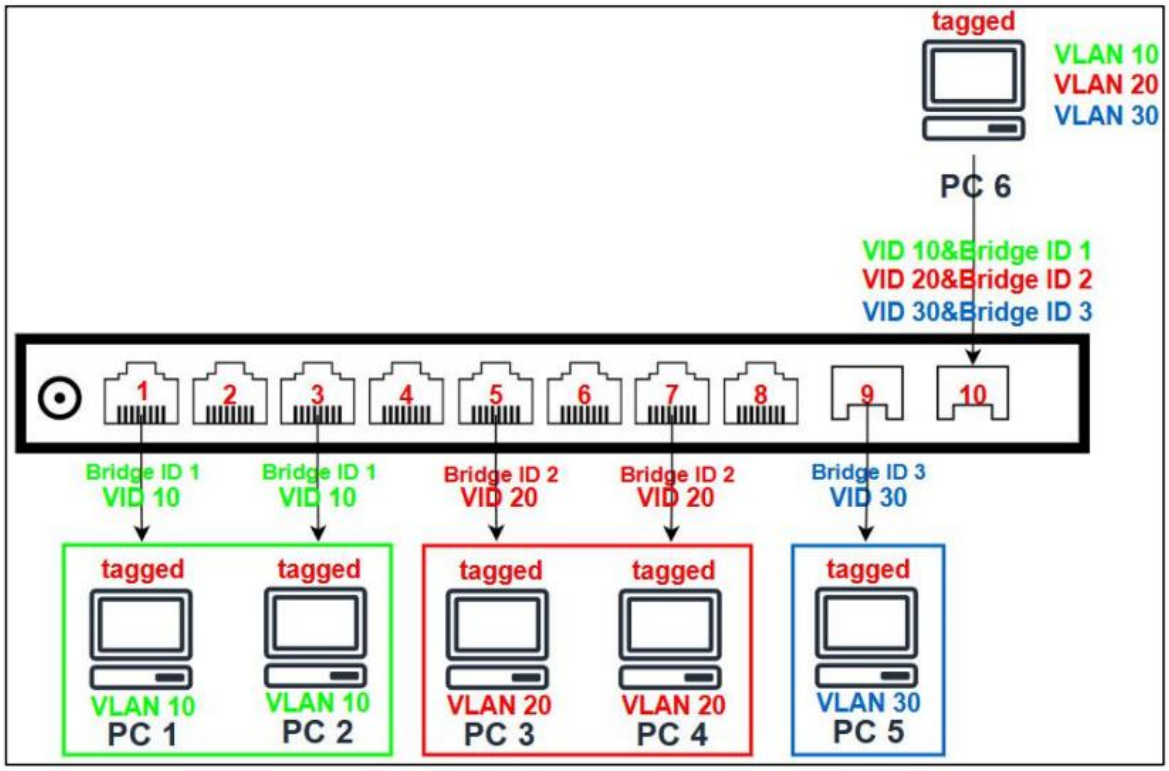
In tag-based VLANs, ports can be configured to transmit data with different VLAN IDs by binding them to different bridge IDs. The bridge ID is associated with the VLAN ID. Ports within the same bridge ID transmit data with consistent VLAN IDs. This is similar to trunk ports in 802.1Q VLANs.

1. Click Advanced Settings — VLAN.
2. This page can be used to configure tag VLANs.



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

query item	Explanation
Tag VLAN enabled	Enable or disable the tag-based VLAN (TBV) feature for each port.
Bridge Port	Assign new virtual bridge ports based on the new TBV rules.
Tag Type	Select single-tag or dual-tag types for the new TBV rules.
Port	Select the physical ports assigned to the bridge ports.
Bridge ID	Select the bridge ID for the bridge ports.
External VLAN	Specify external VLAN ID.
Internal VLAN	Specify internal VLAN ID.
Refresh	Refresh current page.
Apply	Set new configuration.
Save	Save current configuration.



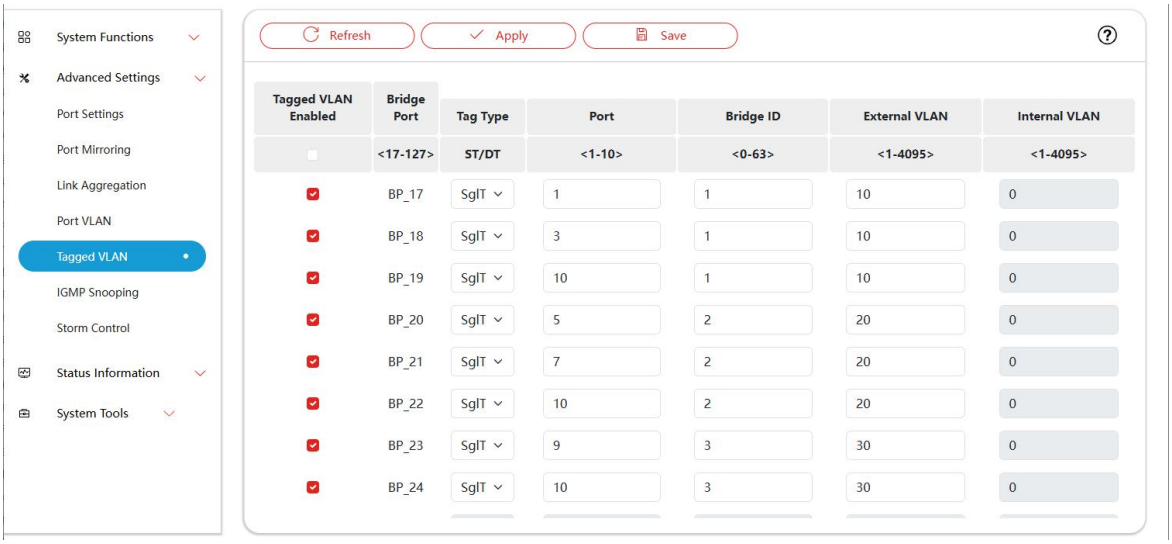
According to the network topology diagram, the corresponding port VLAN settings are as follows:

① Ports 1, 3, and 10 are in bridge ID1 and can receive and send VLAN10 data.

② Ports 5, 7, and 10 are in bridge ID2 and can receive and send VLAN20 data.

③ Ports 9 and 10 are in Bridge ID3 and can both receive and transmit VLAN30 data.

10 ports can output multiple sets of VLAN data.

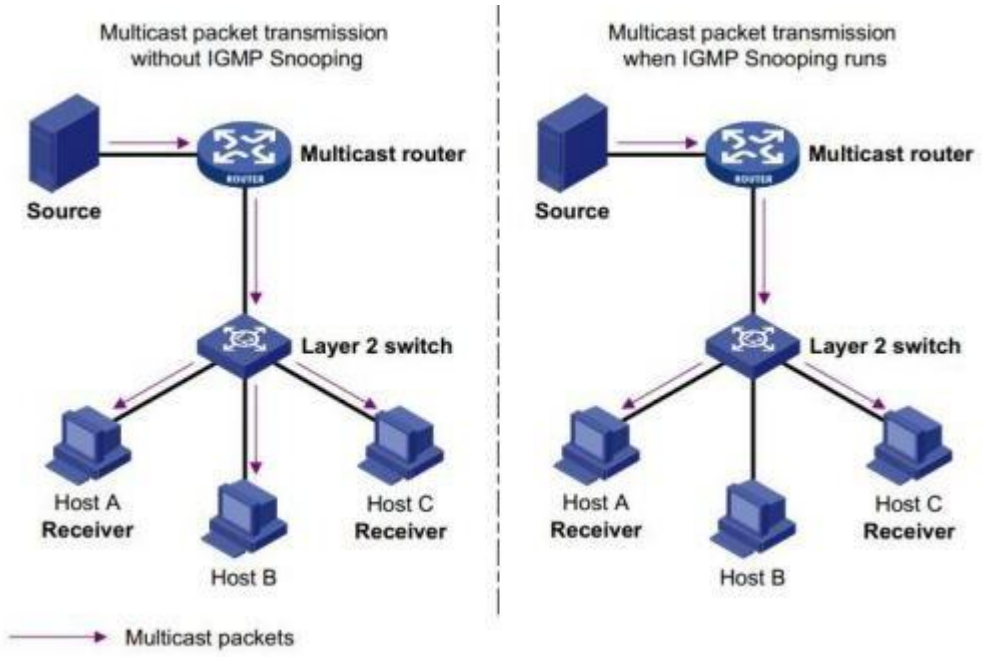


2.6 IGMP Listening

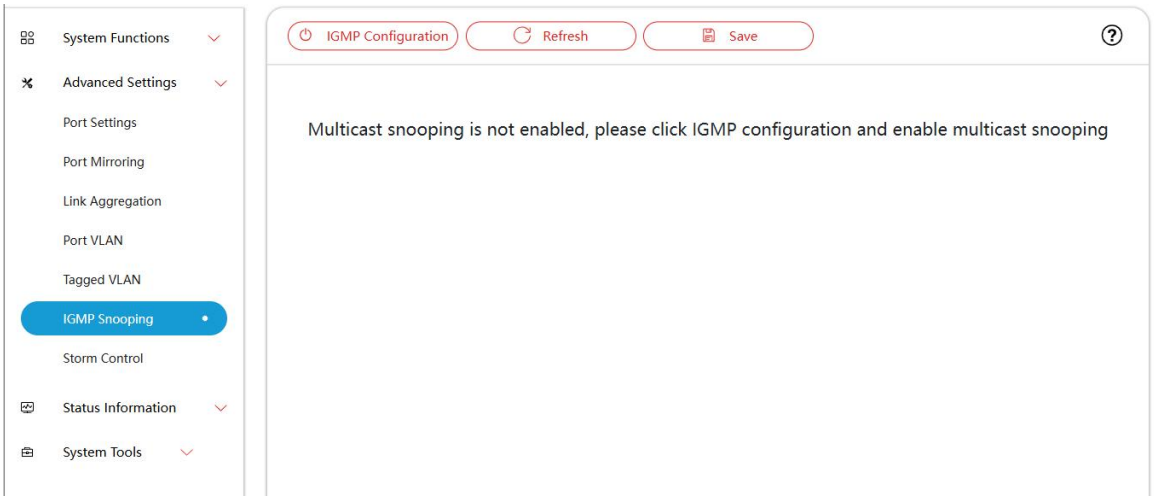
Internet Group Management Protocol Snooping (IGMP Snooping) is a multicast restriction mechanism running on Layer 2 devices for managing and controlling multicast groups.

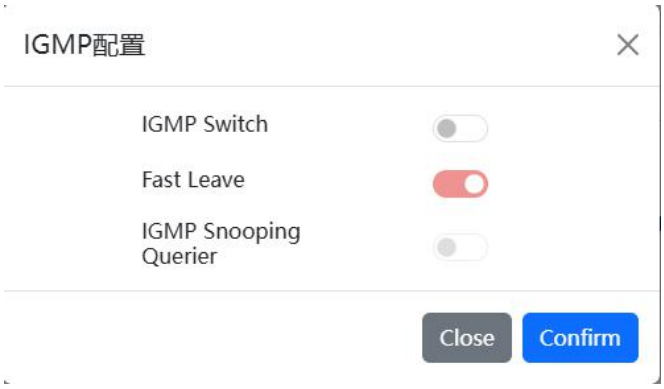
The Layer 2 device running IGMP listening analyzes the received IGMP packets, sets up a mapping relationship between the port and the MAC multicast address, and forwards the multicast data based on the mapping relationship.

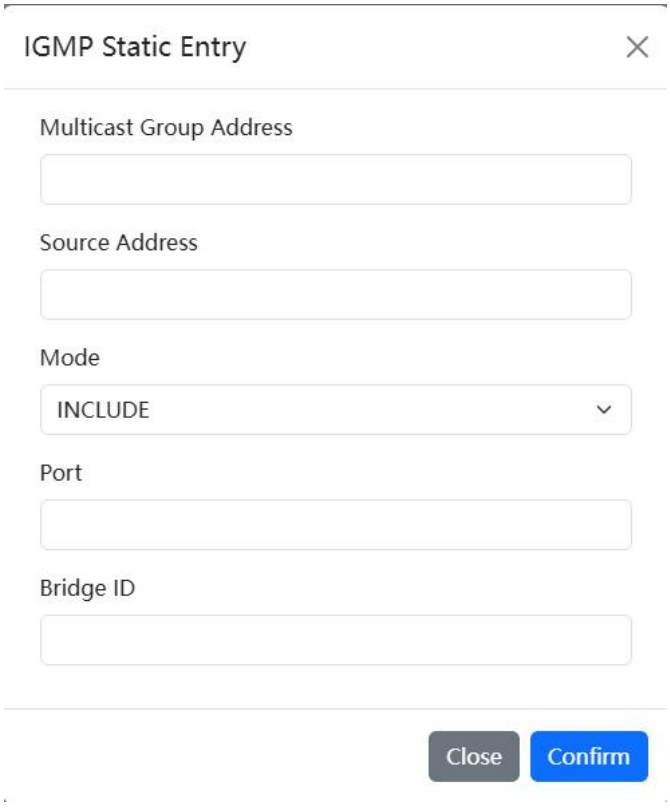
As shown in the following figure, when the Layer 2 device does not run IGMP listening, the multicast data is broadcast at Layer 2. After IGMP interception is enabled on a Layer 2 device, the multicast data of a known multicast group is not broadcast at Layer 2, but is broadcast to a specified receiver at Layer 2. However, the unknown multicast data is still broadcast at Layer 2.



1. Click Advanced Settings ->IGMP Listening.
2. The page is used to configure IGMP listening on the switch. Before setting this parameter, enable multicast listening.





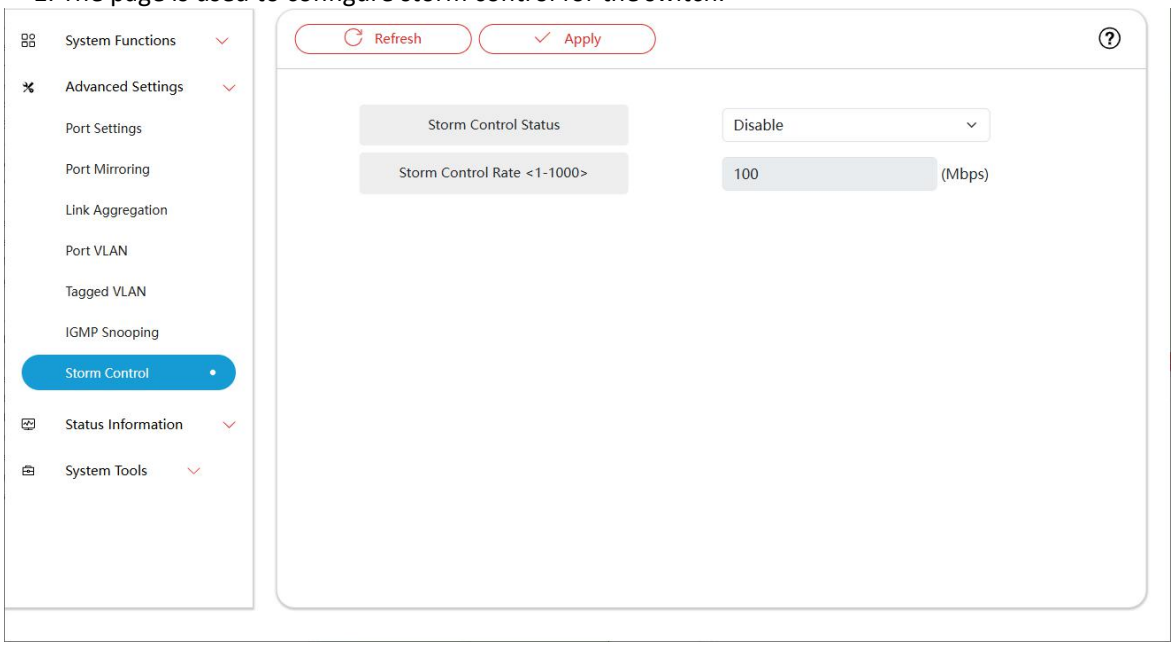


The meaning of the page information is shown in the table below:

Configuration item	Instructions
IGMP switch	Enable or disable IGMP snooping. By limiting the proliferation of multicast traffic, it improves network efficiency.
FAST Leave	Enable or disable fast leave. When enabled, it allows devices to immediately leave multicast groups.
IGMP Snooping Querier	Enable or disable IGMP snooping querier. When enabled, it allows devices to take over the role of multicast routers and send IGMP queries.
IGMP static entries	Allows you to manually add static entries to the IGMP snooping table. It requires specifying the group IP address, source IP address, mode (include/exclude), port (1 to 16), and bridge ID (0 to 63).
Add	Add a new entry.
Delete	Delete Delete an existing entry.
Save	Save the configuration.

2.7 Storm Control

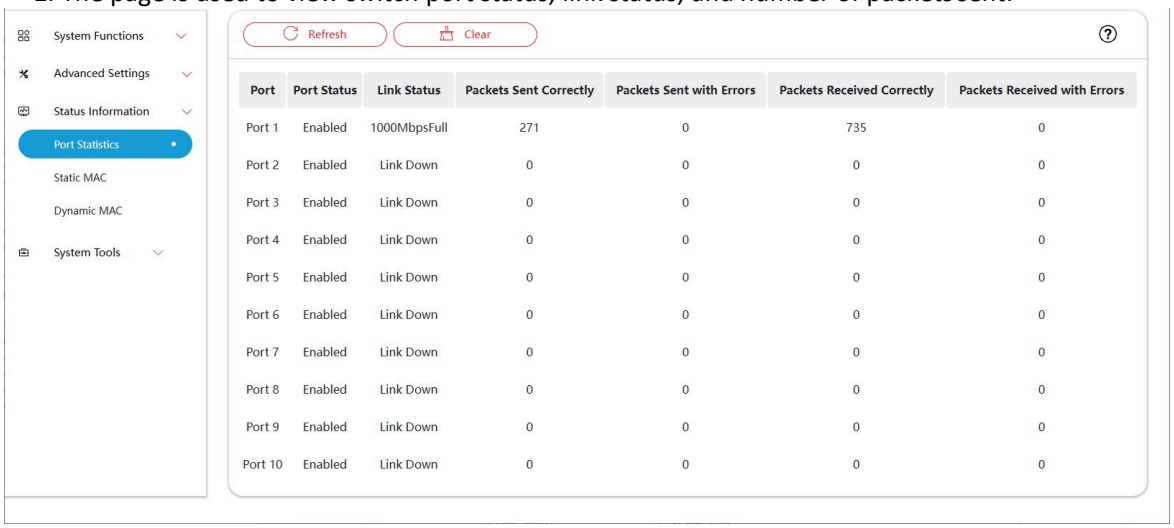
1. Click Advanced Settings -> Storm Control.
2. The page is used to configure storm control for the switch.



Chapter 3 State Information

3.1 Port Statistics

1. Click Status Information -> Port Statistics.
2. The page is used to view switch port status, link status, and number of packets sent.



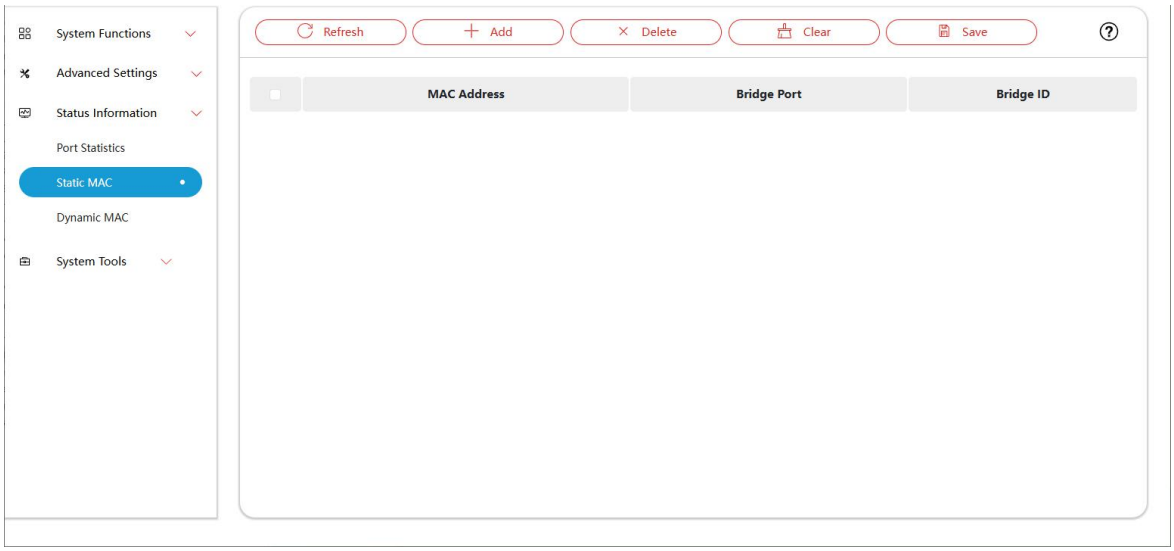
Port	Port Status	Link Status	Packets Sent Correctly	Packets Sent with Errors	Packets Received Correctly	Packets Received with Errors
Port 1	Enabled	1000MbpsFull	271	0	735	0
Port 2	Enabled	Link Down	0	0	0	0
Port 3	Enabled	Link Down	0	0	0	0
Port 4	Enabled	Link Down	0	0	0	0
Port 5	Enabled	Link Down	0	0	0	0
Port 6	Enabled	Link Down	0	0	0	0
Port 7	Enabled	Link Down	0	0	0	0
Port 8	Enabled	Link Down	0	0	0	0
Port 9	Enabled	Link Down	0	0	0	0
Port 10	Enabled	Link Down	0	0	0	0

The following table describes the meanings of interface information:

Configuration item	Instructions
Port	Port list
Port Status	Port status
Link Status	Port link state
Packets Sent Correctly	The port sends the correct number of packets
Packets Sent with Errors	Number of error packets sent by the port
Packets Received Correctly	The port received the correct number of packets
Packets Received Errors	Number of error packets received by the port

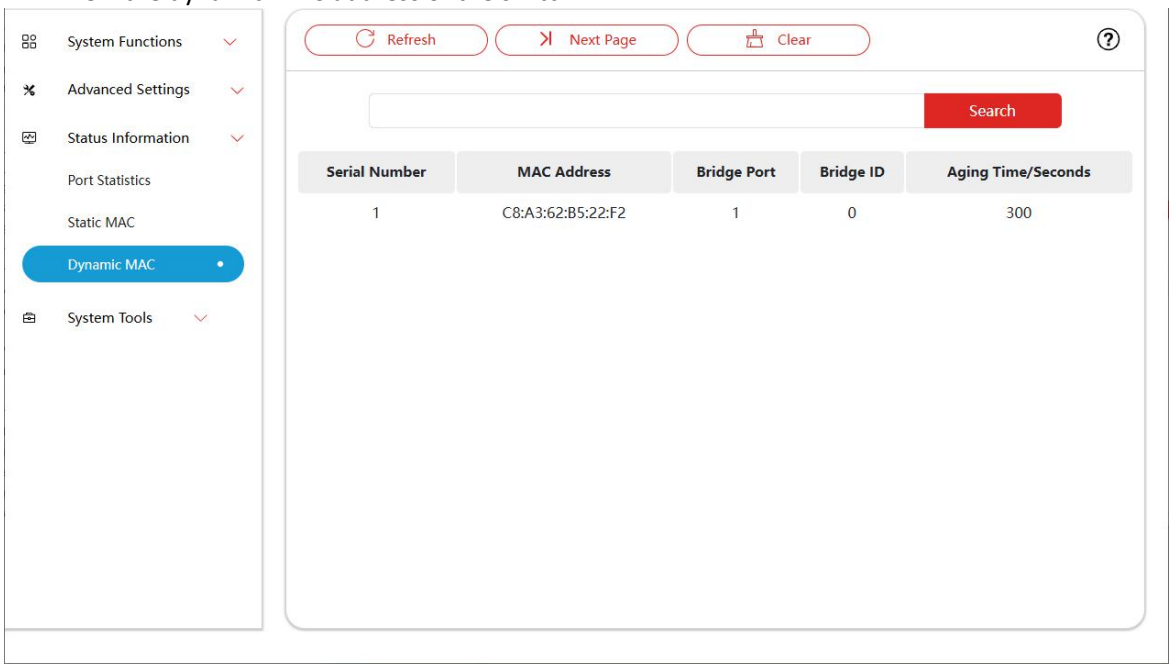
3.2 Static MAC

1. Click Status Info -> Static MAC.
2. This page is used to add and delete static MAC addresses for switches.



3.3 Dynamic MAC

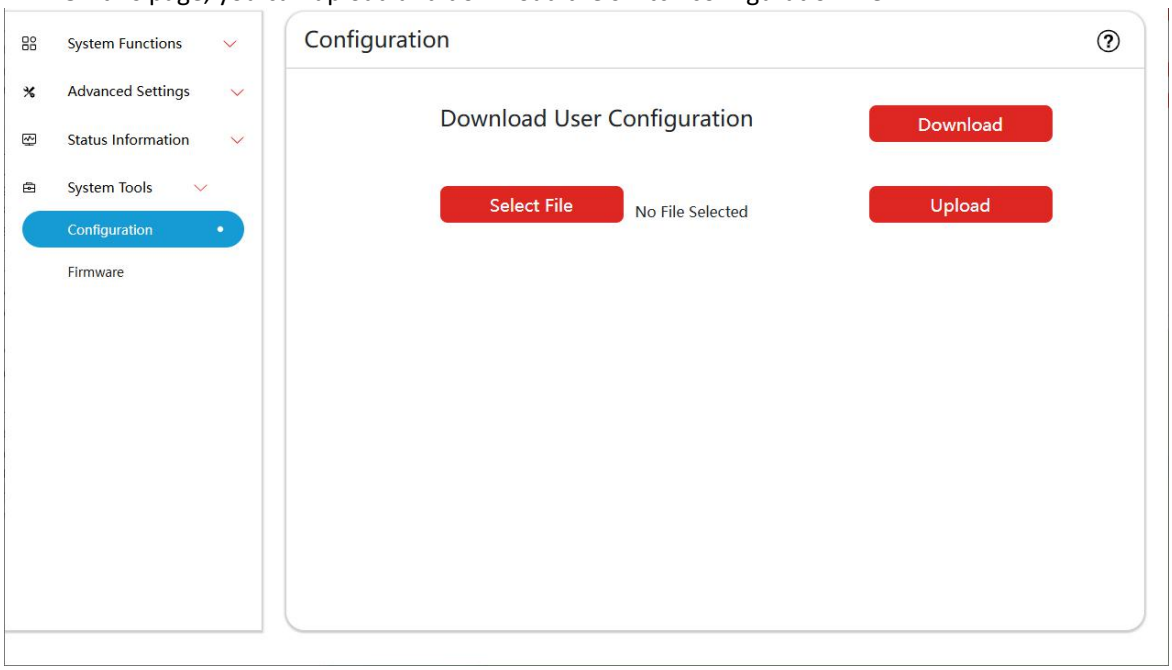
1. Click Status Information -> Dynamic MAC.
2. View the dynamic MAC address of the switch.



Chapter 4 Basic business

4.1 Configuration

1. Click Basic Service > Configuration.
2. On this page, you can upload and download the switch configuration file.



4.2 Firmware

1. Click Basic Service -> Firmware.
2. This page is used to download and upgrade switch firmware.