



**XQS-3126**



# Web Management Guide

# Table of Contents

Chapter 1 Accessing the Switch .....	3
1.1 Accessing the Switch through HTTP.....	3
1.2 Introduction of Web Interface.....	3
1.2.1 Top Control Bar.....	3
1.2.2 Navigation Bar .....	4
1.2.3 Configuration Information Area.....	5
1.2.4 Configuration Area.....	5
Chapter 2 Main.....	6
Chapter 3 Device Status .....	7
3.1 Interface Status.....	7
3.2 Interface Flow .....	7
3.3 MAC Address Table .....	7
3.4 Log Query.....	8
Chapter 4 Basic Configuration .....	9
4.1 Clock Management.....	9
Chapter 5 Configuration of the Physical Interface.....	10
5.1 Configuring the Attributes of the Port .....	10
5.2 Rate control.....	10
5.3 Port mirroring .....	11
5.4 Keepalive Detection .....	11
5.5 Loopback Detection.....	11
5.6 Port security .....	12
5.6.1 IP Binding Configuration .....	12
5.6.2 Static MAC Filtration Mode .....	12
5.6.3 Static MAC Filtration Item .....	13
5.6.4 Dynamic MAC Filtration Mode.....	13
5.7 Storm control.....	14
5.8 Port Protect Group Configuration .....	14
4.8.1 Port Protect Group List.....	14
4.8.2 Port Protect Group Configuration .....	15
Chapter 6 L2 Configuration.....	17
6.1 VLAN Configuration.....	17
6.1.1 VLAN Config .....	17
6.1.2 Port VLAN Config .....	17
6.2 STP Configuration .....	18
6.2.1 STP Status Information .....	18
6.2.2 STP Port Config.....	18
6.2.3 STP Port Guard Config .....	19
6.3 IGMP-Snooping Configuration.....	19
6.3.1 IGMP-Snooping Configuration.....	19
6.3.2 IGMP-Snooping VLAN List .....	20
6.3.3 Static Multicast Address .....	21

---

6.3.4 Multicast List .....	21
6.3.5 IGMP Snooping Statistic Info .....	22
6.4 ARP .....	22
6.4.1 Static ARP .....	22
6.4.2 ARP Information .....	23
6.5 Port Channel .....	23
6.5.1 Port Aggregation Configuration .....	23
6.5.2 Port Channel Group Loading Balance Configuration .....	24
6.6 DHCP Snooping .....	24
6.6.1 Global Configuration .....	24
6.6.2 VLAN Config .....	25
6.6.3 Interface Configuration .....	26
6.6.4 Interface Binding list .....	26
Chapter 7 L3 Configuration .....	28
7.1 Configuring the VLAN Interface .....	28
7.2 Static Routing Configuration .....	29
Chapter 8 Advanced Configuration .....	30
8.1 QoS Configuration .....	30
8.1.1 Configuring QoS Port .....	30
8.1.2 Global QoS Configuration .....	30
8.1.3 IP DSCP Mapping .....	31
8.2 IP Access List .....	32
8.2.1 Setting IP Access List .....	32
8.2.2 Applying the IP Access Control List .....	34
8.3 MAC Access Control List .....	34
8.3.1 Setting the Name of the MAC Access Control List .....	34
8.3.2 Applying the MAC Access Control List .....	36
Chapter 9 System .....	37
9.1 Reboot .....	37
9.1.1 Refactory .....	37
9.1.2 Reboot .....	37
9.2 Upgrade .....	38
9.2.1 System Upgrade .....	38
9.3 Tools .....	39
9.3.1 General Diagnosis .....	39

# Chapter 1 Accessing the Switch

## 1.1 Accessing the Switch through HTTP

interface g0/0/0  
auto-nego: enable

logon Web GUI  
ip address: 192.168.1.1  
subnet mask: 255.255.255.0  
username: admin  
password: admin

interface tg0/0/1 to tg0/0/24  
interface cg0/0/1 to cg0/0/2  
auto-nego: disable

interface vlan1  
ip address: 192.168.2.1  
subnet mask: 255.255.255.0  
username: admin  
password: admin



When the switch is initially used, you can use the Web access without any extra settings:

1. Modify the IP address of the network adapter and subnet mask of your computer to 192.168.1.100 and 255.255.255.0 respectively.
2. Open a browser and enter 192.168.1.1 in the address bar, then press Enter. In the login screen that appears, enter the factory default username admin and password admin, then click OK.
3. If the Google Chrome or Firefox Explorer browser is used, you can see the dialog box in figure 1. Both the original username and the password are “admin”, which is capital sensitive.

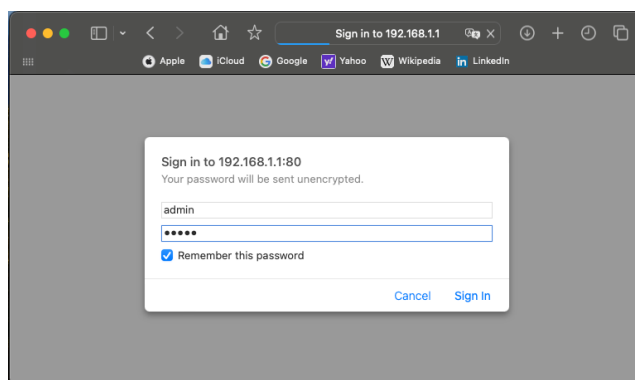


Figure 1: ID checkup of WEB login

## 1.2 Introduction of Web Interface

The homepage consists of the top control bar, the navigation bar, the configuration area and the bottom control bar.

### 1.2.1 Top Control Bar

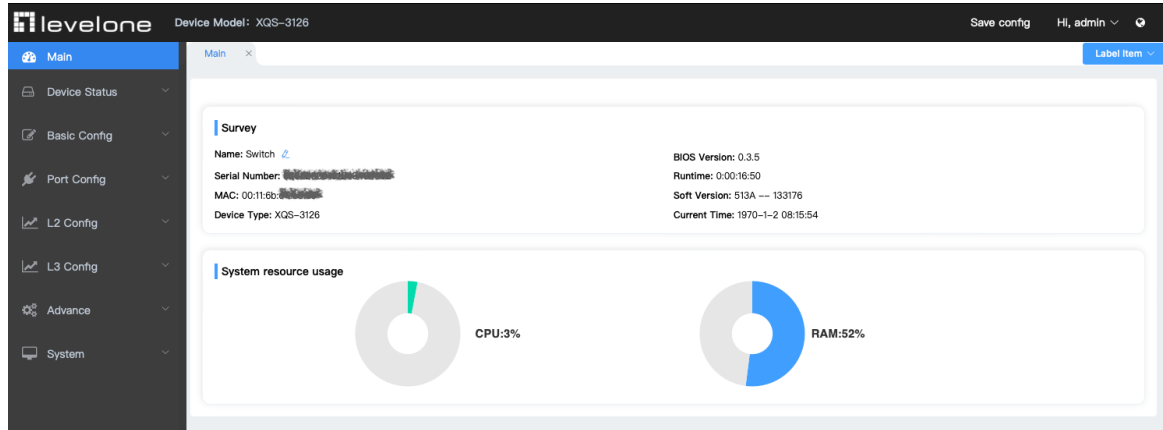


Figure 2: Top control bar

Device Model	Show the current device model.
Save Config	Write the current settings to the configuration file of the device. It is equivalent to the execution of the <b>write</b> command.
About (Hi, admin)	Displays vendor information and sets automatic refresh.
Change Password (Hi, admin)	Change current password.
Logout (Hi, admin)	Exit from the current login state.
	After you click "logout", you have to enter the username and the password again if you want to continue the Web function.

After you configure the device, the result of the previous step will appear on the left side of the top control bar. If error occurs, please check your configuration and retry it later.

### 1.2.2 Navigation Bar

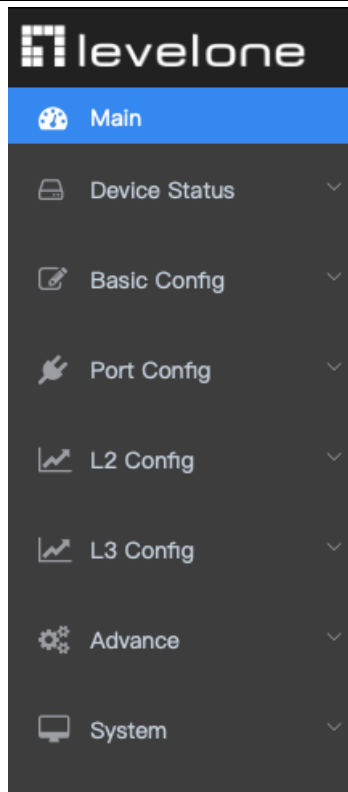


Figure 3 Navigation bar

The contents in the navigation bar are shown in a form of list and are classified according to types. By default, the list is located at “Runtime Info”. If a certain item need be configured, please click the group name and then the sub-item. For example, to browse the flux of the current port, you have to click “Interface State” and then “Interface Flow”.

---

**Note:**

The limited user can only browse the state of the device and cannot modify the configuration of the device. If you log on to the Web with limited user's permissions, only “Interface State” will appear.

---

### 1.2.3 Configuration Information Area

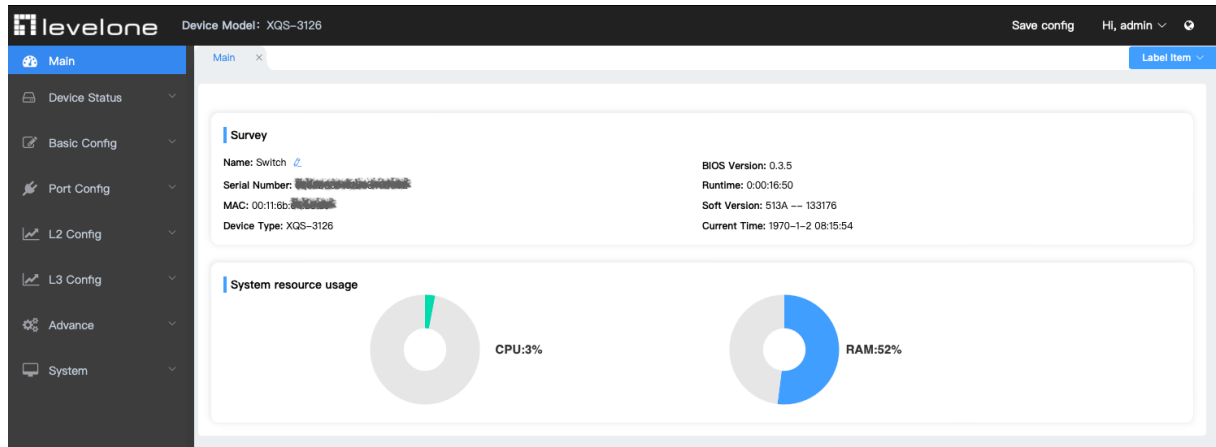


Figure 4 Configuration Area

The configuration display area shows the state and configuration of the device. The contents of this area can be modified by the clicking of the items in the navigation bar.

### 1.2.4 Configuration Area

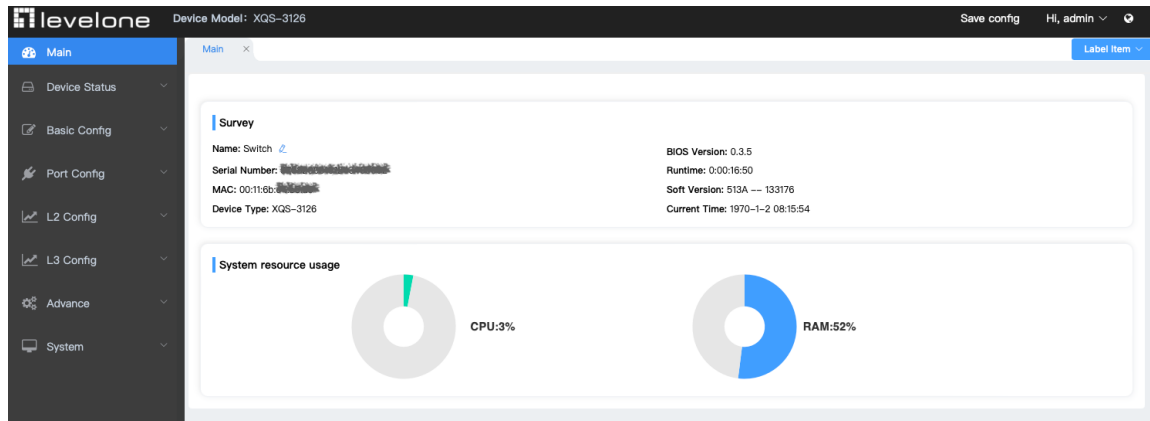
The configuration area is to show the content that is selected in the navigation area. The configuration area always contains one or more buttons, and their functions are listed in the following table:

Refresh	Refresh the content shown in the current configuration area.
Apply	Apply the modified configuration to the device.  The application of the configuration does not mean that the configuration is saved in the configuration file. To save the configuration, you have to click "Save All" on the top control bar.
New	Creates a list item. For example, you can create a VLAN item or a new user.
Delete	Deletes an item in the list.
Back	Go back to the previous-level configuration page.

## Chapter 2 Main

After logging in, the web page will enter the home page, where the basic information of the switch and the system resource usage are displayed.

On the left is the functional navigation bar.





## Chapter 3 Device Status

### 3.1 Interface Status

If you click **Device Status -> Interface Status** in the navigation bar, the **Interface Status** page appears.

Port	Port Desc	Enable	Status	MAC Address	Speed	Duplex	Input Rate	Output Rate	Flow Control
tg1/0/1		Enable	Disable	00:11:db-e4:3d:a6	1000Mb	full	0b/s/sec	0b/s/sec	Disable
tg1/0/2		Enable	Disable	00:11:db-e4:3d:a6	1000Mb	full	0b/s/sec	0b/s/sec	Disable
tg1/0/3		Enable	Disable	00:11:db-e4:3d:a6	1000Mb	full	0b/s/sec	0b/s/sec	Disable
tg1/0/4		Enable	Disable	00:11:db-e4:3d:a6	1000Mb	full	0b/s/sec	0b/s/sec	Disable
tg1/0/5		Enable	Disable	00:11:db-e4:3d:a6	1000Mb	full	0b/s/sec	0b/s/sec	Disable
tg1/0/6		Enable	Disable	00:11:db-e4:3d:a6	1000Mb	full	0b/s/sec	0b/s/sec	Disable
tg1/0/7		Enable	Disable	00:11:db-e4:3d:a6	1000Mb	full	0b/s/sec	0b/s/sec	Disable
tg1/0/8		Enable	Disable	00:11:db-e4:3d:a6	1000Mb	full	0b/s/sec	0b/s/sec	Disable
tg1/0/9		Enable	Disable	00:11:db-e4:3d:a6	1000Mb	full	0b/s/sec	0b/s/sec	Disable
tg1/0/10		Enable	Disable	00:11:db-e4:3d:a6	1000Mb	full	0b/s/sec	0b/s/sec	Disable
tg1/0/11		Enable	Disable	00:11:db-e4:3d:a6	1000Mb	full	0b/s/sec	0b/s/sec	Disable
tg1/0/12		Enable	Disable	00:11:db-e4:3d:a6	1000Mb	full	0b/s/sec	0b/s/sec	Disable
tg1/0/13		Enable	Disable	00:11:db-e4:3d:a6	1000Mb	full	0b/s/sec	0b/s/sec	Disable
tg1/0/14		Enable	Disable	00:11:db-e4:3d:a6	1000Mb	full	0b/s/sec	0b/s/sec	Disable
tg1/0/15		Enable	Disable	00:11:db-e4:3d:a6	1000Mb	full	0b/s/sec	0b/s/sec	Disable
tg1/0/16		Enable	Disable	00:11:db-e4:3d:a6	1000Mb	full	0b/s/sec	0b/s/sec	Disable
tg1/0/17		Enable	Disable	00:11:db-e4:3d:a6	1000Mb	full	0b/s/sec	0b/s/sec	Disable
tg1/0/18		Enable	Disable	00:11:db-e4:3d:a6	1000Mb	full	0b/s/sec	0b/s/sec	Disable
tg1/0/19		Enable	Disable	00:11:db-e4:3d:a6	1000Mb	full	0b/s/sec	0b/s/sec	Disable
tg1/0/20		Enable	Disable	00:11:db-e4:3d:a6	1000Mb	full	0b/s/sec	0b/s/sec	Disable

### 3.2 Interface Flow

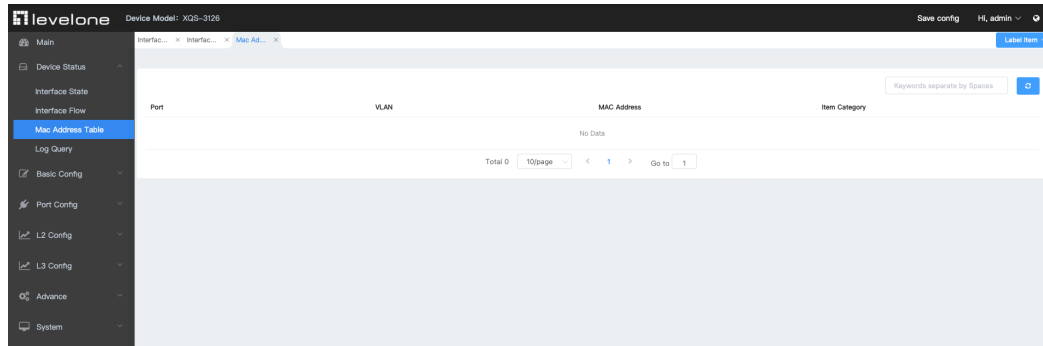
If you click **Device Status -> Interface Flow** in the navigation bar, the **Interface flow** page appears.

Click "Clear" to clear the selected port flow data

Port	Port Desc	Enable	Status	Send Bytes	Send Packets	Receive Bytes	Receive Packets	Discard	Discard Rate
tg1/0/1		Enable	Disable	0	0	0	0	0	0%
tg1/0/2		Enable	Disable	0	0	0	0	0	0%
tg1/0/3		Enable	Disable	0	0	0	0	0	0%
tg1/0/4		Enable	Disable	0	0	0	0	0	0%
tg1/0/5		Enable	Disable	0	0	0	0	0	0%
tg1/0/6		Enable	Disable	0	0	0	0	0	0%
tg1/0/7		Enable	Disable	0	0	0	0	0	0%
tg1/0/8		Enable	Disable	0	0	0	0	0	0%
tg1/0/9		Enable	Disable	0	0	0	0	0	0%
tg1/0/10		Enable	Disable	0	0	0	0	0	0%
tg1/0/11		Enable	Disable	0	0	0	0	0	0%
tg1/0/12		Enable	Disable	0	0	0	0	0	0%
tg1/0/13		Enable	Disable	0	0	0	0	0	0%
tg1/0/14		Enable	Disable	0	0	0	0	0	0%
tg1/0/15		Enable	Disable	0	0	0	0	0	0%
tg1/0/16		Enable	Disable	0	0	0	0	0	0%
tg1/0/17		Enable	Disable	0	0	0	0	0	0%
tg1/0/18		Enable	Disable	0	0	0	0	0	0%
tg1/0/19		Enable	Disable	0	0	0	0	0	0%
tg1/0/20		Enable	Disable	0	0	0	0	0	0%

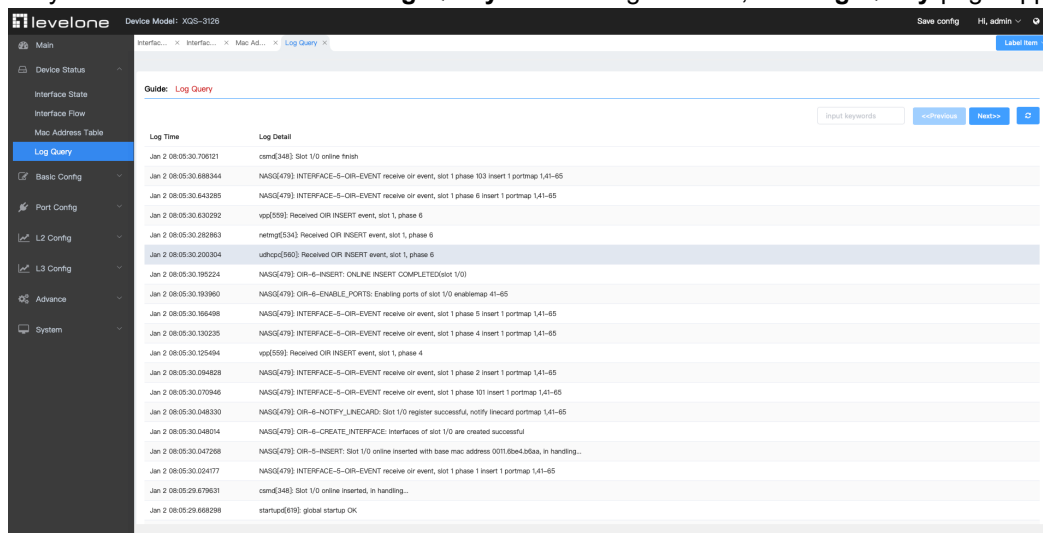
### 3.3 MAC Address Table

If you click **Device Status -> MAC Address Table** in the navigation bar, the **MAC Address Table** page appears.



### 3.4 Log Query

If you click **Device Status -> Log Query** in the navigation bar, the **Log Query** page appears.



## Chapter 4 Basic Configuration

### 4.1 Clock Management

If you click **Basic Configuration -> Clock Mgr.**, the **Time Setting** page appears.

The screenshot shows the H3C Web Configuration interface for a device with model XGS-3126. The left sidebar contains a navigation menu with options: Main, Device Status, Interface State, Interface Flow, Mac Address Table, Log Query, Basic Config (checked), Clock Mgr. (highlighted), Port Config, L2 Config, L3 Config, Advance, and System. The main content area is titled 'Time Setting' and displays the following fields:

- System Time: 1970-1-2 09:38:58
- Model Select: ☒ Set Time Manually, ☐ Network Time Synchronization
- Below the radio buttons are two input fields: 'Select date' and 'Select time'.
- An 'Apply' button is located at the bottom of the form.

This screenshot shows the same H3C Web Configuration interface, but with the 'Network Time Synchronization' option selected. The 'Time Setting' page displays:

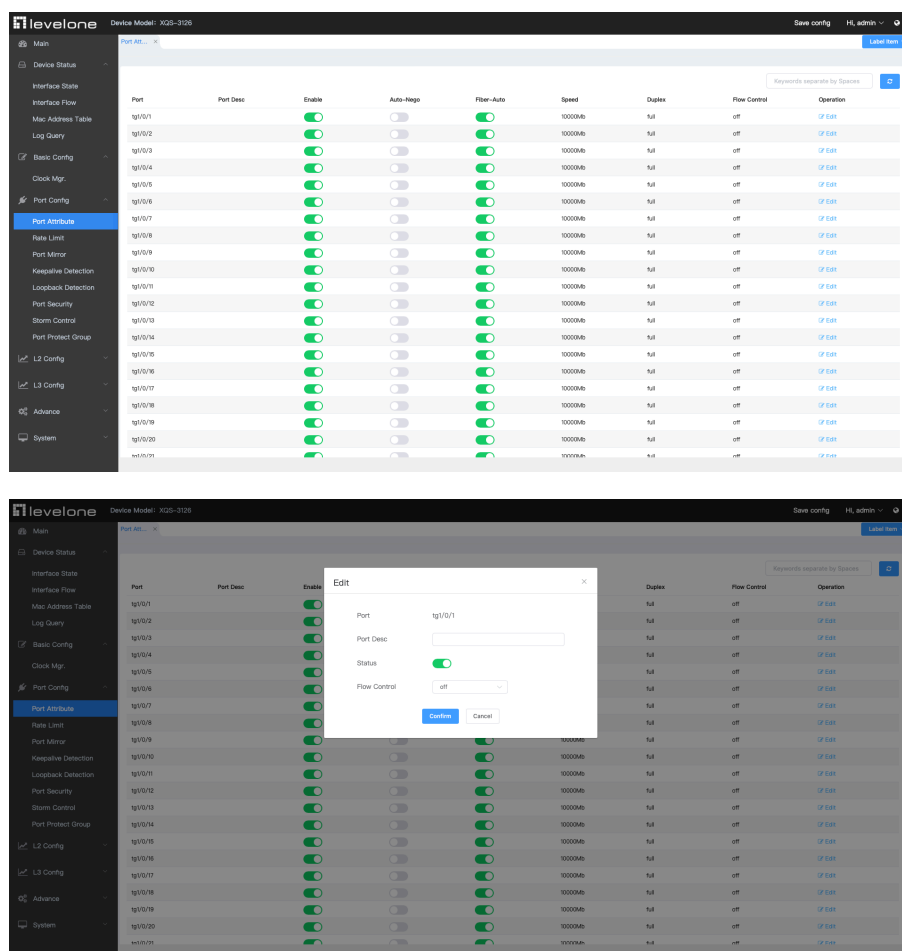
- System Time: 1970-1-2 09:38:58
- Model Select: ☐ Set Time Manually, ☒ Network Time Synchronization
- An 'NTP Server' input field is present below the radio buttons.
- An 'Apply' button is located at the bottom of the form.

When you select “Set Time Manually”, you can set the time of the device manually. When you select “Network Time Synchronization”, you can designate 3 SNTP servers for the device.

# Chapter 5 Configuration of the Physical Interface

## 5.1 Configuring the Attributes of the Port

If you click **Port config** -> **Port Config** in the navigation bar, the **Port Attribute Configuration** page appears, as shown in following figure.



On this page you can modify the on/off status, rate, duplex mode, flow control status and medium type of a port.

### Note:

After the speed or duplex mode of a port is modified, the link state of the port may be switched over and the network communication may be impaired.

## 5.2 Rate control

If you click **Port Config -> Rate-limit** in the navigation bar, the **Port rate limit** page appears, as shown in figure.

The screenshot displays the 'Rate Limit' configuration page for a device (Model: X20-3120). The left sidebar shows the navigation menu with 'Rate Limit' selected. The main area contains a table of ports with the following columns: Port, Rx Status, Rx Rate, Rx Unit, Tx Status, Tx Rate, Tx Unit, and Operation. The table lists 20 ports (1g1/0/1 to 1g1/0/20). An 'Edit' dialog box is open, showing the configuration for port 1g1/0/1. The dialog has fields for Port (1g1/0/1), Rx Status (Disable), and Tx Status (Disable), with 'Confirm' and 'Cancel' buttons at the bottom.

On this page you can set the reception speed and transmission speed of a port. By default, all ports have no speed limited. The receiving and sending rates can be configured either by percentage or by specific units of the switch.

## 5.3 Port mirroring

If you click **Port Config -> Port Mirror** in the navigation bar, the **Port Mirror Config** page appears, as shown in figure. Click "New" to add port mirroring, where Session is required.

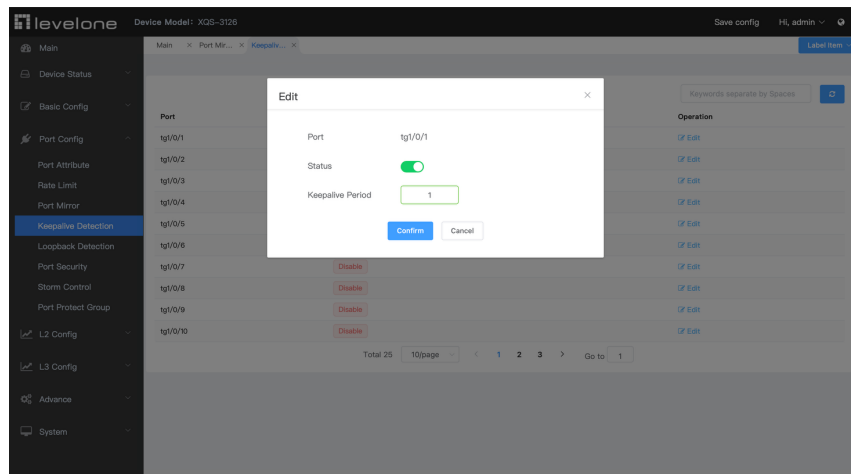
Click "Edit" to modify the corresponding port mirroring.

The screenshot displays the 'Port Mirror' configuration page for a device (Model: X20-3120). The left sidebar shows the navigation menu with 'Port Mirror' selected. The main area contains a table with the following columns: Session, Destination, Rx, Tx, Both, and Operation. The table is currently empty, and a 'No Data' message is displayed. There are 'New' and 'Delete' buttons at the top left of the table area. A 'Total 0' and '10page' indicator is shown at the bottom of the table.

## 5.4 Keepalive Detection

If you click **Port Config -> Keepalive detection** in the navigation bar, the **Keepalive detection** page appears, as shown in figure.

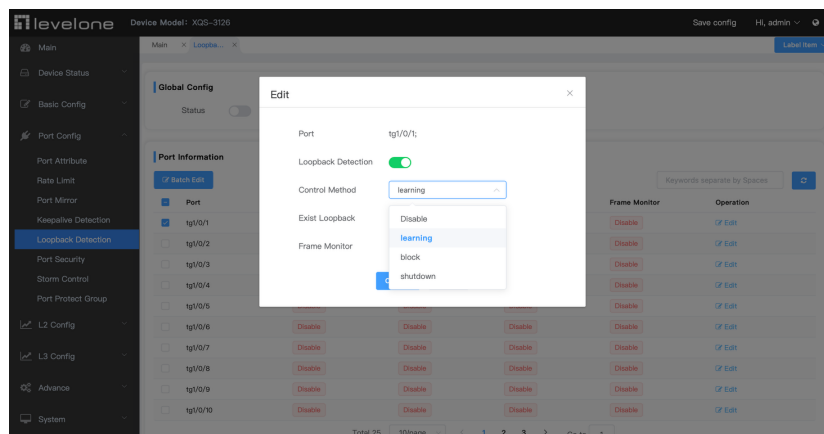
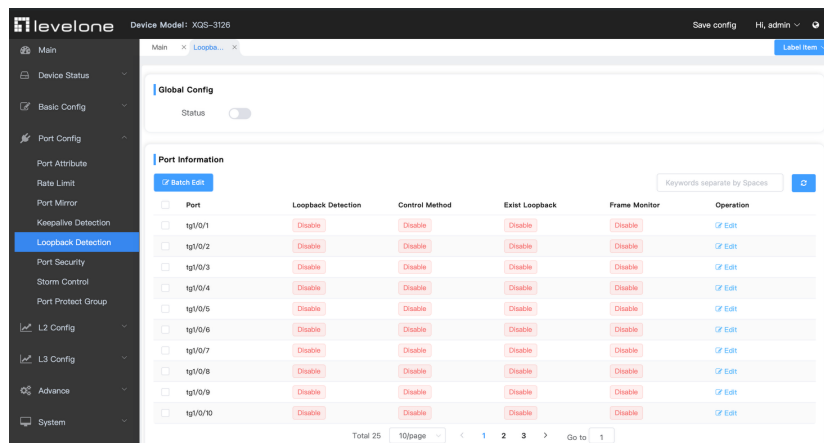
You can set the keepalive detection cycle on the **Keepalive detection** page (1~32767).



## 5.5 Loopback Detection

If you click **Port Config -> Loopback Detection** in the navigation bar, the **Loopback Detection** page appears, as shown in figure.

On the "Loopback Detection" page, you can configure whether to enable loopback detection; you can also click "edit" to modify whether the corresponding port is enabled for loopback detection, control mode, Vlan detection, loopback, and frame detection.



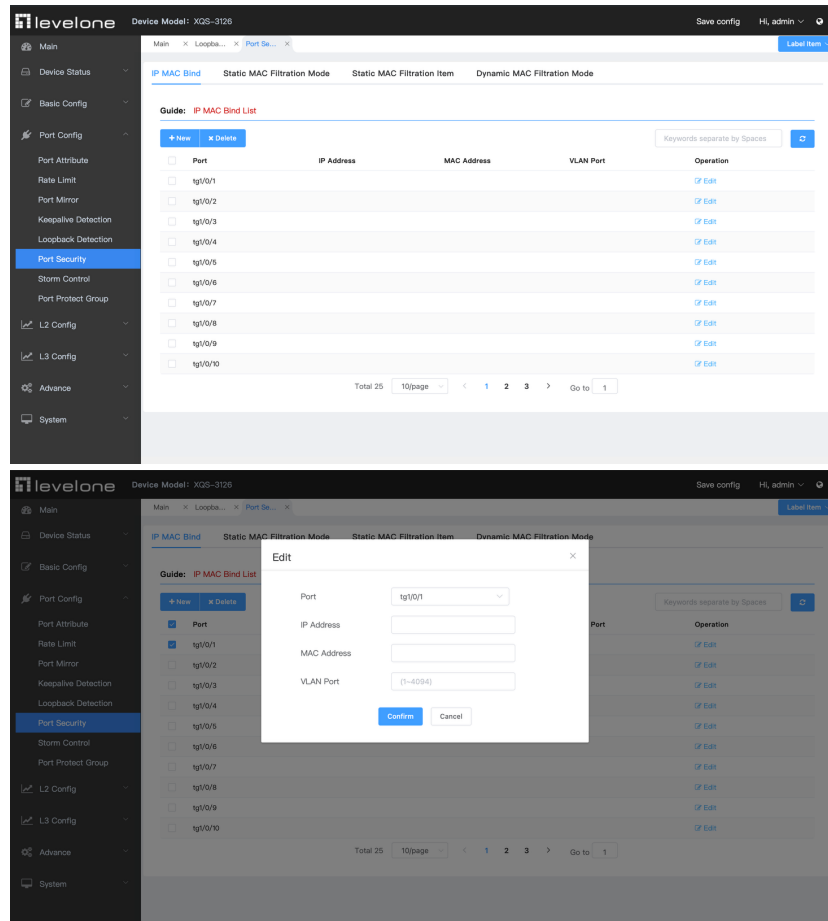
## 5.6 Port security

### 5.6.1 IP Binding Configuration

If you click **Port Config -> Port Security -> IP MAC bind** in the navigation bar, the **IP MAC bind list** page appears, as shown in figure.

Click "New" to add binding of IP address, MAC address and VLAN interface.

Click "Edit" to modify the existing IP-MAC binding information.



### 5.6.2 Static MAC Filtration Mode

If you click **Port Config -> Port Security -> Static MAC filtration mode** in the navigation bar, the **static MAC filtration mode** page appears, as shown in figure.

On this page you can set the static MAC filtration mode. By default, the static MAC filter is disabled. Also, the static MAC filter mode cannot be set on ports in trunk mode.

The top screenshot displays the 'Static MAC Filtration Mode' configuration page. It features a table with columns: Port, Port Mode, Mode, and Operation. The table lists ports from tg1/0/1 to tg1/0/10, all with 'Access' mode. A 'Total 25' and pagination controls are at the bottom.

The bottom screenshot shows the 'Edit' dialog box for a port configuration. It has fields for Port (tg1/0/1), Port Mode, and Mode. The Mode dropdown is open, showing options: Accept, Reject, and a third option (likely 'Limit').

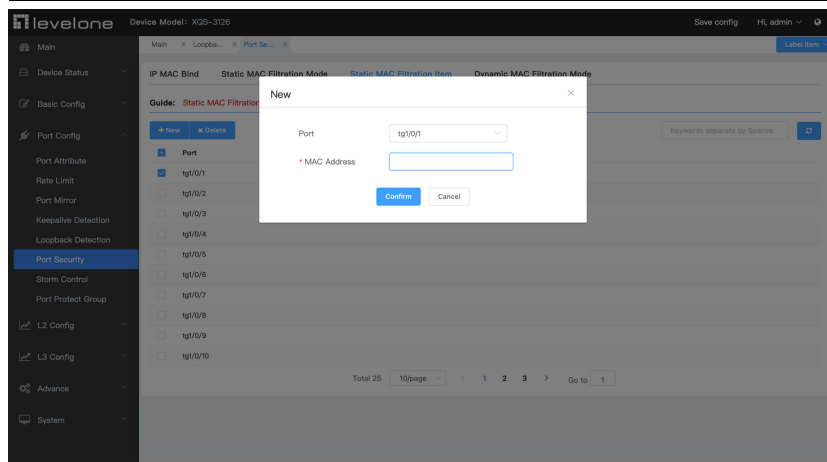
### 5.6.3 Static MAC Filtration Item

If you click **Port Config -> Port security -> Static MAC filtration Item** in the navigation bar, the **static MAC filtration entries** page appears.

If you click “New”, you can conduct the binding of the source MAC address for each physical port. According to the configured static MAC filtration mode, the MAC address of a port can be limited, allowed or forbidden to visit.

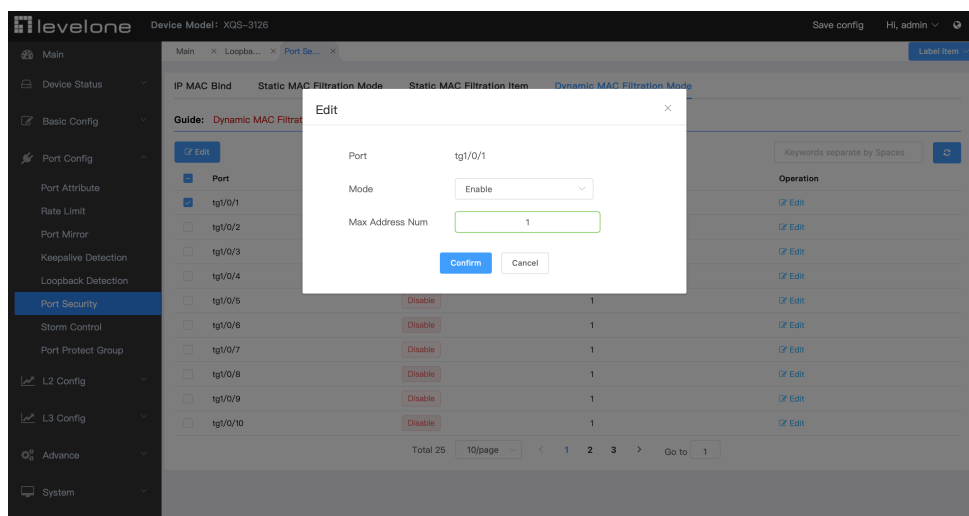
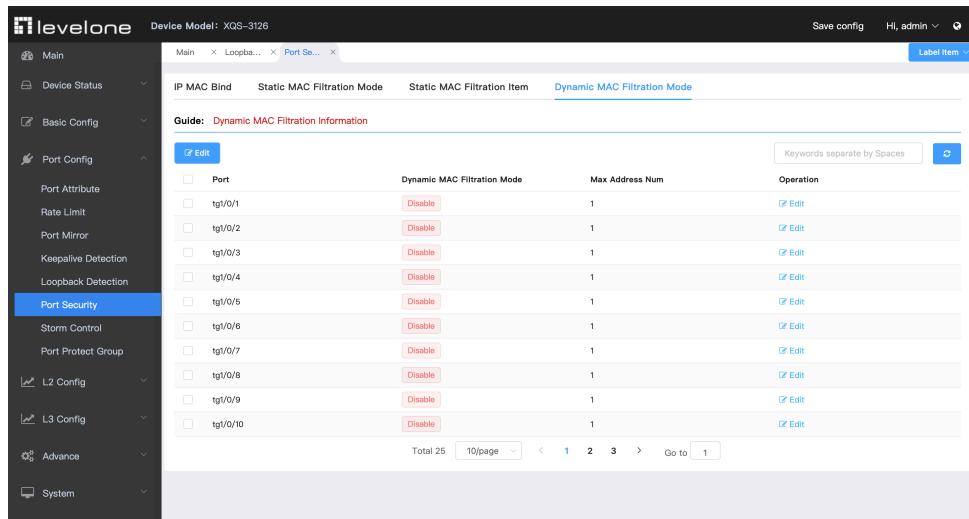
This screenshot shows the 'Static MAC Filtration Item' configuration page. It includes a table with columns: Port and MAC Address. The table lists ports from tg1/0/1 to tg1/0/10. A '+ New' button is visible at the top left of the table area. The bottom of the page shows 'Total 25' and pagination controls.





## 5.6.4 Dynamic MAC Filtration Mode

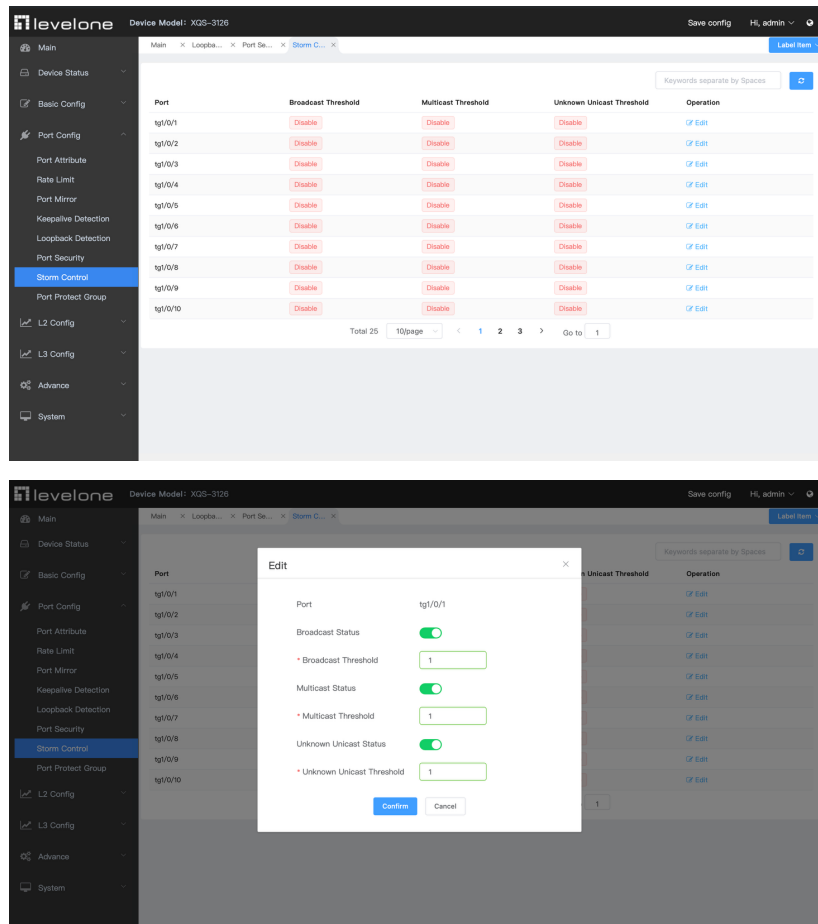
If you click **Port Config -> Port Security -> Dynamic MAC filtration mode** in the navigation bar, the **dynamic MAC filtration mode** page appears, as shown in figure. You can set the dynamic MAC filtration mode and the allowable maximum number of addresses on this page. By default, the dynamic MAC filtration mode is disabled and the maximum number of addresses is 1.



## 5.7 Storm control

In the navigation bar, click **Port Config -> Storm control**. The system then enters the page, on which the broadcast storm control can be set.

Click "Edit", you can modify the broadcast state, multicast state and unknown unicast state of the corresponding port.



## 5.8 Port Protect Group Configuration

### 5.8.1 Port Protect Group List

Click **"Port Config" -> "Port Protect Group"** in the navigation bar, and enter the configuration page of **"Port Protect Group List"**.

Click "New" to create a new port protect group, as shown in the above figure.

Tick one port protect group and click "Delete" to delete it. The port protect group is 0 by default, which cannot be deleted.

The screenshot shows the Hlevelone web configuration interface for a device model XQS-3126. The left sidebar contains a navigation menu with categories: Main, Device Status, Basic Config, Port Config, L2 Config, L3 Config, Advance, and System. The 'Port Config' category is expanded, showing sub-items: Port Attribute, Rate Limit, Port Mirror, Keepalive Detection, Loopback Detection, Port Security, Storm Control, and Port Protect Group. The 'Port Protect Group' item is selected. The main content area displays the 'Port Protect Group List' and 'Port Protect Group Config' tabs. The 'Port Protect Group List' tab is active, showing a table with columns for 'Port Protect' and 'No Data'. The table is empty, and the status bar at the bottom indicates 'Total 0', '10/page', and 'Go to 1'. A search bar with the placeholder 'Keywords separate by Spaces' and a refresh button is located at the top right of the table area.

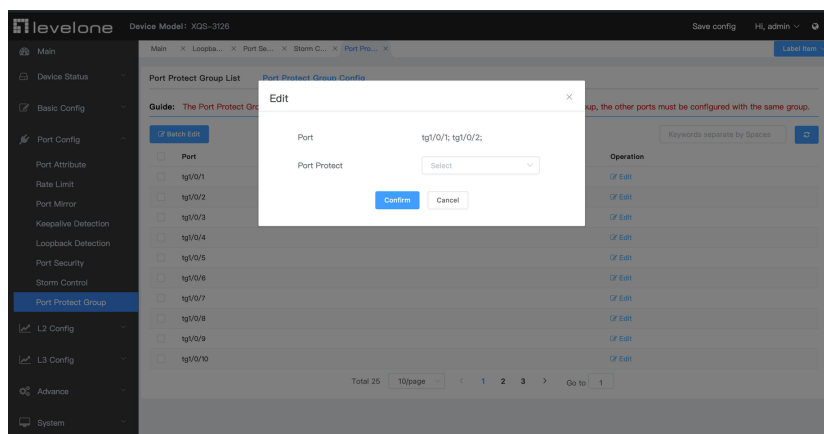
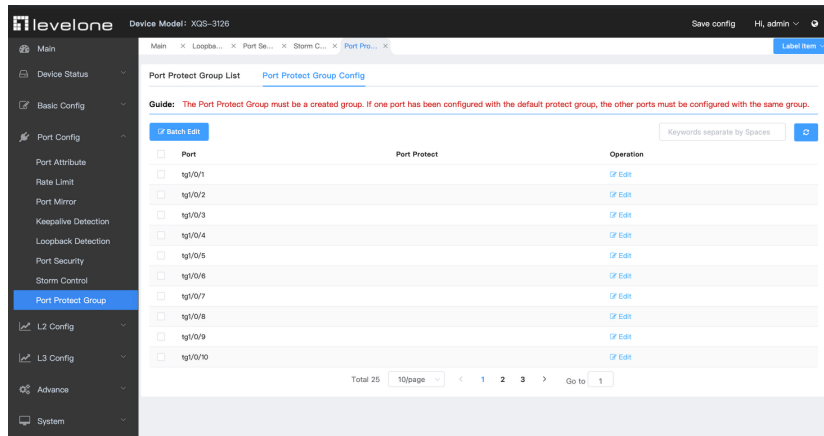
The screenshot shows the Hlevelone web configuration interface for a device model XQS-3126. The left sidebar is the same as in the previous screenshot. The 'Port Protect Group' item is selected. The main content area displays the 'Port Protect Group List' and 'Port Protect Group Config' tabs. The 'Port Protect Group Config' tab is active. A 'New' dialog box is open, showing a form with a red asterisk next to the 'Port Protect' label. The input field contains the value '1' and has a range indicator '(1-16)' to its right. Below the input field are 'Confirm' and 'Cancel' buttons. The background content is dimmed.

## 5.8.2 Port Protect Group Configuration

Click **"Port Config"** -> **"Port Protect Group"** -> **"Port Protect Group Config"** in the navigation bar, and enter the configuration page of **"Port Protect Group Interface Config"**.

The port protect group must be a created group. If one port has configured the default protect group, other ports can only be configured with the default protect group.

Click "Edit" to modify the protection group of the corresponding port.



## Chapter 6 L2 Configuration

### 6.1 VLAN Configuration

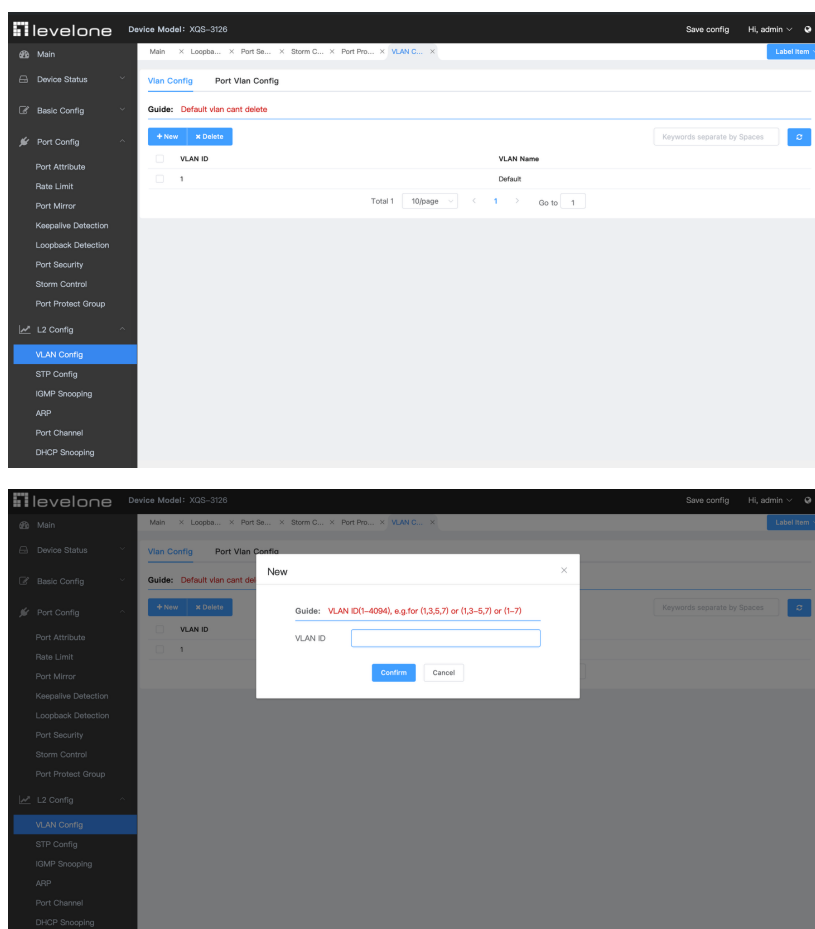
#### 6.1.1 VLAN Config

If you click **L2 Config** -> **VLAN Config** in the navigation bar, the **VLAN Config** page appears, as shown in figure.

The VLAN list will display VLAN items that exist in the current device according to the ascending order. In case of lots of items, you can look for the to-be-configured VLAN through the buttons like “Prev”, “Next” and “Search”.

You can click “New” to create a new VLAN.

You can also click “Edit” at the end of a VLAN item to modify the VLAN name and the port’s attributes in the VLAN.



## 6.1.2 Port VLAN Config

If you click **L2 Config -> VLAN Config** in the navigation bar, the **Port VLAN Config** page appears, as shown in figure.

If you click “Edit” in the VLAN list, the VLAN configuration page appears, on which new VLANs can be created or the attributes of an existent VLAN can be modified.

The top screenshot shows the 'Port VLAN Config' page. It features a table with columns: Port, PVID, Mode, Allowed Range, Untagged Range, and Operation. The table lists 10 ports (tg1/0/1 to tg1/0/10) all configured with PVID 1, Mode Access, and Allowed Range 1-4094. The Operation column contains 'Edit' links for each row.

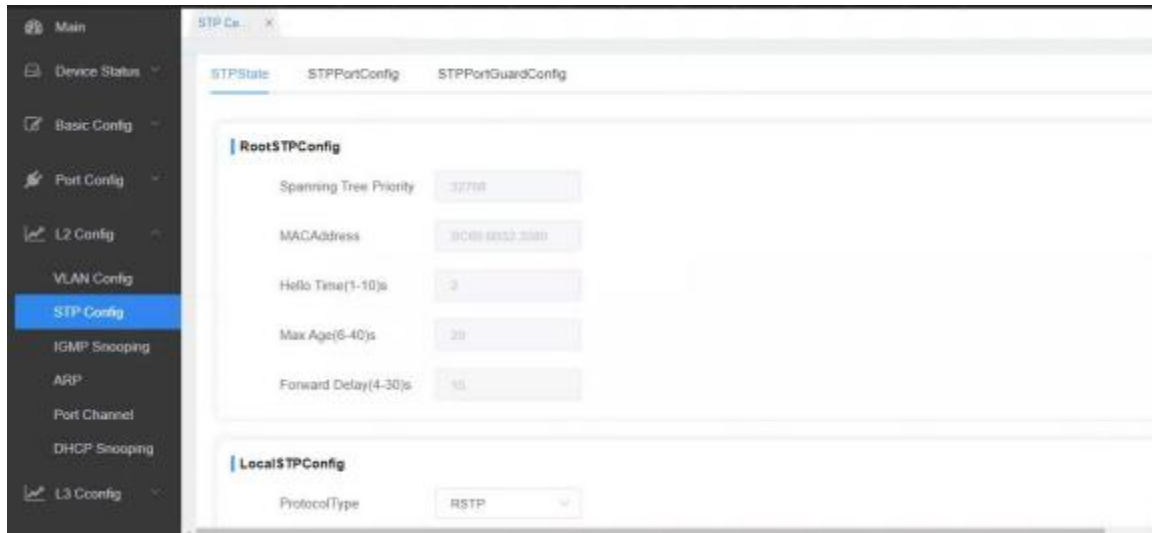
Port	PVID	Mode	Allowed Range	Untagged Range	Operation
tg1/0/1	1	Access	1-4094	1	<a href="#">Edit</a>
tg1/0/2	1	Access	1-4094	1	<a href="#">Edit</a>
tg1/0/3	1	Access	1-4094	1	<a href="#">Edit</a>
tg1/0/4	1	Access	1-4094	1	<a href="#">Edit</a>
tg1/0/5	1	Access	1-4094	1	<a href="#">Edit</a>
tg1/0/6	1	Access	1-4094	1	<a href="#">Edit</a>
tg1/0/7	1	Access	1-4094	1	<a href="#">Edit</a>
tg1/0/8	1	Access	1-4094	1	<a href="#">Edit</a>
tg1/0/9	1	Access	1-4094	1	<a href="#">Edit</a>
tg1/0/10	1	Access	1-4094	1	<a href="#">Edit</a>

The bottom screenshot shows the 'Edit' dialog box for the selected VLAN (tg1/0/1). It contains input fields for: Port (tg1/0/1), VLAN ID (1), Mode (Access), Allowed Range (1-4094), and Untagged Range (1). There are 'Confirm' and 'Cancel' buttons at the bottom.

## 6.2 STP Configuration

### 6.2.1 STP Status Information

If you click **L2 Config -> STP Config** in the navigation bar, the **STP Config** page appears, as shown in figure.



The root STP configuration information and the STP port's status are only-read.

On the local STP configuration page, you can modify the running STP mode by clicking the Protocol type dropdown box. The STP modes include RSTP and disable.

The priority and the time need be configured for different modes.

---

Note:

The change of the STP mode may lead to the interruption of the network.

---

### 6.2.2 STP Port Config

If you click **L2 Config -> STP Config -> STP Port Config** in the navigation bar, the **STP Port Config** page appears, as shown in figure.

Port	ProtocolStatus	Priority(1-240)	PathCost(1-25000000)	Operation
g0/0/1	Enable			<a href="#">Edit</a>
g0/0/2	Enable			<a href="#">Edit</a>
g0/0/3	Enable			<a href="#">Edit</a>
g0/0/4	Enable			<a href="#">Edit</a>
g0/0/5	Enable			<a href="#">Edit</a>
g0/0/6	Enable			<a href="#">Edit</a>
g0/0/7	Enable			<a href="#">Edit</a>
g0/0/8	Enable			<a href="#">Edit</a>
g0/0/9	Enable			<a href="#">Edit</a>
g0/0/10	Enable			<a href="#">Edit</a>

The configuration of the attributes of the port is irrelative of the global STP mode. For example, if the protocol status is set to “Disable” and the STP mode is also changed, the port will not run the protocol in the new mode.

The default value of the path cost of the port is 0, meaning the path cost is automatically calculated according to the speed of the port. If you want to change the path cost, please enter another value.

### 6.2.3 STP Port Guard Config

If you click **L2 Config -> STP Config -> STP Port Guard Config** in the navigation bar, the **STP Port Guard Config** page appears, as shown in figure.

Port	BPDU Guard	Guard	Operation
g0/0/1	Disable	Disable	<a href="#">Edit</a>
g0/0/2	Disable	Disable	<a href="#">Edit</a>
g0/0/3	Disable	Disable	<a href="#">Edit</a>
g0/0/4	Disable	Disable	<a href="#">Edit</a>
g0/0/5	Disable	Disable	<a href="#">Edit</a>
g0/0/6	Disable	Disable	<a href="#">Edit</a>
g0/0/7	Disable	Disable	<a href="#">Edit</a>
g0/0/8	Disable	Disable	<a href="#">Edit</a>

Click "Edit" to enter the corresponding port guard information modification interface.

## 6.3 IGMP-Snooping Configuration

### 6.3.1 IGMP-Snooping Configuration

If you click **L2 Config -> IGMP snooping**, the IGMP-Snooping configuration page appears.

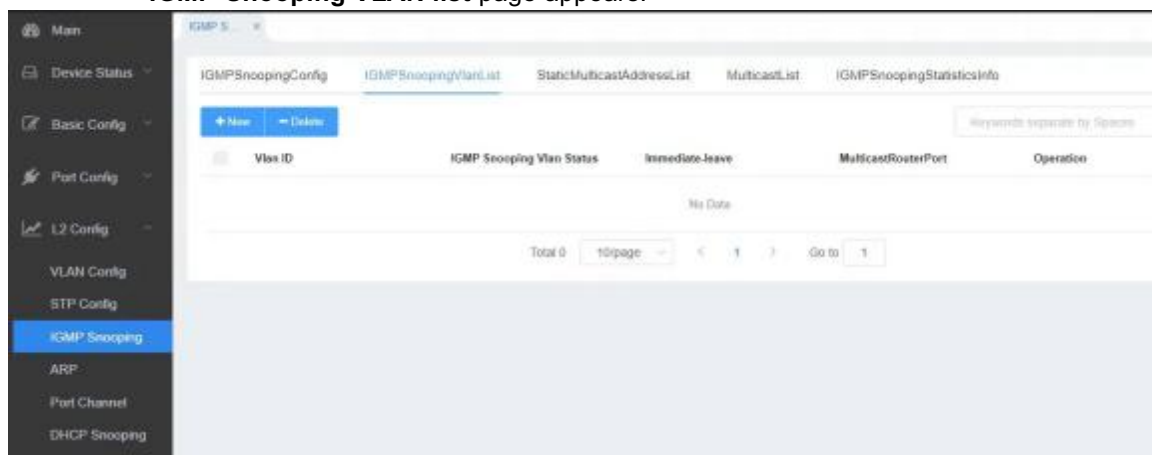




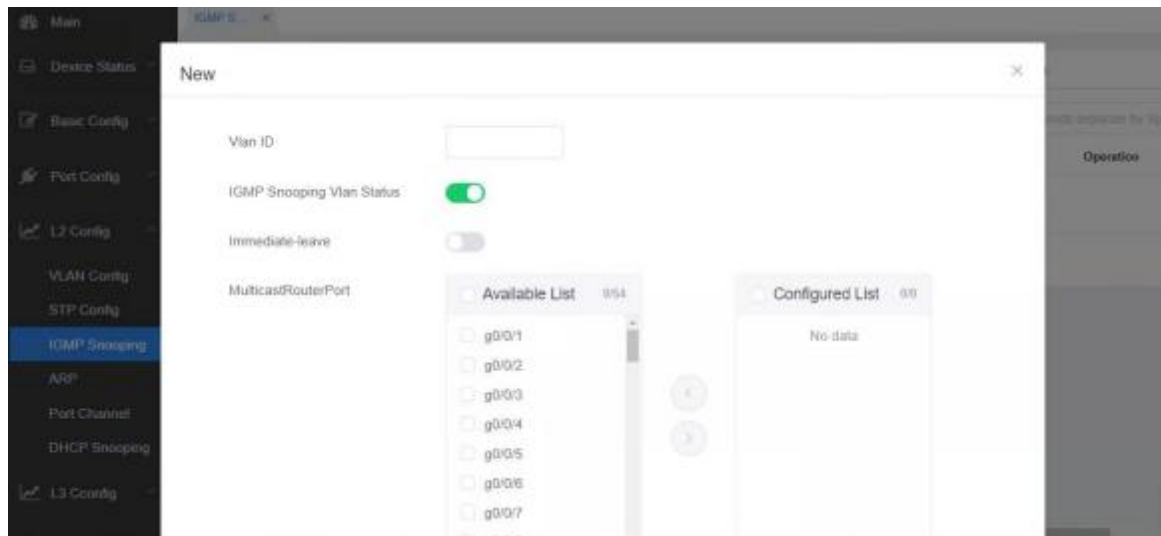
On this page you can set whether to make a switch to forward unknown multicasts, whether to enable IGMP snooping, and whether to configure the switch as the querier of IGMP.

### 6.3.2 IGMP-Snooping VLAN List

If you click **L2 Config -> IGMP snooping -> IGMP snooping vlan list**, the **IGMP-Snooping VLAN list** page appears.



If you click **New**, IGMP-snooping VLAN configuration can be created. If you click **Delete**, a selected IGMP-Snooping VLAN can be deleted; if you click **Edit**, you can modify the member port, running status and immediate-leave of IGMP-Snooping VLAN.

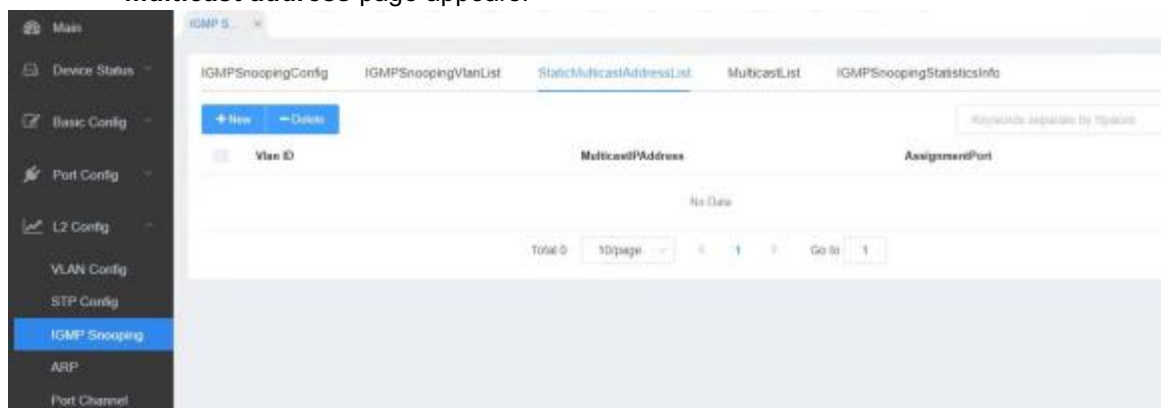


When an IGMP-Snooping VLAN is created, its VLAN ID can be modified; but when the IGMP-Snooping VLAN is modified, its VLAN ID cannot be modified.

You can click “>” and “<” to delete and add a routing port.

### 6.3.3 Static Multicast Address

If you click **L2 Config -> IGMP snooping -> Static multicast address list**, the **static multicast address** page appears.



On this page, the currently existing static multicast groups and port groups in each static multicast group are shown.

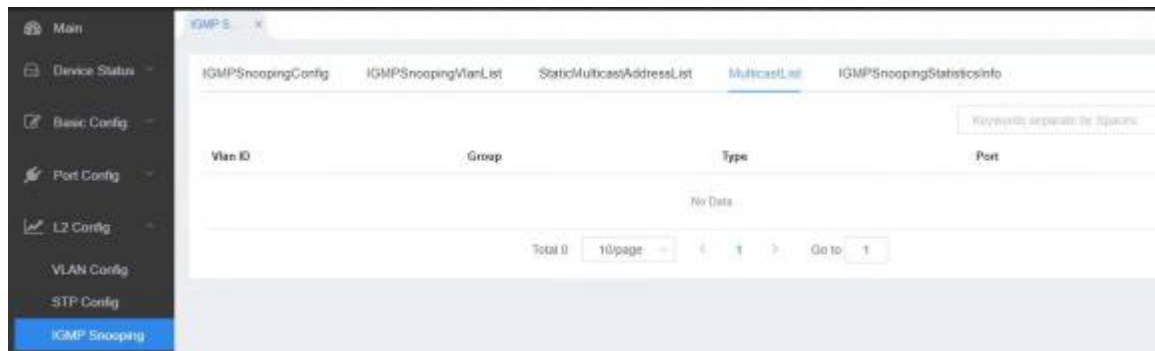
Click "New" to add a static multicast address.

Click "Delete" to delete the static multicast address.

Click “Refresh” to refresh the contents in the list.

### 6.3.4 Multicast List

If you click **L2 Config -> IGMP snooping -> Multicast List** option on the top of the page, the **Multicast List Info** page appears.



On this page the multicat groups, which are existent in the current network and are in the statistics of IGMP snooping, as well as port sets which members in each group belong to are displayed.

Click “Refresh” to refresh the contents in the list.

### 6.3.5 IGMP Snooping Statistic Info

If you click **L2 Config -> IGMP snooping -> IGMP Snooping Statistics Info** option on the top of the page, the **IGMP Snooping Statistics Info** page appears.



## 6.4 ARP

### 6.4.1 Static ARP

If you click **L2 Config -> ARP -> Static AR**, the static ARP configuration page appears.



If you click **New**, you can add an ARP entry. When configuring an ARP entry, you need to specify a VLAN interface.

If you click **Delete**, you can cancel the chosen ARP entry.

## 6.4.2 ARP Information

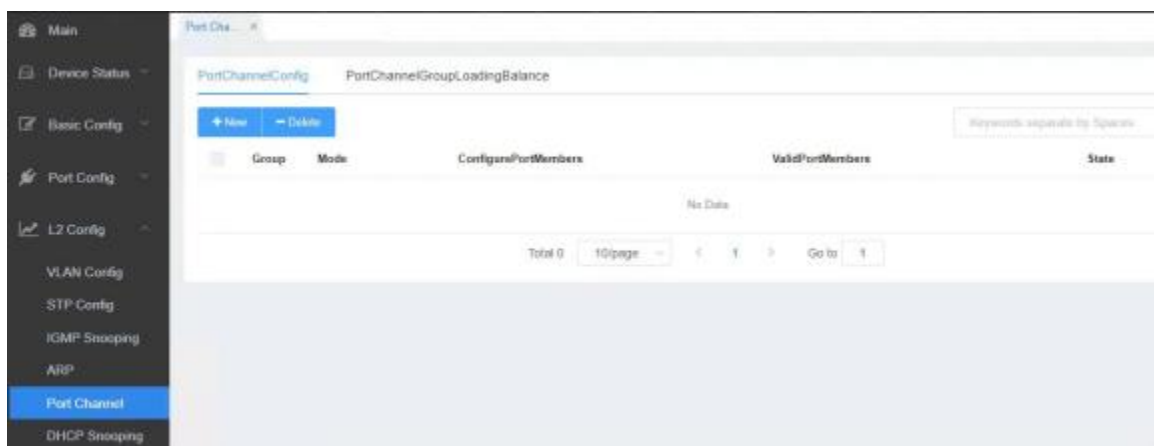
If you click **L2 Config -> ARP -> ARP Information**, the ARP Information page appears.



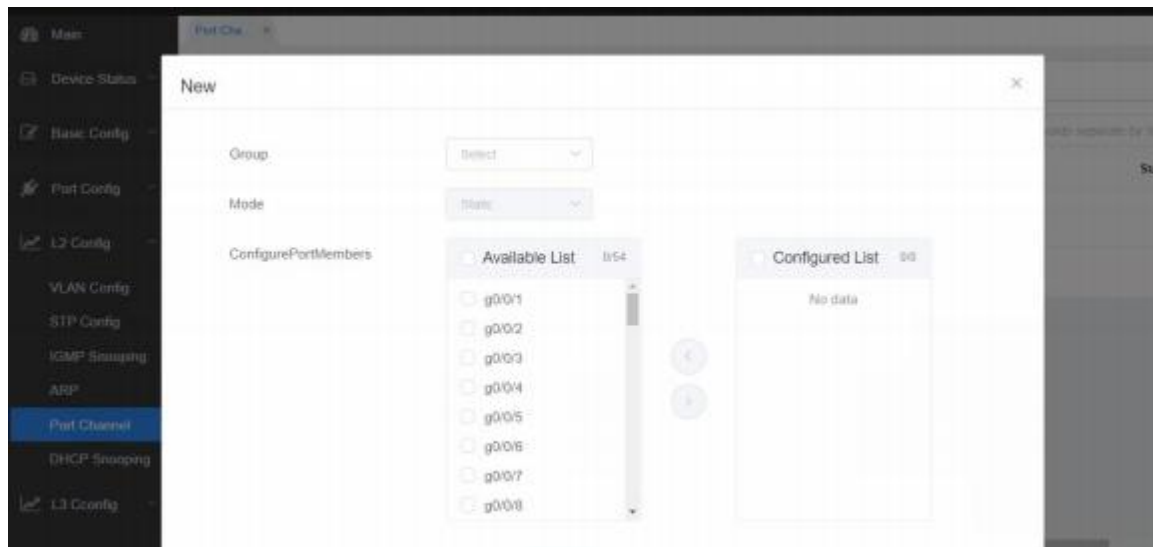
## 6.5 Port Channel

### 6.5.1 Port Aggregation Configuration

If you click **L2 Config -> Port Channel-> Port Channel config**, the **Port Aggregation Config** page appears.



Click **New** to create an aggregation group. It can configure 8 aggregation groups in maximum and each group is with 128 physical ports into aggregation. Click **Delete** to delete the selected aggregation group. Click **Edit** to modify the setting.



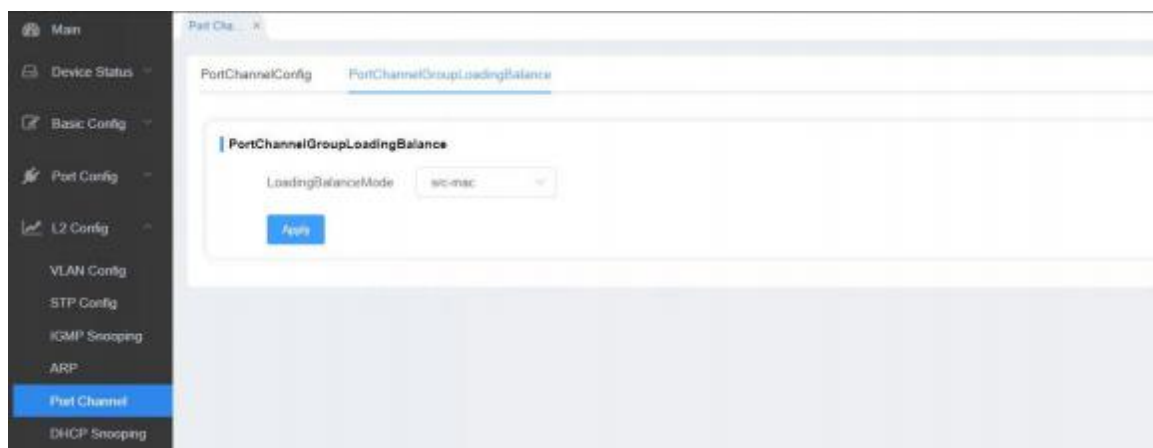
If you create an aggregation group, it is optional; if you modify the aggregation group, it is not optional.

When the aggregation port has a member port, the user can select the aggregation mode: static, LACP Active and LACP Passive.

You can click “>” and “<” to delete and add an aggregation member port.

## 6.5.2 Port Channel Group Loading Balance Configuration

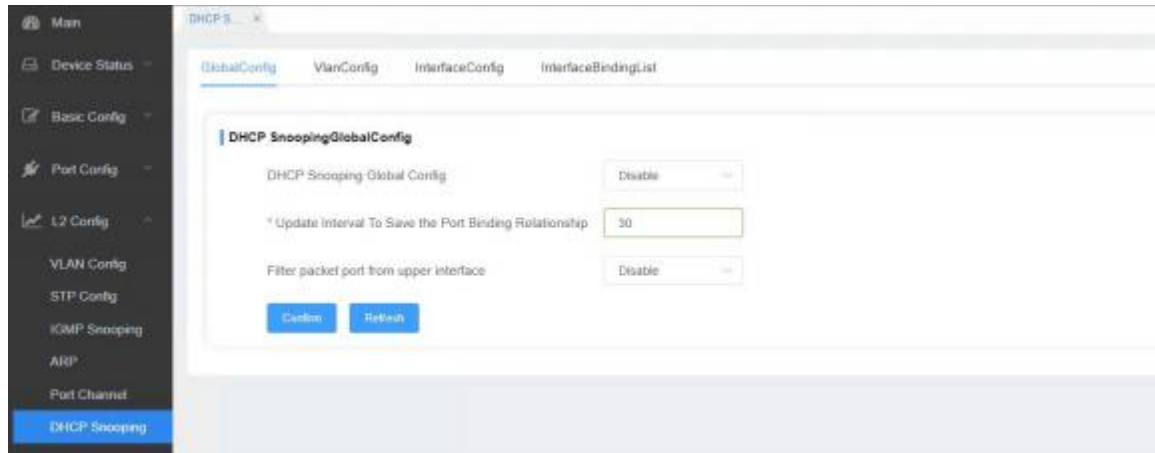
Some models support link aggregation load balancing configuration and others not, but they can be configured in the global configuration mode.



## 6.6 DHCP Snooping

### 6.6.1 Global Configuration

If you click **L2 Config -> DHCP Snooping** in the navigation bar, the **global DHCP Snooping** page appears.



The global DHCP snooping protocol is enabled, and the switch monitors all DHCP packets to form a corresponding binding relationship. If the client obtains the address through this switch before this command is configured, the switch cannot add the corresponding binding relationship.

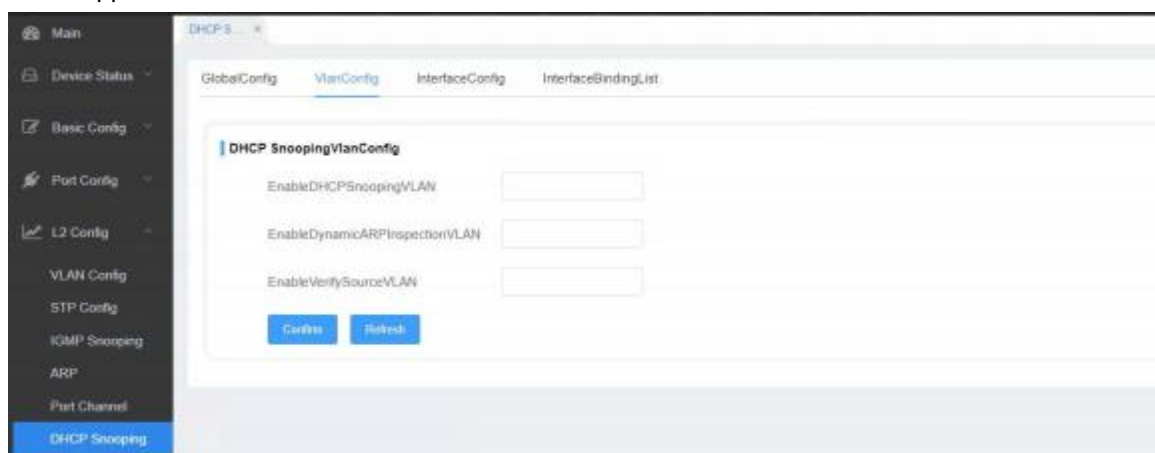
When the switch configuration is saved and restarted, the previous interface binding relationship will be lost. At this time, there is no binding relationship on the interface. After the IP source address monitoring function is enabled, the switch refuses to forward all IP packets. After configuring the backup TFTP server for interface binding relationship, the binding relationship will be backed up to the server through the TFTP protocol. After the switch restarts, it will automatically download the binding table to the TFTP server to ensure normal network operation.

When configuring the backup interface binding relationship, the file name saved on the TFTP server. Different switches can back up their own interface binding tables to the same TFTP server.

The binding relationship table between the MAC address and IP address of an interface changes dynamically. After a certain time interval, check whether the binding is updated. If there is an update (add or delete binding entries), perform the backup again. The default time interval is 30 minutes.

## 6.6.2 VLAN Config

If you click **L2 Config -> DHCP Snooping -> VLAN Config**, the **VLAN Config** page appears.



When the DHCP snooping function is enabled on the VLAN, the legality check is performed on the DHCP packets received by all untrusted physical ports in the VLAN. The DHCP

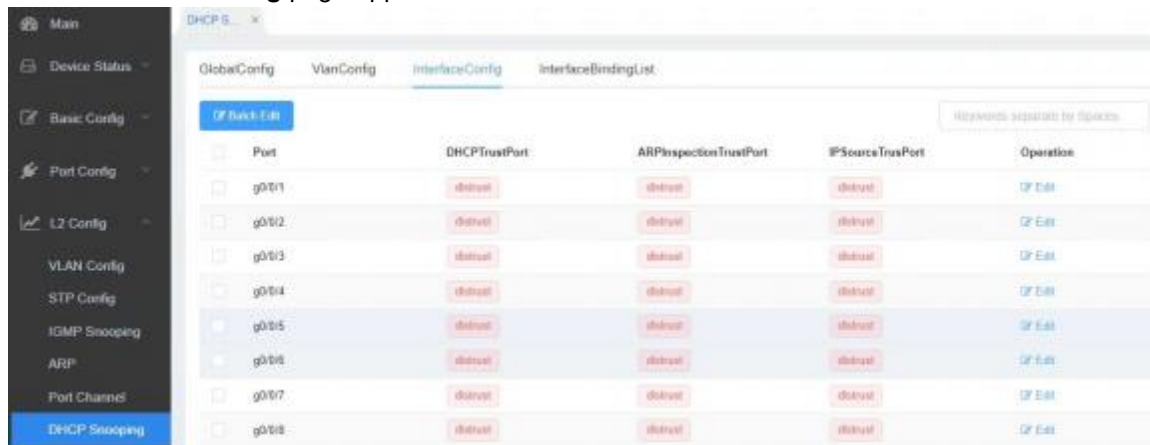
response packets received by the untrusted physical ports in the VLAN will be discarded to prevent users from illegally forging or misconfigured DHCP servers to provide address allocation; For the DHCP request packet of the untrusted port, if the MAC address sent in the packet does not match the hardware address field in the packet, it is considered to be a DHCP DOS (denial of service) attack packet, and the switch will also discard it.

Perform dynamic ARP monitoring on all physical ports belonging to a VLAN. If the source MAC and source IP addresses of ARP packets received by the interface do not meet the binding relationship between the MAC and IP addresses configured on the interface, the packet will be rejected. The binding relationship configured on the interface can be dynamically bound by DHCP or manually configured. If no MAC-IP address binding is configured on the physical interface, the switch refuses to forward all ARP packets.

In the VLAN in which IP source address monitoring is enabled, if the source MAC and source IP addresses of IP packets received by all physical ports belonging to the VLAN do not meet the binding relationship between the MAC and IP addresses configured on the interface, the packets will be rejected. The binding relationship configured on the interface can be dynamically bound by DHCP or manually configured. If no MAC-IP address binding is configured on this physical interface, the switch refuses to forward all IP packets received by this interface.

### 6.6.3 Interface Configuration

If you click **L2 Config -> DHCP Snooping -> Interface Config** in the navigation bar, the **Interface Config** page appears.



If an interface is configured as a DHCP trusted interface, the DHCP packets received by the interface are not checked.

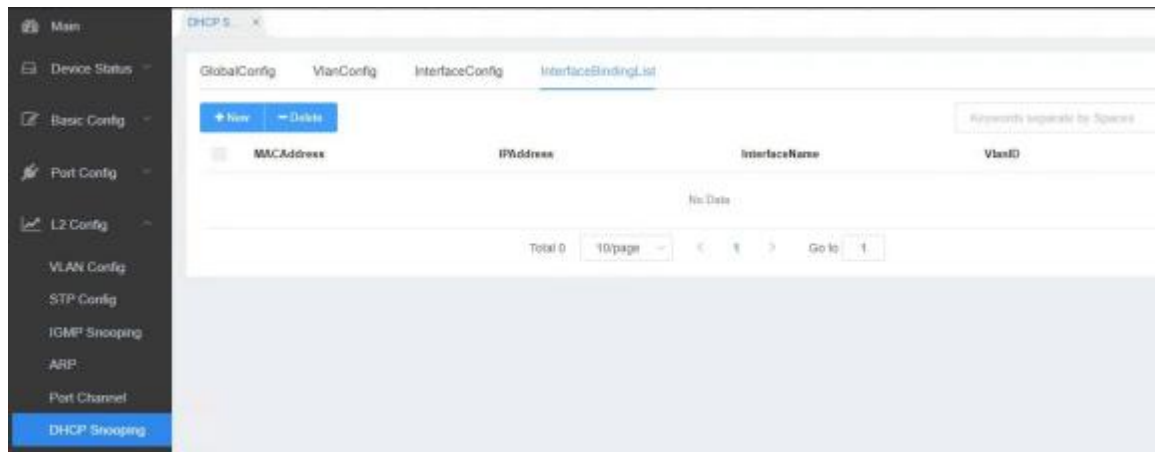
For ARP trusted interfaces, the ARP monitoring function is not enabled. The interface defaults to an untrusted interface.

For the IP source address trusted interface, the source address check function is not enabled.

Click "Edit" to modify the corresponding port configuration.

### 6.6.4 Interface Binding list

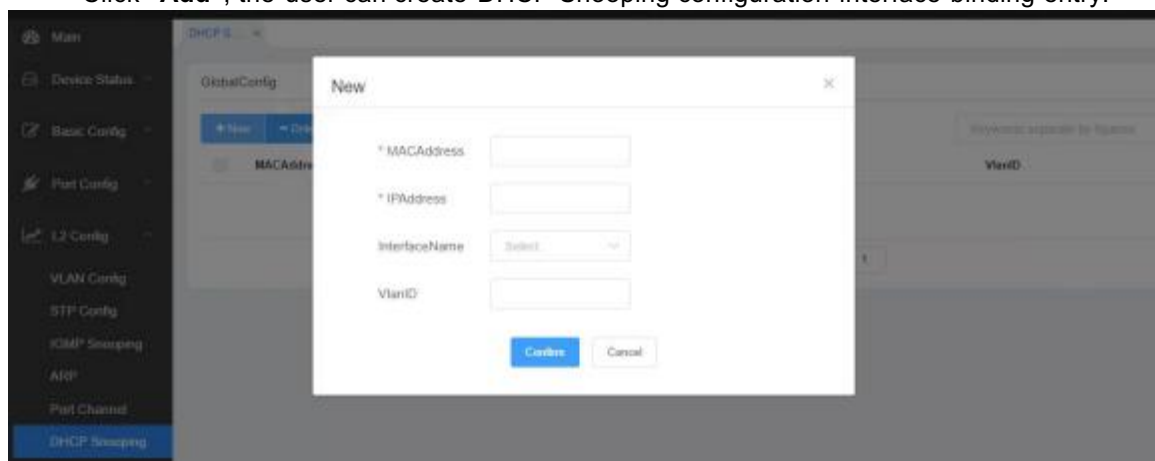
If you click **L2 Config -> DHCP Snooping -> Interface Binding list** in the navigation bar, the **Interface Binding list** page appears.



For hosts that do not obtain addresses with DHCP, you can manually configure and add binding entries on the switch interface so that the hosts can access the network normally. Use the no form of this command to delete binding entries.

The manually configured binding entry has a higher priority than the dynamically configured binding entry. If the MAC address of the configuration entry is the same as that of the dynamic configuration entry, the manually configured dynamic configuration entry is updated. Interface binding entries are uniquely indexed by MAC address.

Click **"Add"**, the user can create DHCP Snooping configuration interface binding entry.



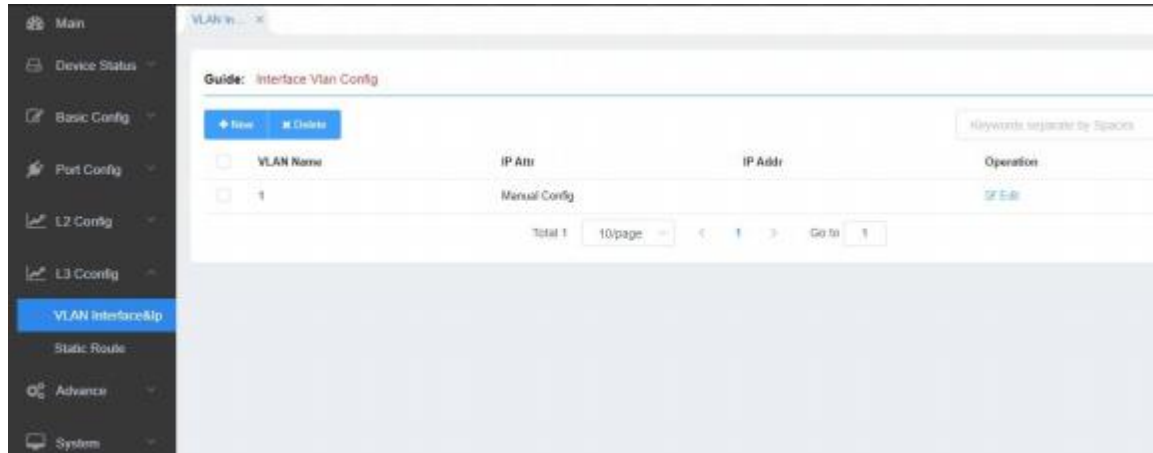
Click **"Delete"** to delete the DHCP Snooping configuration interface binding entry.



## Chapter 7 L3 Configuration

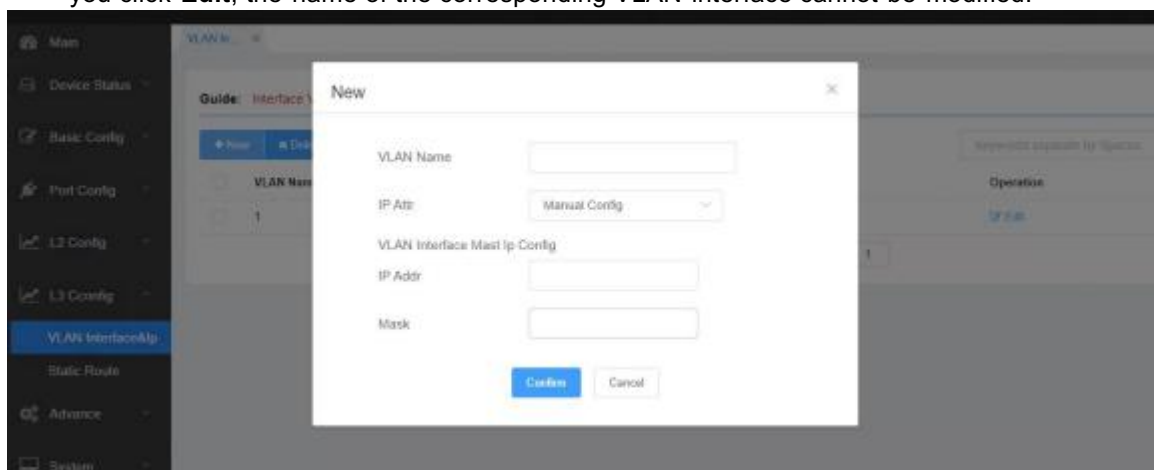
### 7.1 Configuring the VLAN Interface

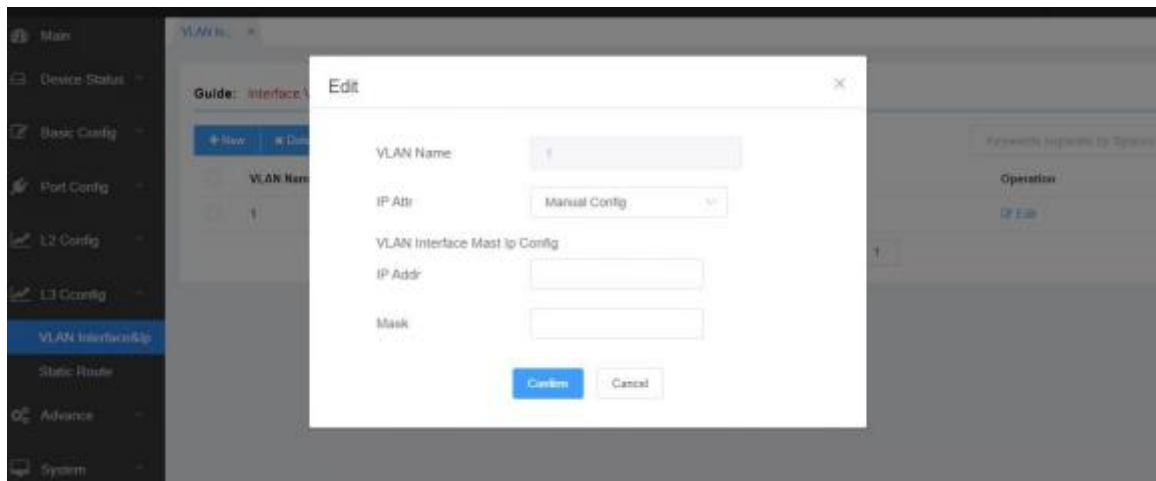
If you click **L3 Config -> VLAN interface &IP**, the **Configuring the VLAN interface** page appears.



Click **New** to add a new VLAN interface. Click **Delete** to delete a VLAN interface. Click **Edit** to modify the settings of a corresponding VLAN interface.

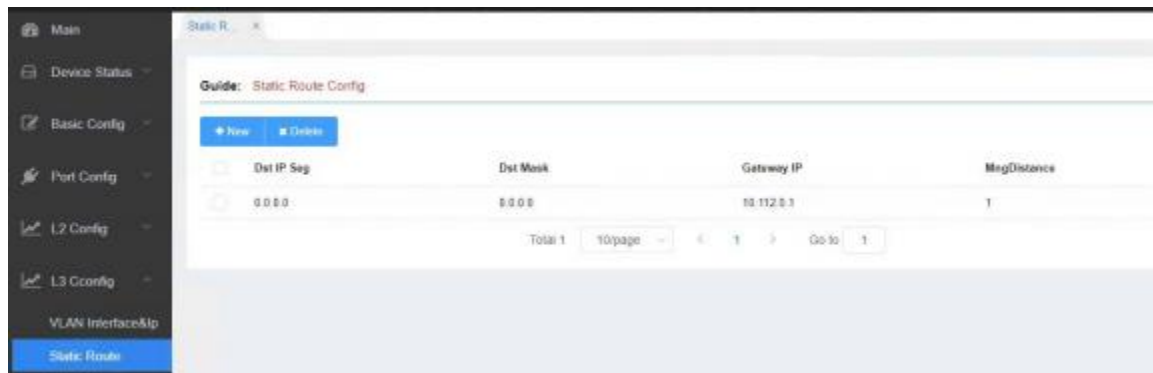
When you click **New**, the name of the corresponding VLAN interface can be modified; but if you click **Edit**, the name of the corresponding VLAN interface cannot be modified.



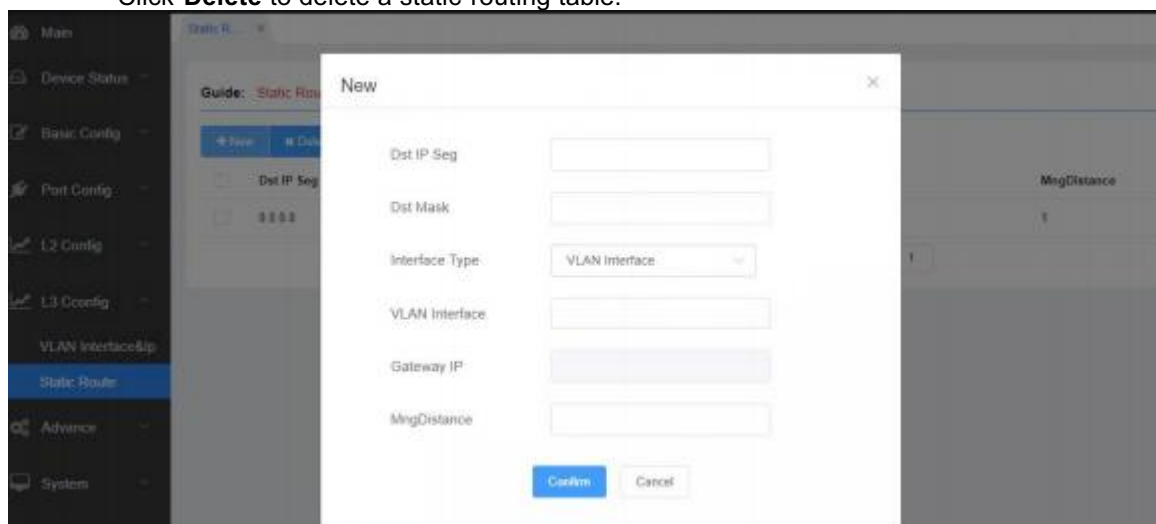


## 7.2 Static Routing Configuration

If you click **L3 Config -> Static Route**, the **Configuring the static routing table** page appears.



Click **New** to add a new static routing table.  
Click **Delete** to delete a static routing table.

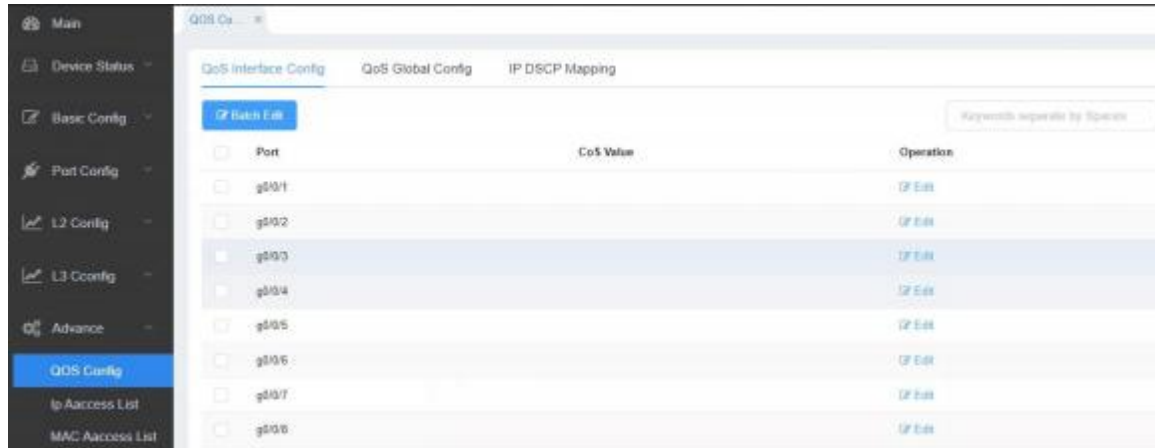


## Chapter 8 Advanced Configuration

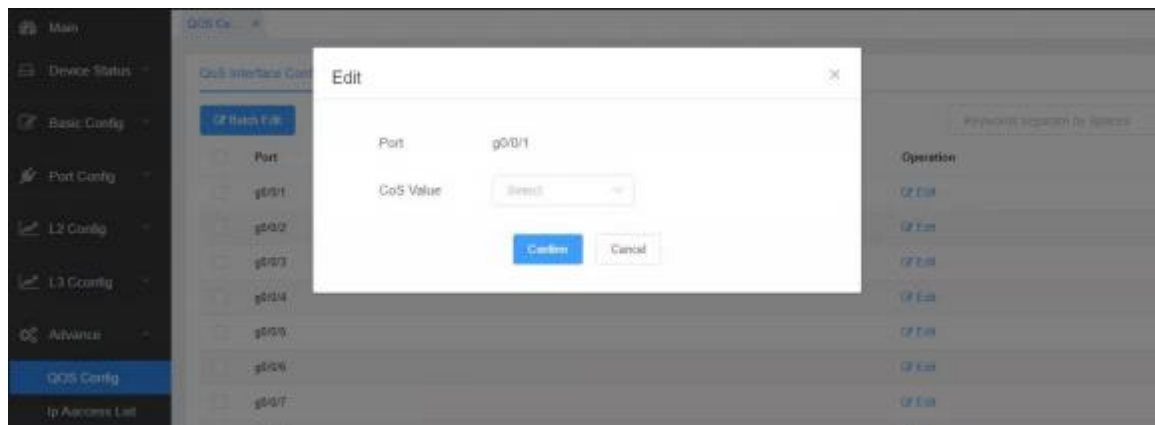
### 8.1 QoS Configuration

#### 8.1.1 Configuring QoS Port

If you click **Advance** -> **QoS Config** -> **QoS Interface Config**, the **QoS parameters Config** page appears.



Click "Edit" to enter the interface for modifying the CoS value of the corresponding port, and set the CoS value of the port through the drop-down box below the port name. The default CoS of the port is 0, indicating the lowest priority. CoS7 is the highest priority.



#### 8.1.2 Global QoS Configuration

If you click **Advance** -> **QoS** -> **Global QoS Config**, the **global QoS parameter configuration** page appears.

The image shows two screenshots of a network device's web configuration interface. The top screenshot displays the 'QoS Global Config' page, and the bottom screenshot displays the 'CoS To Queue Map' page.

**QoS Global Config**

Navigation: QoS Interface Config | **QoS Global Config** | IP DSCP Mapping

**QoS Global Config**

Schedule Policy:

Default CoS Value:

Trust Priority:

Queue	Weight
1	<input type="text" value="1"/> (1-15)
2	<input type="text" value="1"/> (1-15)

**CoS To Queue Map**

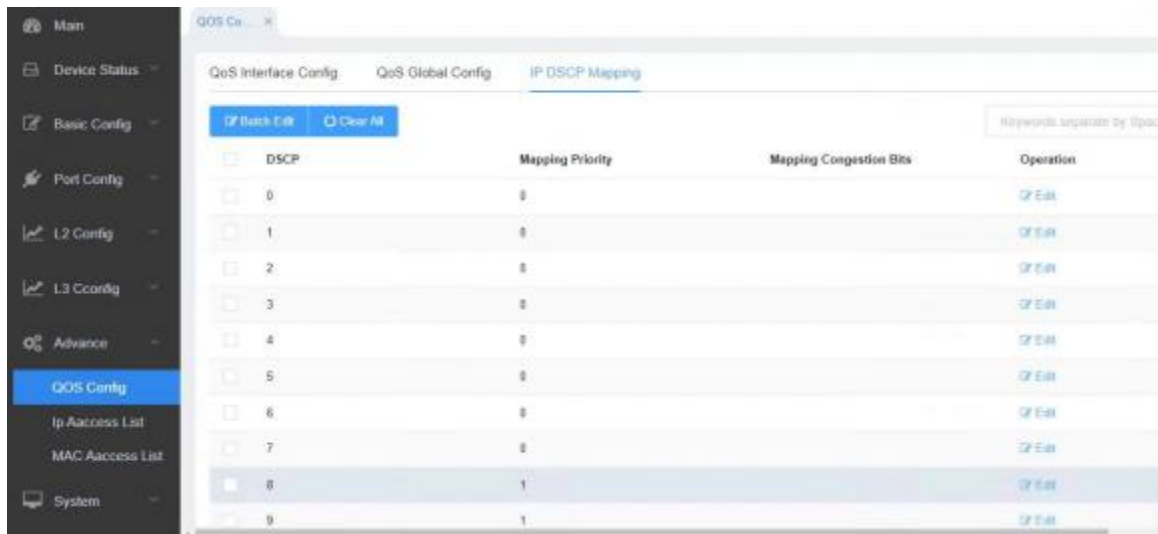
CoS Value	Queue	Operation
0	Queue1	<a href="#">Edit</a>
1	Queue2	<a href="#">Edit</a>
2	Queue3	<a href="#">Edit</a>
3	Queue4	<a href="#">Edit</a>
4	Queue5	<a href="#">Edit</a>
5	Queue6	<a href="#">Edit</a>
6	Queue7	<a href="#">Edit</a>
7	Queue8	<a href="#">Edit</a>

Total 8  < 1 > Go to

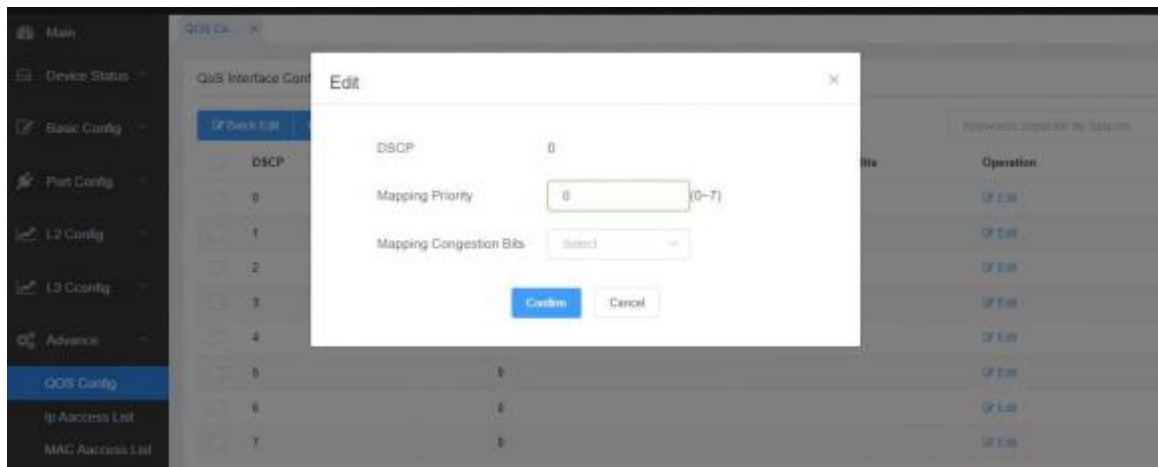
In WRR schedule mode, you can set the weights of the QoS queues. There are 8 queues, among which queue 1 has the lowest priority and queue 8 has the highest priority.

### 8.1.3 IP DSCP Mapping

If you click **Advance -> QoS -> IP DSCP Mapping**, the **Global IP DSCP Mapping** page appears.



Click "Edit" to enter the modification interface of the corresponding DSCP mapping. The priority of the mapping is 0-7.

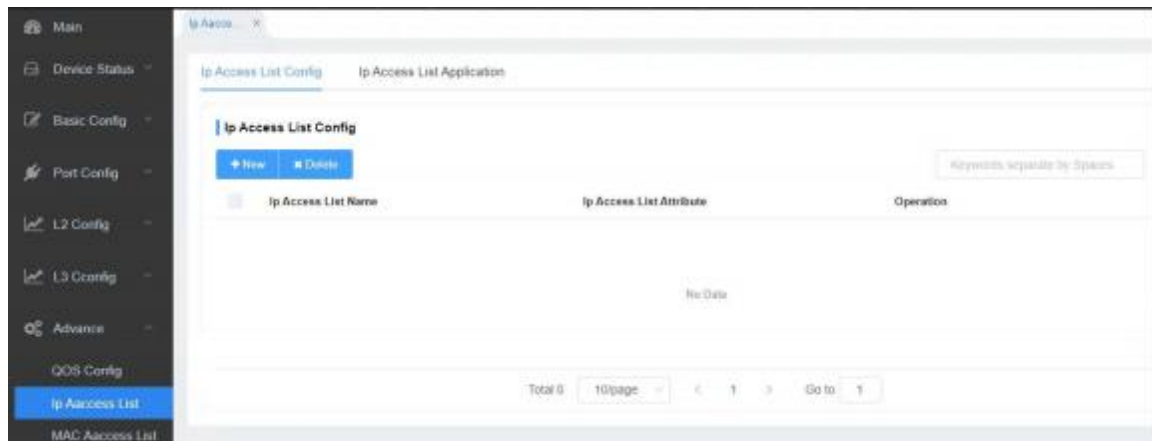


Check the corresponding DSCP and click "Clear" to reset the mapping priority to 0 and the mapping congestion bit to empty.

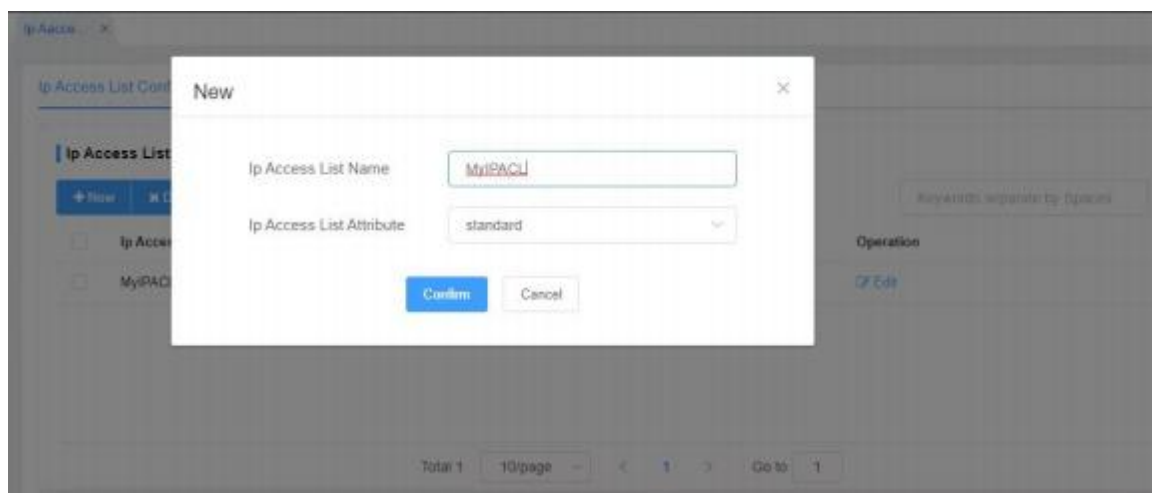
## 8.2 IP Access List

### 8.2.1 Setting IP Access List

If you click **Advance -> IP access list -> IP access list Config**, the IP ACL configuration page appears.



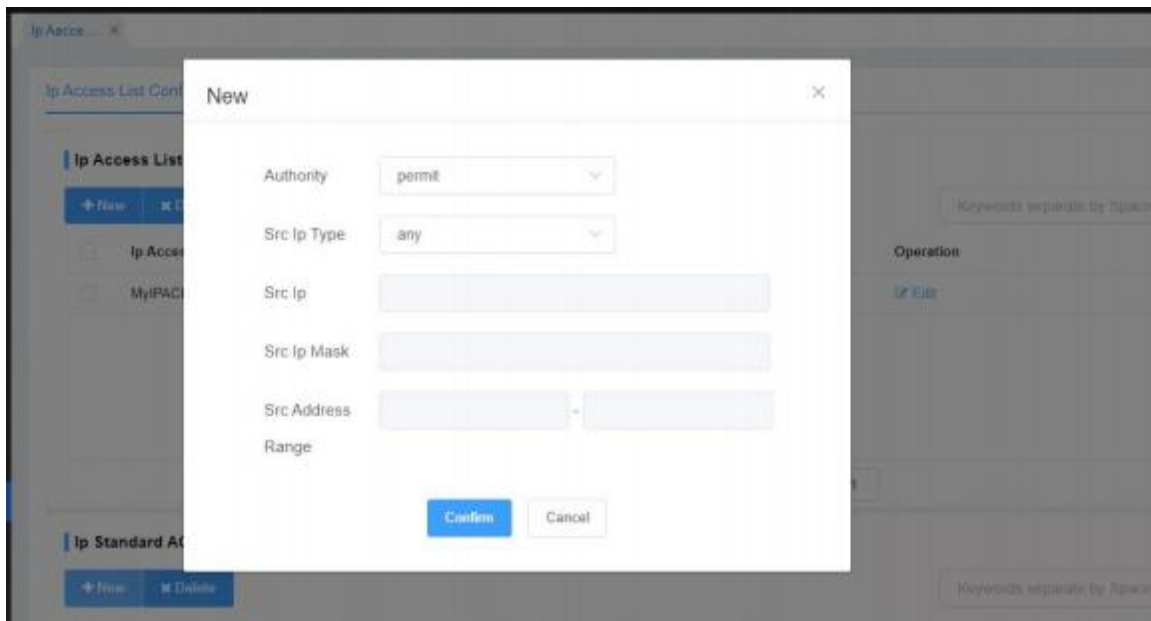
Click **New** to add a name of the IP access control list. Click **Delete** to delete an access control list.



Click "Edit" to enter the corresponding IP access control list and set the corresponding rules. The access control list attribute is "standard"

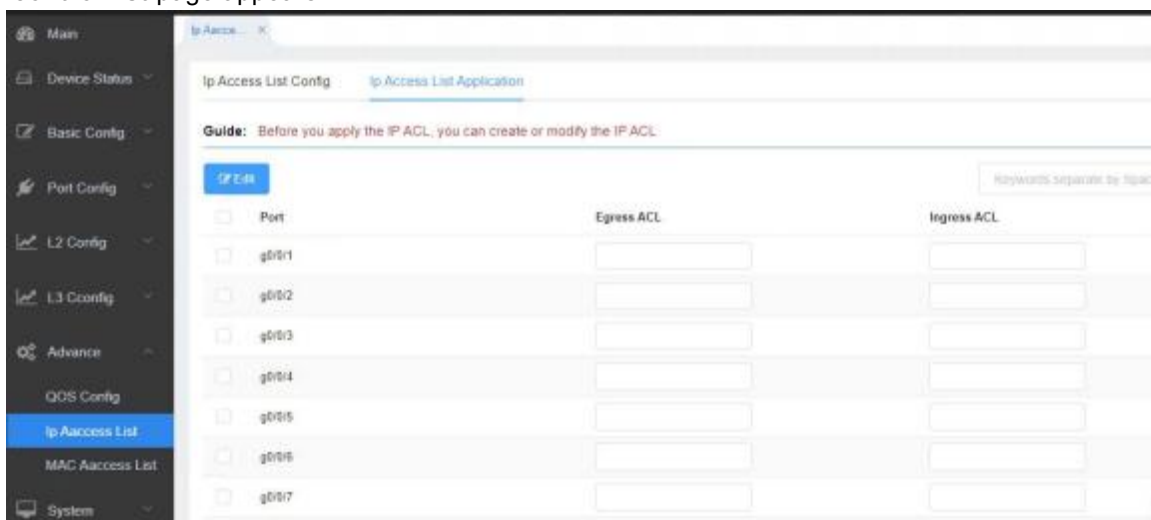


Click **Add** to add an IP access control list rule. Click **Delete** to delete the ACL rule.



### 8.2.2 Applying the IP Access Control List

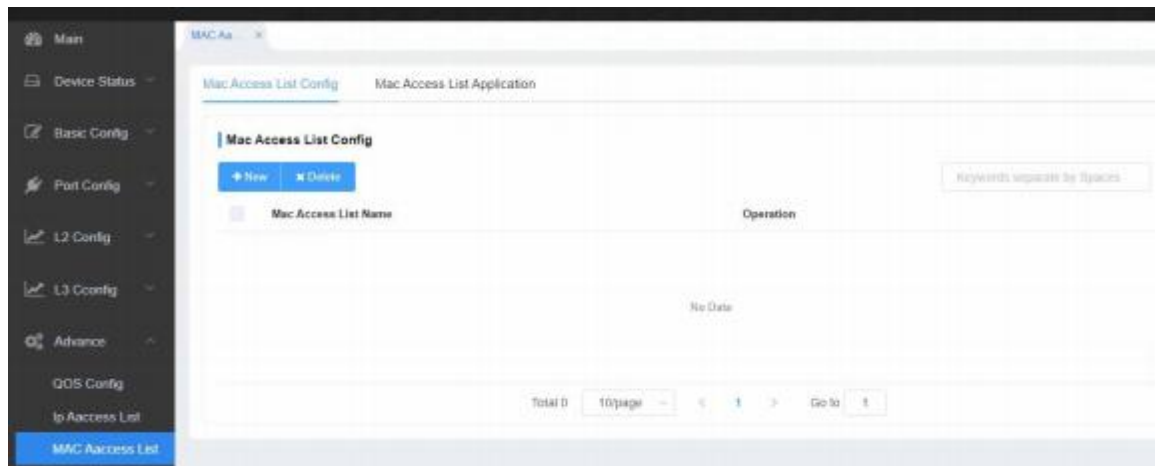
If you click **Advance** -> **IP access list** -> **IP access list application**, the **Applying the IP access control list** page appears.



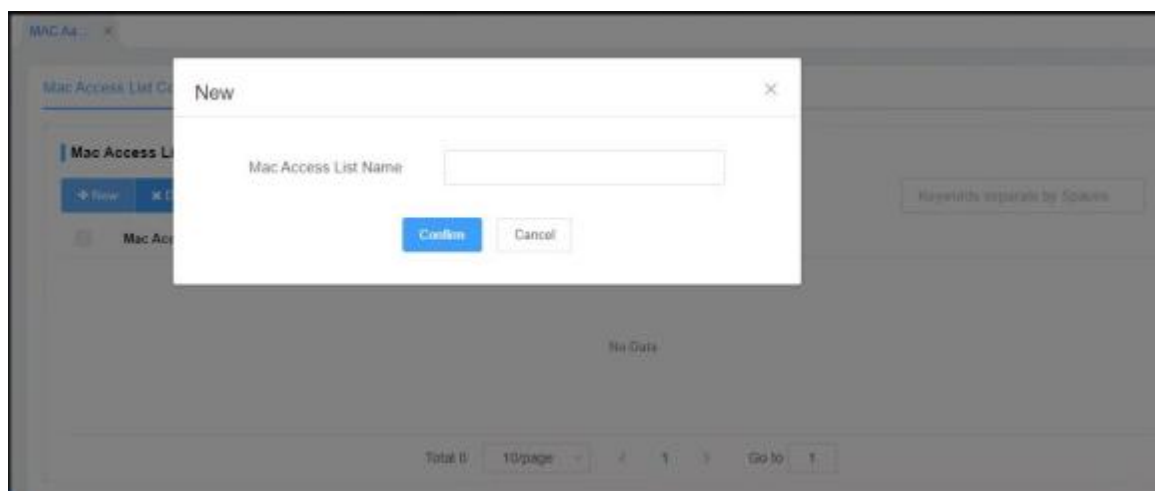
## 8.3 MAC Access Control List

### 8.3.1 Setting the Name of the MAC Access Control List

If you click **Advance** -> **MAC access list** -> **MAC access list Config**, the MAC ACL configuration page appears.



Click **New** to add a name of the MAC access list. Click **Delete** to delete a MAC access control list.



Click **Edit** to enter the corresponding MAC access control list and set the corresponding rules.



Click **Add** to add a MAC access control list rule. Click **Delete** to delete the ACL rule.



**New**

Authority:

Src Mac Type:

Src Mac:

Src Mac Mask:

Dst Mac Type:

Dst Mac:

Dst Mac Mask:

### 8.3.2 Applying the MAC Access Control List

If you click **Advance** -> **MAC access list** -> **MAC access list application**, the **Applying the MAC access control list** page appears.

MAC Access List Config **MAC Access List Application**

**Guide:** Before you apply the MAC ACL, you can create or modify the MAC ACL.

Keywords separate by Space

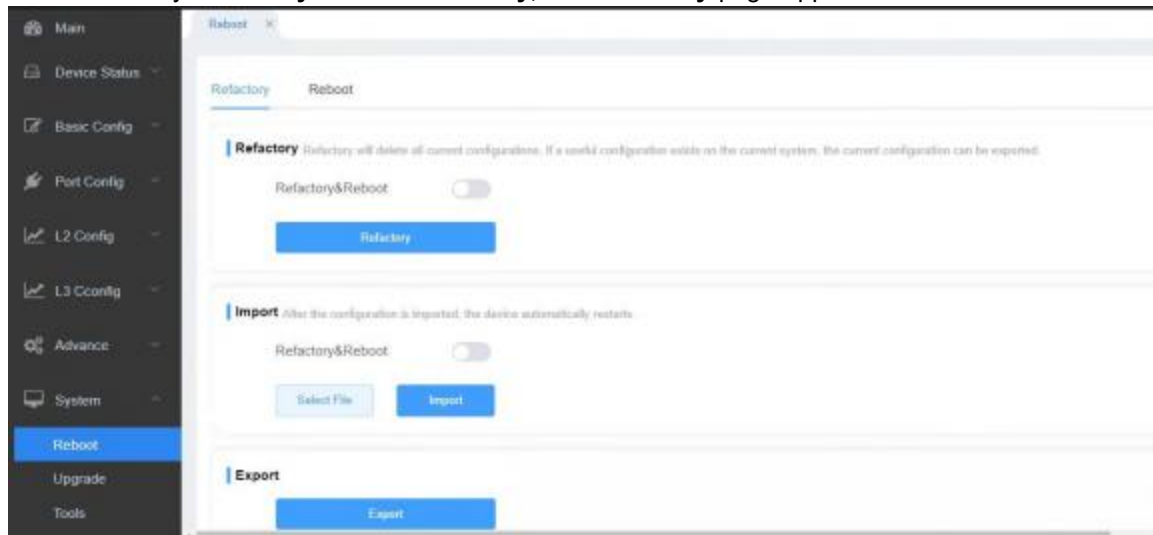
Port	Egress ACL	Ingress ACL
<input type="checkbox"/> g0/0/1	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> g0/0/2	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> g0/0/3	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> g0/0/4	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> g0/0/5	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> g0/0/6	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> g0/0/7	<input type="text"/>	<input type="text"/>

## Chapter 9 System

### 9.1 Reboot

#### 9.1.1 Refactory

If you click **System -> Refactory**, the **Refactory** page appears.



Click **"Refactory"** to restart the device and restore it to its original state.

Click **"Select File"** first to select the correct configuration file, and then click **"Import "**.

Click "Export " will backup the current device configuration file, the file name is startup-config.

---

Caution:

The "Refactory" and "Import " operations need to restart the device to take effect. It is recommended to click "Automatically restart the device after reset"

---

#### 9.1.2 Reboot

If you click **System -> Reboot**, the **Reboot** page appears.

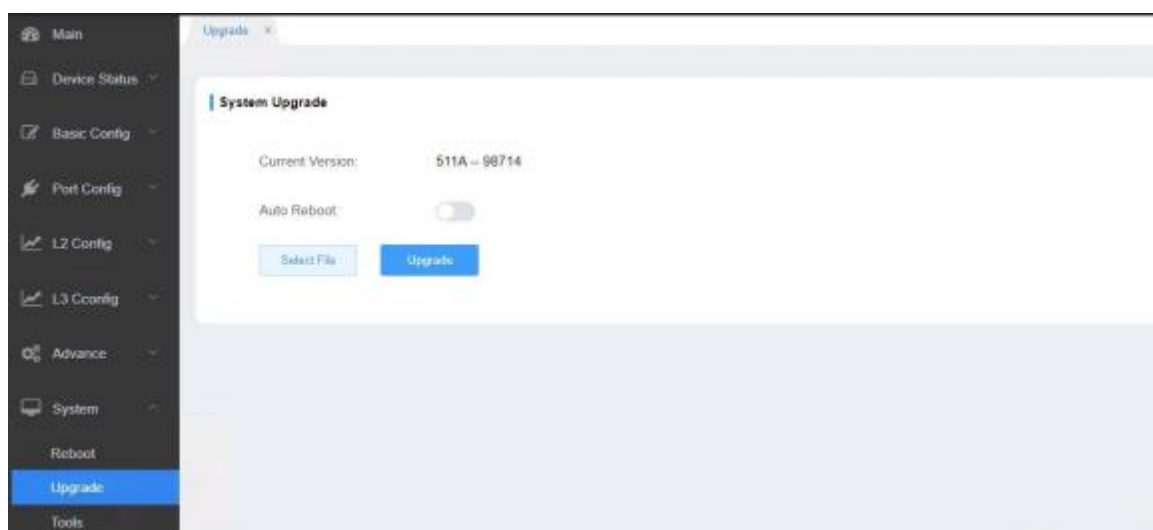


If the device need be rebooted, please first make sure that the modified configuration of the device has already been saved, and then click the “Reboot” button.

## 9.2 Upgrade

If you click **System -> Upgrade**, the System Upgrade page appears.

### 9.2.1 System Upgrade



Note:

1. Please make sure that your upgraded system matches the device type, because the un-matchable system will not lead to the normal startup of the device.
2. The upgrade of system probably takes 3 to 5 minutes; when the “updating” button is clicked, the system files will be uploaded to the device.
3. If errors occur during upgrade, please do not restart the device or cut off the power of the device, or the device cannot be started. Please try the upgrade again.
4. After the upgrade please save the configuration and then restart the device to run the new IOS.

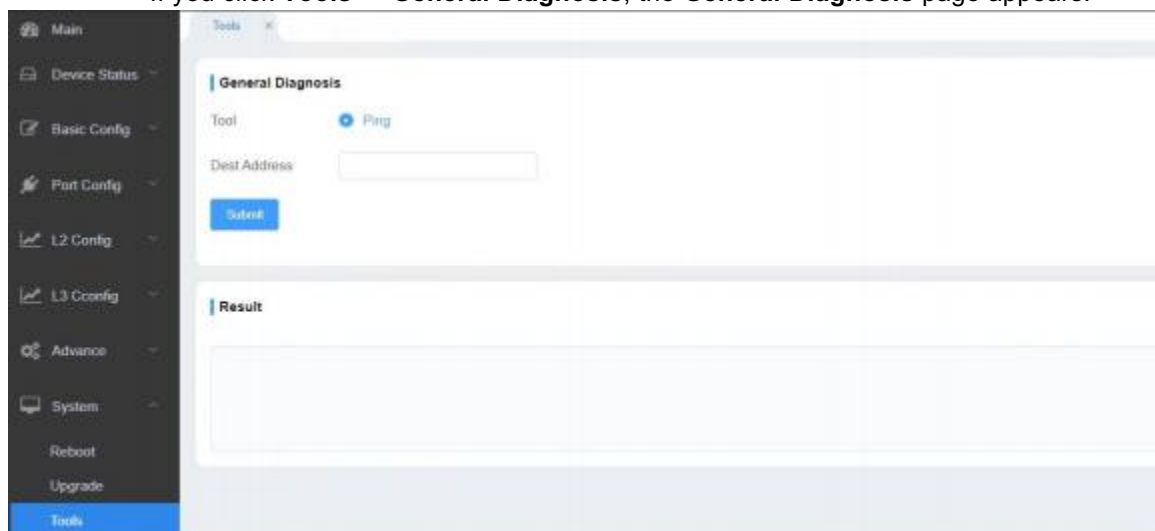


The upgraded system is always used to solve the already known problems or to perfect a specific function. If your device runs normally, do not upgrade your system software frequently.

## 9.3 Tools

### 9.3.1 General Diagnosis

If you click **Tools -> General Diagnosis**, the **General Diagnosis** page appears.



Ping is used to test whether the switch connects other devices.

If a Ping test needs to be conducted, please enter an IP address in the “Destination address” textbox, such as the IP address of your PC, and then click the “submit” button. If the switch connects your entered address, the device can promptly return a test result to you; if not, the device will take a little more time to return the test result.