Ethernet Switch (Industrial Managed Switch)

Web Operation Manual



V1.0.0

Foreword

General

This manual introduces operations on web interface of the Industrial Managed Switch (hereinafter referred to as "the Switch"). You can visit the switch on web browser, configure and manage the switch.

Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

Signal Words	Meaning
DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
TIPS	Provides methods to help you solve a problem or save you time.
NOTE	Provides additional information as the emphasis and supplement to the text.

Frequently Used Functions

Icon/Parameter	Description
	Edit an item.
or **Delete**	Delete items one by one or in batches.
or	Enable or disable items one by one or in batches.
Refresh or **Auto Refresh**	Refresh or auto refresh the content.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	September 2023

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.

- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, and comply with the guidelines when using it.

Transportation Requirements



Transport the device under allowed humidity and temperature conditions.

Storage Requirements



Store the device under allowed humidity and temperature conditions.

Installation Requirements



- Do not connect the power adapter to the device while the adapter is powered on.
- Strictly comply with the local electrical safety code and standards. Make sure that the ambient voltage is stable and meets the power supply requirements of the device.
- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.



- Do not place the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- Put the device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the device label.
- Do not connect the device to two or more kinds of power supplies, to avoid damage to the device.
- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.
- The device must be grounded by a copper wire with a cross-sectional area of 2.5 mm^2 and a ground resistance no more than 4 Ω.
- Voltage stabilizer and lightning surge protector are optional depending on the actual power supply on site and the ambient environment.
- To ensure heat dissipation, the gap between the device and the surrounding area should not be less than 10 cm on the sides and 10 cm on top of the device.
- When installing the device, make sure that the power plug and appliance coupler can be easily reached to cut off power.

Operation Requirements



- Do not disassemble the device without professional instruction.
- Operate the device within the rated range of power input and output.
- Make sure that the power supply is correct before use.
- Make sure the device is powered off before disassembling wires to avoid personal injury.
- Do not unplug the power cord on the side of the device while the adapter is powered on.



- Use the device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the device, and make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Operating temperature: *xx°C–xx°C*.
- This is a class A product. In a domestic environment this may cause radio interference in which case you may be required to take adequate measures.
- Do not block the ventilator of the device with objects, such as a newspaper, table cloth or curtain.
- Do not place an open flame on the device, such as a lit candle.

Maintenance Requirements



- Power off the device before maintenance.
- Mark key components on the maintenance circuit diagram with warning signs.

Table of Contents

Foreword I

Important Safeguards and Warnings III

1 Initialization and Login 1

2 Status Display 4

2.1 Viewing Device Information 4

2.2 Viewing Port Information 4

3 Quick Configuration 6

3.1 Configuring General Information 6

3.2 Configuring VLAN 6

3.3 Configuring Link Aggregation 7

3.3.1 Configuring Static Aggregation 7

3.3.2 Configuring LACP Mode 8

3.4 Configuring IP and Routing 8

4 Maintenance 11

4.1 Device Restart 11

4.2 Restore Factory Default 11

4.3 Configuration Management 11

4.4 Importing Update File 11

4.5 Managing Logs 11

4.6 Configuring Time 11

4.7 Configuring Mirroring 12

4.8 Configuring Ping 13

4.9 Configuring iLinksView 13

4.9.1 Starting and Logging In 13

4.9.2 Uploading and Exporting iLinksView 13

4.9.3 Viewing Legal Information 13

5 Network Settings 14

5.1 configuring Ports 14

5.2 Configuring VLAN 15

5.2.1 VLAN Definition 15

5.2.2 VLAN Function 15

5.2.3 Port-based VLAN 16

5.2.4 Adding VLAN 16

5.2.5 Configuring Port VLAN 16

5.3 Configuring IGMP Snooping 17

5.4 Configuring STP 18

5.5 Configuring Link Aggregation....19
5.6 Loopback Detection....20
5.7 Configuring ERPS....20
5.7.1 ERPS Settings....20
5.7.2 MEP Settings....21
5.8 Configuring IP and Routing....22
5.9 Configuring ARP....22
5.10 Configuring DHCP....23
5.11 Configuring DHCP Relay....25
5.12 Configuring LLDP....25
5.13 Configuring SNMP Protocol....25
5.13.1 Configuring SNMP V1 and V2....26
5.13.2 Configuring SNMP V3....27
5.14 Configuring MAC Table....29
5.14.1 Adding MAC Table....29
5.14.2 Filtering Port MAC....29
6 Security....31
6.1 Configuring Account....31
6.2 Configuring Login Mode....31
6.3 Configuring RADIUS....31
7 Control Policy....33
7.1 Configuring ACL....33
7.2 Configuring QoS Settings....35
Appendix 1 Cybersecurity Recommendations....36

1 Initialization and Login

Prerequisites

Before login, make sure

that IP addresses of the computer and the switch are on the same segment.

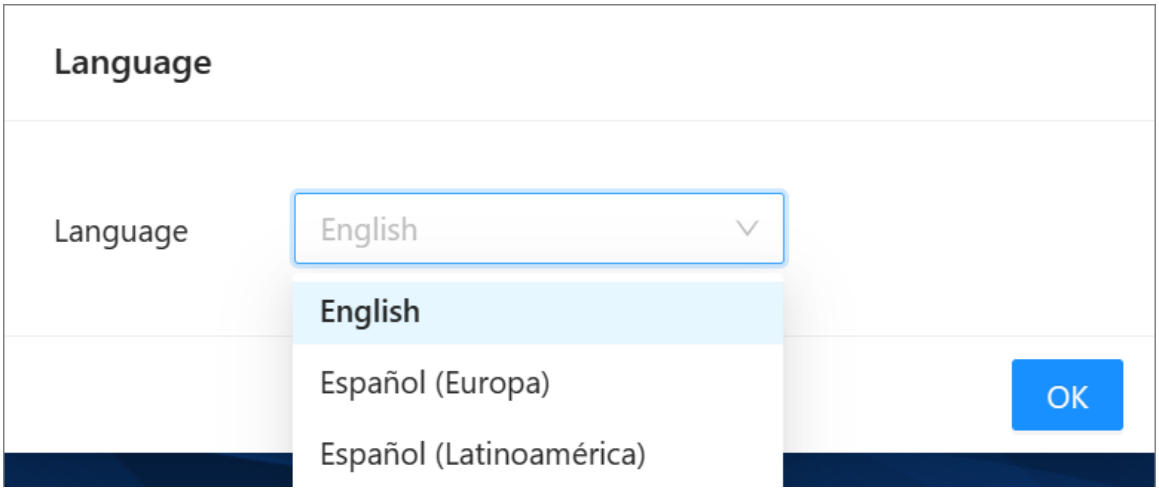
Procedure

Step 1 Enter the IP address (192.168.1.110 by default) of the switch in the address bar of the web browser, and then press the Enter key.

Step 2 Before initializing the switch, you need to select the language and the time zone.

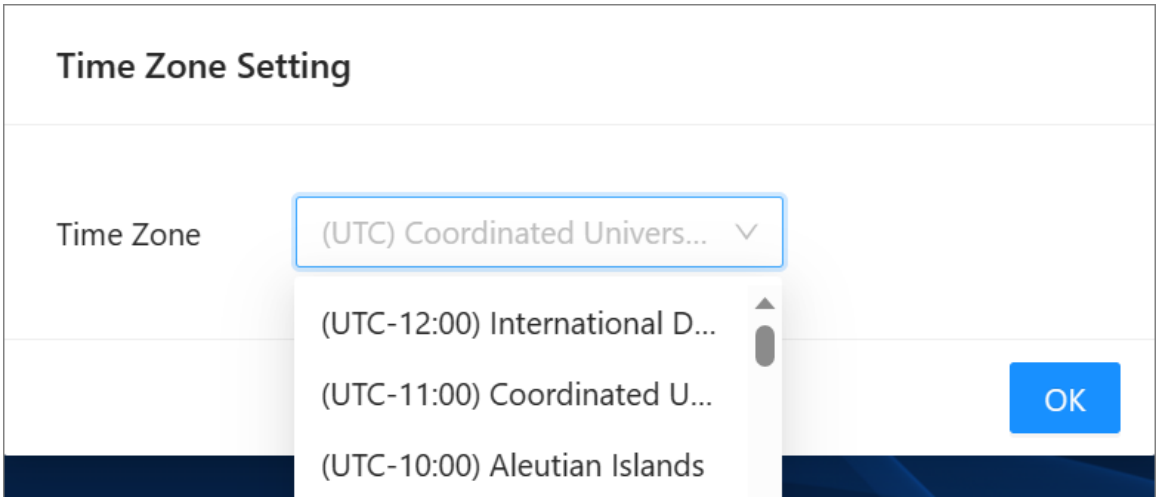
1. Select the language in the **Language** drop-down list.

Figure 1-1 Select language



2. Select the time zone in the **Time Zone** drop-down list.

Figure 1-2 Select time zone



Step 3 Initialize the switch.

1. Enter the username and password.

- The default username is admin.

- Set a high security password according to the prompt of password strength. A password should be 8-32 characters containing at least two types among numbers, letters and common characters (any visble characters other than' " ; : &).

2. After initilizing, the system will be directed to the login page.

Step 4 Log in to the switch.

1. Enter the username and password.
2. Click **Login**.

Figure 1-3 Log in to the web

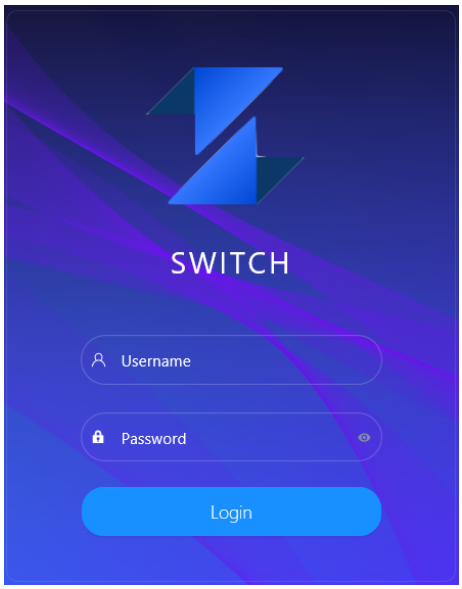


Figure 1-4 Home page

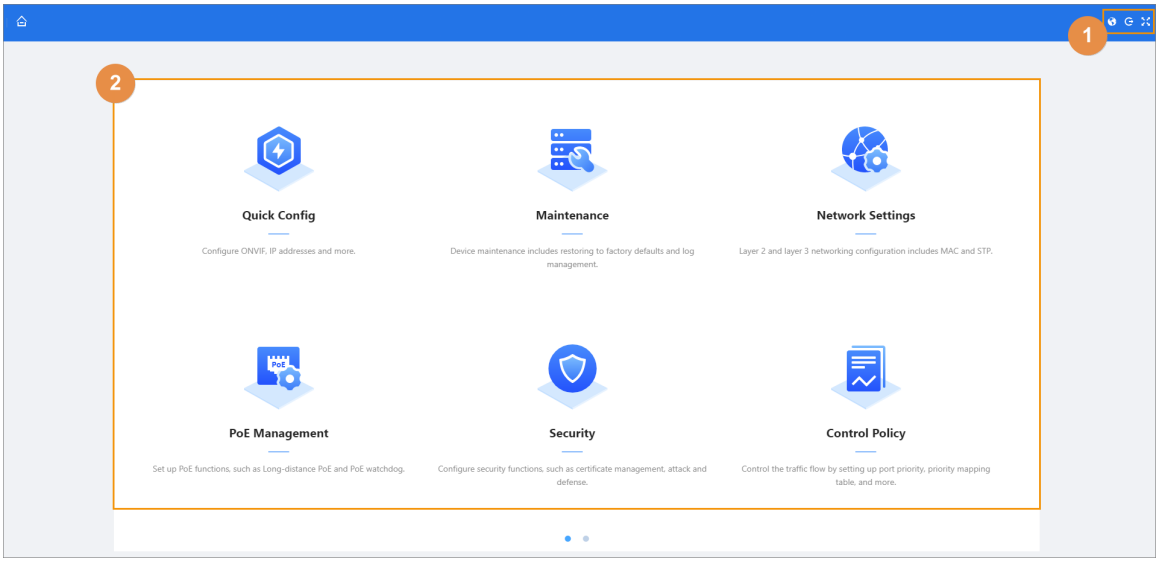


Table 1-1 Description of the homepage

No.	Name	Description
1		Switch the system languages. Supports multiple languages.
		Logout the user, and then return to the login page.

No.	Name	Description
		Full-screen displays the web page.
2	Status Display	Displays the real-time operating status of the device.
	Quick Config	Configure quick settings, including ONVIF, IP address and more.
	Maintenance	Configure maintenance settings, including restoring to factory defaults and log management.
	Network Settings	Configure network settings, including MAC and STP settings.
	Security	Configure security settings, including certificate management, attack and defense.
	Control Policy	Configure traffic flow swttings, including setting port priority, priority mapping table and more.

2 Status Display

2.1 Viewing Device Information

Select **Status Display** > **Device Info** to view the information of the switch, including system, software, hardware, and time.

2.2 Viewing Port Information

Procedure

Step 1 Select **Status Display** > **Port Info**.

Step 2 View the detailed information of the ports.

The port information might differ from different models. Refer to the actual product.

Figure 2-1 Port information

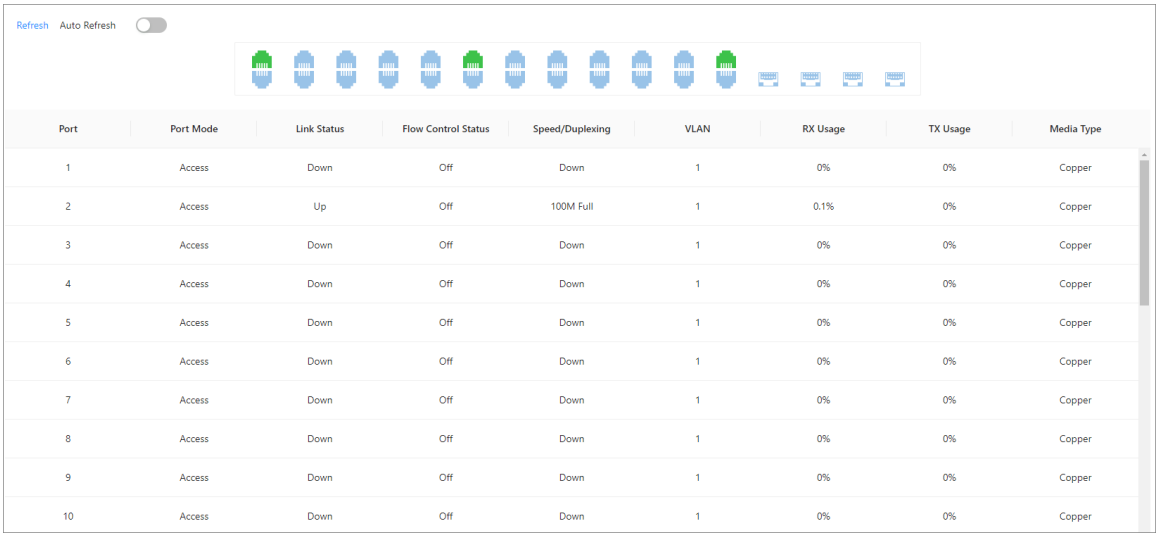


Table 2-1 Description of the port information

Name	Description
Port	Displays all the ports of the switch. ● Green: The port is connected. ● Gray: The port is not connected or the connection fails.

Name	Description
Port Mode	Includes 3 modes: **Access** , **Trunk**, and **Hybrid**. • Access: Belongs to one VLAN. Commonly used to connect computer ports. • Trunk: Allows multiple VLANs through. Receives and sends multiple VLAN packets. Typically used for connection between switches. • Hybrid: Allow multiple VLANs through. Receives and sends multiple VLAN packets. Used for connection between switches, or switch and computer.
Link Status	Includes 2 statuses: **Up** and **Down**. • Up: The port is connected. • Down: The port is not connected or the connection fails.
Flow Control Status	Includes 2 statuses: **On** and **Off**.
Speed/Duplexing	Displays the transmission rate and the duplexing of the port. • Actual data: The transmission rate of the port. • Down: The port is offline.
VLAN	Displays the VLAN of the port. It is VLAN 1 by default.
RX Usage	The value of receiving rate divided by the actual negotiating rate within a certain period (5 minutes).
TX Usage	The value of sending rate divided by the actual negotiating rate within a certain period (5 minutes).
Media Type	Includes two types of transmission media: Copper and fiber.

3 Quick Configuration

You can view the system information, and configure the switch parameters including IP address, VLAN, link aggregation, routing and more. The pages on the manual are for reference only, and might differ from the actual pages.

3.1 Configuring General Information

You can view and configure the general information, including name, IP address, subnet mask, and VLAN.

Procedure

Step 1 Select **Quick Config** > **General**.

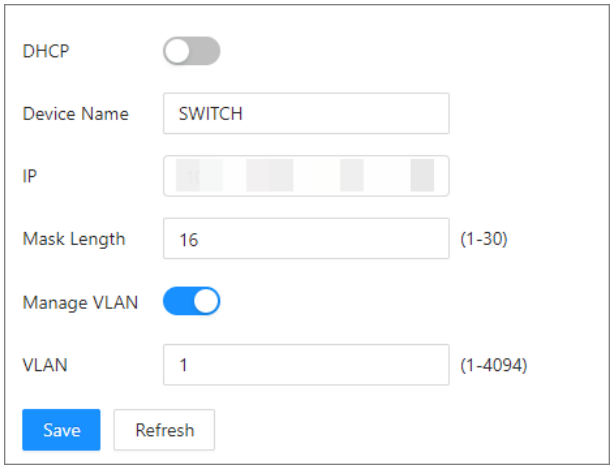
Step 2 (Optional) Click to enable the DHCP function.

Please be advised of this function. Once DHCP is enabled, the router or the DHCP server connected with the switch will automatically assign IP address to the switch. The original IP address will fail to access the webpage.

Step 3 View and configure the general information of the switch.

- **Manage VLAN** is enabled by default. Disable VLAN management can disable access to ConfigTool or iLinks-View. Please be advised.
- VLAN is set as 1 by default.

Figure 3-1 General information



3.2 Configuring VLAN

This section introduces the basic settings of the VLAN configuration. For details, see .

Procedure

Step 1 Select **Quick Config** > **VLAN**.

Step 2 Configure the VLAN parameters, and then click **Save**.

Figure 3-2 Quick settings of VLAN

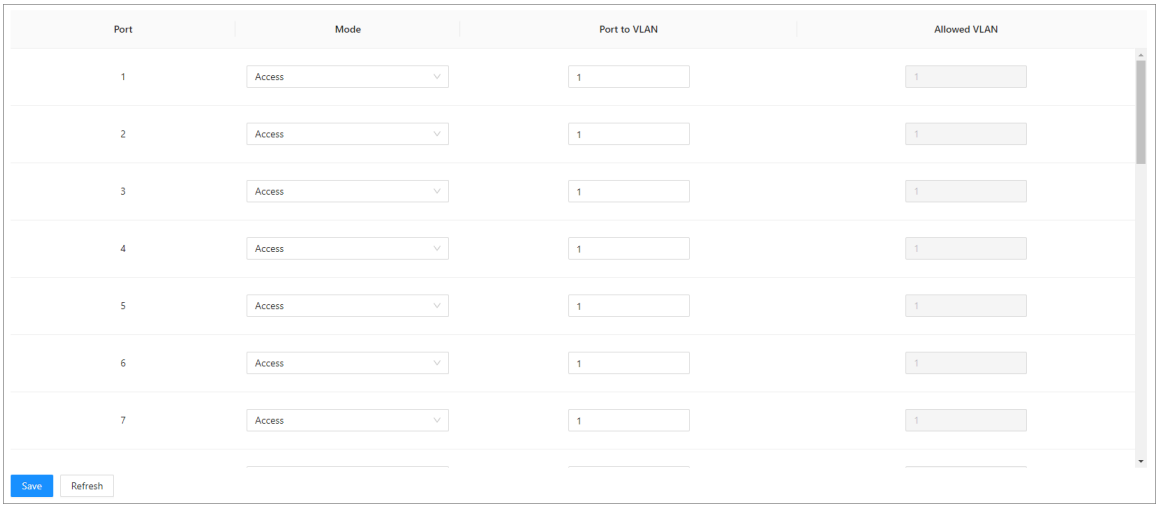


Table 3-1 VLAN description

Parameter	Description
Port	Displays all the ports of the switch.
Mode	Includes three modes: **Access** , **Trunk**, **Hybrid**. For the details on the three modes, see "2.2 Viewing Port Information".
Port to VLAN	Set VLAN for the port. It is VLAN 1 by default, and the range is from 1 to 4094.
Allowed VLAN	Set the allowed VLAN that can get through the port. Only when mode is selected as **Trunk** and **Hybrid**, can this parameter be set.

3.3 Configuring Link Aggregation

This section introduces the quick configuration of link aggregation. For details, see .

3.3.1 Configuring Static Aggregation

Procedure

Step 1 Select **Quick Config** > **Link Aggregation**

Step 2 Click **Add**.

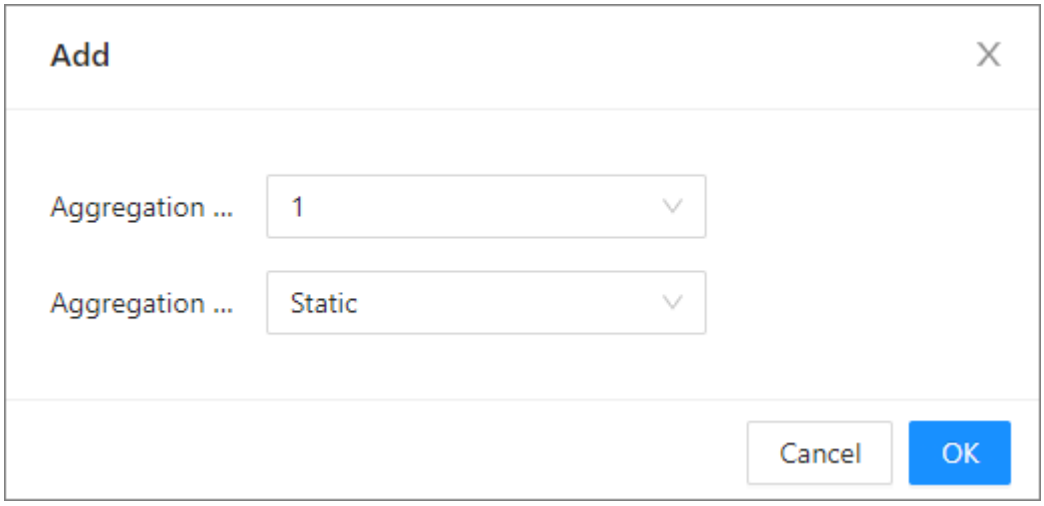
Step 3 On the **Add** page, enter the **Aggregation Group No.**, set **Aggregation Group Mode** as **Static**, and then click **OK**.

Aggregation Group Mode includes 3 types: **Static**, **Active**, and **Passive**.

- Static: Static aggregation.

- Active: This mode places the port in an active negotiating state. In this mode, the port initiates negotiation with other ports by sending LACPDUs.
- Passive: This mode places the port in a passive negotiating state. In this mode, the port responds to the LACPDUs that it receives but does not initiate LACPDU negotiation.

Figure 3-3 Add static aggregation



Step 4 Select the ports that need to be added into the group, and then click **OK**.

3.3.2 Configuring LACP Mode

Procedure

Step 1 Select **Quick Config** > **Link Aggregation**

Step 2 Click **Add**.

Step 3 On the **Add** page, enter the **Aggregation Group No.**, set **Aggregation Group Mode** as **Active** or **Passive**.

Step 4 Select the ports that need to be added into the group, and then click **OK**.

3.4 Configuring IP and Routing

Introduces the IP setings and the routing settings of the switch.

Procedure

Step 1 Select **Quick Config** > **IP & Routing**.

Step 2 On the **IP Settings** tab, click **Add**, and then configure the parameters.

Figure 3-4 IP settings

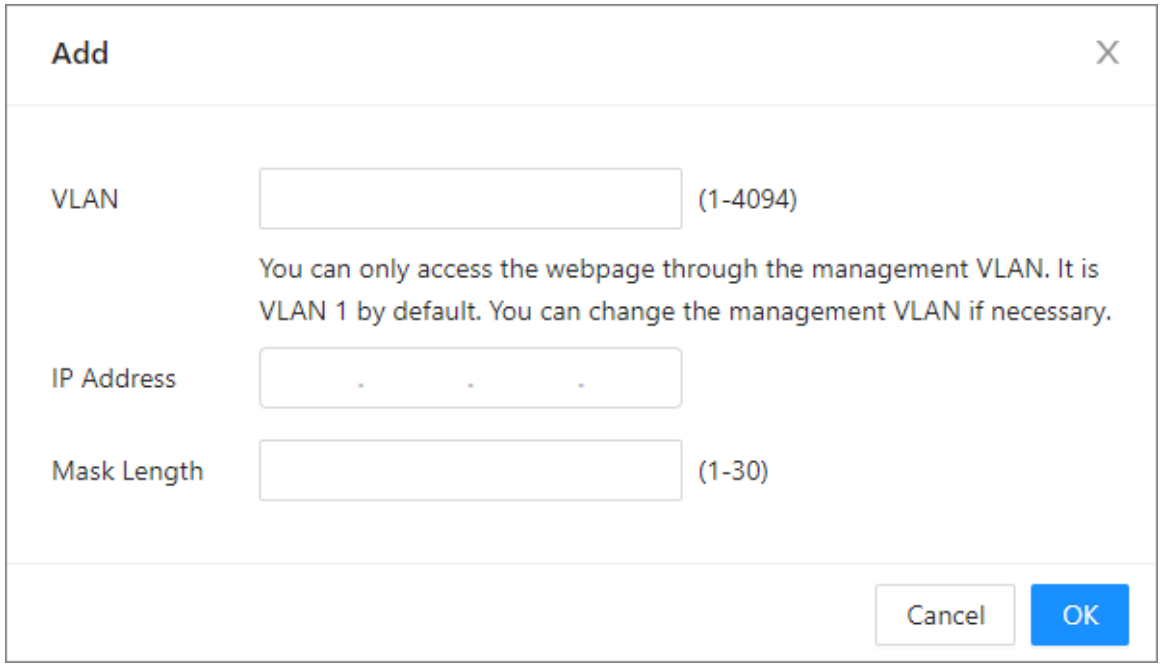


Table 3-2 Description of IP parameters

Parameter	Description
VLAN	Enter the VLAN.
IP Address	Set the IP address of the device.
Mask Length	Set the mask length of the device.

Step 3 On the **Routing Settings** tab, click **Add**, and then configure the parameters.

Figure 3-5 Routing settings



Table 3-3 Description of the routing parameters

Parameter	Description
Network	Enter the destination address or destination network to identify the IP packet.
Mask Length	Set the segment to identify the destination switch or router with the destination address.
Next Hop	Set the next hop address of the router.

4 Maintenance

4.1 Device Restart

Select **Maintenance** > **Device Restart**, and then click **Reboot Now** to restart the switch.

4.2 Restore Factory Default

Select **Maintenance** > **Restore Factory Default**, and then click **Restore Factory Default** to restore to the default settings.

4.3 Configuration Management

Select **Maintenance** > **Configuration** to manage the configuration files.

Upload Configuration File

Click **Browse** to select the file, and then click **Upload** to upload the configuration file.

Export Configuration File

Click **Export** to export the configuration file.

4.4 Importing Update File

Select **Maintenance** > **Update**, click **Browse** to import the update file, and then click **Update now**.

4.5 Managing Logs

You can query and export logs.

Procedure

Step 1 Select **Maintenance** > **Log**.

Step 2 Select **Time** and **Log level**.

Log level includes **All**, **Error**, **Warning**, **Notice**, **Informational**.

Step 3 Click **Query**, and then view the log information.

Step 4 Click **Export** to export the log information.

4.6 Configuring Time

Background Information

You can view and configure the system time of the switch.

Procedure

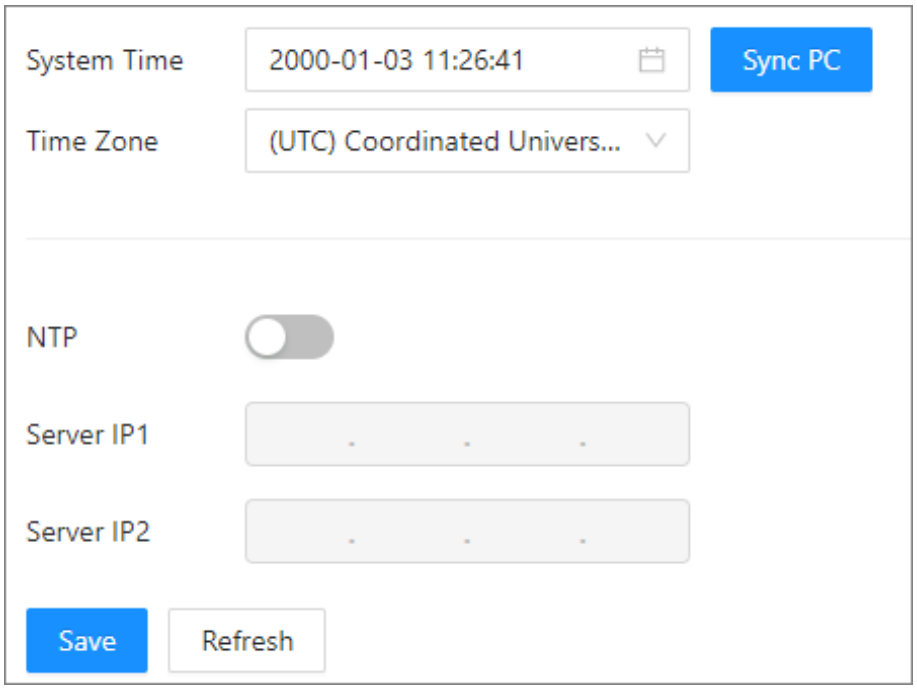
Step 1 Select **Maintenance** > **System Time**.

Step 2 Configure the system time. There are 3 methods:

- Manually configure the **System Time** and **Time Zone**.
- Click **Sync PC** to synchronize the swicth time to the computer time.
- Click to enable **NTP**, and then synchronize the switch time to the server time.

Enabling NTP will automatically synchronize time with server.

Figure 4-1 Configure time



4.7 Configuring Mirroring

Background Information

Mirroring copies traffic received or sent or both on a specified source to a destination port for analysis. The specified source is called mirrored source, the destination port is called observing port, and the copied traffic is called mirrored traffic.Mirroring sends a copy of the traffic through an observing port on the switch to a monitoring device for service analysis.

Procedure

Step 1 Select **Maintenance** > **Mirror**.

Step 2 Click to enable the **Global Config**.

Step 3 Select the port, and then click the checkbox under **Destination** to configure the port as destination port.

Step 4 Select another port, and then select **Source**.

Step 5 Click **Save**.

Table 4-1 Source description

Name	Description
Disabled	No sending or receiving traffic.
TX Only	Only supports sending traffic.
RX Only	Only supports receiving traffic.
Both	Supports both sending and receiving.

4.8 Configuring Ping

You can check if the device with designated IP can be access and if the network connection is normal through ping.

Procedure

Step 1 Select **Maintenance** > **Ping**.

Step 2 Configure **IP Address** , **Ping Size**, **Ping Times**, and **Ping Interval**.

Step 3 Click **Ping**.

4.9 Configuring iLinksView

4.9.1 Starting and Logging In

Procedure

Step 1 Select **Maintenance** > **iLinksView**.

Step 2 On the **iLinksView** tab, click to enable the function.

Step 3 Enter the username and password.

- The username is admin by default. The password is lt_91_il_02_nmp by default.
- You can set your username and password, but they need to be the same as those of the iLinksView platform.

Step 4 Click **Save**.

4.9.2 Uploading and Exporting iLinksView

Procedure

Step 1 Select **Maintenance** > **iLinksView**.

Step 2 On **Upload** tab, click **Browse** to select iLinksView file, and then click **Upload**.

Step 3 On **Export** tab, click **Export** to export iLinksView file.

4.9.3 Viewing Legal Information

Select **Maintenance** > **Legal Info** to view the **Open Source Software Notice**.

5 Network Settings

5.1 configuring Ports

Background Information

You can configure the port parameters, including speed/duplexing, flow control, and other parameters. The port parameters will directly affect the working mode of the port. Make configurations according to the practical requirements.

The webpage might differ from different devices. Refer to the actual pages.

Procedure

Step 1 Select**Network Settings** > **Port**.

Step 2 You can view and configure the parametes.

Figure 5-1 Port settings

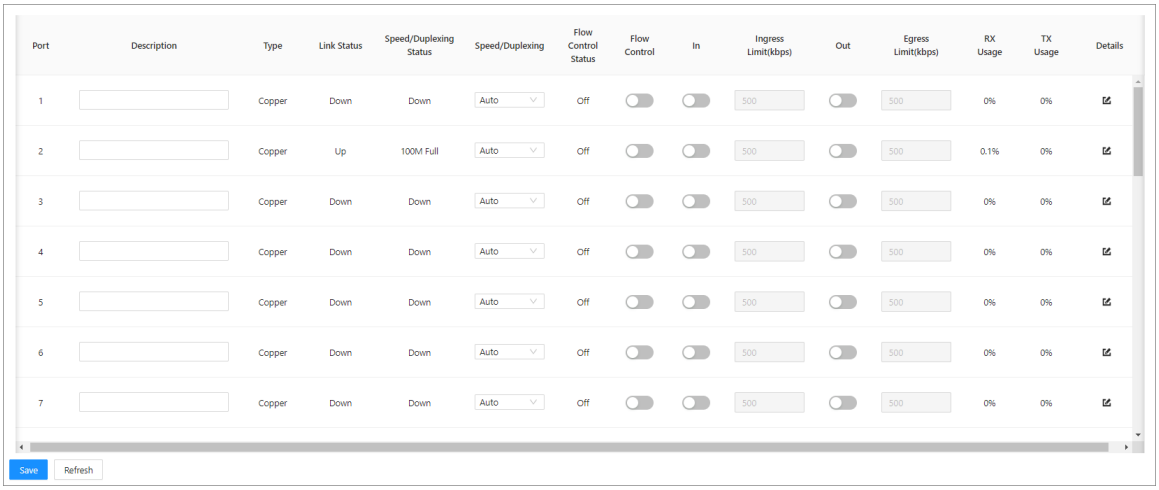


Table 5-1 Port parameters

Parameter	Description
Port	Displays all ports of the switch.
Description	Enter the description of the port. The description can not exceed 64 characters. Only numbers,letters and the following special characters are allowed: . _ -. The first character must be a letter and the last charcter must not be a special character.
Type	Displays ywo kinds of media type, includes two types: **Copper** and **Fiber**. • Copper: Ethernet port. • Fiber: Optical port.

Parameter	Description
Link status	Includes two ststus: **Up** and **Down**. • Up: The port is connected. • Down: The port is not connected or the connection fails.
Speed/Duplexing status	• Online: Displays the port rate and the duplex mode. • Offline: Displays **Down**.
Speed/Duplexing	Set the speed and the duplex mode from **Down** , **Auto**,**10M Half**, **10M Full**,**100M Half**, **100M Full**, and **1G Full**.
Flow Control Status	Displays flow control status.
Flow control	Click to enable or disable the function.
In	Click to enable the ingress function.
Ingress Limit(kbps)	Aftering enabling **In**, you can configure the ingress limit.
Out	Click to enable the egress function.
Egress Limit(kbps)	Aftering enabling **Out**, you can configure the egress limit.
RX usage	Displays the receiving usage.
TX usage	Displays the sending usage.
Details	• View the total transmitting, total receiving and other information of each port. You can refresh or clear the detailed information of each port. • View the number of error bytes.

Step 3 Click **OK**.

5.2 Configuring VLAN

5.2.1 VLAN Definition

Logically, one LAN (Local Area Network) can be divided into many subsets. Each subset has its own broadcast area: virtual LAN (VLAN). A VLAN is divided from a LAN on a logical basis rather than on a physical basis, to realize the isolated broadcast area in the VLAN.

5.2.2 VLAN Function

- Enhance the network performance. The broadcast packets are in the VLAN, which can effectively control the network broadcast storm, reduce network bandwidth and enhance network processing ability.
- Enhance the network security. The switches in different VLANs cannot access each other, and the hosts in different VLAN cannot communicate with each other. They need a router or the three-layer switch to forward the message.
- Simplify the network management. The host of the same virtual working group is not limited in one physical area, which can simplify the network management and facilitate to establish working groups for users in different areas.

5.2.3 Port-based VLAN

The port types include **Access** , **Trunk** and **Hybrid**.

- Access: The port belongs to one VLAN, and is used to connect to the computer port.
- Trunk: The port allows multiple VLANs to pass, to receive and send messages of multiple VLANs, and is used to connect between the switches.
- Hybrid: The port allows multiple VLANs to pass, to receive and send messages of multiple VLANs, and is used to connect between the switches, and connect the computer.

5.2.4 Adding VLAN

Background Information

You can add the port to the VLAN. The VLAN is VLAN1 by default.

Port isolation and VLAN cannot be enabled at the same time. If one of them is enabled, the other one will be automatically disabled. Please be advised.

Procedure

Step 1 Select **Network Settings** > **VLAN**.

Step 2 On the **Add VLAN** page, click **Add**, enter the **VLAN ID** and **Description**.

Step 3 Click **OK**.

VLAN1 can not be deleted.

Related Operations

- Click to edit VLAN.
- Click to delete VLAN.

5.2.5 Configuring Port VLAN

You can configure the port VLAN parameters.

Figure 5-2 Configure VLAN

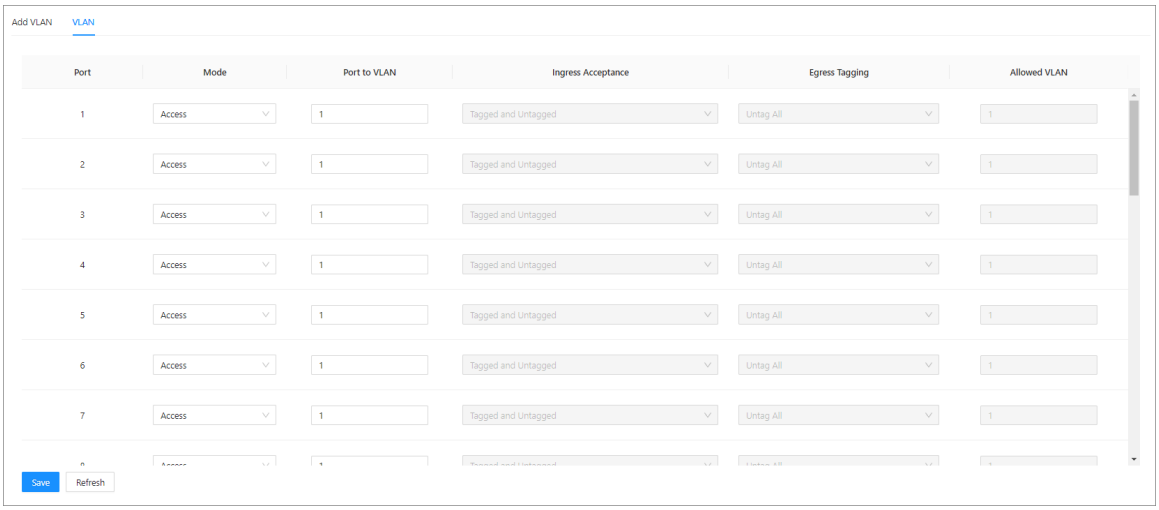


Table 5-2 Port VLAN configuration parameter

Parameter	Description
Port	Displays all ports of the switch.
Mode	Includes three modes: **Access** , **Hybrid**, and **Trunk**. • Access: Belongs to one VLAN. Commonly used to connect computer ports. • Trunk: Allows multiple VLANs through. Receives and sends multiple VLAN packets. Typically used for connection between switches. • Hybrid: Allow multiple VLANs through. Receives and sends multiple VLAN packets. Used for connection between switches, or switch and computer.
Port to VLAN	Add the port to a VLAN, and all ports belong to VLAN 1 by default. The range is from 1 to 4094. After adding the port, the port will display on the **Add VLAN** tab.
Ingress Acceptance	Displays whether the data that will ingress the port. • Only when **Mode** is selected as **Hybrid**, can **Ingress Acceptance** be selected. • All data will ingress the port under other modes. • **Tagged and Untagged** : All data will ingress the port. • **Tagged Only** : Only tagged data will ingress. • **Untagged Only** : Only untagged data will ingress.
Egress Tagging	Displays whether to tag the data that will egress the port. Only when **Mode** is selected as **Trunk** and **Hybrid**, can **Egress Tagging** be selected. • **Untag Port VLAN** : If the data flow tag is the same with PVID, the tag will be peeled. • **Tag All** : All data will be tagged. • **Untag All** : All data will not be tagged.
Allowed VLAN	Configure the VLAN can be allowed through.

5.3 Configuring IGMP Snooping

Background Information

IGMP Snooping (Internet Group Management Protocol Snooping) is the multicast constraint mechanism running on the device of layer 2, for managing and controlling the multicast. Through analyzing the received IGMP packet, the device of layer 2, which runs IGMP Snooping, creates the mapping between the port and the MAC multicast address, and forwards the multicast data according to the mapping.

Procedure

Step 1 Select **Network Settings** > **IGMP Snooping**.

Step 2 Click next to **IGMP Snooping** to enable the function.

Step 3 Click next to **Drop Unknown Multicast Messages** to enable the function.

- Enable the function: Once the function is enabled, if the switch receives group messages that are not registered, it leaves the messages. The bandwidth will be saved, and then the forwarding rate will be increased.
- Disable the function: If the group messages are not registered, the messages will be broadcast in the VLAN. The bandwidth will be occupied, and then the the forwarding rate will be decreased.

Please be advised on enabling **Drop Unknown Multicast Messages**, otherwise the multicast might fail.

Step 4 Click **Add**, and then configure the parameters.

Figure 5-3 IGMP parameter



Table 5-3 Parameter description

Parameter	Description
VLAN	The number of the VLAN.
Querier	Click to enable the function.
Search Address	Enter the IP address of the switch, and then set the switch as the querier.

Step 5 Click **Save**.

5.4 Configuring STP

Background Information

Spanning Tree Protocol (STP) builds a loop-free logical topology for LANs. It blocks redundant links between any two network devices and leaves a single active link between them so as to eliminate loops.

STP, RSTP, and MSTP provide the following capabilities:

- STP: A management protocol at the data link layer, is used to detect and prevent loops on a Layer 2 network. It, however, converges the network topology slowly.
- RSTP: An enhancement to STP, allows for rapid network topology convergence. However, both RSTP and STP have a defect that all the VLANs on the same LAN share the same spanning tree.
- MSTP: A virtual VLAN mapping table in which VLAN IDs are associated with spanning tree instances. Not only this, MSTP divides a switching network into multiple regions, each of which has multiple spanning tree instances that are mutually independent. Unlike STP and RSTP, MSTP provides multiple redundant paths for data forwarding. In addition, it implements load balancing among VLANs.

Procedure

Step 1 Select **Network Setings** > **STP**

5.5 Configuring Link Aggregation

Background Information

Link aggregation is to form a multiple physical ports of the switch into the logical port. The multiple links in the same group can be regarded as a logical link with a larger bandwidth.

Through aggregation, the ports in the same group can share the communication flow, to make a larger bandwidth. Besides, the ports in the same group can back up reciprocally and dynamically to enhance the link reliability.



- The link aggregation is mutually exclusive with STP mode, IGMP Snooping, and 802.1x mode. When STP mode is enabled, link aggregation cannot be configured. You must disable STP mode before configuring link aggregation.
- We do not recommend implementing configuration and advanced functions for the ports which are used for link aggregation.
- Link aggregation can be divided into static aggregation and LACP. Generally, the peer devices with the switch link aggregation are switch and network adapter.
- Only the ports with the same speed rate, duplex, long distance and VLAN configuration can be in the one aggregation group.

Procedure

Step 1 Select **Network Settings** > **Link Aggregation**.

Step 2 Click **Add**.

Step 3 Select the **Aggregation Group No.**.

Step 4 Select the **Aggregation Group Mode** , and then click **OK**.

Aggregation group mode includes static, LACP active, and LACP passive.

- Static: Static is also known as manual mode. The Eth-Trunk interface must be manually created and member interfaces need to be manually added. The LACP protocol is disanbled.
- LACP active: The Eth-Trunk interface must be manually created and member interfaces need to be manually added. Compared with static, the selection of interface is configured by LACP protocol. This mode places an interface in an active negotiating state. In this mode, the interface initiates negotiations with other interfaces by sending LACPDUs.
- LACP passive: The Eth-Trunk interfaces are created and member interfaces are added by LACP protocol. This mode places an interface in a passive negotiating state. In this mode, the interface responds to the LACPDUs that it receives but does not initiate LACPDU negotiation.

Step 5 Select ports to be added, and then click **OK**.

Step 6 Click **OK**.

5.6 Loopback Detection

LBDT periodically sends detection packets on an interface to check whether the packets return to the local device, and determines whether a loop occurs on the interface, on the downstream network or device, or between two device interfaces.

Select **Network Settings** > **Loopback Detection**, click  to enable the function.

5.7 Configuring ERPS

ERPS is a protocol defined by the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) to eliminate loops at Layer 2. Generally, redundant links are used on an Ethernet switching network such as a ring network to provide link backup and enhance network reliability. The use of redundant links, however, may produce loops, causing broadcast storms and rendering the MAC address table unstable. As a result, communication quality deteriorates, and communication services may even be interrupted. ERPS prevents broadcast storms and implements fast traffic switchover on a network where there are loops, provides fast convergence and carrier-class reliability, and allows all ERPS-capable devices on a ring network to communicate.

5.7.1 ERPS Settings

Procedure

Step 1 Select **Network Settings** > **ERPS**.

Step 2 On the **ERPS** tab, click **Add** to add ERPS.

Step 3 Configure the parameters, and then click **OK**.

Figure 5-4 Add ERPS

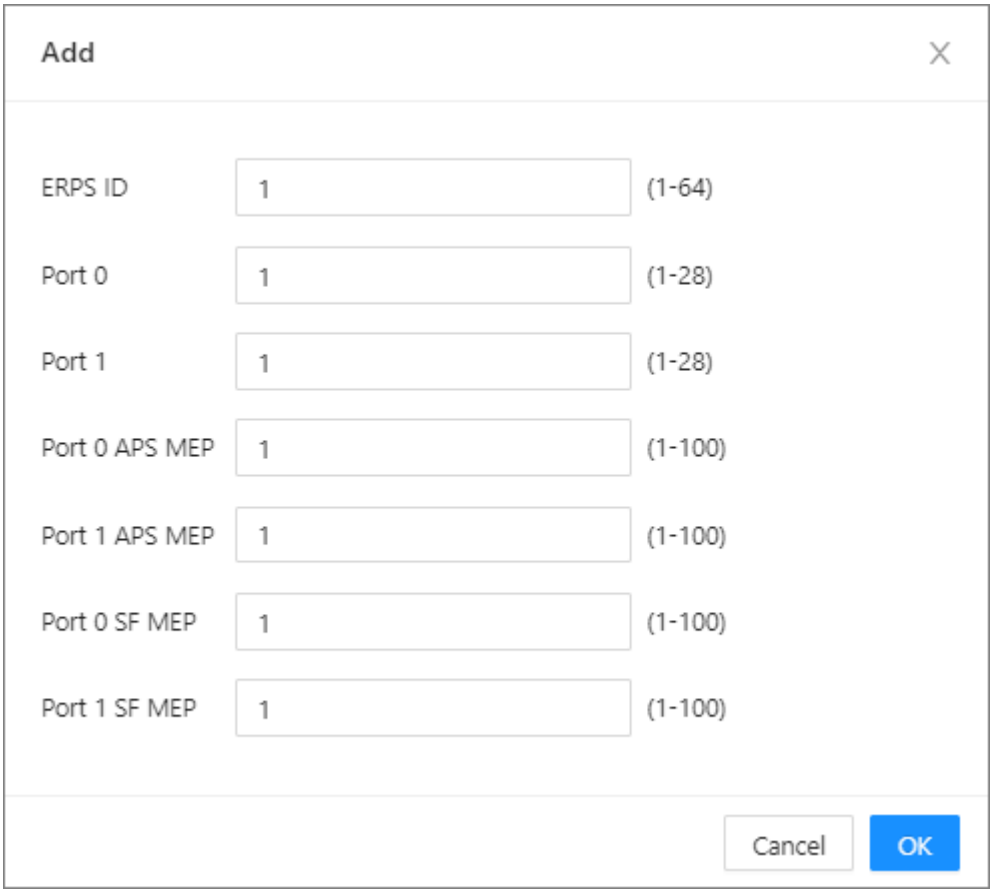


Table 5-4 Parameter description

Parameter	Description
ERPS ID	The ID number of the ERPS.
Port 0	Two ports of the switch to be added into the ERPS.
Port 1	
Port 0 APS MEP	• BPDU MEP of the ERPS port. • Link monitoring MEP of the ERPS port. Port 0 APS MEP keeps the same as Port 0 SF MEP. Port 1 APS MEP keeps the same as Port 1 SF MEP.
Port 1 APS MEP	
Port 0 SF MEP	
Port 1 SF MEP	

5.7.2 MEP Settings

Background Information

MEP (Maintenance Entity Group End Point) is a part of the ERPS ring. A node refers to a Layer 2 switching device added to an ERPS ring. A maximum of two ports on each node can be added to the same ERPS ring.

Procedure

Step 1 Select **Network Settings** > **ERPS**.

Step 2 On the **MEP** tab, click **Add** to add MEP.

Step 3 Configure MEP parameters.

Figure 5-5 Add MEP

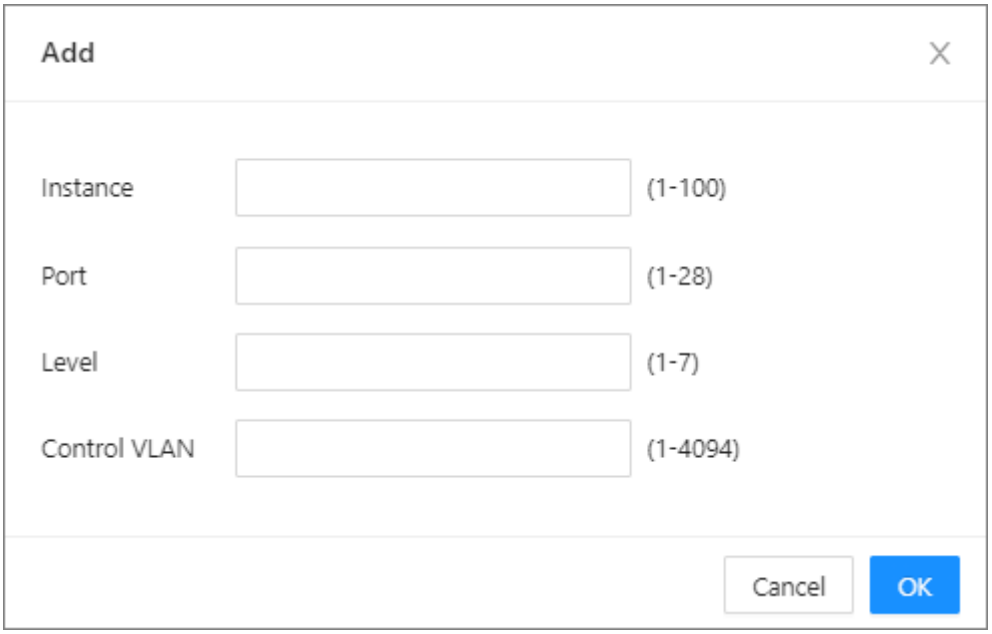


Table 5-5 MEP parameter description

Parameter	Description
Instance	The number of the MEP instance.
Port	The port number of MEP.
Level	Maintenance level. We recommend setting as 0.
Control VLAN	The ID of the control VLAN in a SEP segment.

5.8 Configuring IP and Routing

For details, see "3.4 Configuring IP and Routing".

5.9 Configuring ARP

Background Information

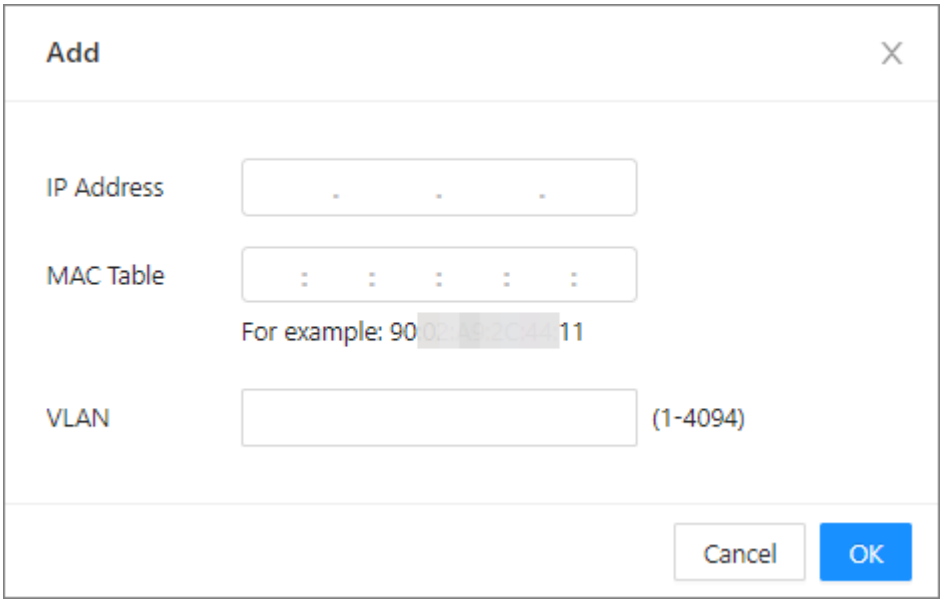
Address Resolution Protocol (ARP) is a protocol used to map IP addresses to MAC addresses. It is therefore necessary for hosts or Layer 3 network devices to maintain an ARP table for storing the mapping information of IP and MAC addresses. There are generally two types of ARP entries: static and dynamic.

Procedure

Step 1 Select **Network Settings** > **ARP**, you can view the IP address, the according MAC address, the type, and the VLAN.

Step 2 Click **Add** , enter the IP address, MAC table, and the VLAN, and then click **OK**.

Figure 5-6 IP and MAC



5.10 Configuring DHCP

Background Information

Dynamic Host Configuration Protocol (DHCP) is a network management protocol for dynamic and centralized IP address allocation and management. DHCP Server is the server for managing DHCP standard in the specific network. DHCP Server is to allocate IP address for the workstation and make sure that the IP address for every workstation is different. DHCP Server simplifies the network management task which should be done manually before.

Generally, in the following scenes, DHCP Server is adopted to allocate IP address.

- The network scale is large. The workload is too heavy if manually configured, and centralized management for network will be difficult.
- The quantity of PC is larger than the quantity of IP address in the network, and it is impossible to allocate a static IP address for every PC. For example, the user quantity that can access network at the same time is limited by ISP, and the user needs to acquire the IP address dynamically.
- Only a small number of PC need the static IP address, and most of the PC do not need the static IP address.

Procedure

Step 1 Select **Network Settings** > **DHCP**.

Step 2 Click to enable **Global Enable**.

Step 3 On **Address Pool** area, click **Add**, and then configure the parameters.

Figure 5-7 Address pool

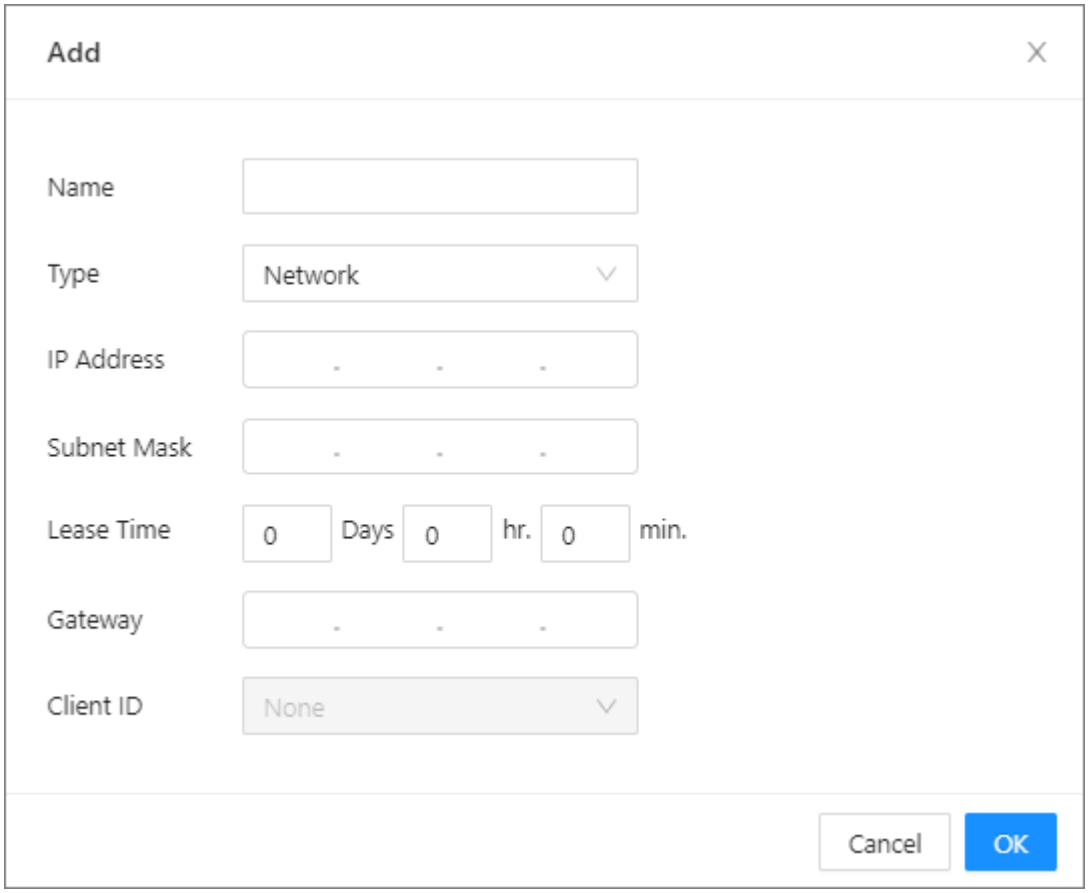


Table 5-6 Address pool description

Parameter	Description
Name	DHCP address pool name, such as “pool01”. Only numbers or letters can be entered, and the length of the string is limited to 1~32.
Type	Includes two types: **Network** and **Host**. • Network: The network segment of an IP • Host: A specific IP
IP Address	The IP address of the host or the network.
Subnet Mask	The subnet mask of the host or the network.
Lease Time	Enter the lease time of the address pool.
Gateway	Configure the default gateway of the address pool.
Client ID	Can not be changed by default.

Step 4 On **Reserved IP** area, click **Add**, and then enter the network segment of the reserved IP address.

Step 5 On **VLAN Mode** area, click **Add**, and then enter the VLAN range.

5.11 Configuring DHCP Relay

Background Information

The DHCP relay function enables message exchanges between a DHCP server and a client on different network segments. When DHCP clients and a server are on different network segments, the DHCP relay agent transparently transmits DHCP messages to the destination DHCP server. In this way, DHCP clients on different network segments can communicate with one DHCP server.

Procedure

Step 1 Select **Network Settings** > **DHCP Relay**.

Step 2 Click to enable **Relay Mode**.

Step 3 Enter **Server IP** , and then click **OK**.

5.12 Configuring LLDP

Background Information

LLDP (Link Layer Discovery Protocol) is a standard link layer discovery way. It can form its main capabilities, management address, device No. and port No. as TLV (Type Length Value), encapsulate it in LLDPDU (Link Layer Discovery Protocol Data Unit), and release it to its neighbor. The neighbor will keep the received information in the form of standard MIB (Management Information Base), so that the network management can query and judge the communication state of the link.

Procedure

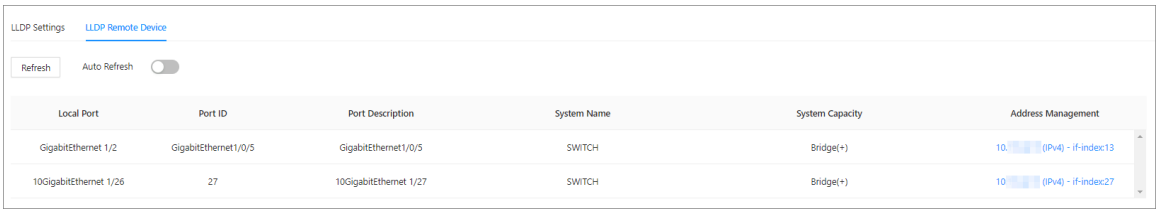
Step 1 Select **Network Settings** > **LLDP**.

Step 2 On the **LLDP Settings** tab, select the port, and then set LLDP mode.

- Enable: Both send and receive LLDP packet.
- Disable: Neither send nor receive LLDP packet.
- Rx only: Only receive LLDP packet.
- Tx only: Only send LLDP packet.

Step 3 On the **LLDP Remote Device** tab, view the information of LLDP remote device.

Figure 5-8 LLDP remote device



5.13 Configuring SNMP Protocol

SNMP (Simple Network Management Protocol) is the standard protocol for network management in Internet, and it is widely applied for accessing and managing the managed devices. SNMP has the following features:

- It supports intelligent management for network device. By using the network management platform based on SNMP, the network administrator can query the running status and the parameters of the network device, and can configure the parameter, find the error, perform fault diagnosis, and then plan the capacity and create the report.

- SNMP supports to manage the devices of different physical features. SNMP provides only the most basic function library. It makes the management task and the physical feature and the networking technology of the managed device independent, to manage the devices from different manufacturers.

SNMP network provides two elements, NMS and Agent.

- NMS (Network Management System) is the manager in SNMP network, and it provides friendly human-machine interface to help the network administrator to finish most of the network management work.
- Agent is the managed role in SNMP network, and it receives and handles the request packet from NMS. In some emergency circumstances, for example, if the port status changes, Agent can send alarm packet to NMS proactively.

5.13.1 Configuring SNMP V1 and V2

Background Information

SNMP is a standard network management protocol that is widely used on TCP/IP networks. It can be used in a network management system to monitor any exception on devices connected to the network.

SNMP comes in three versions: SNMPv1, SNMPv2c, and SNMPv3.

- SNMPv1: SNMPv1 is the initial version of SNMP, which provides a method for monitoring and managing computer networks. It provides authentication based on community names, has a low security level, and can return only a few error codes.
- SNMPv2c: Compared with SNMPv1, SNMPv2c has enhancements to standard error codes, data types, and operations including GetBulk and Inform.
- SNMPv3: Seeing that SNMPv2c was still poor in security, IETF released SNMPv3 that provides User Security Module (USM) authentication and encryption, and View-based Access Control Model (VACM). SNMPv3 is the most secure version so far.

Procedure

Step 1 Select **Network Settings** > **SNMP**.

Step 2 Select SNMP version.

- Select **V1**, and the switch can only process information on SNMP V1.
- Select **V2**, and the switch can only process information on SNMP V2.

When the server needs to access the switch, it needs to set the corresponding username, password and authentication type to complete the security verification, and the V1 and V2 versions are not available.

Step 3 Configure parameters, including **Read Community** , **Write Community**, **Trap Address**, and **Trap Port**.

Table 5-7 Description of SNMP parameters

Parameter	
Read community	The community name to access the network administrator. The permission is read. The default setup is public.

Parameter	
Write community	The community name to access the network administrator. The permission is write. The default setup is private.
Trap address	Specifies the server IP address.
Trap port	Set trap destination port.
Send keep-alive packet	Click the checkbox to enable this function.

Step 4 Click **OK**.

5.13.2 Configuring SNMP V3

Procedure

Step 1 Select **Network Settings** > **SNMP**.

Step 2 Select **V3**.

Step 3 Configure parameters.

Figure 5-9 SNMP V3

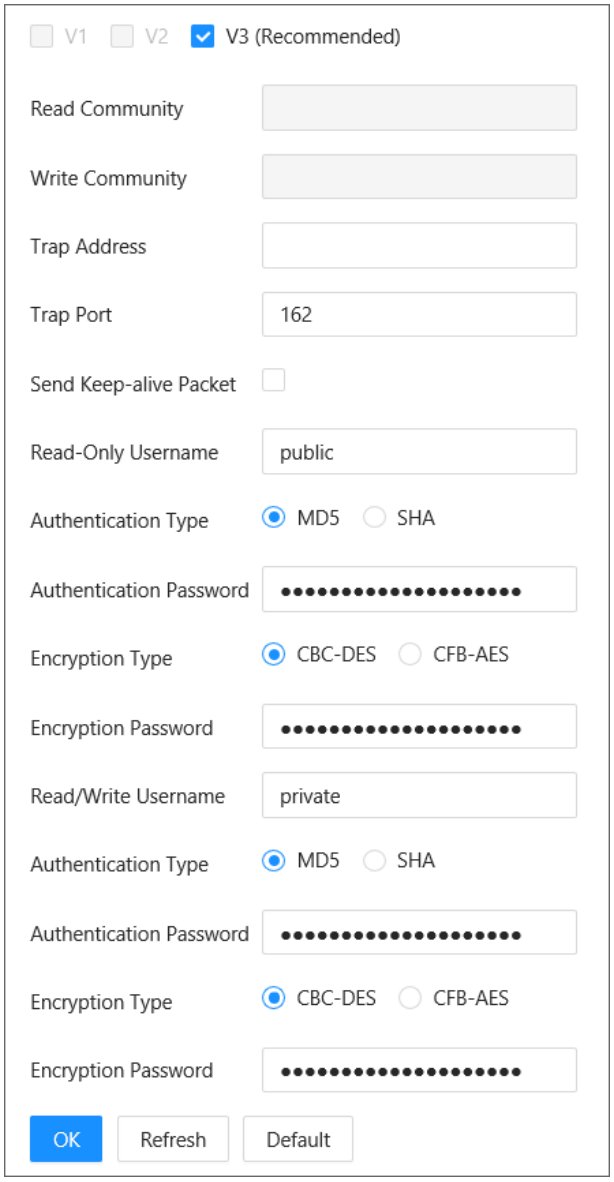


Table 5-8 Description of SNMP parameters

Read community	For description of thses parameters, see "Description of SNMP parameters".
Write community	
Trap address	
Trap port	
Send keep-alive packet	
Read-only username	Set the read-only username. It is for V3 only.
Authentication type	Set authentication mode when the security level is **Authentication no encryption** or **Authentication and encryption**. The authentication mode includes **MD5** and **SHA**.
Authentication password	Set authentication password.

Encryption type	Set encryption mode when the authentication mode is **Authentication and encryption**.
Encryption password	Set the encryption password when the authentication mode is **Authentication and encryption**.
Read/Write username	Set read and write user.

Step 4 Click **OK**.

5.14 Configuring MAC Table

MAC (Media Access Control) Table records the relationship between the MAC address and the port, and the information including the VLAN that the port belongs to. When the device is forwarding the packet, it queries in the MAC address table for the destination MAC address of the packet. If the destination MAC address of the packet is contained in the MAC address table, the packet is forwarded through the port in the table directly. And if the destination MAC address of the packet is not contained in the MAC address table, the device adopts broadcasting to forward the packet to all the ports except the receiving port in VLAN.

5.14.1 Adding MAC Table

Background Information

you can bind the MAC address to the port on certain VLAN.

Procedure

Step 1 Select **Network Settings** > **MAC Table**.

Step 2 On the **MAC Table** tab, click **Add**.

Step 3 Set the MAC address, VLAN, and Port.

For example, bind the MAC address 00:00:00:00:00:01 to the port 3 in VLAN 2.

Step 4 Click **OK**.

Figure 5-10 Add MAC table



5.14.2 Filtering Port MAC

Background Information

After enabling port MAC filtering, the following two MAC devices can communicate with the port.

- Devices in MAC allowlist.
- The static MAC devices changing from the dynamic MAC devices.

After enabling port MAC filtering, the port can not access the managing address or login.

Procedure

Step 1 Select **Network Settings** > **MAC Table**.

Step 2 On the **MAC Filtering** tab, select the port, and then click to enable the filtering function.

Step 3 Configure the MAC filtering of the port.

- Change from dynamic to static.
  1. Select one record, and then select next to **Reserved**.
  2. Click **OK**.

     The type changes from **Dynamic** to **Static**.

     Static MAC devices can communicate with the port normally.
- Create MAC allowlist.
  1. Click **Add**.
  2. Set MAC address and VLAN.
  3. Click **OK**.

6 Security

6.1 Configuring Account

You can add, edit, and delete the user account.

Procedure

Step 1 Select **Security** > **Account**, you can view the account list.

Step 2 (Optional) Click **Add** to add new users by entering username, password, confirming password, and then configuring permission level.

- You can click to edit the user's information, including changing password.
- admin 用户无法被删除。

Related Operations

- Edit user: Select a user account, click to edit the user information.
- Delete user: Select a user account, click to delete the user information.

  Admin user can not be deleted.
- Modify password: Click , click to enable **Modify Password**, and then modify the password.

6.2 Configuring Login Mode

Procedure

Step 1 Select **Security** > **Login Mode**.

Step 2 Click next to **SSH** to enable SSH function.

Step 3 Click next to **HTTPS** to enable HTTPS function.

6.3 Configuring RADIUS

Background Information

Remote Authentication Dial-In User Service (RADIUS) is a distributed information exchange protocol that uses a client/server model. It protects a network against unauthorized access and is often used on networks that require high security and allow remote user access.

Procedure

Step 1 Select **Security** > **RADIUS**.

Step 2 On the **NAS** tab, click next to **Mode** to enable the NAS function.

Step 3 Click next to **Re-authentication** to enable the Re-authentication function.

Authorization Method indludes 4 types of **Force-authorized**, **Force-unauthorized**, **Port-based 802.1x**, and **MAC-based Auth**.

- Force-authorized: The port is always in the authorized status, and users are allowed to access network resources without authentication.

- Force-unauthorized: The port is always in an unauthorized status, and users are not allowed to authenticate. The Switch does not provide authentication services for clients that access through this port.
- Port-based 802.1x: Indicates that the initial state of the port is an unauthorized state, and users are not allowed to access network resources. If the user is authenticated, the port is turned to an authorized state, which allows users to access network resources.

Step 4 On the **RADIUS** tab, click **Add** to add RADIUS.



You need to enable NAS before adding RADIUS.

Step 5 Configure the parameters, and then click **OK**.

7 Control Policy

7.1 Configuring ACL

Background Information

ACL (Access Control List) can be used by a device to deny and permit specific incoming and outgoing traffic. If no ACL is used, all traffic is transmitted freely, making the network vulnerable to attacks.

An ACL is essentially a rule-based packet filter. Packets matching an ACL are processed based on the policy defined in the ACL.

An ACL implements the following functions:

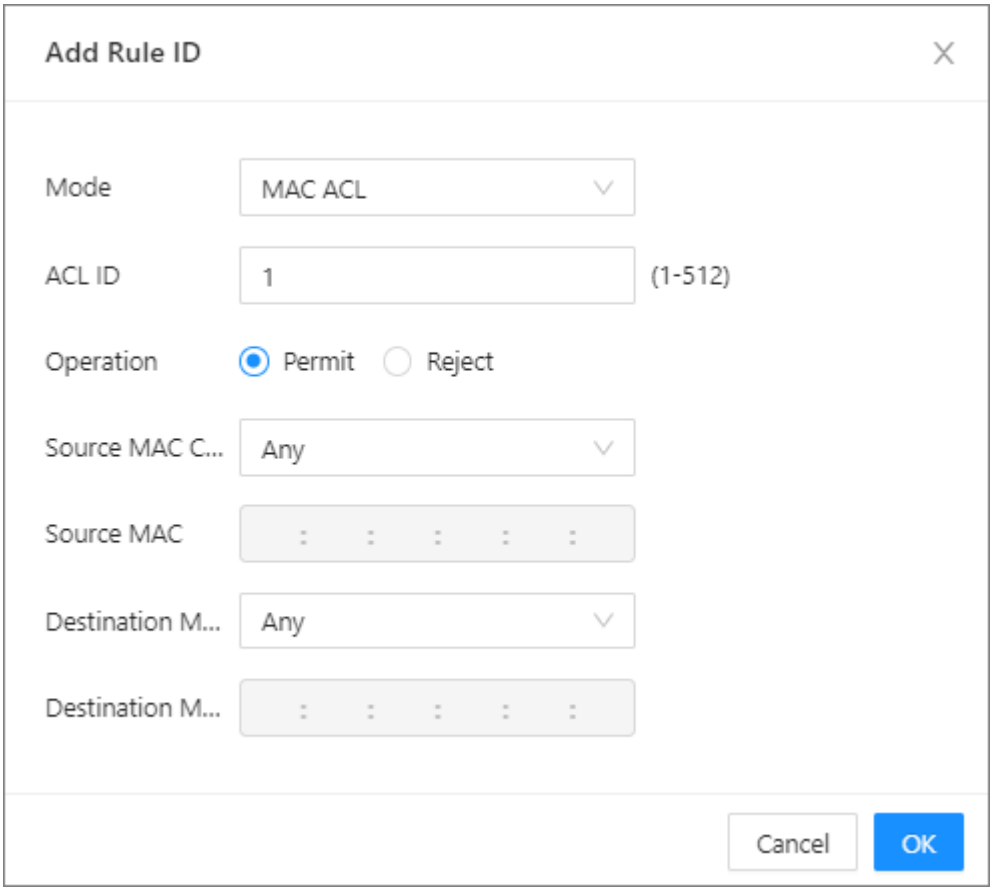
- Provides secure access. If an enterprise's important server resources can be accessed without permission, the enterprise's confidential information is prone to disclosure, causing security risks. You can use an ACL to specify the servers, networks, and services that users can access, preventing unauthorized access.
- Prevents network attacks. Internet viruses invade enterprise intranets, jeopardizing their security. An ACL can be used to block high-risk ports to block external traffic.
- Improves network bandwidth utilization. Network bandwidth is randomly occupied by various services, and the bandwidth of voice and video services that have the highest requirements on service quality cannot be guaranteed, resulting in poor user experience. An ACL can be used to accurately identify and control network traffic and restrict some network traffic to ensure the quality of major services.

Procedure

Step 1 Select **Control Policy** > **ACL**.

Step 2 On the **ACL** tab, click **Add**, and then configure the parameters.

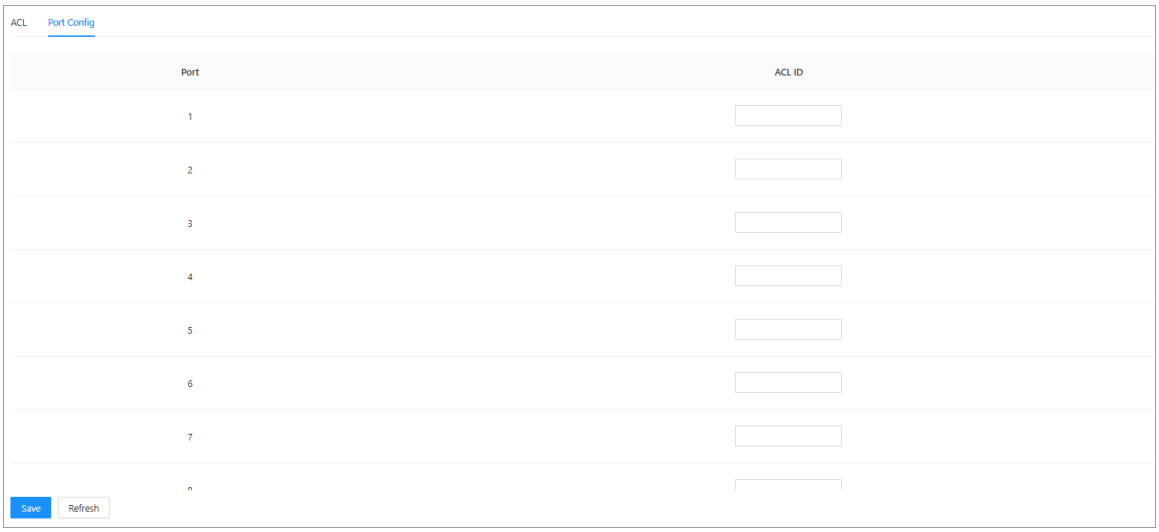
Figure 7-1 ACL parameter



Step 3 On the **Port Config** tab, enter the **ACL ID** of the port.

The ACL ID must be configured in the ACL settings.

Figure 7-2 Port configuration of ACL



7.2 Configuring QoS Settings

Background Information

QoS(Quality of Service) improves network resource utilization and allows different types of traffic to compete for network resources based on their priorities, so that important data applications are preferentially processed on network devices.

Procedure

Step 1 Select **Control Policy** > **Settings**.

Step 2 On the **Priority Mode** tab, select **Priority Mode**, and then click **OK**.

Priority Mode includes **First In, First Out**, **Weighted Round Robin**, and **Strict Priority**.

Step 3 On the **Trust Mode** tab, set **Port Priority**, and then select to enable **Based on 802.1p**, **Based on DSCP** or **TCP/UDP Port**.

Step 4 On the **TCP/UDP Port** tab, select **Options** for different protocols.

Step 5 On the **DSCP Priority** tab, select **Priority for Unmatched DSCP** for different protocols, select port number and priority.

Appendix 1 Cybersecurity Recommendations

Mandatory actions to be taken for basic device network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters.
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols.
   - Do not contain the account name or the account name in reverse order.
   - Do not use continuous characters, such as 123, abc, etc.
   - Do not use overlapped characters, such as 111, aaa, etc.

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

   If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

    Due to the limited storage capacity of the device, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.