Ethernet Switch (Cloud Managed Switch)

User's Manual

V1.0.0

Foreword

This manual introduces the functions and operations of the Ethernet switch (hereinafter referred to as the "device"). Please read carefully before using the product. After reading, please save the document properly for future reference.

Safety Instructions

The following signal words 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, reductions in performance, or unpredictable results.
ESD	Electrostatic Sensitive Devices. Indicates a device that is sensitive to electrostatic discharge.
⚡ ELECTRIC SHOCK	Indicates dangerous high voltage. Take care to avoid coming into contact with electricity.
☀ LASER RADIATION	Indicates a laser radiation hazard. Take care to avoid exposure to a laser beam.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	June 2024

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

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.

Table of Contents

1 Cloud Management

The device can be managed through the DoLynk Care app and DoLynk Care platform without the need for initialization after it is powered on.

1.1 Managed by DoLynk Care App

Procedure

Step 1　Search for DoLynk Care in App store, and then download the app.

📖

For Android users, you can go to Google Play to download DoLynk Care.
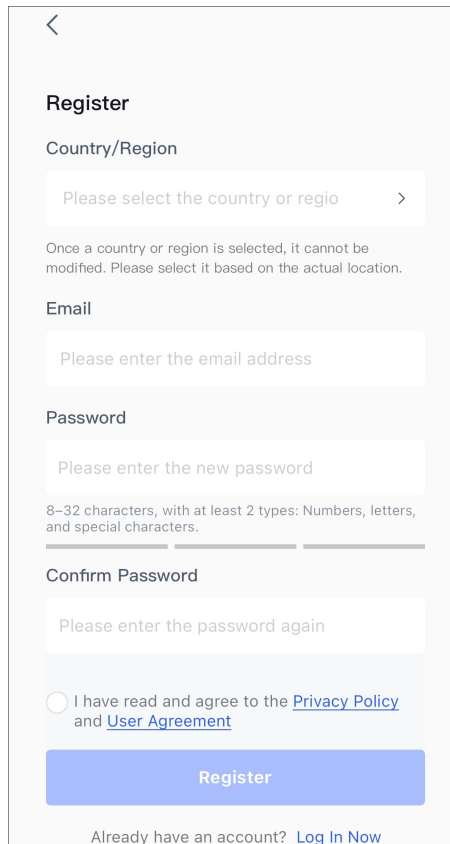
Step 2　On your phone, tap 📱 to start the app. Create an account.

1. On the **Login** screen, tap **Create Account**.
2. On the **Register** screen, fill in the information for the required fields.

　📖

　Some countries or regions support registering an account using the phone number. Please refer to the actual interface for details.

Figure 1-1 Register

3. Read the **Privacy Policy** and **User Agreement**, and then select the **I have read and agree to Privacy Policy and User Agreement** checkbox.
4. Tap **Register** , and then the app returns to the **Login** screen.

Step 3   Enter your email address and password, and then tap **Log in**.

$\square$

- Some countries or regions support using the phone number to log in. Please refer to the actual interface for details.
- You can log in with the account that you have registered in Partner App or DoLynk Dashboard. Tap ⓘ to view the instructions.
- If you log in using your personal account from Partner App and you did not select the country or area when you register the account, you need to select a country when you log in for the first time.
- If you log in using the company account from Partner App, you need to select a role, administrator or employee to log in for the first time. If the selected role is an employee, you must first contact the administrator to create an employee account.

Step 4   Tap 🔧 on the upper-left corner of the page, and then tap the account profile.

Step 5   Tap **Sites**, and then tap ⊕ to add a site.

- **Customer Name** and **Customer Email**: Enter name and email of the end user.

$\square$

Enter the email address of the account that your customer has registered on DMSS app. DoLynk Care will verify it.

- **Country/Region** : The country or area is kept same as the country or region of the account by default.
- **Assign operator**: Select an operator to whom you want to assign this site.

$\square$

Before assigning an operator on the DoLynk Care app, you need to create and manage operator accounts on DoLynk Care portal. For details, see *DoLynk Care User's Manual*.

Figure 1-2 Add a site

Step 6   Add devices by scanning the QR code of the device or manually entering device SN.

1. On the home screen, tap ⊕. Tap **QR**.

Figure 1-3 Add a device
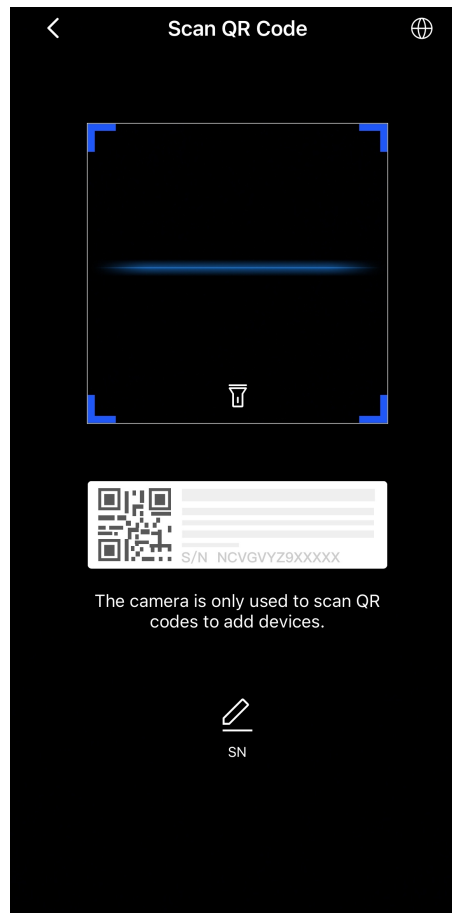
2. Scan device QR code, or tap ✎ to manually enter device SN.

   When adding a device through the SN, you need to enter the SN and password. The default password before device initialization is the SC code, which can be obtained from the labeling on the device.

3. Select a site, and then tap **OK**.
4. On the **Add Device** screen, select a device type.
5. If the device you are adding is uninitialized, enter password and confirm it again, and then tap **Initialize the device** to complete initialization.

   If the device you are adding is initialized, enter the password and then click **OK**.

Figure 1-4 Initialize the device
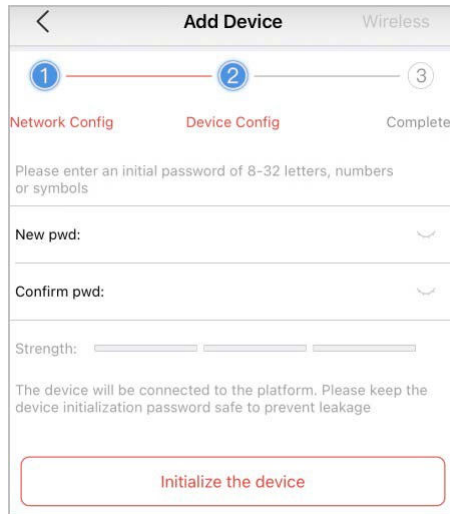
6. Tap **Completed**, and then you can view the device in the device list.

On the console page, tap the company profile to go to the account management page.

Tap ❯ beside **Help and Feedback** to view the document on the app, including user's manual, FAQ, and more.

1.2 Managed by DoLynk Care Platform

Procedure

<u>Step 1</u>   Create an account.

For the first time to log in to DoLynk Care, you must create an account first. The sign up methods include personal account registration and GSP invitation registration.

● Personal account registration

You can sign up through registration portal of the platform login page. The registered account is a personal account. If you need to use features such as entrusting devices and purchasing service packages, you need to authenticate your company after logging in.

1. Enter the platform address in the browser, and then press Enter. Select the language on the upper-right corner of the page.
2. Click **Create Account** to create an account.
3. Select the country or region, enter the email address and password, and then click **Send** to obtain the verification code.
4. Enter the verification code that was sent to the registered email, and then read and select **I have read and agree to Privacy Policy and Terms and Conditions** . Click **Sign up**.

📖

Some countries or regions support registering an account with the phone number to obtain the verification code. Please refer to the actual interface for details.

Figure 1-5 Personal account registration
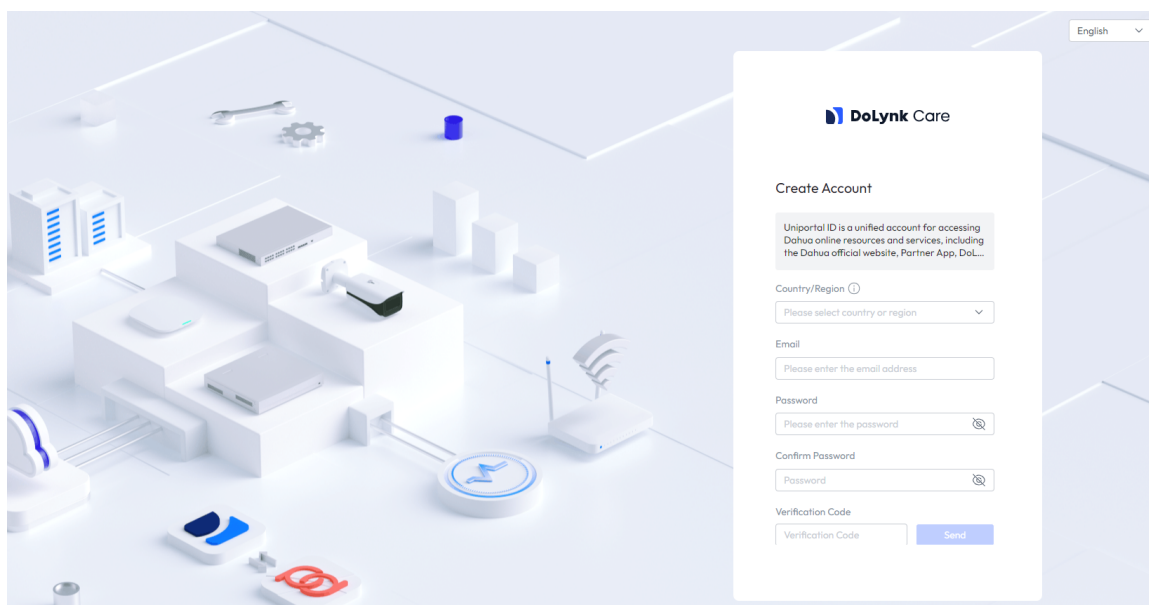
- GSP Invitation Registration: For details, see DoLynk Care User's Manual.

Step 2   Open the browser, enter the web address, and then press the Enter key. Enter email and password, and then click **Log in**.

- Some countries or regions support using the phone number to log in. Please refer to the actual interface for details.
- If you log in using your personal account from Partner app and you did not select the country or area when you registered the account, you need to select a country when you log in for the first time.
- If you log in using the company account from Partner app, you need to select a role, administrator or employee to log in for the first time. If the selected role is an employee, you must first contact the administrator to create an employee account.

Step 3   Add a site.

1. Click **Sites** on the console page.
2. Click **Add** on the site management page, and then configure the parameters.
3. Click **OK**.

Step 4   Add devices.

1. Click **Devices** on the console page.
2. Click **Add**.
3. Enter device Name, device SN and device Password.

   You must select a site for the device. You can select an existing site from the list, or create a new site.

   - When adding a device through the SN, you need to enter the SN and password. The default password before device initialization is the SC code, which can be obtained from the labeling on the device.
   - You cannot add the device which has been bound to a customer.
   - If you add a switch, you can change the device password following the on-screen instructions.

4. Click **OK**.

Click on the upper-right corner to go to **Help** page, view the document on the platform, including user's manual, FAQ, and more.

2 Initialization and Login

The Cloud Managed Switch provides WEB access functionality. You can log in to the web interface to manage and configure the device.

2.1 Initializing the Device

Prerequisites

- Make sure that the device is connected to the power supply.
- Make sure that the device is connected to the computer, and the IP addresses of the computer and the device are on the same segment.
- By default, DHCP is enabled on the device. When connected to a network, the device typically obtains an IP address from a DHCP server, and then you can obtain the IP address of the device from the upstream device, such as a router. If a DHCP server is not available, the IP address of the device is 192.168.1.110 by default.

☷

You can use the Configtool to obtain the IP address on select models of devices.

Procedure

Step 1   Enter the IP address of the device in the address bar of the web browser, and then press the Enter key.

Step 2   Select the language and then click **Next**.

Step 3   Read the legal statement, select **I have read and agree to the terms of the Software License Agreement and Privacy Policy** , and then click **Next**.

Step 4   Configure the password.

☷

- The default username is admin.
- Configure 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 visible characters other than' " ; : &).

Figure 2-1 Configure password

Step 5   Click **Complete**.

2.2 Login the Device

Prerequisites

- The device has been initialized.

- Make sure that the device is connected to the computer, and the IP addresses of the computer and the device are on the same network segment.

Procedure

Step 1   Enter the IP address of the device in the address bar of the web browser, and then press the Enter key.

Step 2   Enter the password.

Step 3   Click **Login**.

2.3 Home Page

After login, the system will be directed to the **Home** page.

The left side of the page consists of a menu bar. At the top, there is a graphical display of the port status. In the upper-right corner, supports hiding or showing the port information, logging out, restarting the device, switching the system languages, and scanning QR codes to access information.

The webpage are for reference only, and might differ from your device.

Figure 2-2 Home page

Port Information

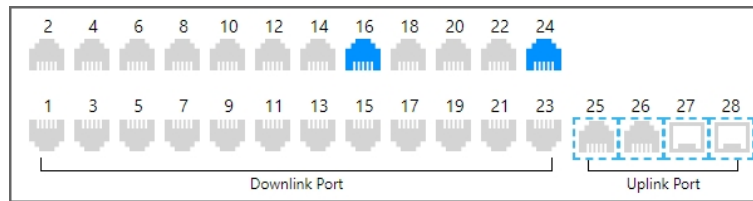- Blue port: The port connected to device.
- Grey port: The port not connected to device.
- Hover over a port to view its connection information, including port status, link status, and power consumption.
- Click a port, and then go to the **Port** page.

Figure 2-3 Port information

Home Page

Home page supports the following functions.

- **Device Info** : Configure the device name, management VLAN, and cloud management.

  ⚠️

  ◇ Cloud management is enabled by default, if you disable this feature, the device cannot be managed through the DoLynk Care app. For details to using cloud management, see "1 Cloud Management".
  ◇ After enabling management VLAN, you can only access the web page of the device through a management VLAN IP address.

- **Port Info** : Displays the link status, flow control status, and VLAN mode of each port.

Table 2-1 Description of port information

Parameter	Description	
Port	Displays all ports of the device.	
Port description	Configure the port description, you can also go to **Switch Config** > **Port** to configure.	
Link Status	- Displays the port rate and the duplex mode: The port is connected. - DOWN: The port is not connected or the connection fails.	
Flow Control Status	View the status of the flow control function, including **On** and **Off**. You can go to **Switch Config** > **Port** to configure.	
VLAN Mode	Includes **Access** and **Trunk**.	
PVID	The VLAN of the port.	Go to **Switch Config** > **VLAN** to configure.
Tagged VLAN	The VLAN ID for the port that is allowed to be tagged when sending packets.	
Untagged VLAN	The VLAN ID for the port that is allowed to be untagged when sending packets.	
TX/RX Rate	The current reception rate or sending rate divided by the actual negotiated rate for a period of time(usually 5 minutes).	
Media Type	Includes two types: **COPPER** and **FIBER**. **COPPER**: RJ-45 port. **FIBER**: Fiber port.	

3 Switch Configuration

3.1 Configuring Port 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.

Procedure

Step 1   Select **Switch Config** > **Port**.

Step 2   Select the port number, configure the parameters, and then click **Save**.

- **Speed/Duplexing** : Configure the speed and the duplex mode. The speed/duplexing is set as **Auto** for combo port.
- **Flow Control** : Enable the flow control function can effectively relieve network congestion, reduce data loss, and improve network stability and data reliability.
- **EEE Config** : Enable the EEE (Energy-Efficient Ethernet) function can reduce power consumption when the network is idle and achieve energy saving effect.

Figure 3-1 Port config (1)

Step 3   In the **Port Description** box, enter the description of the port.

The description cannot exceed 16 characters. Only numbers, letters and the special character (_).

Figure 3-2 Port config (2)

Table 3-1 Description of the port parameters

Parameter	Description
Media Type	Includes two types: **COPPER** and **FIBER**. • **COPPER**: RJ-45 port. • **FIBER**: Fiber port.
Speed/Duplexing Config	The parameters configured for this port are displayed.

Parameter	Description
Speed/Duplexing Status	• Online: Displays the port rate and the duplex mode. • Offline: Displays **DOWN**.
Flow Control	Displays whether the flow control function is enabled and the current flow control status.
Flow Control Status	
EEE Config	Displays whether the EEE function is enabled.

3.2 Configuring VLAN

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

Background Information

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.

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

- **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.

Procedure

Step 1   Select **Switch Config** > **VLAN** > **Add VLAN**.

Step 2   Enter the VLAN ID and description, and then click **Save**.

📖

Select the VLAN and then click **Delete** to delete the VLAN. VLAN1 cannot be deleted.

Figure 3-3 Add VLAN

Step 3   Click the **VLAN** tab to configure the port VLAN parameters.

1. Select one or more ports.

2. Select the VLAN mode, including **Access** and **Trunk**.

Figure 3-4 VLAN

Port	Mode	PVID	Tagged VLAN(s)	Untagged VLAN(s)
Port1,Port2	Trunk	VLAN1	VLAN2,VLAN3	

Save

Port	Mode	PVID	Tagged VLAN	Untagged VLAN
Port1	Access	1	-	1
Port2	Access	1	-	1
Port3	Access	1	-	1
Port4	Access	1	-	1
Port5	Access	1	-	1
Port6	Access	1	-	1

3. Configure PVID, tagged VLAN, and untagged VLAN.

- When the mode is Access, you should configure the untagged VLAN. Untagged VLAN indicates the VLAN ID for the port that is allowed to be untagged when sending packets.
- When the mode is Trunk, you should configure PVID and tagged VLAN.

PVID indicates that the port is added to a VLAN. By default, the port belongs to VLAN 1. The VLAN ID for the port that is allowed to be tagged when sending packets.

Table 3-2 Frame processing comparison

Port type	Untagged frame processing	Tagged frame processing	Frame transmission
Access	Receives an untagged frame and adds a tag with the default VLAN ID to the frame.	• Accepts the tagged frame if the frame's VLAN ID matches the default VLAN ID. • Discards the tagged frame if the frame's VLAN ID differs from the default VLAN ID.	After the PVID tag is removed, the frame is transmitted.

Port type	Untagged frame processing	Tagged frame processing	Frame transmission
Trunk	- Adds a tag with the default VLAN ID to an untagged frame and accepts the frame if the interface permits the default VLAN ID. - Adds a tag with the default VLAN ID to an untagged frame and discards the frame if the interface denies the default VLAN ID.	- Accepts a tagged frame if the VLAN ID carried in the frame is permitted by the interface. - Discards a tagged frame if the VLAN ID carried in the frame is denied by the interface.	- If the frame's VLAN ID matches the default VLAN ID and the VLAN ID is permitted by the interface, the device removes the tag and transmits the frame. - If the frame's VLAN ID differs from the default VLAN ID, but the VLAN ID is still permitted by the interface, the device will directly transmit the frame.

4. Click **Save**.

3.3 PoE Management

PoE refers to that the device uses network cables to externally connect PD (Powered Device) for remote power supply through Ethernet electrical ports. PoE function enables centralized power supply and convenient backup. Network terminals do not need external power supply, but only one network cable.

Non-PoE switches do not support this function.

3.3.1 Global Configuration

You can configure perpetual PoE, available power, and alert power.

Procedure

Step 1   Select **Switch Config** > **PoE** > **Global Config**.

Step 2   Select **Perpetual PoE** , and then click **Save**.

Enable perpetual PoE, which allows the powered devices to continue receiving power even after the device is restarted.

Step 3   Configure available power and alert power.

The total power, available power, alert power, power consumption, reserved power, remaining power and perpetual PoE are displayed at the bottom of the page. The reserved power = Total power – Alert power.

- The alert power must be greater than the available power.
- Available power refers to the maximum power that can be provided to powered devices. When the power consumption is less than available power, new powered devices are allowed to be powered on.

- During operation, the actual power usage might fluctuate. When the power consumption exceeds the alert power, the ports will be powered from low to high according to the priority (the larger the port number, the lower the priority), until the power consumption is less than the alert power.

Figure 3-5 Global config

Step 4   Click **Save**.

3.3.2 Port Configuration

Configure the PoE function of the port.

Procedure

Step 1   Select **Switch Config** > **PoE** > **Port Config**.

Step 2   Select the port number, enable the PoE, long distance PoE, PoE watchdog, and force PoE as needed.

- **PoE** : The device uses network cables to externally connect PD for remote power supply through Ethernet electrical ports.
- **Long Distance PoE** : After you enable long distance PoE, the maximum transmission distance will change from 100 m to 250 m, and the transmission speed will be reduced to 10 Mbps.

The actual transmission distance might vary due to power consumption of connected devices or the cable type and status.

- **PoE Watchdog** : With PoE watchdog enabled, you can monitor PD and keep it online, and check the status of PD devices based on the time intervals. If there is no data transmission, the PoE port will be automatically powered off and restarted.

The time intervals for PD devices status checks progressively increase, starting from 1 minute and doubling each time (1, 2, 4, 8, 16, and more). The maximum time intervals is 1024 minutes.

- **Force PoE** : When the powered device connected to the port is a non-standard device, use this function to force PoE power supply.

⚠️

After force PoE is enabled, the port will force power supply to the powered device, whether or not the device connected to the port meets the requirements. Please be advised.

📖

Force PoE and **PoE watchdog** cannot be enabled at the same time.

Figure 3-6 Port config

Step 3   Click **Save**.

Table 3-3 Description of PoE parameters

Parameter	Description
Level	Displays the power supply level of the terminal devices. The power supply level ranges from 0 through 8, and the Hi-PoE power supply standard level is displayed as 5+.
Power Consumption(W)	Displays the current PoE power consumed by the corresponding single port.
PoE Enable	Displays whether PoE is enabled for the port.
Long Distance PoE	
PoE Watchdog	
Force PoE	

4 Security

4.1 Configuring Port Isolation

Port isolation is to achieve layer 2 isolation between messages. The port isolation function provides users a safer and more flexible networking solution.

Procedure

Step 1   Select **Security** > **Port Isolation**.

Step 2   Enable port separation.

📖

> After port isolation is enabled, downlink ports will be isolated and uplink ports will not be isolated. (Data can only be transferred between uplink and downlink ports.).

Step 3   Click **Save**.

4.2 Configuring Storm Control

The broadcast frames on the network are forwarded continuously, which affects the proper communications, and greatly reduces the network performance. The storm control can limit the broadcast flows of the port and discard the broadcast frames once the flow exceeds the specified threshold, which can reduce the risk of the broadcast storm and ensure the network proper operation.

Procedure

Step 1   Select **Security** > **Storm Control**.

Step 2   Select the type and port, enable storm control, and then enter the speed.

Figure 4-1 Storm control

Step 3   Click **Save**.

4.3 Configuring Port Speed Limit

Configure the rate limiting policy of ports to control the flow of data packets entering and exiting the port at a desired rate.

Procedure

Step 1   Select **Security** > **Port Speed Limit**.

Step 2   Select port and direction, enable port speed limit, and then enter the speed.

The direction includes out and in.

Figure 4-2 Port speed limit

Port	Direction	Enable	Speed Limit (Mbit/sec)
Port 1,Port 2	In ⌄	On ⌄	100 (1~1000)M

Save

Port	Port Type	Input Port Speed (Mbit/sec)	Output Port Speed (Mbit/sec)

Step 3   Click **Save**.

5 Network Settings

5.1 Configure MAC Tables

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.

Procedure

Step 1   Select **Network Settings** > **MAC Management** > **Static MAC**, view the MAC table information.

Step 2   Configure the MAC address, VLAN ID and port, and then click **Add**.

📖

- You can only configure up to 16 static MACs.
- Select a MAC and then click **Delete**, you can delete the static MAC.

Figure 5-1 Static MAC

Step 3   Click the **MAC Search** tab, enter the MAC address or select the port, and then click **Search** to quickly search the MAC address.

Figure 5-2 MAC search

Step 4   Click the **MAC List** tab, and then view MAC addresses.

Up to 100 items can be displayed. To search more information, go to **MAC Search**.

📖

Click **Clear** , and then click **OK** to clear the information.

5.2 Configuring Loop Protection

Select **Network Settings** > **Loop Protection**, enable loop protection, and then click **Save**. After loop protection is enabled, if a loop is detected, the port which caused the loop will be disabled and then automatically restored after the loop is eliminated.

5.3 Configuring STP

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.

The STP is only available on select models.

5.3.1 STP

Procedure

Step 1   Select **Network Settings** > **STP** > **STP**.
Step 2   Enable the STP.
Step 3   Select the working mode, including STP and RSTP.
Step 4   Configure the parameters.

Figure 5-3 STP config

Working Mode	Hello Timer	Max. Aging Time	Forwarding Delay Time	Bridge Priority
STP	2 (1~10)s	20 (6~40)s	15 (4~30)s	32768 (0~61440)s

Working Mode	Hello Timer	Max. Aging Time	Forwarding Delay Time	Bridge Priority
STP	0	0	0	0

Table 5-1 Description of the STP parameters

Parameter	Description
Hello Timer	The period of root bridge sending BPDU. The time ranges from 1 second to 10 seconds.
Max. Aging Time	The aging time of current BPDU. The time ranges from 6 seconds to 40 seconds.
Forwarding Delay Time	After setting topological change, the bridge maintains the time of snooping and study state. The time ranges from 4 seconds to 30 seconds.
Bridge Priority	The value ranges from 0 to 61440.

Step 5　Click **Save**.

5.3.2 Port Instance

Select **Network Settings** > **STP** > **Port Instance**, select the port, enter the priority and root path cost, and then click **Save**.

The value of **Priority** ranges from 0 to 240, and must be an integral multiple of 16.
The value of **Priority** is 128 by default.

Figure 5-4 Port instance

Port	Role	Status	Priority	Root Path Cost	Designated Bridge ID	Designated Port ID
Port 1	Disabled Port	Discard	128	0	-	-
Port 2	Disabled Port	Discard	128	0	-	-
Port 3	Disabled Port	Discard	128	0	-	-
Port 4	Disabled Port	Discard	128	0	-	-
Port 5	Disabled Port	Discard	128	0	-	-
Port 6	Disabled Port	Discard	128	0	-	-
Port 7	Disabled Port	Discard	128	0	-	-
Port 8	Disabled Port	Discard	128	0	-	-

5.4 Configuring Link Aggregation

Link aggregation is to form 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.

Background Information

In order to successfully establish a link aggregation, the link aggregation settings on the peer device need to be the same as the settings on this device.

Procedure

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

Step 2   In the **Load Balancing** area, select the type and then click **Save**.

The type includes **Source MAC Config** , **Destination MAC Config**, **Source IP Config**, **Destination IP Config**, **TCP/UDP Source Port** and **TCP/UDP Destination Port**.

Figure 5-5 Link aggregation

Step 3   Select the **Aggregation Group No.** and port number.

The aggregation group mode is **Static** by default.

⚠

Ports with storm control or port speed limit enabled cannot be added to aggregation groups.

Step 4   Click **Add**.

Select the aggregation group and then click **Delete** to delete the aggregation group.

6 Smart Monitoring

6.1 Viewing Port Statistics

Procedure

Step 1   Select **Smart Monitoring** > **Port Statistics**.

Step 2   View the port type, receiving usage, and sending usage.

Click **Reset** to reset the port statistics.

Figure 6-1 Port statistics

Port	Port Type	RX Usage	TX Usage	RX/TX Bytes	Successful RX/TX Packet	Failed RX/TX Packet
Port 1	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0
Port 2	Physical Port	0.05%	0.05%	201.94MB/4.23MB	2938753/40057	0/0
Port 3	Physical Port	0%	0%	163.29KB/103.64KB	1325/450	0/0
Port 4	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0
Port 5	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0
Port 6	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0

Reset

6.2 Viewing Device List

LLDP (Link Layer Discovery Protocol) is a standard link layer discovery way. It can form its main capabilities, management address, device number and port number 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 Monitoring** > **Device List**.

Step 2   Enable the LLDP, and then Click **Save**.

Step 3   View the information of LLDP remote device.

Figure 6-2 Device list

If LLDP is turned off, cloud topology of the device will work abnormally.

LLDP ☑

Save

Port	Peer Port Name	Device Name	MAC Address	IP
Port 2				
Port 2				
Port 2				

7 Maintenance

7.1 Configuring Port Mirroring

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** > **Port Mirroring**.

Step 2   Select the source port, direction, and destination port.

Directions include Tx Only, Rx Only, and Both.

- **Tx Only** : Only supports sending traffic.
- **Rx Only** : Only supports receiving traffic.
- **Both** : Supports both sending and receiving.

Figure 7-1 Port mirroring

Step 3   Click **Save**.

7.2 Configuring Firmware

7.2.1 Restore Factory Default

Procedure

Step 1   Select **Maintenance** > **Firmware Config**.

Step 2   Click **Default** , enter the password, and then click **OK**.

⚠️

- All parameters restore to default settings except the IP address, subnet mask, gateway, and DNS.
- Yon can restore all parameters though the reset button.

7.2.2 Update Software

Procedure

Step 1   Select **Maintenance** > **Firmware Config**.

Step 2   Click **Browse** to import the update file, and then click **Update**.

Step 3   Click **OK**.

It might take 3 minutes to update the software. After the update, the system will automatically restart.

7.2.3 Restart Device

Select **Maintenance** > **Firmware Config**, click **Restart** , and then click **OK**.

You can also use the upper-right corner ⟳ to restart the device.

7.3 Changing Password

Procedure

Step 1   Select **Maintenance** > **Change Password**.

Step 2   Enter the old password, new password, and confirm password.

The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).

Figure 7-2 Change password

Step 3   Click **Save**.

7.4 Configuring Network

Configure the IP address and DNS server.

Procedure

Step 1   Select **Maintenance** > **Network**.

Step 2   Configure the parameters.

- Enable DHCP: After enabling DHCP, new IP will be automatically acquired and assigned.
- Disable DHCP: Enter the IP address, subnet mask, and gateway to configure a static IP address.
- Enable Auto Obtain DNS: The device automatically obtains the IP address of the DNS server in the network.
- Disable Auto Obtain DNS: Enter the IP addresses of the DNS1 and DNS2.

Figure 7-3 Network

DHCP	IP Address	Subnet Mask	Gateway	Auto Obtain DNS	DNS1	DNS2
Off ▾		255.255.252.0		Off ▾	8.8.8.8	8.8.4.4
Save						

Step 3   Click **Save**.

7.5 Viewing Device Information

Select **Maintenance** > **Device Info**, you can view the information such as the device name, software version, MAC address, and running time. You can also enable cloud management through this page.

7.6 Viewing Log Information

Select **Maintenance** > **Log Info**, view the log information.

7.7 Viewing Legal Information

Select **Maintenance** > **Legal Statement**, click the corresponding tab to view the software license agreement, privacy policy, and open source software notice.

Appendix 1 Security Recommendation

Account Management

1. **Use complex 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: 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 repeating characters, such as 111, aaa, etc.

2. **Change passwords periodically**

   It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

3. **Allocate accounts and permissions appropriately**

   Appropriately add users based on service and management requirements and assign minimum permission sets to users.

4. **Enable account lockout function**

   The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

5. **Set and update password reset information in a timely manner**

   The device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. **Enable HTTPS**

   It is recommended that you enable HTTPS to access web services through secure channels.

2. **Encrypted transmission of audio and video**

   If your audio and video data contents are very important or sensitive, it is recommended to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.

3. **Turn off non-essential services and use safe mode**

   If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

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

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

4. **Change HTTP and other default service ports**

   It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allow list**

   It is recommended that you turn on the allow list function, and only allow IP in the allow list to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allow list.

2. **MAC address binding**

   It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.

3. **Build a secure network environment**

   In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

   - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
   - According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
   - Stablish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

   It is recommended to check online users regularly to identify illegal users.

2. **Check device log**

   By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.

3. **Configure network log**

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

Software Security

1. **Update firmware in time**

   According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.

2. **Update client software in time**

   It is recommended to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control

and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).