



Ethernet Switch (Cloud Managed Switch)

User Manual



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.

Symbols

The following symbols might appear in the manual.

Symbol	Description
 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.
 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
V1.0.2	- Added VIP port. - Added STP. - Added system time. - Added alarm center.	July 2026
V1.0.1	- Updated initialization and login, switch configuration, network settings, security and system. - Added cable test.	February 2026
V1.0.0	First release.	August 2024

Privacy Protection Notice

As the device user, you might collect the personal data of individuals such as their names, email addresses, face images, audio and fingerprints. You shall be fully responsible for any activities associated with processing personal data. You commit to comply with your local privacy protection laws and regulations to protect the legitimate rights and interests of individuals, and shall implement measures which are required by applicable law, including but not limited to, providing clear and comprehensive information to individuals before processing their personal data, obtaining consent from individuals when necessary, informing individuals of the existence of the surveillance area, and providing required contact information.

Intelligent Product Usage Statement

Intelligent products utilize AI technology to effectively enhance security. The intelligent recognition and alarm functions of the product might be affected by factors such as environmental lighting, camera angles, object obstructions, and network delays, potentially leading to false alarms, missed alerts, or response delays. This intelligent product is solely intended to be used as a security assistance tool. The results from performing identification are for reference only and do not constitute absolute guarantee of personal or property safety. Users need to combine these products with necessary physical security measures to enhance overall protection. Except as otherwise provided by laws or in the event of intentional or gross negligence on the part of the company, the company shall not be liable for any losses caused by the aforementioned factors not attributable to the company.

About the Manual

- This manual is provided for general reference only. Discrepancies might exist between the product and this manual, including but not limited to printed, electronic, or any other editions.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. Specifications and documentation are subject to change without prior notice. For the latest versions, as well as legal notices, consult the printed manual, the product webpage, our official website, or scan the QR code to access the electronic edition.
- The manual will be updated as necessary to reflect product changes and applicable legal requirements. These updates will not diminish your statutory rights, nor will they remove or weaken the safety information or essential instructions provided at the time of purchase.
- Although we make every effort to ensure accuracy, errors or deviations in descriptions of functions, operations, or technical data might occur. If there is any uncertainty or controversy, we reserve the right of final explanation.
- All trademarks, registered trademarks and company names referenced in this manual are the property of their respective owners.

Table of Contents

Foreword.....	I
1 Initialization and Login.....	1
1.1 Initializing the Device.....	1
1.2 Logging in to the Device.....	1
1.3 Home Page.....	2
2 Port Management.....	5
2.1 Port.....	5
2.2 PoE.....	6
2.2.1 Global Configuration.....	6
2.2.2 Port Configuration.....	7
2.3 VIP Port.....	9
2.4 Port Statistics.....	9
2.5 Link Aggregation.....	10
2.6 Cable Detection.....	11
2.7 Port Mirroring.....	12
3 Network Settings.....	13
3.1 VLAN.....	13
3.2 Neighbor List.....	15
3.3 MAC Management.....	15
3.4 Loop Protection.....	16
3.5 STP.....	17
3.5.1 STP Configuration.....	17
3.5.2 Port Instance.....	18
4 Security.....	20
4.1 Port Isolation.....	20
4.2 Port Speed Limit.....	20
4.3 Storm Control.....	20
5 System.....	22
5.1 System Time.....	22
5.2 System Management.....	22
5.2.1 Factory Default.....	23
5.2.2 Software Update.....	23
5.2.3 Device Restart.....	23
5.3 Login Management.....	23
5.4 Device Information.....	24
5.5 Alarm Center.....	24
5.6 Log Information.....	25

5.7 IP Management.....	25
5.8 Legal Statement.....	25
Appendix 1 Security Commitment and Recommendation.....	26

1 Initialization and Login

The Managed Switch provides Web access functionality. You can log in to the web manager to manage and configure the device.

1.1 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 network.
- 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 **ConfigTool** to obtain the IP address on select models of devices.

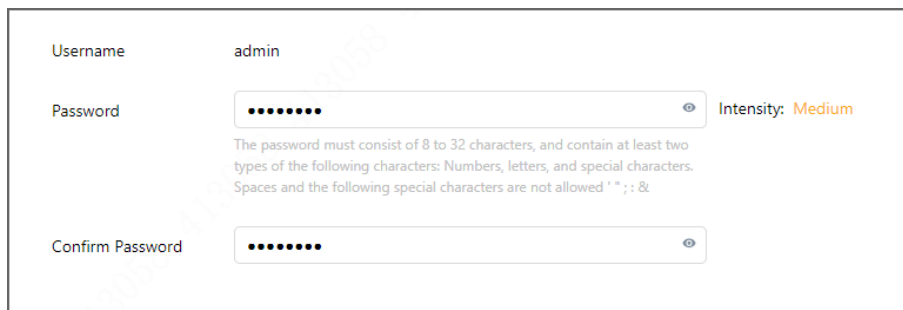
Procedure

- 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 user name is admin.
- Configure a high security password according to the prompt of password strength. A password must be 8-32 characters containing at least 2 types among numbers, letters and common characters (any visible characters other than ' ', ' ', ' ', and '&').

Figure 1-1 Configure password



- Step 5** Click **Complete**.

1.2 Logging in to 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.

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**.

1.3 Home Page



The page might vary depending on the product model. Please refer to the actual device.

Figure 1-2 Home page

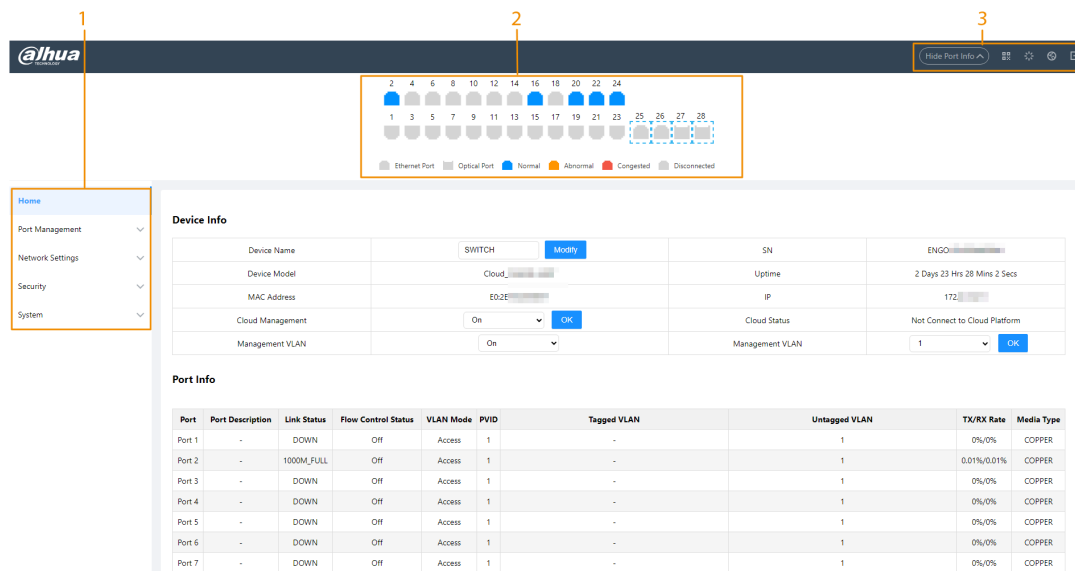


Table 1-1 Home page description

No.	Description
1	Displays the main menu.
2	Graphically displays the port status.
3	Supports hiding or showing the port information, logging out, restarting the device, switching the system languages, and scanning QR codes to access information.

Port Information

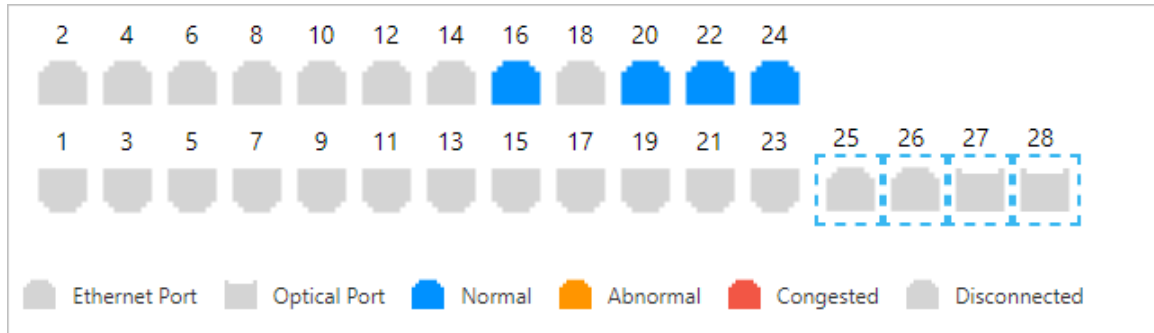


Hover over a port to view its connection information, including port status, link status, and power consumption.

- Ports are divided into uplink ports and downlink ports.

- ◇ The ports circled by blue dashed lines are uplink ports, which are used to connect to the upper-level network devices (such as core switches).
- ◇ The uncircled part is the downlink port, which is used to connect the next-level devices (such as access switches, terminal devices).
- The port in blue indicates a successful connection. The port in gray indicates no connection.
- Click any port to go to the **Port** page.

Figure 1-3 Port information



Home Page

Home page supports the following functions.

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



After enabling **Management VLAN**, you can only access the webpage of the device through an IP address belong to the management VLAN.

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

Table 1-2 Description of port information

Parameter	Description	
Port	Displays all ports of the device.	
Port description	Displays the port description. You can go to Port Management > Port to configure this parameter.	
Link Status	◇ DOWN: The port is not connected or the connection fails. ◇ Displays the port rate and the duplex mode: The port is connected. ○ FULL : The port can simultaneously receive and transmit data, achieving maximum throughput at double the rate. ○ HALF : The port can only either receive or transmit data at the same time.	
Flow Control Status	View the status of the flow control function, including On and Off . You can go to Switch Config > Port to configure this parameter.	
VLAN Mode	Includes Access and Trunk .	
PVID	Displays the VLAN of the port.	You can go to Switch Config > VLAN to configure this parameter.
Tagged VLAN	Displays the VLAN ID for the port that is allowed to be tagged when transmitting packets.	

Parameter	Description	
Untagged VLAN	Displays the VLAN ID for the port that is allowed to be untagged when transmitting packets.	
TX/RX Rate	Displays the current reception rate or sending rate divided by the actual negotiated rate for a period of time.	
Media Type	Includes 2 types: COPPER and FIBER . ◇ COPPER : RJ-45 port. ◇ FIBER : Optical port.	

2 Port Management

2.1 Port

You can configure the port parameters, including speed/duplexing, flow control, and other parameters.

Procedure

- Step 1** Select **Port Management** > **Port**.
- Step 2** In the **Port** list, select the port number, configure the parameters, and then click **Save**.
- **Speed/Duplexing** : In the **Speed/Duplexing** list, select the speed and the duplex mode. The speed/duplexing is set as **Auto** for combo port.
 - **Flow Control** : In the **Flow Control** list, select **on** to enable this function, which effectively relieves network congestion, reduces data loss, and improves network stability and data reliability.
 - **EEE Config** : In the **EEE Config** list, select **on** to enable this function, reducing power consumption when the network is idle and achieve energy saving.

Figure 2-1 Port configuration (1)

Port	Speed/Duplexing	Flow Control	EEE Config
Port 1, Port 2	AUTO	On	On

Save

- Step 3** In the **Port Description** box, enter the description of the port, and then press Enter key or click any other area on the page to save the configuration.



The port description supports numbers, letters, special character (_), with a maximum length of 16 characters. The default value is empty.

Figure 2-2 Port configuration (2)

Port	Port Description	Media Type	Speed/Duplexing Config	Speed/Duplexing Status	Flow Control	Flow Control Status	EEE Config
Port 1		COPPER	AUTO	DOWN	On	Off	Off
Port 2		COPPER	AUTO	DOWN	Off	Off	Off
Port 3		COPPER	AUTO	DOWN	Off	Off	Off
Port 4		COPPER	AUTO	DOWN	Off	Off	Off
Port 5		COPPER	AUTO	DOWN	Off	Off	Off
Port 6		COPPER	AUTO	DOWN	Off	Off	Off
Port 7		COPPER	AUTO	DOWN	Off	Off	Off
Port 8		COPPER	AUTO	100M_FULL	On	On	Off
Port 9		COPPER	AUTO	DOWN	Off	Off	Off
Port 10		COPPER	AUTO	DOWN	Off	Off	Off

Refresh

Table 2-1 Description of the port parameters

Parameter	Description
Media type	Includes 2 types: COPPER and FIBER. • COPPER: RJ-45 port. • FIBER: Optical port.

Parameter	Description
Speed/Duplexing configuration	Displays the configured parameters of this port.
Speed/Duplexing status	● DOWN : Displays the port is not connected or the connection fails. ● Displays the port rate and the duplex mode: Displays the port is connected. ◇ FULL : The port can simultaneously receive and transmit data, achieving maximum throughput at double the rate. ◇ HALF : The port can only either receive or transmit data at the same time.
Flow control	Displays whether the flow control function is enabled and the current flow control status.
Flow control status	
EEE configuration	Displays whether the EEE function is enabled.

2.2 PoE

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 devices do not support this function.

2.2.1 Global Configuration

You can configure the perpetual PoE and available power.

Procedure

Step 1 Select **Port Management** > **PoE** > **Global Config**.

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

Enable perpetual PoE, which continues to supply power to powered devices when the device is soft-rebooted. If the device is power off and restart, it will not continue to supply to powered devices after the reboot.

Step 3 Configure the available power.

Displays information such as total power, available power, alert power, consumed power, remaining power and perpetual PoE at the bottom of the page.



- Available power refers to the maximum power that can be provided to powered devices. When the consumed power is less than available power, new PD is allowed to be powered on.
- During operation, the actual power consumption might fluctuate. When the consumed power exceeds the alert power, the ports will be powered down from low to high according to the priority (the higher the port number, the lower the priority), until the consumed power is less than the alert power.

Figure 2-3 Global configuration

Global Config

Port Config

Perpetual PoE

☒

Save

Available Power

99

(1~110)W

Save

Total Power(W)	Available Power(W)	Alert Power(W)	Consumed Power(W)	Remaining Power(W)	Perpetual PoE
110	99	110	0	110	On

Refresh

Step 4 Click **Save**.

2.2.2 Port Configuration

Configure the PoE function of the port.

Procedure

Step 1 Log in to the web manager.

Step 2 Select **Port Management** > **PoE** > **Port Config**.

Step 3 Configure the port parameters.

- Configure the port. In the **Port** list, select the port number, enable the PoE, long distance PoE, PoE watchdog, enhanced PoE, and force PoE as needed.

Figure 2-4 Port configuration (1)

Port	PoE	Long Distance PoE	PoE Watchdog	Enhanced PoE	Force PoE
Port 1, Port 2	On	Off	On	Off	Off

Save

Table 2-2 Description of PoE parameters

Parameter	Description
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, the device periodically checks the status of the PD. If no data transmission is detected, it automatically powers off and restarts the PoE port, ensuring port monitoring and maintaining PD connectivity. Force PoE and PoE watchdog cannot be enabled at the same time.

Parameter	Description
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, connecting a non-PoE device to a forced PoE port might result in PD damage.
Enhanced PoE	When disabled, this function only supports PD compliant with standard PoE protocols, delivering power based on the device's defined power class. When enabled, it extends compatibility to both standard PoE devices and some non-standard PoE devices, delivering power based on the device's defined power class. The port types and the corresponding output power are as follows. ◇ AF/AT: 30 W. ◇ Hi-PoE: 60 W. ◇ BT: 90 W.  This configuration option is available only for standard PoE devices.

- View the PoE parameter configuration of each port.

Figure 2-5 Port configuration (2)

Port	Level	Consumed Power(W)	PoE Enable	Long Distance PoE	PoE Watchdog	Enhanced PoE	Force PoE
Port1	-	0	On	Off	Off	Off	Off
Port2	-	0	On	Off	Off	Off	Off
Port3	-	0	On	Off	Off	Off	Off
Port4	-	0	On	Off	Off	Off	Off
Port5	-	0	On	Off	Off	Off	Off
Port6	-	0	On	Off	Off	Off	Off
Port7	-	0	On	Off	Off	Off	Off
Port8	-	0	On	Off	Off	Off	Off

Table 2-3 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+.
Consumed power (W)	Displays the current PoE power consumed by the corresponding single port.
PoE enable	Displays whether these 5 types of PoE features are enabled on the ports.
Long distance PoE	
PoE watchdog	
Enhanced PoE	
Force PoE	

Step 4 Click **Save**.

2.3 VIP Port

Configure QoS and PoE power supply priority mechanisms for ports. When traffic congestion occurs, the system will schedule and forward the traffic of the ports based on the priority of the configured ports. When the power supply is insufficient, the system schedules PoE power supply based on priority to ensure the transmission of critical data and the power supply quality of ports.

Background Information

For interfaces connected to the network administrator, the configuration of VIP ports will automatically adopt the highest priority policy, and users are not allowed to modify it manually.



When the device does not have PoE functionality, the power-related configuration is unavailable. Please refer to the actual page.

Procedure

Step 1 Select **Port Management** > **VIP Port**.

Step 2 Select the port from the port list, and configure the QoS priority and the PoE priority.

Figure 2-6 VIP port configuration

You cannot configure VIP port settings on an uplink port. If you select an uplink port, the configuration will be skipped. If a port is detected as an uplink port, its priority will be set to high and cannot be manually changed.

QoS Priority: Streams from ports that are set to high priority are forwarded first.

PoE Priority: Ports that are set to high priority receive PoE power first. If the priorities are equal, the lower-numbered port takes precedence.

Port	QoS Priority	PoE Priority
Port 1, Port 2, Port 3, Port 4, Port 5, Port 6, Port 7	Medium	Medium

Save
Clear

Port	QoS Priority	PoE Priority
Port 1	Low	Low
Port 2	Low	Low
Port 3	Low	Low
Port 4	Low	Low
Port 5	Low	Low
Port 6	Low	Low
Port 7	Low	Low

Step 3 Click **Save**.

2.4 Port Statistics

Procedure

Step 1 Select **Port Management** > **Port Statistics**.

Step 2 View the information of port such as port type, receive usage, transmit usage, and more.

Step 3 (Optional) Click **Reset** to clear port statistics.

Figure 2-7 Port statistics

Port	Port Type	RX Usage	TX Usage	RX/TX Bytes (KB)	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%	0%	0.00B/0.00B	0/0	0/0
Port 3	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0
Port 4	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0
Port 5	Physical Port	0%	0%	85.22KB/117.18KB	735/423	0/0
Port 6	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0
Port 7	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0
Port 8	Physical Port	0.03%	0.01%	8.82GB/122.34MB	91483274/1412498	54076/0
Port 9	Physical Port	0%	0%	13.34KB/8.78KB	206/133	0/0
Port 10	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0

Table 2-4 Description of PoE parameters

Parameter	Description
Port	Displays the port number.
Port type	Displays the port type, indicating the type of port, such as Physical Port .
RX usage	Displays the receive usage, indicating the percentage of bandwidth utilization for incoming traffic.
TX usage	Displays the transmit usage, indicating the percentage of bandwidth utilization for outgoing traffic.
RX/TX Bytes (KB)	Displays the received/transmitted Bytes (KB), showing the total data volume.
Successful RX/TX packet	Displays the successful received/transmitted packets, indicating the number of successfully received and sent data packets.
Failed RX/TX Packet	Displays the failed received/transmitted packets, indicating the number of failed received and sent data packets.

2.5 Link Aggregation

Link aggregation allows traffic to be spread across member ports in an aggregation group to increase bandwidth. Each member port of the same aggregation group dynamically backs up to each other, improving the reliability of the link.

Procedure

- Step 1** Select **Port Management > Link Aggregation**.
- Step 2** Select the load balancing as needed, and then click **Save**.

Figure 2-8 Load balancing

Load Balancing
☒ Source MAC Config
☒ Destination MAC Config
|
☒ Source IP Config
☒ Destination IP Config
|
☒ TCP/UDP Source Port
☒ TCP/UDP Destination Port

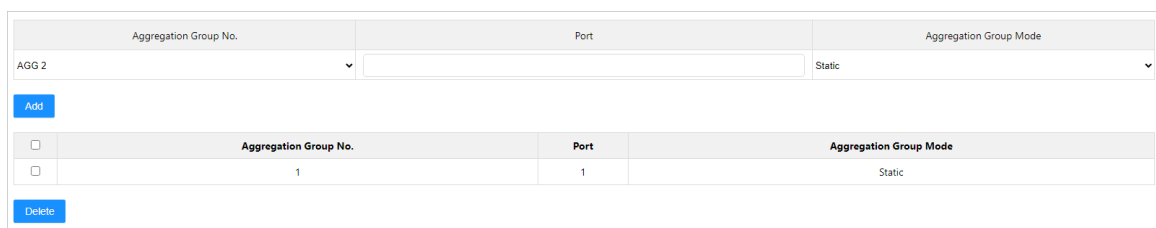
Save

Table 2-5 Load balancing description

Parameter	Description
Source MAC Config	Divert traffic based on the source MAC address of the data packet.
Destination MAC Config	Divert traffic based on the destination MAC address of the data packet.
Source IP Config	Divert traffic based on the source IP address of the data packet.
Destination IP Config	Divert traffic based on the destination IP address of the data packet.
TCP/UDP Source Port	Divert traffic based on the source port of the TCP/UDP protocol.
TCP/UDP Destination Port	Divert traffic based on the destination port of the TCP/UDP protocol.

Step 3 Select aggregation group number, port, and aggregation group mode.

Figure 2-9 Aggregation group



- Aggregation group No.: Except for special chips, the specification of the aggregation group is the total number of ports of the device divided by 2, with a maximum of 8 groups.
- Port: Select the number of ports as needed. The total bandwidth after merging multiple ports = the sum of the bandwidths of each port.
- Aggregation group mode: It is **Static** by default.

Step 4 Click **Add**, and then the aggregation group will be added to the list.

Related Operations

Select groups from the list, and then click **Delete** to delete the aggregation groups.

2.6 Cable Detection

Background Information

Detect the status of network cables connected to ports to quickly locate faulty cables and their corresponding positions.

- The maximum detectable length is 100 meters for network cables.
- Only copper ports support cable testing; optical ports do not.
- The test results are based on signal attenuation and are for reference only. When the cable is connected and shorter than 3 meters, signal attenuation primarily comes from connectors rather than the cable itself, leading to relatively higher measurement errors.

Procedure

Step 1 Log in to the web manager.

- Step 2** Select **Port Management** > **Cable Detection**.
- Step 3** In the **Select Port** list, select the port number as needed, and then click **Search**.
- Step 4** Confirm the cable status based on the test results.
- Normal: The cable is functioning properly.
 - Open circuit: No cable is connected, or the cable is broken.
 - Short circuit: The cable is faulty.

Figure 2-10 Cable detection

Select Port
Port 8

Search

The test results are for reference only. They also might have been affected by signal attenuation in the network cable. If the cable is less than 3 meters, signal attenuation might still occur due to the connectors rather than the cable. As a result, there is a relatively large margin of error in the test results.

Selected Ports 8

Length(cm)	Results	View Details
-	Normal	☒

Channel	Length (cm)	Channel Status
RX Channel	-	Normal
TX Channel	-	Normal

- Step 5** (Optional) Click ☒ under the **View Details** to view the distance from the normal or fault point to the port.

2.7 Port Mirroring

Port mirroring, also known as port monitoring, is a packet technique. By configuring the device, you can copy data packets from one or more source ports (mirrored ports) to a specific destination port (monitoring port). A host running packet analysis software is connected to the destination port to analyze the collected packets, enabling network monitoring and troubleshooting.

Procedure

- Step 1** Select **Port Management** > **Port Mirroring**.
- Step 2** In the **Select Port** list, select the port number, direction and destination port as needed.
- Direction supports Tx only, Rx only and bidirectional modes.
- Tx only: Only copies transmitted packets.
 - Rx only: Only copies received packets.
 - Bidirectional: Copies both transmitted and received packets.

Figure 2-11 Port mirroring

Input and output messages from the source port will be mirrored to the destination port.

Source Port	Direction	Destination Port
Port 2	Tx Only	Port 3

Save

Source Port	Direction	Destination Port
-------------	-----------	------------------

- Step 3** Click **Save**, and then the added mirroring information is displayed at the bottom of the page.

3 Network Settings

3.1 VLAN

You can add the port to the VLAN, and then you can configure the VLAN parameters.

Procedure

- Step 1** Select **Network Settings** > **VLAN** > **Add VLAN**.
- Step 2** Enter the VLAN ID and description, and then click **Save**.
- The added VLAN information is displayed at the bottom of the page.
 - You can select the VLAN and then click **Delete** to delete the VLAN.



VLAN1 cannot be deleted.

Figure 3-1 Add VLAN

Add VLAN
VLAN

VLAN ID	Description
2 (2-4094)	

Save

☐	VLAN ID	Description	Tagged Port List	Untagged Port List
☐	1	Default_VLAN		1-6
☐	2	VLAN2		
☐	3	VLAN3		
☐	6	VLAN6		
☐	7	VLAN7		
☐	8	VLAN8		
☐	1234	VLAN1234		

Delete

- Step 3** Select **Network Settings** > **VLAN** > **VLAN**.
- In the **Port** box, select one or more ports.
 - In the **Mode** list, select the VLAN mode, including **Access** and **Trunk**.
 - Configure PVID, tagged VLAN, and untagged VLAN.
 - When the **Mode** is **Access**, you must 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 must 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.

Figure 3-2 VLAN

Add VLAN
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

Table 3-1 Frame processing comparison

Port Type	Untagged Frame Processing	Tagged Frame Processing	Frame Transmission
Access	Adds the port PVID tag 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.
Trunk		- Accepts a tagged frame if the VLAN ID carried in the frame is permitted by the port. - Discards a tagged frame if the VLAN ID carried in the frame is denied by the port.	- If the frame's VLAN ID matches the default VLAN ID and the VLAN ID is permitted by the port, 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 port, the device will directly transmit the frame.

- Click **Save**, and then the added VLAN information is displayed at the bottom of the page.

3.2 Neighbor List

LLDP (Link Layer Discovery Protocol) is a standard link-layer discovery method. It organizes the local device's main capabilities, management address, device identifier, port identifier, and other information into different TLVs (Type Length Value) and encapsulates them in LLDPDU (Link Layer Discovery Protocol Data Unit). These are then sent to directly connected neighbors. Upon receiving this information, the neighbors store it in a standard MIB (Management Information Base) format, allowing network management systems to query and assess the communication status of the link.

Procedure

Step 1 Select **Network Settings** > **Neighbor List**.

Step 2 Select **LLDP** checkbox, and then click **Save**.

Figure 3-3 LLDP neighbor list

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

Port	Peer Port Name	Device Name	MAC Address	IP
8	GigabitEthernet1/0/8	SWITCH	00:00:00:00:00:00	192.168.1.1
8	GigabitEthernet1/0/1	SWITCH	00:00:00:00:00:00	192.168.1.2
8	GigabitEthernet1/0/1	SWITCH	00:00:00:00:00:00	192.168.1.3
8	FE8	SWITCH	00:00:00:00:00:00	192.168.1.4
8	GE1	SWITCH	00:00:00:00:00:00	192.168.1.5

3.3 MAC Management

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 Add the Static MAC.



- The maximum number of static MAC entries that can be configured depends on the specific device.
- Select a MAC and then click **Delete**, you can delete the static MAC.

- Select **Network Settings** > **MAC Management** > **Static MAC**.
- Configure the MAC address, VLAN ID and port, and then click **Add**.



VLAN ID is available on select models. The actual configuration shall go prevail.

Figure 3-4 Static MAC

Static MAC MAC Search MAC List

You can only configure up to 16 static MACs.

MAC Address	VLAN ID	Port
00:00:00:00:00:00	4094 (1-4094)	Port 8

Add

No.	MAC Address	VLAN ID	Port
☐	1	00:00:00:00:00:00	4094
☐			Port 8

Delete

Step 2 Search the MAC address.

1. Select **Network Settings > MAC Management > MAC Search**.
2. Enter the MAC address or select the port, and then click **Search**.

Figure 3-5 MAC search

Static MAC **MAC Search** MAC List

MAC Address	Port
00:00:00:00:00:00	Port 8

Search

MAC Address	MAC Type	VLAN ID	Port
00:00:00:00:00:00	Static	4094	Port 8

Step 3 View MAC address.

Select **Network Settings > MAC Management > MAC List** to view the added MAC address information.

Up to 100 items can be displayed. For details, go to **MAC Search**.



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

Figure 3-6 MAC list

Static MAC MAC Search **MAC List**

No.	MAC Address	MAC Type	VLAN ID	Port
1	00:00:00:00:00:00	Static	4094	Port 8

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

Refresh **Clear**

3.4 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.



Loop Protection is used to detect and block the abnormal loop. It is not designed for backuping the redundant links.

3.5 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.

3.5.1 STP Configuration

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 3-7 STP configuration

Enable		☒		
$\text{Max Aging Time} \geq (\text{Hello Timer} + 1) \times 2$ $\text{Max Aging Time} \leq (\text{Forwarding Delay Time} - 1) \times 2$				
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
Save				
Working Mode	Hello Timer	Max. Aging Time	Forwarding Delay Time	Bridge Priority
STP	0	0	0	0

Table 3-2 Description of the STP parameters

Parameter	Description
Working Mode	Select STP or RSTP as needed. - STP: It is suitable for environments compatible with outdated devices or small networks without redundant links that only require ring placement. - RSTP: It has a faster convergence speed and more efficient topology changes, making it suitable for environments such as enterprise campus networks or data center access layers.
Hello Timer	The time interval for regularly sending protocol data, the smaller the interval, the faster the convergence speed, but it will increase network consumption. The time ranges from 1 second to 10 seconds.
Max. Aging Time	The maximum time that protocol data is retained on the port, usually set to about ten times the Hello time. If no new data is received within this time, the port considers the upstream link to have failed and begins to recalculate the topology. The time ranges from 6 seconds to 40 seconds.
Forwarding Delay Time	The time required for a port to transition from the Listening/Learning state to the Forwarding state. It is used to ensure the stability of the topology before forwarding data to prevent loops. The time ranges from 4 seconds to 30 seconds.
Bridge Priority	Used for the election root bridge. The smaller the value, the higher the priority. If multiple devices have the same priority, the root bridge is determined by comparing the MAC addresses. The value ranges from 0 to 61440.

Step 5 Click **Save**.

3.5.2 Port Instance

Configure the STP (Spanning Tree Protocol) related parameters to the port.

Procedure

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

Step 2 Select port, configure the priority, and the root path cost.

Figure 3-8 Configure the port instance

Port	Priority	Root Path Cost
Port 2, Port 3, Port 4, Port 5, Port 6, Port 7	128 (0~240)	0 (0~200000000)

Save

Port	Role	Status	Priority	Root Path Cost	Designated Bridge ID	Designated Port ID
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	-	-

Table 3-3 Port instance description

Parameter	Description
Port	Select the target port.
Priority	Configure the priority of ports in STP, which ranges from 0 to 240.
Root Path Cost	Configure the path cost from this port to the root bridge, which ranges from 0 to 2,000,000,000. The smaller the value, the better the path.

Step 3 Click **Save**.

4 Security

4.1 Port Isolation

By using the port isolation feature, isolation between ports within the same VLAN can be achieved. The port isolation function provides users a safer and flexible networking solution.

Procedure

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

Step 2 Enable port isolation.



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

Step 3 Click **Save**.

4.2 Port Speed Limit

Configure port rate limiting policies to restrict the rate of data packet exchange in and out of the port.

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 in and out.

Figure 4-1 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**, and then the information that has been set is displayed at the bottom of the page.

4.3 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 proper network operation.

Procedure

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

Step 2 Configure suppression for the rates of broadcast, multicast, and unknown unicast.

- Select the packet type and port number, enable storm control, and then enter the speed limit.
- For the same port, the speed of multicast, broadcast, and unknown unicast types can be configured with different values.

Figure 4-2 Storm control

For the port being configured, the suppression rate must be the same for its multicast, broadcast, and unknown unicast.

Type	Port	Enable	Speed Limit (Mbit/sec)
Broadcast ▼		On ▼	100 (1~100)M

[Save](#)

Port	Port Type	Broadcast	Multicast	Unknown Unicast	Speed Limit (Mbit/sec)
Port 1	Physical Port	On	Off	Off	100
Port 2	Physical Port	On	Off	Off	100

Step 3 Click **Save**, and then the information that has been set is displayed at the bottom of the page.

5 System

5.1 System Time

Procedure

- Step 1 Select **System** > **System Time**.
- Step 2 Configure the system time.

Figure 5-1 Configure the system time

Only devices connected to the cloud can successfully synchronize their system time.

System Time	2000 - 01 - 04	08 : 34 : 03	Sync PC
Time Zone	(UTC+08:00) Beijing, Chongqing, Hon		
Time Synchronization	Cloud Platform ▼		
DST	☒		
Type	Date ▼		
Start Time	01 - 01	00 : 00	
End Time	01 - 02	00 : 00	

Save
Refresh

- Time synchronization.
 - ◇ Cloud platform: The system automatically synchronizes the time on the cloud platform. It will only take effect after the device is uploaded to the cloud.
 - ◇ Do not sync: You can manually configure the system time and time zone, or click **Sync PC** to automatically synchronize the system time on the PC.
- DST (Daylight Saving Time): After enabling it, you need to configure the daylight saving time period separately.

- Step 3 Click **Save**.

5.2 System Management

5.2.1 Factory Default

Procedure

- Step 1 Select **System** > **System**.
- 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.
- If you want to restore all configurations to the factory default, press the Reset button of the device.

5.2.2 Software Update

Procedure

- Step 1 Select **System** > **System**.
- Step 2 Click **Browse** to import the update file, and then click **Update**.
- Step 3 Click **OK** in the pop-up prompt box.

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

5.2.3 Device Restart

Procedure

- Step 1 Select **System** > **System**.
- Step 2 Click **Restart**.
- Step 3 Click **OK** in the pop-up prompt box to restart the device.



You can also restart the device by clicking  in the upper-right corner of the page.

5.3 Login Management

Changing the login password for the device web page.

Procedure

- Step 1 Select **System** > **Login Management**.
- Step 2 Enter the old password, new password, and then confirm the new password.



The password must consist of 8 to 32 characters, and contain at least 2 types of characters among upper case, lower case, number, and special characters (excluding ', ", ,, :, and &).

Figure 5-2 Change password

Regularly change your password to prevent unauthorized users from accessing the system.

Old Password

New Password

Intensity: **Strong**

The password must consist of 8 to 32 characters, and contain at least two types of the following characters: Numbers, letters, and special characters. Spaces and the following special characters are not allowed ' " ; &

Confirm Password

Save

Step 3 Click **Save**.

5.4 Device Information

Select **System** > **Device Info**, and then you can view the information such as the device name, software version, MAC address, and running time.

It also supports enabling cloud management functionality.

5.5 Alarm Center

Procedure

Step 1 Select **System** > **Alarm Center**.

Step 2 View the alarm information generated by the system history.

Figure 5-3 Alarm information

No.	Alarm Type	Alarm Time	Alarm Details
No data			
Refresh			

Step 3 (Optional) Click **Refresh** to refresh the alarm list.

5.6 Log Information

Select **System** > **Log Info**, view the user login log information.

5.7 IP Management

Configure the IP address, DNS server, and more.

Procedure

Step 1 Select **System** > **IP Management**.

Step 2 Configure the parameters.

- **Enable DHCP** : After enabling DHCP, the device will automatically acquire and assign an IP address, provided that a DHCP server is available in the network.
- **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, provided that a DNS server is available in the network.
- **Disable Auto Obtain DNS** : Enter the IP addresses of the DNS1 and DNS2.

Figure 5-4 Network information

DHCP	IP Address	Subnet Mask	Gateway	Auto Obtain DNS	DNS1	DNS2
Off ▼				Off ▼		
Save						

Step 3 Click **Save**.

5.8 Legal Statement

Select **System** > **Legal Statement**, click the corresponding tab to view the software license agreement and privacy policy.

Appendix 1 Security Commitment and Recommendation

Zhejiang Dahua Vision Technology Co., Ltd. (hereinafter referred to as "Dahua") attaches great importance to cybersecurity and privacy protection, and continues to invest special funds to comprehensively improve the security awareness and capabilities of Dahua employees and provide adequate security for products. Dahua has established a professional security team to provide full life cycle security empowerment and control for product design, development, testing, production, delivery and maintenance. While adhering to the principle of minimizing data collection, minimizing services, prohibiting backdoor implantation, and removing unnecessary and insecure services (such as Telnet), Dahua products continue to introduce innovative security technologies, and strive to improve the product security assurance capabilities, providing global users with security alarm and 24/7 security incident response services to better protect users' security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report any potential risks or vulnerabilities discovered on Dahua devices to Dahua PSIRT, for specific reporting methods, please refer to the cyber security section of Dahua official website.

Product security requires not only the continuous attention and efforts of manufacturers in R&D, production, and delivery, but also the active participation of users that can help improve the environment and methods of product usage, so as to better ensure the security of products after they are put into use. For this reason, we recommend that users safely use the device, including but not limited to:

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

Dahua 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, we recommend you 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 Allowlist

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

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;
- Establish 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**

We recommend you 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).

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188