

COME-STAR

Managed Industrial Ethernet Switch

WEB User Manual

——Applied for MBN9000 Series

Version number: V1.0

Wuhan COME-STAR Communication Co., Ltd.

Instructions

This manual is a general guide. Configuration pages and functions may vary slightly depending on the specific model. Please refer to your actual device for accurate details.

Important Statement

Any information provided by the Company in this manual does not imply that any corresponding authorization is granted for such information.

The Company endeavors to ensure that the information provided in this manual is accurate and applicable. However, the Company assumes no responsibility for the use of such information, nor any joint and several liability for the use of such information. The product and user manual may contain technical or typographical errors. The Company reserves the right to change all or part of the contents of this user manual without prior notice.

Statement:

Duo to continuous update and improvement of products and technology, the contents of this document may not be completely consistent with the actual products, appreciate for your understanding. If necessary to inquiry the updates of the product, please check our official website or contact our representative directly.

Revision History

Version number	Date	Revision Record
V1.0	2024.8.30	Create file

Safe Use Instructions

This product performance is excellent and reliable in the designed range of use, but it's necessary to avoid man-made damage or destroy for the equipment.

- Read the manual carefully and keep this manual for reference if need afterwards.
- Do not put the device close to the water sources or damp places.
- Do not put anything on the power cable, it should be placed out of reach.
- To avoid causing fire, do not knot or wrap the cable.
- Power connector and other device connectors should be firmly connected with each other, frequently inspection is needed.
- Please keep the fiber socket and plug clean. Do not look directly at the fiber section when the equipment is working.
- Please keep the equipment clean and wipe it with a soft cotton cloth if necessary.
- Please do not repair the equipment by yourself, unless there is clear instructions in the manual.

Under the following circumstances, please cut off power immediately and contact us.

- Equipment water damage.
- The equipment is broken or the casing is broken.
- The equipment works abnormally or the performance has completely changed.
- The equipment produces odor, smoke or noise.



Note :Explanatory information necessary during the use of this manual



Caution :Matters requiring special attention when using this manual

1 Configuration Preparation

1.1 Configuring the Switch

Our managed industrial Ethernet switches have a built-in Web server. Users can configure the switch by accessing the Web server. Before accessing the Web, please configure the switch as follows:

- Configure the IP address of the VLAN 1.1 interface to ensure that the route between the PC and the switch VLAN 1.1 interface is reachable. The configuration commands are as follows:

```
switch#configure terminal
```

```
switch(config)#interface vlan1.1
```

```
switch(config-vlan1.1)#ip address 192.168.16.253/24
```

- To configure the user name, password and user authority level (level 3 is administrator authority), the configuration command is as follows:

```
switch#configure terminal
```

```
switch(config)#username xxx password xxx privilege <0-3>
```

Among them, <0-3> represents the user authority: 0-visitor, 1-observer, 2-operator, 3-manager. Privilege, the larger the value, the higher the user authority, and the third-level user has full access authority.



Note

1. After the above configuration commands are executed, use the "write" command to save all configurations.
2. The web server is enabled by default when the switch leaves the factory.
3. The factory default IP address of the switch is 192.168.16.253, and the default user name/password is admin/admin.

1.2 Configuring the PC

To access the switch through the Web, the IP of the switch and the PC must be in the same network segment. For Windows users, please refer to the following steps:

Start → Control Panel → Network and Internet Connections → Network Connections → Local Area Connection → Properties → Internet Protocol (TCP/IP)

The specific operation page of Windows system is shown in Figure 1.

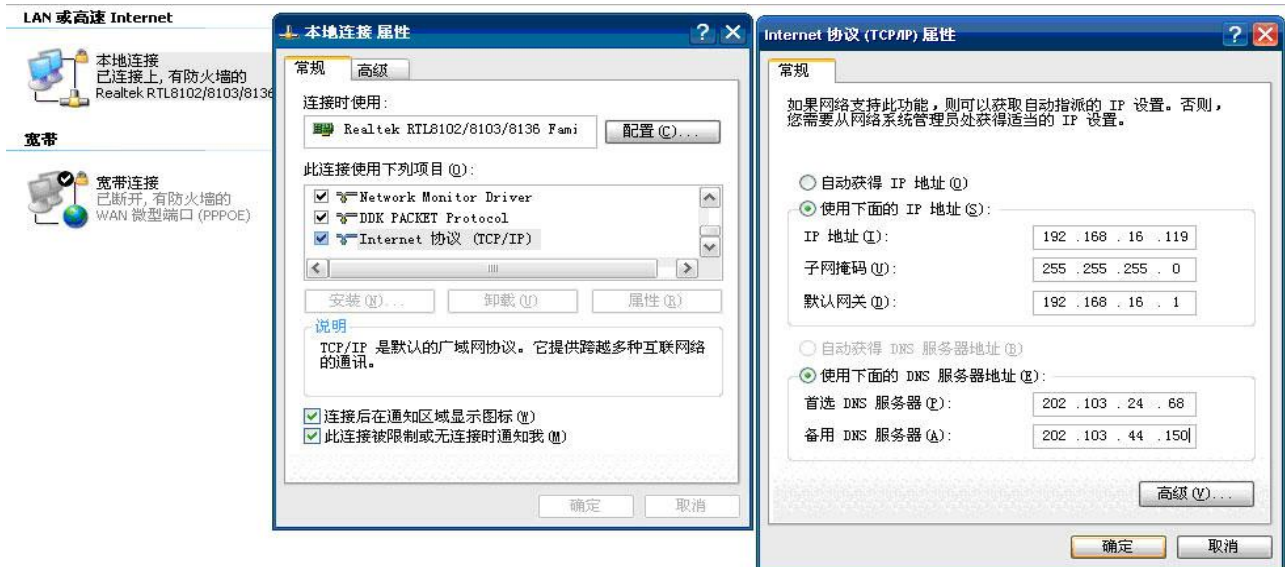


Figure 1 Windows IP Setting Interface

The default IP address of the switch is 192.168.16.253. Follow the above steps to change the PC's IP address to 192.168.16.X (where X is any valid value from 2 to 254 except 253). After the modification is successful, you can use this IP address to access the Web.

1.3 Ping Testing

After both the switch and the PC are configured, you can use the ping command to check whether the connection between the PC and the switch is normal. For Windows users, please refer to the following operations:

- **Start → Run → input "cmd" → click "OK".**
- **Enter the command "ping 192.168.16.253" in the command line program of the Windows system, as shown in Figure 2.**

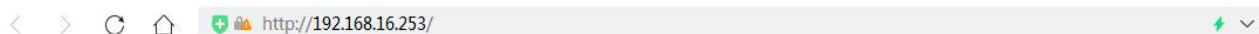


Figure 2 Using the ping command in Windows

If the ping is successful, it indicates that the connection between the PC and the switch is normal. Otherwise, please check the network connection.

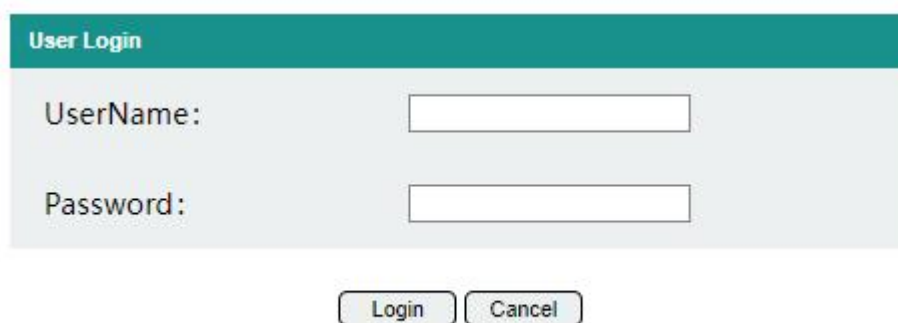
1.4 Login WEB

Open a browser and enter the switch's default IP address "192.168.16.253" in the address bar, as shown in Figure 3.



Picture 3 Interface for entering the IP address in the address bar

Figure 4 will pop up, prompting the user to enter the user name and password.



Picture 4 Login WEB



1. It is recommended that users use Google, Firefox or IE7.0 and above browsers.
2. If the web page displays "Request Timeout" after you enter the IP address and jump to the page,

please check whether the network connection is normal. If the network connection is normal but the page is still inaccessible, use the "web enable http" or "web enable https" command in the command-line configuration mode to enable Web access.

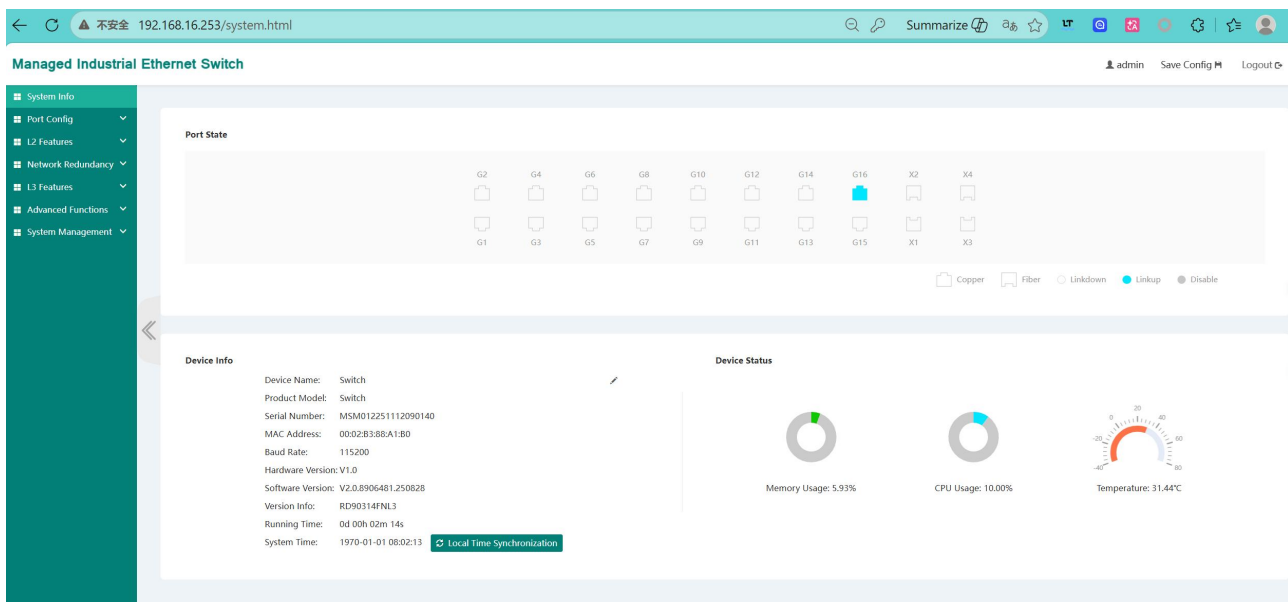
2 Web Page Overview



All pages and configurations of the following functions are subject to the actual product.

2.1 Overall Page

After login authentication is passed, you will enter the Web main page of the switch. The title bar displays the current switch product model. The Web page is divided into four major areas: the upper area is the logo display and shortcut key area, the left side is the menu area, the right side is the main function display area, and the lower area is the browser information display area, as shown in Figure 5.



Picture 5 Web Main Page

2.2 Top Area

The left side of the top area is the logo, and the right side contains shortcut keys, which implement administrator, configuration saving, and exit, as shown in Figure 6.

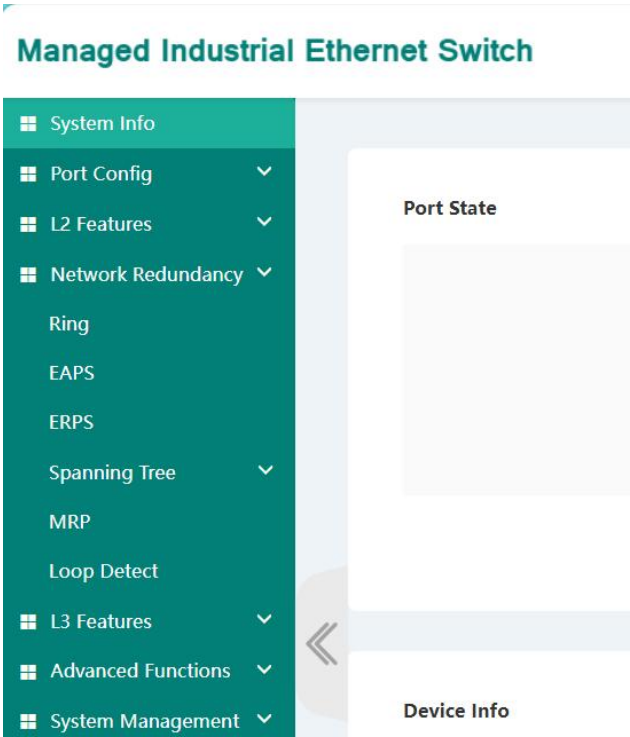


Picture 6 Top Area

2.3 Left Menu Area

The left area is the configurable function menu, where a three-level directory structure is used. The first-level directory is system information, port configuration, layer-2 features, ring redundancy, layer-3

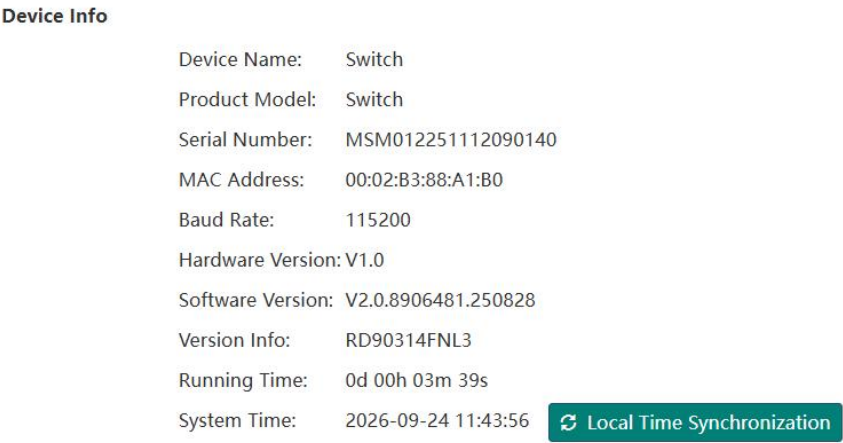
features, advanced functions, and system management. Click "Expand" and "Collapse" to quickly expand and collapse all secondary menus. Click the  sign in front of each level of directory to expand the corresponding submenu. As shown in Figure 7.



Picture 7 Left area menu

2.4 Right functional area

The right side is the function display area, which can view and configure various parameters of the function. As shown in Figure 8.



Picture8 Right function area

2.5 Bottom Area

The bottom area displays browser usage recommendations. As shown in Figure 9.

3 System Status

3.1 Basic Information

The basic information page displays the device name, product model, serial number, MAC address, hardware version, software version, version information, running time and system time information of the switch. As shown in Figure 10.

Device Info	
Device Name:	Switch
Product Model:	Switch
Serial Number:	MSM012251112090140
MAC Address:	00:02:B3:88:A1:B0
Baud Rate:	115200
Hardware Version:	V1.0
Software Version:	V2.0.8906481.250828
Version Info:	RD90314FNL3
Running Time:	0d 00h 03m 39s
System Time:	2026-09-24 11:43:56
	

Picture10 Basic information area

3.2 Running Information

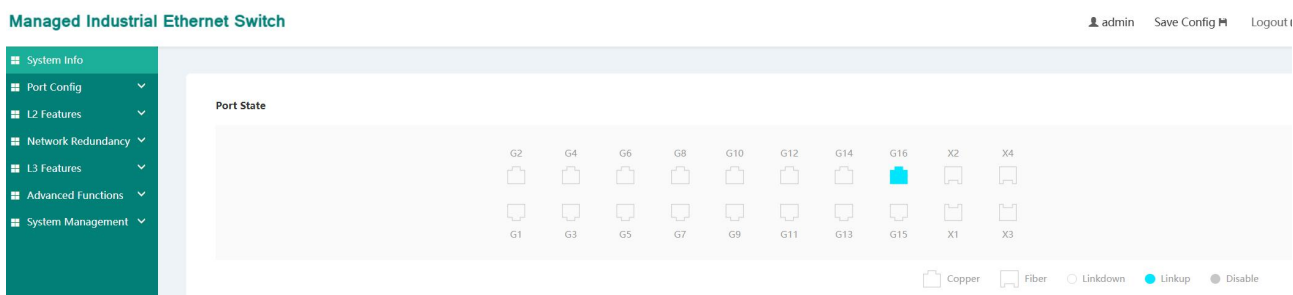
The Running Information page displays the switch's running time, CPU usage, and memory usage and operating temperature information. As shown in Figure 11.

系统信息 >> 运行信息	
运行信息	
运行时间	DAY:0 HOUR:0 MIN:28 SEC:24
CPU利用率	1.00%
内存利用率	5.24%
工作温度	35.25 °C
	

Picture11. Running information page

3.3 Port Status

The port status page can be automatically refreshed to display the connection status of each port in real time. When the port is connected, the port number will be highlighted. As shown in Figure 12.



Picture 12 Port statuses page

3.4 Port Flow

The port flow page displays the traffic statistics of each port, including the number of bytes received, unicast packets received, non-unicast packets received, error packets received, bytes sent, unicast packets sent, non-unicast packets sent, error packet sent. As shown in Figure 13.

Managed Industrial Ethernet Switch

admin Save Config Logout

Port Config > Port Statistics

Clear Refresh

Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts	InErrors	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts	OutErrors
G1	0	0	0	0	0	0	0	0	0	0
G2	0	0	0	0	0	0	0	0	0	0
G3	0	0	0	0	0	0	0	0	0	0
G4	0	0	0	0	0	0	0	0	0	0
G5	0	0	0	0	0	0	0	0	0	0
G6	0	0	0	0	0	0	0	0	0	0
G7	0	0	0	0	0	0	0	0	0	0
G8	0	0	0	0	0	0	0	0	0	0
G9	0	0	0	0	0	0	0	0	0	0
G10	0	0	0	0	0	0	0	0	0	0
G11	0	0	0	0	0	0	0	0	0	0
G12	0	0	0	0	0	0	0	0	0	0
G13	0	0	0	0	0	0	0	0	0	0
G14	0	0	0	0	0	0	0	0	0	0
G15	0	0	0	0	0	0	0	0	0	0
G16	521867	2148	360	92	357	2773485	3208	73	3	0

Picture 13 Port flow page

3.5 Optical Module Diagnostics (DDM)

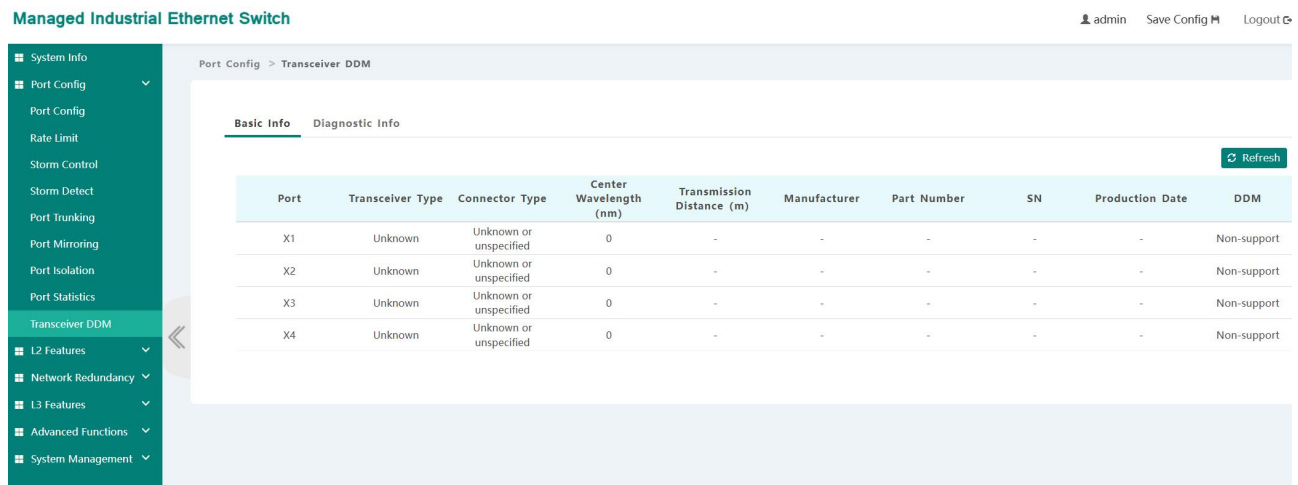
The content of this chapter is only applicable to our company's switch equipment with DDM function.

DDM (Digital Diagnostic Monitoring) is an effective method for monitoring important performance parameters of optical transceiver modules. It monitors parameters such as temperature, operating voltage, bias current, transmit optical power, and receive optical power. With the digital diagnostic function of the optical module, the switch can monitor these five key performance parameters in real time, quickly locate faults in the fiber-optic link, simplify maintenance, and improve overall system reliability.

This switch supports optical module diagnostics for pluggable transceiver modules on various interfaces. It provides access to general module information and key operating parameters, together with real-time

digital diagnostic monitoring. This function helps users quickly identify optical module faults, detect potential issues in advance, and resolve transceiver-related problems in a timely manner.

The Optical Module Diagnostics page is shown in Figure 14.



Picture 14 Optical module diagnostics page

This page consists of two lists. The upper list displays the main operating parameters of the optical transceiver modules installed on each optical port of the switch, while the lower list displays general module information.

The page parameters are described as follows:

Port: The port that supports the optical module diagnostic function.

Module Status: The current status of the optical module.

- Normal: The module supports DDM and is operating normally.
- Abnormal!: The module supports DDM, but the connection is abnormal.
- Non-DDM: The module does not support DDM.

Temperature (°C): The real-time temperature of the module.

Voltage (V): The real-time operating voltage of the module.

Current (mA): The real-time operating current of the module.

Tx Power (dBm): The transmit optical power of the module.

Rx Power (dBm): The receive optical power of the module.

Module Type: The type of the optical module.

Interface Type: The interface type of the module.

Wavelength (nm): The operating wavelength of the module.

Transmission Distance (m): The maximum transmission distance supported by the module.

Vendor Name: The name of the module manufacturer.

Part Number: The part number of the module.

Serial Number: The serial number of the module.

Manufacturing Date: The manufacturing date of the module.

DDM: Indicates whether the module supports DDM.

Attention:

1, In the query results, parameters such as temperature, voltage, current, transmit power, and receive power are displayed in the following format:

“<Real-Time Measured Value><Alarm Indicator> [<Low Alarm Threshold> ~ <High Alarm Threshold>]”

The values enclosed in [] indicate the valid range of the corresponding DDM parameter.

For the <Alarm Indicator>:

↑ indicates that the current parameter value is too high.

↓ indicates that the current parameter value is too low.

If no indicator is displayed, the current parameter value is within the normal range.

4 Port Configuration

4.1 Port Configuration

The port configuration function is used to configure and display the port, port type, current status, speed duplex, flow control, MTU of the port. As shown in Figure 15.

Managed Industrial Ethernet Switch admin Save Config

Port Config > Port Config Modify

Port	Port Type	Current Status	Speed Duplex	Port Enable	Flow Control	MTU	Port Des
G1	Copper	-	Auto	Enable	Disable	1500	-
G2	Copper	-	Auto	Enable	Disable	1500	-
G3	Copper	-	Auto	Enable	Disable	1500	-
G4	Copper	-	Auto	Enable	Disable	1500	-
G5	Copper	-	Auto	Enable	Disable	1500	-
G6	Copper	-	Auto	Enable	Disable	1500	-
G7	Copper	-	Auto	Enable	Disable	1500	-
G8	Copper	-	Auto	Enable	Disable	1500	-
G9	Copper	-	Auto	Enable	Disable	1500	-
G10	Copper	-	Auto	Enable	Disable	1500	-
G11	Copper	-	Auto	Enable	Disable	1500	-
G12	Copper	-	Auto	Enable	Disable	1500	-
G13	Copper	-	Auto	Enable	Disable	1500	-
G14	Copper	-	Auto	Enable	Disable	1500	-
G15	Copper	-	Auto	Enable	Disable	1500	-
G16	Copper	1G/full	Auto	Enable	Disable	1500	-

Picture 15 Port configuration page

The description of each configuration item is as follows:

Port Number: The label of the switch port. A port set whose properties need to be modified, it is automatically added to the text box after checking it.

Port Type: Displays the type of the interface, such as: copper port, optical port, and optoelectronic multiplexing port, etc.

Current Status

Speed Duplex: Set the duplex status and speed mode of the port.

Flow Control: Enable/disable traffic congestion control in the ingress direction, disabled by default.

MTU: Maximum Transmission Unit

Port description: Set the description information of the port, no more than 256 characters.

4.2 Port Rate Limiting

Port rate limiting is a network management function used to balance bandwidth allocation, control network traffic, ensure bandwidth availability for critical applications, prevent bandwidth abuse, and improve network security. As shown in Figure 16.

Port	Ingress Limit	Ingress Burst	Egress Limit	Egress Burst	Rate Unit
G1	-	-	-	-	kbps
G2	-	-	-	-	kbps
G3	-	-	-	-	kbps
G4	-	-	-	-	kbps
G5	-	-	-	-	kbps
G6	-	-	-	-	kbps
G7	-	-	-	-	kbps
G8	-	-	-	-	kbps
G9	-	-	-	-	kbps
G10	-	-	-	-	kbps
G11	-	-	-	-	kbps
G12	-	-	-	-	kbps
G13	-	-	-	-	kbps
G14	-	-	-	-	kbps
G15	-	-	-	-	kbps

Picture 16 Port rate limiting

To configure the parameters of one or more ports, select the checkboxes in front of the desired ports. The parameters of the selected ports will be mapped to the configuration area above. Modify the required parameters in the configuration area, and then click Configure to save the settings.

The configuration items are described as follows:

Port: Specifies the group of ports whose attributes need to be modified. Selected ports are automatically added to the text box.

Ingress Rate Limit: Sets the rate limit for ingress traffic.

Ingress Burst: Sets the burst traffic value for ingress traffic.

Egress Rate Limit: Sets the rate limit for egress traffic.

Egress Burst: Sets the burst traffic value for egress traffic.

Attention:

1. When the rate limit is below 640 K, the burst value should be set to 64 K.
2. When the rate limit is above 640 K, the burst value must not exceed 1/10 of the rate limit.
3. A larger burst value may result in greater fluctuations in the actual rate-limiting performance. Likewise, longer packet frame lengths may also cause greater fluctuations in the actual rate.

4.3 Storm Suppression

The storm control function is used to rate-limit broadcast packets, unknown multicast packets, and unknown unicast packets. It restricts ingress and egress traffic on each port to a specified range, thereby effectively suppressing network storms. The Storm Suppression page is shown in Figure 17.

Port	Broadcast	Unknown Multicast	Unknown Unicast	Storm Unit
G1	1000	-	-	pps
G2	1000	-	-	pps
G3	1000	-	-	pps
G4	1000	-	-	pps
G5	1000	-	-	pps
G6	1000	-	-	pps
G7	1000	-	-	pps
G8	1000	-	-	pps
G9	1000	-	-	pps
G10	1000	-	-	pps
G11	1000	-	-	pps
G12	1000	-	-	pps
G13	1000	-	-	pps
G14	1000	-	-	pps
G15	1000	-	-	pps
G16	1000	-	-	pps

Picture 17 Storm suppression setting interface

Each configuration item is described as follows:

Port : Port set to be configured, which cannot be entered manually, but can only be selected below.

Broadcast: broadcast data packets limit rate, unit pps, range 0~100000, default value 1000.

Unknown Multicast: The rate limit of multicast packets, in pps, range from 0 to 100000, the default value is disable.

Unknown unicast: Unknown unicast packet rate limit, unit pps, range 0 to 100000, the default value is disable.

Attention:

1. The Reset button restores the selected port parameters to their default values. The default broadcast storm control threshold is 1000 pps.

4.4 Storm Detection

The Storm Detection page provides port-based packet-type detection for broadcast and multicast traffic. Users can enable or disable broadcast and multicast detection on each port and manually configure the corresponding detection thresholds. The threshold range is 0–1,000,000 pps, with a minimum granularity of 1 pps.

When the real-time traffic on a port exceeds the configured threshold, the specified action is triggered and the recovery timer starts. After the recovery time expires, the port returns to normal operation and traffic detection resumes.

Two trigger actions are available:

Block: Blocks the port.

Down: Disables the port.

The device supports rate monitoring for two packet types:

Broadcast packets: The number of broadcast packets received per second.

Multicast packets: The number of multicast packets received per second.

For ports with storm detection enabled, the corresponding real-time broadcast and multicast traffic rates are displayed. The Storm Detection page is shown in Figure 18.

Modify

* Port List:

☐ G1☐ G2☐ G3☐ G4☐ G5☐ G6☐ G7☐ G8☐ G9
☐ G10☐ G11☐ G12☐ G13☐ G14☐ G15☐ G16☐ X1☐ X2
☐ X3☐ X4☐ All

* Broadcast Detect:

☐ Enable☒ Disable

pps(0~14881000)

* Multicast Detect:

☐ Enable☒ Disable

pps(0~14881000)

* Unicast Detect:

☐ Enable☒ Disable

pps(0~14881000)

* Trigger Action:

☒ down☐ block

* Recovery Time:

60

s(3~36000)

ResetCancelConfirm

Broadcast Packets: Configures broadcast packet detection for each port. The available rate range depends on the actual device model.

18/60

Unicast Packets: Configures unicast packet detection for each port. The available rate range depends on the actual device model.

Trigger Action: Configures the action to be triggered on each port. Two actions are available: Block (blocks the port) and Down (disables the port).

Recovery Time: Specifies the time interval from when a trigger action is activated until the port returns to its normal state.

Real-Time Port Status: Displays Forward when the port is in the normal link or forwarding state, Block when the port is blocked, and Down when the port is disabled.

Real-Time Broadcast Traffic: Displays the real-time broadcast traffic rate after storm detection is enabled on the port.

Real-Time Multicast Traffic: Displays the real-time multicast traffic rate after storm detection is enabled on the port.

Modify: After configuring the above items, click this button to apply the settings.

Reset: Restores all selected configuration items to their default values.

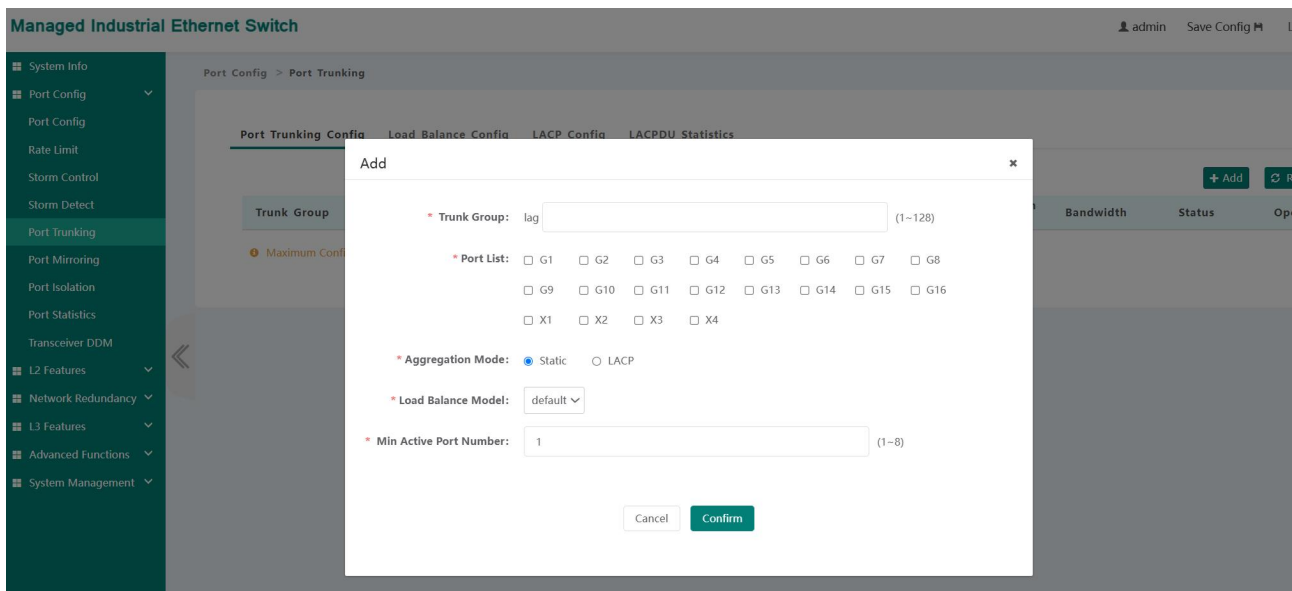
Attention:

1. The Storm Detection function cannot be used simultaneously with link redundancy functions such as ring networking, ERPS, port mirroring, link aggregation, and MSTP. Otherwise, ports blocked by these redundancy mechanisms may be affected by Storm Detection, which may interfere with the normal operation of the redundancy functions.
2. Multicast traffic detected by the Storm Detection function includes both known multicast and unknown multicast traffic. Therefore, the traffic volume of known multicast should be taken into account when setting the multicast threshold.

4.5 Port Aggregation

4.5.1 Static Aggregation

The static aggregation function binds multiple physical ports into one logical port, increasing the bandwidth between switches. As shown in Figure 19.



Picture 19 static aggregation

Each configuration item is described as follows:

Trunk Group: The ID of the static aggregation group. The specific range is subject to the actual model.

Port List: The interface name of the static aggregation group.

Aggregation Mode: List of ports added to the static aggregation group.

Load balancing Mode: The load balancing mode of the static aggregation group is divided into six modes: src-mac, dst-mac, src-dst-mac, src-ip, dst-ip, and src-dst-ip. The default mode is Src-Dst-Ip.

Main Active Port Number: 1-8 available

Attention: The load-balancing mode is globally unique for all aggregation groups. After the load-balancing mode is modified, the new setting is automatically applied to all other aggregation groups, including both static aggregation groups and LACP groups.

When a new aggregation group is created without specifying a load-balancing mode, the default load-balancing mode will take effect globally.

4.5.2 LACP

LACP binds physical ports to logical ports, and only ports that pass the negotiation are allowed to bind, and others are not allowed. As shown in Figure 20.

System Info
Port Config
Port Config
Rate Limit
Storm Control
Storm Detect
Port Trunking
Port Mirroring
Port Isolation
Port Statistics
Transceiver DDM
L2 Features
Network Redundancy
L3 Features
Advanced Functions
System Management

Port Config > Port Trunking

Port Trunking Config
Load Balance Config
LACP Config
LACPDU Statistics

Trunk Group	Aggregation Mode	Member Ports	Load Balance Model	Min Active Port Number	Max Active Port Number	LACP Preemption	LACP Election Method	Bandwidth	Status	Oper
lag1	LACP	G1 G2	default	1	8	Enable	Port Priority	-	down	

Maximum Configurable Number: 20

The first section is used to modify dynamic aggregation system attributes, create or delete dynamic aggregation groups, add or remove member ports, modify the load-balancing mode of a dynamic aggregation group, and configure the attributes of its member ports. The second section displays the member list and load-balancing mode of each dynamic aggregation group. The third section displays the connection information of the specified dynamic aggregation group.

The configuration items are described as follows:

Port: the member port to be added to the aggregation group.

Group ID: the ID of the dynamic aggregation group. The supported range depends on the actual device model.

Mode: the operating mode of the port. Two modes are available: Active and Passive.

LACP System Priority: the system priority of the dynamic aggregation group, which is used to determine the priority between the devices at both ends of the link. The valid range is 0–65535.

Port Priority: the priority of a member port in the dynamic aggregation group. It is used to determine which member ports have higher priority to become selected ports. The valid range is 0–65535.

Port Timeout Mode: the timeout mode of a member port in the dynamic aggregation group and determines the timeout interval for the peer device. Two modes are available: Long and Short.

Link: Displays the LACP negotiation status of a port in the dynamic aggregation group. Ready indicates that the port has been successfully aggregated. Individual indicates that the port is in standby status and has not been selected for aggregation. Ports that are not displayed in the table do not meet the negotiation requirements.

Load Balancing: the load-balancing mode of the dynamic aggregation group. Six modes are available: Src-Mac, Dst-Mac, Src-Dst-Mac, Src-Ip, Dst-Ip, and Src-Dst-Ip. The default mode is Src-Dst-Ip.

The aggregation group information is described as follows:

Aggregator: Consists of the aggregation group name + aggregation group index ID and serves as the unique local identifier of the aggregation group.

LAG ID: Consists of the system priority + system MAC address and serves as the negotiation identifier of the aggregation group. It can be used during port negotiation within the aggregation group.

Key: the Key value of the dynamic aggregation group, which generally corresponds to the aggregation group ID.

Receive Link Count: Displays the number of ports in the dynamic aggregation group that are enabled for receiving traffic.

Transmit Link Count: Displays the number of ports in the dynamic aggregation group that are enabled for transmitting traffic.

4.5.3 LACP Port Information

The LACP port information page displays the detailed configuration and status information of the member ports of the dynamic aggregation group, as shown in Figure 21.

端口配置 >> 端口汇聚 >> LACP端口信息

动态汇聚端口信息

端口: ge3

详细信息:

LACP link info:	ge3 - 5003
LAG ID:	32768,00-00-00-00-00-0c
Partner oper LAG ID:	32768,00-01-90-aa-bb-cc
Actor priority:	0x8000 (32768)
Admin key:	0x0001 (1)
Oper key:	0x0001 (1)
Physical admin key:	0x0001 (1)
Receive machine state :	Current
Periodic Transmission machine state :	Slow periodic
Mux machine state :	Collecting/Distributing
Oper state:	ACT(1) TIM(0) AGG(1) SYN(1) COL(1) DIS(1) DEF(0) EXP(0)
Partner oper state:	ACT(0) TIM(0) AGG(1) SYN(1) COL(1) DIS(1) DEF(0) EXP(0)
Partner link info:	admin port 0
Partner oper port:	2
Partner admin LAG ID:	(32768)00-00-00-00-00-00
Admin state:	ACT(1) TIM(0) AGG(1) SYN(0) COL(0) DIS(0) DEF(1) EXP(0)
Partner admin state:	ACT(0) TIM(0) AGG(1) SYN(0) COL(0) DIS(0) DEF(1) EXP(0)
Partner admin system priority:	32768
Partner oper system priority:	32768
Aggregator ID:	5018

刷新

此部分没有

Figure 21 LACP port information page

This page displays detailed information about each port in the aggregation group. Some of the parameters are described as follows:

LACP Link Info: Consists of the port name + port index ID and serves as the unique local identifier of the port.

Admin/Oper Key: Indicates the Key value of the member port used during aggregation negotiation.

Physical Admin Key: Indicates the Key value assigned to the interface based on the physical attributes of the port.

Mux Machine State: Indicates the MUX state of the port. When the value is Collecting/Distributing, the port has successfully completed LACP negotiation.

4.6 Port mirroring

The port mirroring function is to copy the data in the specified direction of one or more mirrored ports to the monitoring port, and observe the data of the mirrored port through the monitoring port. Port mirroring is commonly used to troubleshoot, debug, and analyze networks. As shown in Figure 22.

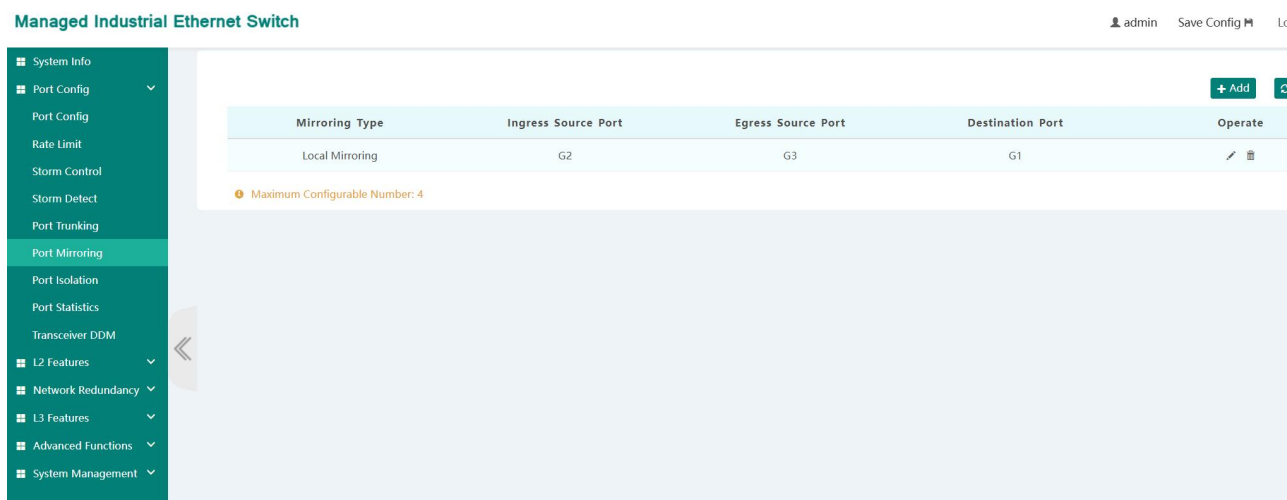


Figure 22 Port mirroring page

Each configuration item is described as follows:

Monitoring port: The monitoring port, which can only be unique, monitors the data in the specified direction of the mirror port.

Ingress Source Port: Mirrors incoming (RX) traffic from the selected source port to the monitoring port.

Egress Source Port: Mirrors outgoing (TX) traffic from the selected source port to the monitoring port.

Direction Port: The data collection direction of the mirror port, divided into inbound direction, outbound direction and bidirectional.

Attention:

1. Multiple mirroring groups can be configured, but the maximum number of groups depends on the actual device model.
2. Within a mirroring group, multiple mirrored ports can be configured, but only one monitoring port is allowed.
3. Across all mirroring groups, each monitoring port and mirrored port must be unique and cannot be reused.
4. Port mirroring is mainly intended for debugging and troubleshooting. Under normal operating conditions, it should be disabled; otherwise, other functions on the mirrored ports may be affected or become unavailable.

4.7 Port Isolation

The port isolation function is used to prohibit data forwarding between different ports in a VLAN. Ports

with isolation enabled cannot communicate; ports without isolation, or between isolated ports and un-isolated ports, can communicate normally. As shown in Figure 23.

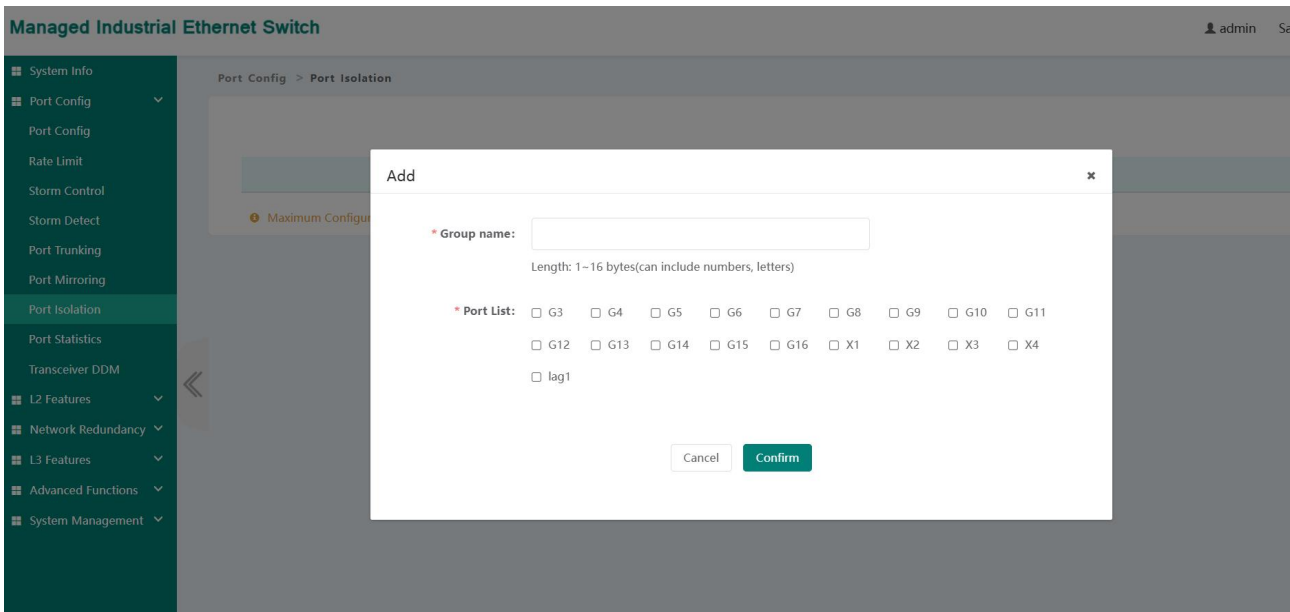


Figure 23 Port Isolation Page

After selecting ports from the list, you can configure whether to enable port isolation at the top.

Each configuration item is described as follows:

Group Name: The name of Port Isolation group(1~16 bytes)

Port list: Select the ports to be added to this isolation group.

Caution

1. Port isolation can only be configured on Layer 2 interfaces.
2. Port isolation cannot be configured on aggregation group or aggregation group member ports.
3. All ports share an isolation group.

5 Layer 2 Features

5.1 VLAN

VLAN (Virtual Local Area Network) refers to the virtual local area network technology, which divides a physical LAN into multiple logical LANs, and each VLAN is a broadcast domain. Hosts in a VLAN exchange packets through traditional Ethernet communication. Hosts in different VLANs cannot communicate directly so they need the assistance of Layer 3 network devices.

5.1.1 VLAN Configuration

As show in Figure 24:

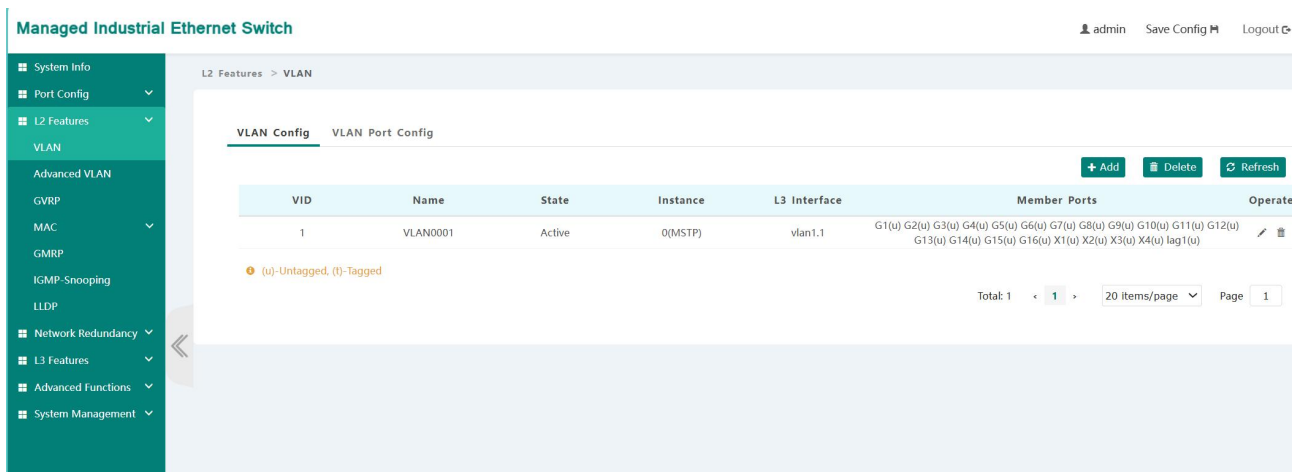


Figure 24 VLAN Configuration Page

Each configuration item is described as follows:

VLAN ID: range from 2 to 4094. Use "-" to connect in batch configuration.

Name: the name of VLAN.

State: active or suspended, default active.



Caution

1. It is recommended to batch create or delete a maximum of 100 VLANs at a time.

5.1.2 Port VLAN

As show in Figur 25:

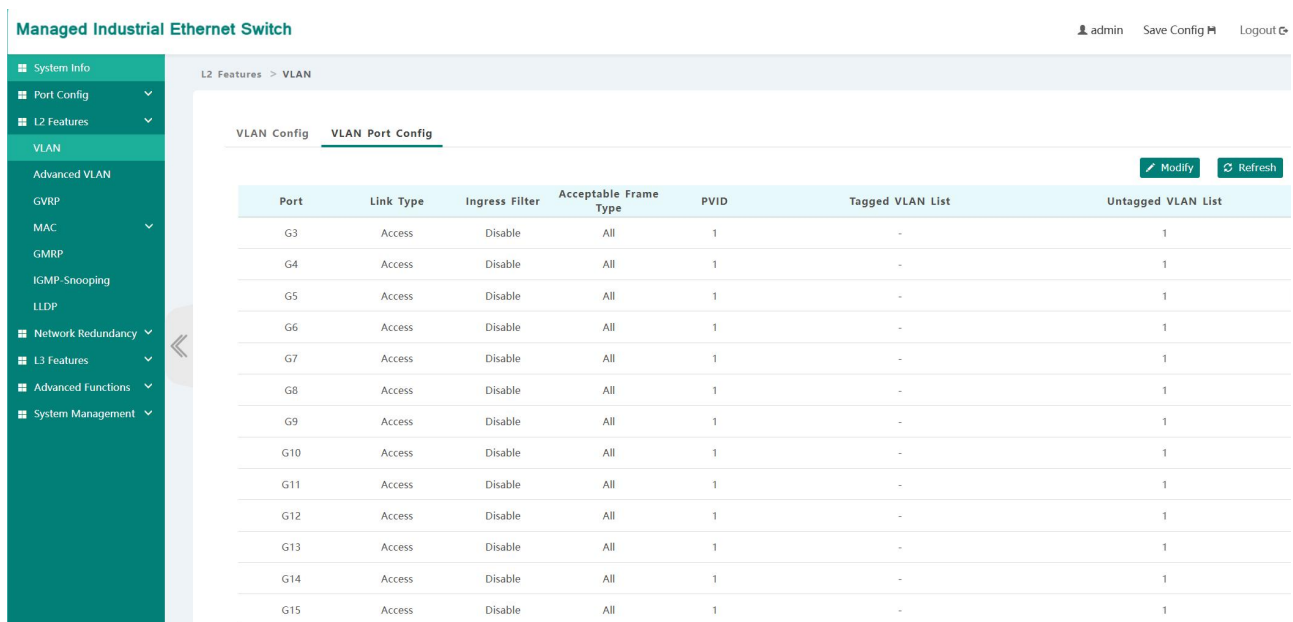


Figure 25 Port VLAN Page

Each configuration item is described as follows:

Port: The set of Layer 2 ports whose properties need to be modified.

Link Type: The optional link type is Access, Trunk or Hybrid, and the default is Access.

Ingress Filter: Enable or disable, disabled by default.

Acceptable Frame Type: All means receiving all packets, Vlan-untagged means only receiving packets without VLAN tags, Vlan-tagged means only receiving packets with VLAN tags, the default is All.

 **Caution**

1. The VLAN attributes of different types of ports cannot be set at the same time.
2. After modifying the link type first, then you can set Allowed VLAN ID, Egress-tagged and Default VLAN ID.

5.1.3 MAC VLAN

As show in Figure 26:

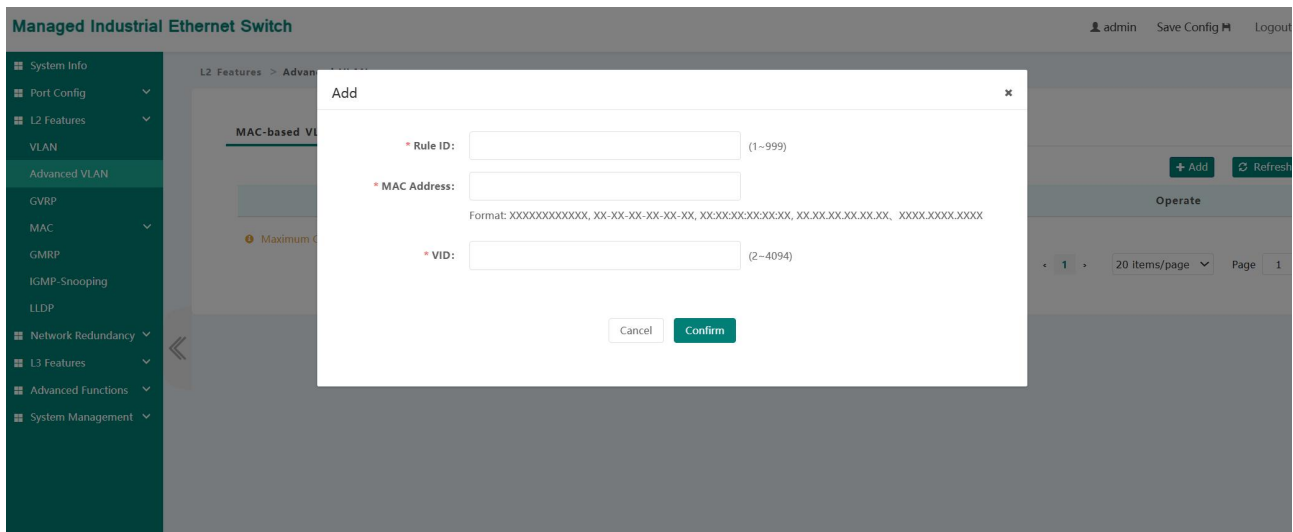


Figure 26 MAC VLAN Page

Each configuration item is described as follows:

Rule ID: Identifies the MAC VLAN rule, ranging from 1 to 999.

MAC Address: The MAC address to which the VID needs to be assigned.

VID: The VID to be allocated, ranging from 2 to 4094.

 **Caution**

1. Only one rule can be configured per MAC, that is, only one VID can be assigned to each MAC.

5.1.4 Subnet VLAN

As show in Figure 27:

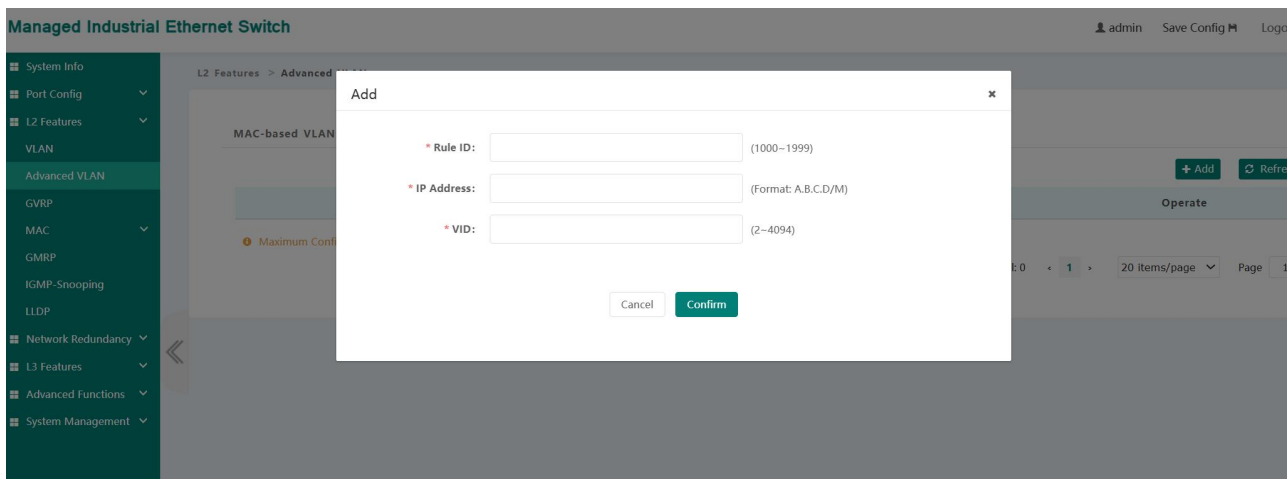


Figure 27 Subnet VLAN Page

Each configuration item is described as follows:

Rule ID: Identifies the subnet VLAN rule, ranging from 1000 to 1999.

IP Address: The subnet network segment to which the VID needs to be assigned.

VID: The VID to be allocated, ranging from 2 to 4094.



1. Only one rule can be configured for each subnet segment, that is, only one VID can be assigned to each subnet segment.

5.1.5 Protocol VLAN

As show in Figure 28:

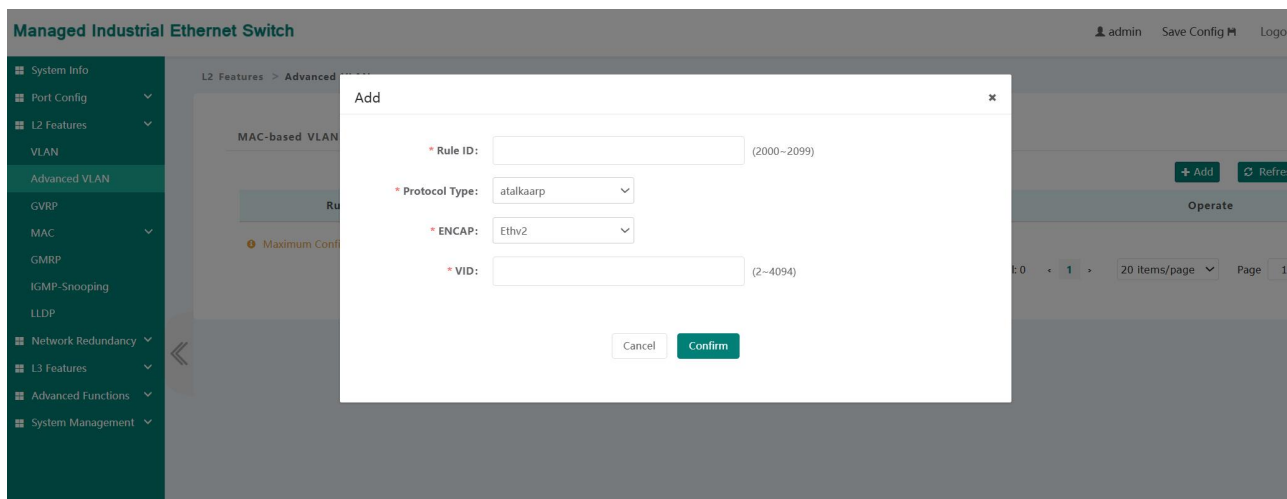


Figure 28 Protocol VLAN Page

Each configuration item is described as follows:

Rule ID: identifies the protocol VLAN rule, ranging from 2000 to 2099.

Protocol Type: The protocol type for which VID needs to be assigned.

ENCAP: Layer 2 encapsulation type; supports three types: ethv2, nosnapllc, and snapllc.

VID: The VID to be allocated, ranging from 2 to 4094.

⚠ Caution

1. Only one rule can be configured for each protocol, that is, only one VID can be assigned to each protocol.

5.1.6 VLAN Roles

Configure VLAN mapping rules for ports: including MAC, subnet and protocol-based VLAN rules. As shown in Figure 29:

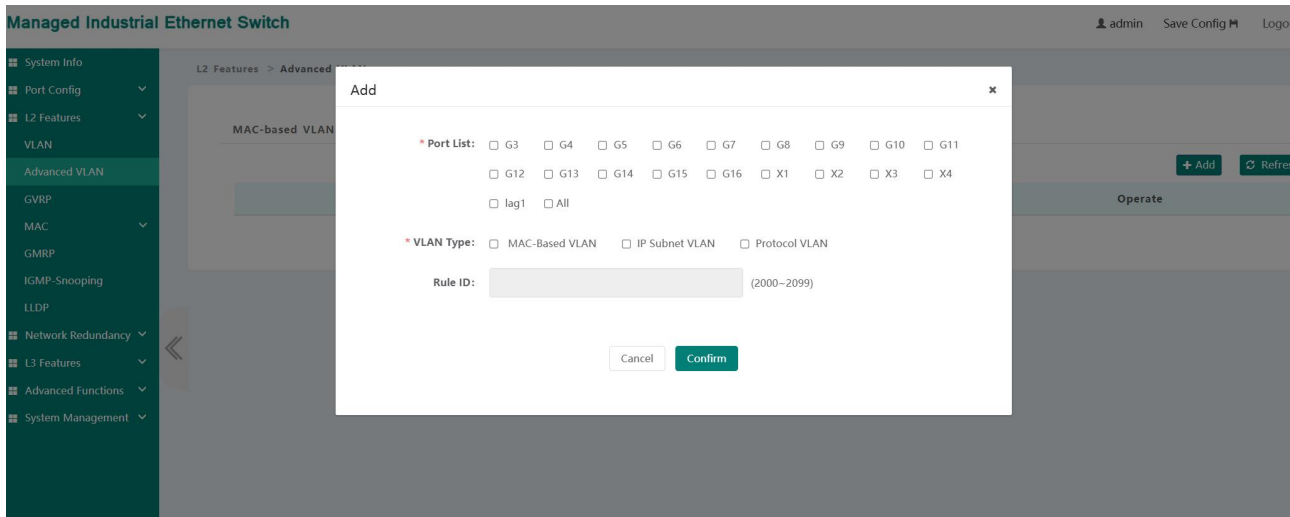


Figure 29 VLAN Rules Page

Each configuration item is described as follows:

Port List: Ports to which VLAN rules are applied.

VLAN Type: The VLAN type used by the port, there are three options: MAC-Based VLAN, IP Subnet VLAN, Protocol VLAN.

⚠ Caution

1. VLAN rules based on MAC, subnet and protocol must be enabled to take effect.

5.2 MAC

5.2.1 MAC Address Table List

The MAC address table is a port-based Layer 2 forwarding table and is the basis for fast forwarding of packets. The MAC address table contains several forwarding entries, and each forwarding entry has a corresponding destination MAC, port VID, and forwarding port. As shown in Figure 30:

Figure 30 MAC Address Table Page

Each configuration item is described as follows:

MAC Address: Delete the dynamic forwarding entry of the specified MAC address.

VLAN: Delete the dynamic forwarding entry of the specified VLAN.

Port: Delete the dynamic forwarding entry of the specified port. MAC address entry type.

Type: MAC address entry type.

Aging Time: unit s, range 0, 10~100000, default 300s. 0 means no aging.

Caution

1. Delete and clear only for dynamic MAC entries.
2. The clear operation deletes all dynamic MAC entries.

5.2.2 Static MAC

This function is used to configure the forwarding and filtering of static unicast MAC addresses:

- ☐ The static MAC does not age, and the packets matching the MAC and VLAN in the static MAC forwarding table are forwarded to the specified port.
- ☐ MAC filtering is a security mechanism that applies to all ports. Packets matching the MAC and VLAN in the MAC filtering list are filtered by all ports. As shown in Figure 31:

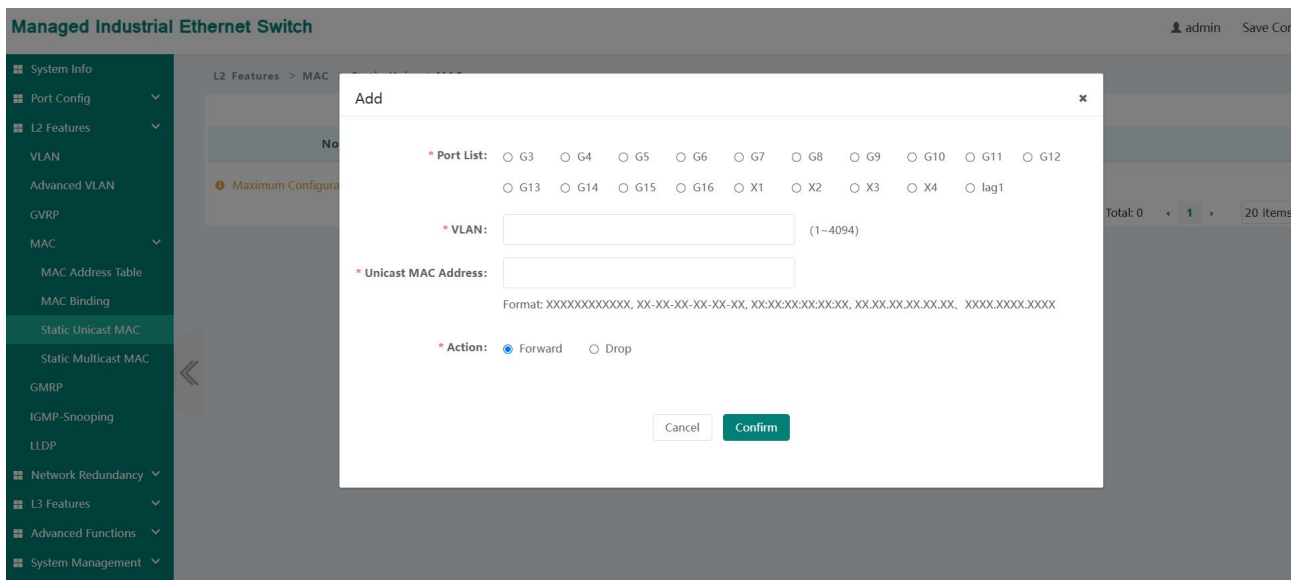


Figure 31 Static MAC Page

Each configuration item is described as follows:

Port List: Select the port(s) to which this static MAC address is bound

VLAN: The VLAN to which the static MAC belongs.

Unicast MAC Address: Static unicast MAC address.

Action: Operation applied to frames matching this static MAC entry. Forward: Forward the frames normally. Drop: Discard the frames.

 **Caution**

1. MAC filtering, also known as black hole MAC, is a security mechanism that will cause specified packets to fail to pass through the switch. Please use it as appropriate.
2. Static MAC and black hole MAC do not age out automatically and can only be deleted manually.

5.2.3 MAC Binding

MAC binding binds the port to the specified MAC. Only the packets whose source MAC or destination MAC is equal to the binding MAC can be received and forwarded by the specified port, and all other packets are discarded. As shown in Figure 32:

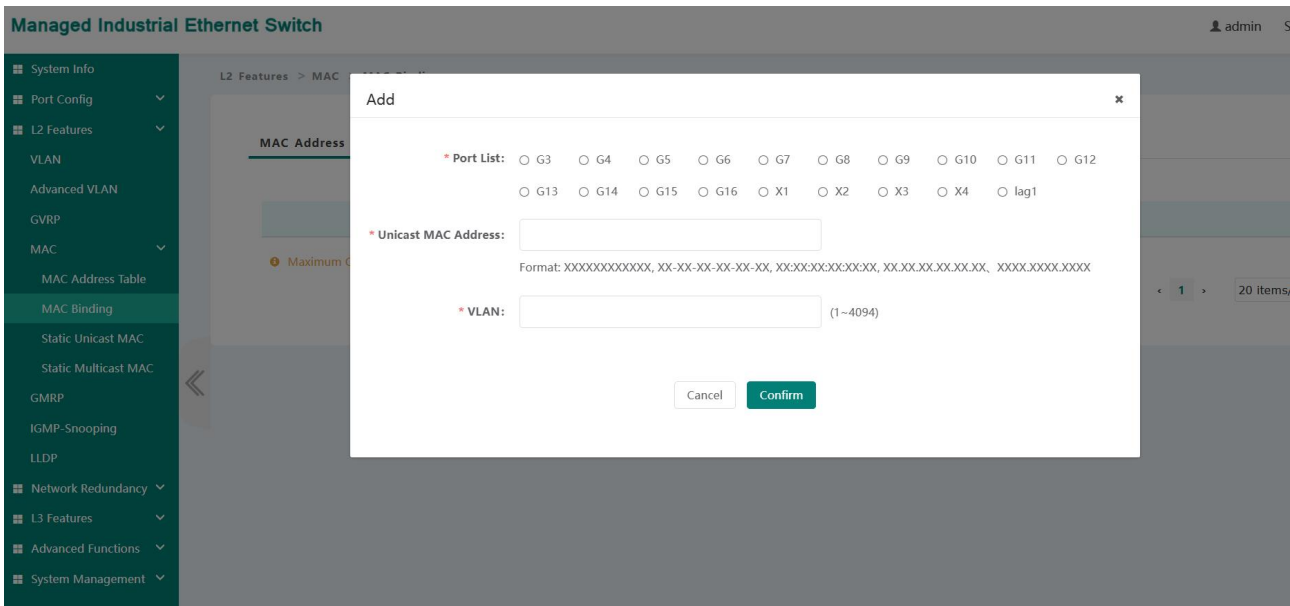


Figure 32 MAC Binding Page

Each configuration item is described as follows:

Port List: The port bound to the MAC.

Unicast MAC Address: The unicast MAC bound to the port.

VLAN: Bind the corresponding VLAN.

 **Caution**

1. MAC binding binds the port to the MAC, which causes other packets to fail. Please use it with caution.
2. MAC binding is for the specified port, and MAC filtering is for all ports.
3. The bound MAC address does not age out automatically and can only be deleted manually.

5.2.4 MAC Automatic Binding

As shown in Figure 33:

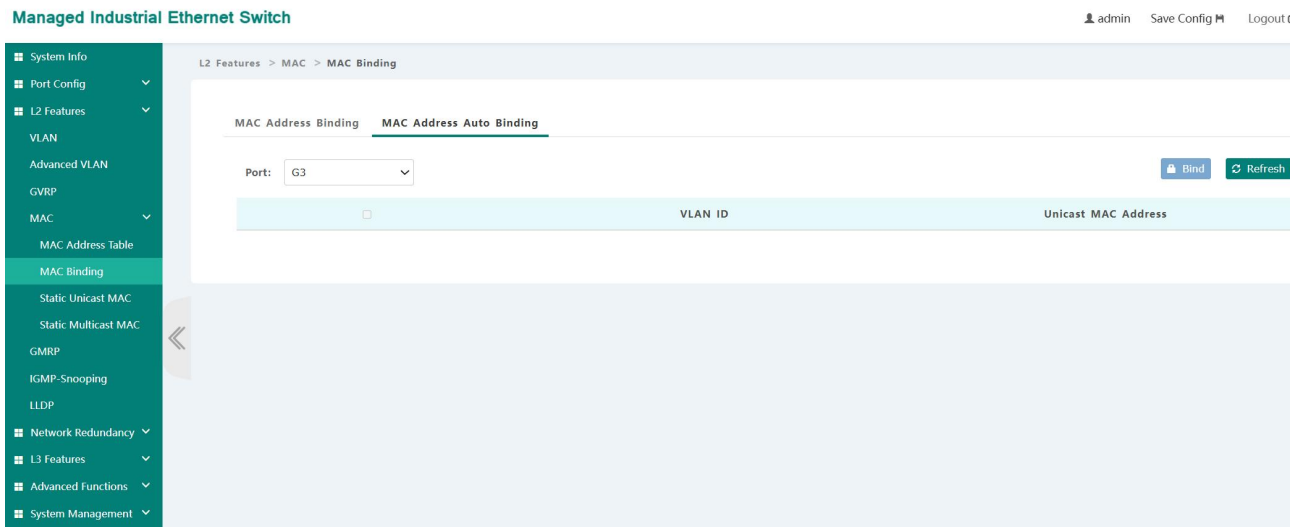


Figure 33 MAC Automatic Binding Page

MAC auto binding is a complement to MAC binding. First select the port, and the page will display all

dynamic MACs under this port; then select the entry and click "Bind" to automatically bind the MAC to the port.

5.3 Multicast

5.3.1 IGMP-Snooping

The IGMP Snooping (Internet Group Management Protocol Snooping) function page is shown in Figure 34:

The screenshot shows the 'Managed Industrial Ethernet Switch' interface. On the left is a sidebar with a tree view containing 'System Info', 'Port Config', 'L2 Features', 'VLAN', 'Advanced VLAN', 'GVRP', 'MAC', 'GMRP', 'IGMP-Snooping' (highlighted), 'LLDP', 'Network Redundancy', 'L3 Features', 'Advanced Functions', and 'System Management'. The main panel is titled 'L2 Features > IGMP-Snooping'. It shows a configuration for a specific VLAN with a 'VLAN ID' field. Below this, there are several configuration items: 'IGMP-Snooping Status' (radio buttons for Enable and Disable), 'Unknown Multicast Flow' (a dropdown menu set to 'Flooding'), 'IGMP Version' (a dropdown menu set to 'IGMPv3'), 'IGMP Fast Leave' (radio buttons for Enable and Disable), 'IGMP Querier' (radio buttons for Enable and Disable), 'IGMP Query Time Interval' (a text input set to '125' with a range '(1~18000)'), 'IGMP Query Source IP' (a text input with a format hint '(Format: A.B.C.D)'), and 'Maximum Groups Count' (a text input with a range '(1~1023)'). A modal window titled 'Add' is overlaid on the main panel, containing the same configuration fields. At the bottom of the modal are 'Cancel' and 'Confirm' buttons.

Figure 34 IGMP Snooping Page

Each configuration item is described as follows:

VLAN ID: VLAN ID of IGMP Snooping, range: 1 to 4094.

IGS Status: Enable/disable the IGMP Snooping function in the vlan, disabled by default.

Unknown Multicast Flow: Specifies how to handle multicast traffic when no matching group entry exists.

IGS Version: The version of the IGMP protocol in the vlan, the default version is IGMPv3.

IGMP Fast Leave: Enable/disable IGMP quick leave group in vlan, disabled by default.

IGMP Querier: Enable/disable the IGMP querier within the vlan, disabled by default.

Query Time Interval: The time interval for sending general query packets within the vlan, the range is 1 to 18000 seconds, and the default is 125 seconds.

Source IP: The source IP address of the intra-VLAN query packet must be a valid unicast IP address. The default value of 0.0.0.0 means not specified.

Max Group Num: The maximum number of groups allowed in the vlan, the range is 1 to 1023.



1. The querier's query packet source IP must be a valid unicast IP. When the querier is disabled, the

default value is 0.0.0.0.

5.3.2 Static Multicast

Static multicast is used to configure and display static multicast groups within a vlan. Once a port joins a static multicast group, it can receive data for that group without needing to actively join it. As shown in Figure 35:

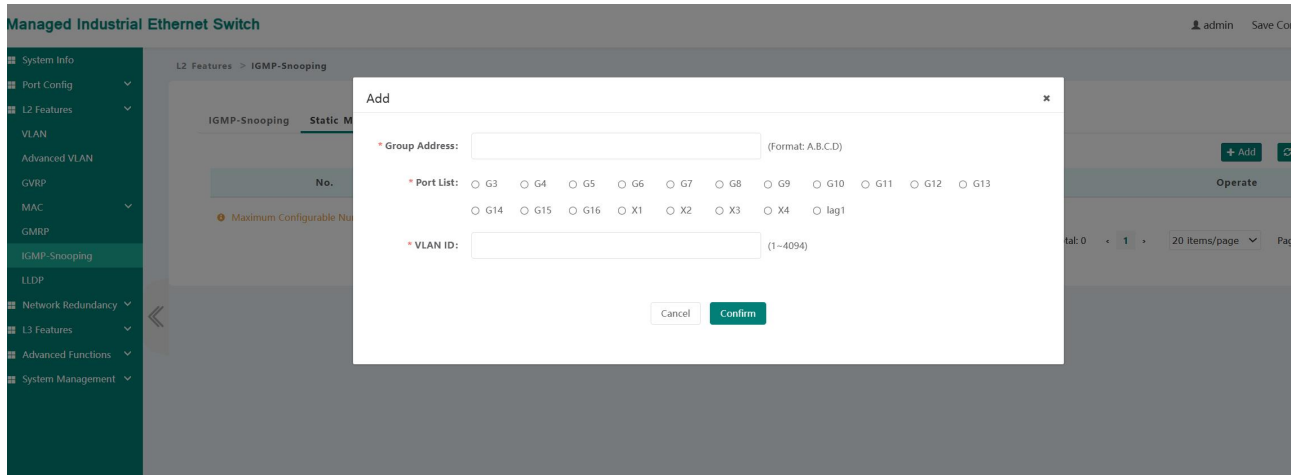


Figure 35 Static Multicast Page

Static Multicast Configuration: Configure static multicast groups within a VLAN.

Static Multicast Table: Displays all configured static multicast group entries.

Each configuration item is described as follows:

Group Address: The statically added multicast group address, ranging from 224.0.1.0 to 239.255.255.255.

Port List: The physical port bound by static multicast.

VLAN ID: static multicast VLAN ID, range: 1 to 4094.



Caution

1. The static multicast table of the VLAN can be configured only after IGMP Snooping of the VLAN is enabled.
2. Disabling the IGMP snooping function within a VLAN will clear any existing static multicast groups in that VLAN.
3. The static multicast table does not age and can only be deleted manually.
4. If the same entry is both a static multicast group and a dynamically learned multicast group, it is displayed only on the "Static Multicast" page.
5. Static multicast and IGMP snooping share a combined limit of 1,023 multicast group entries on the device; for example, if 23 static multicast groups are already configured, IGMP snooping can dynamically learn a maximum of only 1,000 multicast groups. When used independently, IGMP snooping allows up to 1,023 group entries, whereas static multicast allows up to 128 entries.

5.4 LLDP

LLDP Link Layer Discovery Protocol is a neighbor discovery protocol that defines a standard method for

Ethernet network devices, such as switches, routers, and wireless LAN access points, to advertise their presence to other nodes in the network, and save discovery information for nearby devices.

5.4.1 LLDP Configuration

As shown Figure 36:

The screenshot shows the 'LLDP Global Config' page. On the left is a navigation menu with categories like System Info, Port Config, L2 Features, L3 Features, Advanced Functions, and System Management. Under L2 Features, LLDP is selected. The main area has tabs for LLDP Global Config, LLDP Port Config, LLDP Local Information, LLDP Neighbor Information, and LLDPDU Statistics. The 'LLDP Global Config' tab is active, displaying four configuration items: 'Protocol State' with radio buttons for 'Enable' and 'Disable' (Disable is selected), 'Transmit Interval' with a text box containing '30' and a range '(5~32768)', 'Hold Multiplier' with a text box containing '4' and a range '(2~10)', and 'Reinit Delay' with a text box containing '2' and a range '(1~10)'. At the bottom right are 'Reset', 'Cancel', and 'Submit' buttons.

Figure 36 LLADP Configuration Page

Each configuration item is described as follows:

LLDP Protocol State: Enable/disable global LLDP, the default is disabled.

LLDPDU Tx Interval: The interval for sending global LLDP packets, the range is 5 to 300 seconds, and the default is 30 seconds.

Hold Multiplier: Multiplier used to calculate the LLDP neighbor aging time. Aging time = Transmit Interval × Hold Multiplier. Range: 2–10.

Reinit Delay: Delay before LLDP reinitializes and starts transmitting after a port is re-enabled. Range: 1–10 seconds.

⚠ Caution

1. In the working mode of LLDP, Tx means only sending but not receiving, Rx means only receiving but not sending, TxRx means both sending and receiving, Disable means neither sending nor receiving.
2. If the port is not configured with an LLDP management address, the primary IP address of the VLAN with the lowest VLAN ID (among those allowed on the port) is selected as the LLDP management address by default. If the VLAN to which the port belongs is not configured with a primary IP or the port is disconnected, the port's LLDP management address defaults to the loopback address 127.0.0.1 in this case. The management address is not updated in real time; in most instances, an LLDP packet must be transmitted from the port for the address to be updated.

6 Ring Redundancy

6.1 Loopback Detection

A loop in the network will cause the device to repeatedly send broadcast, multicast, and unknown

unicast packets, resulting in wasted network resources or even network paralysis. In order to detect loops in the Layer 2 network in time and avoid serious impact on the entire network, loopback detection provides a detection function, so that when a loop occurs in the network, users can be notified to check the network connection and configuration in time, and make the problematic interface under control. Loopback detection periodically sends detection packets to check whether the packets are returned to the device, and then determines whether there is a loop between the interface, the network connected to the device, or the dual interfaces of the device. After a loop is found, the loopback detection sends an alarm and records a log to the NMS, and processes the interface according to the configuration, so that the interface is in a controlled state, reducing the impact of the loop on the device and the entire network. As shown in Figure 37.

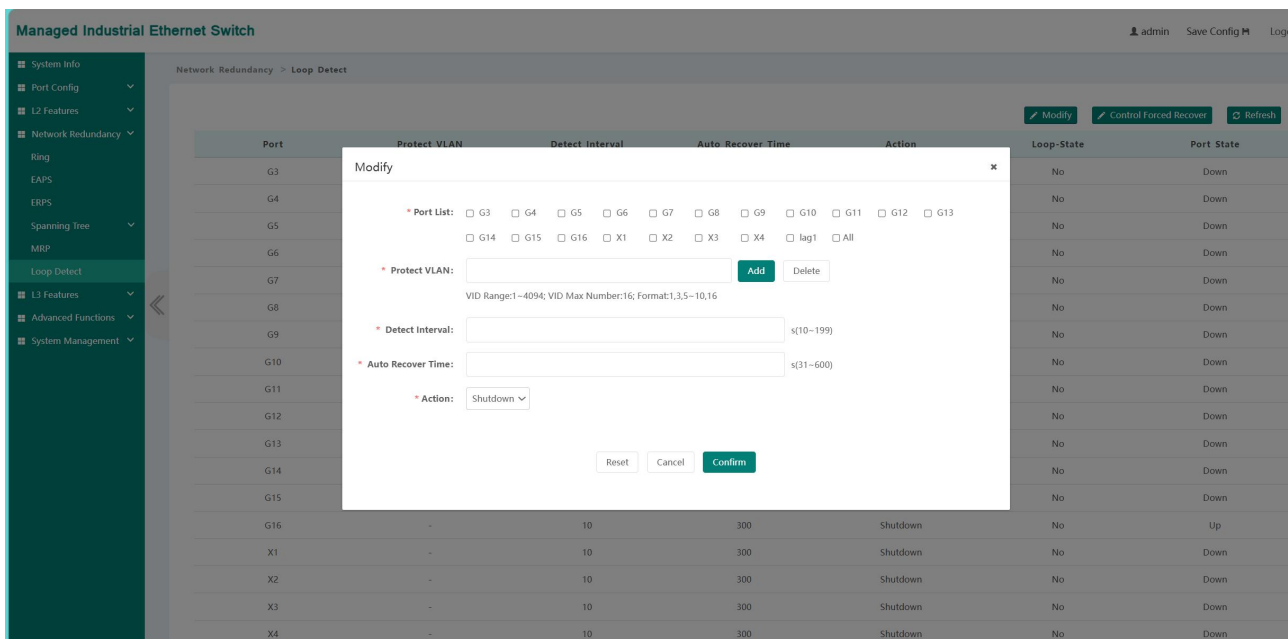


Figure 37 Loopback detection page

This is the loopback detection page.

Each configuration item is described as follows:

Port List: Select the ports to which loopback detection is applied.

Protect VLAN: The VLAN ID corresponding to loopback detection.

Detect Interval: The interval for sending loopback detection packets.

Auto Recover time: The interface in the controlled state, after the auto-recovery time elapses, the state returns to up, and the loopback detection is restarted.

Action: After loopback detection is enabled, the response action of the interface when a loop exists.



Caution

1. The recovery time should be greater than 3 times the detection packet sending period.

6.2 Fast Ring Network

6.2.1 RingV2

RingV2 is an upgraded version of Ring, which belongs to the company's private fast ring network

technology. When the network connection is interrupted, the ring network redundancy mechanism immediately enables the backup link to quickly restore the network communication. As shown in Figure 38.

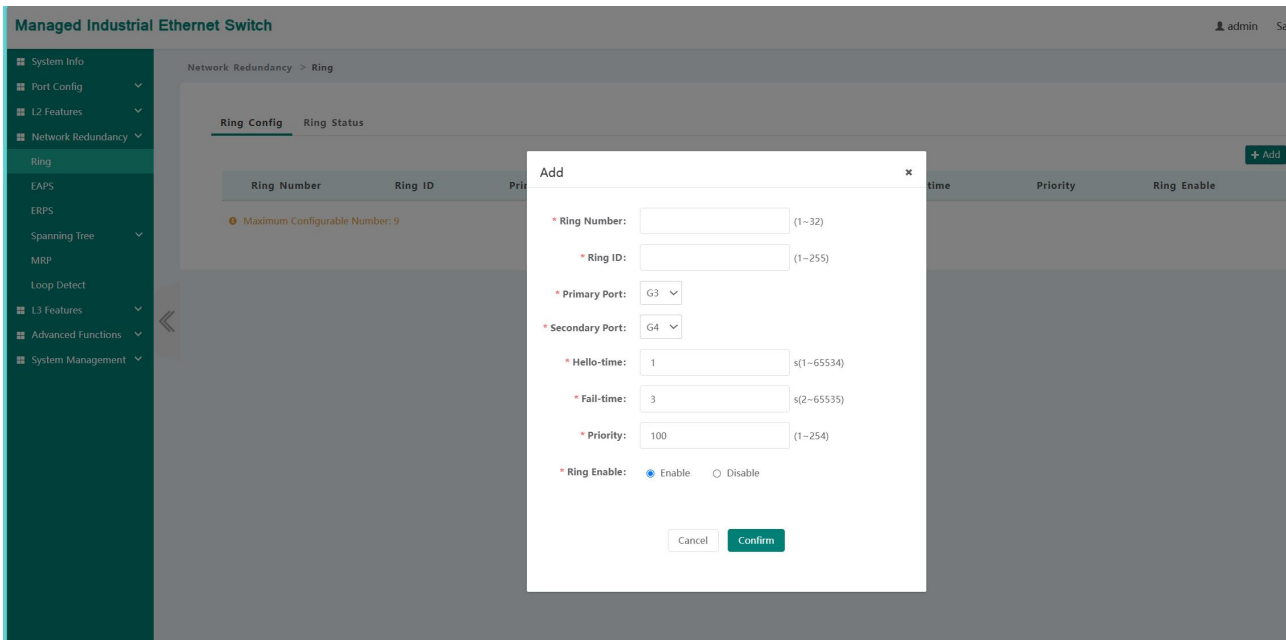


Figure 38 RingV2 page

The page is the Add configuration page of RingV2 ring network.

Each configuration item is described as follows:

Ring Number: The number of the ring network group. Up to total number of ports / 2(rounded down) groups of fast ring networks can be enabled on each switch.

Ring ID: The network ID of the ring, ranging from 1 to 255.

Primary Port: The priority forwarding port of the ring network node.

Secondary Port: The priority blocking port of the ring network node.

Hello-time: The interval for sending hello packets on the ring network. The value ranges from 1 to 65534 seconds. The default value is 1 second.

Fail-time: Delay of the fail timer of the ring node. The value ranges from 2 to 65535 seconds. The default value is 3 seconds.

Priority: The priority of the ring node, the value ranges from 1 to 254, and the default value is 100.

Ring Enable: Enable or disable the ring network. This function is enabled by default.



Caution

1. Only ring network groups with complete configurations can be enabled.
2. The switches in the same ring network group use the same ring network ID.
3. Switches in different ring groups use different ring IDs.
4. When modifying the parameters of the ring network group, the ring network must be disabled first, and then enabled after the modification is completed.
5. A switch can be designated as the master node by configuring the priority. The smaller the value,

the higher the priority.

6. The Fail-Time of the ring network must be greater than the Hello-Time.
7. The master port and slave port cannot be the same port.
8. It is recommended not to enable fast ring/ERPS/EAPS/MSTP/port aggregation functions at the same time.

6.3 EAPS

EAPS is a link-layer Ethernet ring protection protocol that can simultaneously provide fast convergence and redundant link protection. When the ring network topology is complete, it blocks one link to prevent the broadcast storm caused by the loop. When a link failure occurs, it quickly restores the blocked link, re-establishing communication between nodes in the ring. As shown in Figure 39.

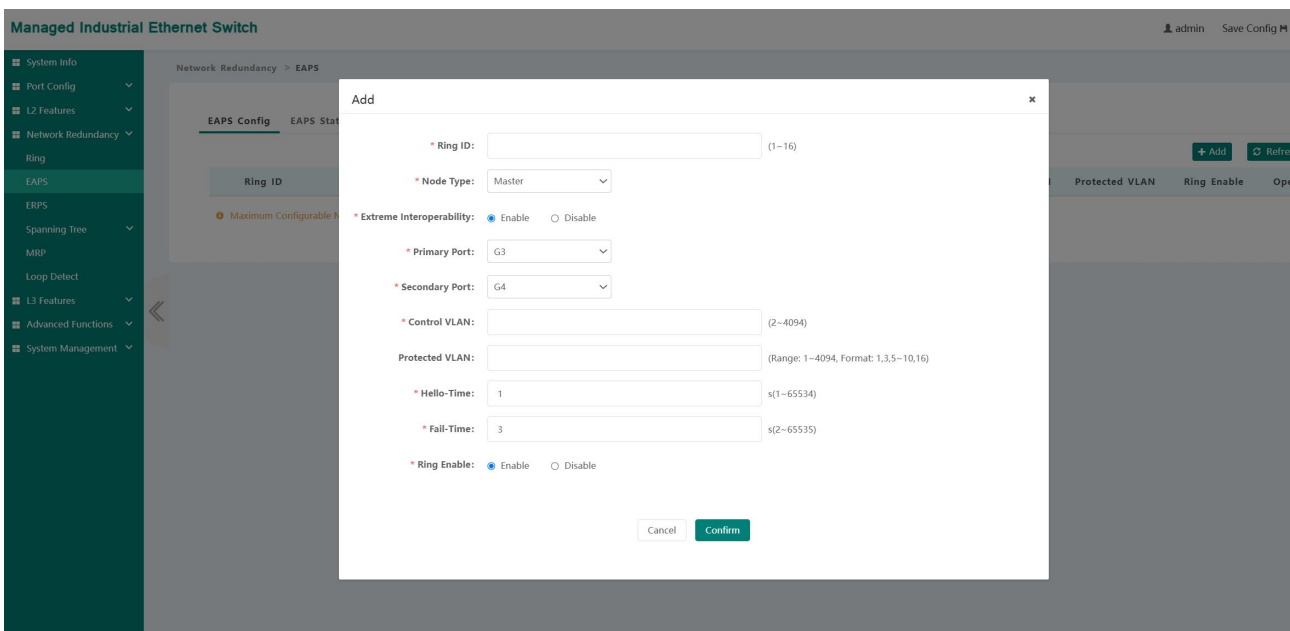


Figure 39 EAPS page

The page is the Add configuration page of EAPS ring network, used to create a new EAPS ring group.

Each configuration item is described as follows:

Ring ID: The ID of the ring network. The value ranges from 1 to 16.

Node Type: The mode of the switch in the ring, Master or Transit.

Extreme Interoperability: Compatible with Extreme EAPS packets.

Primary Port: The primary port of the node.

Secondary Port: Secondary port of the node.

Control VLAN: Control VLAN of the ring network. It is used to transmit protocol packets. The value ranges from 2 to 4094.

Protected VLAN: The ring network data VLAN used to transmit service data. The value ranges from 1 to 4094.

Hello-Time: The unit is s. The value ranges from 1 to 65534. The value of Fail-Time must be greater than the value of Hello-Time.

Fail-Time: The unit is s. The value ranges from 2 to 65535. The value of Fail-Time must be greater than the value of Hello-Time.

Ring Enable: Enables or disables the ring network. This function is enabled by default.



Caution

1. The Control VLAN and Data VLAN cannot be the same.
2. Nodes within the same EAPS ring must use the same control VLAN.
3. When modifying the parameters of the ring network, the ring network must be disabled first, and then enabled after the modification is completed.
4. Link redundancy protocols such as EAPS, Spanning Tree, ERPS, Fast Ring, and loopback detection cannot be enabled simultaneously.
5. The control VLAN cannot be a Layer 3 interface VLAN.
6. A port can belong to only one EAPS ring.
7. A ring port cannot be an aggregation port.

6.4 ERPS

ERPS (Ethernet Ring Protection Switching), the Ethernet multi-ring protection technology, is a layer-2 network redundancy protection method. It can prevent the broadcast storm caused by the loop when the Ethernet ring is complete, and can quickly restore the pass link of each node on the ring network when the Ethernet link fails, and has a high convergence speed.

The ERPS configuration page is shown in Figure 40.

The screenshot shows the 'Managed Industrial Ethernet Switch' configuration interface. On the left is a navigation menu with options like System Info, Port Config, L2 Features, Network Redundancy, Ring, EAPS, ERPS (selected), Spanning Tree, MRP, Loop Detect, L3 Features, Advanced Functions, and System Management. The main area is titled 'Network Redundancy > ERPS'. Below this, there are tabs for 'ERPS Config' and 'ERPS Ring'. The 'ERPS Config' tab is active, showing a table with columns 'Ring ID' and 'Protocol M...'. A modal dialog box titled 'Add' is open in the foreground, containing the following fields:

- * Ring ID: (1~255)
- * Protocol Dest Mac: 01:19:A7:00:00:01
- * Ring Type: Major
- * Node Type: Normal
- * East Port: G3
- * West Port: G4
- RPL Port: East Port
- Major Ring: (1~255)
- * Revertive Mode: Revertive
- * Control VLAN: (2~4094)
- Protected VLAN: (Range: 1~4094, Format: 1,3,5~10,16)
- * WTR: 5 min(1~12)
- * Guard: 500 ms(10~2000)
- * HoldOff: 0 ms(0~10000)
- * Ring Enable: ☒ Enable ☐ Disable

At the bottom of the dialog are 'Cancel' and 'Confirm' buttons.

Figure 40 ERPS page

The page is the Add configuration page of ERPS ring network, used to create a new ERPS ring group.

Each configuration item is described as follows:

Ring ID: Uniquely identifies an ERPS ring, ranging from 1 to 255.

Protocol Dest MAC: The destination MAC address of ERPS protocol packets can be 01-19-A7-00-00-01, or the Ring ID can be used as the last byte of the destination address, i.e., 01-19-A7-00-00-[Ring ID]. The destination MAC address of protocol packets must be the same within the same ring network.

Ring Type: Major(main ring) or Sub(sub ring). The main ring is a closed ring, and the sub ring is a non-closed ring. The ERPS ring can be composed of a single main ring, or a multi-ring structure can be formed by the main ring and sub-rings.

Node Type: The node type of the switch in the ring, including:

- Normal node: receive and forward protocol packets and service packets in the link;
- RPL Owner node: The function is to block or open the RPL link (Ring Protection Link, that is, the link between the Owner node and the Neighbor node) to prevent the formation of loops.
- RPL Neighbor node: The node directly connected to the Owner node on the RPL link is the Neighbor node, which blocks and opens the RPL port on this node together with the Owner node.

East Port/West Port: In the main ring, each node has 2 member ports, which are called east and west ports; in the sub-ring, the node connected to the main ring is called the interconnection node, and the sub-ring interconnection node. There is only one member port, and only one of the east and west ports needs to be configured during configuration, and the other is configured as none; the configuration for non-ring interconnection nodes is the same as that for main ring nodes, both east port and west port must be configured.

RPL Port: When the node type is Owner/Neighbor, the RPL port indicates which port is used as the port on the RPL link, and either east or west port can be selected. When the node type is Normal, this item is not configurable.

Major Ring: When the node type is Main Ring, this item cannot be configured. When the node type is Sub-Ring, configure the main ring ID for this sub-ring node. In particular, for a sub-ring interconnection node, the corresponding main ring must already exist on the current node for the configuration to be successful.

Revertive Mode: When the ERPS link returns to normal, you can decide whether to block the RPL link again by setting the revertive/non-revertive mode of the ERPS. Except for special needs, the configuration should be kept in revertive mode.

- Revertive: If the faulty link recovers, after the WTR time, the RPL link will be blocked again, and all nodes will be stable in the Idle state.
- Non-Revertive: If the faulty link recovers, the blocked link remains on the original faulty link, the RPL link will not be blocked again, and all nodes are stable in the Pending state.

Control VLAN: A VLAN used to transmit protocol packets. The value ranges from 2 to 4094. It must be a pre-existing VLAN, and the ring ports must be configured to allow this VLAN to pass through. All nodes within the same ERPS ring must use the same protocol VLAN.

Protected VLAN: A VLAN used for transmitting service data, the value ranges from 1 to 4094. Ring network ports must allow the protected VLAN to pass through.

WTR: In revertive mode, the WTR timer is used to prevent frequent switchover protection operations when frequent link failures are detected. Before the timer expires, the RPL link keeps forwarding, and the port that recovers from the fault remains blocked. During this period, if the Owner node receives the SF protocol packet, it means that there is still a fault in the ring network, the timer is turned off, and the RPL link remains on. Otherwise, after the timer expires, the RPL link is blocked, and the Owner node sends (NR, RB) packets to notify the failure recovery node, release the temporarily blocked port, and refresh the MAC address table. The unit is min (minutes), with a range from 1 to 12.

Guard: This timer is started after the node detects the fault recovery or executes the Clear command. It is used to prevent the old R-APS packets caused by the forwarding delay in the ring network from causing unnecessary oscillation to the network. Before this timer expires, any R-APS messages received, except event messages, will be ignored. Note that the duration of this timer should be greater than the delay for the R-APS packet to reach all nodes in the ring, but the longer the duration, the longer the node misses processing new requests from other nodes. The unit is ms (milliseconds), with a range from 10 to 2000.

HoldOff: This timer is started when the node detects a fault, and the fault is not reported immediately. After the timer expires, if the fault still exists, it will be reported, which provides the service layer with the opportunity to repair the link. Note that the length of this timer will affect the reporting speed of the link failure, and ultimately affect the switching performance of the link. The unit is ms (milliseconds), with a range from 0 to 10000.

Ring Enable: Enable or Disable the ring network. Generally, after the configuration is successful, the ring network is disabled by default and needs to be manually enabled.

Cancel: Abandons all current configuration entries on this page and closes the pop-up window. No ERPS ring group will be created or modified.

Confirm: Saves the filled parameters and submits them to create or update the ERPS ring group.

 Caution

1. The east port and the west port cannot be the same.
2. A port can only belong to one ERPS ring.
3. The control VLANs of nodes in the same ERPS ring must be the same.
4. The control VLAN of ERPS must be a created VLAN, and cannot be configured on other ports except the east port or west port of the ring.
5. In addition to the control VLAN and the protection VLAN, it is better not to have other VLANs on the group ring port, to prevent packets from other VLANs from causing a broadcast storm.
6. ERPS, EAPS, spamming tree and private ring functions are mutually exclusive.

6.5 Spanning Tree

The MSTP (Multi Spanning Tree Protocol) protocol eliminates Layer 2 loops by selectively blocking redundant links in the network, and also has a link backup function. MSTP can make up for the

shortcomings of STP and RSTP. It can not only converge quickly, but also forward traffic of different VLANs along their own paths, thus providing a better load sharing mechanism for redundant links.

6.5.1 MSTP Configuration

As shown in Figure 41.

Managed Industrial Ethernet Switch

Network Redundancy > Spanning Tree > Spanning Tree Config

Global Config Port Config

* Protocol State: ☐ Enable ☒ Disable Submit

* Bridge Priority: s(4~30)

* Forward Delay: s(4~30)

* Hello Time: s(1~10)

* Max Age: s(6~40)

* Max Hops: (1~40)

* BPDU Filter: ☐ Enable ☒ Disable

* BPDU Guard: ☐ Enable ☒ Disable

* Errdisable Timeout: ☐ Enable ☒ Disable

* Errdisable Timeout Period: s(10~1000000)

* Cisco Interaction: ☐ Enable ☒ Disable

Reset Cancel Submit

Figure 41 MSTP configuration page

The page is used for global parameter configuration of MSTP.

Each configuration item is described as follows:

Protocol State: Enable or disable the MSTP function, disabled by default.

Bridge Priority: The priority of the bridge.

Forward Delay: The forward delay time of the spanning tree.

Hello Time: The interval for sending BPDU hello packets.

Max Age: The maximum lifetime of BPDU packets.

Max Hops: The maximum hop count of BPDU packets.

BPDU Filter: Enable or disable the BPDU filter function.

BPDU Guard: Enable or disable the BPDU guard function.

Errdisable Timeout: Enable or disable the errdisable timeout function.

Errdisable Timeout Period: The recovery time of the errdisable state.

Cisco Interaction: Enable or disable compatibility with Cisco devices.

6.5.2 MSTP Port Instance Relationship

As shown in Figure 42.

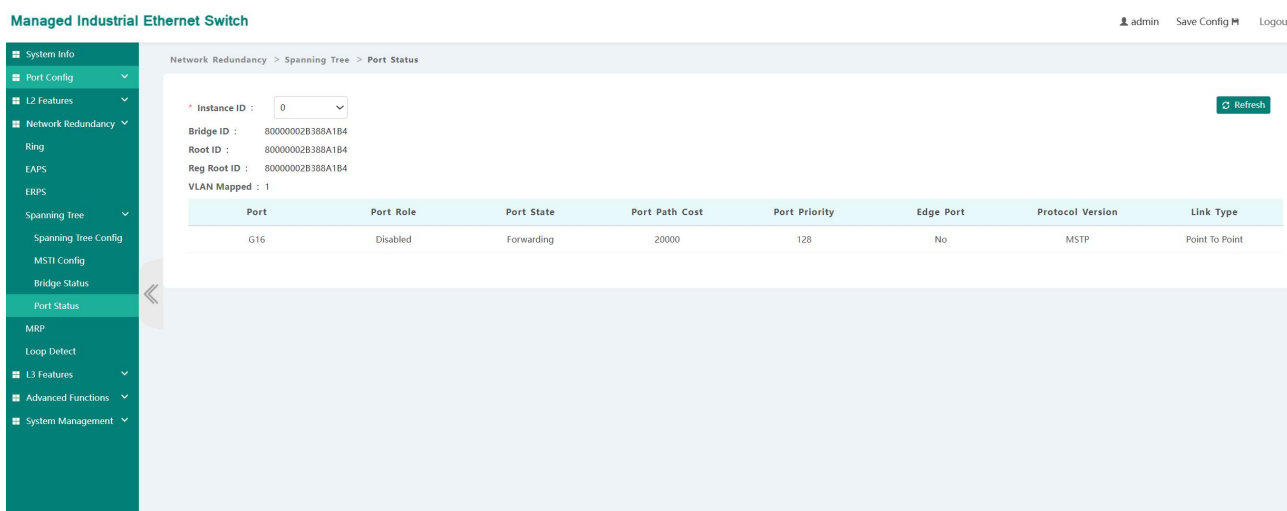


Figure 42 MSTP port instance relationship page

7 Layer 3 Features

The content in this chapter is only applicable to our layer 3 managed switch series products.

7.1 Layer 3 Interface

As shown in Figure 43.

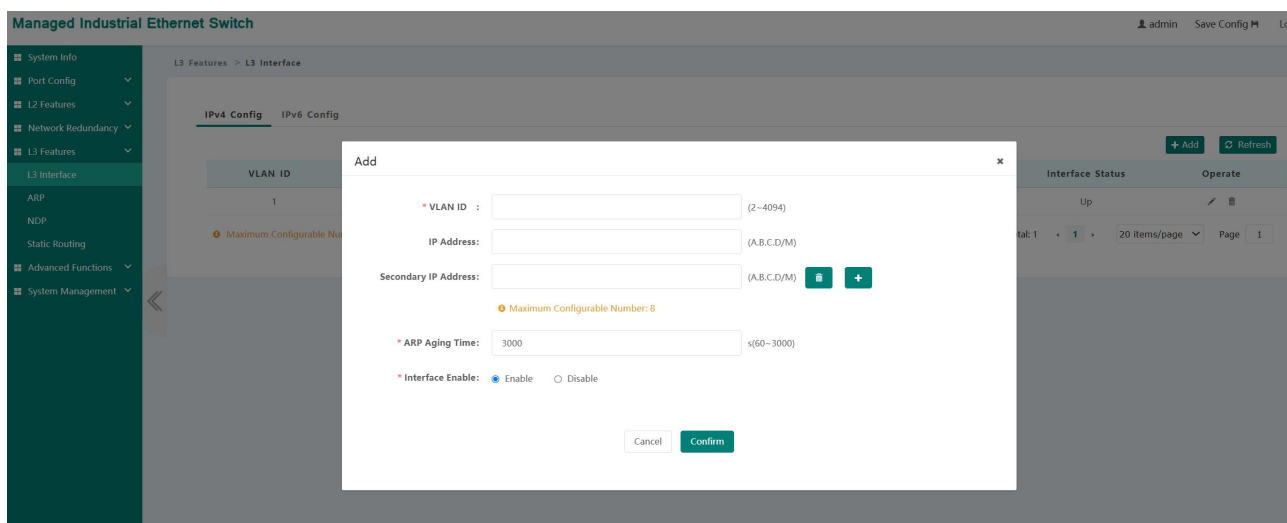


Figure 43 Layer 3 interface page

The page is the Layer 3 interface parameters configuration page.

Each configuration item is described as follows:

VLAN ID: The VID of the Layer 3 interface.

IP Address: The primary IP address of the Layer 3 interface.

Secondary IP Address: The secondary IP of the Layer 3 interface.

ARP Aging Time: The ARP aging time of a Layer 3 interface, in seconds, and the default value is 3000.

Interface Enable: Enable or Disable the interface. It is enabled by default.

⚠ Caution

1. You must create a Layer 3 interface and configure the primary IP address, and then select the Layer 3 VLAN interface in the list before configuring its secondary IP address.
2. You must delete all secondary IP addresses on the Layer 3 interface before deleting the primary IP address.
3. A Layer 3 interface can be configured with multiple slave IPs, but only the first one can be displayed on the web page.

7.2 ARP

Static ARP specifies the mapping relationship between IP and MAC and is not affected by aging time. As shown in Figure 44.

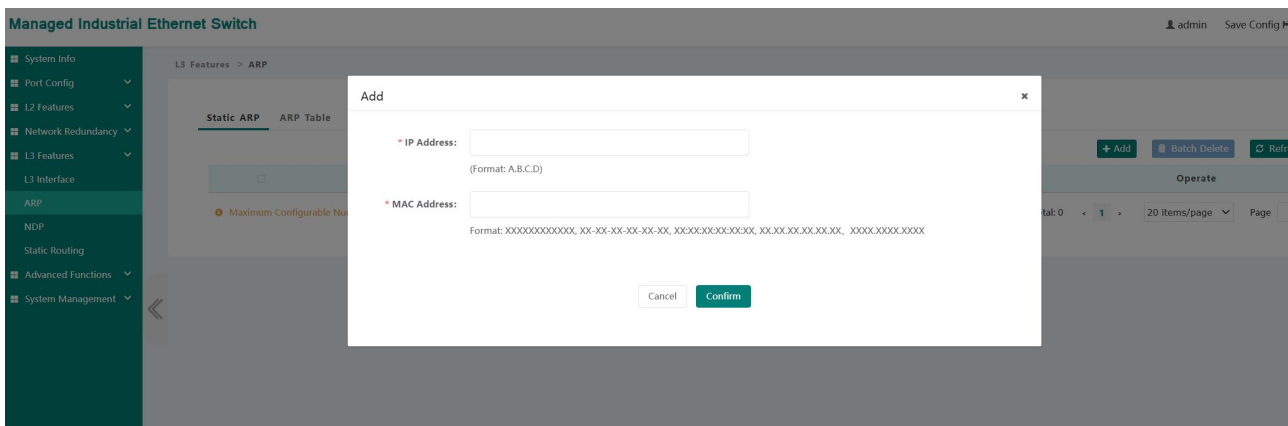


Figure 44 ARP page

The page is the static ARP configuration page.

Each configuration item is described as follows:

IP address: The IP in the static ARP entry.

MAC address: The MAC corresponding to the IP in the static ARP entry.

⚠ Caution

1. Static ARP is not affected by aging time.

7.3 Static Routing

As shown in Figure 45.

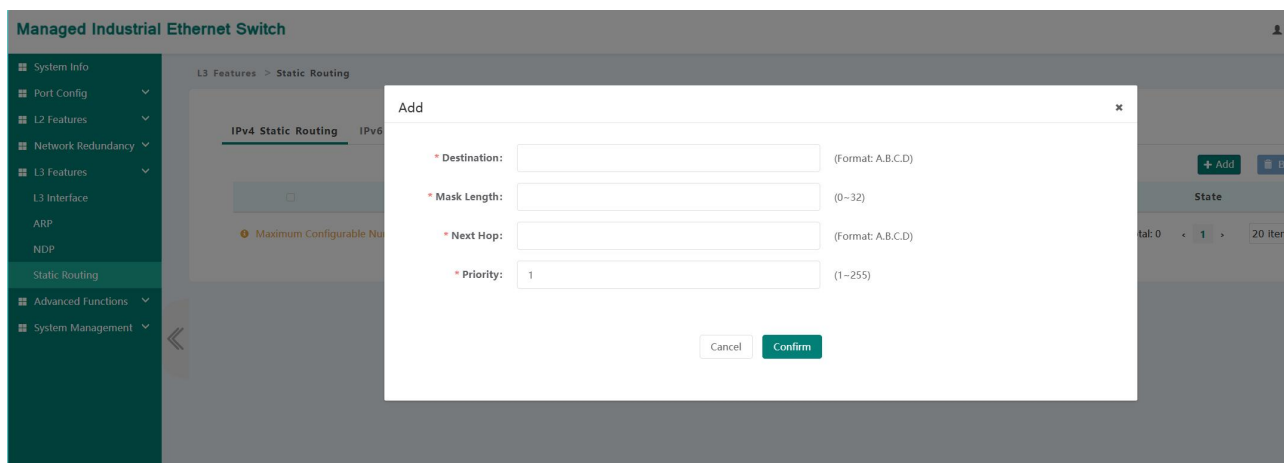


Figure 45 Static routing

The page is the static route configuration page.

Each configuration item is described as follows:

Destination: The destination network segment of the static route.

Mask Length: The subnet prefix length of the destination network segment, ranging from 0 to 32.

Next Hop: The next-hop address of the static route.

Priority: The priority of the static route, ranging from 1 to 255.



Caution

1. The static routing page can only add and delete static routes, but you can view all routing information.
2. The next hop IP cannot be the local interface IP.

8 Advanced Functions

8.1 SNMP

8.1.1 SNMP Configuration

Configure the administrator ID and device location, as shown in Figure 46.

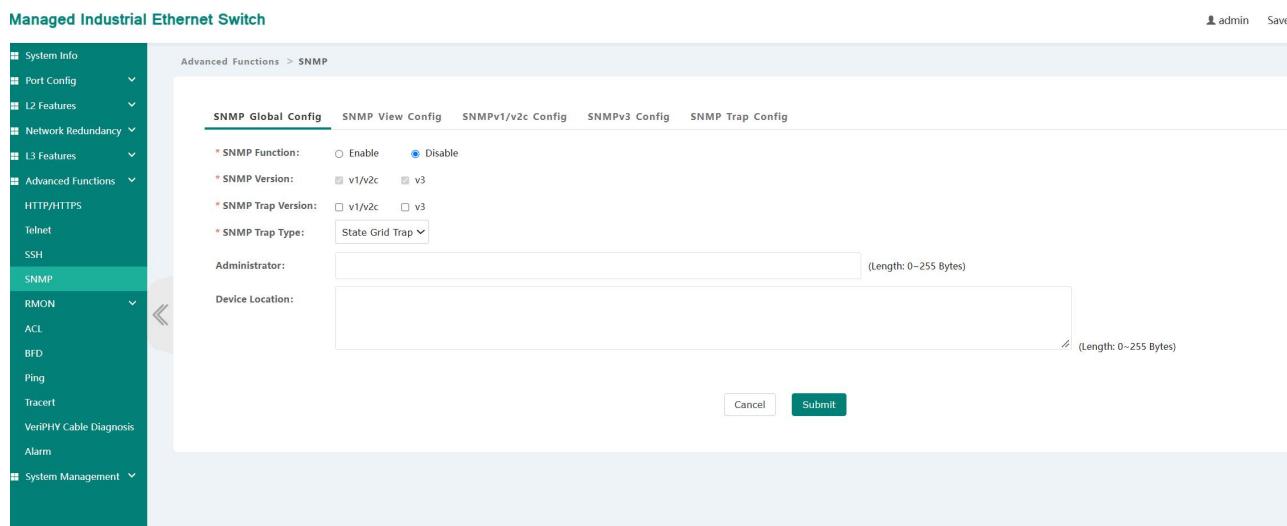


Figure 46 SNMP configuration page

Each configuration item is described as follows:

SNMP Function: Enable or disable the SNMP function. It is disabled by default.

SNMP Version: The supported SNMP protocol versions.

SNMP Trap Version: The protocol version for SNMP Trap.

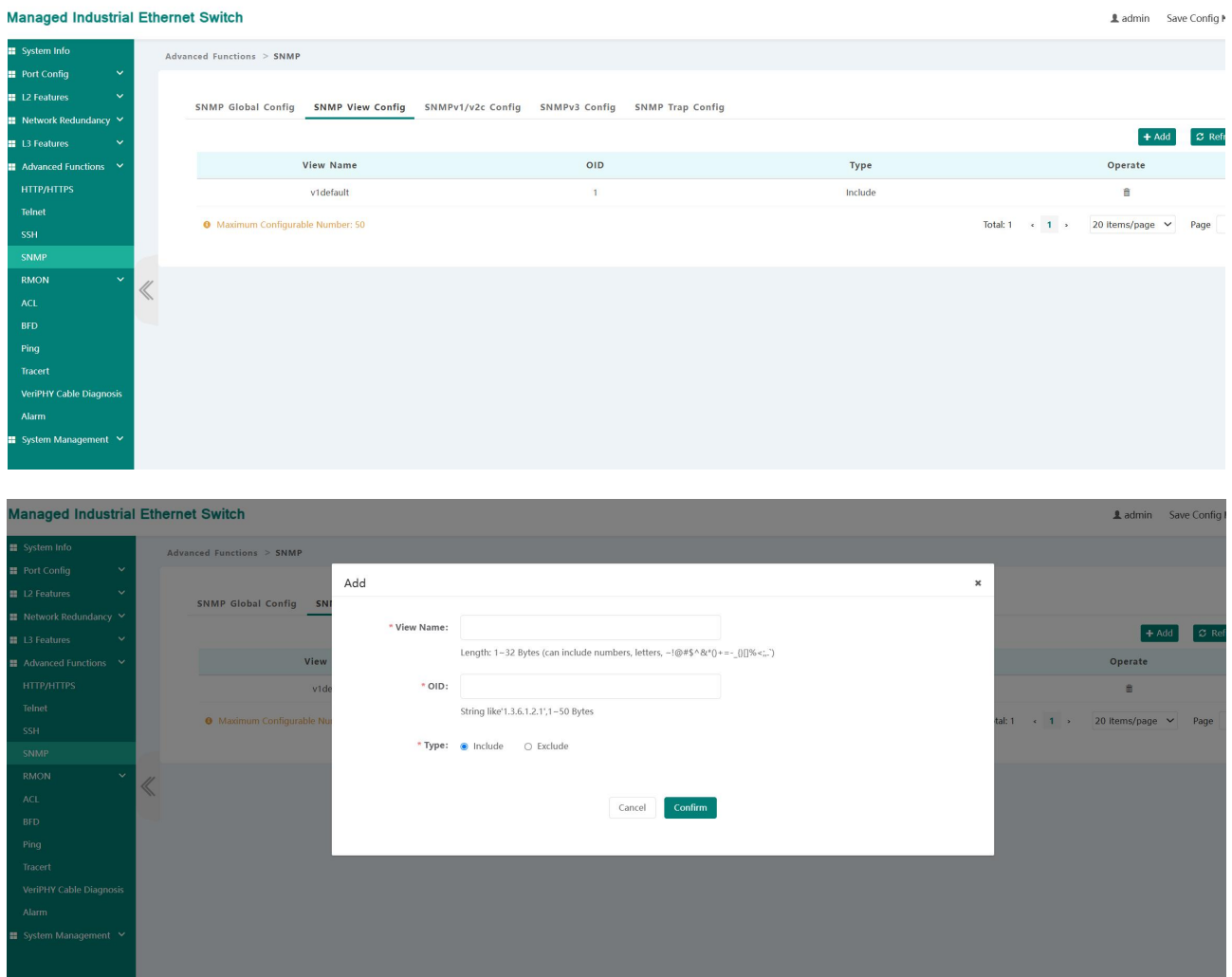
SNMP Trap Type: The type of SNMP Trap.

Administrator: Administrator contact information.

Device Location: The address where the device is located.

8.1.2 Group Configuration

As shown in Figure 47.



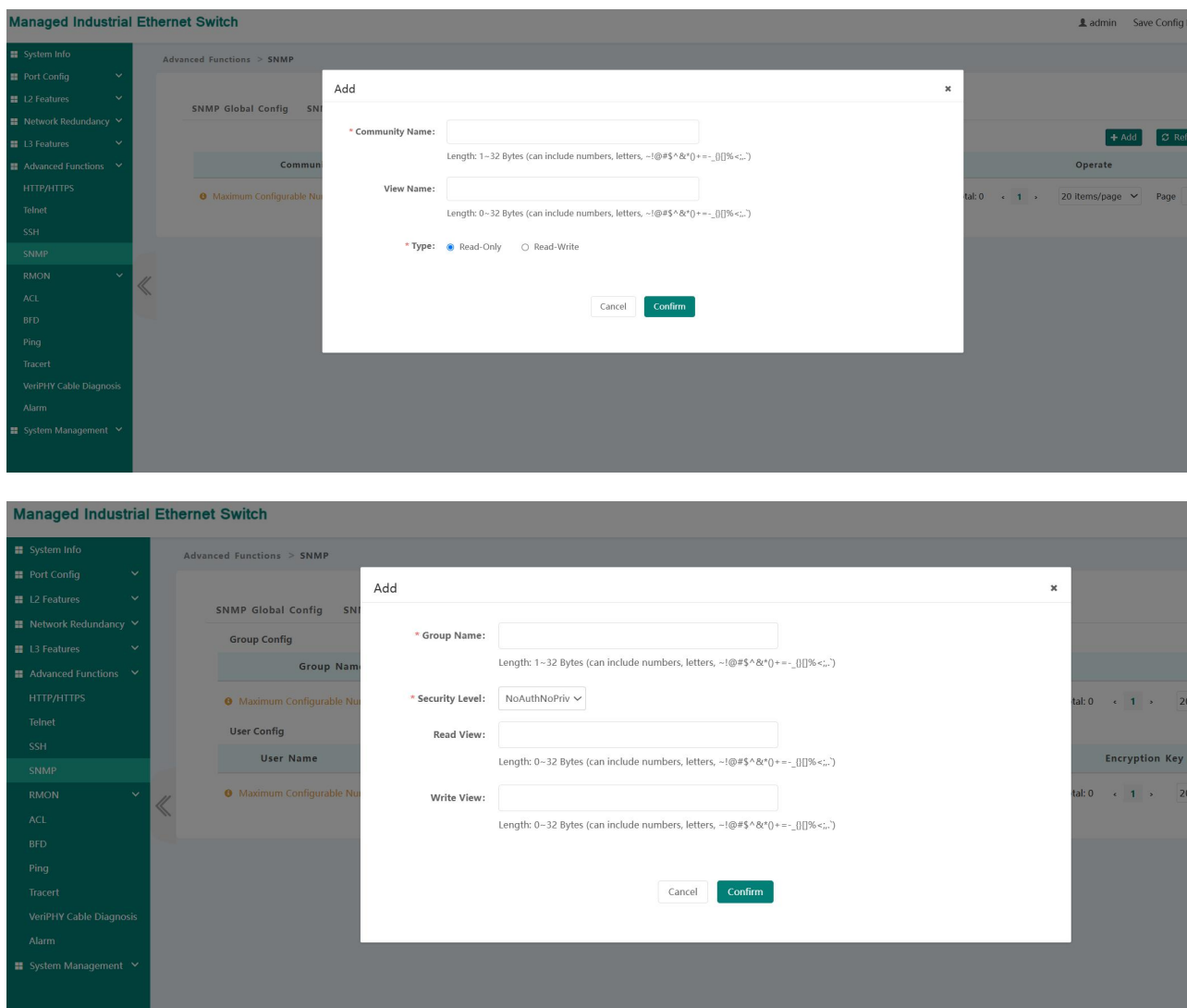


Figure 47 Group Configuration Page

The configuration items are described as follows:

View Name: Specifies the name of the SNMP view.

OID: Specifies the Object Identifier (OID) associated with this view.

Community Name: An SNMP community name—also known as a community string—is a name designated by a character string.

Permissions: Set permissions for Get and Set operations on the community name using `ro` and `rw`.

- Ro:Read-only permission
- Rw:Read and write permissions

Group Name: Specifies the name of the SNMP group.

Security Level: Sets the security level applied to the group. The dropdown menu is currently set to the default value NoAuthNoPriv.

8.1.3 Trap Configuration

As shown in Figure 48.

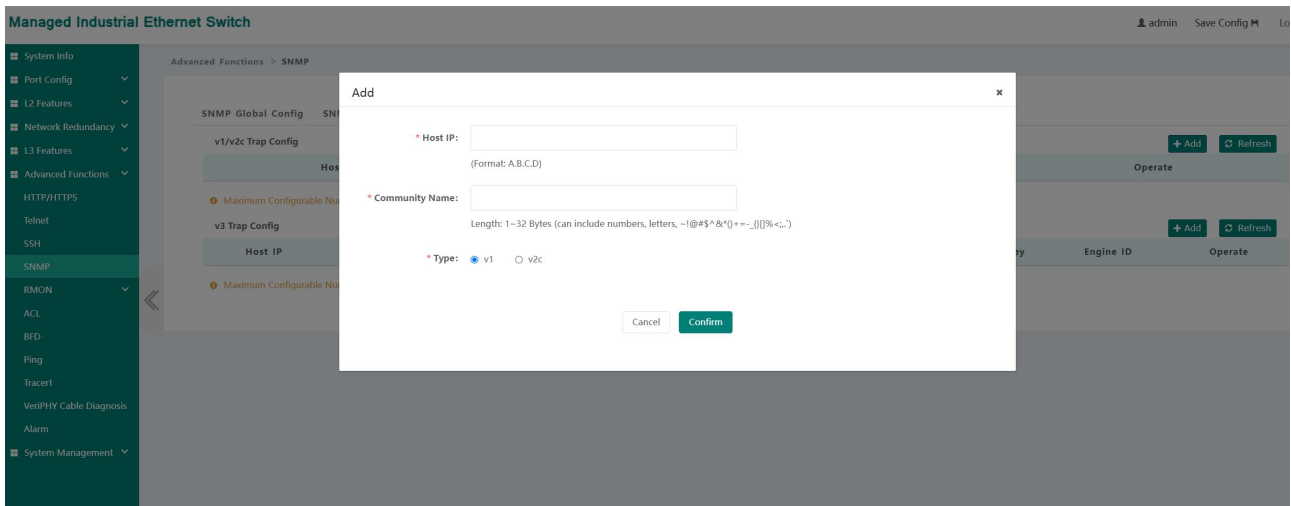


Figure 48 Traps configuration page

The page is divided into two parts. The upper part configures the SNMP Traps global switch, version, trap host and community name. The lower part displays the Trap list and its delete button.

The configuration items are described as follows:

SNMP Trap: Global switch for SNMP Traps.

Trap Version: Supports SNMP Trap versions; the corresponding Trap is sent after configuration. The supported versions are V1 and V2c.

Host IP: The network IP address of the recipient that receives anomaly alert messages.

SNMP Community Name: Also known as a community string, it is designated by a text string. Must be 1 to 32 bytes in length.

8.2 ACL

ACL (Access Control List) implements packet filtering by configuring matching rules and processing operations for packets. The matching rules include the source address, destination address, and port number of the data packet.

An ACL consists of a series of entries, called an access control list entry (Access Control Entry: ACE). Each ACL entry declares the matching conditions and behaviors that satisfy the entry.

8.2.1 MAC ACL Configuration

MAC ACL formulates matching rules based on the source/destination MAC address and Ethernet II type of packets. As shown in Figure 49.

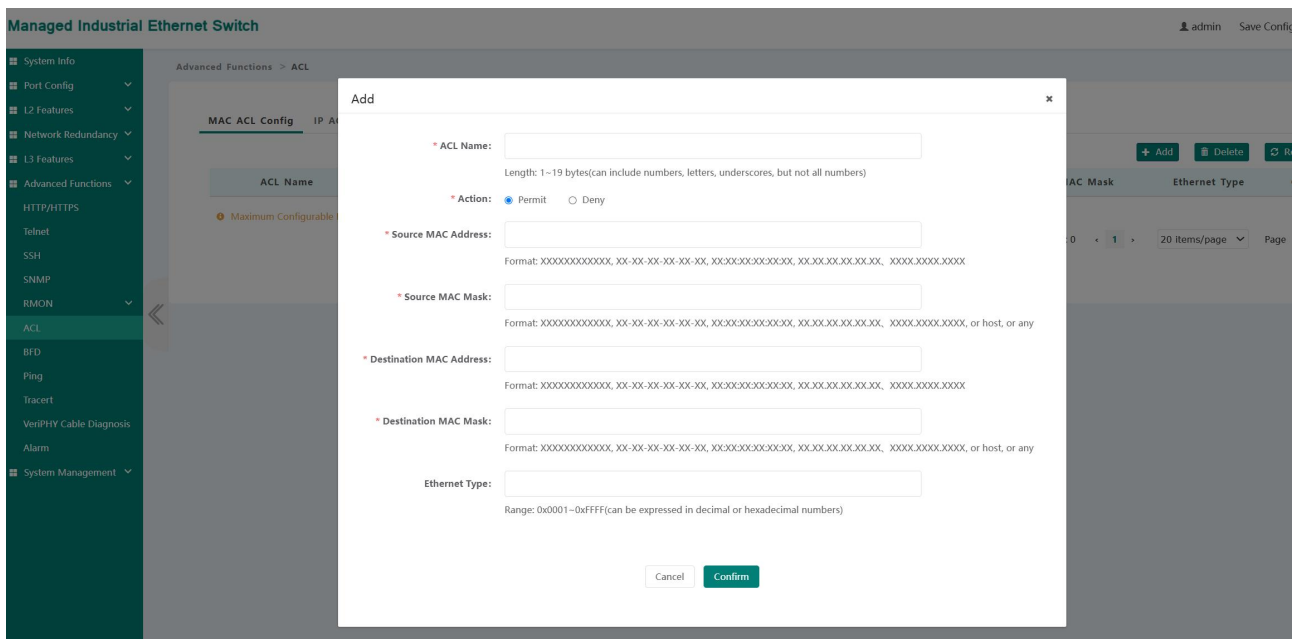


Figure 49 MAC ACL page

Each configuration item is described as follows:

ACL name: consists of letters, numbers or underscores, cannot be pure numbers, and is less than 20 in length.

Action: The processing action of the packet matching, permit or deny.

Source MAC Address: XXXXXXXXXXXX, XX-XX-XX-XX-XX-XX, XX:XX:XX:XX:XX:XX, XX.XX.XX.XX.XX.XX, XXXX.XXXX.XXXX, or any.

Source MAC Mask: XXXXXXXXXXXX, XX-XX-XX-XX-XX-XX, XX:XX:XX:XX:XX:XX, XX.XX.XX.XX.XX.XX, XXXX.XXXX.XXXX, host, or any.

Destination MAC Address: XXXXXXXXXXXX, XX-XX-XX-XX-XX-XX, XX:XX:XX:XX:XX:XX, XX.XX.XX.XX.XX.XX, XXXX.XXXX.XXXX, or any.

Destination MAC Mask: XXXXXXXXXXXX, XX-XX-XX-XX-XX-XX, XX:XX:XX:XX:XX:XX, XX.XX.XX.XX.XX.XX, XXXX.XXXX.XXXX, host, or any.

Ethernet Type: Decimal or hexadecimal representation, the value range is 0x0001~0xFFFF.

Cancel: To discard changes and close the window.

Apply: A green button to save and apply the new ACL rule.

Attention

- 1.* Indicates that it must be configured when adding ACL rules.
2. The name of the MAC ACL cannot be a pure number.
3. Creating a MAC ACL will automatically add an ACE at the end: deny any any, which can be replaced with permit any any.
- 4.ACE: deny any any /permit any any cannot be deleted with [Delete ACE], but can only be cleared with [Delete ACL].

8.2.2 IP ACL Configuration

IP ACL formulates matching rules based on Layer 3 and Layer 4 information of packets. As shown in Figure 50.

The screenshot displays the 'Managed Industrial Ethernet Switch' configuration interface. On the left, a sidebar lists various system functions, with 'ACL' highlighted. The main area shows the 'IP ACL Config' tab. A modal window titled 'Add' is open, allowing for the creation of a new ACL rule. The form includes the following fields and options:

- ACL Type:** Radio buttons for 'Basic' (selected) and 'Advanced'.
- ACL ID:** A text input field with a range of 1-99, 1300-1999.
- Action:** Radio buttons for 'Permit' (selected) and 'Deny'.
- IP Protocol:** A dropdown menu with a range of 0-255 or protocol names (ah, eigrp, esp, gre, icmp, igmp, ip, ipinip, iposp, ipcp, pim, tcp, udp).
- Source IP Address:** A text input field with a format of *.*.*.*.
- Source IP Mask:** A text input field with a format of *.*.*.* or host, or any. A note explains that a mask is a 32-bit binary number in dotted decimal notation, where 1s represent match bits and 0s represent don't-care bits.
- TCP/UDP Source Port:** A dropdown menu with a range of 1-65535 or port names in TCP/UDP packets.
- Destination IP Address:** A text input field with a format of *.*.*.*.
- Destination IP Mask:** A text input field with a format of *.*.*.* or host, or any.
- TCP/UDP Destination Port:** A dropdown menu with a range of 1-65535 or port names in TCP/UDP packets.

Figure 50 IPC ACL page

This page is used to configure IP ACL parameters.

Each configuration item is described as follows:

ACL Type:

Basic ACL: Make matching rules based on the source IP of packets.

Advanced ACL: According to the source/destination IP, source/destination port, IP protocol type and other Layer 3/4 information of the packet, the matching rules are formulated.

ACL ID:

The number range of the basic ACL is 1 to 99 and 1300 to 1999.

The number range of an advanced ACL is 100 to 199 and 2000 to 2699.

Action: The processing action of the packet matching, permit or deny.

IP Protocol Type: The IP protocol type carried by the packet, ranging from 0 to 255, or the IP protocol name.

Source IP Address: The source IP address of the packet, in the format *.*.*.*.

Source IP Mask: The format is *.*.*.* or host or any.

TCP/UDP Source Port: The value ranges from 1 to 65535, or the TCP/UDP packet port name.

Destination IP Address: The format is *.*.*.*.

Destination IP Mask: the format is *.*.*.* or host or any.

TCP/UDP Destination Port: the value ranges from 1 to 65535, or the port name for TCP/UDP packet.

Attention

1. Indicates that it must be configured when adding ACL rules.
2. The IP wildcard mask is expressed in dotted decimal, binary 1 means match, 0 means don't care.
3. IP protocol names include: ahp, eigrp, esp, gre, icmp, igmp, ip, ipinip, ospf, pcp, pim, tcp, udp.
4. The TCP packet port names include: ftp, ftp-data, pop3, smtp, telnet, www.
5. UDP packet port names include: rip, snmp, snmp-trap, tftp.
6. Creating a basic ACL will automatically add an ACE at the end: deny any, which can be replaced with permit any.
7. Creating an advanced ACL will automatically add an ACE at the end: deny ip any any, which can be replaced with permit ip any any.
8. ACE: deny/permit any and deny/permit ip any any can only be cleared by [Delete ACL].

8.2.3 Applying ACLs to Ports

Applying an ACL to a port means applying an ACL rule to an interface to filter the packet flow received by the interface. As shown in Figure 51.

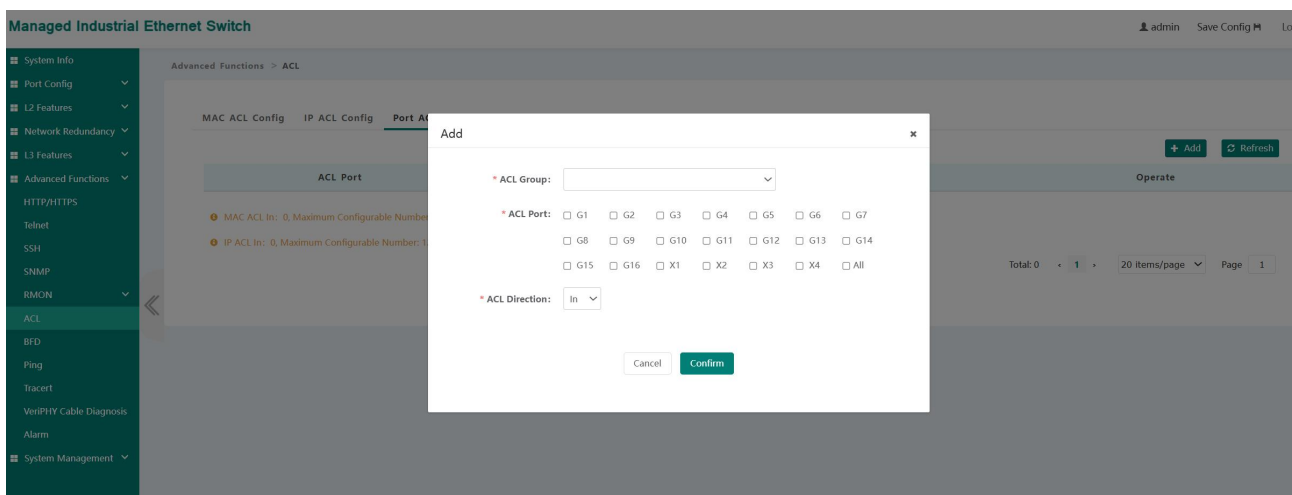


Figure 51 Port ACL Application Page

This page is used to configure the ACL parameters applied to the port.

Each configuration item is described as follows:

ACL Group: any group of ACLs configured previously.

ACL Port: The port to which the ACL is applied.

ACL Direction: the application direction of the port ACL, in or out.

Attention

Before applying an ACL to a port, you must configure an ACL rule.

8.3 Network Diagnostics

8.3.1 Ping

The Ping function is used to detect whether the network connection is normal, as shown in Figure 52. The page is divided into two sections: the first is for entering the IP address to be pinged, and the second displays the ping results.

Each configuration item is described as follows:

IP address: The unicast IP address to be pinged.

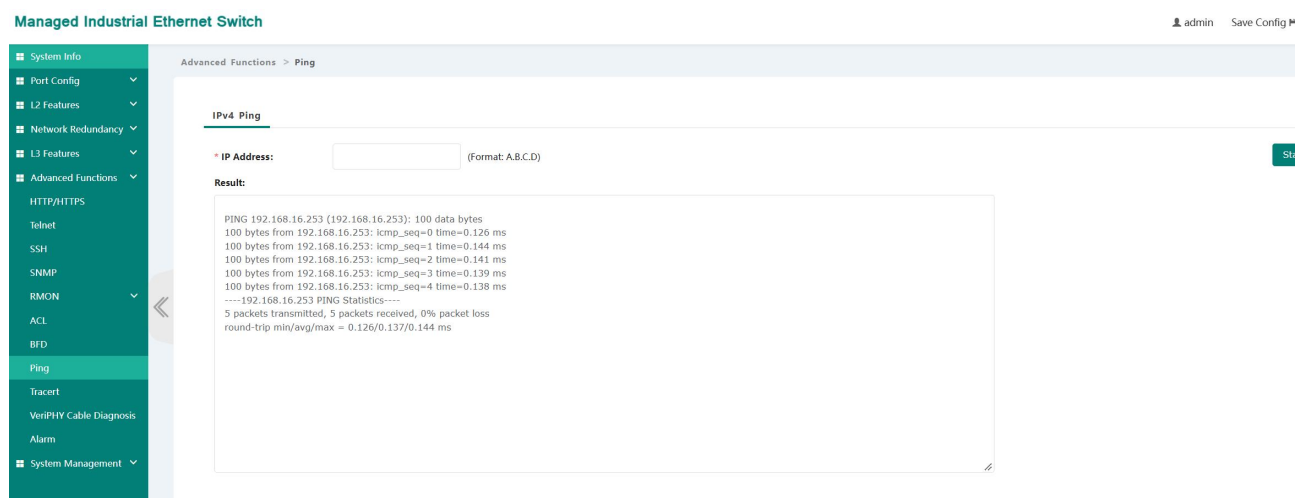


Figure 52 Ping page

8.3.2 Tracert

The tracert function is used to detect the path taken to reach the IP, as shown in Figure 53.

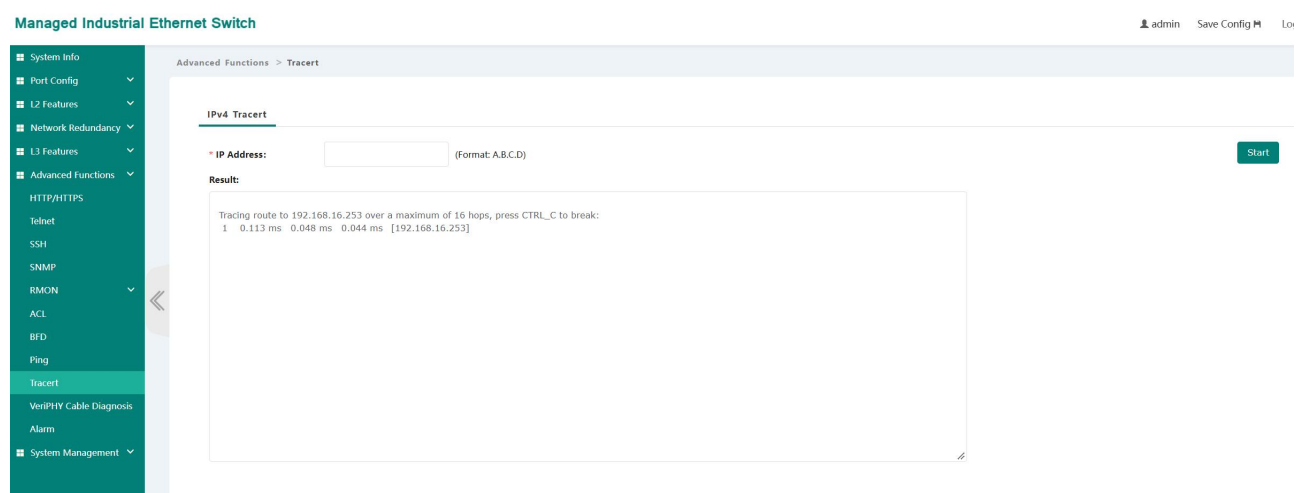


Figure 53 Tracert page

The page is divided into two sections: the first section is used to enter the IP address for Tracert, and the second section displays the Tracert results.

Each configuration item is described as follows:

IP address: The unicast IP address for which the Tracert operation is required.

8.4 Login Control

Configure and display the global switches for SSH and Telnet servers, as shown in Figure 54.

The figure consists of two screenshots of the 'Managed Industrial Ethernet Switch' configuration interface.

Top Screenshot: Telnet Configuration

- Page Title:** Managed Industrial Ethernet Switch
- Breadcrumb:** Advanced Functions > Telnet
- Left Menu:** System Info, Port Config, L2 Features, Network Redundancy, L3 Features, Advanced Functions, HTTP/HTTPS, Telnet (selected), SSH, SNMP, RMON, ACL, BFD, Ping, Tracert, VeriPHY Cable Diagnosis, Alarm, System Management.
- Main Content:**
 - Telnet Service:** ☐ Enable ☒ Disable
 - Submit:** A green button to save the configuration.

Bottom Screenshot: SSH Configuration

- Page Title:** Managed Industrial Ethernet Switch
- Page Header:** admin Save Config Log
- Breadcrumb:** Advanced Functions > SSH
- Left Menu:** Same as the top screenshot, with 'SSH' selected.
- Main Content:**
 - Server Config:**
 - SSH Service:** ☐ Enable ☒ Disable
 - Password Auth:** ☒ Enable ☐ Disable
 - SSH Port:** (22/1025-65535, default 22)
 - Buttons:** Cancel, Submit
 - Public Key Management:**
 - Buttons:** + Add, Refresh
 - Table:**

Username	Auth Type	Public Key Name	Operate
Maximum Configurable Number: 16			

Figure 54 Login control page

Each configuration item is described as follows:

SSH: Enable or disable the SSH function; disabled by default.

TELNET: Enable or disable the Telnet function; disabled by default.

SSH Port: Specifies the port number used by the SSH service. The default port is 22, and the valid range is 22 to 65535.

Cancel: Cancels the current configuration changes.

Submit: Saves and applies the SSH configuration.

Add: Adds a new public key authentication entry.

Refresh: Refreshes the public key list.

Attention

1.The maximum configurable number of usernames is 16.

9 PoE

PoE (Power over Ethernet, also known as remote power supply) It means that the device is connected to some IP-based external PD devices (Powered Device, such as IP phones, wireless APs, network cameras, etc.) through the Ethernet interface. , the technology of remote DC power supply while transmitting data signals.

The content of this chapter applies only to our company's switches with PoE functionality.

9.1 PoE

As shown in Figure 55.

PoE >> PoE

设备参数配置

最大功率

370

(10~370W)

输出功率

0.00

(W)

输出电流

0.00

(A)

修改

重置

端口参数配置

端口范围

使能

☒ Enable ☐ Disable

优先级

Low

最大功率

(1~30W)

修改

重置

☐	端口	使能	优先级	最大功率(W)	状态	功率(W)	电压(V)	电流(A)	PD类型
☐	ge1	Enable	Low	30	Down	0.00	0.00	0.00	0
☐	ge2	Enable	Low	30	Down	0.00	0.00	0.00	0
☐	ge3	Enable	Low	30	Down	0.00	0.00	0.00	0
☐	ge4	Enable	Low	30	Down	0.00	0.00	0.00	0
☐	ge5	Enable	Low	30	Down	0.00	0.00	0.00	0
☐	ge6	Enable	Low	30	Down	0.00	0.00	0.00	0
☐	ge7	Enable	Low	30	Down	0.00	0.00	0.00	0

Figure 55 PoE configuration page

The page is divided into two sections: the upper section configures the global parameters of the PoE device, and the lower section configures the PoE port parameters. (First, select the checkbox in the list to map the PoE port attributes to the upper configuration area, and then modify the parameter settings.)

The descriptions of the device parameter configuration items are as follows:

Maximum power: The maximum total output power of POE, the unit is W, the range is 10W~ 370W, the default is 370W.

Output Power: Real-time total PoE output power, in watts (W).

Output Current: The real-time total PoE output current, in amperes (A).

The descriptions of the port parameter configuration items are as follows:

Port Enable: Enables or disables the PoE power supply function for the port; enabled by default.

Port Priority: Port power supply priority; default is Low; value range:

- Critical: Highest priority
- High: Higher priority
- Medium: Normal priority
- Low: Lowest priority

Maximum power: The maximum power that the port can provide externally, in W, ranging from 1W to 30W, and the default is 30W.

Status: Real-time power output status of the port; "Up" indicates power is being supplied, while "Down" indicates no power is being supplied.

Power (W): Real-time power of the PD device on the port, in watts (W).

Voltage (V): Real-time voltage of the PD device on the port, in volts (V).

Current (A): Real-time current of the PD device on the port, in amperes (A).

PD Type: Based on power supply levels, PD devices can be classified as follows:

- Class 0: corresponding reference power 15.4W
- Class 1: corresponding reference power 4W
- Class 2: corresponding reference power 7W
- Class 3: corresponding reference power 15.4W
- Class 4: corresponding reference power 30W
- Class 5: corresponding reference power 45W
- Class 6: corresponding reference power 60W
- Class 7: corresponding reference power 60W
- Class 8: corresponding reference power 60W

Attention

1. PoE interface priority refers to the priority level for power allocation among PoE interfaces within the total power limit. It serves as a mechanism to ensure that critical devices receive power first when the total power consumed by Powered Devices (PDs) exceeds the total power capacity of the Power Sourcing Equipment (PSE).
2. When the total output power of the PoE switch is insufficient, the PD on the PoE port with higher priority is powered first. If the PoE ports have the same priority, the PD on the PoE port with the lower port number is powered first.
3. Supports a high-priority automatic preemption function, allowing a PD connected to a higher-priority PoE port to automatically preempt the power currently being used by a PD on a

lower-priority PoE port. When the switch is operating near full power output capacity and the global maximum power is insufficient to start all PDs, you can raise the PoE priority of the port where the PD is connected. This causes the system to cut power to the port with the lowest PoE priority, forcibly ensuring that the port with the higher PoE priority is powered first.

10 System Management

10.1 System Time

The switch's system time maintains a unified time standard across the network, thereby ensuring the accuracy and synchronization of data transmission between devices. The switch system time page is shown in Figure 56.

Managed Industrial Ethernet Switch

The screenshot displays the 'System Time' configuration page. On the left is a sidebar menu with options: System Info, Port Config, L2 Features, Network Redundancy, L3 Features, Advanced Functions, System Management, System Time (selected), User Management, Log Information, Config File Management, Device Reboot, Factory Reset, and Device Upgrade. The main content area is titled 'System Management > System Time'. It shows the 'System Time' as 'Thu 24 Sep 2026 12:12:11'. Under 'Timezone Config', the 'Timezone' is set to '(GMT+08:00)Beijing, Chongqing, Hong Kong, Singapore' and 'Daylight Time' is unchecked. The 'time Config' section has two radio buttons: 'Local Time Synchronous' (selected) and 'Network Time Synchronization'. Under 'Local Time Synchronous', the 'Local Time' is 'Thu Sep 24 2026 12:12:10 GMT+0800'. Under 'Network Time Synchronization', there are fields for 'SNTP Time Interval' (3600), 'Primary SNTP Server', and 'Secondary SNTP Server', all with format instructions. At the bottom, there is a 'Manual Config Time' section with input fields for year, month, day, hour, minute, and second, along with 'Cancel' and 'Submit' buttons.

Figure 56 System Time Page

Manual configuration: The time range available for manual configuration is 1970 to 2037.

Local Synchronization: Synchronizes the switch's system time with the time of the PC accessing the switch; the supported time range is 1970 - 2037.

Time Zone: The time zone is configured specifically for SNTP. Global time zones are divided based on the Prime Meridian. The area extending from 7.5 ° West longitude to 7.5 ° East longitude (a longitudinal span of 15°) constitutes the zero zone. Starting from the boundaries of the zero time zone and moving eastward and westward, time zones are demarcated at 15-degree longitude intervals; twelve time zones are established in each direction, with the East 12 and West 12 zones coinciding, resulting in a total of 24 time zones worldwide. In each time zone, the local mean solar time of the central meridian serves as the standard time for that zone. The standard times of adjacent time zones differ by

one hour. In principle, time zone boundaries follow geographic meridians; however, in practice, they are often determined by national administrative borders or natural features to facilitate usage.

Time synchronization interval: Configures the time interval for SNTP synchronization with the server; the configurable range is 10 – 86,400 seconds, and the default value is 3,600.

SNTP Time Interval: Specifies the interval, in seconds, at which the device synchronizes its system time with the SNTP server. The configurable range is 10 to 86,400 seconds.

Primary SNTP Server: Specifies the IPv4 address of the primary SNTP server used for time synchronization. Enter the address in A.B.C.D format.

Secondary SNTP Server: Specifies the IPv4 address of the secondary SNTP server, which serves as a backup time source if the primary server is unavailable. Enter the address in A.B.C.D format.

Attention

1. The current system time is obtained based on the user's manual time configuration only when no SNTP servers are configured or all of them have failed.
2. When an unreachable or non-existent SNTP server is configured, the page will freeze for approximately 12 seconds.
3. Manually configuring the time or synchronizing with the local PC time will clear the SNTP configuration.
4. The time range for SNTP synchronization servers is 1970 – 2036.

10.2 User Management

Add or delete users, and modify the passwords and permissions of the selected users, as shown in Figure 57.

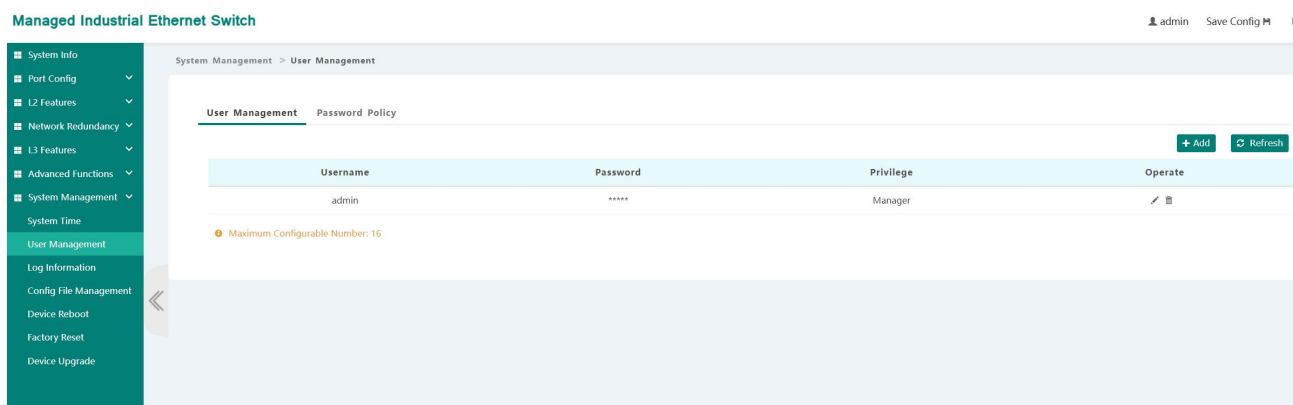


Figure 57 User management page

Attention

1. Only the user's password and authority can be modified, but the user name cannot be modified.
2. You cannot modify the authority of the currently logged-in user on the command line, and cannot delete the currently logged-in user on the command line.
3. The length of the password must be less than 16 characters. Special characters include ~ ! @ # \$ % ^

& * _ - . () + { } | < > = [] , / . The new password and the confirmation password must be the same.

10.3 Log Information

Configure the host IP of the remote log server, and display, clear, and export local log information. As shown in Figure 58.

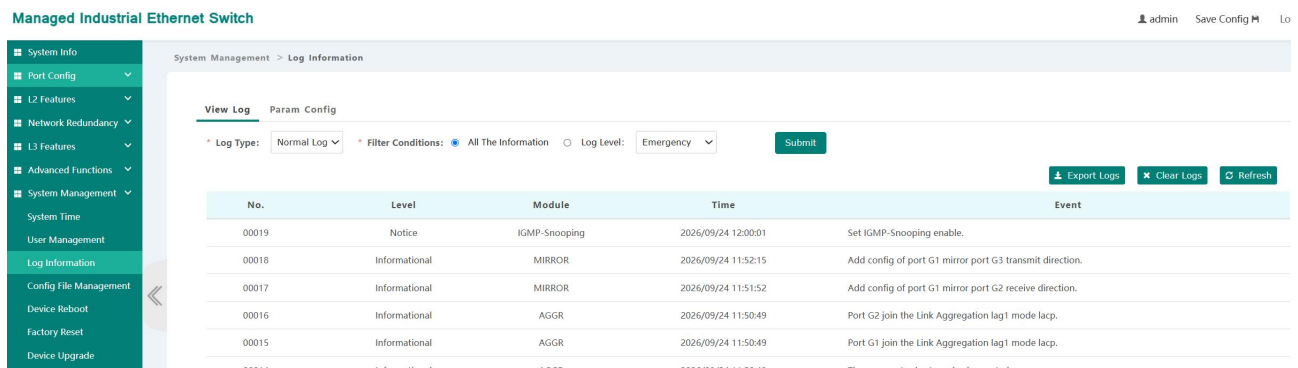


Figure 58 Log Information Page

Each configuration item is described as follows:

Log host IP address: The host IP of the remote log server.

Clear: Clear the local log information.

Export: Export local log information.

10.4 Restart the Switch

Software-reboot the switch, as shown in Figure 59.

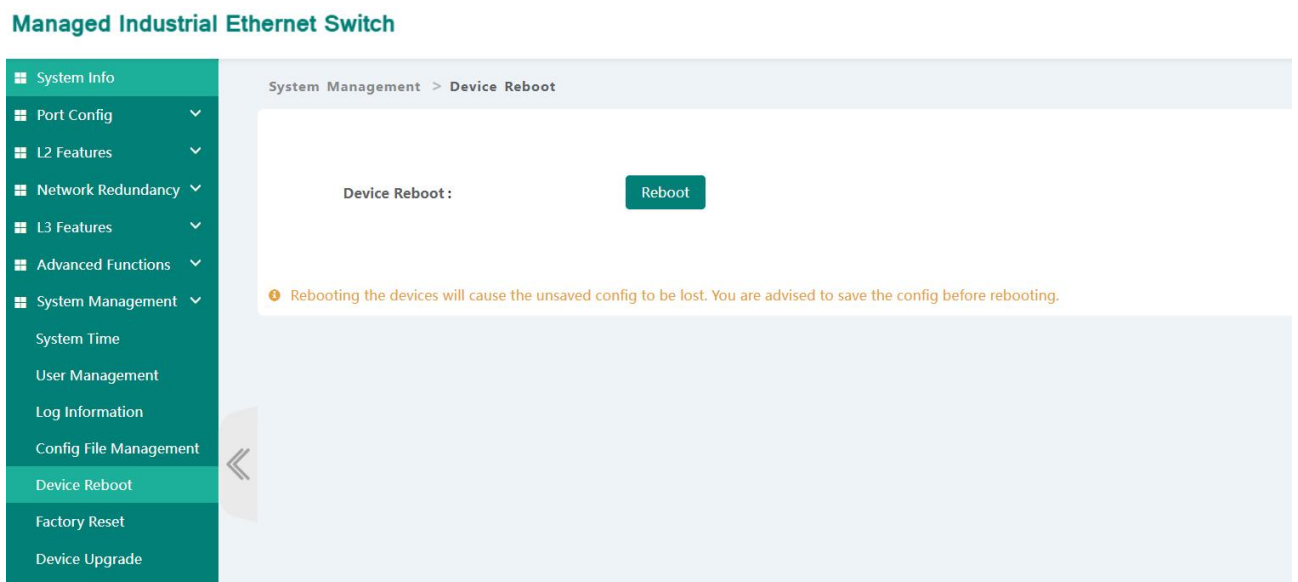


Figure 59 Switch Reboot Page

Attention

1. It is recommended to save the current configuration before restarting the system, otherwise the unsaved configuration will be cleared after restarting.

2. If a new configuration is uploaded, do not select "Keep current configuration", otherwise the current configuration will overwrite the uploaded configuration.

10.5 Restore Factory Configuration

As shown in Figure 60.

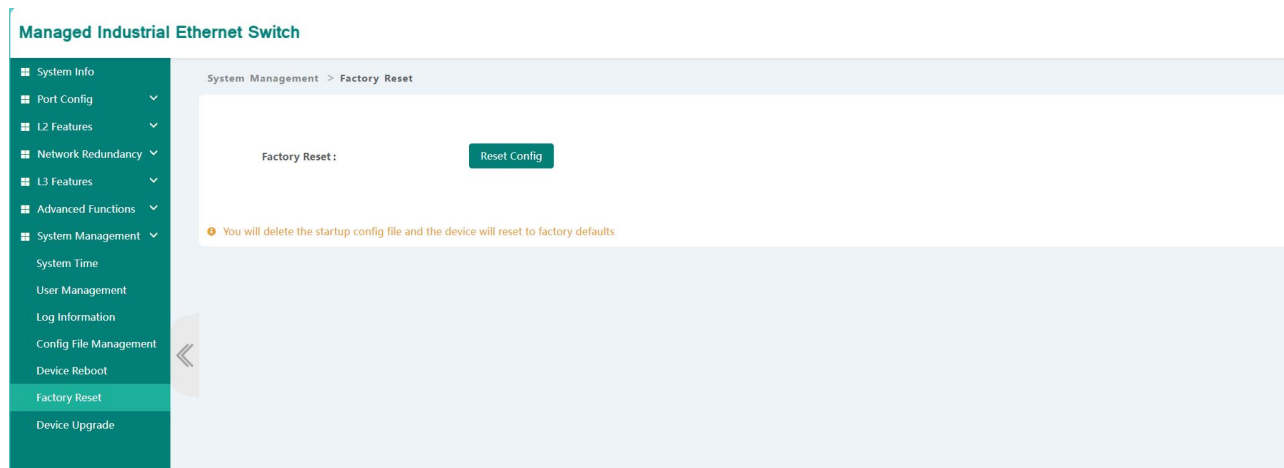


Figure 60 Factory Reset Page

Attention

1. After restoring factory settings via the web interface, all switch configurations (including the IP address) will revert to their default values, and the switch will automatically restart.

10.6 File Management

File management includes version upgrade, configuration file upload and download, running status file download, and configuration save. As shown in Figure 61.

Managed Industrial Ethernet Switch

System Management > Config File Management

Running Config Export Startup Config Import Startup Config Export Running State File

Save Config (Save the current running-config to startup-config, and also save all user accounts information.)

```

!
spanning-tree mst config
!
link-aggregation model create default
link-aggregation group 1
!
vlan database
vlan 1
!
interface vlan1.1
ip address 192.168.16.253/24
!
interface G1
mirror interface G2 direction receive
mirror interface G3 direction transmit
link-aggregation join group 1
!
interface G2
link-aggregation join group 1
!
interface lag1
link-aggregation mode lacp
!
ip igmp snooping
!
line vty
login local
!
end
    
```

System Management > Device Upgrade

The Current Version : V2.0.8906481.250828

Version Upgrade : Browse File Format: .img Suffix File **Upgrade**

⚠ Upgrading the devices will cause the unsaved config to be lost. You are advised to save the config before upgrading.

有较大改动

Figure 61 File management page

Save Config: This operation saves the current running configuration to the startup-config and also saves all user account information. This means the device will load this configuration upon restart.

Attention

1. Upgrading the devices will cause the unsaved config to be lost. You are advised to save the config before upgrading.

10.7 Exit the System

Log out of the web and return to the login page. As shown in Figure 62.

Figure 62 System Exit Page