

L2+ Managed Industrial Ethernet Switches

WEB User Manual

Version number: V1.0

Important statement

The provision of any information in this brochure by the Company does not imply that a corresponding license is provided for such information.

We have endeavored to make the information provided in this manual accurate and applicable, however, we do not accept any responsibility for the use of this information, nor do we accept any joint and several liability for its use. Products and user manuals may contain technical or typographical errors. The Company reserves the right to change all or part of the contents of this manual without prior notice.

Statement:

Please note that due to the constant updating and improvement of products and technologies, the contents of this material may not correspond exactly to the actual products. For product updates, please consult our website or contact our sales representatives directly.

Revision history

Version number	Date	Reasons
V1.0	2022.08	Creating documents

Instructions for safe use

The product is designed to perform well and reliably within the scope of use, but human damage or vandalism to the equipment needs to be avoided.

- Read this manual carefully and keep it for future reference
- Do not place the appliance near water or in a wet location
- Do not put anything on the power cable, keep it out of reach
- To avoid fire, do not knot or wrap the cable
- Power connectors and other equipment connections should be securely connected to each other and should be checked regularly
- Please take care to keep the fiber optic sockets and plugs clean. Do not look directly at the fiber cross section when the unit is in operation
- Please take care of the cleanliness of the equipment and wipe with a soft cotton cloth if necessary
- Do not repair the equipment yourself, except as expressly instructed in the manual

In the following cases, disconnect the power supply immediately and contact our company.

- Equipment water intake
- Broken equipment
- The equipment is working abnormally or the demonstrated performance has completely changed
- Smell, fumes or noise from equipment

Instruction: Explanatory information necessary in the use of this manual

Attention: Matters requiring special attention in the use of this manual

Catalogue

1 CONFIGURATION PREPARATION ..... - 6 -

1.1 Configuring the PC ..... - 6 -
1.2 Ping test ..... - 6 -
1.3 Logging in to the Web ..... - 7 -

2 INTRODUCTIONS TO WEB PAGES ..... - 9 -

2.1 Overall page ..... - 9 -
2.2 Upper area ..... -10 -
2.3 Central Region ..... - 12 -
2.4 Lower area ..... - 13 -

3 SYSTEM STATUS ..... - 13 -

3.1 Equipment information ..... - 13 -
3.2 Equipment status ..... - 14 -
3.3 Port information ..... - 15 -

4 PORT CONFIGURATION ..... - 15 -

4.1 Port configuration ..... - 15 -
4.2 Port Speed Limiting ..... - 17 -
4.3 Storm suppression ..... - 18 -

5 SECOND LEVEL CHARACTERISTICS ..... - 20 -

5.1 QoS configuration ..... - 20 -
5.2 VLAN configuration ..... - 24 -
5.3 MAC VLANs ..... - 29 -
5.4 Subnet VLANs ..... - 30 -
5.5 Protocol VLANs ..... - 31 -
5.6 IGMP eavesdropping ..... - 32 -
5.7 Static multicast tables ..... - 34 -
5.8 LLDP configuration ..... - 36 -
5.9 Port Isolation ..... - 38 -
5.10 MAC ACL ..... - 40 -
5.11 IP ACLs ..... - 42 -

6 LINK BACKUP ..... - 44 -

6.1 ERPS ..... - 44 -
6.2 Port aggregation ..... - 49 -
6.3 Fast spanning trees ..... - 50 -

7 ACCESS CONTROL ..... - 54 -

7.1 User passwords ..... - 54 -
7.2 Login control ..... - 55 -
7.3 Port authentication ..... - 57 -

7.4 Certification database ..... - 62 -
7.5 MAC port locking ..... - 64 -

8 REMOTE MONITORING ..... - 66 -

8.1 SNMP configuration ..... - 66 -

9 PORT STATISTICS ..... - 72 -

9.1 Receiving frame statistics ..... - 72 -
9.2 Sending frame statistics ..... - 73 -
9.3 Total flow statistics ..... - 74 -
9.4 MAC address table ..... - 75 -

10 NETWORK DIAGNOSTICS ..... - 77 -

10.1 Port mirroring ..... - 77-
10.2 Network diagnosis ..... - 78 -

11 SYSTEM ADMINISTRATION ..... - 79 -

11.1 Time Configuration ..... -79 -
11.2 Device addresses ..... - 82 -
11.3 System information ..... - 83 -
11.4 Log messages ..... - 84 -

1 Configuration preparation

1.1 Configuring the PC

To access the switch via the Web, the IP addresses of the switch and the PC must be in the same network segment. The switch is shipped with an initial IP address of 192.168.40.253. To modify the IP address of the PC to ensure that it is on the same local area network as the IP of the switch, Windows users should refer to the following steps:

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

The specific operating pages of the Windows system are shown inFigure1 shown in Figure 1.

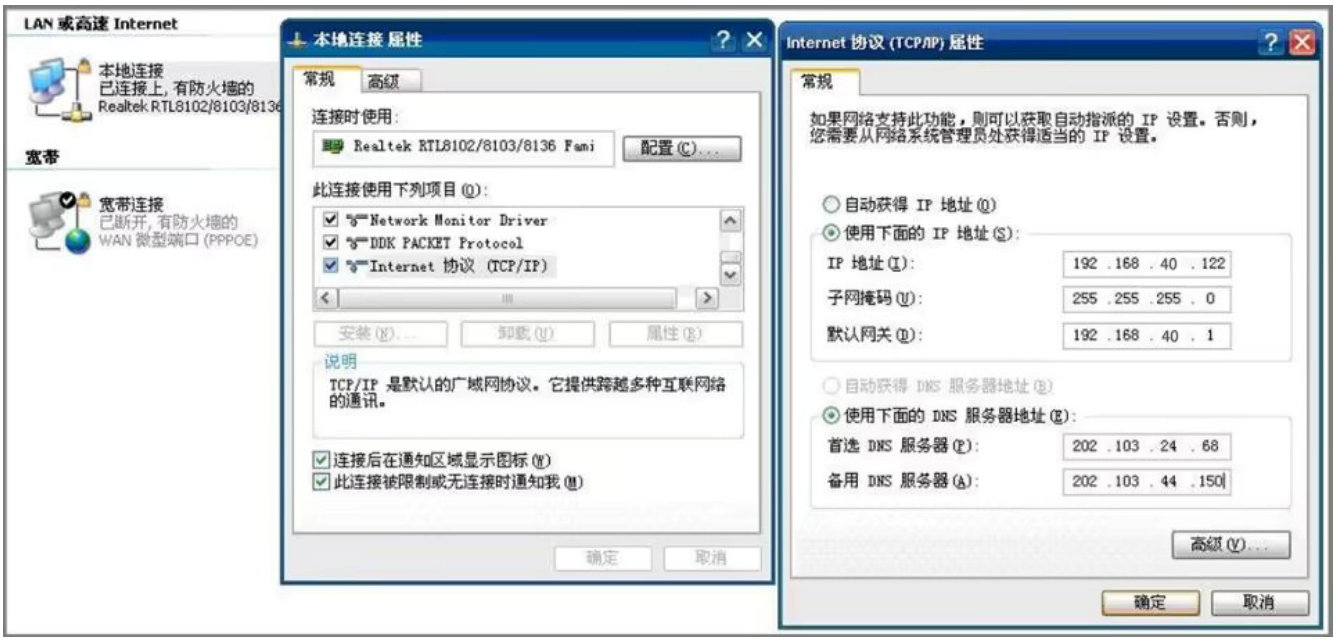


Figure1 IP settings page for Windows environment

Follow the above operation to change the IP address of the PC to 192.168.40.X (X is any valid value from 2 to 254 except 253), and after successful modification, you can use this IP address to access the Web.

1.2 Ping Test

When 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. windows users, please refer to the following operation:

- **Start → Run → type "cmd" → click "OK".**
- Enter the command "ping 192.168.40.253" in the command line program on Windows, as shown inFigure2 shown in Figure 2.

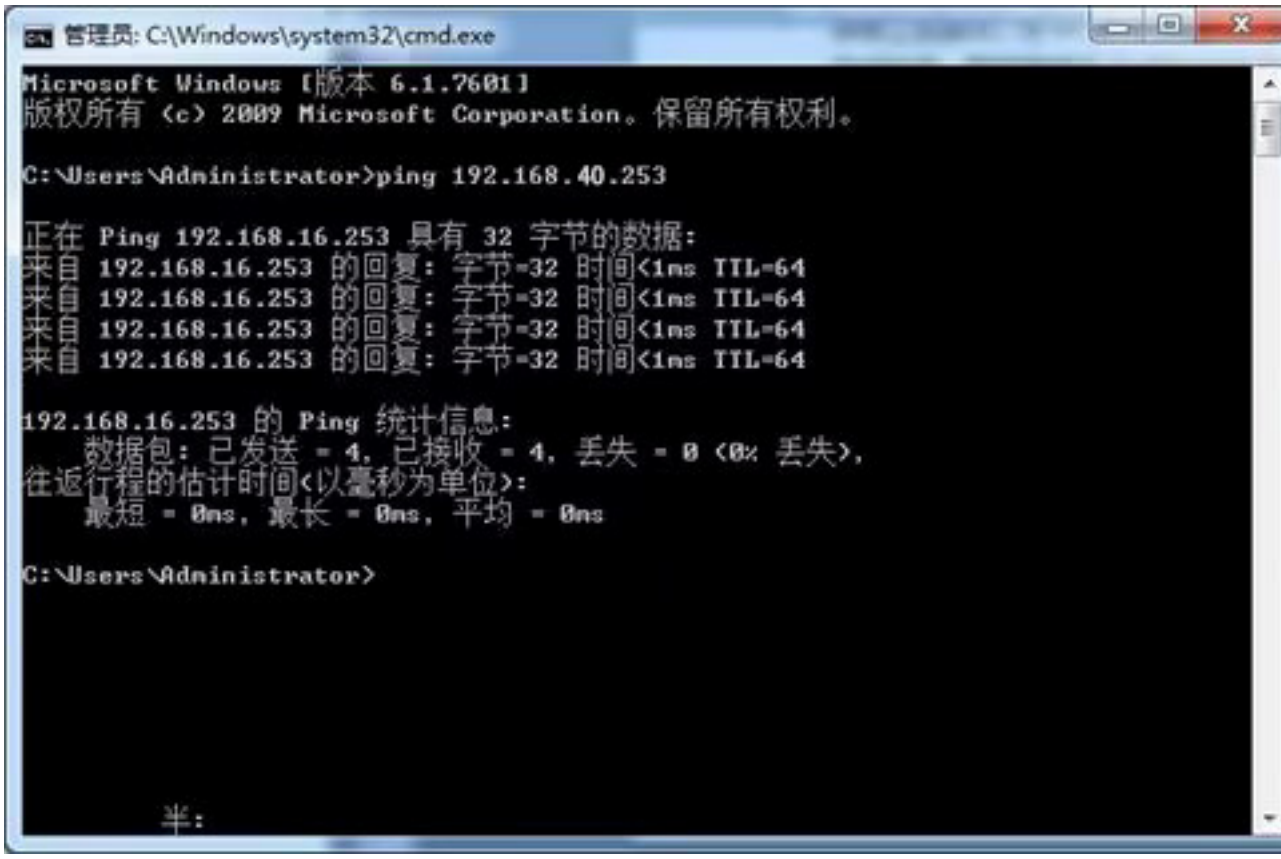


Figure2 Using the ping command in a Windows environment

If the Ping works, the PC and the switch are connected properly, otherwise check the network connection.

1.3 Login to Web

Open your browser and enter the default IP address of this switch in the address bar, asFigure3 shown.



Figure3 Browser address bar page

After hitting the Enter key, a pop-up will appear as shown inFigure4 The user login page shown in Figure 4 prompts for a username and password.



Figure4 User login page

The default username and password are both "admin". If the user name or password is not entered correctly, the switch's web server will provide three chances to enter the user name and password, if the

user name and password are entered incorrectly three times, the browser will display the error message "401 Unauthorized" and you will need to re-enter the switch's IP address after the error message. Enter the correct user name and password and you will be taken to the main page of the web server after successful authentication.

2 Web Page Introduction

2.1 Overall page

说明

The following pages and configurations of all features are based on the actual product.

After login verification, you will enter the main web page of the switch, which is divided into three main areas: the upper part is for the logo, shortcut keys and menu bar, the middle part is for the main function display, and the lower part is for the copyright display. As shown inFigure5 The web page is divided into three main areas, the top area is for the logo, shortcut keys and menu bar, the middle area is for the main function display and the bottom area is for the copyright display.

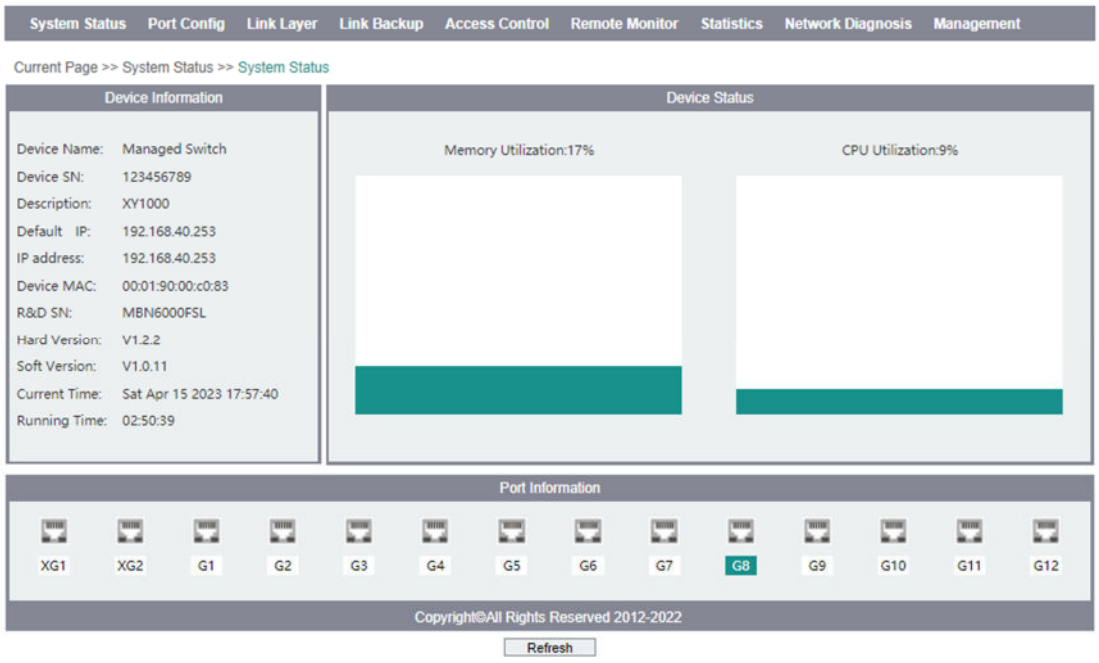


Figure5 Web server main page

Attention!

This user can use IE, Firefox, Google and other browsers to access the web server. The pages displayed by different browsers may vary, so if this affects normal usage, please change to a

mainstream browser such as IE, Firefox, Google and other browsers.

2.2 Upper area

The upper area includes the company logo, shortcut keys (to enable switching between English and Chinese and to exit), the IP and MAC address of the PC, and the function menu bar.

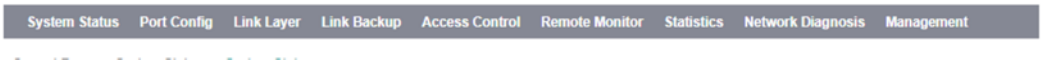


Figure6 Upper area page

At any time the user can log out by clicking on the "Logout" link in the top right hand corner of each page, which displays as followsFigure7 The page shown in Figure 7 is displayed.

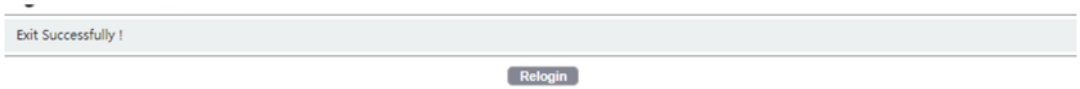


Figure7 Logging out of the login page

Clicking on the "Re-login" button will bring you back to the login authentication window.

The function menu has a two-level directory structure. The primary directories are System Status, Port Configuration, Layer 2 Features, Link Backup, Access Control, Remote Monitoring, Port Statistics, Network Diagnostics and System Management. Mouse over the first level directory will have the second level directory expanded. The web menu is shown inFigure8 shown in Figure 8, with the following functionsTable1 The functions are shown in Table 1.

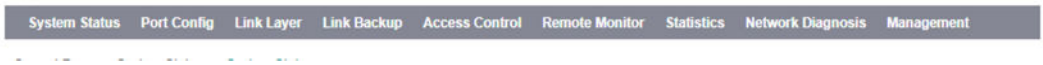


Figure8 WEB menu page

Table1 Table of menu function descriptions

Menu items	Page tabs	Page Features
System Status	Equipment information	Device information , e.g. device name, device number, software version, factory default IP address, etc.
	Equipment status	Device operation, e.g. CPU utilization, memory utilization, etc.
	Port Information	Port information, e.g. port status, number of ports, etc.
Port configurati onon	Port configuration	Configure the basic information of each port of the switch, such as: rate mode, flow control status, etc.
	Port Speed Limit	Control and management of the rate of each entrance and exit of the switch

Menu items	Page tabs	Page Features
	Storm suppression	Rate control management of the data types for each entrance and exit of the switch
Second layer characteristics	QoS configuration	Set 802.1p priority, port priority, DSCP priority, etc.
	VLAN configuration	Configure 802.1Q VLANs, display VLAN list
	MAC VLAN	Configuring MAC-based VLANs
	Subnet VLAN	Configuring VLANs based on IP subnets
	Protocol VLAN	Configuring protocol-based VLANs
	IGMP Listening	Configure IGMP snooping function
	Static Multicast Table	Configure static multicast MAC addresses and their corresponding ports
	LLDP configuration	Configuring the LLDP function
	Port Isolation	Configuring port isolation
	MAC ACL	Configuring MAC ACL rule lists
	IP ACL	Configuring IP ACL rule lists
Link backup	ERPS	Set ERPS port and node type etc.
	Port aggregation	Set the aggregation group of the port
	Fast spanning tree	Setting parameters for fast spanning trees
Access control	User Password	Management of user rights and passwords
	Login control	Client IP address for restricted access
	Port Authenticationn	Separation of business and authentication
	Certification database	Adding and deleting usernames and passwords saved in the database
	MAC port lockout	Binding a MAC address to a port can be set
Remote monitoring	SNMP configuration	Provide SNMP agent to manage switch devices
	Email Log	Periodic email delivery of system logs to user specified mailboxes

Menu items	Page tabs	Page Features
Port statistics	Receiving frame statistics	Statistics of various received frames, e.g. unicast, multicast, etc.
	Sending frame statistics	Statistics for various transmit frames, e.g. unicast, multicast, etc.
	Total traffic statistics	Statistics of various transmitted and received frames, e.g. unicast, multicast, etc.
	MAC address table	Display of MAC address status
Network Diagnostics	Port Mirroring	Set the mirrored and capture ports
	Network Diagnostics	Network fault analysis, network testing or problem solving
System administration	Time Configuration	Setting the system time, etc.
	Set address	Setting the IP address
	System Information	Equipment model, CPU and other relevant parameters
	Log information	Display of log information and the possibility of managing it
	Document Management	Perform switch software upgrades to obtain, save or restore switch settings

2.3 Central Region

The central area is the function display area, where the parameters of the function can be viewed and configured. AsFigure9 is shown.

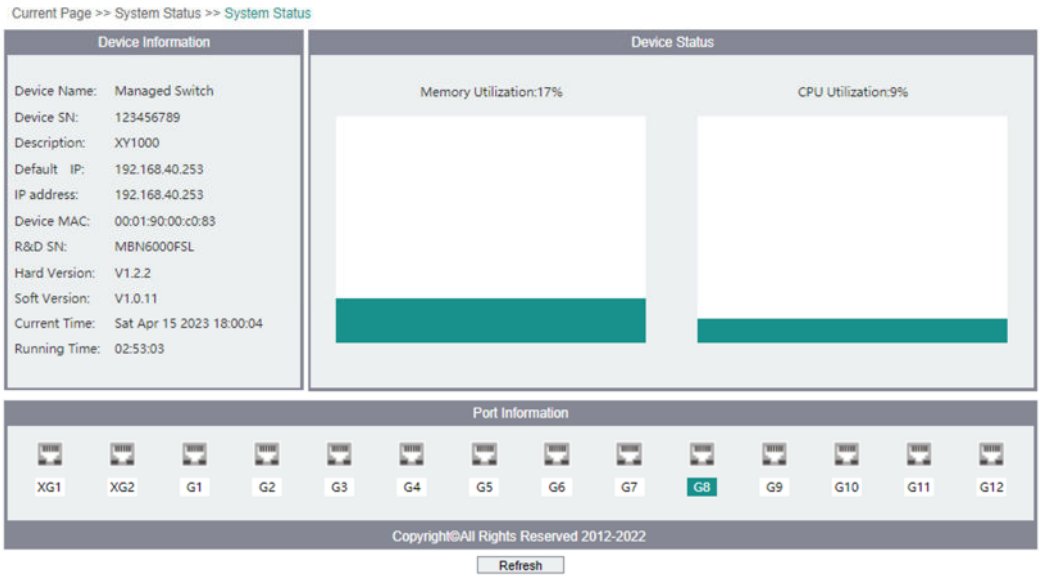


Figure9 Function display area page

2.4 Lower area

The bottom area displays the system copyright information. As shown in Figure10

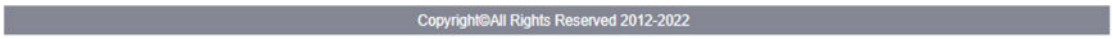


Figure10 Bottom area page

3 System Status

3.1 Equipment information

The device information includes the switch name, number, description, factory IP, MAC address, hardware version, software version, etc. The page is shown in Figure11

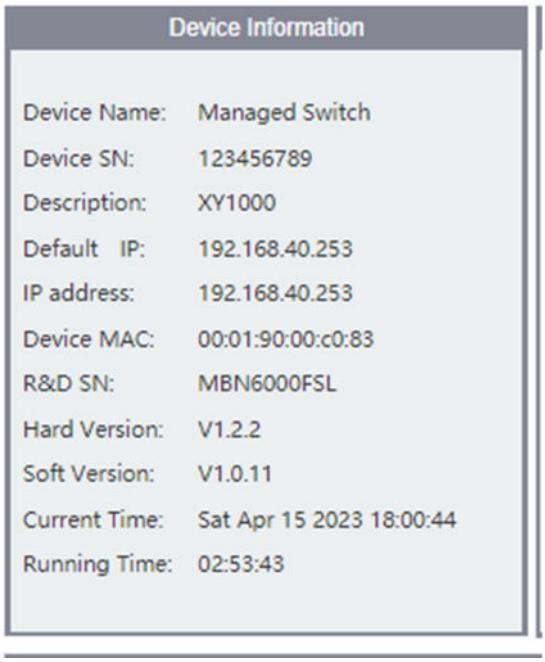


Figure11 Equipment information page

Device name: The name of the switch.

Device Number: Describes the switch's factory number.

Device Description: Provides a summary description of the switch.

Factory IP: The IP address of the switch after it has been restored to its factory settings.

MAC address: MAC address of the switch.

Development code: The current development code of the switch.

Hardware version: The current hardware version of the switch.

Software version: The firmware version currently installed on the switch.

Current time: The current time of the switch.

Runtime: A running timer from the time the switch is powered on, this time will also be re-calculated from zero when the switch is reset or restarted from a power failure.

3.2 Equipment status

The device status shows the system memory and CPU usage in green bars, as shown in Figure12. Changes to this value must be manually refreshed on this page to be seen.

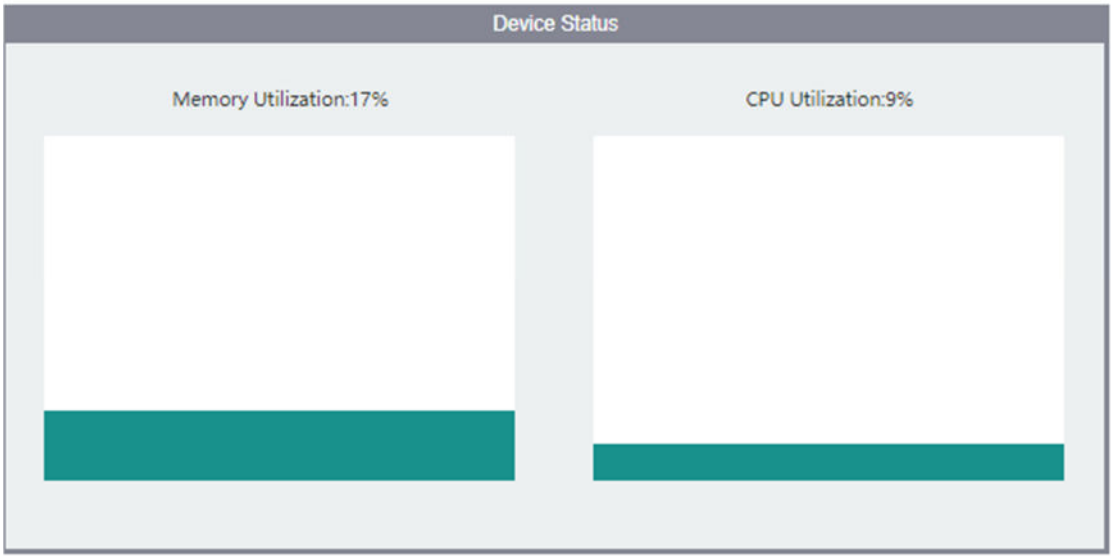
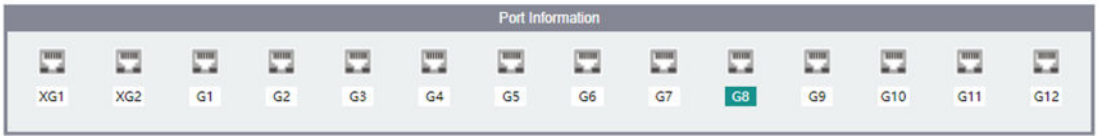


Figure12 Device status page

Memory Utilisation: The utilisation of the switch's memory, reflecting how much memory is used.

CPU Utilisation: The CPU utilisation of the switch, reflecting how busy the CPU is being used.

3.3 Port Information



For different switch models, the total number of ports varies. The background colour of the port number is shown in green when the port is properly connected and in white when the connection is bad or not connected, as shown Figure13.

Figure13 Port information page

4 Port configuration

Port configuration includes: port configuration, port speed limiting and storm suppression.

4.1 Port configuration

The Port Configuration page is where port parameters are configured and the port status is displayed. The port configuration page is shown inFigure14 shown in Figure 14.

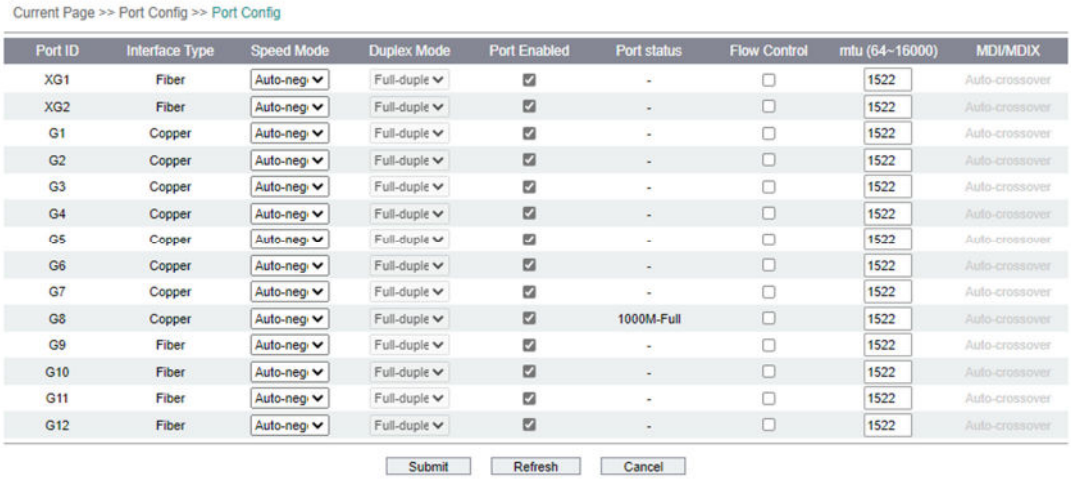


Figure14 Port configuration page

Configuration notes

Port number: The label of the switch port.

Interface type: shows the type of interface, e.g. electrical, optical, etc.

Rate modes: including auto-negotiation, 10 Gigabit rate, 100 Gigabit rate, Gigabit rate, etc. The range of rate modes and default rate modes supported by different types of ports vary, depending on the actual model.

Duplex mode: includes full duplex and half duplex and is only enabled in forced rate mode.

Port Enabled: Check to enable the port, uncheck to disable this port.

Port Status: Shows the rate status of the port.

Flow control: Flow control is used to handle data transfer rate management between two transmission nodes, both nodes must support flow control mechanism to play its role, if the connected network equipment does not support flow control mechanism, it is recommended that users turn off this function, because too many pause frames or conflicting signals may cause communication problems.

Pole shift: The switch supports Auto-MDI/MDIX technology, with automatic port flipping on all ports, allowing free switching between MDI (Medium Dependent Interface) and MDIX (Medium Dependent Interface Crossover) as required. Interface) as required.

Instructions

The switch provides a web page for configuration, all configuration parameters will be submitted to the switch after the "Configure" button is clicked and any changes made by the user will be cancelled if you exit this page before then. Clicking the "Cancel" button will not commit the user's changes and will restore the settings to the way they were before the changes were made.

Attention!

1. Gigabit optical ports support only auto-negotiation and Gigabit full duplex rate modes;

2. (a) Auto-negotiation mode is the default rate mode for all electrical ports. When an electrical port is in auto-negotiation mode, the network equipment connected to it should also be in auto-negotiation mode, otherwise the auto-negotiation failure switch will set the port to the default half-duplex mode, which may cause communication problems;
3. Flow control is used to handle data transfer rate management between two transmission nodes, both nodes must support flow control mechanism to play its role, if the connected network equipment does not support flow control mechanism, it is recommended that users turn off this function;
4. Flow control can be enabled or disabled, the default is disabled. The use of flow control can cause a lot of pause frames to be sent out and a pause frame storm can occur when there is a lot of data, so please use the flow control function with caution.

4.2 Port Speed Limit

The Port Speed Limit page provides port-based speed limits, including ingress and egress speed limits. Users are able to limit traffic per port or remove port traffic limits. Users are able to select a fixed speed in the range of: 64Kbps ~ 1000Mbps with a minimum granularity of 64Kbps (subject to actual model). The device provides rate limiting in two directions, where the ingress speed is the actual speed at which traffic flows from other devices such as PCs to the switch port. The egress speed is the actual speed flowing from the switch port to other devices.

The Port Speed Limit page is shown in Figure15

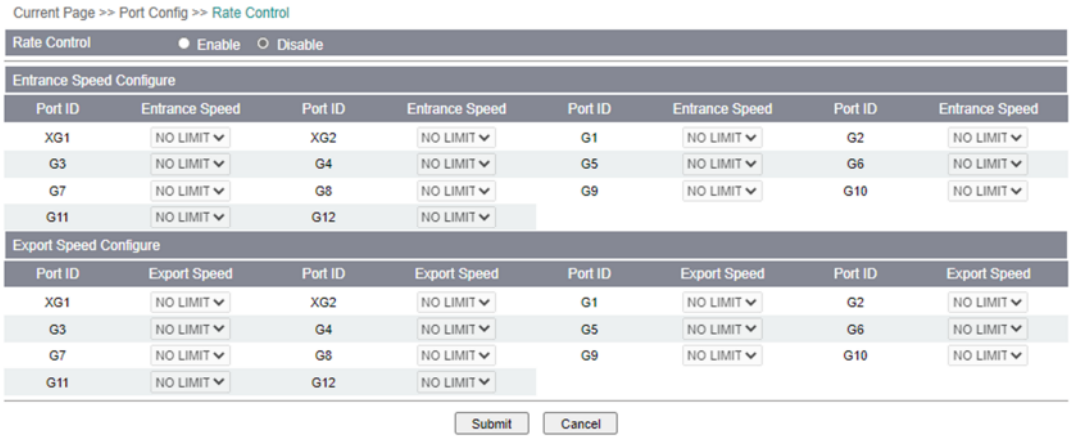


Figure15 Port Speed Limit page

Configuration notes

Port Speed Limit: Enables or disables the rate configuration function.

Ingress speed configuration: ingress speed configuration for each port, the selectable rate range is based on the actual port bandwidth.

Egress speed configuration: Egress speed configuration for each port, the selectable rate range is based on the actual port bandwidth.

Configuration: After you have configured the above entries, you need to click on this button for the configuration to take effect.

Cancel: By clicking this button, the unsaved configuration will not take effect and the page will refresh and revert to what it was before the operation.

Attention!

If both ingress and egress speeds are restricted on a link, the actual speed is the lesser of the two values.

4.3 Storm suppression

The Storm Suppression feature is used to prevent the switch's ports from being damaged by broadcast, unknown multicast or unknown unicast storms in the network.

The storm suppression page is shown inFigure16 shown in Figure 16.

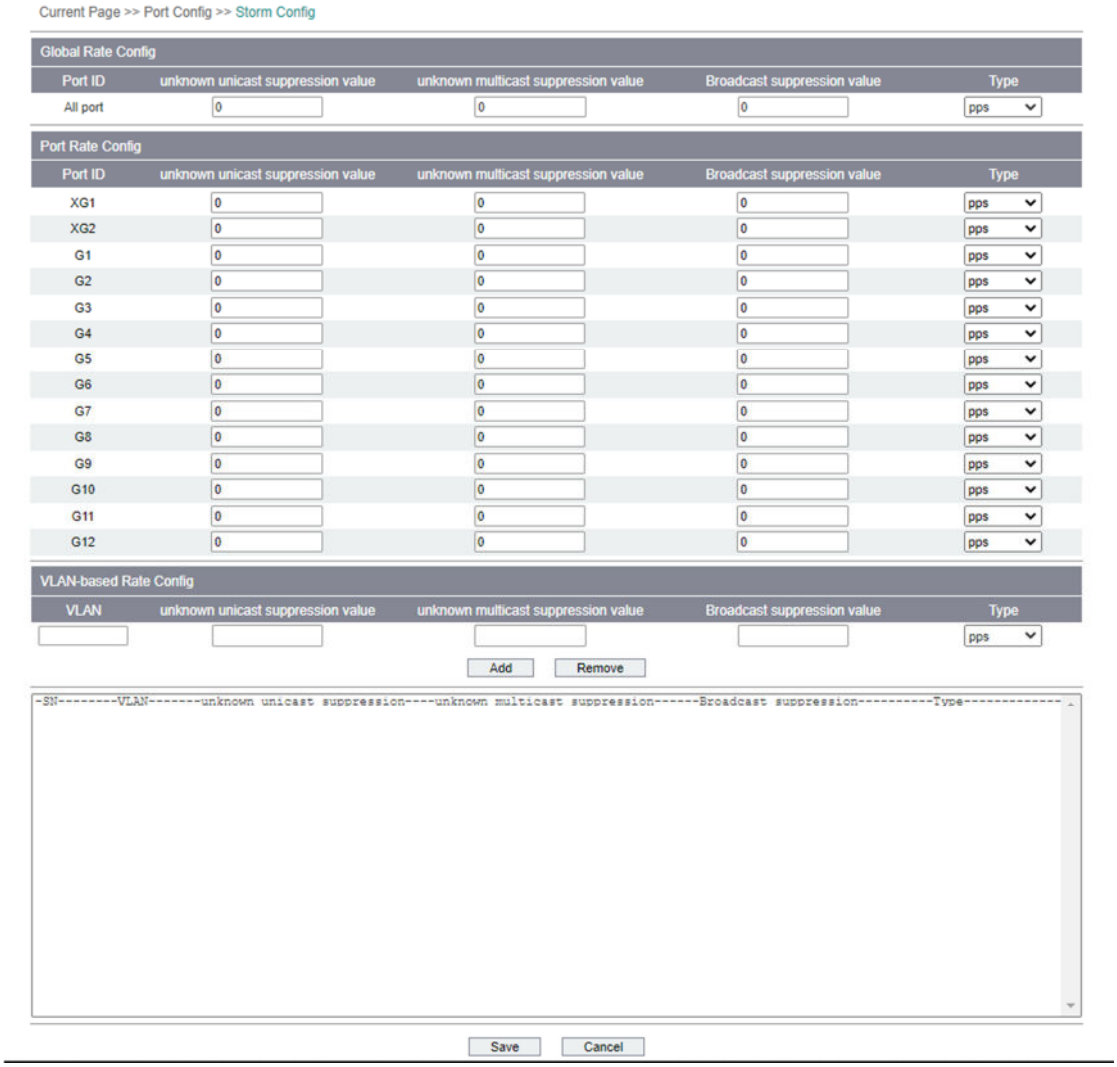


Figure16 Storm suppression page

Storm Suppression Control: Select the type of control for storm suppression, which can be global or port.

Global storm suppression: When the control type of storm suppression is global, the storm suppression parameters of all ports can be configured uniformly here.

Port storm suppression: When the control type of storm suppression is port, the storm suppression parameters for each port can be configured separately here.

Port number: displays the name of the port to be configured, either all ports or a specified port.

Unknown unicast suppression value: Configure the suppression rate for unknown unicast packets.

Unknown multicast suppression value: Configure the suppression rate for unknown multicast packets.

Broadcast suppression value: Configure the broadcast packet suppression rate.

Suppression type: Configure the unit of rate suppression, kbps and pps are available.

Configuration: After you have configured the above entries, you need to click on this button for the configuration to take effect.

Cancel: By clicking this button, the unsaved configuration will not take effect and the interface will refresh and revert to what it was before the operation.

5 Second layer characteristics

Layer 2 feature configuration includes: QoS configuration, VLAN configuration, MAC VLAN, subnet VLAN, protocol VLAN, IGMP listening, static multicast table, LLDP configuration, port isolation, MAC ACL, IP ACL.

5.1 QoS Configuration

QoS (Quality of Service), the quality of service function, is implemented by the switch's internal priority queue, with packets in the higher priority queue staying in the switch for a shorter period of time, and packets in the lower priority queue the opposite. Based on the port ID, MAC address, 802.1p priority tag, DiffServ and IP TOS, the switch is able to classify packets to an appropriate level and then forward them to the appropriate egress queue by level.

The entire QoS configuration page is divided into five sections, Qos configuration, Qos control type, Qos weight, 802.1p priority configuration and DSCP priority configuration, as shown in Figure17

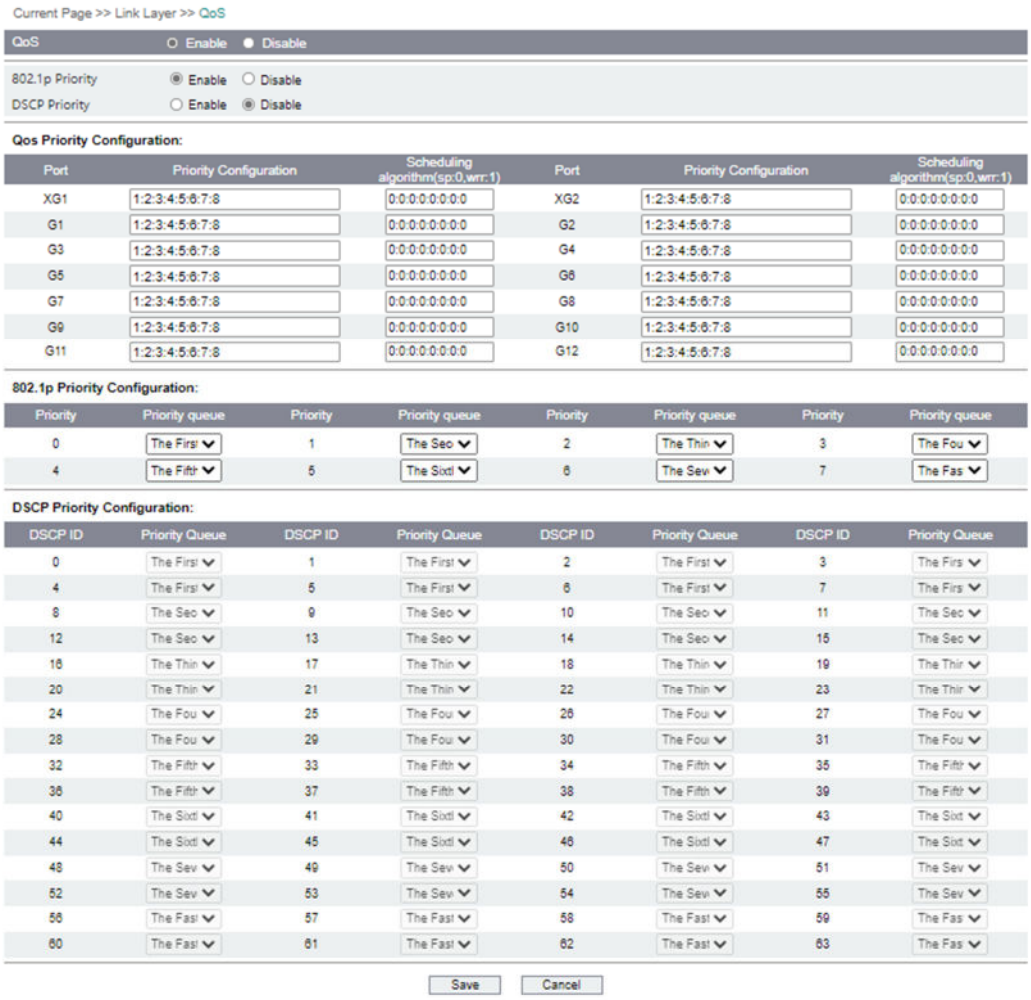


Figure17 QoS configuration page

Description of configuration parameters

QoS configuration: Enabling/disabling of the entire functionality of Qos.

QoS control type: choice of priority mode, with absolute/relative priority available.

802.1p priority: enable/disable this priority.

DSCP priority: enable/disable this priority.

QoS weight: Configure the weight ratio of the 8 priority output queues of each port in the format of "First queue weight:Second queue weight:Third queue weight:Fourth queue weight:Fifth queue weight:Sixth queue weight:Seventh queue weight: Fastest queue weight", the values of the weights of each queue range from 1 to 8.

802.1p Priority Configuration: Configure the mapping relationship from 802.1p priority to priority queue.

Priority marker: 802.1p priority marker, 8 in total (3 bits).

Priority queues: Handle packets of different priority levels, up to 8 priority queues are provided per port. They are: first queue, second queue, third queue, fourth queue, fifth queue, sixth queue, seventh queue and fastest queue, in descending order of priority.

DSCP priority configuration: Configure the mapping relationship of DSCP priority to priority queue.

DSCP logo: DSCP priority flag, 64 in total (6 bits).

QoS configuration



When QoS is disabled, all the options below are disabled and all packets go to the lowest priority queue. Setting up QoS starts with selecting the Enable item, as shown in Figure18

Figure18 QoS configuration page

Type of QoS control

QoS control types include "absolute priority" and "relative priority". When "Absolute Priority" is selected, the switch will process the packets in the high priority queue before processing the packets in the low priority queue; when "Relative Priority" is selected, the switch will prioritize the data in the high priority queue while When "Relative Priority" is selected, the switch will give priority to the data in the high priority queue while processing the data in the low priority queue.

There are two types of priority: 802.1p priority and DSCP priority, and several can be enabled at will, as shown in Figure19.



Figure19 Priority type configuration page

When the priority enable type is selected, the QoS priority adjudication mechanism forwards the incoming packets to the appropriate egress queue according to the rules specified by the switch chip. If both priority levels are turned on at the same time, only the priority type with the highest level works; the lower priority level works only if the higher priority level is not enabled.

802.1p priority

802.1p is an extension of the IEEE802.1Q (VLAN tagging technology) standard and they work in tandem. In essence, it provides a mechanism for enforcing QoS at the Layer 2 MAC (Media Access

Control) layer. there are two parts to a VLAN tag: the VLAN ID (12 bits) and the priority (3 bits). the priority field is not defined and used in the IEEE802.1Q VLAN standard, whereas it is defined in 802.1p, so There are 8 classification levels (3 bits) available for IEEE802.1p priority, and 3 bits in the IEEE802.1Q tag as user priority. This is shown in Figure20

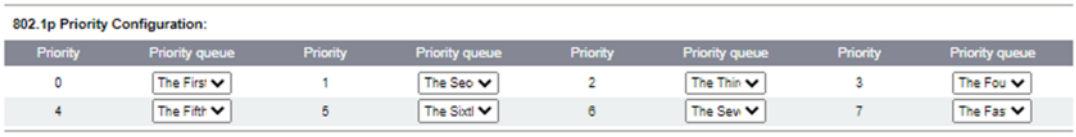


Figure20 802.1p priority configuration page

802.1p priority 0 is the default value and is automatically enabled if no other priority value is set. By default, the device maps 802.1p priority 0 to 6 to queues 1 to 7 respectively, and 802.1p priority 7 to the fastest queue.

DSCP Priority

DiffServ, or Differentiated Services, is specified as a simple, scalable, roughly segmented computer network architecture that is used at Layer 3 in recent IP networks to manage network communications and provide quality of service guarantees. For example, DiffServ can be used to provide short response times to ensure the smooth passage of critical network data such as audio or video, and to provide simple, best-effort communication guarantees for non-critical data communications such as web communications or file transfers.

DiffServ is a three-layer representation scheme that uses the DSCP field in the IP header to store priority information, using 6 of the 8 bits of the TOS field in the IP header (note the bit order here), so there are a total of 64 priority divisions that are also TOS compatible. DSCP is an advanced and intelligent approach when differentiating the priority of different classes of traffic. Based on the DSCP (DiffServ Code Point) value in the IP message header, the switch is able to classify the class of service for communication packets. The switch supports DSCP for both IPv4 and IPv6. if DSCP prioritisation is enabled, the switch will prioritise traffic based on the DSCP value. the DSCP configuration is shown inFigure22 The DSCP configuration is shown in Figure 22.

DSCP priority 0 is the default value and is automatically enabled if no other priority value is set. By default, the device maps DSCP priority 0~7 to the first queue, i.e. the lowest priority queue; DSCP priority 8~15 to the second queue; DSCP priority 16~23 to the third queue; DSCP priority 24~31 to the fourth queue; DSCP priority 32~39 to the fifth queue; DSCP priority 40~47 to the sixth queue; DSCP priority 48~55 to the seventh queue; and DSCP priority 48~55 to the seventh queue. to the sixth queue; map DSCP priority 48~55 to the seventh queue; map DSCP priority 56~63 to the highest priority queue, i.e. the queue with the fastest forwarding.

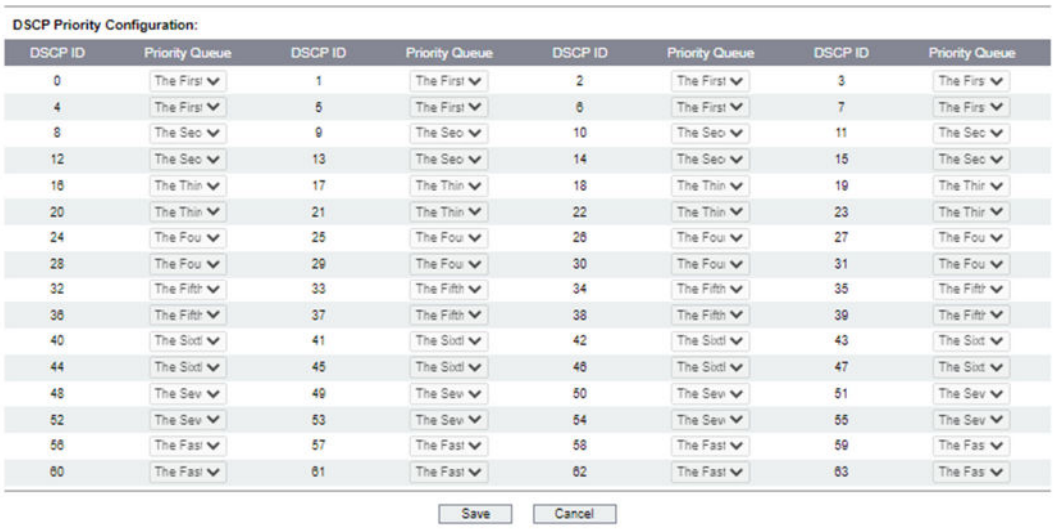


Figure21 DSCP priority configuration page

Attention!

1. Since there are only 8 priority forwarding queues inside the switch, but a total of 64 DSCP priorities, multiple DSCP priorities will be in the same forwarding queue by default, and all packets in the same forwarding queue will have the same priority at the true "hardware" level, regardless of the fact that they may be set to different priorities at the software level. They may be set to different priorities at the software level.
2. Absolute priority means that the data in the fastest priority queue is processed first, then the data in the lower priority queue is processed, and finally the data in the lowest priority queue is processed; while relative priority means that the data in the fastest priority queue is processed along with the data in the lower priority queue. The forwarding ratio of each queue on each port is set according to the QoS weighting ratio.
3. DSCP priority > 802.1p priority when multiple priority levels are enabled at the same time.
4. 802.1p is an extension of 802.1Q, and the priority mark is stored in the VLAN Tag, so it is only valid for 802.1Q VLAN packets.
5. The DSCP priority identifier is stored in the IP header and is therefore only valid for IP packets; the priority of DSCP data frames can traverse the entire Internet; DSCP is backwards compatible with IPv4 TOS and allows corresponding operation with devices using the Layer 3 TOS priority scheme.

5.2 VLAN Configuration

VLAN (Virtual Local Area Network) refers to Virtual Local Area Network technology. VLANs are a method of creating separate logical networks from an actual physical network, enabling several virtual LANs to exist simultaneously within an actual physical network.VLANs are effective in reducing broadcast range and facilitating network management through separate logical network segments (e.g. company

departments) that cannot exchange data.VLANs are effective in suppressing broadcast storms.

IEEE 802.1Q VLAN

Virtual LANs can be partitioned across multiple switches through the IEEE802.1Q protocol. The same VLAN of different switches can communicate, and different VLANs of different switches cannot communicate. This switch supports the standard IEEE802.1Q protocol and is compatible with other switches that support the IEEE802.1Q protocol standard. It also supports the modification of 802.1Q tags and can connect devices that can recognize 802.1Q tags or cannot recognize 802.1Q tags.

The networking method can be found belowFigure22 shown below.

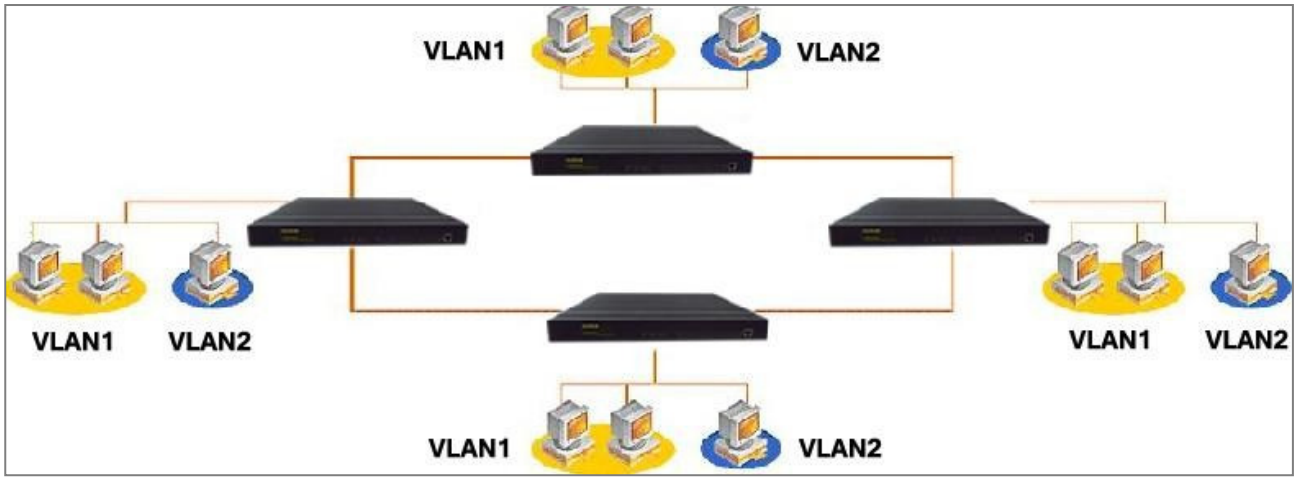


Figure22IEEE 802.1Q VLAN topology diagram

IEEE 802.1Q VLANs can be configured via the Web page as shown in Figure23

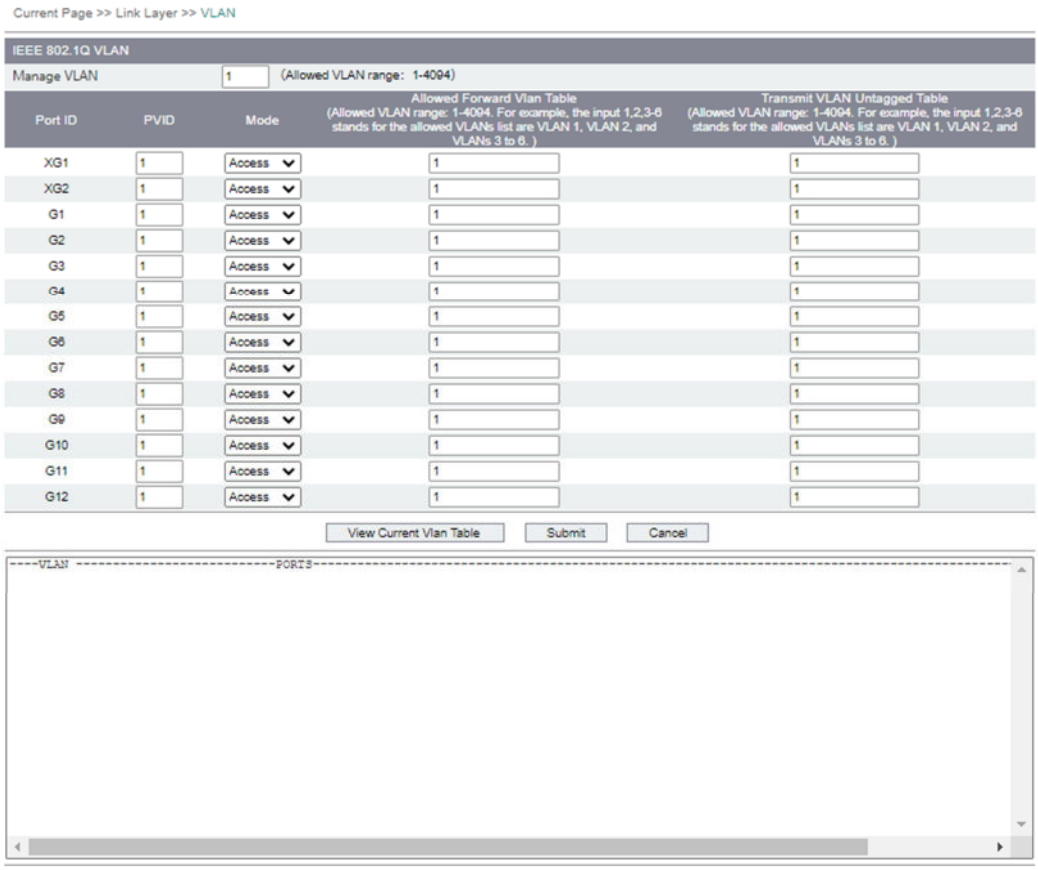


Figure23 IEEE 802.1Q VLAN configuration page

The page is divided into two areas, the upper part is the IEEE 802.1Q VLAN function configuration area, and the lower part shows the list of 802.1Q VLAN groups currently configured by the device and their corresponding ports.

Configuration notes

Management VLAN: The management VLAN is used for Trunk link bearing and identifying management control information. When a user wants to manage the switch, the switch port connected to the PC must join the management VLAN, otherwise it cannot be accessed. The default management VLAN for this switch is 1.

Port number: The label of the switch port.

PVID: The default VLAN ID of the port. the PVID of an Access port is the same as the VLAN it is allowed to pass through. the PVID of a Trunk port and Hybrid port must be one of the VLANs it is allowed to pass through.

Port Mode: The type of switch port, classified as Access port, Trunk port and Hybrid port.

The list of allowed VLANs: The set of allowed VLANs, which can also be interpreted as the set of

VLANs added to this port; there can only be one allowed VLAN for Access ports, and multiple allowed VLANs for Trunk and Hybrid ports. The range of values is from 1 to 4094, and the VIDs are connected by "," and "~". For example, "1,2,4~6" means the port allows VLANs 1, 2, 4, 5 and 6 to pass through.

Egress Untagged VLAN List: The set of egress untagged VLANs. For Hybrid ports, this value is configurable from 1 to 4094, with "," and "~" connecting each value. For example, "1,2,3~6" means that messages exiting the port with VIDs 1, 2, 3, 4, 5 or 6 will be stripped of their tags, while the tags of other messages will be retained.

View the currently configured VLAN table: When the VLAN configuration is complete, you can click on "View currently configured VLAN table", which will display a list of currently configured 802.1Q VLAN groups and their corresponding ports in the box below. If you have not reached your target, you can continue to configure in the configuration area above, or click "Configure" to save if you have reached your target.

The processing policy of each port of this series of switches for messages is as followsTable2 The policy for each port of this series is shown in Table 2.

Table2 Port handling policies for 802.1Q VLANs

Port Type	Port Description	Default PVID	Processing of incoming telegrams (incoming)		Processing of sent telegrams (out)
			Without Tag	With Tag	
Access	Access ports, which connect PCs or terminals, can only belong to 1 VLAN.	1	Receive the message, tag it with the port PVID and look up the VLAN Table for forwarding	Receive the message and find the VLAN Table for forwarding	Delete the Tag of the message and send it again
Trunk	Trunk ports, connecting between network devices with VLAN capability, can allow multiple VLANs to pass through and can receive and send messages for multiple VLANs.	1	Ibid	Ibid	Determine the VID of the message, if the VID is the same as the PVID then strip the Tag and send it, otherwise keep the Tag and send it

Hybrid	Hybrid ports, which can be used to connect between switches or to connect PCs, can allow multiple VLANs to pass through and can receive and send messages from multiple VLANs.	1	Ibid	Ibid	Determine if the VID of the message is in the "untagged VLAN list for egress", if so, strip the tag and send it, otherwise keep the tag and send it

Attention!

1. This switch has a default VLAN of 1 in IEEE 802.1Q VLAN mode, and all ports are configured as Access ports by default.
2. The PVID of the Access port is 1 by default, and the user can only configure the "List of allowed VLANs" table entry, which can only be configured for one VLAN since the Access port can only belong to one VLAN. After configuration, both the PVID of the port and the value of "VLAN list without tagging" are automatically set to the same value as the VLAN, which means that the VLAN Tag of all the messages out of the Access port will be stripped.
3. Trunk ports are added to the management VLANs by default, and users can only configure the "List of allowed VLANs" table entry. Once configured, the Trunk port will join all VLANs contained in this list (regardless of whether the list contains management VLANs or not, the port will join by default), and the value of "Egress Untagged VLAN List" is the management VLAN, which means that the VLAN Tag will be stripped when the management VLAN's packets exit the Trunk port, and the rest of the packets will be retained. Tag will be stripped from the management VLAN when it exits the Trunk port, and the rest of the messages will be retained.
4. The user can configure the PVID of the port and one or more values for the "List of allowed VLANs" table entry, but it cannot be empty; when the "List of untagged VLANs on egress" is configured as empty, it means that the VLAN Tag of all messages going out of the port will be retained and can only be within the parameters of the "List of allowed VLANs" configuration. When the "VLAN list for untagged egress" is configured as empty, it means that the VLAN Tag of all the messages going out from this port will be retained and can only be within the configuration parameters of the "VLAN list for allowed pass-through".
5. Once the configuration is complete, the user can click on the "View currently configured VLAN table" button. This button will check if the configuration values are correct and if so, the configuration of each VLAN will be displayed in the list below. This button only serves as a check and preview, it does not make the configuration effective. Once the user has confirmed that the current configuration is correct, they can click on the "Configure" button to save the configuration

and make it effective.

6. If the user wants to access a non-directly connected switch, they must ensure that the port connected to the PC is in the management VLAN, and if the port is a Hybrid port (not recommended), they must also ensure that its PVID is within the VLAN range allowed on the Trunk port used to interconnect the switch.
7. Some PC's NICs cannot receive messages with VLAN Tag, so be careful to strip the VLAN Tag from the ports connected to the switch and PC.

5.3 MAC VLAN

There are three types of VLAN mapping rules for the series' ports: MAC-based, subnet-based and protocol-based VLAN rules.

The MAC VLAN configuration page is shown inFigure25 shown in Figure 24.

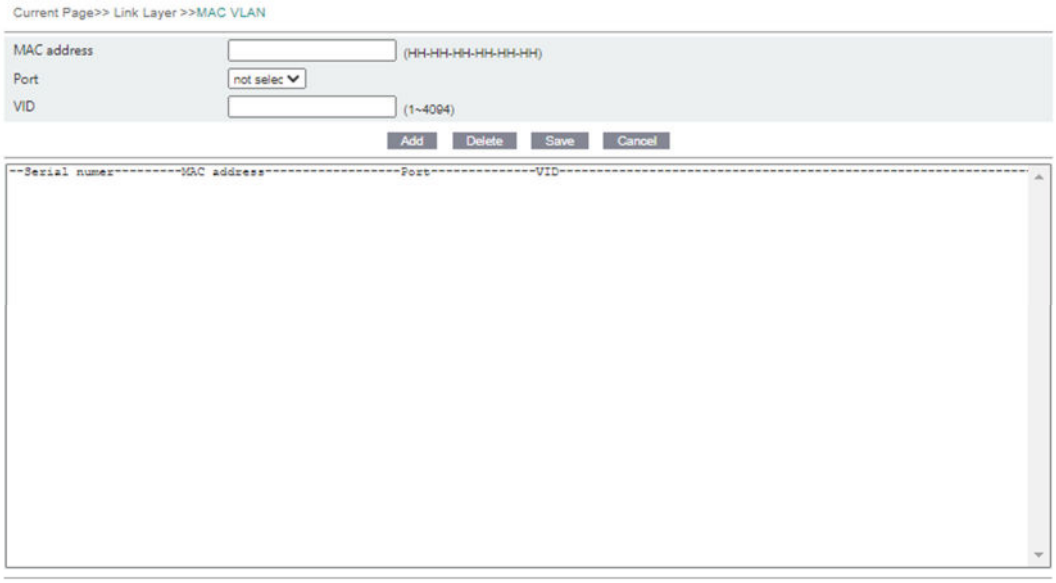


Figure24 MAC VLAN configuration page

This page is divided into two parts, the upper part configures the MAC VLAN rules of the port, and the lower part displays the MAC VLAN rules list of the port. The description of each configuration item is as follows:

MAC address: the source MAC address matched by the rule, expressed as a hexadecimal number in the format HH-HH-HH-HH-HH-HH-HH.

Port: The port number of the switch that the rule matches.

VID: The VID to be assigned, the range of values is 1 to 4094.

Add: Adds the above VLAN rule configuration to the below VLAN rule list.

Delete: Delete the VLAN mapping rule selected in the VLAN rule list below.

Save configuration: Save all VLAN mapping rule configurations in the VLAN rule list below.

Cancel: By clicking this button, the unsaved configuration will not take effect and the interface will refresh and revert to what it was before the operation.

Attention!

1. Only one VID can be assigned to the same MAC and port.

5.4 Subnet VLAN

The configuration page for the subnet VLAN is shown inFigure26 shown in Figure 25.

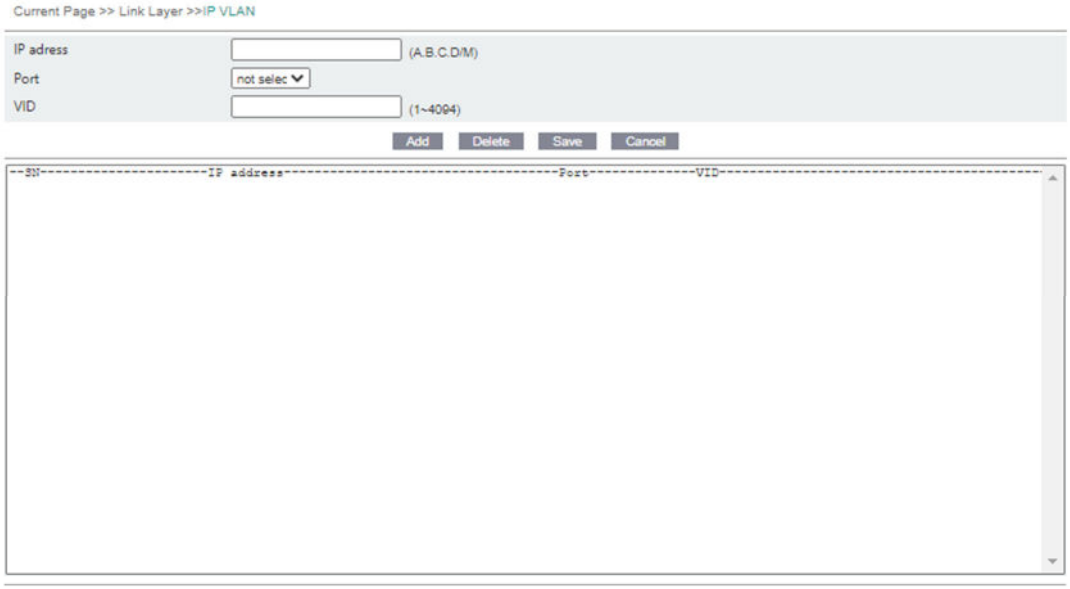


Figure25 Subnet VLAN configuration page

This page is divided into two parts, the upper part configures the subnet VLAN rules of the port, and the lower part displays the list of subnet VLAN rules of the port. The description of each configuration item is as follows:

IP address: the IP address and mask length of the subnet matched by the rule in the format A.B.C.D/M.

Port: The port number of the switch that the rule matches.

VID: The VID to be assigned, the range of values is 1 to 4094.

Add: Adds the above VLAN rule configuration to the below VLAN rule list.

Delete: Delete the VLAN mapping rule selected in the VLAN rule list below.

Save configuration: Save all mapping rule configurations in the VLAN rule list below.

Cancel: By clicking this button, the unsaved configuration will not take effect and the interface will refresh and revert to what it was before the operation.

Attention!

1. Only one VID can be assigned to the same subnet IP and port.

5.5 Protocol VLAN

The configuration page for the protocol VLAN is shown inFigure27 shown in Figure 26.

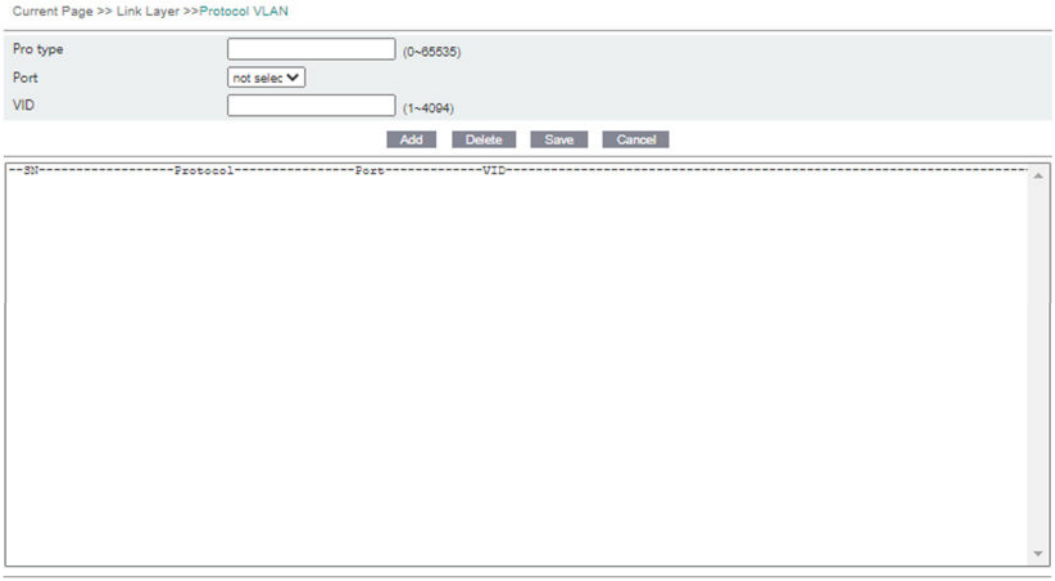


Figure26 Protocol VLAN configuration page

This page is divided into two parts, the upper part configures the protocol VLAN rules of the port, and the lower part displays the list of protocol VLAN rules of the port. The description of each configuration item is as follows:

Protocol type: the protocol type of etherType in the message, the value range is 0~65535.

Port: The incoming port number of the switch that the rule matches.

VID: The VID to be assigned, the range of values is 1 to 4094.

Add: Adds the above VLAN rule configuration to the below VLAN rule list.

Delete: Delete the VLAN mapping rule selected in the VLAN rule list below.

Save configuration: Save all mapping rule configurations in the VLAN rule list below.

Cancel: By clicking this button, the unsaved configuration will not take effect and the interface will refresh and revert to what it was before the operation.

Attention!

1. Only one VID can be assigned to the same protocol type and port.

5.6 IGMP Listening

The switch provides Internet Multicast Management Protocol, which allows the switch to automatically listen for IGMP packets, automatically query multicast group members, and dynamically maintain a multicast forwarding table based on multicast group information. This is shown in Figure27

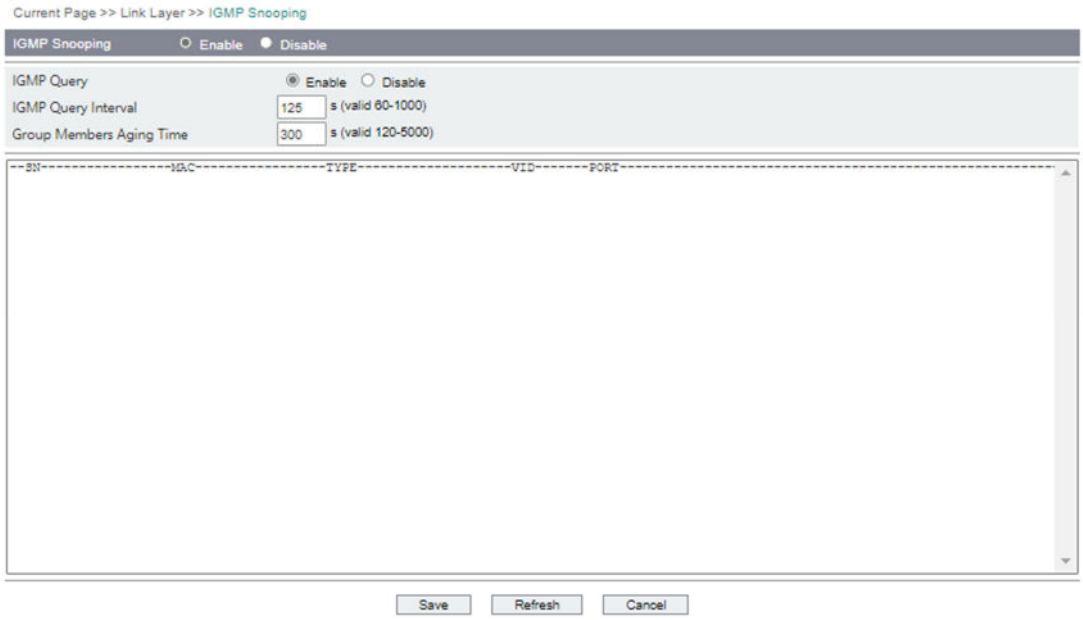


Figure27 IGMP Listening Configuration page

Configuration notes

IGMP Listening: Select whether to enable IGMP listening function, the default is disabled.

IGMP query: select whether to enable the multicast group member query function, IGMP query packet (query) is used to query the existing multicast group, the query interval time can be set by the user. Whenever a multicast group member receives this query, it will respond with an answer packet (report), and the switch will update the multicast table and recalculate the survival time of the member after receiving the answer packet (report). The switch will automatically delete the member from the multicast group after the member's survival time is exceeded.

This feature allows the switch to act as an IGMP state machine if there is no router in the network,

or if the router does not support multicast. If other IGMP query devices already exist in the network, you can disable this query feature, and without this option you will not periodically query multicast group members, which can reduce the network load.

This function is enabled by default.

IGMP query interval: This option is only enabled when the "IGMP query" option is enabled, as the name implies, it sets the time interval for sending IGMP query packets (query), this interval cannot be set too short, too short a time will increase the load on the network, likewise cannot be set too long, too long This interval cannot be set too short, as a short time will increase the load on the network, nor too long, as a long time will result in slow dynamic updates to the multicast group.

The interval time is set from 60 to 1000 seconds and the default value is 125 seconds.

Group member survival time: The survival time of a multicast group member. Whenever a member joins a multicast group or receives a REPORT message from that member, the member will be deleted from the group. This time cannot be set too long or too short, the range is 120~5000 seconds, the default value is 300 seconds.

Members can join multiple multicast groups and are timed separately and independently of each other in each multicast group. This time is a software calculation and will not be very accurate, but is within the margin of error.

IGMP Configuration DescriptionTable3 shows.

Table3 IGMP Configuration Description Table

Setting up the project	Description	Default value
IGMP Listening Enable	Enable IGMP listening	Prohibition of use
IGMP Query Enable	Enable switch IGMP query configuration	Enable
IGMP Query Interval	Switch Query Interval	125s (as standard time for the protocol)
Group member survival time	Switch multicast address aging time	300s

When IGMP listening is enabled, the switch dynamically maintains a multicast forwarding table.

The line items 1 and 2 are dynamically maintained multicast address forwarding entries, and the line item 3 is a manually added static multicast table entry of type "fixed", as described later. The contents of the IGMP multicast address forwarding table will be updated whenever the IGMP listening page is opened again.

Attention!

1. If the PC is a network port with multiple IP addresses, the Windows system always answers with the bottom IP address and problems are likely to occur.
2. It is better not to have multiple IGMP queriers in the network and waste resources.

5.7 Static Multicast Table

This switch provides a manual add/drop static MAC multicast address forwarding function as shown in Figure28

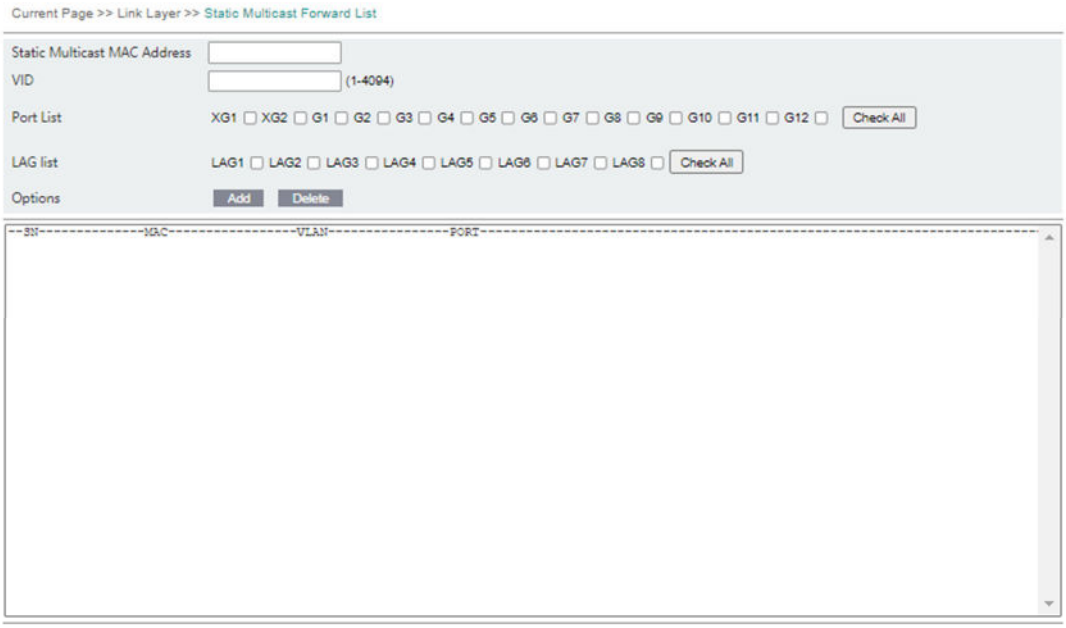


Figure28 static MAC multicast address forwarding function

The difference between this static multicast table entry and the IGMP listen dynamic multicast table entry described above is that IGMP listen dynamically adds and removes multicast table entries according to the IGMP protocol and enables ageing timing to remove obsolete multicast groups and their members, while the static multicast table entry provides the user with the ability to manually add and remove multicast table entries. This table entry is defined as static in the multicast table and the static MAC address performs the forwarding function, but it is not governed by the ageing process and packets whose destination address contains a static MAC address will be forwarded to the specified port.

Configuration notes

Static Multicast MAC Address: Fill in this box with the MAC multicast address to be added in the format XX-XX-XX-XX-XX-XX-XX, the first three bytes of the multicast address are all in hexadecimal 01-00-5E, the following multicast address is reserved for this switch, please do not use:

01-00-5E-00-00-XX (reserved multicast management MAC address)

01-80-C2-XX-XX-XX (reserved Ethernet bridge management MAC address)

Port List: Select the default forwarding port for multicast packets with a destination address of this multicast MAC address, and check the port to which you want to forward them.

Processing List: This section is used to manipulate the multicast table, the buttons "Add" and "Delete"

are used to add/modify and delete static MAC addresses. Existing static multicast table entries are displayed in the table box below, which is updated whenever the user opens the "Static Multicast Forwarding Table" web page or performs an add and delete operation.

Attention!

1. The buttons "Add" and "Delete" take effect immediately, unlike other pages which require a similar action of "Save".
2. Please do not use unicast addresses as input addresses.
3. Please do not enter reserved multicast MAC addresses, e.g. 01-00-5E-00-00-XX (reserved multicast management MAC address), 01-80-C2-XX-XX-XX-XX (reserved Ethernet bridge management MAC address).
4. Once added successfully, please refresh the page.

5.8 LLDP Configuration

LLDP (Link Layer Discovery Protocol) is a standard layer 2 discovery protocol defined in IEEE802.1ab. LLDP is a standard layer 2 discovery method that organises the management address and device identity of the local device and publishes it to its neighbours, who receive the information in the form of a standard management information base (MIB). The neighboring devices receive this information and store it in the form of a standard Management Information Base (MIB) for the network management system to query and judge the communication status of the link.

The entire LLDP configuration web page is under the Layer 2 feature and is divided into three sections: LLDP Global Configuration, LLDP Port Configuration and LLDP Neighbourhood Information, as shown in Figure29

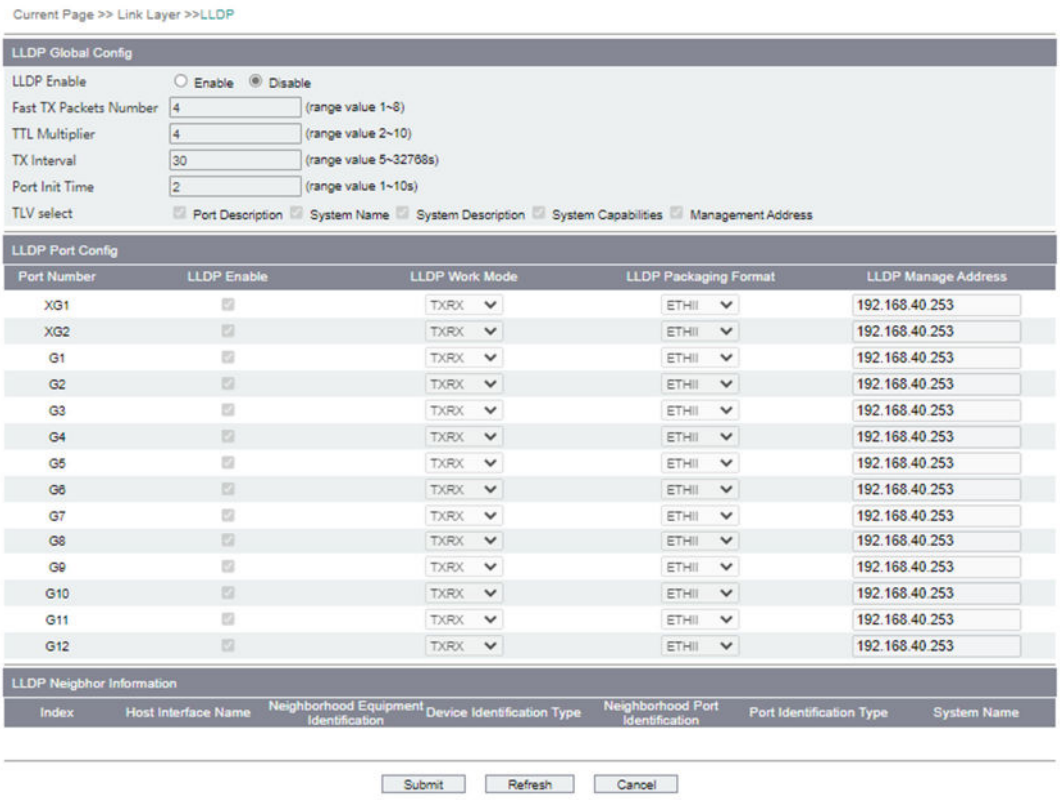


Figure29 LLDP configuration page

LLDP Global Configuration

The global configuration is used to configure the number of fast sending messages, TL multiplier, sending interval, port initialization delay, and TLV optional sending. The configuration of these parameters all relate to changes in the properties of LLDP messages going out of all ports.

Configuration notes

Number of messages sent fast: This item defines the timer interval between transmissions during a fast transmission (i.e. a non-zero configuration). The default value for the number of fast transmission messages is 1, which can be changed by the user to any value from 1 to 8.

TTL multiplier: This is used as a multiplier for the sending interval to calculate the TTL value in LLDP frames; the default value for the TTL multiplier is 4, and managers can change this value to any value from 2 to 10. (TTL = transmission interval * TTL multiplier)

Send Interval: This item defines the timer timing interval between transmissions during normal transmission (i.e. non-zero configuration). The default value for the transmission interval is 30 seconds and the user can change this value to any value from 5 to 32768.

Port Initialization Delay Time: This item is the amount of delay in trying to reinitialize from TX, TXRX to RX, Disable in LLDP operating mode. The default value of Port Initialization Delay Time is 2 seconds, and the user can change this value to any value from 1 to 10.

TLV Optional Send: When the desired parameter message is checked, the checked TLV information will be added to the LLDP message sent by the switch after configuration.

LLDP port configuration

The port configuration is used to configure LLDP enable, LLDP operating mode, LLDP message format, and LLDP management address. These parameters are configured to change the variation of messages going out of each port, as well as the operation of the LLDP function between each port and the port.

Configuration notes

LLDP enable: Different from the global enable switch, when there is a port that does not check LLDP enable, the corresponding unchecked port will turn off the LLDP function, and does not affect the normal use of LLDP function of other ports.

LLDP operating modes: The LLDP operating modes for each port can be divided into the following four types

- Tx: Only send and not receive LLDP frames.
- Rx: Only receive and not send LLDP frames.
- TxRx: both sends and receives LLDP frames.
- Disable: Neither send nor receive LLDP frames.

When the LLDP operating mode is set to Disable mode, the effect is the same as if the LLDP port enable was disabled.

LLDP message encapsulation format: Each port can choose what encapsulation format to send its messages in. There are two encapsulation formats: ETHII (Ethernet II) and SNAP (Subnetwork Access Protocol).

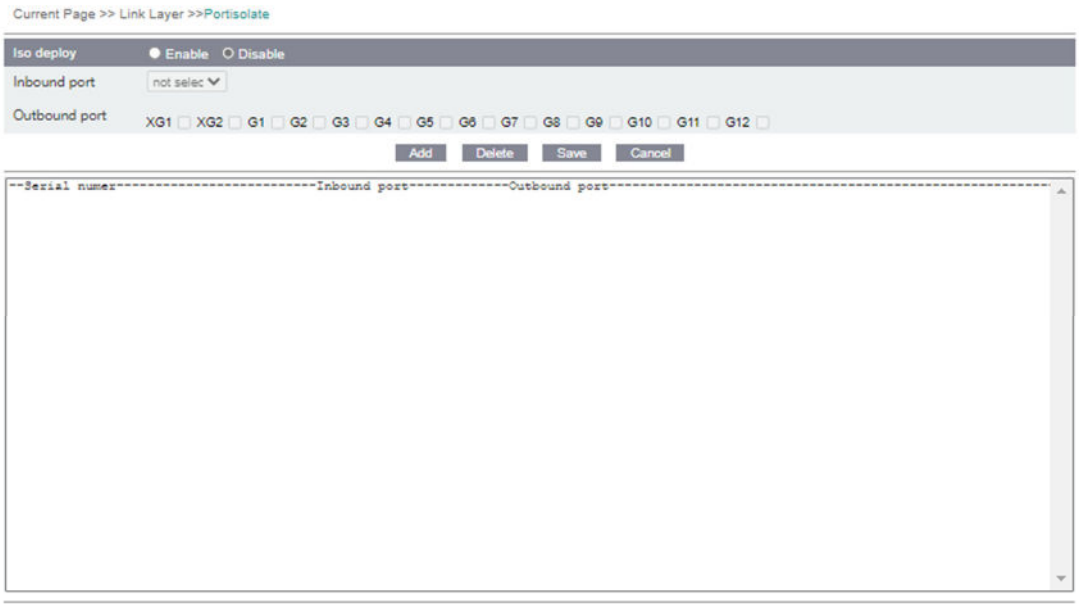
LLDP Management Address: defines a set of management objects and their functions that allow the management configuration and monitoring of LLDP operations. The configured management address is added to the sent management address TLV, which will be disabled if "Management address" is not ticked in the "TLV optional send" of the LLDP global configuration.

LLDP Neighbourhood Information

The first two parts can be configured manually and generally do not require any special configuration to enable LLDP global enable to enable normal LLDP sending and receiving. The third part is only a neighbour device display function and cannot be configured.

When a switch is connected to another switch and if both sides have the LLDP function enabled, information about the switch connected at the other end will be displayed under this section.

5.9 Port Isolation



The port isolation function is used to prohibit data forwarding between different ports in a VLAN. Ports with isolation enabled cannot communicate with each other; ports without isolation enabled can communicate normally with each other, or with isolated ports and unisolated ports. As shown inFigure33 is shown in Figure 30.

Figure30 Port Isolation Configuration Page

The individual configuration items are described as follows:

Port Isolation Configuration: Enables/disables the port isolation function, disabled by default.

Incoming port: Select the incoming port of the isolation group.

Out Port: Select the out port of the isolation group, multiple selections are possible.

Add: Adds the above port isolation configuration to the list of port isolation groups below.

Delete: Delete the port isolation group selected in the Port Isolation Group list below.

Save Configuration: Saves all port isolation group configurations in the Port Isolation Group list below.

Cancel: By clicking this button, the unsaved configuration will not take effect and the interface will refresh and revert to what it was before the operation.

Attention!

1. The incoming and outgoing ports of the same isolation group cannot be the same port.
2. An incoming port corresponds to a maximum of one isolation group.
3. If the incoming port is the same for both isolation group configurations, the original isolation group configuration will be overwritten by the new configuration.

5.10 MAC ACL

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

An ACL consists of a series of table entries called Access Control Entry (ACE). Each Access Control Entry specifies the match conditions and behaviour that satisfy the table entry.

MAC ACLs set up matching rules based on the source/destination MAC of the message, and the EthernetII data frame type. AsFigure34 is shown in Figure 31.

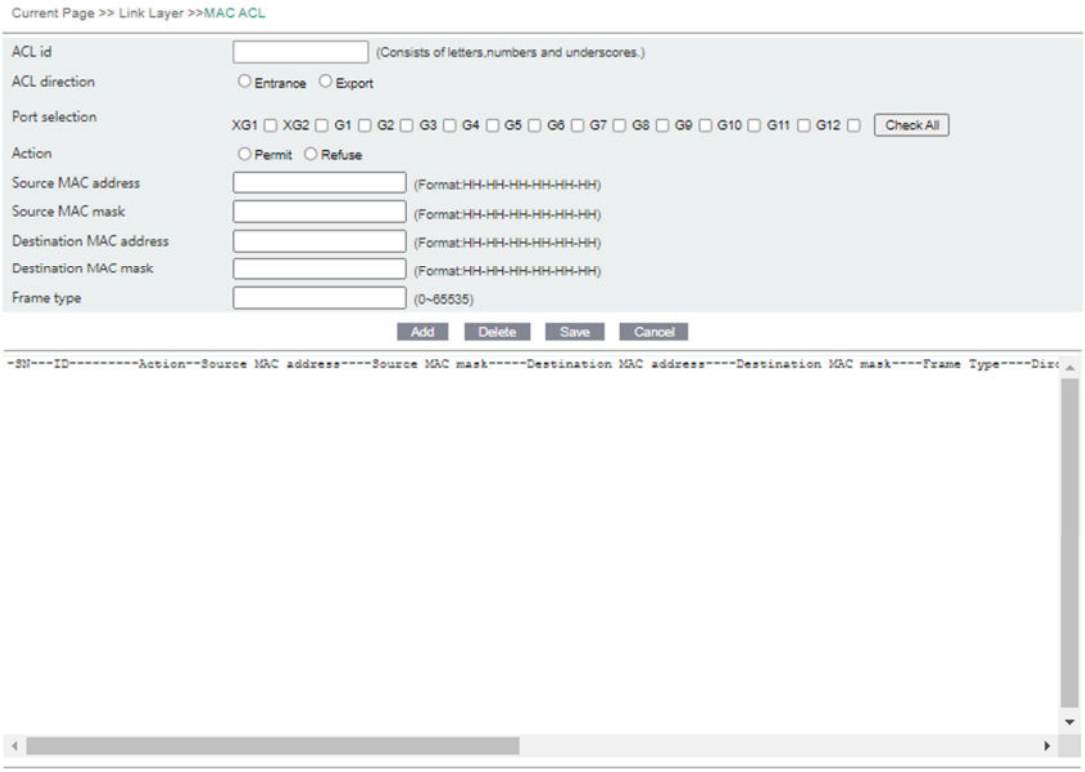


Figure31 MAC ACL Configuration Page

This page is divided into two parts, the top configures the MAC ACL parameters and the bottom displays the MAC ACL list.

The individual configuration items are described as follows:

ACL name: The ACL name must be less than 8 digits and can only be a combination of letters, numbers or underscores.

ACL Direction: Select the direction in which the ACL rule will be applied, with ingress or egress options.

Port selection: Check the port to which the ACL rule will be applied.

Action: The processing action of the message match, allow or deny.

Source MAC address: in the format HHHH.HHHH.HHHH.

Source MAC mask: in the format HHHH.HHHH.HHHH.

Destination MAC address: in the format HHHH.HHHH.HHHH.

Destination MAC mask: in the format HHHH.HHHH.HHHH.

Data frame type: EthernetII data frame type, expressed as a decimal number, with a value range of 0 to 65535.

Add: Adds the ACL rule configuration parameters above to the ACL rule list below.

Delete: Delete the selected ACL rule table entry.

Save configuration: Save all ACL rule table entries in the ACL rule list below.

Cancel: By clicking this button, the unsaved configuration will not take effect and the interface will refresh and revert to what it was before the operation.

5.11 IP ACL

IP ACLs make matching rules based on the Layer 3 and 4 information of the message. AsFigure32 is shown.

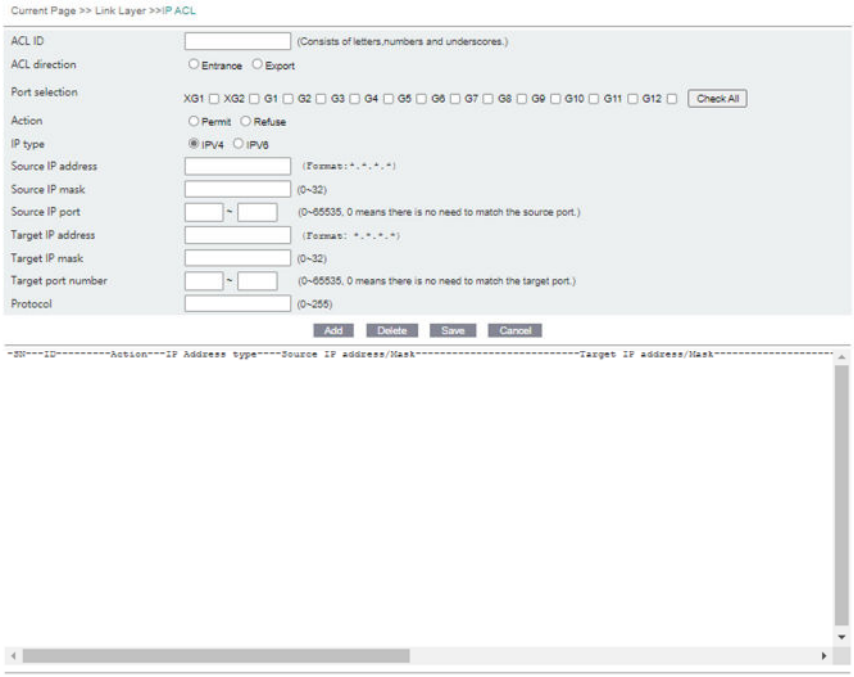


Figure32 IPC ACL configuration page

This page is divided into two parts, the upper part configures the IP ACL parameters and the lower part displays the IP ACL list.

The individual configuration items are described as follows:

ACL number: The ACL number must be less than 8 digits and can only be a combination of letters, numbers or underscores.

ACL Direction: Select the direction in which the ACL rule will be applied, with ingress or egress options.

Port selection: Check the port to which the ACL rule will be applied.

Action: The processing action of the message match, allow or deny.

Source IP address: the source IP address of the message, in the format *. *. *. *.

Source IP mask: the length of the source IP mask, the value range is 0~32.

Source port number: the value range is 0~65535, 0 means no need to match the source port number.

Destination IP address: in the format *. *. *. *.

Destination IP mask: the length of the destination IP mask, the value range is 0~32.

Destination port number: the value range is 0~65535, 0 means no need to match the destination port number.

Protocol: the type of IP protocol carried by the message, the value range is 0 to 255.

Add: Adds the ACL rule configuration parameters above to the ACL rule list below.

Delete: Delete the selected ACL rule table entry.

Save configuration: Save all ACL rule table entries in the ACL rule list below.

Cancel: By clicking this button, the unsaved configuration will not take effect and the interface will refresh and revert to what it was before the operation.

6 Link backup

Link backup features include: ERPS, Trunk Port Aggregation and RSTP Rapid Spanning Tree.

6.1 ERPS

ERPS (Ethernet Ring Protection Switching), or Ethernet Multi-Ring Protection Technology, is a layer 2 network redundancy protection tool. It prevents broadcast storms caused by loops when the Ethernet ring is intact, quickly restores the prevailing link to each node on the ring network in the event of an Ethernet link failure, and has a high convergence speed.

The entire ERPS configuration page is divided into three parts: ERPS parameter configuration, ERPS ring reversal and ERPS status display, as shown in Figure33

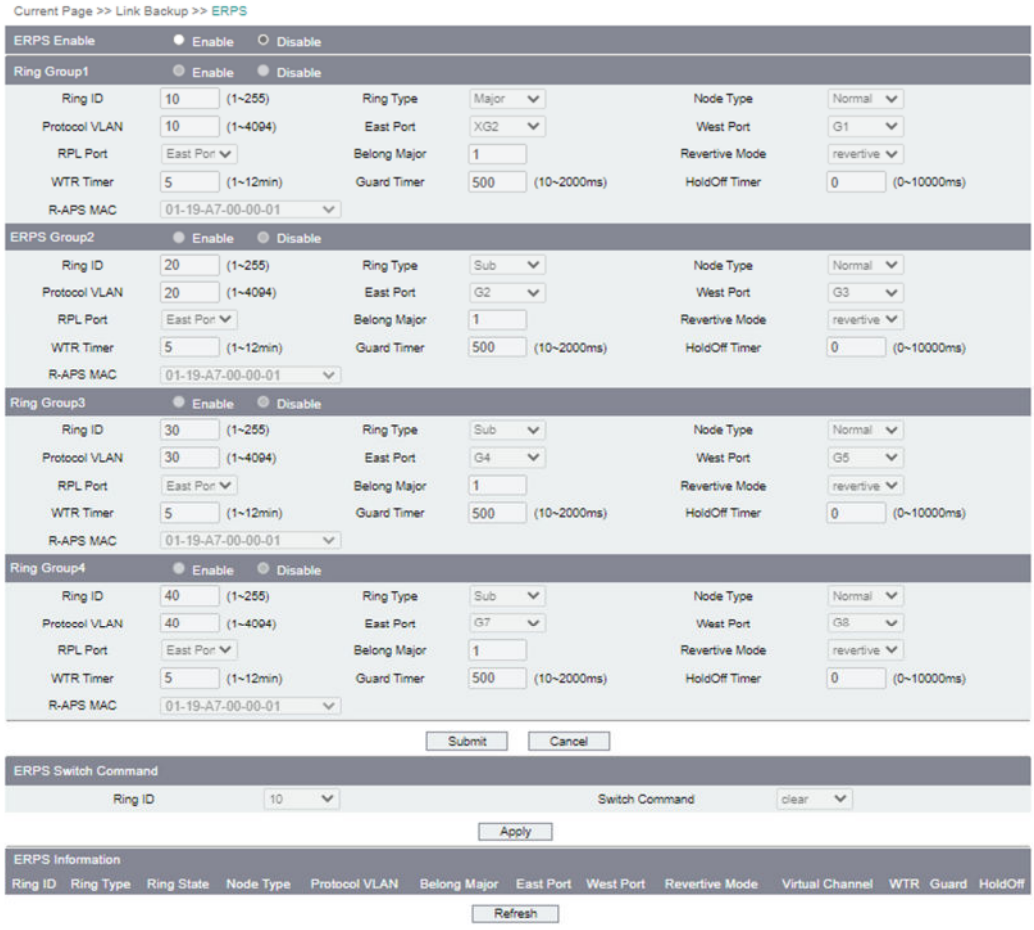


Figure33 ERPS configuration page

Configuration notes

Ring ID: The ring ID is used to uniquely identify an ERPS ring, and the same ring ID should be configured on all nodes on the same ERPS ring.

Ring types: ERPS rings are divided into a main ring, which is a closed ring, and a sub-ring, which is a non-closed ring.ERPS rings can consist of a single main ring, or a multi-ring structure consisting of a main ring plus sub-rings.

Node type: A switch that joins an ERPS ring is called a node.

The types are as follows:

- Owner node: The role is to block or open the RPL link (Ring Protection Link, i.e. the link between the Owner node and the Neighbor node) to prevent the formation of a loop.
- 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.
- Normal node: receives and forwards protocol messages and service messages on the link.

Protocol VLAN: A VLAN dedicated to the delivery of protocol messages. The protocol VLANs of nodes within the same ERPS ring must be the same.

Eastbound port/Westbound port**: In the main** ring, each node has 2 member ports, called eastbound and westbound ports; in the sub-ring, the nodes connected to the main ring are called interconnection nodes, the sub-ring interconnection nodes have only one member port, and only one of the eastbound and westbound ports needs to be configured during configuration, the other one is configured as none, the configuration of non-sub-ring interconnection nodes is the same as the main link point, both eastbound and westbound ports need to be The configuration of the non-sub-ring interconnection node is the same as the main link point, with both eastbound and westbound ports configured.

RPL Port**: When the Node Type** is Owner/Neighbor, the RPL Port specifies which port is to be used as the port on the RPL link, either Eastbound or Westbound. When the node type is Normal, this is not available.

Primary ring**: When the node** type is primary, this item is not configurable; when the node type is subring, the ID of the primary ring to which the subring point belongs must be configured.

Cutback mode**:** Once the ERPS link has been restored to normal, the cutback/non-cutback mode of the ERPS can be set to determine whether to block the RPL link again. The configuration should remain in cutback mode unless specifically required.

- Cutback: If the faulty link is restored, after WTR time, the RPL link will be blocked again and all nodes will be stable in Idle state.
- No cutback: If the faulty link is restored, the blocking link remains on the original faulty link, the RPL link does not block again and all nodes are stable in the Pending state.

WTR timer**:** In cutback mode, the WTR timer is used to prevent frequent switchover protection operations when frequent link failures are detected. Before this timer times out, the RPL link keeps forwarding and the fault recovery port maintains blocking. During this period, if the Owner node receives an SF protocol message indicating that a fault still exists in the ring, this timer is turned off and the RPL link still keeps forwarding; otherwise, after this timer times out, the RPL link blocks and the Owner node sends a (NR, RB) message to notify the fault recovery node to release the temporary blocking port and flush the MAC address table.

Guard Timer**:** This timer is started after a node detects a fault recovery or executes the Clear command and is used to prevent old R-APS messages caused by forwarding delays in the ring from causing unnecessary shocks to the network. Before this timer times out, any R-APS messages received, except for the event messages, are ignored. Note that the duration of this timer should be greater than the delay of R-APS messages arriving at all nodes in the ring, but the greater the duration, the longer the node will miss processing new requests from other nodes.

HoldOff Timer**:** This timer is activated when a fault is detected by the node, at which point the fault is not immediately reported, and is only reported if the fault is still detected after the timer has timed out, giving the service layer the opportunity for link repair. Note that the duration of this timer affects the speed at which link faults are reported and ultimately the performance of the link reversal.

Virtual channel**: In the** intersecting ring network, the transmission of subring protocol messages can

be carried out in two ways: virtual channel and non-virtual channel. This device is disabled by default and is not configurable.

Protocol message destination MAC address**:** This configuration is a compatibility option. In older versions, the destination MAC address of ERPS protocol messages was fixed at 01-19-A7-00-00-01, while in newer versions the ring ID is used as the lowest byte of the destination address, 01-19-A7-00-00-[Ring ID]. This configuration needs to be considered when networking compatibility with switches from other vendors.

Attention!

ERPS does not have an automatic election mechanism and its operation is very dependent on the correct configuration of each node in the ring, so please ensure that the configuration is correct.

Inversion of command

ERPS can artificially select the blocking state of a port by manually issuing a reverse command, including Clear, Forced Reverse (FS), and Manual Reverse (MS). Once the configuration has been selected in the drop down menu, click the "Reverse" button to take effect. This is shown in Figure34

- Clear command: can be used to clear locally configured FS or MS operations, or the Clear command can be used to bring a node back to the Idle state early before the WTR times out.
- Forced Reversal (FS): Any of the east-west ports can be selected. The port being forced to reverse is immediately blocked, regardless of the presence of a faulty link in the ring.
- Manual Swapping (MS): Any of the east-west ports can be selected. The port being manually swapped will only block when the ring state is Idle or Pending, and if the link fails at this point, the ring will switch from MS to Protection for protection swapping.

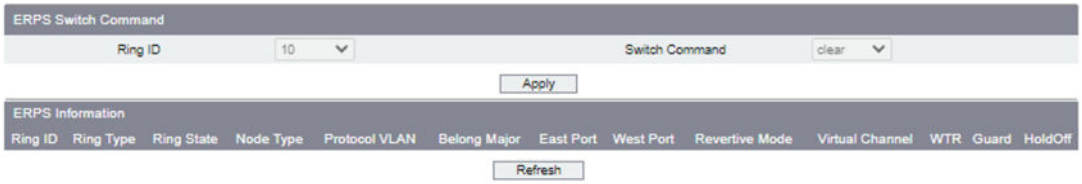


Figure34 ERPS Reversal Command Configuration Page

Ring Network Information

With the ERPS ring running, click the "Refresh" button to obtain or refresh the ring information, including the ring node status, port status and some configuration information, to facilitate the monitoring of the ring operation.

There are six ring network node states:

- init: This state is the first state the device enters when the ERPS is switched on, and its main

job is to initialize the timer and ring member ports.

- idle: This state is stabilized when each link in the ring is normal. In this state the RPL port is blocked and the Owner node periodically sends (NR, RB) messages to inform the other nodes that the RPL link is blocked.
- protection: This state is stabilized when there is a link failure in the ring network. In this state, the faulty node periodically sends (SF) messages to notify other nodes that a fault has occurred, and the Owner and Neighbor nodes will open the RPL link upon receipt of the (SF) messages to complete the protection reversal of the link.
- FS: After issuing the force-flip command (FS), the node enters this state and periodically sends a (FS) message, which is received by other nodes and enters the FS state.
- MS: Only in the pending or idle state, after the manual reversal command (MS) is issued, the node enters this state and periodically sends a (MS) message, which is received by other nodes and enters the MS state.
- pending: When a node resumes from protection to idle, or clears FS/MS operations with the clear command, the node will first enter this state in the cutback mode and then transition to idle after WTR time; in the non-cutback mode the node will stabilize in this state.

6.2 Port aggregation

The main function of port aggregation (TRUNK) is to bind multiple physical ports (typically 2-4) into a logical channel so that they work as one channel. By bundling multiple physical links together, not only does it improve the bandwidth of the entire network, it has the effect of link redundancy, so that in the event of a network failure or other reason to disconnect one or more of the links, the remaining links can still work. Figure39 below shows an illustration of a case study using Trunk.

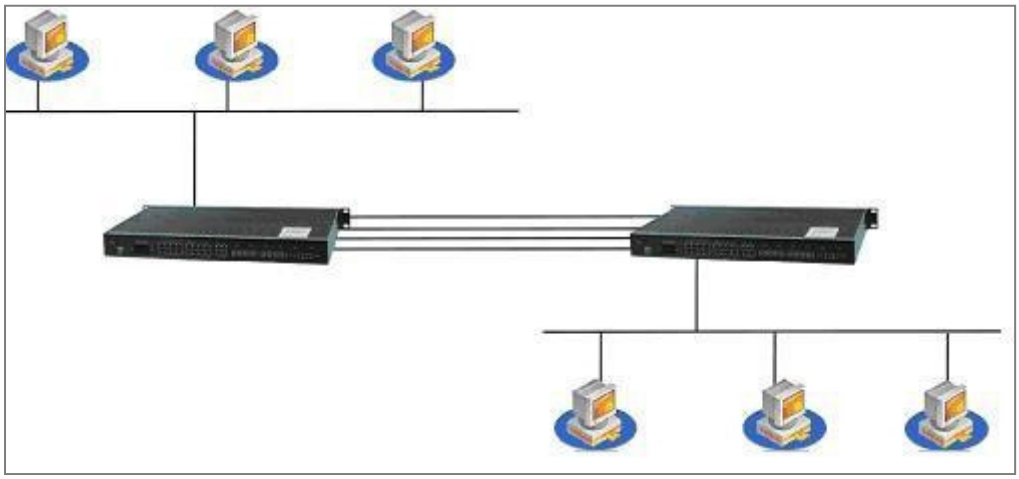


Figure35Schematic diagram of a case using Trunk

The diagram above shows a computer network between two switches via a Trunk, with four ports connected together between the two switches to achieve increased bandwidth and link redundancy.

Each Trunk group can contain 2 to 8 ports as a single logical link to enhance bandwidth and link redundancy. When one of the physical connections fails to communicate or fails, the other links in the Trunk group immediately take over and maintain communication, thus providing a fast recovery mechanism after a communication interruption. The Trunk function is configured via theFigure40 The configuration of the Trunk function is done via the web page shown in Figure 36

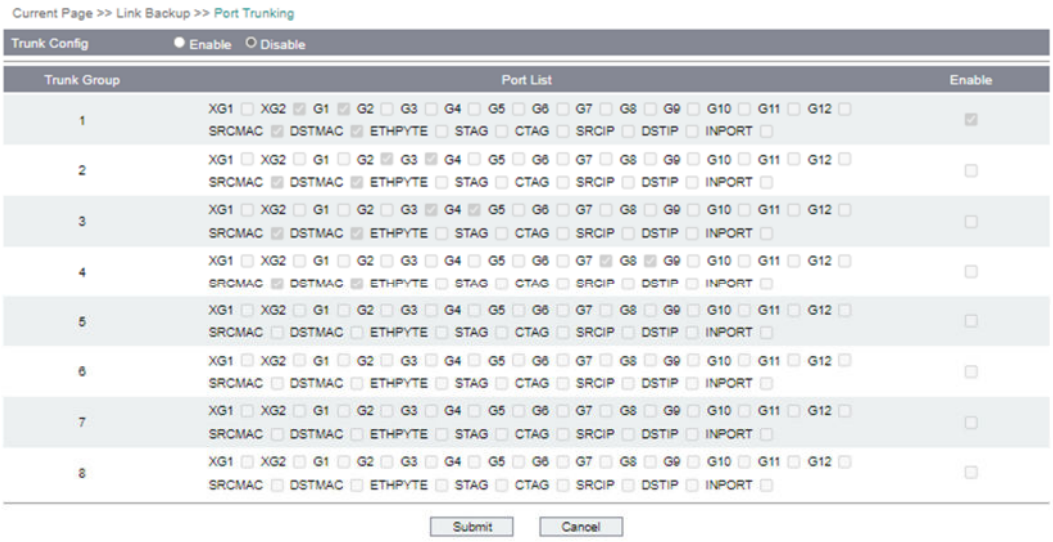


Figure36 Port aggregation configuration page

Configuration notes

Convergence group: Convergence group number.

Port List: Select the ports assigned to each group of Trunk.

Enable: Select whether to enable Trunk for this group, check the box to enable it.

Attention!

1. The maximum number of Trunk groups and group members supported by the switch is based on the actual model.
2. The same port cannot exist in two Trunk groups at the same time.
3. When using Trunk, it must be enabled before a physical connection can be made.
4. The increase in bandwidth is not simply a multiple of the number of ports, but instead often shows no increase in the total bandwidth of the aggregation, which is determined by the forwarding mechanism of the switching chip.

6.3 Fast spanning tree

Introduction to Spanning Tree Protocol (STP)

Spanning Tree Protocol is a Layer 2 management protocol that eliminates network Layer 2 loops by selectively blocking redundant links in the network, while providing link back-up functionality.

Rapid Spanning Tree Protocol (RSTP)

The Rapid Spanning Tree Protocol (RSTP) is defined in the IEEE 802.1w standard as a complement to the 802.1d standard.

Configuration notes for Rapid Spanning Tree (RSTP)

Clicking on the Quick Generate Tree submenu on the menu will bring up a pop-up likeFigure41 The configuration page is shown in Figure 37.

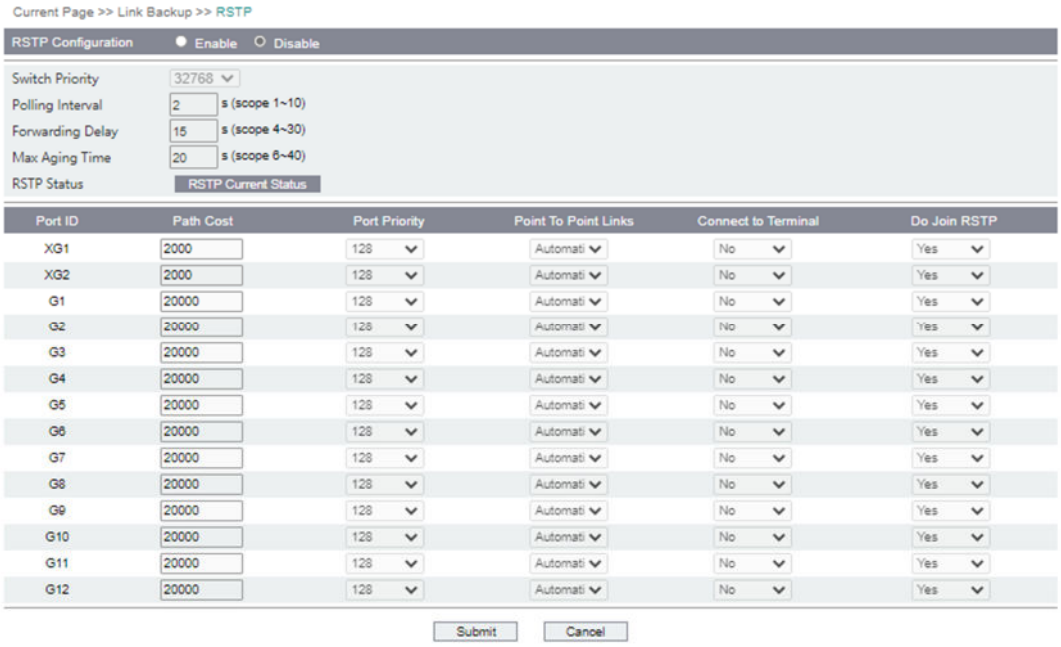


Figure37 Quick spanning tree configuration page

Configuration notes

RSTP configuration: enable/disable the Rapid Spanning Tree feature, the default is disabled. As shown Figure38



Figure38 Enable fast spanning tree

Switch Priority: Set the priority of the switch (bridge). The switch priority and the switch MAC address are combined to form the bridge ID, the switch (bridge) with the lowest bridge ID will become the root bridge in the network. The smaller this value the higher the priority, the more likely it is to become the root bridge, the default value is 32768.

Polling interval: set how often the switch sends packets of BPDUs, a small packet sending interval will speed up the convergence speed of RSTP, but will increase the network burden, set too large, it will make the convergence time of RSTP longer. The default value is 2, and the value range is an integer between 1~10, in seconds.

Forwarding delay: The time in seconds for the switch's port state to maintain a forward delay in the transition state (listening and learning). The default value is 15, and the range is an integer between 4 and 30.

Maximum aging time: refers to how long a BPDU packet is valid after a switch receives it from another switch, in seconds. The default value is 20, and the range of values is an integer between 6 and40.

Go to RSTP Status Information: Click on the "Quick Spanning Tree Current Status" button to view the current status information of the RSTP.

This page shows that the current root bridge in the network is the switch with MAC address 00-02-b3-04-40-02 instead of the local machine, and the local machine's root port is G7, which is in Forwarding state (Forwarding); port G8 is the designated port, which is in Blocking state (Discarding), indicating that port G8 is a redundant link. The information on this page shows the current status of RSTP. RSTP is always in the process of dynamic detection and negotiation, so every time you refresh this page, you will see the latest status, and the information you get is not necessarily the same every time you refresh this page.

Port Roles: The roles of the ports, of which there are five:

- Root: The port that receives the configuration messages sent by the root bridge at regular intervals, i.e. the root port. The root bridge is the only device in the entire network that does not have a Root port.
- Alternate port: is a reserve port for the root port, except that it will be blocked due to the receipt of better configured messages from other switches.
- Designated: indicates the designated port, i.e. the port responsible for forwarding BPDU optimal configuration messages inside a LAN, on both the root and designated bridges, as opposed to the Root port.
- Backup port: is a backup port for the specified port, which will be blocked due to the receipt of its own better configuration message.

- Unknown: Not any of the above ports.

Forwarding state: refers to the operational state of the port, of which there are four:

- Disabled: Disabled state, indicating that this port is not connected and that ports that are not connected are in this state.
- Discarding: Blocking state, BPDU packets can be received at this time, if the BPDUs are not received during the period, the port will go to learning state, the port is blocking when the link is first connected.
- Learning: learning state, at this time can receive packets, immediately after the connection, the switch stays in the blocking state for max age time, to determine whether the port of the switch can become the root port or the designated port, during the period of sending and receiving BPDU packets, to complete the election and construction of the root of the spanning tree, to complete the decision of the port state to go. If it is decided to be the root port or designated port, it will stay forward delay time and continue to calculate to determine whether the port can become the root port or designated port, which has the function of learning MAC address at this time. If it is the root port or designated port, it will switch to forward state, if not, it will switch to blocking state.
- Forwarding: Forwarding state, when the port can send and receive packets normally.

In order to speed up the self-healing process of RSTP and reduce the network load, users can configure the port information of Spanning Tree on the page shown in Figure39 below.

Port ID	Path Cost	Port Priority	Point To Point Links	Connect to Terminal	Do Join RSTP
XG1	2000	128	Automati	No	Yes
XG2	2000	128	Automati	No	Yes
G1	20000	128	Automati	No	Yes
G2	20000	128	Automati	No	Yes
G3	20000	128	Automati	No	Yes
G4	20000	128	Automati	No	Yes
G5	20000	128	Automati	No	Yes
G6	20000	128	Automati	No	Yes
G7	20000	128	Automati	No	Yes
G8	20000	128	Automati	No	Yes
G9	20000	128	Automati	No	Yes
G10	20000	128	Automati	No	Yes
G11	20000	128	Automati	No	Yes
G12	20000	128	Automati	No	Yes

Figure39 RSTP port information configuration page

Port Path Overhead: The port path overhead, together with the port priority, forms the port ID for comparison purposes. The path overhead is determined by the physical link of the network and the user should modify this value according to the specific physical link.

Port Priority: The priority of the port in the bridge, together with the port path overhead it forms the port ID for comparison, the smaller the value the higher the priority. The default is 128.

Point-to-point network connections: A switch port is a point-to-point interface if there is only a direct connection between the switch port and the switch port. rstp uses a negotiation mechanism for point-to-point links, which allows for fast port state transitions.

Directly connected terminals: Switches at the edge of the network are generally connected to end devices, such as PCs and workstations. The ports connected to these end devices are configured to become directly connected to the endpoints, allowing for fast port state transitions without the need for the Discarding, Learning, Forwarding conversion process.

Participation in Spanning Tree Structure: Specifies whether the port participates in the operation of the Spanning Tree Protocol. The complexity of RSTP operations can be reduced by reducing the number of ports participating in spanning tree, thus reducing the self-healing time of RSTP.

Attention!

1. The RSTP protocol is defined in the 802.1w standard and is an open standard protocol. The RSTP protocol of our switches is interoperable with non-our network devices that support the standard RSTP protocol.
2. When RSTP is enabled, RSTP will first disable all ports and wait for the convergence period to complete before enabling and blocking certain ports, during which time the web server will lose response, and when convergence is over (about 10s or more), the web server can be used again.
3. Whenever the link changes, the RSTP will have a time varying convergence process again, but it may also cause the web server to be inaccessible, which can be re-accessed when the convergence is over.
4. When RSTP is enabled, each switch will periodically send query packets from each connected port at a user-set packet interval, thus increasing the network load.
5. The following condition must be met between the maximum ageing time and the forwarding delay: 2*(forwarding delay - 1) ≥ maximum ageing time.
6. The following condition must be met between the maximum ageing time and the polling interval: maximum ageing time >= 2*(polling interval+1)
7. In order to reduce the complexity of network calculation and convergence time, it is recommended that users set port information to reduce the number of ports involved in spanning tree; reducing forwarding delay and maximum aging time can speed up the self-healing of RSTP.

7 Access control

Access control features include: user passwords, login control, port authentication, authentication database, MAC port lockout.

7.1 User Password

The switch's web server can be configured with up to three users with different names. User 1 has an access level of Administrator, while User 2 and 3 can have an access level of Observer or Administrator. Only if you know the user name and password can you log in to the web server and access or manage the switch. The user name and password can be changed for each user, but only user 2 and user 3 can be added or deleted. The switch is shipped with a default username and password of "admin" and an access level of administrator.

Both the username and password must be legal characters and can consist of letters (case sensitive),

numbers, underscores and spaces, but the username and password cannot be empty. If the current login username or password is changed to something different, you will be prompted to re-enter the username and password when you visit the web page again. This is shown in Figure40

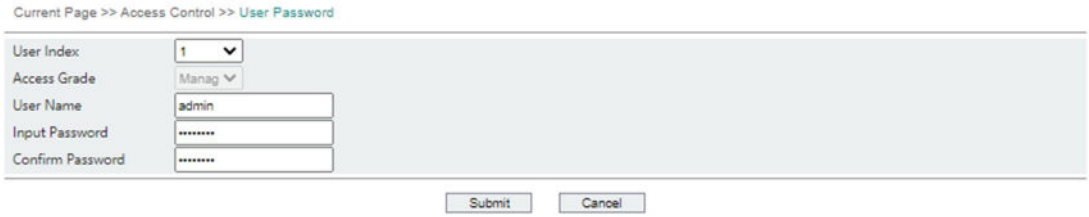


Figure40 User password configuration page

Configuration notes

User index: user number, takes values 1, 2, 3, maximum 3 users.

Access levels: There are two access levels, administrator and observer, with the administrator having the right to view and modify all settings; the observer has the right to view all settings only. User 1 is fixed in administrator mode.

User name: The user name can only consist of 1 to 16 bytes of English, numbers, underscores or spaces.

Enter a password: The user password can only consist of 8 to 16 bytes of English, numbers or special characters.

Confirm password: Repeat the password in case it is entered incorrectly.

Attention!

1. User 1 can only be set to administrator mode, this is to ensure that at least one of the system is an administrator account.
2. For security reasons, it is recommended that administrators change the default password for user 1 after the first login.
3. Whenever a user logs into the Web server, the server will be idle for about 5 minutes to let this login authentication expire, then the operation Web page will ask the user to log in again, this is to prevent others from misuse of the Web when the administrator is not present, this time is software calculation time, will not be very accurate.
4. The user can log out of the web server at any time by clicking on the "Logout" link in the top right hand corner of the page, actively deactivating the last valid login authentication and reactivating it for any subsequent web operations.

7.2 Login control

Login control is used to restrict the switch's remote access features such as SSH, Telnet and Web, as shown in Figure41

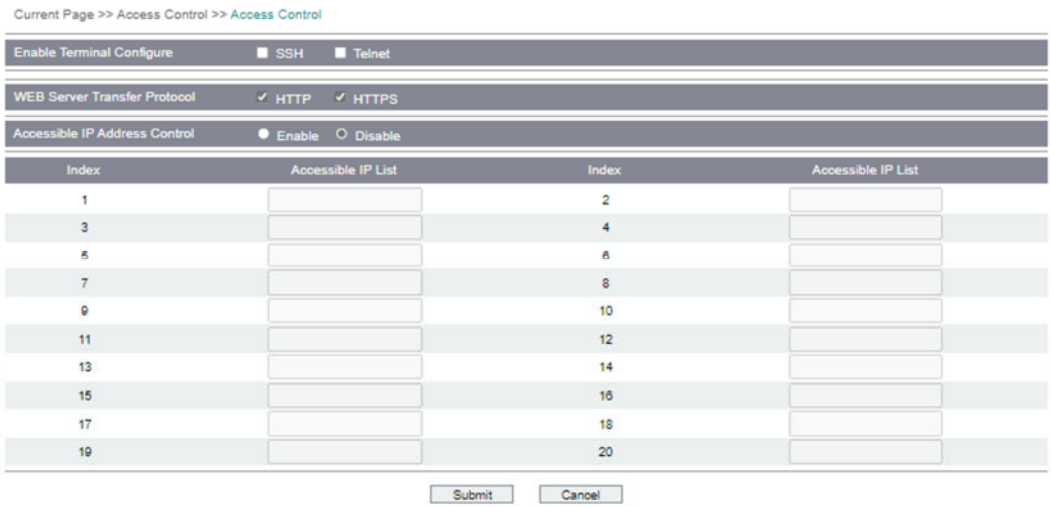


Figure41 Login control configuration page

Configuration notes

Enable terminal configuration: This option is used to enable SSH, Telnet remote terminal access protocols for the switch, both are disabled by default.

WEB server transfer protocol: This option is used to enable the transfer protocol supported by the web server, the default is to support both http and https, it is recommended that users do not need to modify this option.

HTTP: HTTP (HyperTextTransferProtocol) is an acronym for Hypertext Transfer Protocol, which is used to transfer data in a WWW way, see RFC2616 for more information on the HTTP protocol. HTTP uses a request/response model. The client sends a request to the server with a request header containing the requested method, URL, protocol version, and a MIME-like message structure containing the request modifier, client information and content. The server responds with a status line containing the version of the message protocol, a success or error code plus information about the server, entity meta information and possibly entity content.

HTTPS: HTTPS is a secure version of the HTTP protocol, developed for confidentiality purposes, and is based on the SSL protocol, which sits between the TCP/IP protocol and various application layer protocols to provide security support for data communications.The SSL protocol can be divided into two layers: the SSL Record Protocol, which builds on top of a reliable The SSL Handshake Protocol is built on top of the SSL Record Protocol and is used for authentication, negotiation of encryption algorithms and exchange of encryption keys between the two parties before the actual data transfer takes place.

When the switch ip address is the default ip, the user enters "https://192.168.40.253" directly in the address bar of the browser and clicks the Enter key, which means that the web server is accessed through the https protocol, and a warning may pop up as shown Figure47



Figure47 Warning message page

When logging in for the first time, sometimes the home page is not displayed properly, this is due to the web script program not running properly, refresh a few times and it will be displayed normally.

Login IP Address Control: When this feature is enabled, only computers with the assigned IP address can access the device, all other IP addresses not listed are blocked from accessing the switch's web server.

Allow access to the IP address list: Enter in the box the IP addresses of the network devices that are allowed to access the Web, a total of 20 records are allowed and the user can use several of them. The user must set at least one IP address list and this address cannot be the switch's own address, otherwise the Web server will not be accessible.

Attention!

1. HTTP, HTTPS must be enabled for at least one access protocol.
2. Some browsers cannot display the home page completely when opened for the first time using HTTPS, but it will be displayed normally after a few more refreshes, which is caused by the web script program not running properly.
3. The accessible IP address must be a legitimate IP address, at least one of which should be in the same network segment as the device IP, otherwise the device will determine that the setting is invalid.
4. The address list is the IP addresses that are allowed in, so at least one address must be set, otherwise the web server on this switch will not be accessible.
5. Do not use the switch's own address input, as incorrectly allowing only this one address can cause problems with inaccessible web servers.

7.3 Port Authentication

The authentication architecture of IEEE 802.1X adopts the logical functions of "controlled port" and "uncontrolled port", thus enabling the separation of service and authentication. After the user has been authenticated, the service flow and the authentication flow are separated, and there are no special

requirements for subsequent packet processing.

The 802.1X architecture has three main components:

- Applicant supplicant: a user or customer who wants to be certified.
- Authentication server: Typical example is a RADIUS server.
- Authentication system authenticator: for inter-end devices such as wireless access points, switches, etc.

Our device can play the role of both an authentication system and an authentication server, or it can use an external authentication server and support an external billing system at the same time. The page for port authentication is shown in Figure42

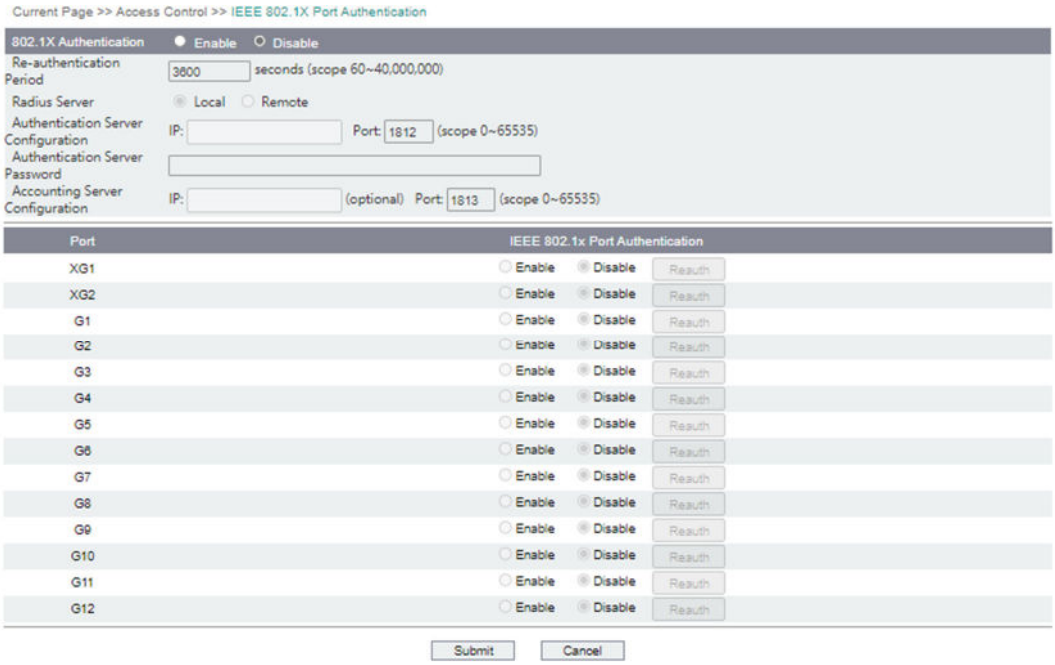


Figure42 IEEE 802.1X authentication configuration page

Configuration notes

Timed update authentication: The re-authentication period of 802.1X. After this time, the last successful authentication is invalid, and re-authentication is required to enhance the security of authentication. The setting range is 60~40000000 seconds, the default value is 3600 seconds, i.e. re-authentication is required every 1 hour.

Radius Server: i.e. setting up a RADIUS authentication server with two options: "Local" and "Remote".

- **Local**: means using this switch as a RADIUS authentication server, this switch has a built-in RADIUS server, the applicant will only be able to use the user and password from the switch's internal RADIUS database, the following three are disabled.
- **Remote**: means using a RADIUS server external to the switch to authenticate to the local port of this switch. External RADIUS authentication server means a RADIUS server that is not built into the switch, and the built-in RADIUS server of this switch cannot be used as a remote authentication server for other switches. When this option is enabled, the following three items

are enabled, the billing server is optional and the rest are required.

Authentication Server Configuration: This option is enabled when the "Remote" server is selected. Fill in the IP address and port of the remote server, the IP address must be accessible to the device and the default port is 1812.

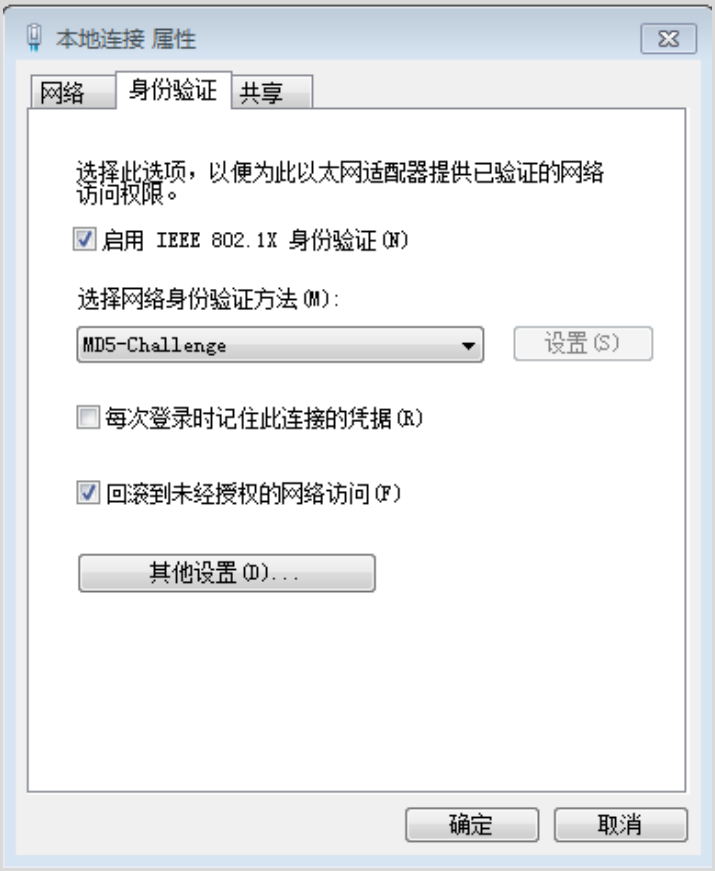
Authentication Shared Password Value: This option is enabled when a "remote" server is selected, and fills in the shared password string for this switch to access the remote authentication server.

Billing server configuration: This option is only enabled when the "remote" server is selected, it is an optional setting, the function of the billing server is billing, the IP address set must be accessible to the device, the default port is 1813, the wrong setting of the billing server will cause the applicant to fail authentication, there is no billing server There is no need to set the billing server.

The port will be "disabled" until the authentication is passed, and will only enter the normal forwarding state once the authentication is passed. Clicking on the "Re-authenticate" button will invalidate the last authentication and the port will need to be re-authenticated.

Attention!

1. In windows, open Network connections → Properties page:



If the "Authentication" tab is not available, select "Control Panel" → "Administrative Tools" → "Component Services "Services" → "Services" and enable the "Wireless Zero Configuration" and "Wired AutoConfig "services. Use MD5-questioning in the "Select network authentication method (M):" option, other methods are not supported, as shown in the figure.

2. If 802.1X authentication is enabled and the username and password for the authentication database are set, the following authentication dialog box will appear when connecting to the network on a windows system:



Enter the set username and password to be authenticated.

3. If authentication is enabled on the switch port used by the user to access the web server, the user will not be able to access the web server normally once the authentication function is activated and will need to be authenticated in order to access the web server again, which is a normal phenomenon and not a fault behavior.
4. All uplink, downlink and billing server ports must be mandatorily authenticated, i.e. the use of authentication is "forbidden", otherwise the remote server cannot be used unless an internal authentication server is used.
5. An incorrectly set billing server will also result in the applicant failing to authenticate, which is not necessary if there is no billing server.
6. When using a remote server, the administrator must ensure that the device can access the remote server, i.e. that the gateway in the "Device Address" is set correctly and that the DNS is set correctly if a domain name is used.
7. The built-in authentication server of this switch cannot be used as a remote authentication server for another switch.
8. If the authentication database does not have any user names and passwords, all ports are automatically authenticated.

7.4 Certification database

RADIUS is a Remote Authentication Dial In User Service (RADIUS) protocol for transferring authentication, authorisation and configuration information between a Network Access Server and a shared authentication server. RADIUS uses UDP as its transport protocol. RADIUS is also responsible for the transfer of billing information between the Network Access Server and the shared billing server.

The RADIUS authentication database, as part of the 802.1X authentication and authorization, holds multiple sets of user names and passwords for authentication, and users can add or delete user names and passwords saved in the database through this page. The RADIUS authentication database configuration page is shown in Figure 50.Figure50 The RADIUS authentication database configuration page is shown in Figure 43.

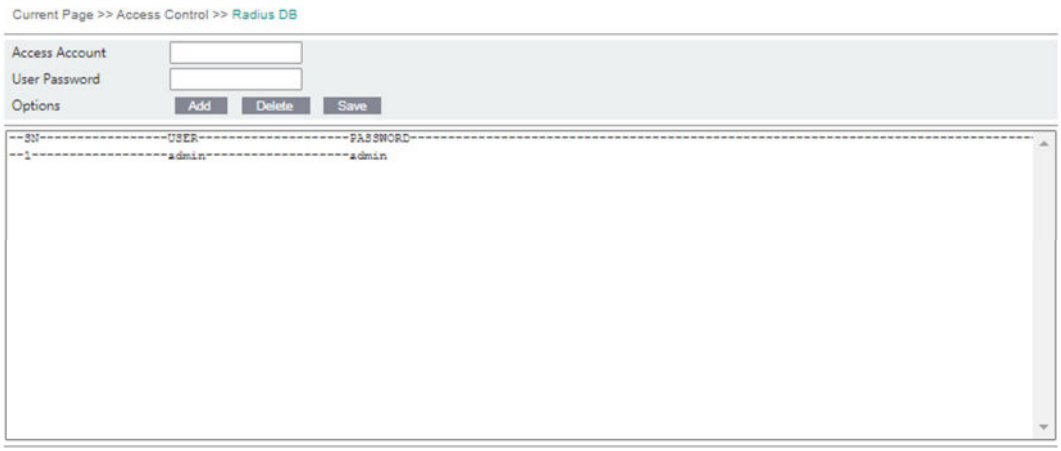


Figure43 RADIUS authentication database configuration page

Configuration notes

Login account: Set the new authentication username, consisting of a number and letter (case sensitive) no larger than 16 bytes.

User Password: A new user password, also consisting of a number and letter (case sensitive) no larger than 16 bytes.

Processing List: Click on "Add User" and "Delete User" to add and delete usernames and passwords in the table boxes below, all additions and deletions will be submitted to the switch by clicking on the "Save Configuration All additions and deletions will be submitted to the switch by clicking the "Save Configuration" button and will trigger a database update and restart of the entire 802.1X authentication. Exit this page before clicking the "Save Configuration" button and all changes will be undone.

Attention!

1. When clicking on "Add User" and "Delete User", the added and deleted table entries will appear in the table box as changed, but not saved, only when the "Save Configuration" button is clicked will the changes be Only when the "Save Configuration" button is clicked will these changes be committed to the switch and trigger an update to the database and a restart of the entire 802.1X authentication.
2. Please use a standard 802.1X login tool such as the one that comes with windows.
3. The total number of user groups is not greater than 128.
4. Without local RADIUS authentication enabled, the contents of this database are effectively invalid.
5. If the authentication database does not have any user names and passwords, all ports are automatically authenticated.
6. Some models do not support 802.1X authentication function, subject to the actual page.

7.5 MAC port lockout

MAC port locking means manually adding a static MAC address to the switch's address forwarding table and binding this address to a port so that all data sent to this address will only be forwarded to that port, also known as MAC address binding.

A static MAC address is different from a dynamic MAC address that is learned. A dynamic address is deleted after the maximum ageing time has elapsed, whereas a static address, once added, is not subject to the maximum ageing time and will always exist if it is not deleted artificially. A MAC address in the static address table corresponds to a port, which is also known as binding a static address to a port. The purpose of binding is to restrict the movement of computers, where the MAC of a computer is bound to a port, the computer cannot communicate if it moves to another non-locked port, while other computers can still communicate if they move to this bound port. Binding is specific to the MAC address, so it restricts the computer, as opposed to port protection, which restricts the port. The configuration page for this feature is shown in Figure44

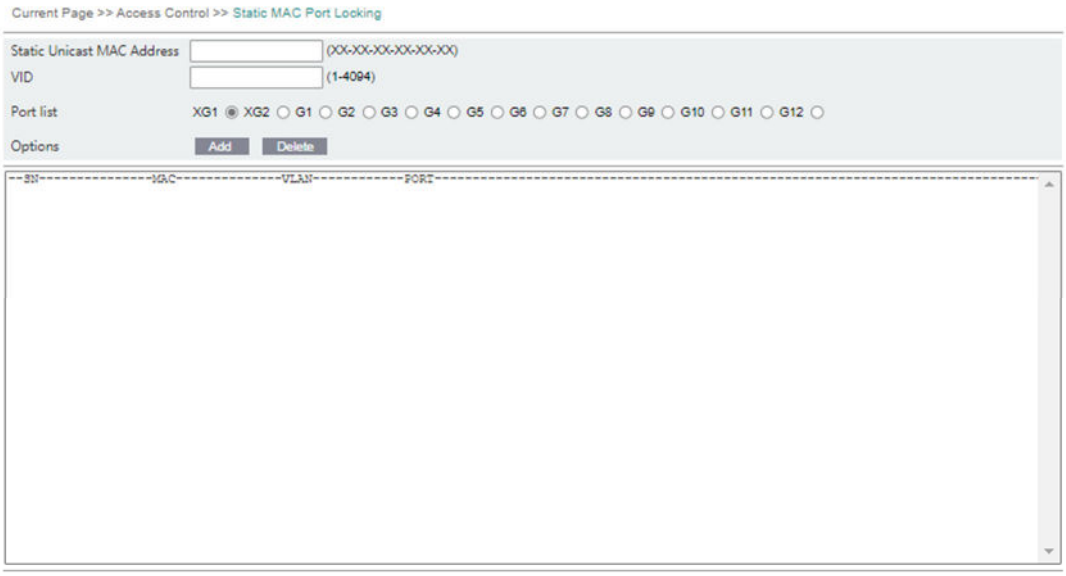


Figure44 Static MAC Port Lockout Configuration Page

The MAC port locking configuration page is very similar to the static multicast table and operates in the same way, except that the former is a one-to-one relationship, meaning that a MAC address corresponds to only one port, whereas the latter is a one-to-many relationship.

Configuration notes

Static Unicast MAC Address: Fill in this box with the static MAC unicast address to be added in the format XX-XX-XX-XX-XX-XX-XX, with the first byte of the unicast MAC address having the lowest bit 0.

Port List: Select the binding forwarding port for the packets of this unicast MAC address, just select the port to which you want to forward them, only one port is allowed to be selected here.

Processing List: This section is used to manipulate the unicast table. The buttons "Add" and "Delete" are used to add/modify and delete static MAC addresses. Existing static address table entries are displayed in the table box below, which will be updated whenever the user opens this web page or performs an add or delete operation.

Attention!

1. "The "Add" and "Delete" operations take effect immediately, unlike other pages where the configuration needs to be saved.
2. This feature is a security mechanism, so please check the settings carefully or use with caution.
3. Please do not use multicast addresses as input addresses.
4. Please do not enter a reserved MAC address, such as the MAC address of the local machine.

8 Remote monitoring

Remote monitoring features include: SNMP configuration and Email logging.

8.1 SNMP Configuration

The Simple Network Management Protocol (SNMP) is defined by the Internet Engineering Task Force and is part of the constituent Internet protocols. The SNMP protocol consists of a series of standard network management, application layer protocols, databases, and data objects. SNMP is capable of displaying management numbers, such as system description configurations, through management system forms. The SNMP protocol is based on the TCP/IP protocol and SNMP typically uses UDP ports 161 (SNMP) and 162 (SNMP-Trap), SNMP protocol agents (SNMP Agents) are present in the network devices and use standard MIBs (information specific to the device) as the device interface, through which these network devices can be monitored or controlled. When a Trap event occurs, the message is transmitted by the SNMP Trap, at which point an available Trap receiver can receive the Trap message.

SNMP v1 and SNMP v2c use community name authentication. the SNMP community is named with a string called Community Name or Community Name. the SNMP community name is used to define the relationship between the SNMP manager and the SNMP agent. The community name acts as a password-like function to restrict the SNMP manager's access to the SNMP agent on the Ethernet switch.

SNMP v3 uses a configured user for authentication, along with a security level, authentication algorithm and password, encryption algorithm and password. trap for SNMP v3 also needs to be configured based on the username and algorithm password configured on the management side, and also requires the engine ID to be consistent with the management side configuration.

Configuration notes

The SNMP enable configuration page is shown inFigure52 shown in Figure 45.



Figure45 SNMP Enablement Configuration page

SNMP configuration: Enable or disable the SNMP function, the default is disabled.

The SNMP view configuration page is shown inFigure46 shown in Figure 46.

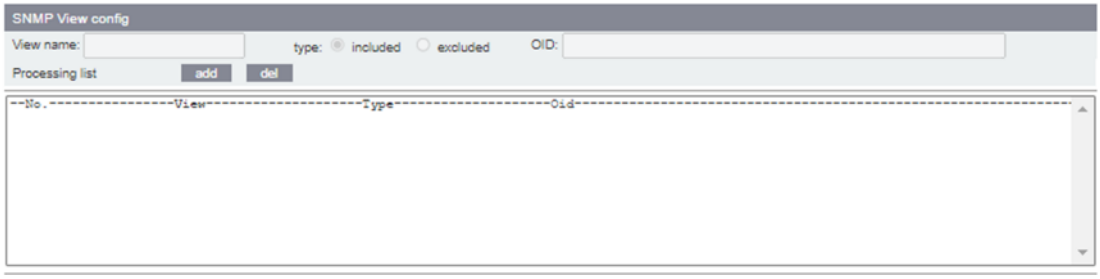


Figure46 SNMP view configuration page

View name: The name of the SNMP view configuration, named with a string.

Type: Access or inaccessibility to OID nodes is set by "Include" and "Exclude".

OID: ID of the node to be accessed.

Add: Adds a configuration to the list.

Delete: removes the selected configuration from the list.

The SNMP v1/v2c configuration page is shown inFigure54 shown in Figure 47.



Figure47 SNMPv1/v2 configuration page

Community name: The SNMP community name, also called the group name, is named with a string.

Type: Permissions for the community name Get and Set operations are set by "Read Only" and "Read/Write".

View: The view can be filled in with the view name in the view configuration or left blank, by default all nodes can be accessed.

Add: Adds a configuration to the list.

Delete: removes the selected configuration from the list.

The SNMP v3 configuration page is shown inFigure48 shown in Figure48.

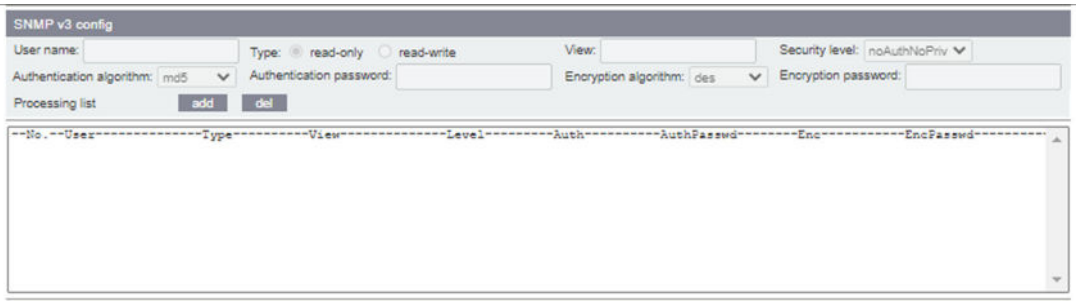


Figure48 SNMP v3 configuration page

Username: The SNMP v3 username is named with a string.

Type: Set the permissions for the user name Get operation and Set operation by "Read Only" and "Read/Write".

View: The view can be filled in with the view name in the view configuration or left blank, by default all nodes can be accessed.

Security level: SNMP v3 users can specify three security levels: "no authentication without encryption", "authentication only without encryption" and "authentication with encryption". The authentication algorithm and password, and the encryption algorithm and password should be configured accordingly.

Authentication algorithm: SNMP v3 users can specify MD5 and SHA authentication algorithms.

Authentication password: The password is 8-16 characters and contains upper and lower case letters and numbers.

Encryption algorithm: SNMP v3 users currently only support the DES encryption algorithm.

Encrypted password: The password is 8-16 characters and contains upper and lower case letters and numbers.

Add: Adds a configuration to the list.

Delete: removes the selected configuration from the list.

The SNMP v1/v2c TRAP gateway configuration page is shown inFigure56 shown in Figure 49.

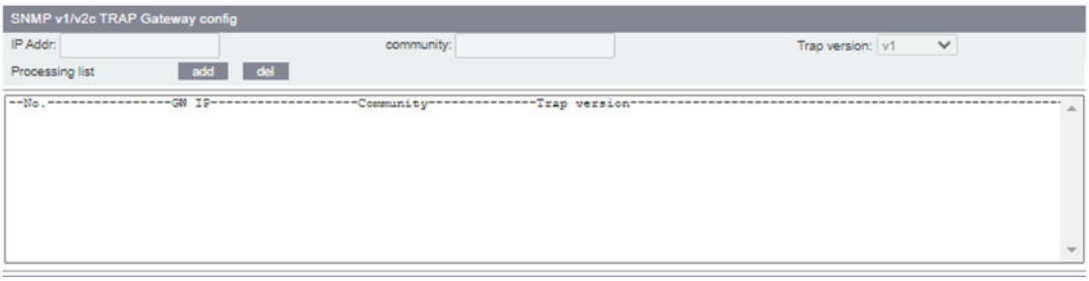


Figure49 SNMP v1/v2c TRAP Gateway configuration page

IP address: the network IP address of the recipient of the exception alert message.

Community: The SNMP community name, also called the group name, is named with a string.

Trap versions: versions are divided into v1 and v2c.

Add: Adds a configuration to the list.

Delete: removes the selected configuration from the list.

The SNMP v3 TRAP gateway configuration page is shown inFigure57 shown in Figure 50.

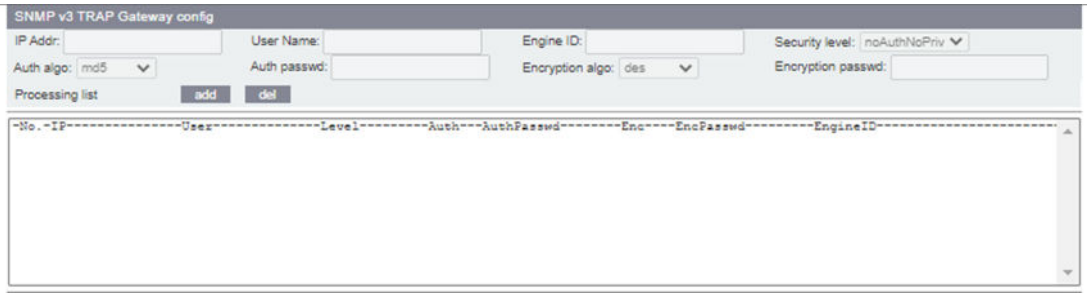


Figure50 SNMP v3 TRAP Gateway configuration page

IP address: the network IP address of the recipient of the exception alert message.

Username: The SNMP v3 username is named with a string.

Security Engine ID: The security parameter configured by SNMP v3 TRAP.

Security level: SNMP v3 users can specify three security levels: "No authentication and encryption", "Authentication without encryption" and "Authentication and encryption required". The authentication algorithm and password, and the encryption algorithm and password should be configured accordingly.

Authentication algorithm: SNMP v3 users can specify MD5 and SHA authentication algorithms.

Authentication password: The password is 8-16 characters and contains upper and lower case letters and numbers.

Encryption algorithm: SNMP v3 users currently only support the DES encryption algorithm.

Encrypted password: The password is 8-16 characters and contains upper and lower case letters and numbers.

Add: Adds a configuration to the list.

Delete: removes the configuration from the list.

Attention!

1. The switch's SNMP Agent supports part of the standard MIB-2 and RMON, and can only use get operations; it also supports our private MIBs, which can be used for simple configuration of the switch using get and set operations, but the private MIBs only have some of the functions of Web Network Management, so users are advised to use them with caution.
2. Please note the issue of read and write permissions in the SNMP browser, if you cannot read or write properly, please check the group name used.

9 Port statistics

Port statistics include configuration of: received frame statistics, sent frame statistics, total traffic statistics and MAC address table. The specific statistics are subject to the actual content of each model.

9.1 Receiving frame statistics

The switch automatically monitors each port, counts all network packets and displays these statistics on the web page as shown Figure51. These statistics are an accumulation of network packets since the switch was powered on and will all be set to zero when the switch is soft reset or rebooted after a power failure.

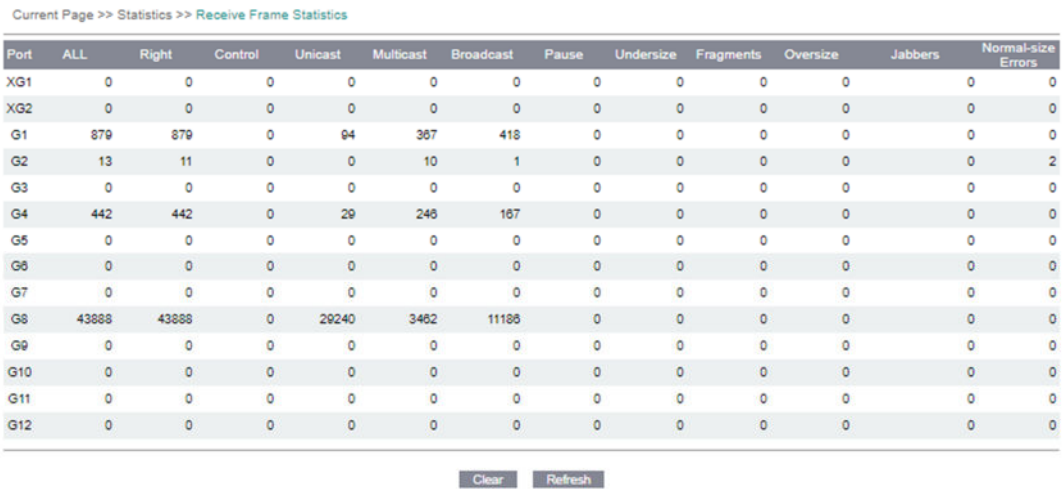


Figure51 Receiving frame statistics page

Configuration notes

All frames: the number of all packets received by the port.

Correct frames: the number of correct packets received by the port.

Control frames: The number of Ethernet control frames received by the port.

Unicast frames: the number of packets received by the port whose destination address is a unicast address.

Multicast frames: the number of packets received by the port whose destination address is a multicast address.

Broadcast frames: the number of packets received by the port whose destination address is a broadcast address.

Pause frame: Ethernet control frame received by the port with protocol 0x8808, in full duplex state, this packet is used to control how often the port sends data.

Very Short Frame: The number of packets less than 64 bytes in length, including FCS, received by the port.

Erroneous Very Short Frame: The number of packets received by the port that are less than 64 bytes in length, including FCS, and have incorrect FCS or non-complete characters.

Extra-long frames: The number of packets greater than 1518 or 1522 (VLAN on) bytes in length, including FCS, received by the port.

Incorrect over-length frame: The number of packets received by the port that are greater than 1522 bytes in length, including FCS, and have incorrect or incomplete FCS characters.

Error frame: The number of packets received by the port that are between 64 and 1518 or 1522 (VLAN on) bytes in length including FCS and have incorrect or incomplete FCS and are detected as invalid characters.

9.2 Sending frame statistics

The sending frame statistics page is shown inFigure61 shown in Figure52.

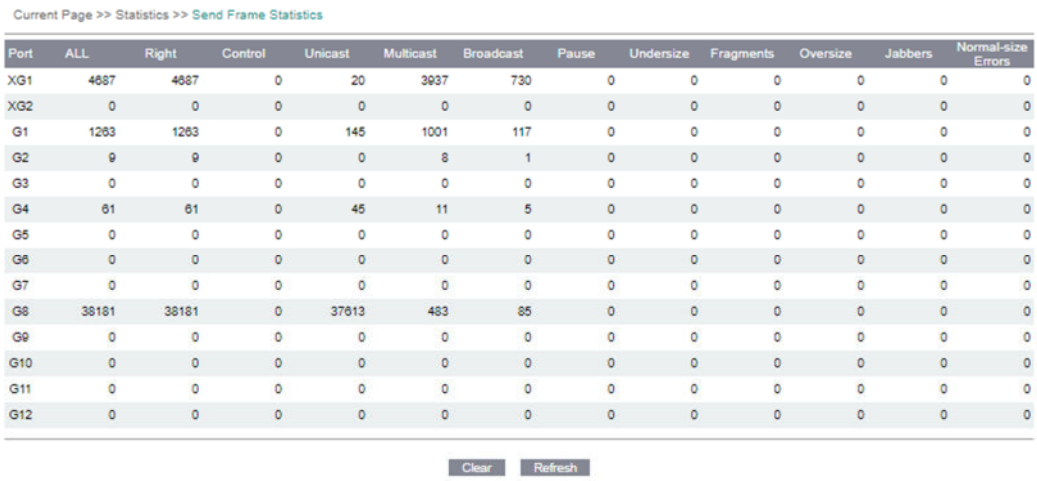


Figure52 Sending frame statistics page

Configuration notes

All frames: the number of all packets sent by the port.

Correct frames: the number of correct packets sent by the port.

Control frames: The number of Ethernet control frames sent by the port.

Unicast frames: the number of packets sent by the port whose destination address is a unicast address.

Multicast frames: the number of packets sent by the port whose destination address is a multicast address.

Broadcast frames: the number of packets sent by the port whose destination address is a broadcast address.

Pause frame: Ethernet control frame sent by the port with protocol 0x8808, in full duplex state, this packet is used to control how often the port sends data.

Very Short Frame: The number of packets less than 64 bytes in length, including FCS, sent by the port.

Incorrect ultra-short frame: The number of packets sent by the port that are less than 64 bytes in length, including FCS, and have incorrect FCS or non-complete characters.

Extra-long frames: The number of packets greater than 1518 or 1522 (VLAN on) bytes in length, including FCS, sent by the port.

Incorrect over-length frame: The number of packets sent by the port that are greater than 1522 bytes in length including FCS and have incorrect or incomplete FCS characters.

Error frames: The number of packets sent by the port that are between 64 and 1518 or 1522 (VLAN on) bytes in length including FCS and have incorrect or incomplete FCS and invalid characters detected.

9.3 Total traffic statistics

The total traffic statistics page is shown inFigure62 shown in Figure 53.

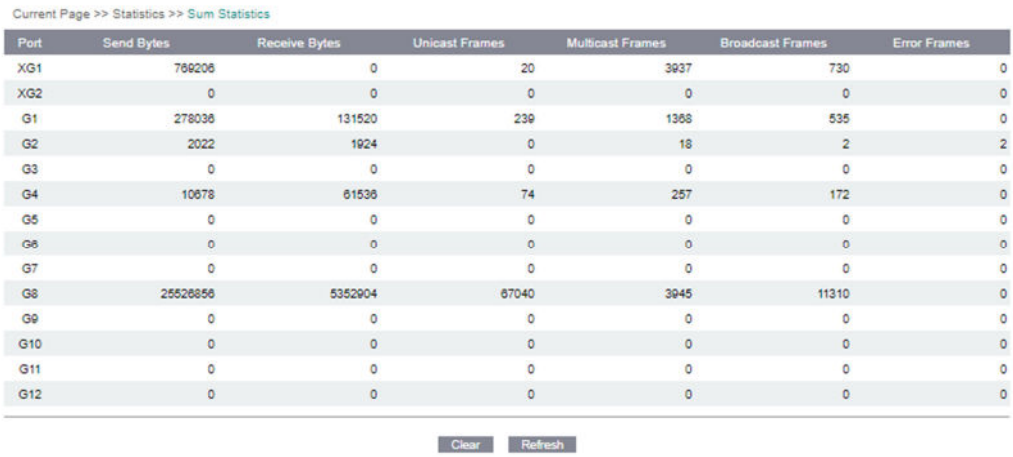


Figure53 Total traffic statistics page

Configuration notes

Total bytes sent: The total number of bytes sent by the port for all packets.

Total bytes received: the total number of bytes of all packets received by the port.

Total number of unicast packets: the number of packets sent and received by the port with a unicast destination address.

Total number of multicast packets: the number of packets sent and received by the port with a multicast destination address.

Total number of broadcast packets: the number of packets sent and received by the port with a broadcast address as the destination address.

Total number of error packets: the number of packets sent and received by the port to and from the destination address for various reasons.

9.4 MAC address table

A MAC (Media Access Control) address is a hardware identifier of a network device and the switch forwards messages based on the MAC address, which is unique and this ensures that messages are forwarded correctly. Each switch maintains a MAC address table, as shown in Figure54. In this table, the MAC addresses correspond to the ports of the switch one by one. The MAC address table is the basis and prerequisite for fast forwarding on the switch.

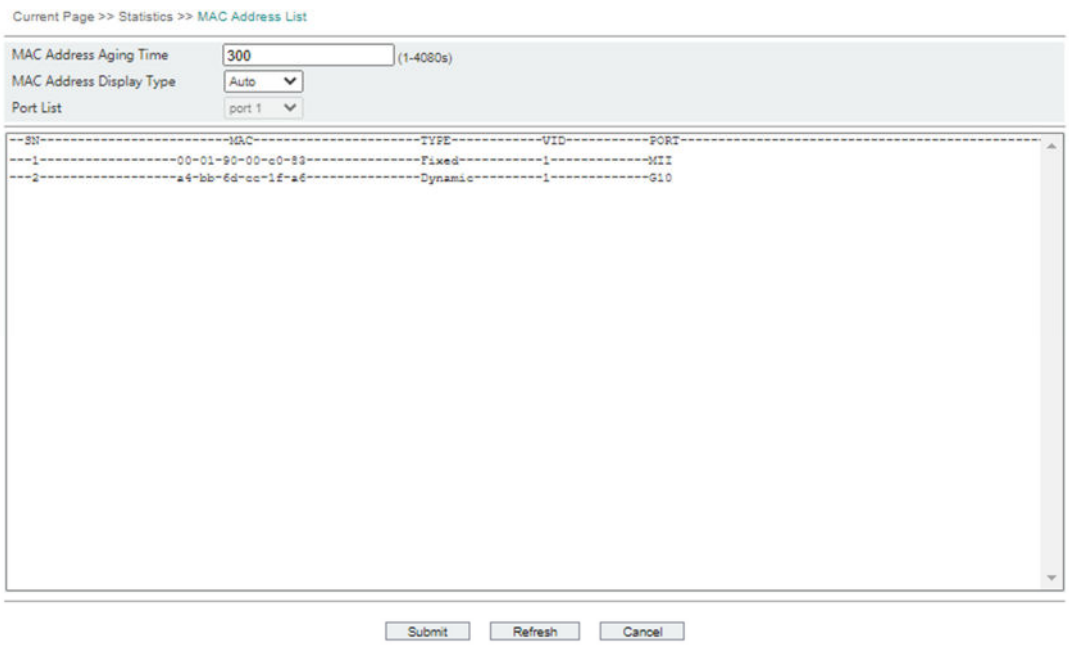


Figure54 MAC address table page

Configuration notes

MAC address aging time: After the MAC address aging time, the MAC address table previously dynamically learned will be gradually deleted. The MAC address aging time of the switch is generally 300 seconds by default.

Address display type: Specify the sorting type of the MAC address table, you can select "Auto" and "Port", when you select "Auto", all MAC addresses of all ports will be listed. Selecting "Auto" will list all MAC addresses of all ports, while selecting "Port" will only list the corresponding MAC addresses of the specified port.

Port List: Select which port's MAC address list to be displayed, this item will only be enabled if the "Address Display Type" option is "Port", when "Auto" is selected it will This item is only enabled when the "Address Display Type" option is "Port".

The MAC addresses of this switch are divided into the following three types:

- Dynamic MAC address

The type field for this type of address in the MAC address list is "dynamic". Dynamic MAC addresses are learned by the switch through data frames in the network and are deleted when the aging time comes. When the port of the switch to which the device is connected changes, the corresponding MAC address in the MAC address table and the port will also change. Dynamic MAC addresses disappear after the switch is powered down and rebooted and need to be learned again.

- Static MAC address

The type field of this type of address in the MAC address list is "static". Static MAC addresses are generated through manual user configuration and are not aged out by the switch. No matter what happens

to the ports of the switch to which the device is connected, the correspondence between MAC addresses and ports in the MAC address list will never change. Unsaved static MAC addresses will also disappear when the switch is powered down and rebooted.

- Permanent static (solidified) MAC address

The type field in the MAC address list for this type of address is "solid", a permanent static MAC address that comes with the system software and will not be aged out. No matter what happens to the ports on the switch to which the device is connected, the correspondence between the MAC address and the port in the MAC address list remains unchanged. The permanent MAC address will not disappear after the switch is powered down and rebooted.

Attention!

1. The default ageing time for MAC addresses is 300 seconds (5 minutes) and can be set via the WEB administrator.
2. The contents of the MAC address table display are subject to the actual model.

10 Network Diagnostics

Network diagnostic functions include: port mirroring and network diagnostics.

10.1 Port Mirroring

Port mirroring is the process of copying all the incoming and outgoing data from one or more ports to the designated other port. By designating a port as a mirror port of another port, all the data sent and received by the other port can be observed through that port. The port mirroring function is used for troubleshooting, debugging and analysis of the network.

The switch port mirroring feature provides multiple mirroring rules that allow users to capture incoming, outgoing or all data. The actions related to the mirroring function can be performed through the web page of this switch. Port mirroring is to copy the data on the monitored port to the designated monitoring port to analyse and monitor the data. The switch supports many-to-one mirroring, i.e. copying messages from multiple ports to one monitored port. The user can specify the direction of the monitored messages, e.g. only the messages sent by the specified port are monitored. The device uses port mirroring groups to configure the port mirroring function. Each port mirroring group contains one monitored port, and one group of monitored ports. The configuration page of this function is shown in Figure55

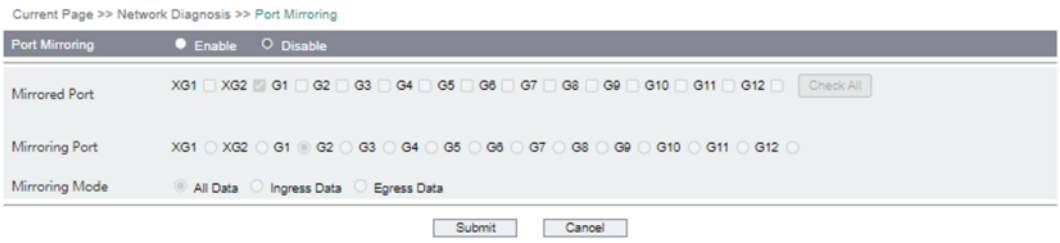


Figure55 Port Mirroring Configuration Page

Configuration notes

Port Mirroring: Enables or disables the port mirroring feature, the default is disabled.

Mirrored port: refers to the mirroring of the source port, or the port on which data is collected. The functional understanding of mirroring is that it refers to the port on which the incoming and outgoing data will be copied, and several can be set.

Mirror port: refers to the port that mirrors the destination port, or the port that collects the data. It is understood from the function of mirroring to mean the port on which the copied data is collected, and only one can be selected.

Port mirroring mode: refers to the selection of the direction in which data is collected.

Attention!

1. This feature must be disabled in normal use, otherwise all advanced port-based management features such as RSTP, IGMP Snooping will not be available.
2. The mirroring function only handles FCS normal packets and cannot handle all kinds of incorrect data frames.
3. The port mirroring function is generally used for diagnostic and debugging functions and is generally recommended to be used with caution.
4. Mirror port mode is subject to actual model, some models only support egress data and full data mirroring.

10.2 Network Diagnostics

The switch supports the ping network diagnostic function, i.e. network fault analysis, network testing or problem solving through the ping command. The configuration page is shown in Figure56

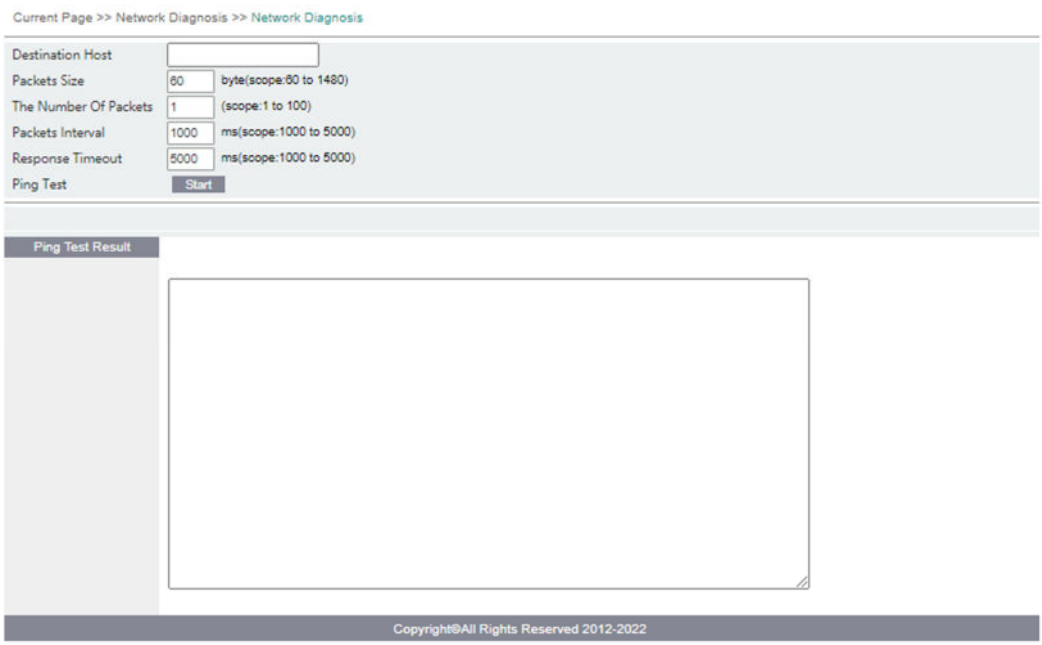


Figure56 ping network diagnostics configuration page

The Ping function uses a simple ping command to give users a simple and powerful tool for diagnosing network problems. The most unique feature of this function is the ability to enter a ping command via the web page, have the switch send a ping command itself and output the results to the web page. In this way, the user can easily control the switch to send ping commands out and output the results.

The settings for each Ping function are as followsTable4 is shown below.

Table4 Ping function configuration description table

Configuration items	Description	Default value
Destination host	Ping's IP address	Blank
Message size	Ping package length	60 (bytes)
Number of messages	Number of ping packets sent	1 (one)
Message spacing	Interval for sending Ping packets	1000 (milliseconds)
Response timeout	Ping overflow time	5000 (milliseconds)

Attention!

1. Before using the ping network diagnostic function, make sure that the first item "Allow incoming echo requests" is checked in the local connection ICMP settings of the destination windows firewall, otherwise the destination host will not be pinged.
2. The domain name of the "destination host" does not support unlimited extensions, only domain names below the third level, such as "mail.sina.com".
3. If all the "Request timeout" messages appear, the other NIC is not working properly or the network line is faulty.
4. Pinging a domain name with a "unknown host name" message indicates a DNS configuration error.
5. If a "Request timeout" message appears for a Ping domain name, there is an error in the gateway settings.

11 System administration

System administration functions include: time configuration, setting addresses, system information, log information and file management.

11.1 Time Configuration

The system time of the switch is set by the time configuration function. The switch does not have a battery backup to save the system time value, when it loses power, the system time will be lost, after power on and reboot, the system time of the switch will be restored to linux time i.e. day 1 month 1 year 1970, so you must synchronize the switch time after each power on and reboot of the switch. The time configuration page is shown in Figure57.

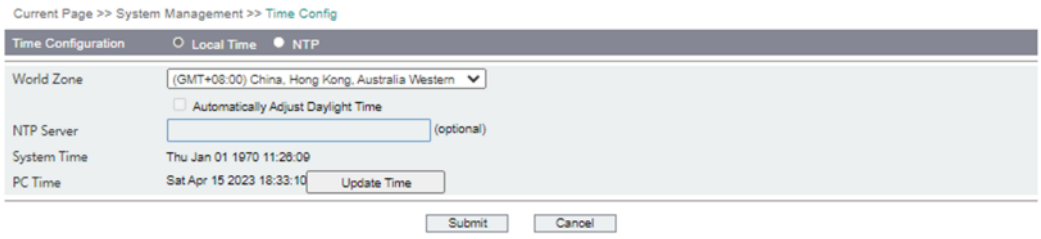


Figure57 Time configuration page

Configuration notes

Time configuration: The switch offers two different time configuration options: "Local time" and "Use NTP".

Local time: Local time is the time set by the user, usually the PC time used to access this page. When the user selects this and clicks on "Configure", the "Update time to switch" button will appear on the "PC time" line, after clicking on it, the access PC time will be updated to the switch.

Using NTP: Using NTP means that the switch automatically synchronises its time with a time server on the Internet. ntp (The Network Time Protocol) is a network time synchronisation protocol that uses the UDP protocol and port 123, the NTP protocol counteracts unstable network response times to improve the accuracy of corrected time.

World Time Zone: The division of the world time zone is based on the Prime Meridian. From 7.5° W to 7.5° E (at 15° longitude intervals) is the zero area. From the two boundaries of the zero time zone to the east and west respectively, a time zone is drawn at 15° longitude intervals. 12 time zones are drawn to the east and 12 to the west, with the 12 eastern time zones overlapping with the 12 western time zones; the globe is divided into 24 time zones. Each time zone uses the local equinox of the central meridian as the standard time of the zone. The standard time of two adjacent time zones differs by one hour. In principle, time zone boundaries follow geographical meridians, but in practice they are often determined according to the administrative or natural boundaries of countries for ease of use.

The relevant time zone can be selected in the device according to the typical geographical area and the device automatically adjusts the internal time offset according to the selected time zone.

Automatic adjustment of daylight saving time: Automatic adjustment of daylight saving time: Daylight saving time is one hour earlier than standard time. For example, during daylight saving time, 10 a.m. in standard time becomes 11 a.m. in daylight saving time. Daylight saving time, also known as daylight saving time or summer time, is a system of artificially set local times to save energy. Daylight saving time is currently practised in nearly 110 countries around the world each year. When selecting a specific geographical area, the option can be set if the area allows "daylight saving time", otherwise it is greyed out and invalid.

NTP Server: The host name or IP address that can provide NTP time service, can be empty.

System time: The current system time of the device itself, which is "Thursday, 01 January 1970 08:00:00" after power on, can be updated manually to the switch or automatically using NTP.

PC time: the system time of the PC accessing the web server. If the current time is configured as "local time", the "Update time to switch" button will appear after the PC time, click this button to synchronise the PC time to the switch at this time.

Attention!

1. When selecting "Use NTP", the NTP server can be empty and the switch should be able to access the internet and use a public internet NTP server.
2. The "Update time to switch" button will only pop up after the user has selected "Local time" and clicked "Configure", and will only disappear when the user switches to " When the user switches to "Select NTP", it must also disappear after clicking "Configure".
3. Only the "Administrator" has the right to configure the time of the device manually.
4. The time zone and daylight saving time must be configured, either using "local time" or "NTP time".
5. The NTP server or visitor's PC time configuration may cause the display to be off, and the display can be adjusted by changing the time display format.

11.2 Equipment Address

This function will assign an IP address to the switch. Normally IP addresses are assigned in two ways: automatically (DHCP) or by assigning an IP address. The switch is shipped with a fixed IP address of 192.168.40.253 by default. the configuration page is shown inFigure58 The configuration page is shown in Figure58.



Figure58 Device address configuration page

Configuration notes

DHCP Dynamic IP Address: Uses the DHCP protocol to dynamically assign an IP address from a DHCP server, requiring a DHCP server in the network. Users are advised to use caution because access to the web server requires explicit knowledge of the switch's IP address, whereas a dynamic IP address cannot be determined until it is assigned, and a new IP address may be assigned each time it is rebooted.

Static IP address: Manually set a fixed static IP address. It is recommended that users use this option to manually set a fixed IP address for the convenience of the webmaster, and the set IP address must not be in conflict.

IP address: An IP address is a 32-bit-long address assigned to a device connected to the Internet. IP addresses consist of two fields: a network number field (net-id) and a host number field (host-id). IP

addresses are assigned by the Network Information Center (NIC) of the U.S. Defense Data Network. IP addresses are divided into five categories for ease of IP address management.

Class A, B and C addresses are unicast addresses; Class D addresses are multicast addresses; and Class E addresses are reserved for special use in the future. Class E addresses are reserved for special use in the future. The IP addresses currently in heavy use belong to classes A, B and C.

IP addresses are recorded in dotted decimal format. Each IP address is represented as four decimal integers separated by a decimal point, each corresponding to one byte, e.g. 10.110.50.101.

The mask is a 32-bit number corresponding to an IP address, some of which are 1's and some are 0's. In principle, these 1's and 0's can be combined in any way, but the mask is generally designed so that the beginning consecutive bits of the mask are set to 1. The mask divides the IP address into two parts: the subnet address and the host address. The mask for a class A address is 255.0.0.0; for a class B address it is 255.255.0.0; for a class C address it is 255.255.255.0.

The use of masks splits a Class A network, which can include more than 16 million hosts, or a Class B network of more than 60,000 hosts, into many smaller networks, each of which is called a subnet.

Default gateway: The default gateway in a host is often referred to as the default route. A default route is the route chosen by a router when no other route exists for the destination address in an IP packet. The default route is used for all packets whose destination is not in the router's routing table. This route generally connects to another router, which also processes the packet, and if it knows how to route the packet, the packet is forwarded to the known route; otherwise, the packet is forwarded to the defaultroute, which reaches another router.

DNS address: The full name of DNS is Domain Name Server, which serves to resolve domain names, which are easy for us to remember, into IP addresses that are recognisable on the Internet. If our device needs to access a host name, we need to use this server to resolve it into an IP address.

Attention!

1. The range of IP addresses we can set should be 192.168.x.x, 172.[16-31].x.x or 10.x.x.x.
2. NTP and Email will make use of the DNS service, so please make sure you fill in the correct DNS address if applying these two services.

11.3 System Information

The System Information page displays basic information about the switch system. The page shown

in Figure59 allows users to learn system-related information about the switch and set the name and location of the switch.

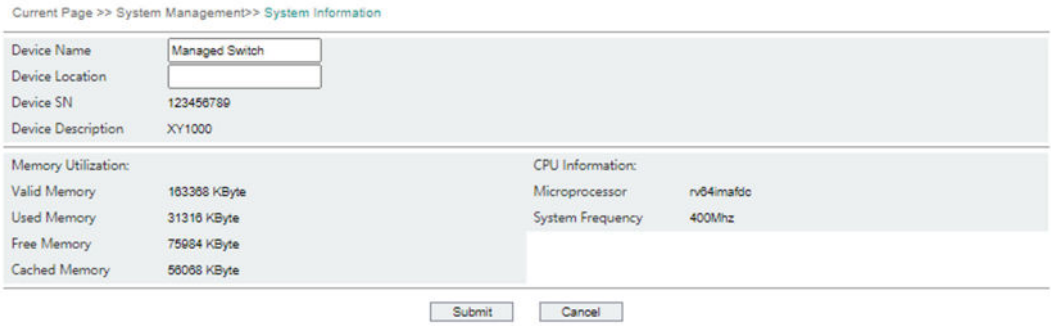


Figure59 System information configuration page

Configuration notes

Device name: User-defined switch name for differentiation and support for Chinese input.

Device location: User-defined device location.

Device Number: Describes the switch's factory number.

Device description: i.e. the model number of the switch, determined by the hardware and cannot be modified by the user.

Memory usage: Describes the switch system memory usage.

CPU information: describes the basic information of the CPU of the switch system.

11.4 Log information

The device provides a logging function for users to refer to possible setup problems. When this feature is enabled, the switch will record relevant events that occur and save them to a log message file. The logging feature saves all records to memory and can store over 2000 records. When the maximum number of records is exceeded, old records will be automatically deleted and new records will be added. The following events are saved to the log file:

- System reboot
- Port Link Down/UP
- Login information
- When the radio storm happened
- System action and operation logging
- NTP time synchronisation information
- Records of RING/ RSTP/ SNMP etc. operations
- Some other system information

The log information display page is shown in Figure60

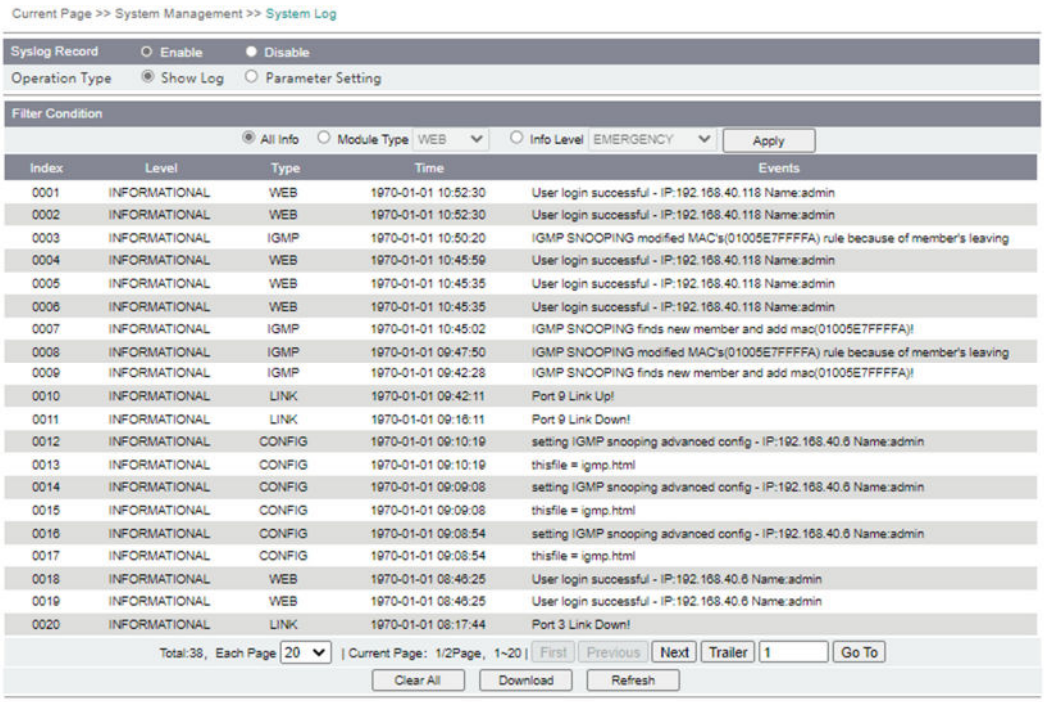


Figure60 Log display page

Configuration notes

Logging: Enable or disable the logging function, the default is enabled, the logging function does not delete the log content when disabled, it just does not add new log information.

Type of operation: Switching between the "Log display" and "Parameter settings" pages.

Filter criteria: Display a certain type of message, you can switch between "All messages", "Module type" and "Message level".

Apply: Once you have selected the filter criteria, click Apply to refresh the log display information.

Home: When clicked, the log displays information directly back to the first page.

Previous page: When clicked, the log displays information forward one page.

Next page: When clicked, the log displays information backwards one page.

Last page: When clicked, the log display information jumps directly to the last page.

Clear all messages: Click this button to clear all log messages.

Download Logs: Click this button to download the log information from the web server and save it to the accessing PC, the file name is syslog.cfg, please use your browser to download it directly, the web server of this switch does not support multi-threaded download tools such as Xunlei.

Refresh: When clicked, the log display information will be refreshed to show the first page of log content, with the latest log at the top.

The logging parameter setting page is shown inFigure61.

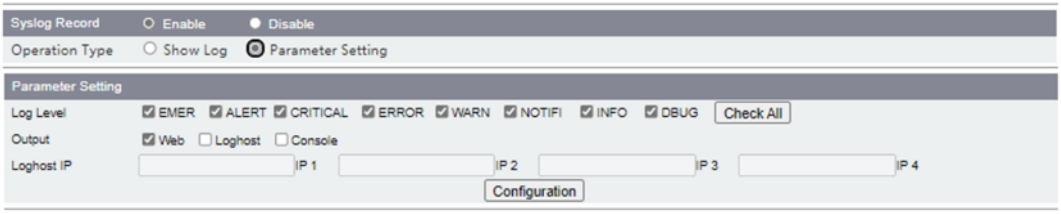


Figure61 Logging parameters setting page

Configuration notes

Log Levels: Depending on the severity of the logs, there are seven levels of logging: Emergency / Alert / Critical / Error / Warning / Notification / Informational / Debug.

Log output: The log output is directed to the WEB page, the log host and the console.

Log Host IP: Set the IP address of the log host. This parameter can only be filled in if the log host is checked in the log output.

Configuration: After configuring the logging parameters, click on the "Configure" button for the settings to take effect, otherwise they will not take effect.

11.5 Document Management

The file management page is shown inFigure72 shown in Figure 62. This page performs some non-routine system operations on the switch and users are advised to use caution as improper operation may damage the switch. These operations can only be performed by the "Administrator".



Figure62 Document management page

The information in this document is subject to change without notice. E-link China Technology Co., Ltd. has made all effects to ensure the accuracy of the information, but all information in this document does not constitute any kind of warranty. If you have any questions please feel free to contact to us.

E-link China Technology Co., Ltd
www.e-linkchina.com.cn
Support: sales@e-linkchina.com
Telephone: +86-755-83128674