EN50155 MANAGED ETHERNET SWITCH

WEB MANAGEMENT

USER GUIDE

Technical Service E-mail: service@xallcom.com

www.xallcom.com/en/

THANK YOU FOR CHOOSING OUR PRODUCTS

Thank you for buying our products. To help you use our products quickly and correctly, we recommend that you read this manual carefully. If you encounter problems in your use or have good suggestions, please contact us in time.

COPYRIGHT STATEMENT
ALL RIGHTS RESERVED

Contents

1. Log in to the WEB interface

1.1 Log in to the WEB configuration interface

To log in to the WEB configuration interface for this series of switches, the user should confirm the following conditions:

- The switch has been IP configured and the default IP address is 192.168.1.254
- Users guarantee that the IP of their local PC (management host) network card(adapter) is the network segment of 192.168.1. *.
- The user guarantees that the network cable of his local PC is connected to any RJ 45 Ethernet port of the switch.
- A host with a Web browser installed is connected to the network, and the host has the PING pass of switch.

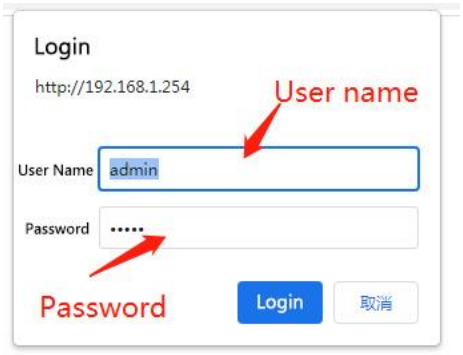
Log on to the WEB configuration interface:

Step1 Run the browser in the PC.

Step2 Enter the address of the switch "http: // 192.168.1.254" in the browser address bar and press Enter.

Step3 As shown in Figure 1-1, enter the user name and password in the login window (the default user name and password are admin) and click OK.

Figure 1-1 WEB interface login window



After successful login, you can configure the relevant parameters and information of the WEB interface as required.

2. System Information

2.1 System Information

[Function Description]

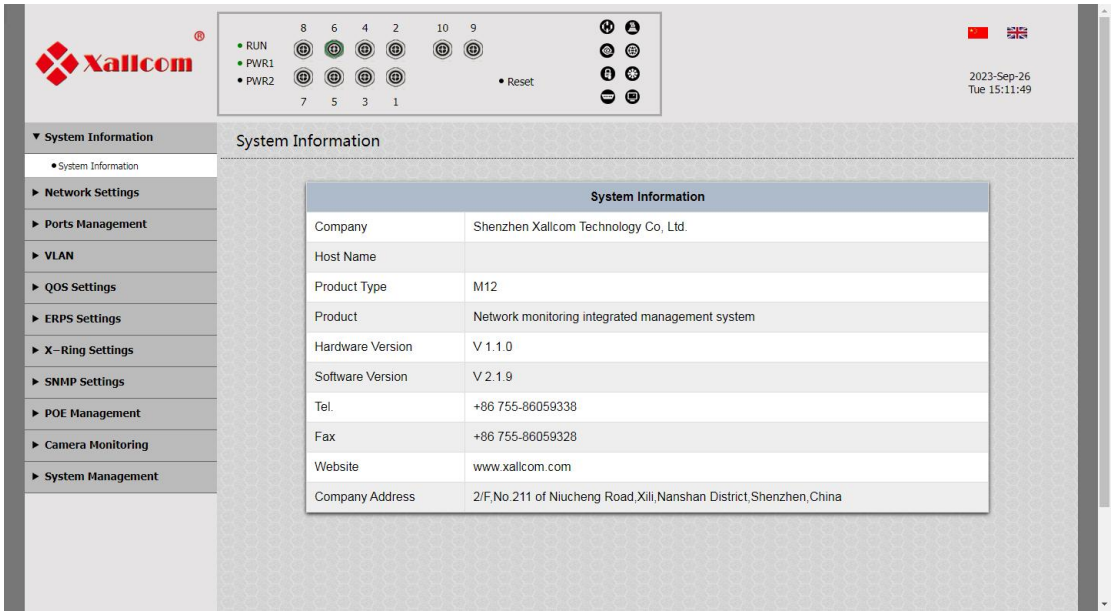
On the System Information page, you can view the product model, hardware version, software version, company information, system time and other information.

[Operation Path]

System Information> System Information

[Interface Description]

Figure 2-1 System Information Interface



Click the two small flags in the upper right corner of the page to choose the language.

The optional language is simple Chinese and English.

Figure 2-2 Main Elements of The System Information Interface

System Information	
Company	Shenzhen Xallcom Technology Co, Ltd.
Host Name	
Product Type	M12
Product	Network monitoring integrated management system
Hardware Version	V 1.1.0
Software Version	V 2.1.9
Tel.	+86 755-86059338
Fax	+86 755-86059328
Website	www.xallcom.com
Company Address	2/F,No.211 of Niucheng Road,Xili,Nanshan District,Shenzhen,China

3. Network Setting

3.1 Parameter Setting

[Function Description]

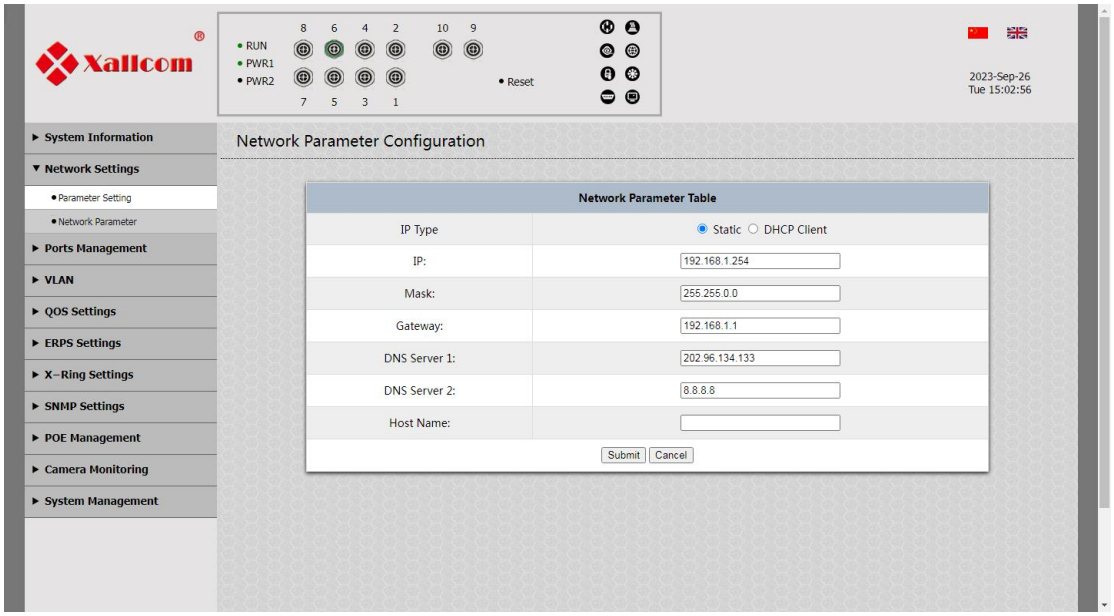
First, the user can choose the type of IP (IP Type). Static IP type (static) can be selected, and users need to set up IP, Mask (subnet mask), Gateway, and DNS Server (domain name system server). The next time the user logs in to the configuration interface, he/she should fill in the same IP address in the web page. You can also choose the dynamic IP type (DHCP Client), IP, Mask (subnet mask), Gateway (gateway) will automatically match, just set the DNS Server (domain name system server).

[Operation Path]

Network Settings> Parameter Setting

[Interface Description]

Figure 3-1 Network Parameter Configuration Interface



3.2 Network Parameter

[Function Description]

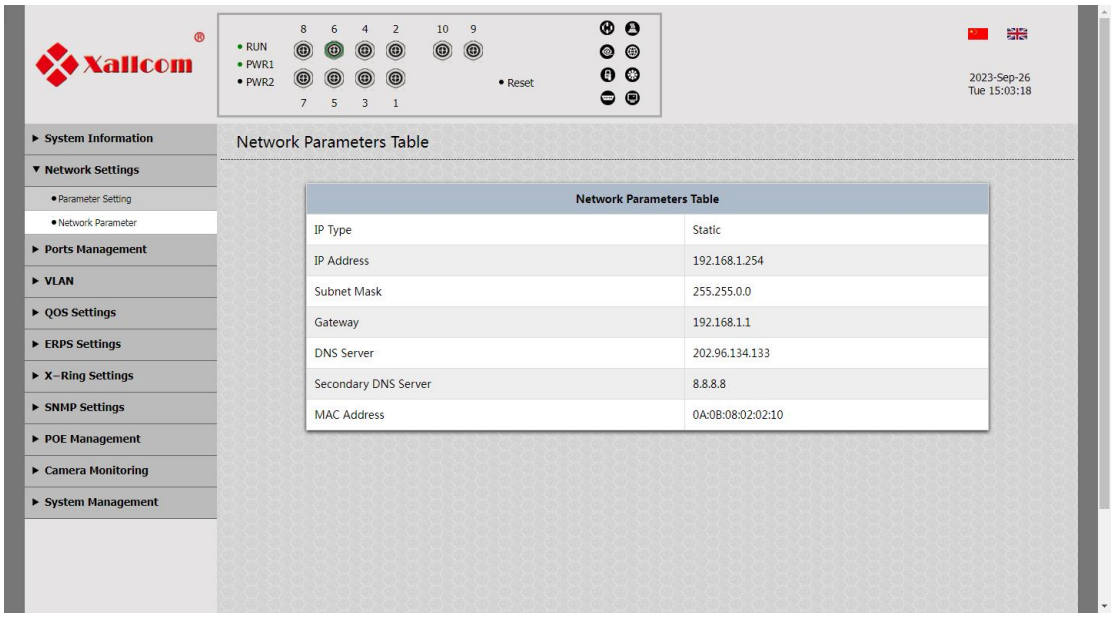
Users can obtain local network parameters, including the type of IP (IP Type), IP address, IP, Mask (subnet mask), Gateway, DNS Server (domain name system server), Alternate DNS Server, MAC address.

[Operation Path]

Network Settings> Network Parameter

[Interface Description]

Figure 3-2 Network Parameter Interface



4. Port Management

4.1 Port Configuration

[Function Description]

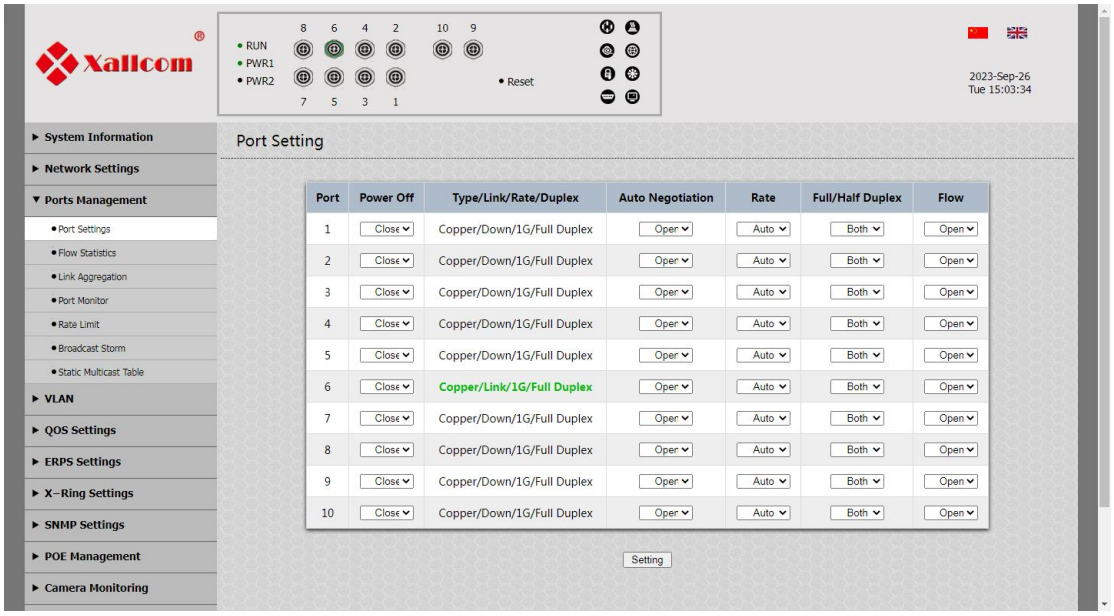
On the Port Configuration page, you can enable or disable ports, enable or disable port auto negotiation, set port rate, full duplex, flow control; Click “Setting” after the configuration is completed. Or to view the basic information for all of the ports.

[Operation Path]

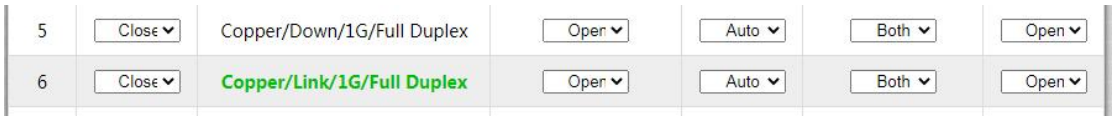
Ports Management> Port Settings

[Interface Description]

Figure 4-1 Port Setting Interface



As shown in the figure, in the switch port configuration interface, please click "Ports Management" and then click "Port Settings". From the configuration area, we can see the type of each port, connection status, port rate, duplex mode, flow control status, auto negotiation mode; opening and closing of ports, as well as rate, duplex mode, sending and receiving direction flow control function, and auto negotiation mode are configurable.



- Port: display the switch port number;
- Power Off: to open or close the corresponding port;
- Type/ Link/ Rate/Duplex: display the port connection status;

Color of Light	Meaning
Green	The link is connected (Link)
Black	Indicate that the link is unconnected (Down)

- Rate(Available Options as Follows): displays the current port rate;
- Full/Half Duplex(Available Options as Follows): configure the port duplex mode;

Rate	Duplex Mode
Auto	Both
1G	Full
100M	Half
10M	

4.2 Flow Statistics

[Function Description]

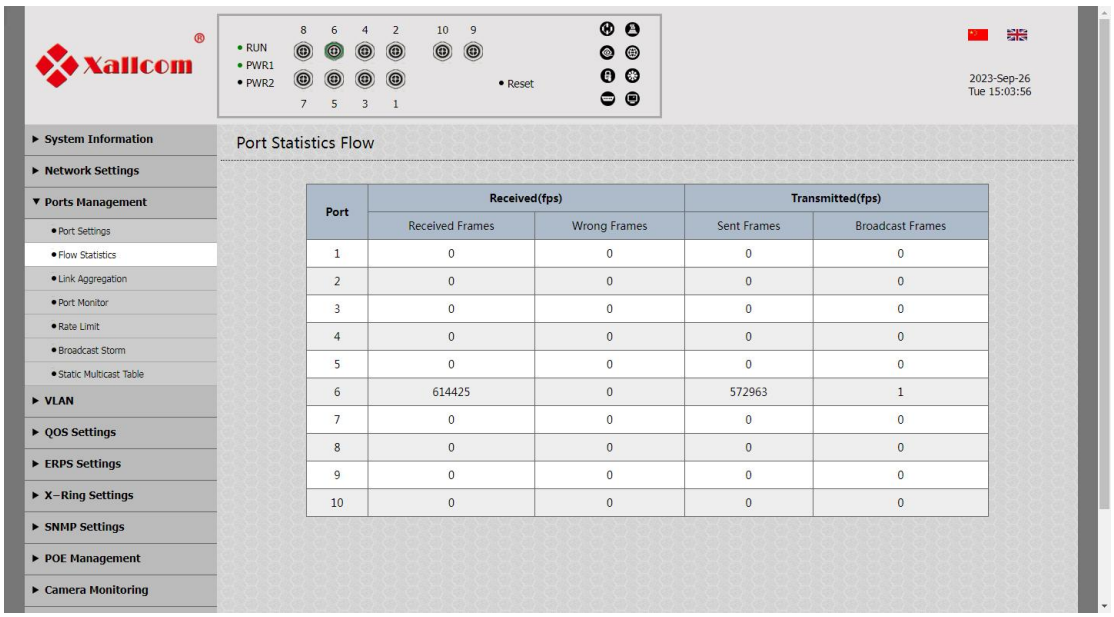
In the normal running network, each port will generate traffic, for this reason, the flow memory statistics is in the web interface

[Operation Path]

Ports Management> Flow Statistics

[Interface Description]

Figure 4-2 Flow Statistics Interface



Port	Received(fps)		Transmitted(fps)	
	Received Frames	Wrong Frames	Sent Frames	Broadcast Frames
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	614425	0	572963	1
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0

Port: you can see the traffic packets received and sent by each port, measuring by frame, recording how many frames and wrong packets are received or sent by now. Wrong packet refers to the received Ethernet package which has the failed verification.

4.3 Link Aggregation

[Function Description]

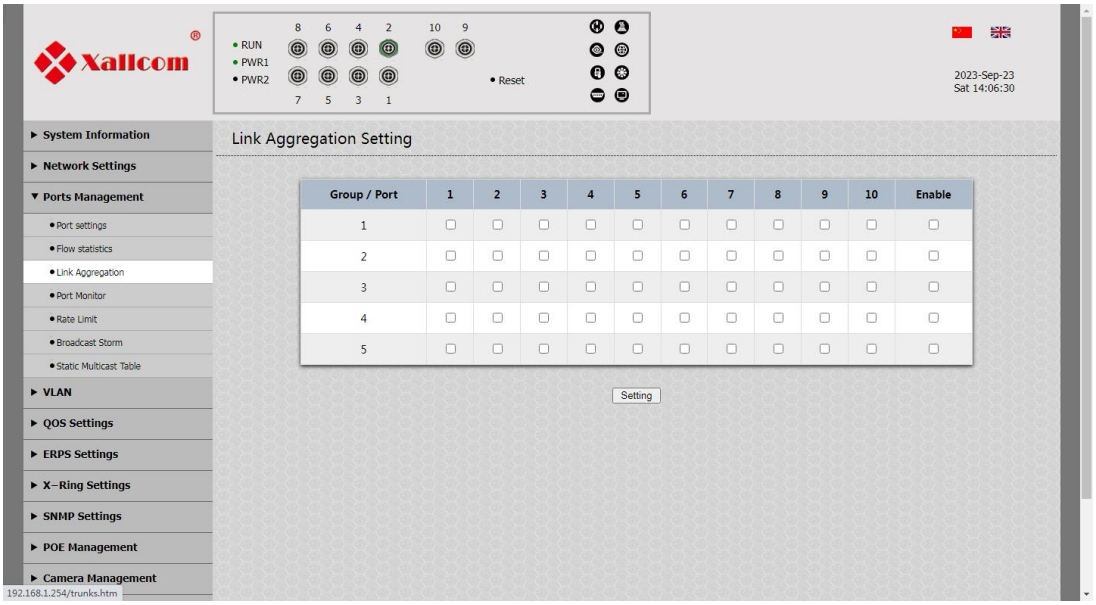
This industrial switch provides Trunking function, it allows two or more ports as a single logical link as a group of Trunking, used to improve bandwidth and link redundancy, when a physical connection cannot communicate or failure, other links in the Trunking group immediately take over and maintain communication, so you can provide a quick recovery mechanism after communication interruption.

[Operation Path]

Ports Management> Link Aggregation

[Interface Description]

Figure 4-3 Link Aggregation Interface



This industrial switch provides 5 groups of Trunking selection. A port cannot exist in both two Trunking groups. Click the check box to add port to Trunking group, the port marked with " √ " belongs to a member of a Trunking group and not with " √ " means not a member of a Trunking group. When you use Trunking, you must enable it before physical connect.

4.4 Port Mirror

[Function Description]

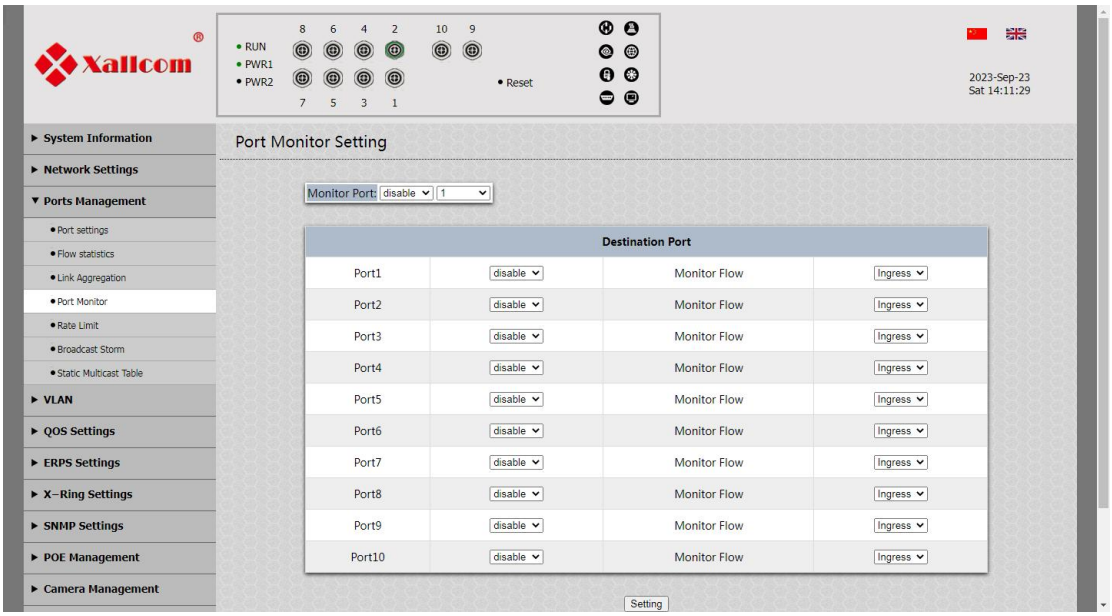
Port Mirror is also called port monitoring. Port monitoring is a kind of packet acquisition technology, through the configuration switch, can realize a / several ports (mirror source port) packet copy to a specific port (mirror destination port), in the mirror port with a host installed packet analysis software, the collected packet analysis, so as to achieve the purpose of network monitoring and troubleshooting network faults.

[Operation Path]

Ports Management> Port Mirror

[Interface Description]

Figure 4-4 Port Mirror Interface



- Mirror Destination Port: the port to listen on, only one is allowed to select, disabled by default;
- Mirror Source Port-Port: the port to be listened on, you can select one or more;
- Mirror Source Port-Mode:three modes: Ingress, Egress, All ;

4.5 Rate Limit

[Function Description]

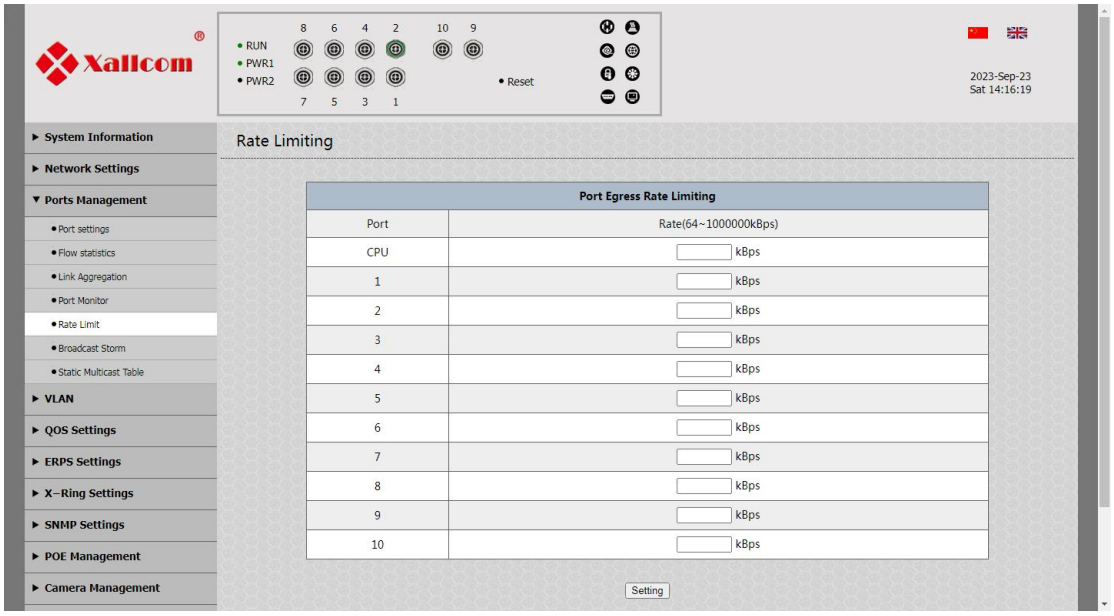
The rate limit of the industrial switch is mainly limiting the data entry bandwidth and outlet bandwidth, and clearly defines the packet receiving type and bandwidth limit. This helps the administrator to control all ports of the switch and avoid unpredictable failures. The types of input control packages are: 1, all packages; 2, broadcast, multicast, unknown unicast; 3, broadcast, multicast; 4, multicast. It can be reasonably configured according to the data in the network, and limit the bandwidth to achieve the effect of saving CPU resources. The limitation of output bandwidth can improve the condition of the network. The limiting units are the kBps

[Operation Path]

Ports Management> Rate Limit

[Interface Description]

Figure 4-5 Rate Limit Interface



4.6 Storm Control

[Function Description]

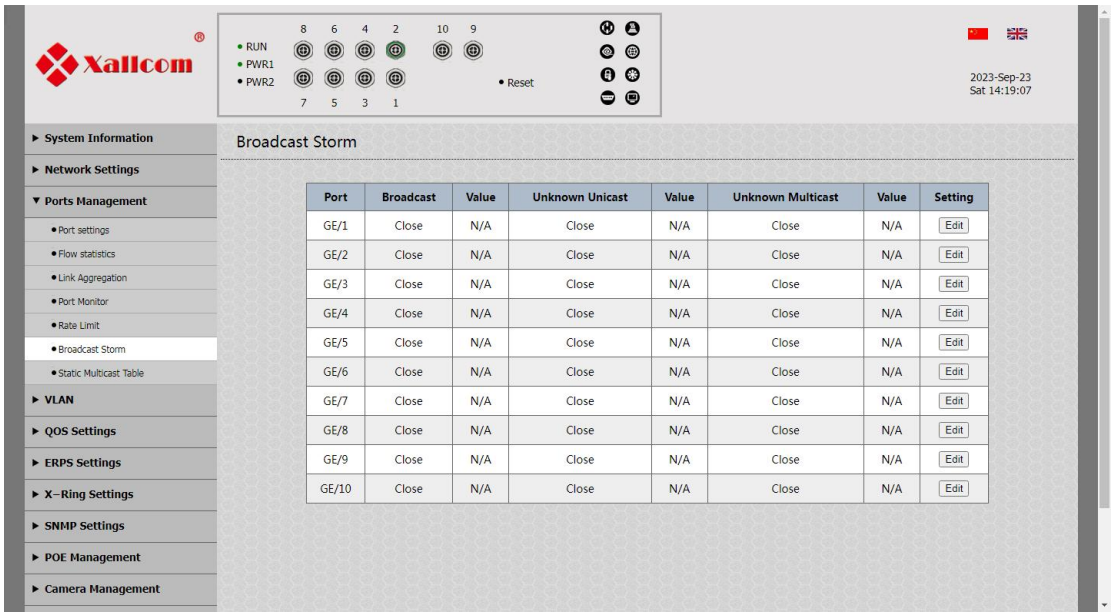
Broadcast storm simply means that when the broadcast data fills the network and the data can not be processed and occupies a lot of network bandwidth, resulting in normal business can not run, or even completely paralyzed, this is the "broadcast storm". A data frame or packet is transmitted to every node of a local network segment (defined by the broadcast domain) is a broadcast; Broadcasts are heavily replicated within a network segment, data frames are transmitted crazily which leading to network performance degradation, or even network paralysis, owing to network design, connection problems of network topology or other reasons, it is also a broadcast storm. The industrial switch can limit the broadcast package, unknown single broadcast package, unknown multicast package.

[Operation Path]

Ports Management> Broadcast Storm

[Interface Description]

Figure 4-6 Storm Suppression Interface



4.7 Static Multicast Filtering

[Function Description]

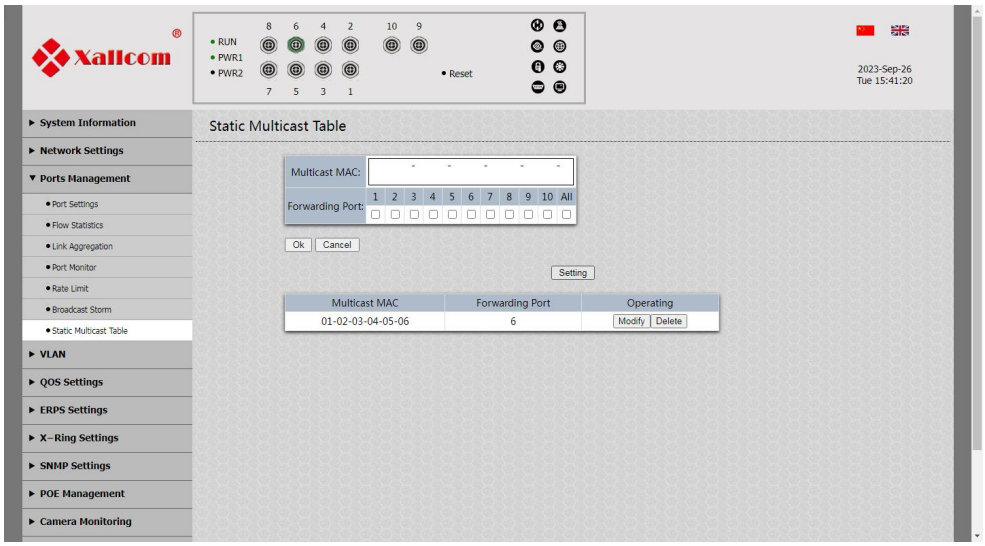
Users can configure the MAC address of the multicast for different ports, and the data can be transmitted according to the multicast address. One port can belong to different multicast groups. The lowest bit of the first byte in the multicast address is 1

[Operation Path]

Ports Management> Static Multicast Table

[Interface Description]

Figure 4-7 Static Multicast Table Interface



Setups:

1. In the text box after the "Multicast MAC", fill in the multicast MAC address such as:

01-00-11-00-00-00, which must be separated by a horizontal bar.

2. After the "Forwarding port" column, you need to tick the output port number;

3. Click the “OK” button, and the multicast and port information will appear below

the “Setting”;

4. Click the “Setting” button, and the prameters in the table will be set to the switch.

If you find that some entries have been wrong, you can click the “Modify”, then to enter the right entries, after that, click “Setting” to confirm the new entries; If you don’t need the entry, click the “Delete” button, then click the “Setting” to confirm the modification, and then the entry will be deleted from the table.

5. VLAN

[Function Description]

A virtual LAN, often called a vLAN or a VLAN (Virtual Local Area Network). Virtual LAN is a method to create a separate logical network from a practical physical network that enables several virtual LAN to be stored in a practical physical network at the same time. This can effectively reduce the broadcast range and facilitate network management through separated logical network segments (such as company departments) that cannot conduct data exchange. In fact, if a router is added between these different virtual network segments, data can still be exchanged between them.

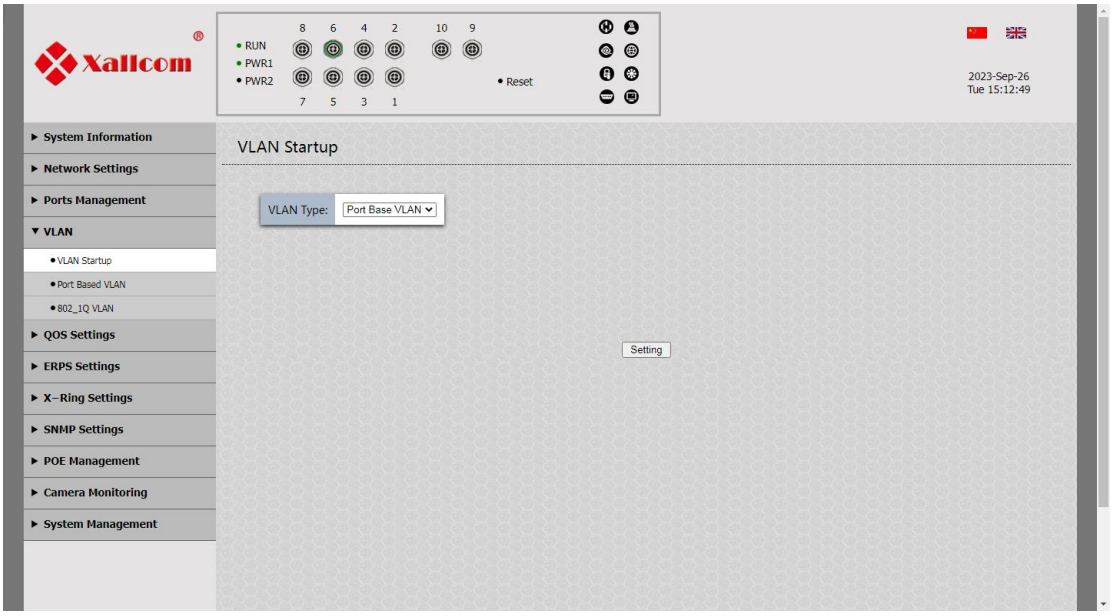
This industrial switch supports port-based VLAN and 802.1Q-based VLAN .

[Operation Path]

VLAN > VLAN Startup

[Interface Description]

Figure 5 VLAN Startup Interface



5.1 Port-Based VLAN

[Function Description]

VLAN can effectively suppress the occurrence of broadcast storms. Port-based VLAN provides a solution that divides switch ports into different virtual private domains. Data exchange is not allowed between different private domains, so the data maintenance in each private domain becomes relatively secure.

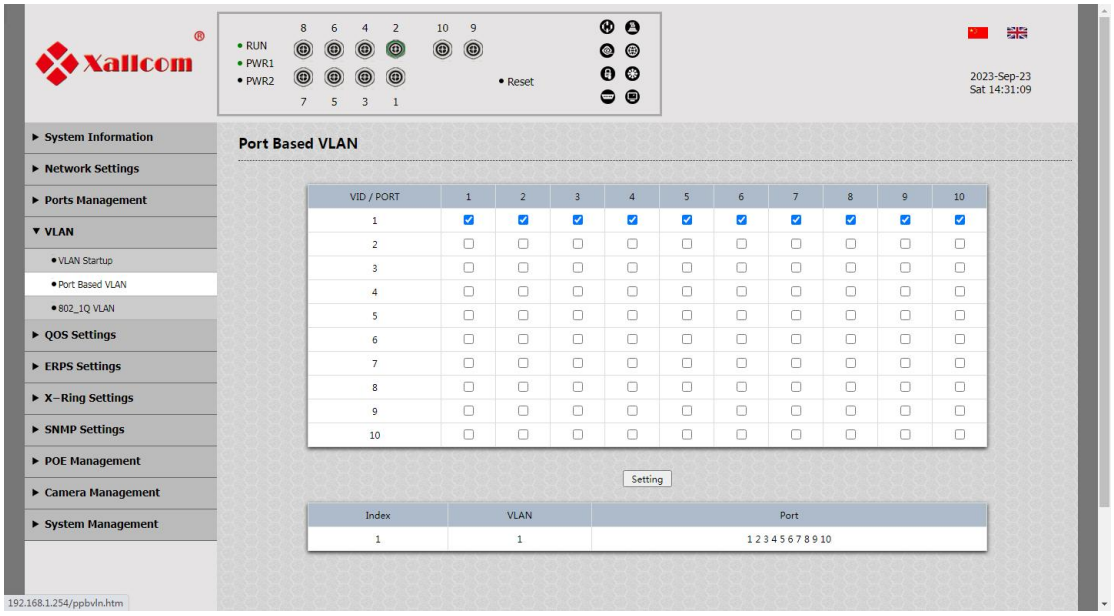
This industrial switch provides a flexible VLAN configuration for each port, and the port VLAN acts as a filter to filter out traffic on ports that are not private domains. Configure the port VLAN through the Web page below. This industrial switch provides 10 groups of port based VLAN, one port can belong to any VLAN group or all VLAN groups. Ports can overlap. Port-based priority is higher than 802.1QVLAN-based, while effective.

[Operation Path]

VLAN > Port Based VLAN

[Interface Description]

Figure 5-1 Port Based VLAN Interface



5.2 802.1Q Based VLAN

[Function Description]

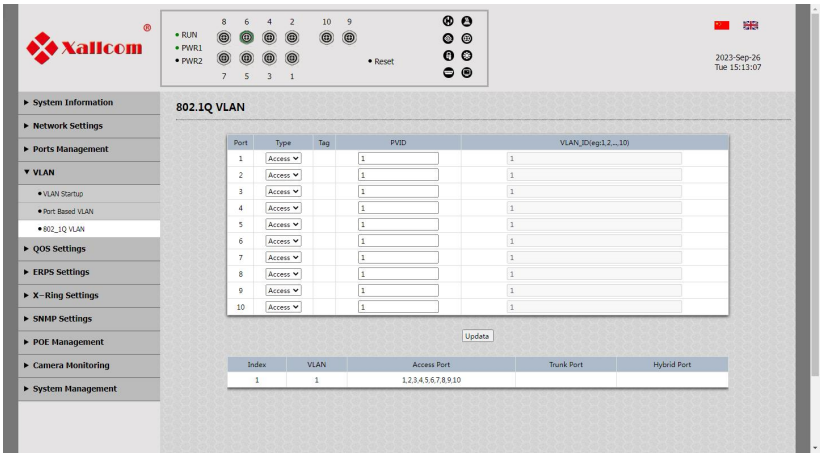
This industrial switch also supports IEEE 802.1Q VLAN . The virtual LAN can be divided across multiple switches through the IEEE802.1Q protocol. Support standard IEEE802.1Q protocol and can be compatible with other switches that support IEEE802.1Q protocol standard. Can connect devices that recognize or cannot recognize 802.1Q tags.

[Operation Path]

VLAN> 802.1Q VLAN

[Interface Description]

Figure 5-2 802.1Q VLAN Interface



PVID: Since the ACCESS port should not be with TAG, but it is supposed to be with the 802.1Q tag to exchange inside the switch, then PVID is the VLAN ID to add. TRUNK ports have TAG, but if there is Ethernet package which has no TAG to reach the port, PVID will be added to the Ethernet package so that it can be switched inside the switch. Similarly, if an Ethernet package with a TAG enters the ACCESS port, the switch will remove the original TAG, then add the PVID.

If you want to support a 802.1Q VLAN on a network, the ports connected between the switches are basically set to TRUNK ports to deliver different TAGs for each port. If all VLAN ID on a network are the same, it doesn't matter that the ports connected between the switches have been set to ACCESS.

IEEE 802.1Q VLAN can be configured through the Web page. In the above figure, two VLAN are configured, in which all UNTAG ports correspond to the port type ACCESS in WEB. Generally, they are the port directly connected to the computer, and the sending and receiving data are all without TAG. The ports connected to the two switches in the figure above must be set to be with a TAG, corresponding to the port type TRUNK in WEB, and two VLAN ID must be set.

In the setting of 802.1Q VLAN , the user can set different switch ports on the same VLAN, normally select the Access port type that ports not connected to other switches, and the PVID should set the same to communicate. Network lines connected to other switches should be set to the Trunk type, and all VLAN ID passing through that path are added with a "," in the back space for a comma separation. As shown in the figure below:

- Port default VLAN : Port default VLAN , or port PVID. The default VLAN of the Access port is the VLAN where it is located; the Trunk port and Hybrid ports can allow multiple VLAN passes to configure the default VLAN .
- Tag: Set up whether to add Tag to the port, Access port without Tag, and Trunk port generally adds Tag, mainly in Hybrid mode.
- VLAN_ID: the VLAN of the port. If set 1-3 or 1,2,3, the port belongs to VLAN 1-3.
- Type: Access, Trunk and Hybrid.

Access: The port can only send one VLAN message, and the message is sent without VLAN Tag. Generally used to connect to user terminal devices that cannot recognize VLAN Tag or do not need to distinguish different VLAN members.

Trunk: The port can send multiple VLAN messages, the port sends the default VLAN messages without VLAN Tag, other VLAN messages must bring VLAN Tag. Usually used for interconnections between network transmission devices.

Hybrid: The port can send multiple VLAN messages, and the messages sent by the port can be configured with some VLAN messages with VLAN Tag as needed, and

some VLAN messages without VLAN Tag. The Hybrid type port can be both used to interconnect between network transmission devices and directly connect to terminal devices.

6. QOS Settings

[Function Description]

The queue mechanism supported by this industrial switch includes: weighted fair queueing and strict priority scheduling.
The weight fair means that when a port is congested, the port sends the message according to a traffic ratio of 8:4:2:1 of the queue priority High, Medium, Normal, Low. If the port transmission rate is less than the bandwidth, the message in each priority queue can be sent normally; if the port keeps the full transmission rate, the unsent message in each priority queue will be discarded. Strict priority scheduling: it means that the message of the highest priority is processed before the next priority is processed. After the message of the last priority is forwarded, the message in the low priority queue is discarded; but the message in the highest priority has not reached the rate limit of the port , the other lower priority messages are sent in turn, but the data may be lost due to insufficient bandwidth. Ports always allow low priority messages to send only when all high priority queue messages are sent.

The QOS functions of this industrial switch have three ways: port priority, CoS priority, and ToS priority.

6.1 QOS Map Table

[Function Description]

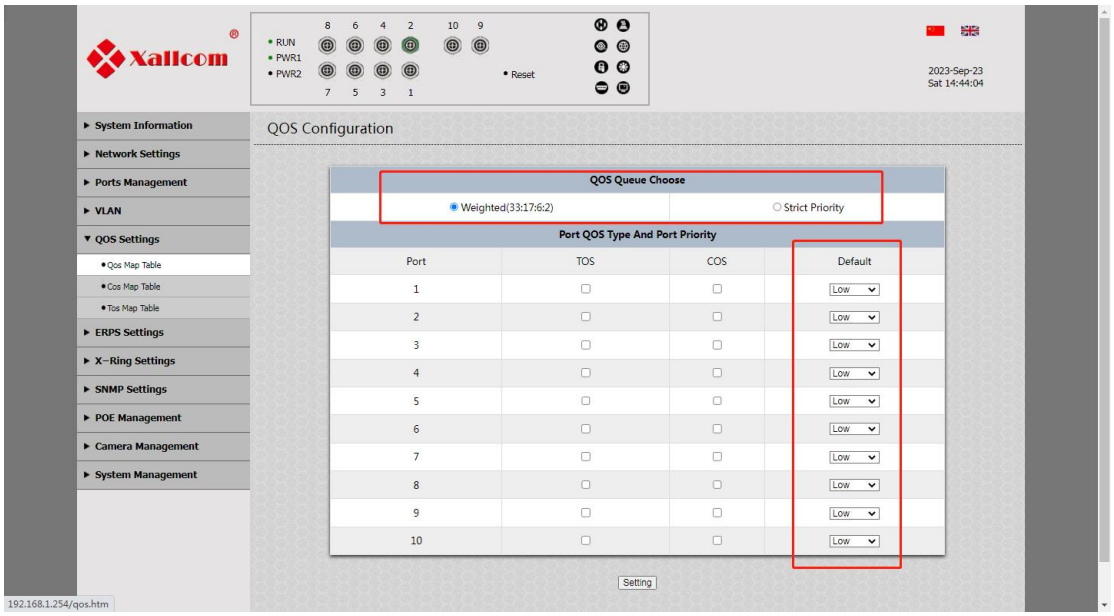
Port priority mainly supports four priority queues, respectively, namely Low, Normal, Medium and High. Generally, the default priority is Low.
When the port priority is used, the port determines what the packet priority is based on the TAG, and the priority is forwarded first if the priority is high, and later if the priority is low. For example, data A and B on two lines must be forwarded from one route. Because the bandwidth is not enough, all priorities can be set according to the ports through the two lines. If data A should be forwarded first, the port of forwarding data A can be set as the higher priority than the port of forwarding data B.

[Operation Path]

QOS Settings> Qos Map Table

[Interface Description]

Figure 6-1 The QOS configuration interface



6.2 COS Map Table

[Function Description]

<CoS-TAG> is the VLAN priority marker for 802.1Q, so CoS priority is related to VLAN tags, and if the port has data packages, the packages need to have COS or VLAN tags. CoS priority assigned eight priority markers with values of 0,1,2,3,4,5,6,7. There are four priority queues available for each priority marker: Low, Normal, Medium, and High. When the forwarding data enters the port, the port will check the CoS value of the data and line up the corresponding data. The data is put into four queues with different priority levels. (The initial priority queues are all: Low). When the packets entering the port have Tag, VLAN is enabled and VLAN-based priority marker substitution is enabled, the packets entering the port are first replaced by VLAN-based priority marker, then CoS priority mapping, and finally forwarded. When the packets entering the port have Tag but are not enabled by VLAN , the packets entering the port directly undergo CoS priority mapping and are eventually forward.

[Operation Path]

QOS Settings> Cos Map Table

[Interface Description]

Figure 6-2-1 QOS Map Table Interface

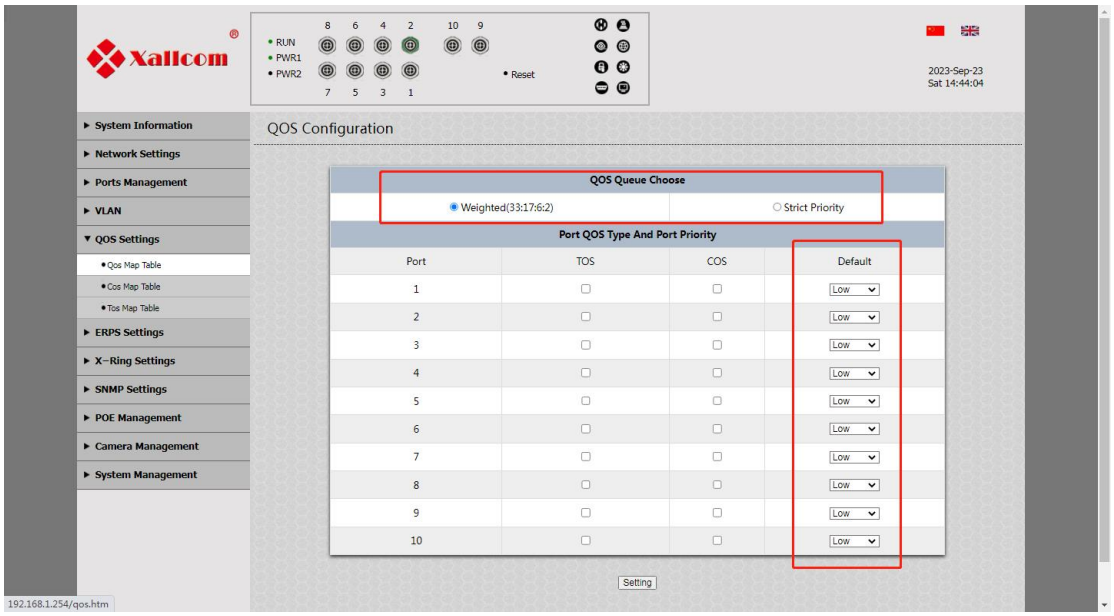
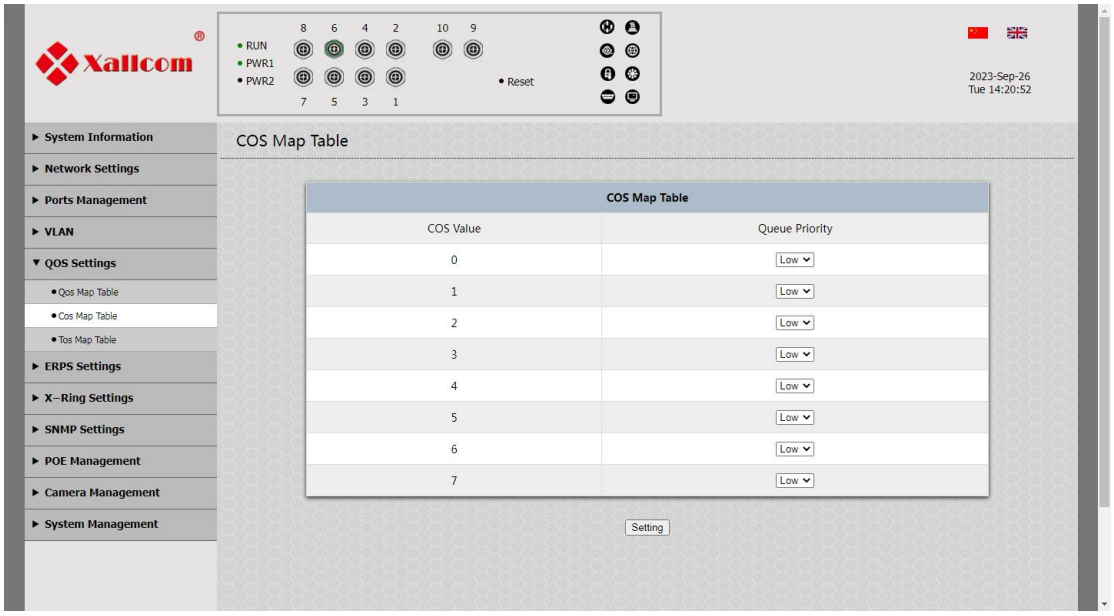


Figure 6-2-2 COS Map Table Interface



First, you need to choose the queuing type in the QOS Map table(Figure 6-2-1), and then tick the port in the selection box of "COS" column. After that, go to COS Map Table to set queue priority.

6.3 TOS Map Table

[Function Description]

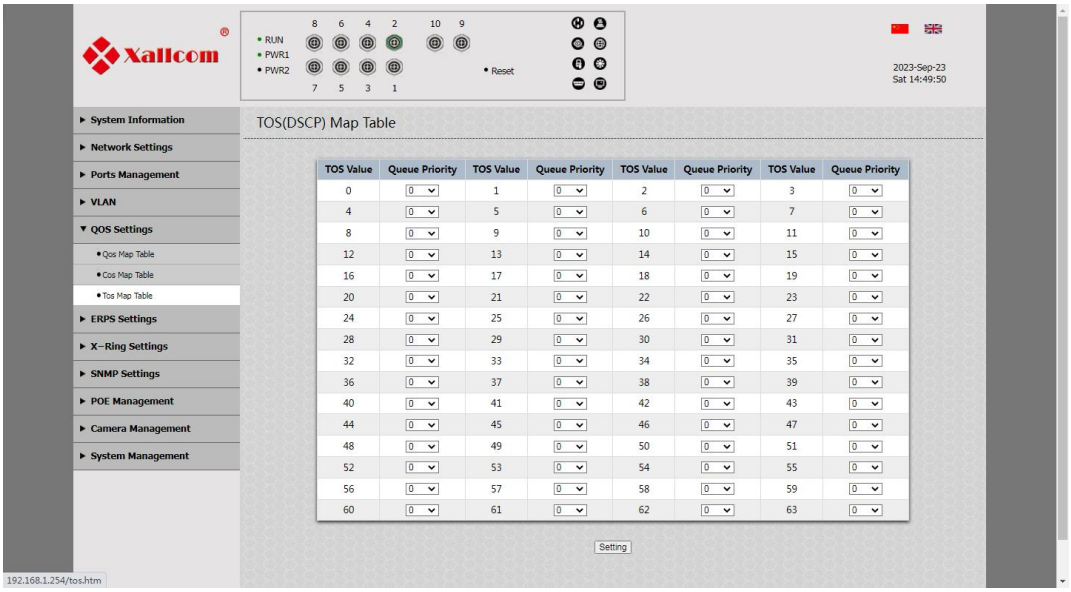
TOS Priority means when sorting the data flow, the prioritization is determined by TOS field of the marked IP header at layer 3. DSCP uses the first 6 bits of ToS (Type Of Service) in the IP header to carry taxonomic information for the message, which defines only low 6 bits valid, a number of no more than 63. This definition supports both IPv4 (ToS field) and IPv6 (Traffic Class field). The DSCP has 64 priority (0-63) values, with 0 having the lowest priority and 63 having the highest priority.

[Operation Path]

QOS Settubgs> TOS Map Table

[Interface Description]

Figure 6-3 TOS Map Table Interface



7. ERPS Settings

[Function Description]

ERPS is a link layer protocol that specifically applies to Ethernet rings and prevents broadcast storms caused by data loop; when one link is disconnected, the backup link is quickly enabled to restore communication between the nodes at the Ethernet Ring. Compared with STP protocol, ERPS protocol has fast topological convergence rate (less than 50ms) and convergence time independent of the number of nodes on the ring network. ERPS ring protection function is similar to STP and MSTP, but ERPS ring protection has no IEEE standard, which belongs to the private protocol. The configuration is simple to use, and the convergence time is also second level. For simple ring network topology and ordinary network services, the advantages in line backup are also obvious.

7.1 ERPS Settings

[Function Description]

From the configuration area, we can configure the ERPS group. The basic principle is: when the network is normal, block a port to prevent the ring, which is called the Ring Protection Link (RPL) port. In case of network failure, opening the RPL port enables data frames to protect the network.

[Operation Path]

ERPS Settings> ERPS settings

[Interface Description]

Figure 7-1 ERPS Setting Interface

- Ring ID: it is an ERPS domain ID. When the ring protection group is added, the ID of the first ERPS group is 1, and the second one is 2, and so on;
- Ring State: select the current ring protection group to open or close the ring protection function.
- Ring Role: it is determined by the user's configuration, divided into the following types:

  a. Owner node: Master node, responsible for blocking and releasing the port on the RPL to prevent the formation of a loop and thus link switching.

  b. Normal Node: Ordinary nodes, all nodes except the two nodes described above are Normal nodes. Normal node is responsible for receiving and forwarding protocol and data messages in the link.
- Ring Port 1: Port 1 of the participating group ring, optional for all ports;
- Ring Port 2: Port 2 of the participating group ring, optional for all ports, and cannot be repeated with the selected port of Ring Port 1;
- RPL Port: ERPS ring is composed of many nodes. Some nodes use RPL (Ring Protection Link) to protect the ring network from the loop. This item sets the blocking port;

- Revertive mode: the Owner node will start the WTR / WTB timer after receiving the NR message after the trouble shooting; Before the timer timeout, if the Owner node does not receive the SF message, change the port status, block the RPL port, clear the MAC address table, send (NR, RB) message, and other nodes release the non-fault blocking port and clear the respective MAC address table. After the timer times out, change back to the initial state;

7.2 ERPS Info

[Function Description]

From this web page you can view the status of the current ERPS ring, the information contained in the ring.

[Operation Path]

ERPS Settings> ERPS Info

[Interface Description]

Figure 7-2 ERPS Information Interface

8. X-Ring Settings

8.1 X-Ring Configuration

[Function Description]

It is very important to have a communication redundancy function in industrial Ethernet networks, and the communication redundancy function allows the redundant rings appearing in the Ethernet to enable backup data links when the

cable is disconnected or damaged. This is an important feature for industrial applications, as taking a long time to locate disconnected or damaged cables can cause huge losses to industrial applications. Support the communication redundancy function. Redundancy types mainly include: single(normal) ring, intersecting(coupling) ring, chain ring and dual homing ring.

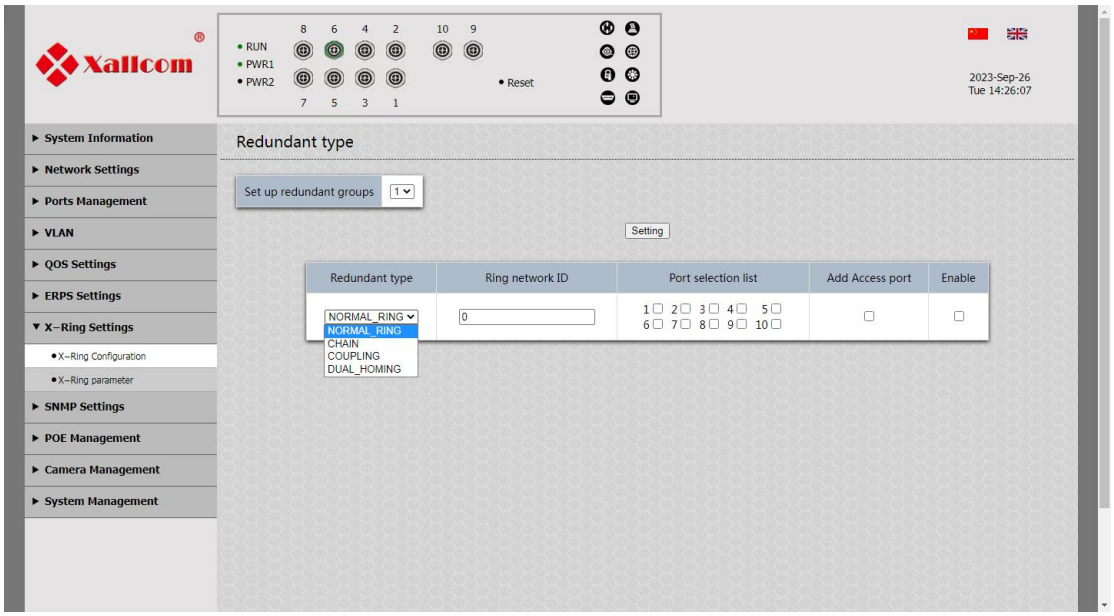
X-Ring ring protection function is similar to ERPS, but ring protection has no IEEE standard, belongs to private protocol, configuration is simple to use, intelligent election method blocking port, short self-healing time, for simple ring network topology and ordinary network services, the advantages in line backup are also obvious.

[Operation Path]

X-Ring Settings> X-Ring Configuration

[Interface Description]

Figure 8-1 X-Ring Configuration Interface



As shown in the figure, on the ring protection page, please click "X-Ring Settings" from the navigation bar first, and then click "X-Ring Configuration". From the configuration area, we can see that the functions mainly include the following parts: redundant type, ring network ID, port selection list, and redundant groups configuration enable.

- Redundancy type(set the redundancy type that requires ring protection): the default is single ring(normal ring); chain, coupling ring, dual-homing ring, and other different ring network protection methods according to the requirements are available.
- Port (display the port number of the device): select the corresponding ring

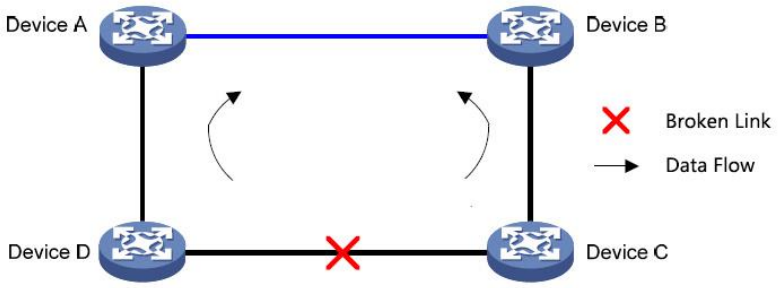
network protection port by checking;

- Enable-check box, selecting the check box means the port ring protection function is turned on, not selecting the check box means the port ring protection function is not enabled;

The following is explained according to the network topology of commonly used industrial ring networks:

① Single Ring

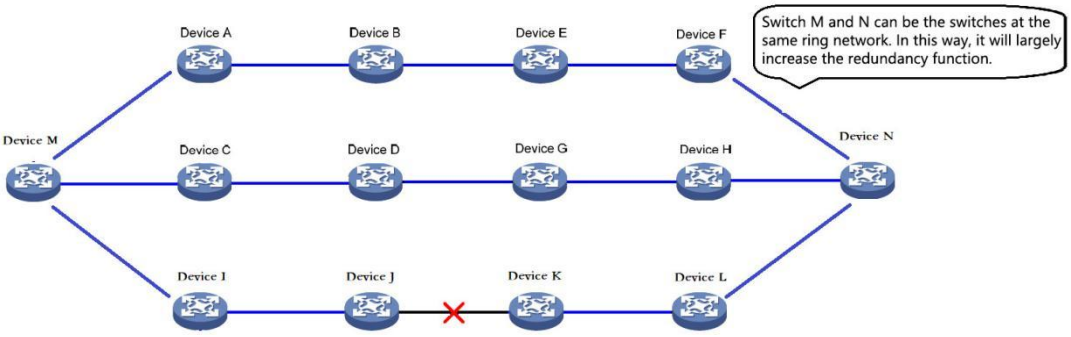
A single ring(normal ring) consists of several switches. Even if there is fiber breakage in the network, the network communication industry will return to normal in a short time. There is no main station structure, and it will not cause abnormal ring network operation causing by abnormal of the main station. As shown in the figure below:



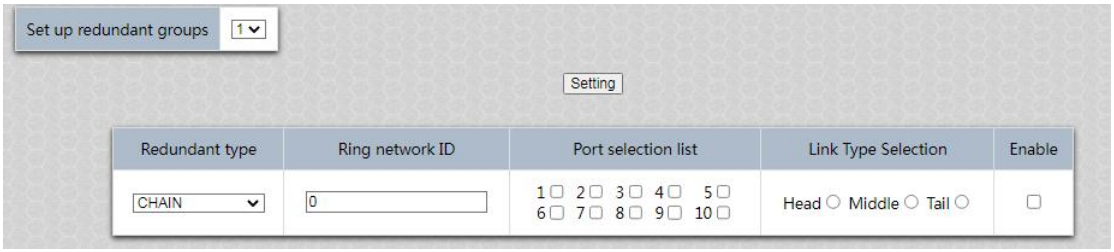
This industrial switch has rich networking capability. If two single rings are set in a switch, it is the tangent ring.

② Chain Ring

The two switches are connected by multiple switches, forming a chain, and several chains between the two switches to form the redundancy of the chain. As shown in the figure below:



The user selects the chain in the redundant type, makes the ring network ID customization, and selects the type of port and chain. According to the position of the industrial switch in the link, it further selects link type: head, middle, and tail. As shown in the figure below, the set is for the switch in middle chain and connected to the chain through port 1 and port 2. The Web Settings interface is shown below:



Once set, view the redundancy parameter table to see the redundancy status that has been set.

③ Intersecting Ring

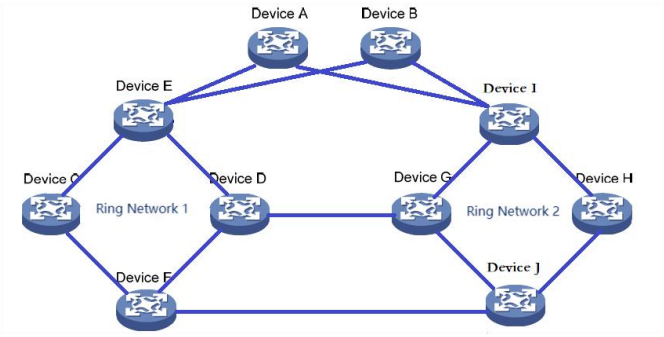
The intersecting ring, also called a coupling ring, is our connection to two existing single-ring networks, forming an intersecting ring. As shown in the figure below:

The user selects the COUPLING ring in the redundancy type, defines the ring network ID, and selects the port. The first problem of setting the intersecting ring is that the switch has a single ring, and then connects the switch to another ring network through a port. Refer to the previous chapter for details. There is only one port available. The Web setup interface is as follows:

Once set, view the redundancy parameter table to see the redundancy status that has been set.

④ Dual Homing Ring

Dual homing refers to the switch Device A and Device B simultaneously connected to multiple ring networks (ring network 1 and ring network 2), which is equivalent to backup. The switch can get data from different ring networks. As shown in the figure below:



The user selects DUAL-HOMMING in the redundant type, selects the port, selects two ports through which they connect to two switches with two rings or one ring, so that this switch can obtain data from two places. The Web Settings are shown below:

Once set, view the redundancy parameter table to see the redundancy status that has been set.

8.2 X-Ring Parameter

[Function Description]

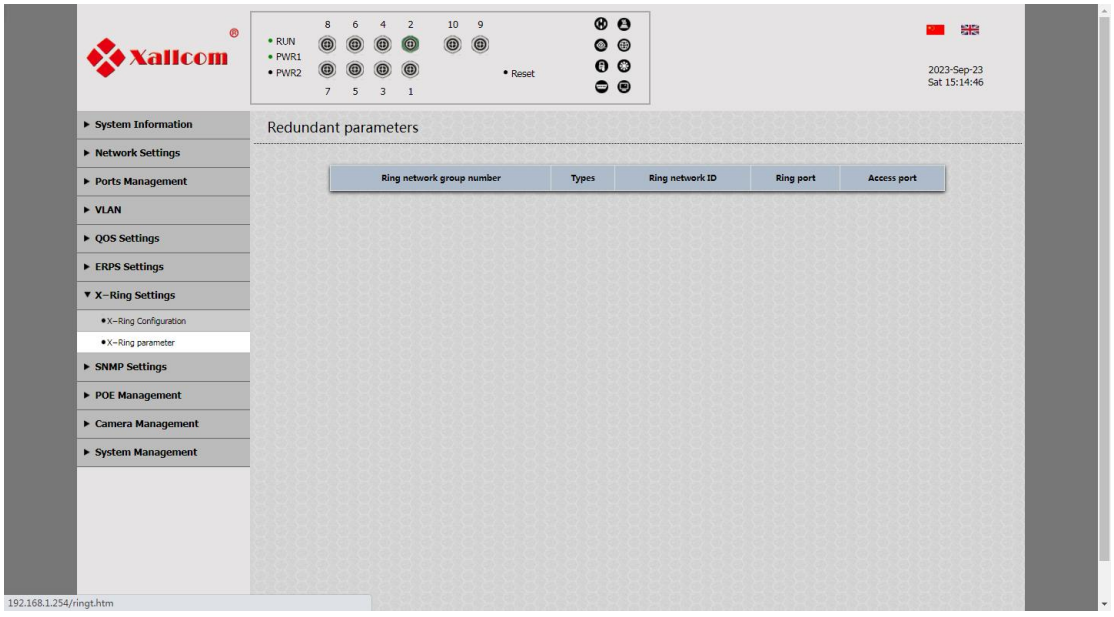
From this web page you can view the status of the current X-Ring, the information contained in the ring.

[Operation Path]

X-Ring Settings> X-Ring parameter

[Interface Description]

Figure 8-2 X-Ring Parameter Interface



9. SNMP Configure

9.1 SNMP Configuration

[Function Description]

SNMP Simple Network Management protocol is part of the TCP / IP protocol family, a framework for network management using UDP, an application level protocol, which provides a set of simple standard operation area collection, modification and exchange network management consultation between network devices to monitor and maintain network devices. The SNMP protocol just solves two major problems of the growing popularity on the Internet:

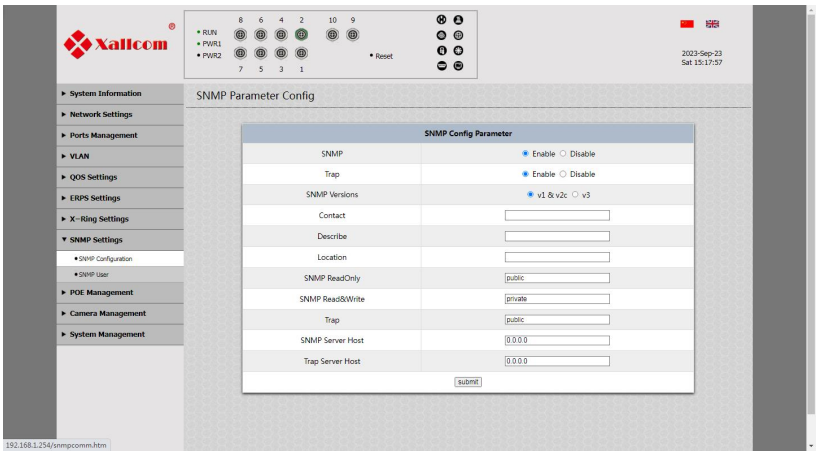
1. The network scale is gradually increasing, plus the number of network devices is increasing exponentially, so it is difficult for network administrators to monitor the status of all devices in time, find and repair faults.
2. Network equipment may come from different vendors. If each vendor provides a set of independent management interfaces (such as the command line), network management will become more and more complicated.

[Operation Path]

SNMP Settings> SNMP Configuration

[Interface Description]

Figure 9-1 SNMP Configuration Interface



Network administrators can use the SNMP function to query device information, modify device parameter values, monitor device status, automatically discover network faults, generate reports, etc. In the above figure, on the SNMP parameter config page, please click "SNMP Settings" first from the navigation bar, and then click "SNMP Configuration". From the configuration area, we can enable the SNMP function and configure the SNMP v1 & v2. Meanwhile, the relevant contact information, system name and device location must be filled in.

9.2 SNMP V3

[Function Description]

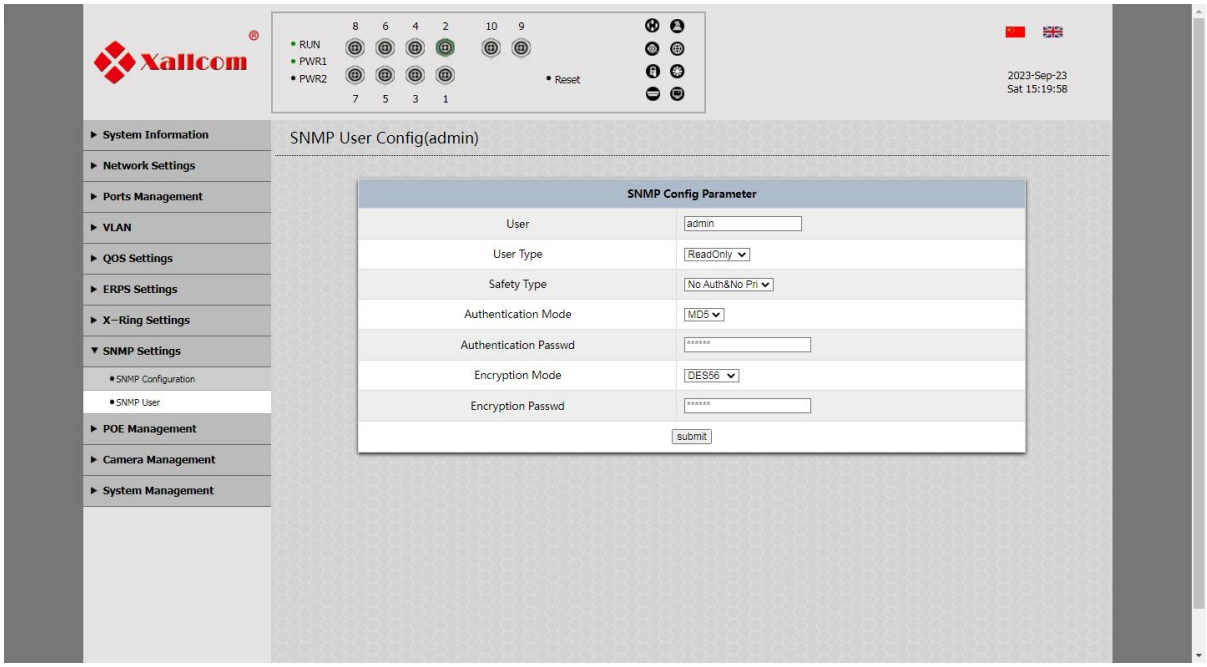
For users using SNMP v3, please set it up as shown in the figure above. First, start the SNMP v3 version function.

[Operation Path]

SNMP Settings> SNMP User

[Interface Description]

Figure 9-2 SNMP v3 Interface



Then, the user name and user type are set in the figure. There are three safety types optional, namely, "No Auth&No Pri" , "No Pri", and "Auth&Pri". The password must be set greater than 8 bits. (“Auth” means authentication, “Pri” means privacy)

10. POE Management

10.1 POE Management

[Function Description]

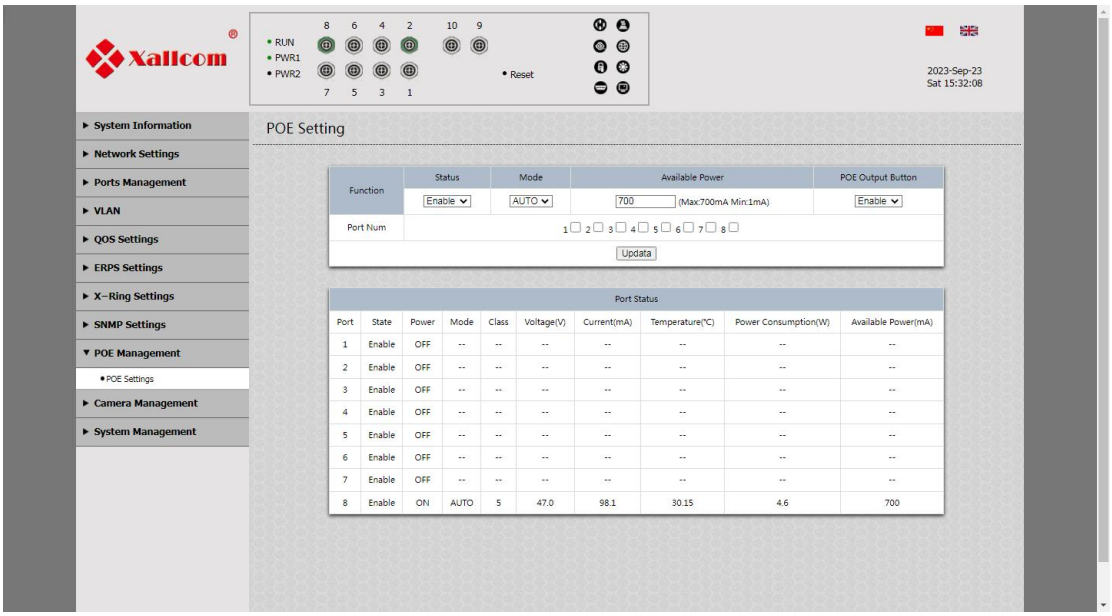
POE (Power Over Ethernet) refers to in the existing Ethernet Cat.5 cabling infrastructure, and without any changes, it can transmit data signals for some terminals based on IP (such as IP phones, wireless LAN access point AP, network cameras, etc.), while also provide DC power supply for such devices.

[Operation Path]

POE Management> POE Settings

[Interface Description]

Figure 10-1 POE Settings Interface



This page is used to configure the POE parameters of each port, including turning off all POE ports through the button(POE Output Button) by remote, and setting the status and mode of each POE port by remote.

POE State: Enable and Disable are optional. The enabled port can normally supply power to the PD device connected to this port. The “Disable” state is to close the power supply to the PD device of that port, and the default is enabled.

POE Mode: optional AUTO, AF or AT. AF mode according to IEEE 802.3af protocol, supplies up to 15.4W for each POE port; AT mode according to IEEE 802.3 at protocol, supplies up to 25.4W (30W) per POE port, which is AUTO by default.

Available Current: allocate the maximum power to the corresponding port according to the selected POE mode. AF mode can provide maximum power 15.4W for the corresponding port, and AT mode can provide maximum power 30W for the corresponding port.

11. Monitor IP-Camera

11.1 Camera Settings

[Function Description]

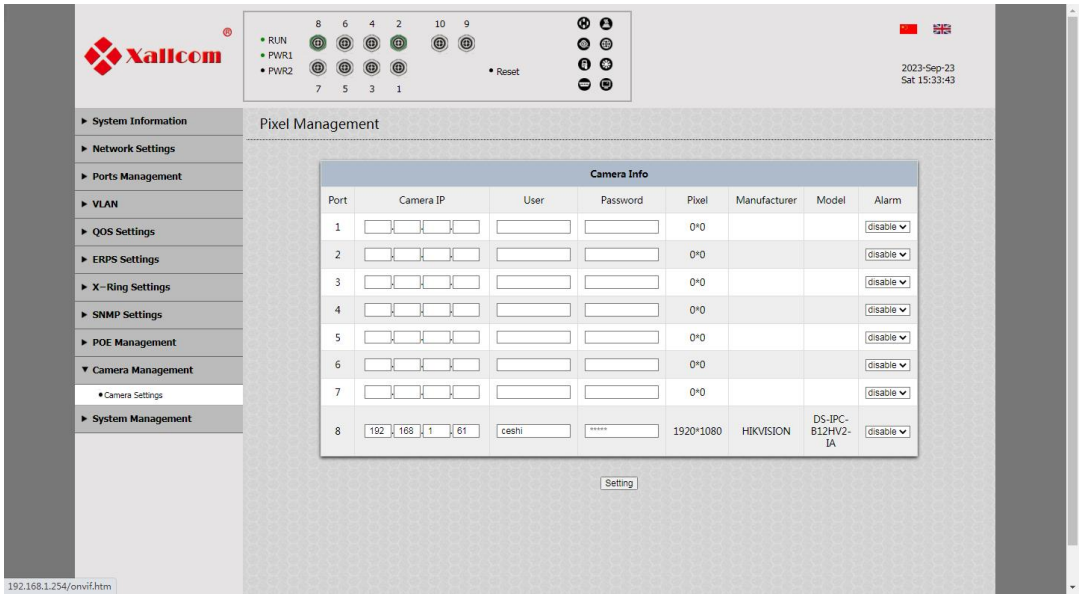
The camera status information of the device, including port, camera IP, pixel, manufacturer, model, etc.

[Operation Path]

Camera Management> Camera Settings

[Interface Description]

Figure 11-1 Camera Settings Interface



When using this function, please note that accurately set the IP of the camera at a space of the port bar corresponding to the camera, and then click the "Setting" button below the functional area. After a moment, the device will automatically search the pixels, manufacturer and model of the corresponding IP camera, and display them in the status bar on the right. If “Alarm” is “enabled”, the device can upload the alarm information generated by the fault of the camera to the background through the network by UDP protocol.

12. System Management

12.1 Alarm Status

[Function Description]

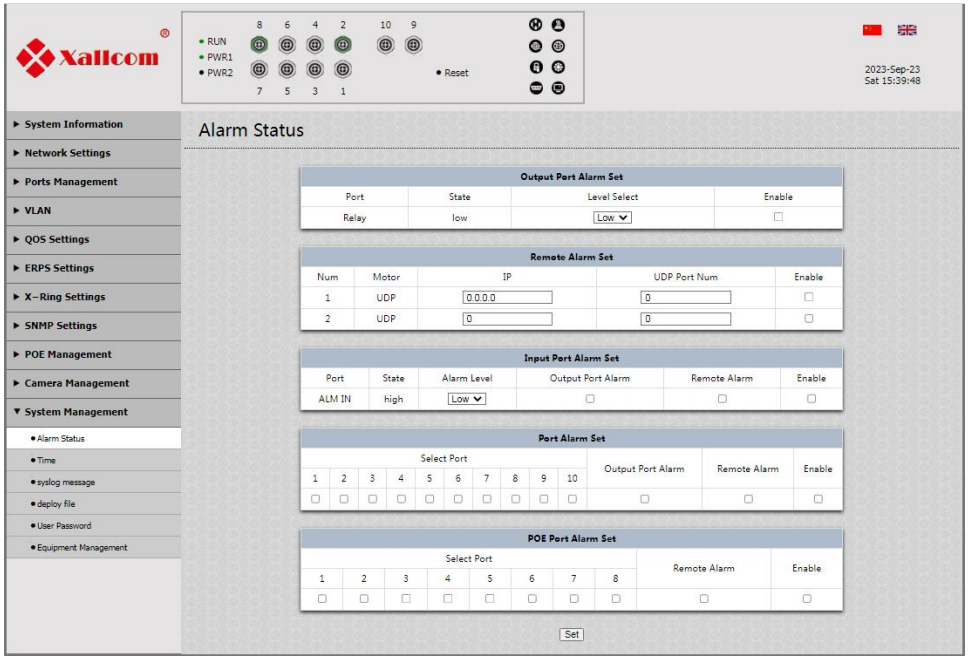
This switch supports remote alarm. When the output terminal, input terminal, port link drops, and PoE port is disconnected, the remote alarm passes through UDP.

[Operation Path]

System Management> Alert Status

[Interface Description]

Figure 12-1 Alarm Status Interface



1. Input Port Alarm Set: the input port status can be seen in column 2, 1 is high level and 0 is low level. In Alarm Level column, you can choose a high level or a low level. Output Port Alarm column indicates whether the input port alarm is output to the output port. The remote alarm column indicates whether to output to the remote server. If Enable ticked, the previous settings will take effect.

Input Port Alarm Set

Port	State	Alarm Level	Output Port Alarm	Remote Alarm	Enable
ALM IN	high	Low	☐	☐	☐

2. Port alarm se: if a port is ticked, an alarm will occur after the port Link Down and sent to the background.

Port Alarm Set

Select Port										Output Port Alarm	Remote Alarm	Enable
1	2	3	4	5	6	7	8	9	10			
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

3. POE Port Alarm Set: if a POE port is ticked , it indicates that the power supply is stopped or the load is off, an alarm will occur and sent to the background.

POE Port Alarm Set

Select Port								Remote Alarm	Enable
1	2	3	4	5	6	7	8		
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

4. Output Port Alarm Set: the level when the alarm output occurs. After “Enable” ticked, it will take effect.

Output Port Alarm Set

Port	State	Level Select	Enable
Relay	low	Low	☐

5. Remote alarm, now only supports UDP alarm, set the IP and port number of the remote computer, and the alarm of the switch will be output to the server.

Remote Alarm Set

Num	Motor	IP	UDP Port Num	Enable
1	UDP	0.0.0.0	0	☐
2	UDP	0	0	☐

12.2 Time and Date

[Function Description]

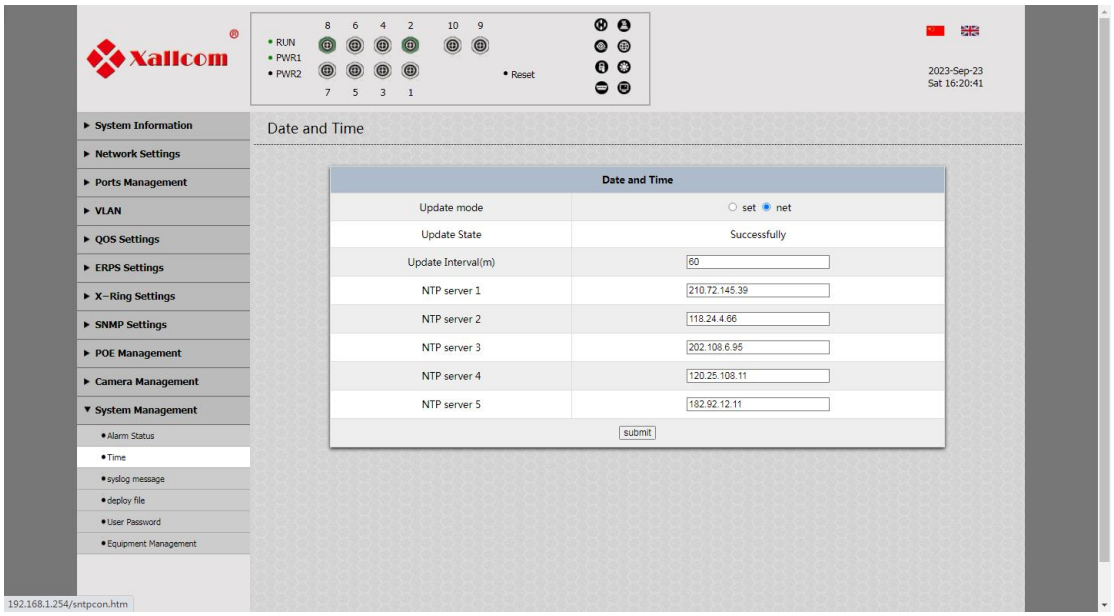
This switch supports SNTP (Simple Network Time Protocol). The SNTP protocol works as a client / server and can be operated in unicast (point-to-point) or broadcast (point-to-multipoint) mode. The SNTP server serves as a time reference for the system by receiving a GPS signal or an internal atomic clock. In unicast mode, SNTP client can obtain accurate time information by regularly accessing SNTP server, which is used to adjust the time of the client's own system to achieve the purpose of synchronization time. In the broadcast mode, the SNTP server periodically sends messages to the specified IP broadcast address or IP multicast address. The SNTP clients acquire the time information by listening on for these addresses.

[Operation Path]

System Management> Time

[Interface Description]

Figure 12-2 Time Interface



12.3 Syslog Message

[Function Description]

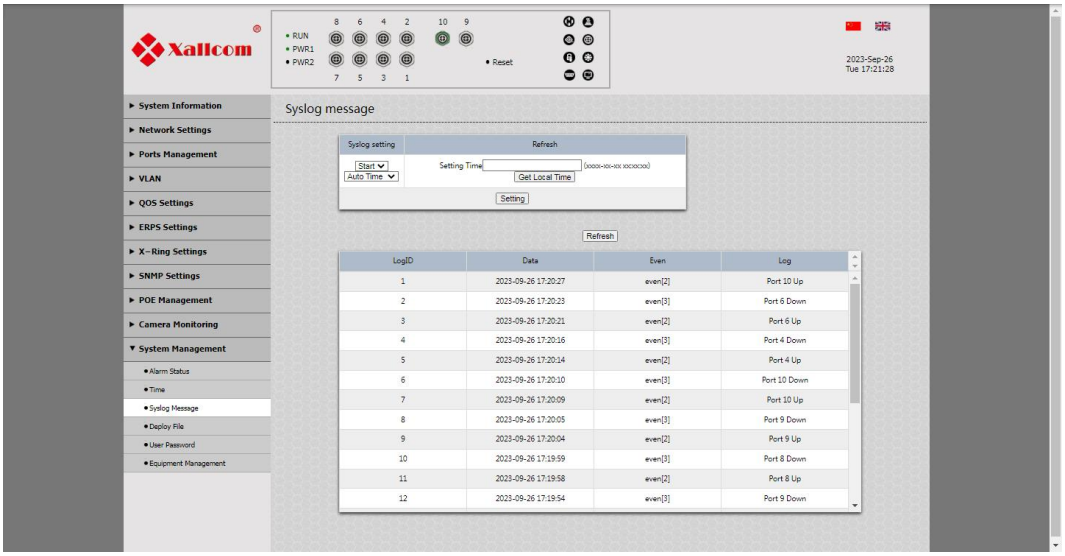
Syslog Message records all the status information of the industrial switch since out of the factory.

[Operation Path]

System Management> Syslog Message

[Interface Description]

Figure 12-3 Syslog Message Interface



As shown in the figure, the syslog message page. You can start or stop(“start” means start recording the log information of the switch, “stop” means stop recording), Auto Time means automatically acquring time, Local Time means acquiring time from local server or PC.

12.4 Deploy File

[Function Description]

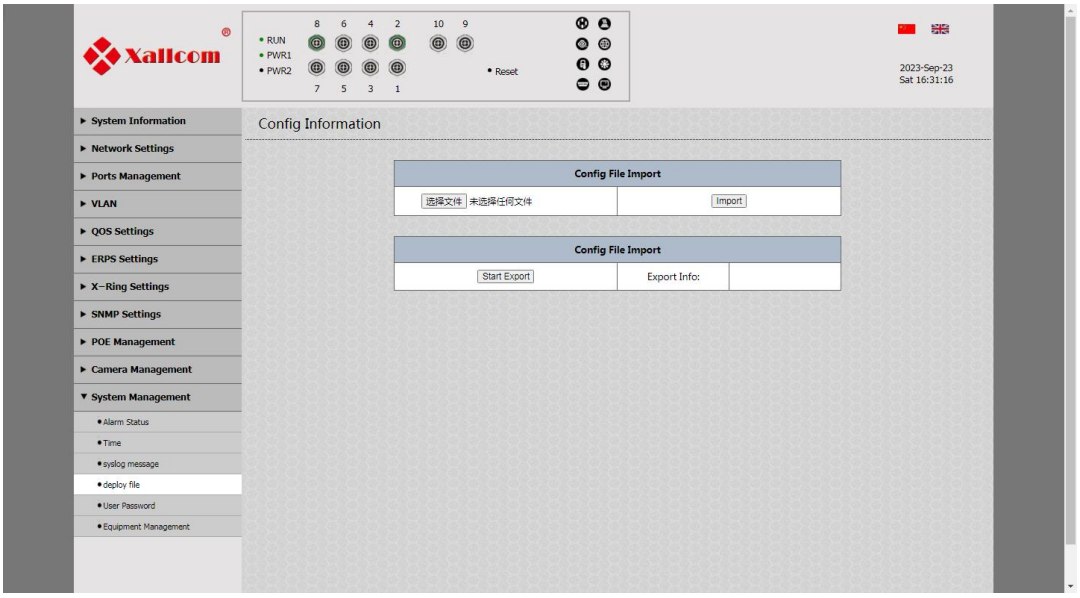
This industrial switch supports the import or export of function profiles for rapid deployment of each switch. After one switch is configured, the file can be exported for other rapid configuration of switches of the same model.

[Operation Path]

System Management> Deploy File

[Interface Description]

Figure 12-4 Deploy File Interface



12.5 User Password

[Function Description]

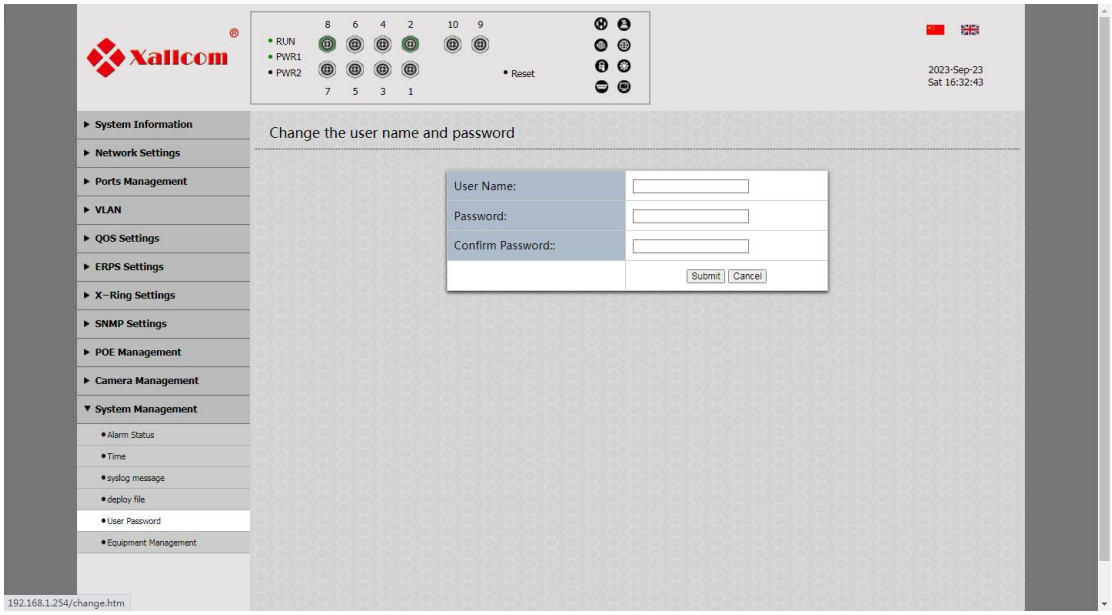
User Password can access the user properties of the switch in WEB interface to protect the switch settings and prevent illegal users from access

[Operation Path]

System Management> User Password

[Interface Description]

Figure 12-5 User Password Interface



From the configuration area, we can modify the information of existing users. We need to enter a new user name in the user name text box. The password and the confirmation password item must be exactly the same to take effect.

12.6 Equipment Management

[Function Description]

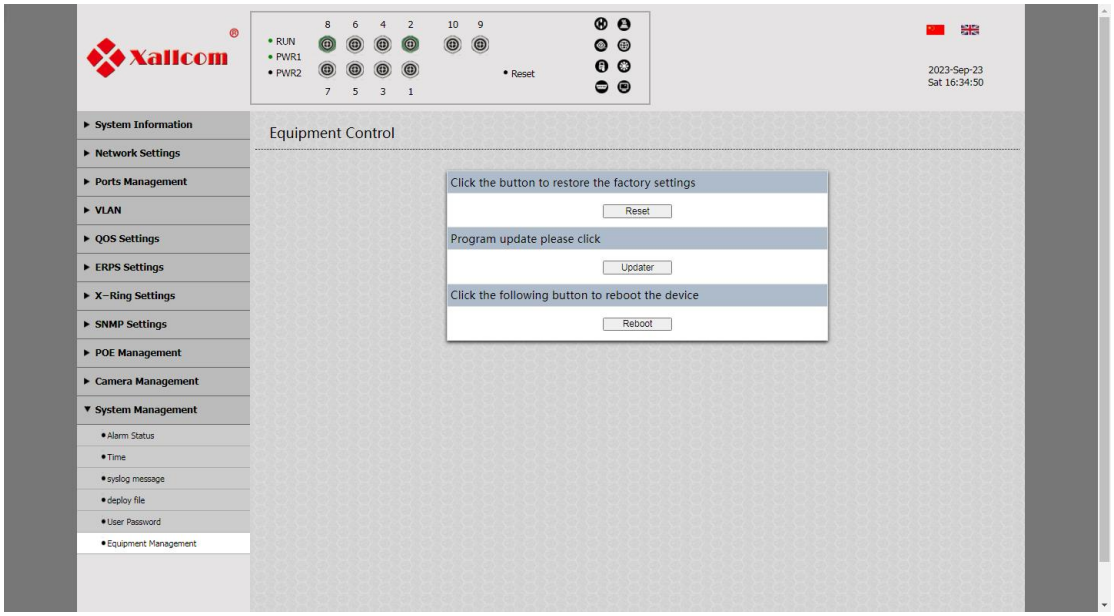
In equipment management, users can update programs, restore factory settings, and restart the equipment.

[Operation Path]

System Management> Equipment Management

[Interface Description]

Figure 12-6 Equipment Management Interface



1. After restoring the factory Settings, the web interface will return to the initial state. The default IP is 192.168.1.254, which users can view and set under the http://192.168.1.254/ web interface.

2.The user click on the updater, web interface will jump right into http://192.168.1.254/upload.htm. In the html interface, the user can update the APP.

3. If the user clicks on the reboot, the device will restart.