MakerLink

Smart-Web PoE Switches

POE-G080GM

Web Manual

Ver. 1.0

Revision history

Date	Version	Description
May. 17, 2022	V 1.0	The first edition

Contents

1 Foreword

1.1 Target Audience

This manual is prepared for the installers and system administrators who are responsible for network installation, configuration and maintenance. It assumes that the user has understood all network communication and management protocols, as well as the technical terms, theoretical principles, practical skills, and expertise of devices, protocols and interfaces related to networking.

1.2 Manual Convention

The following approaches should prevail.

GUI Convention	Description
Interpretation	Describe operations and add necessary information.
⚠ Notice	Remind the user of cautions as improper operations will result in data loss or equipment damage.

2 Web Page Login

2.1 Log in the Network Management Client

Type in the default switch address: http://192.168.2.1 and press "Enter".

📖 Description:

Browser standards: superior to IE 9.0, Chrome 23.0 and Firefox 20.0
Keep the IP network segment of PC consistent with that of switch but differentiate the IP address as you log in. Set PC's IP address of 192.168.2.x and the subnet mask of 255.255.255.0 for the first login (1< x ≤254).

A login window appears as follows. Type in the default username of "**admin**" and the password of "**admin**". Click the "Log in" to see the switch system.
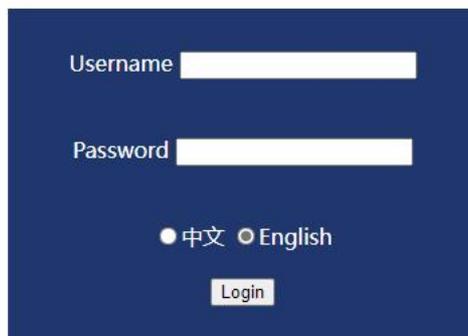
2.2 Constitution of Client Interface

The typical operation interface of Web network management system is as follows.

System Information	
System Model	ZX500-AFGW-82S
MAC Address	11:11:11:11:11:11
IP Address	192.168.2.1
Netmask	255.255.255.0
Gateway	192.168.2.254
Firmware Version	1.0.0
Firmware Date	May 17 2022
Hardware Version	1.0.0
Running Time	0 Days 0 Hours 5 Minutes
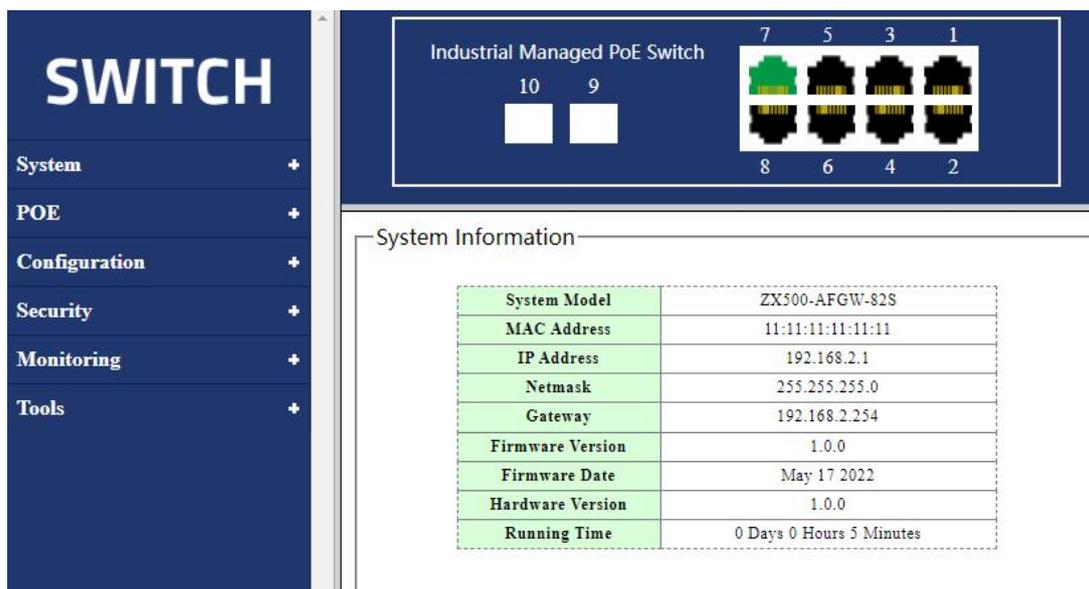
2.3 Navigation Bar on Web Interface

Menu items such as System, Configuration, Security, Monitoring, and Tools are available on the web network management client. Each item contains submenus. Navigation bar is detailed as follows:

Menu Items	Submenus	Secondary Submenus	Description
System	Information		Display the port state and product info
	IP Setting		Configure and view the management IP address
	User Account		Configure and view the management account
	Port Setting		Configure and view all ports
PSE	System		Configure and view the current equipment system power and consumption
	Port		Configure and view device PSE port information
Configuration	VLAN	Static VLAN	Configure and view the VLAN
		VLAN Setting	Configure and view the PVID of port
	QOS	Priority selection	Configure and view the priority selection setting
		Dscp remapping	Configure and view the DSCP mapping setting
		Priority to Queue	Configure and view the priority to queue setting
		Port—based Priority	Configure and view the priority of port
		Queue Weight	Configure and view the queue weight
	IGMP		Configure and view the igmp snooping
	Trunk Group Setting		Configure and view the trunk groups
	Loop Prevention		Configure and view the Loop setting
	RSTP global		Configure viewing RSTP global information
	RSTP port		Configure and view RSTP port information
	Port—based Mirroring		Configure and view the port mirror
	Port Isolation		Configure and view the port isolation
	Bandwidth Control		Configure and view the port rate—limit
	Jumbo Frame		Configure and view the length of the max message forwarded by system
	MAC Constraint		Configure and view the MAC limit
	Green Ethernet		Configure and view the green Ethernet setting

	EEE		Configure and view the EEE state and information
	SNMP		Configure and view SNMP information
Security	MAC Address	MAC Table	Configure and view the dynamic MAC addresses and aging time of the device
		MAC Search	Search MAC address
		Static MAC	Configure and view the static MAC address
	Storm Control		Configure and view the port storm policing
Monitoring	Port Statistics		Display the port statistics
	Cable Diagnostic		Electrical interface link diagnostics by VCT
Tools	Firmware Upgrade		Update software
	Configuration Backup		Update and save configuration files
	Reset		Restore factory settings
	Save		Save configuration
	Reboot		Restart system

3 System

3.1 Information

Display system information, including model, version, MAC, etc.
Instructions:
1. Click the "System > Information" in the navigation bar as follows:

3.2 IP Setting

Change the management IP address on web interface

1. Click the "System > IP Setting" in the navigation bar as follows：

Interface data are as follows.

Query Items	Description
DHCP Setting	Enable：Enable DHCP client in system Disable：Disable DHCP client
IP Address	Manager IP address
Subnet Mask	Manager IP mask
Gateway	Manager IP default gateway

3.3 User Account

Users can check and modify the current username and password of the switch.
Instructions：

1．Click the "System ＞ User Account" in the navigation bar as follows：

Interface data are as follows.

Query Items	Description
New Username	New Username
New Password	New Password
Retry Password	Enter the new user name again

3.4 Port Setting

Querying and configuring Ethernet ports.

Instructions：

1．Click the "System ＞ Port Setting" in the navigation bar as follows：

Port Setting

Port	Name	State	Speed/Duplex	Flow Control
Port 1 Port 2 Port 3 Port 4 Port 5 Port 6		Enable ⌄	Auto ⌄	Off ⌄

Apply

Port	Name	State	Speed/Duplex	Flow Control
port 9 port 10		Enable ⌄	Auto ⌄	Off ⌄

Apply

Port	Name	State	Speed/Duplex		Flow Control	
			Config	Actual	Config	Actual
Port 1		Enabled	Auto	Link Down	Off	Off
Port 2		Enabled	Auto	Link Down	Off	Off
Port 3		Enabled	Auto	Link Down	Off	Off
Port 4		Enabled	Auto	Link Down	Off	Off
Port 5		Enabled	Auto	Link Down	Off	Off
Port 6		Enabled	Auto	Link Down	Off	Off
Port 7		Enabled	Auto	1000Full	Off	Off
Port 8		Enabled	Auto	Link Down	Off	Off
port 9		Enabled	Auto	Link Down	Off	Off
port 10		Enabled	Auto	Link Down	Off	Off

Interface data are as follows.

Query Items	Description
Name	Port description
State	Enable or disable port
Speed/Duplex	Configure the rate and negotiation status of the port. You can configure the forced 10M/Half, 10M/Full, 100M/Half and 100M/Full
Flow Control	After it is enabled on both local network and opposite network devices, the local one will notify the other to stop transmitting messages in the presence of network congestion. The opposite one will execute

	the command temporarily to ensure zero message loss.
	Off—Disabled reception and transmission of PAUSE frame;
	On—Enabled reception and transmission of PAUSE frame;

4 PSE

4.1 System

Poe refers to a technology that transmits power through network cable. With the help of existing Ethernet, Poe can simultaneously transmit data and supply power to IP terminal equipment (such as IP phone, AP, IP camera, etc.).

Configure and view the power and consumption of the PSE of the device.

Operation steps:

1. Click the "System >PSE> System" in the navigation bar as follows:
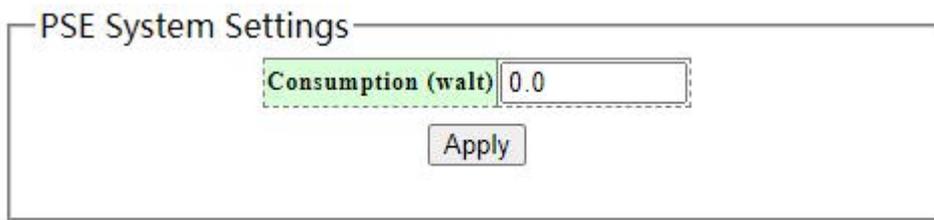
Interface data are as follows.

Query Items	Description
Consumption	Display power consumption

4.2 port

Configure and view the port PSE of the device.

Operation steps:

1. Click the "System >pse> port" in the navigation bar as follows:

PSE Port Settings

Port	State
Port 1	
Port 2	
Port 3	Disable
Port 4	
Port 5	
Port 6	

Apply

Port	State	Power On/Off	Type	Power(w)	Voltage(v)	Current(ma)
Port 1	Enable	Off	-	-	-	-
Port 2	Enable	Off	-	-	-	-
Port 3	Enable	Off	-	-	-	-
Port 4	Enable	Off	-	-	-	-
Port 5	Enable	Off	-	-	-	-
Port 6	Enable	Off	-	-	-	-
Port 7	Enable	Off	-	-	-	-

Interface data are as follows.

Query Items	Description
State	Port switch

5 Configuration

5.1 VLAN

VLAN is formulated not restricted to physical locations, which means the hosts in a same VLAN can be placed at will. As shown below, each VLAN, as a broadcast domain, divides a physical LAN into logical LANs. Hosts can exchange messages by means of traditional communication. For the hosts in different VLANs, the device such as router or L3 switch is a must.
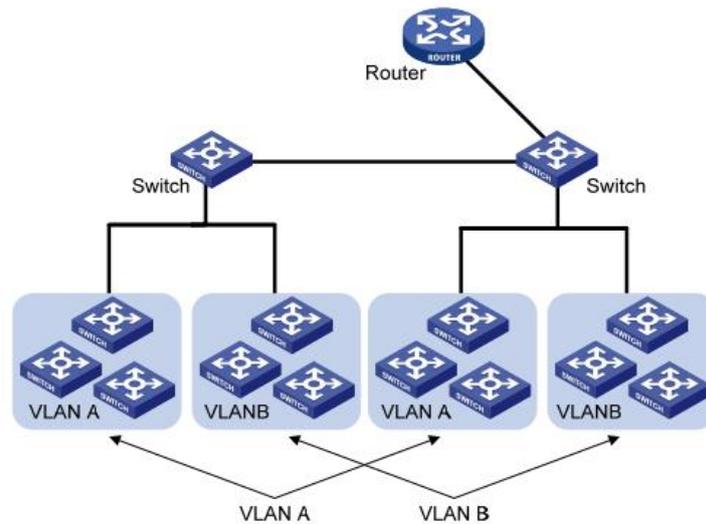
VLAN is superior to the traditional Ethernet in terms of:

- Broadcast domain coverage: the broadcast message in a LAN is limited in a VLAN to save the bandwidth and handle the network-related issues more efficiently.
- LAN security: VLAN hosts fail to communicate with each other since the messages are separated by the broadcast domain in the data link layer. They need a router or a Layer 3 switch for Layer 3 forwarding.
- Flexibility of creating a virtual working team: VLAN can create a virtual working team beyond the control of physical network. Users have access to the network without changing the configuration if their physical locations are moving within the scope. This management switch is compatible with VLAN types based on 802.1Q, protocols, MAC, and ports. For default configuration, 802.1Q VLAN mode should be adopted. Port VLAN is divided subject to a switch's interface No. Network administrator gives each switch interface a different PVID, namely a port default VLAN. If a data frame without a VLAN tag flows into a switch interface with a PVID, it will be marked with the same PVID, or it will get rid of an additional tag even though the interface has a PVID.
- The solution to a VLAN frame depends on the interface type, which eases member definition but re-configures VLAN in case of member mobility.

5.1.1 Static VLAN

1. Click the "Configuration > VLAN > Static VLAN", in the navigation bar as follows:

Interface data are as follows

Configuration Items	Description
VLAN ID	It is required to select an ID ranging from 1 to 4,094
VLAN Name	It is optional to modify the VLAN description as required.

⚠️Note：

● VLAN 1 is the system default VLAN and does not support deletion

5.1.2 VLAN Setting

1. Click the "Configuration ＞ VLAN ＞ VLAN Setting", in the navigation bar as follows：

VLAN Port Setting

Port	PVID	Accepted Frame Type
Port 1 Port 2 Port 3 Port 4 Port 5 Port 6		All ▾

Apply

Port	PVID	Accepted Frame Type
Port 1	1	All
Port 2	1	All
Port 3	1	All
Port 4	1	All
Port 5	1	All
Port 6	1	All
Port 7	1	All
Port 8	1	All
port 9	1	All
port 10	1	All

Interface data are as follows

Configuration Items	Description
PVID	Set the port PVID
Accepted Frame Type	Set the port receive frame type

5.2 QOS

QoS (Quality of Service) assesses the ability of service providers to meet customer needs and the ability of transmitting packets over the Internet. Diversified services can be assessed based on different aspects. QoS usually refers to the evaluation of service capabilities that support core requirements such as bandwidth, delay, delay variation, and packet loss rate during delivery. Bandwidth, also known as throughput, refers to the average business flow within a certain period of time, with the unit of Kbit/s. Delay refers to the average time required for business flowing through the network. For a network device, the followings are general levels of delay requirements. There are two delay levels, that is, the high-priority business can be served as soon as possible by scheduling method of priority queue, while

16

the low—priority business gets services after that. Delay variation refers to the time change of business flowing through the network. Packet loss rate refers to the percentage of lost business flow during transmission. As modern transmission systems are very reliable, information is often lost in network congestion. Packet loss due to queue overflow is the most common situation.

All messages in a traditional IP network are treated equally. Every network device processes the messages on a FIFO basis, and makes every effort to transmit them to destinations without guaranteeing reliability, transfer delay, or other performance.

Network service quality is constantly improved as new applications keep springing up in the rapidly changing IP network. For example, VoIP, video and other delay—sensitive services have set higher standards on message transmission delay. Message transmission in a short period has been the common trend. In order to support voice, video and data services with different requirements, the network needs to identify business types and provide corresponding services.

The ability to distinguish business types is the prerequisite to provide corresponding services, so the traditional best—effort service no longer meets the application needs. Therefore, QoS comes into being. It regulates the network flow to avoid and handle network congestion and reduce packet loss rate. Meanwhile, users can enjoy dedicated bandwidths while business can improve service quality, thus perfecting the network service capacity.

QoS priorities vary with message types. For instance, the VLAN message uses 802.1p, also known as the CoS (Class of Service) field, while the IP message uses DSCP. To maintain the priority, these fields need to be mapped at the gateway connected with various networks when messages flow through the network.

802.1p priority in the VLAN frame header

Typically, VLAN frames are interacted between Layer 2 devices. The PRI field (i.e. 802.1p priority), or CoS field, in the VLAN frame header identifies the quality of service requirements according to the definitions in IEEE 802.1Q.

802.1p priority in the VLAN frame
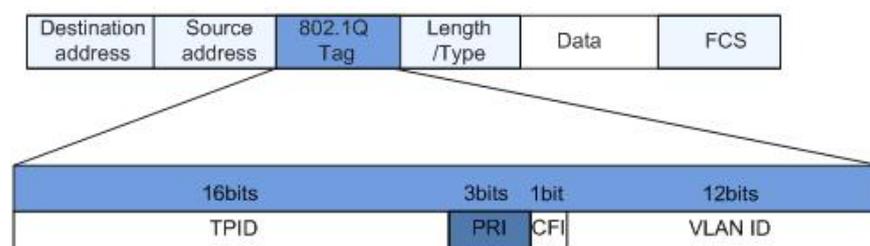
The 802.1Q header contains 3—bit PRI fields. PRI field defines 8 CoS of business priority ranging from 7 to 0 from high to low.

IP Precedence/DSCP Field

According to RFC791 definition, ToS (Type of Service) domain in the IP message header is composed of 8 bits. Among them, the 3—bit long Precedence field, as located in the following, identifies the IP message priority.

IP Precedence/DSCP Field
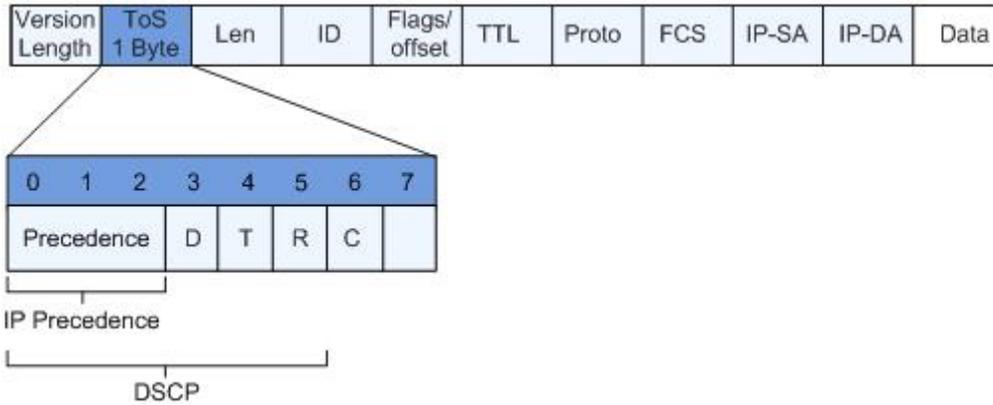
0 to 2 bits are Precedence fields representing the 8 priorities of message transmission ranging from 7 to 0 from high to low, with either Level 7 or 6 as the highest priority that is generally reserved for routing or updating network control communication. User—level applications only have access to Level 0 to 5.

ToS domain, in addition to Precedence fields, also includes D, T and R bits: D—bit represents the Delay requirement (0 for normal delay and 1 for low delay). T—bit represents the throughput (0 for normal throughput and 1 for high throughput). R—bit represents the reliability (0 for normal reliability and 1 for high reliability). ToS domain reserves the 6 and 7 bits.

RFC1349 redefines the ToS domain by adding a C—bit to represent the Monetary Cost. The IETF DiffServ group then redefines the 0 to 5 bits of ToS domain in the IPv4 message header of RFC2474 as DSCP and renames it as DS (Differentiated Service) byte as shown in the figure above.

The first 6 bits (0—5 bits) of DS field distinguish the DSCP (DS Code Point), and the higher 2 bits (6—7 bits) are reserved. The lower 3 bits (0—2 bits) are CSCP (Class Selector Code Point), with the same CSCP value representing the DSCP of the same class. DS nodes select corresponding PHB (Per—Hop Behavior) according to DSCP values.

5.2.1 Priority selection

Set processing priority for different tags of data frames
1. Click the "Configuration > QOS > Priority selection", in the navigation bar as follows:

Interface data are as follows

Configuration Items	Description
Priority	Tag type of data frame
Decision	Processing weight priority

5.2.2 Dscp remapping

1. Click the "Configuration > QOS > Dscp remapping", in the navigation bar as follows:

Interface data are as follows.

Configuration Items	Description
DSCP	Value of IP DHCP
Priority	Value of IP DHCP domain priority

5.2.3 Priority to Queue

1. Click the "Configuration > QOS > Priority to Queue", in the navigation bar as follows：

Interface data are as follows.

Configuration Items	Description
Priority	Priority value
Queue ID	The queue value of port

5.2.4 Port-based Priority

1. Click the "Configuration > QOS > Port-based Priority", in the navigation bar as follows：

Interface data are as follows.

Configuration Items	Description
Priority	The priority of port

5.2.5 Queue Weight

1. Click the "Configuration > QOS > Queue Weight", in the navigation bar as follows:

Interface data are as follows.

Configuration Items	Description
Priority Queue	The queue of port
Weight	The weight mode of port, SP or WRR

5.3 IGMP

IGMP Snooping (Internet Group Management Protocol Snooping) is a constraint mechanism on L2 devices to manage and control multicast groups.

By analyzing the IGMP messages received, L2 devices establish a mapping between ports and MAC multicast addresses and forward the multicast data accordingly.

As shown below, multicast data are transmitted on L2 without IGMP snooping. When IGMP snooping runs, known multicast group data are transmitted to specified receivers while unknown multicast data are still on Layer 2.
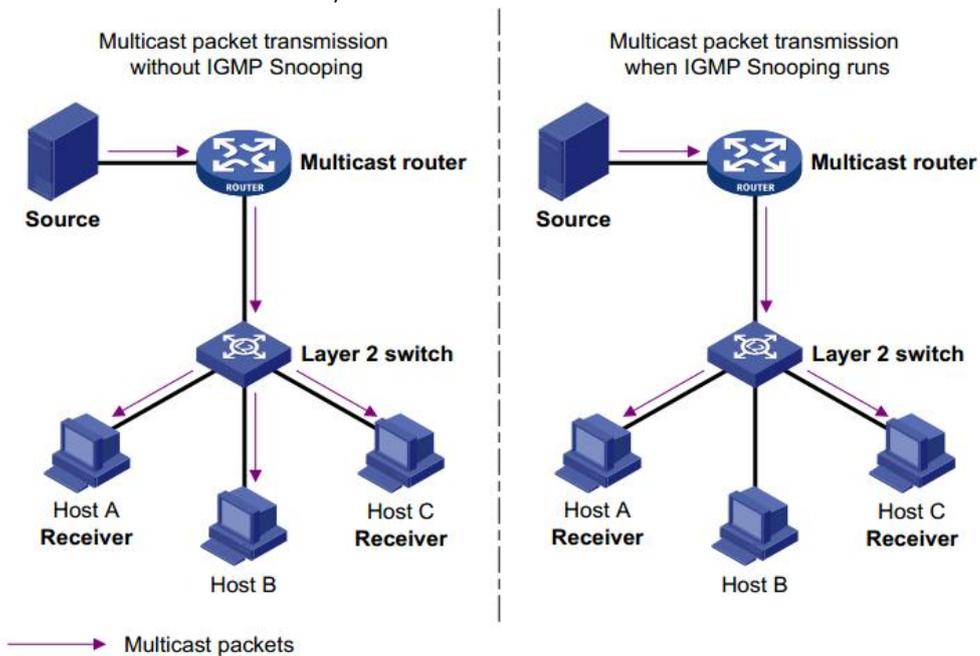
Instructions:

1. Click the "Configuration > IGMP", in the navigation bar as follows:

Interface data are as follows.

| Configuration Items	Description
Enable	Enable or disable the IGMP Snooping
Dump IGMP entry	Display multicast group entries

5.4 Trunk Group Setting

Link Aggregation broadens bandwidth and reliability by bundling a group of physical interfaces into a single logical interface.
LAG (Link Aggregation Group) is a logical link bundled by multiple Ethernet links (Eth-Trunk).

Ceaselessly expanding network size increases users' demands of link bandwidth and reliability. Traditionally, high-speed interface board or the compatible equipment is usually replaced to optimize bandwidth, which is expensive and inflexible.
Link Aggregation Technology bundles multiple physical interfaces into a single logical interface without upgrading hardware. Its backup mechanism not only improves reliability, but also shares the flow load on different physical links.

As shown below, Switch A is linked with Switch B through three Ethernet links which are bundled into an Eth-Trunk logical link. Its bandwidth equals to that of the three links in total, thus broadening the bandwidth. Meanwhile, these three links back up mutually to be more reliable.
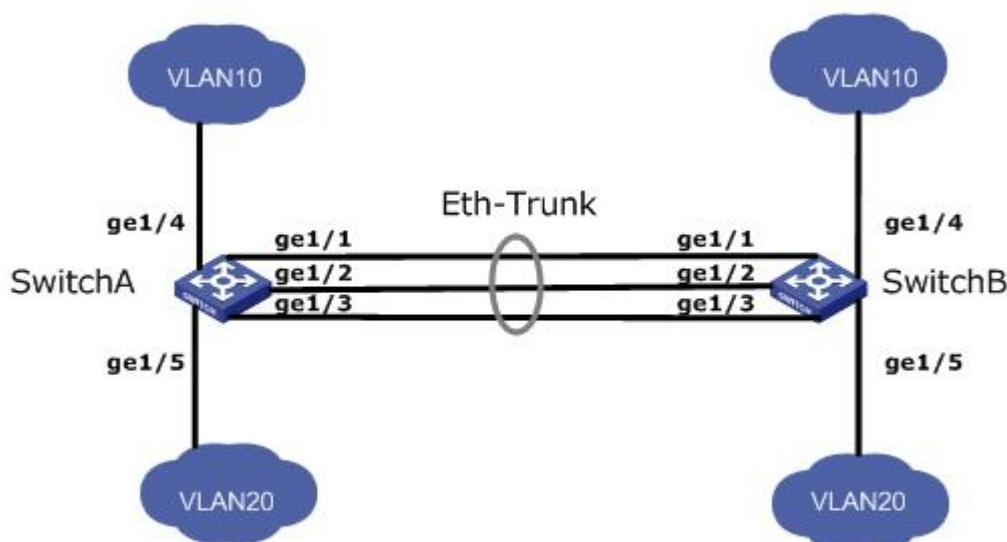
Instructions:

1. Click the "Configuration > Trunk Group Setting", in the navigation bar as follows：

Interface data are as follows

Configuration Items	Description
Group ID	There are 2 LAGs numbering from 1 to 2.
Ports	Up to 4 member ports are available in LAG.

⚠Note：

● The first four ports and the last four ports do not support forming an aggregation group

5.5 Loop Prevention

Loop Prevention is configured as follows：it enables the global ring network and disables the configuration of switch ports so that users can modify the inspection intervals and the port shutdown time. It configures the loops of one or more ports and determines whether to adopt auto inspection mode or not under the circumstance of enabling the global ring network. Instructions：

1. Click the "Configuration > Loop Prevention", in the navigation bar as follows：

Interface data are as follows.

Configuration Items	Description
Loop function	Enable of disable Loop prevention. Loop Prevention: check the loop port and block the port while the LED flashes Loop Detection: check the loop port. When the loop network occurs, the LED of the port flashes
Time Interval	Inspection interval
Recover Time	Recovery interval

5.6 RSTP global

Fast spanning tree protocol (RSTP) is used to eliminate the physical loop of data link layer in LAN. Its core is fast spanning tree algorithm. RSTP is fully downward compatible with STP protocol. In addition to the functions of avoiding loops and dynamically managing redundant links like the traditional STP protocol, RSTP greatly shortens the topology convergence time. Under the ideal network topology scale, all switching devices support RSTP protocol, and when configured properly, the time to restore stability after topology changes (link up ╱ down) can be controlled at the second level. The main functions of RSTP can be summarized as follows:

1、 Discover and generate an optimal tree topology of LAN;

2、Discover and recover the topology failure, automatically update the network topology, enable the backup link, and maintain the best tree structure;

Instructions:

1. Click the "Configuration >RSTP global", in the navigation bar as follows:

Spanning Tree Setting

Spanning Tree Status	Disabled	
Force Version	RSTP	
Priority	32768	
Maximum Age	20	(6~40 Sec)
Hello Time	2	(1~10 Sec)
Forward Delay	15	(4~30 Sec)
Root Priority	32768	
Root MAC Address	00:23:79:00:23:79	
Root Path Cost	0	
Root Port	None	
Root Maximum Age	20 Sec	
Root Hello Time	2 Sec	
Root Forward Delay	15 Sec	

Apply

Interface data are as follows.

Configuration Items	Description
Force Version	Configure view STP mode
Maximum Age	Configure view maximum age time
Hello Time	Configure view Hello time
Forward Delay	Configure and view forwarding delay time

5.7 RSTP port

Instructions：

1. Click the "Configuration >RSTP port", in the navigation bar as follows：

Interface data are as follows.

Configuration Items	Description
Path Cost	Configure view port path Cost
Priority	Configure view port priority
P2P	Configure and view P2P
Edge	Configure view edge ports

5.8 Port-based Mirroring

Port Mirroring copies the message of a specified switch port to the destination port. The copied port is the Source Port, and the copying port is the Destination Port. Destination Port accesses to data inspection devices so that users can analyze the messages received to monitor network and troubleshoot as follows：
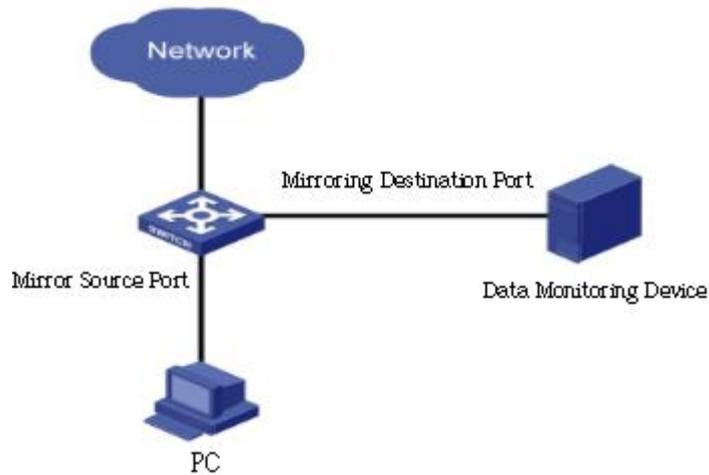
Instructions：
1. Click the "Configuration ＞ Port-based Mirroring", in the navigation bar as follows：

Interface data are as follows

Configuration Items	Description
Mirror Direction	Enable or disable port mirroring, support Rx, Tx, and Both
Mirroring Port	Only one ordinary physical port can be selected, excluding link aggregation port and source port.
Mirrored Port List	List of mirrored source ports

5.9 Port Isolation

Messages of broadcast, multicast, etc. will flood at each port even though the flow needs no mutual communication sometimes. Under this circumstance, port isolation can separate the messages between two ports.
Instructions：
1. Click the "Configuration ＞ Port Isolation", in the navigation bar as follows：

Interface data are as follows

Configuration Items	Description
Port	Port list
Port Isolation List	Establish the member list of interworking group

5.10 Bandwidth Control

It refers to the rate restriction on transmitting and receiving data at physical interfaces.

Restrict the rate limiting at the egress before transmitting flow, thus controlling all outgoing message flow;

Restrict the rate limiting at the ingress before receiving flow, thus controlling all incoming message flow;

Instructions:

1. Click the "Configuration > Bandwidth Control", in the navigation bar as follows:

Interface data are as follows

Configuration Items	Description
Type	Ingress: inbound port direction Degree: direction of outgoing port
State	Enable or de enable port restrictions
Rate	Rate limit, range: 8 to 1000000 kbps

5.11 Jumbo Frame

Set the MTU (Maximum Transmission Unit) of the port

Instructions:

1. Click the "Configuration >Jumbo Frame", in the navigation bar as follows:

Interface data are as follows

Configuration Items	Description
Jumbo Frame	Set the MTU of the port

5.12 MAC Constraint

MAC address learning limit of port

Instructions：

1. Click the "Configuration ＞ MAC Constraint", in the navigation bar as follows：

Interface data are as follows.

Configuration Items	Description
Learn over Action	Action triggered after MAC learning number exceeds threshold
State	Enable or disable MAC constraint
Entry Limits	Limited number of MAC address learning

5.13 Green Ethernet

1．Click the "Configuration ＞ Green Ethernet"，in the navigation bar as follows：

Green Ethernet Setting

| Green Ethernet | Disable ∨ |

Apply

5.14 EEE

1．Click the "Configuration ＞ EEE"，in the navigation bar as follows：

EEE Setting

| EEE function | Disable ∨ |

Apply

5.15 SNMP

SNMP simple network management protocol is a standard protocol specially designed to manage network nodes (servers，workstations，routers，switches and hubs) in IP network．It is an application layer protocol．Instructions：

1．Click the "Configuration ＞ SNMP"，in the navigation bar as follows：

SNMP设置

SNMP函数	关闭 ∨
Trap IP地址	192.168.2.254
读共享	public
写共享	private

应用

Interface data are as follows.

Configuration Items	Description
SNMP function	Enable or disable SNMP function
Trap IP Address	Network management node IP
Read Community	Download and view node configuration information password
Write Community	Upload and execute node configuration command password

6 Security

6.1 MAC Address

Ethernet switches are mainly innovated to forward according to the purposes in the data link layer. That is, MAC address will transmit the messages to corresponding ports according to the purposes. MAC address forwarding table is a L2 table illustrating MAC addresses and forwarding ports, which is the basis of fast forwarding of L2 messages.

MAC address forwarding table contains following data:

- Destination MAC Address
- VLAN ID belonging to port
- Forwarding ingress No. of this device

There are two message forwarding types according to MAC address table info:

- Unicast mode: the switch directly transmits the messages from the table's egress when MAC address forwarding table contains corresponding entries with the destination MAC address.
- Broadcast mode: When the switch receives the messages with the destination address full of F—bits, or there is no entry corresponding to the MAC destination address in the forwarding table, the switch will forward the messages to all ports excluding the receiving port in this way.

6.1.1 MAC Table

MAC address table needs constant updates to cater to network changes. It automatically generates entries that are limited by their lifetime (i.e. aging time). Those entries not refreshed after expiration will be deleted. The aging time of an entry will be recalculated if its record is refreshed before expiration.

Proper aging time helps to achieve the aging target of MAC address. Shortage of aging time may lead many switches broadcast to discover the packets of destination MAC addresses, thus influencing the switch performance.

Aging too long can cause the switch to save outdated MAC address entries, thus exhausting the forwarding resources and failing to update the forwarding table based on network changes.

The switch may remove valid MAC address table entries due to too short aging time, thus reducing forwarding efficiency. In general, the aging time recommended is 300 seconds by default.

Instructions for aging time setting:

1. Click the "Security > MAC Address > MAC Table", in the navigation bar as follows:

6.1.2 MAC Search

1. Click the "Security > MAC Address > MAC Search", in the navigation bar as follows:

Interface data are as follows.

Configuration Items	Description
MAC Address	MAC address for search
VLAN	VLAN of MAC address

6.1.3 Static MAC

　　Static table is manually configured by users and distributed to each interface board, which won't age.

Instructions:

1. Click the "Security > MAC Address > Static MAC", in the navigation bar as follows:

Interface data are as follows.

Configuration Items	Description
MAC Address	Enter the new MAC address e.g.: HH:HH:HH:HH:HH:HH
VLAN ID	Specify the VLAN ID
Port	Select the interface type and enter the port list
Source MAC Blocking	Enable or disable MAC address filtering

6.2 Storm Control

Storms generated via broadcast, unknown multicast and unicast messages are prevented as follows. These messages will be suppressed subject to packet rates respectively. The average rate of the messages received by monitoring interfaces will be compared with the max threshold configured during an inspection interval. Configured storm policing will be performed at this interface if the average rate exceeds the max threshold.

When a L2 Ethernet interface receives the broadcast, unknown multicast or unicast messages, the device will forward them to other L2 interfaces in a same VLAN (Virtual Local Area Network) if the egress interface cannot be recognized according to destination MAC addresses. As a result, broadcast storm may occur to degrade device operation performance.

Three kinds of message flow can be controlled by storm policing characteristics to stay away from broadcast storms.

Instructions：

1. Click the "Security ＞ Storm Control", in the navigation bar as follows：

Interface data are as follows.

Configuration Items	Description
Storm Type	The storm type, like Broadcast, Multicast, Unicast
Port	Port list
State	Enable or disable storm control
Rate	Rate ranges from 8 to 1,000,000 Kbps

7 Monitoring

7.1 Port Statistics

Display port statistics information.

Instructions:

1. Click the "Monitoring > Port Statistics", in the navigation bar as follows:

Interface data are as follows.

Configuration Items	Description
Port	Port list
State	Switch status of the port
Link Status	Link status of the port
TxGoodPkt	Send normal packet statistics
TxBadPkt	Send bad packet statistics
RxGoodPkt	Received normal packet statistics
RxBadPkt	Received bad packet statistics

7.2 Cable Diagnostic

Copper diagnostic evaluates the ingress cable state and locates the faults (about 5 m by error) according to the reflected voltage strength

Instructions:

1. Click the "Monitoring > Port Statistics", in the navigation bar as follows:

8 Tool

8.1 Firmware Upgrade

System version firmware upgrade

Instructions：

1. Click the "Tool ＞ Firmware Upgrade", in the navigation bar as follows：

2. Click the "System ＞ HTTP Firmware Upgrade", in the navigation bar as follows：

8.2 Configuration Backup

System configuration upgrade or backup

Instructions

1．Click the "Tool ＞ Configuration Backup", in the navigation bar as follows：

Interface data are as follows.

Configuration Items	Description
Backup	Backup configuration
Upload	Upload configuration

8.3 Reset

Restore factory settings

Instructions

1．Click the "Tool ＞ Reset", in the navigation bar as follows：

8.4 Save

Instructions

1．Click the "Tool ＞ Save", in the navigation bar as follows：

8.5 Reboot

Restart the system.

Instructions

1. Click the "Tool ＞ Reboot", in the navigation bar as follows：

Reboot

Reboot the switch.

Reboot