Smart-Web Switch

SL-SWTGW218AS

Tech Support: Sodola-Networking@outlook.com

Web Manual

Ver. 1.0

Revision history

Date	Version	Description
Aug. 3, 2024	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

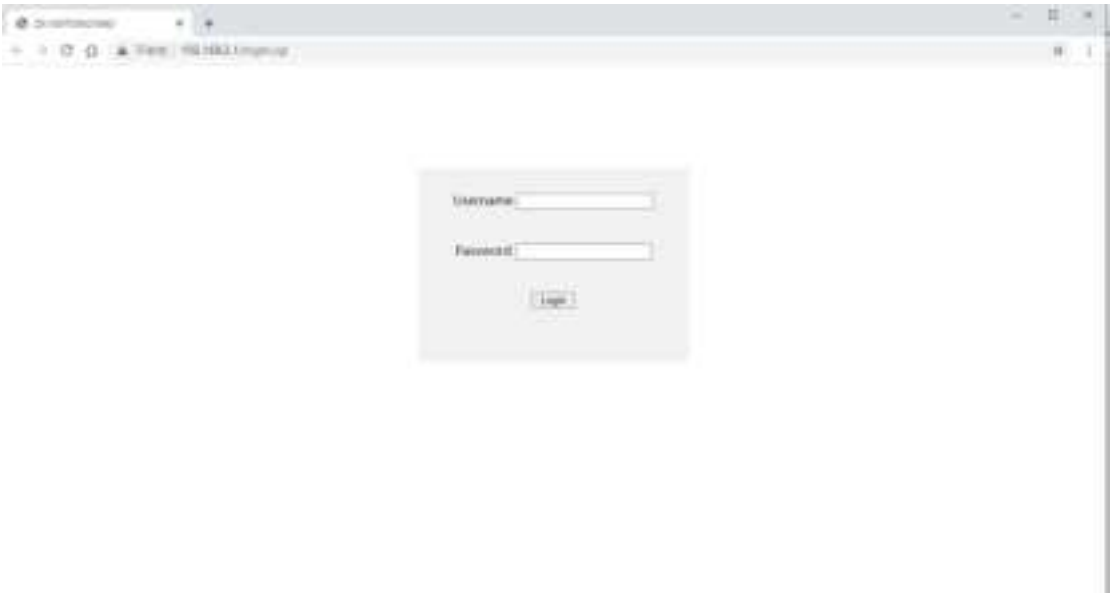
Type in the default switch address: **http://192.168.2.1** and press "Enter".

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.

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
Configuration	VLAN	802.1Q VLAN	Configure and view the VLAN
		802.1Q VID	Configure and view the PVID of port
	QOS	Port to Queue	Configure and view the Port to Queue
		Queue Weight	Configure and view Queue Weight
	Loop	Loop Protocol	Configure and view Loop Protocol
		STP global	Configure and view STP global
		STP port	Configure and view STP port
	IGMP Snooping		Configure viewing IGMP Snooping information
	Trunk Group Setting	static	Configure and view Trunk Group Setting information
		LACP	Configure and view LACP Group Setting
	Port-based Mirroring		Configure and view the Port-based Mirroring
	Port Isolation		Configure and view the Port Isolation
	Bandwidth Control		Configure and view the Bandwidth Contro
	Jumbo Frame		Configure and view the Jumbo Frame
	MAC Constraint		Configure and view MAC Constraint
	EEE		Configure and view EEE
Security	MAC Address	MAC Search	Display the mac address table
		Static MAC	Configure and view Static

			MAC
	Storm Control		Configure and view Storm Control
Monitoring	Port Statistics		Display Port Data Statistics
Tools	Firmware Upgrade		Save configuration
	Configuration Backup		Save and Restore Configuration
	Reset		Factory reset
	Save		Save Configuration
	Reboot		Restart system
	Logout		Exit the system

3 System

3.1 Information

Display system information, including model, version, MAC, etc.

Instructions:

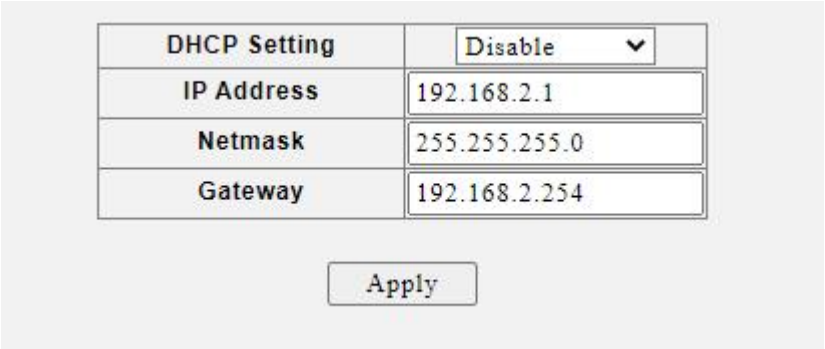
1. Click the “System > Information” in the navigation bar as follows:

Device Model	ZX-SWTGW218AS
MAC Address	1C:2A:A3:1A:9B:B5
IP Address	192.168.2.1
Netmask	255.255.255.0
Gateway	192.168.2.254
Firmware Version	V1.9
Firmware Date	Jan 03 2024
Hardware Version	V1.1

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
Netmask	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.

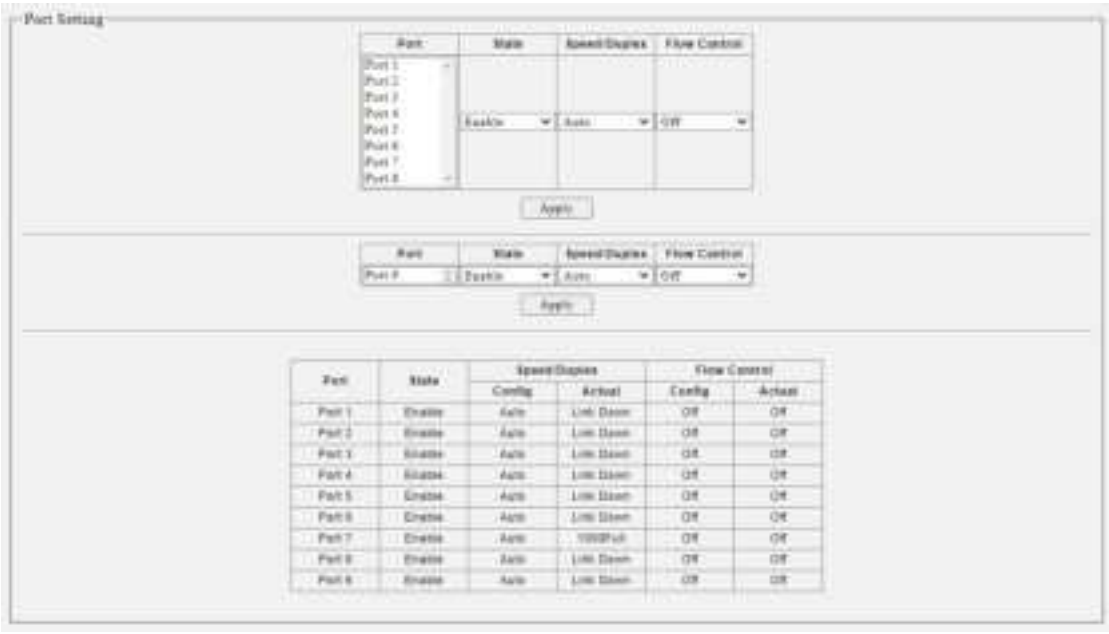
Query Items	Description
New Username	New Username
New Password	New Password
Confirm Password	Enter the new user name again

3.4 Port Setting

Querying and configuring Ethernet ports.

Instructions:

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



Interface data are as follows.

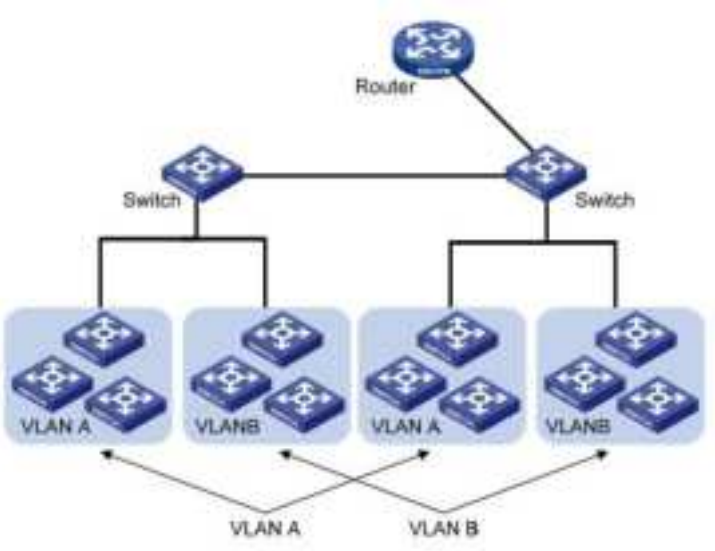
Query Items	Description
State	Enable or disable port
Speed/Duplex	Configure the rate and negotiation status of the port. You can configure the forced 10M/Half, 10M/Full, 100M/Half,100M/Full 1000M/Full , 2500M/Full
Flow Control	After it is enabled on both local network and opposite network devices, the 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 Configuration

4.1 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.

4.1.1 802.1Q VLAN

1. Click the "Configuration > VLAN > 802.1Q 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

4.1.2 802.1Q VID

1. Click the “Configuration > VLAN >802.1Q VID”, in the navigation bar as follows:

Interface data are as follows

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

4.2 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 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.

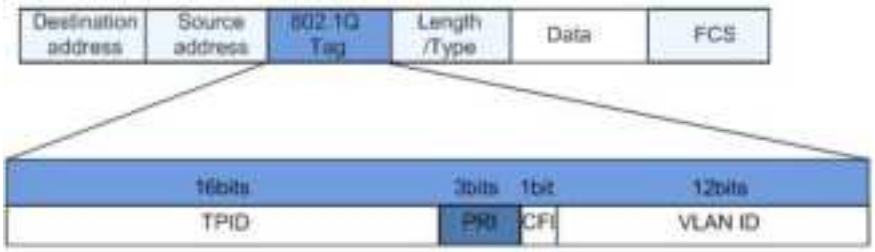
The ability to distinguish business types is the prerequisite to provide corresponding services, so the traditional best-effort service no longer meets the application needs. Therefore, QoS comes into being. It regulates the network flow to avoid and handle network congestion and reduce packet loss rate. 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

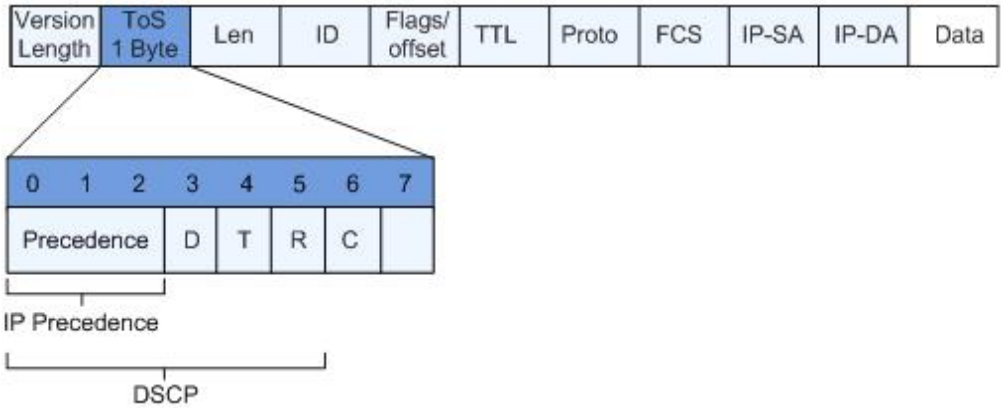


The 802.1Q header contains 3-bit PRI fields. PRI field defines 8 CoS of business priority ranging from 7 to 0 from high to low.

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.

4.2.1 Port to Queue

Sets processing priorities for different tags of the data frame

1. Click the “Configuration > QOS > Port to Queue”, in the navigation bar as follows:

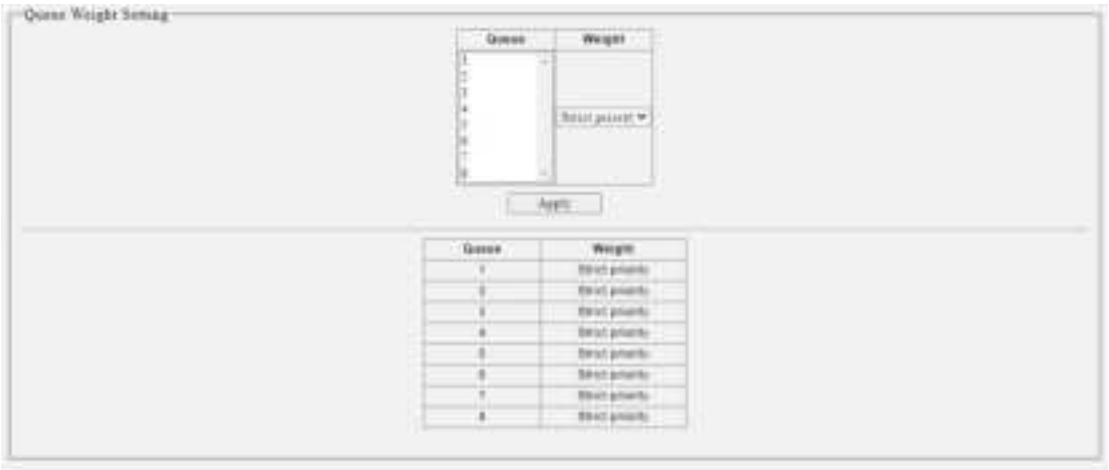
Interface data are as follows

Configuration Items	Description
Queue	1-8

4.2.2 Queue Weight

When the weight is strict priority, it is equivalent to SP, and when the weight is 1-15, it is equivalent to WRR (weighted cyclic Scheduling algorithm).

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



Interface data are as follows.

Configuration Items	Description
Weight	The default value is strict priority. The weight ranges from 1 to 15

4.3 Loop

4.3.1 Loop detection/loop prevention

The device sends loop detection packets and checks whether the packets are returned to the device (the receiving and sending interfaces are not required to be the same) to check whether loops exist. If a port receives a loop detection packet from the local device, it is determined that the link to which the port resides has a loop. When a loop occurs on the network, the LED of the corresponding port blinks (blocking the loop when loop avoidance is enabled) to alert the network administrator that a loop exists on the port

Instructions:

1. Click the “Configuration >Loop> Loop Protocol”, in the navigation bar as follows:

Interface data are as follows.

Configuration Items	Description
Loop Protocol	off, loop detection, loop Prevention, Spanning tree

4.3.2 STP 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>Loop >STP global”, in the navigation bar as follows:

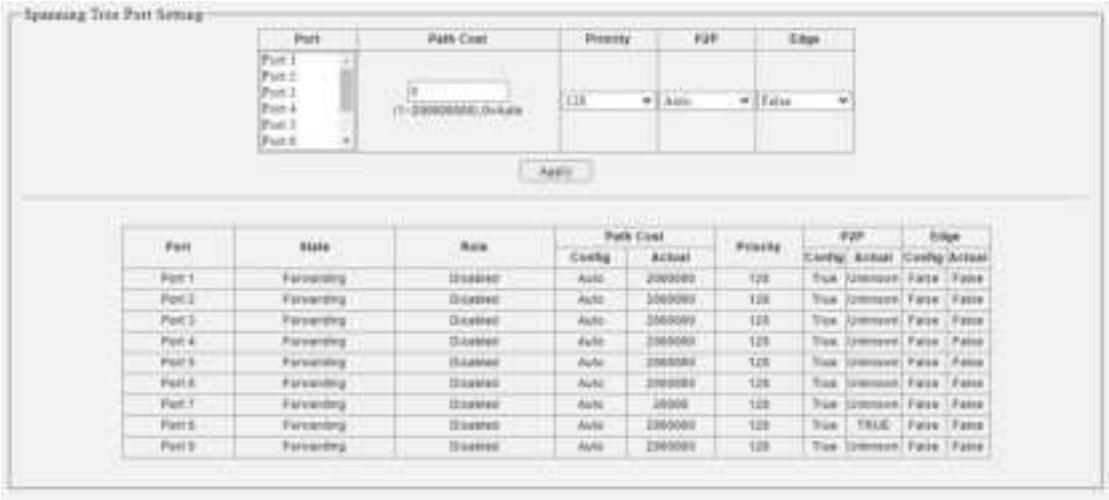
Interface data are as follows.

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

4.3.3 STP port

Instructions:

1. Click the “Configuration >Loop>STP port”, in the navigation bar as follows:



Interface data are as follows.

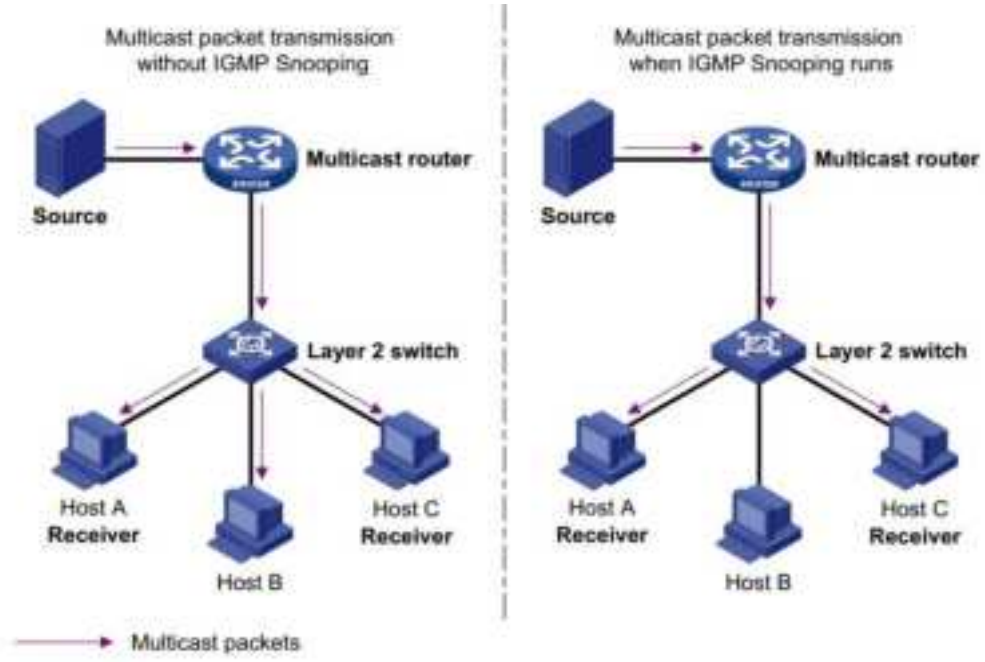
Configuration Items	Description
Path Cost	Configure view port path Cost
Priority	Configure view port priority
P2P	Configure and view P2P
Edge	Configure view edge ports

4.4 IGMP Snooping

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

4.5 Trunk Group Setting

4.5.1 static

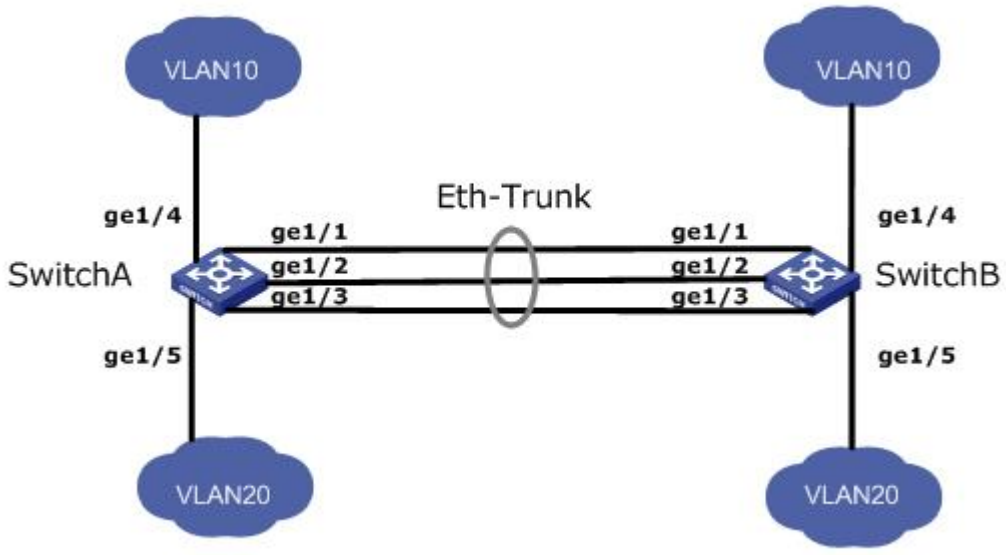
Link Aggregation broadens bandwidth and reliability by bundling a group of physical interfaces into a single logical interface.

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.



When there are the following requirements, link aggregation can be configured to achieve:

- When the bandwidth between two switch devices connected through a link is

insufficient.

- When the reliability of connecting two switch devices through a link does not meet the requirements.

Link aggregation is divided into static mode and LACP mode based on whether the Link Aggregation Control Protocol (LACP) is enabled or not. In static mode, the establishment of Eth Trunk and the addition of member interfaces are manually configured without the involvement of link aggregation control protocols. In this mode, all active links participate in data forwarding and evenly share traffic, hence it is called load sharing mode. If an active link fails, the link aggregation group automatically shares the traffic equally among the remaining active links. When it is necessary to provide a larger link bandwidth between two directly connected devices and the devices do not support the LACP protocol, static mode can be used.

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.

4.5.2 LACP

LACP (Link Aggregation Control Protocol), based on IEEE 802.3ad Standard, dynamically aggregates and disaggregates links. It exchanges info with the opposite network devices through LACPDU (Link Aggregation Control Protocol Data Unit).
After a port uses LACP, it will inform the opposite network device of system priority, system MAC, port priority and No., and operation Key by transmitting a LACPDU. The opposite device will compare such info with that saved by other ports after receiving it,

thus reaching an agreement on port participation in or quitting from a dynamic aggregation.

Dynamic LACP aggregation is automatically created or deleted by system, that is, internal ports can be added or removed by themselves. Only the ports connected to a same device with the same rate, duplex, and basic configuration can be aggregated.
Instructions for adding a dynamic link aggregation:

1. Click the “Configuration > Trunk Group Setting” in the navigation bar, select the LAG ID and LACP mode, “Edit” them as follows:

2. Click the “Configuration > Trunk Group Setting” Select LACP, select two ports to add as one LACP group

Interface data are as follows

Configuration Items	Description
Type	Static mode: When it is necessary to increase the bandwidth or reliability between two devices, and one of the devices does not support the LACP protocol, a static link aggregation can be created on the device and multiple member interfaces can be added to increase the bandwidth and reliability between the devices. LACP mode: In dynamic LACP mode, the link between two devices has the ability of redundant backup. When some links fail, the backup link is used to replace the faulty link, maintaining uninterrupted data transmission.
System Priority	LACP determines the active and passive modes between two devices subject to priority standard.

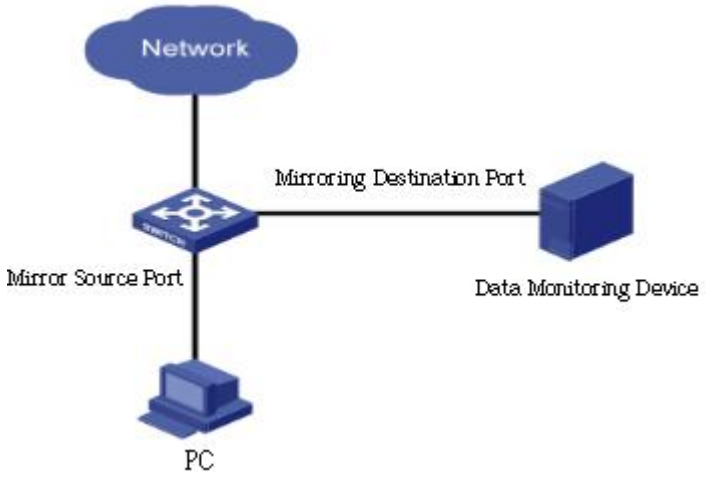
Port	Port list
Port Priority	LACP determines the dynamic LAG member mode subject to the port priority with a superior system.
Timeout	It decides the transmission frequency of LACP messages.

Description:

Please make sure there is no member interface accessing the Eth-Trunk before changing its work pattern, otherwise it fails.

4.6 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

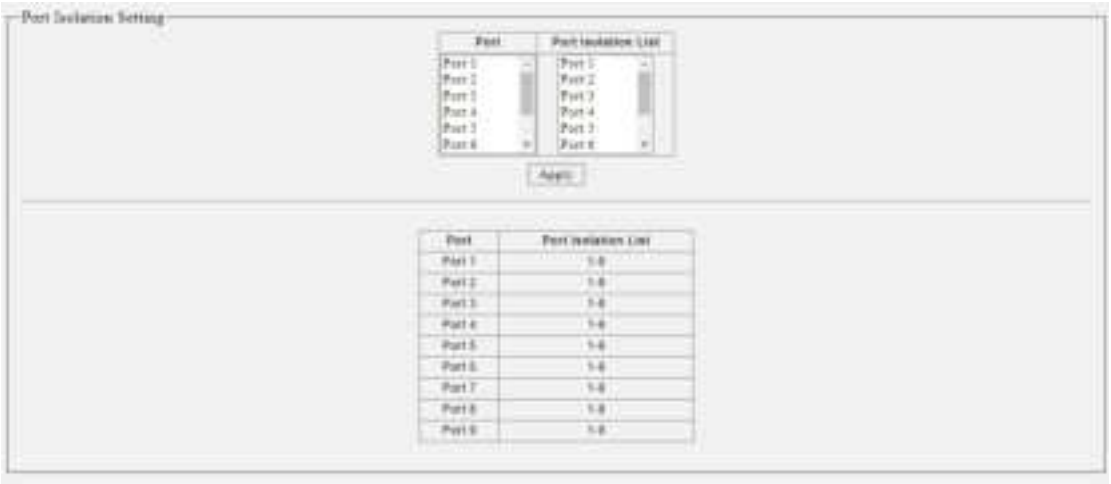
Configuration Items	Description
Mirror Direction	Enable or disable port mirroring, support Rx, Tx, and Both
Mirroring Port	Only one ordinary physical port can be selected, excluding link aggregation port and source port.
Mirrored Port List	List of mirrored source ports

4.7 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

4.8 Bandwidth Control

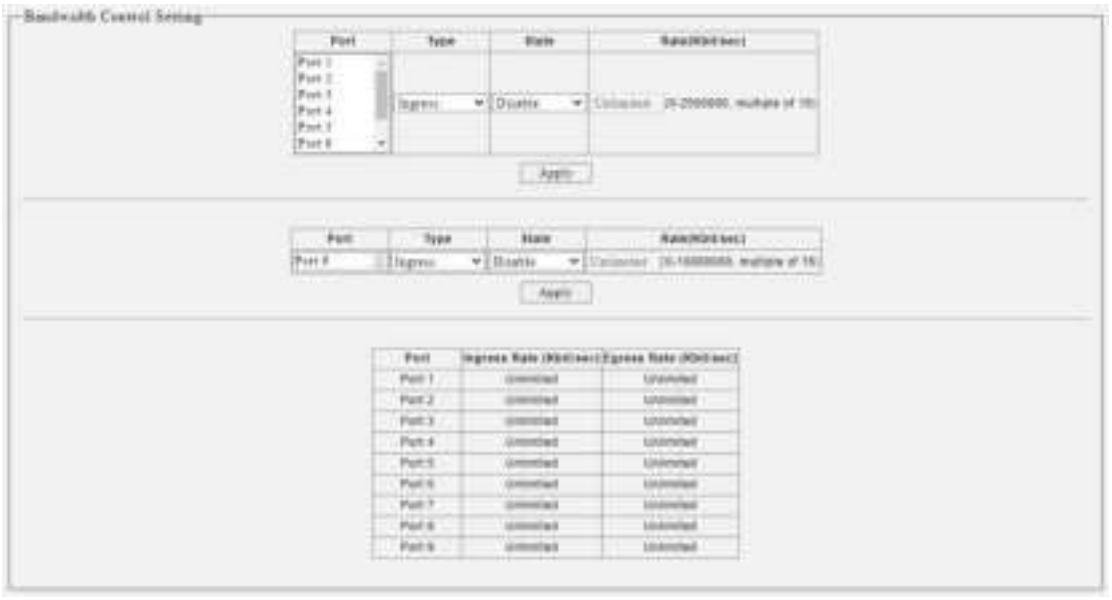
It refers to the rate restriction on transmitting and receiving data at physical interfaces.

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 disenable port restrictions
Rate	Rate limit, Port1-8 range: 0 to 25000000 Kbit,Port9 range:0to10000000Kbit

4.9 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

4.10 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
State	Enable or disable MAC constraint
Entry Limits	Limited number of MAC address learning

4.11 EEE

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

5 Security

5.1 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.

5.1.1 MAC Search

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 Search", in the navigation bar as follows:

5.1.2 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

5.2 Storm Control

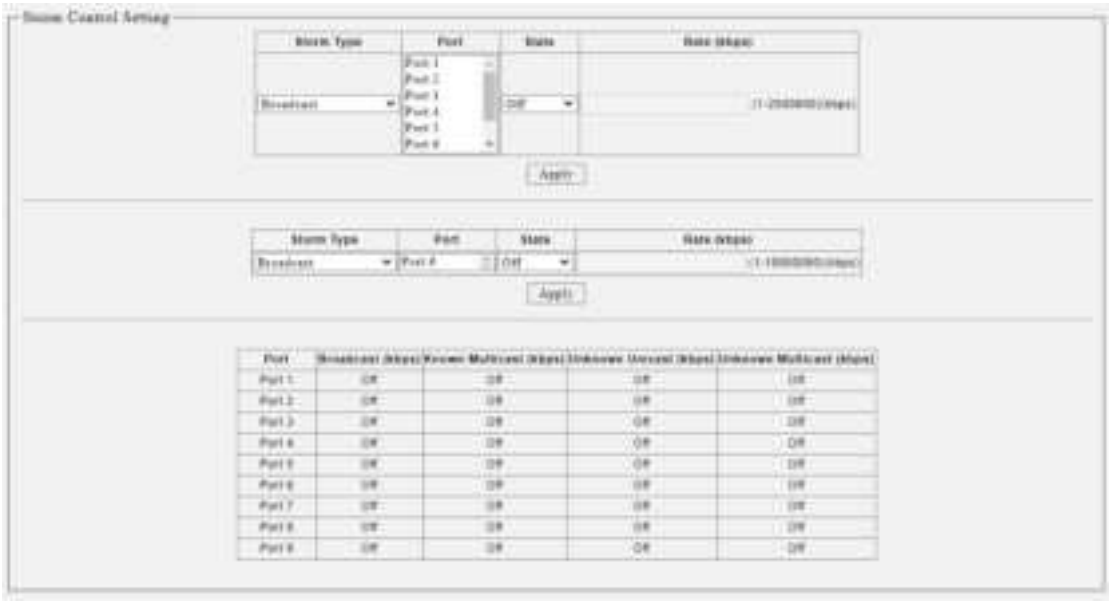
Storms generated via broadcast, unknown multicast and unicast messages are prevented as follows. These messages will be suppressed subject to packet rates respectively. The average rate of the messages received by monitoring interfaces will be compared with the max threshold configured during an inspection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

6 Monitoring

6.1 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 Tools

7.1 Firmware Upgrade

System version firmware upgrade

Instructions:

1. Click the “Tools> Firmware Upgrade”, in the navigation bar as follows:

Note: After clicking OK, do not power off during the upgrade process, stay on the upgrade page for about 1 minute until the upgrade is complete

7.2 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
Restore	Upload configuration

7.3 Reset

Restore factory settings

Instructions

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

7.4 Save

Instructions

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

7.5 Reboot

Restart the system.

Instructions

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

7.5 Logout

Exit the system

Instructions

1. Click the “Tools> Logout”, in the navigation bar as follows: