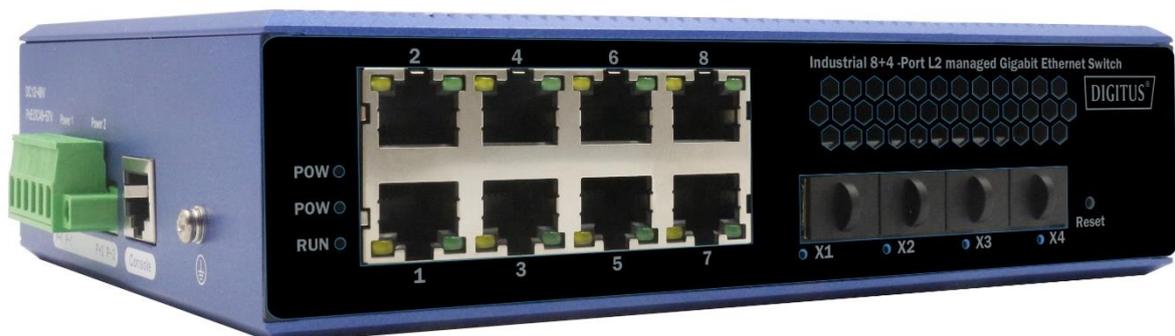




Industrial 8 + 4-port L2 managed Gigabit Ethernet (PoE) Switch



Web-Manual

DN-651160, DN-651161

Table of content

1. Log in to the switch web	4
1.1 System requirements for WEB access.....	4
1.2 Log in to the WEB configuration interface.....	4
2. System Information.....	5
2.1 Global Information	5
2.2 Statistics	6
2.3 Log.....	7
3. Port Management.....	7
3.1 Port Config.....	7
3.2 Port Isolate	8
3.3 Port Mirror	9
3.4 Port Limit.....	9
3.5 Storm Control.....	10
3.6 EEE(Energy-Efficient-Ethernet)	11
4. Basic(Layer 2 Management)	11
4.1 MAC Table	11
4.2 VLAN	12
4.3 GVRP.....	14
4.4 Link aggregation	15
4.5 MSTP Configuration	18
4.6 ERPS.....	20
4.7 Loop Protect.....	22
4.8 PTP.....	23
4.9 DHCP-snooping	24
4.10 802.1X.....	25
5. Layer 3 Config	27
5.1 Interface Config.....	27
5.2 Route Config.....	27
5.3 ARP	29
5.4 ND Config	30
5.5 DHCP Server	31
5.6 DHCP Relay.....	33
5.7 RIP	34
5.8 OSPF	36
5.9 RIPng	39
5.8 OSPFv3	40
6. Multicast Management.....	41
6.1 IGMP Snooping.....	41
6.2 MLD Snooping.....	42
6.3 IP Multicast	43
6.4 IGMP.....	43

7. Advance.....	45
7.1 QOS	45
7.2 ACL.....	46
7.3 SNMP	49
7.4 RMON	52
7.5 LLDP	54
7.6 NTP	55
7.7 Secure.....	56
8. System Management	56
8.1 User Config.....	56
8.2 Network.....	57
8.3 Service Config.....	58
8.4 Configuration management	58
8.5 Firmware Upgrade	58
8.6 Diagnostic.....	59
8.7 Restart	59

1. Log in to the switch web

1.1 System requirements for WEB access

Using this series of switches, the system should meet the following conditions.

Hardware Software	System Requirement
CPU	Pentium 586 ↑
RAM	128MB ↑
Resolution	1024x768 ↑
Browser	IE 8.0↑ /Firefox/Google Chrome/Opera, etc.
OS	Windows, Linux, Unix

1.2 Log in to the WEB configuration interface

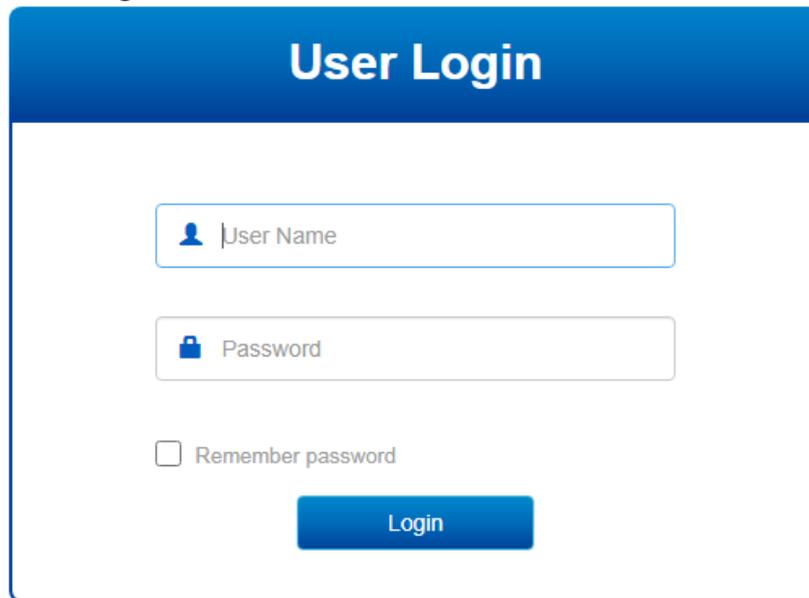
To log in to the WEB configuration interface of this series of switches, the user needs to confirm the following conditions:

- The switch has been configured with IP. By default, the interface IP address of VLAN1 of the switch is 192.168.10.12;
- The user ensures that the IP of the network card of his local PC (management host) is in the 192.168.10.* network segment;
- The user ensures that the network cable of his local PC is connected to any RJ45 network port of the switch;
- A host with a web browser has been connected to the network, and the host can ping the switch.

The steps to log in to the WEB configuration interface are as follows:

- Step 1 Run the computer browser;
- Step 2 Enter the address of the switch "http://192.168.10.12" in the address bar of the browser, and press Enter;
- Step 3 as shown in Figure 1-1, enter the user name and password in the login window (the default user name and password are both admin), and click "OK".

Figure 1-1 WEB interface login window



After successfully logging in, you can configure the relevant parameters and information of the WEB interface according to your needs.

2. System Information

2.1 Global Information

【Function Description】

On the "System Information" page, you can view Product Model, Serial Number, MAC Address, Firmware Version, Uptime, System Time and other information.

【Operation path】

Information > Global

【Interface description】

Figure 2-1 System Information Interface

Ports Status	
Global	
Product Model	YH6824GST4-SFP
Serial Number	SN20210301
MAC Address	AC:90:00:40:3D:00
Firmware Version	V1.0.0.1-gd06e45122
Uptime	0 Day 18 Hours 10 Minutes
System Time	2021-05-13 09:32:52 Time Sync
System	

Table 2-1 Main elements of the system information interface

Interface elements	Description
Product Model	Display the product model of the switch.
Serial Number	Display the serial number of the switch.
MAC Address	Display the MAC address of the switch.
Firmware Version	Display the firmware version of the switch.
Uptime	Display the operating time of the switch (the time from startup to the present).
System Time	Display the current time of the system.

2.2 Statistics

【Function Description】

On the "Statistics" page, you can view port summary statistics and detailed port statistics related information.

【Operation path】

Information > Statistics

【Interface description】

Figure 2-2 Port data statistics

Port	Rx Bytes	Rx Packets	Rx Dropped	Rx Errors	Tx Bytes	Tx Packets	Tx Dropped	Tx Errors
G1	0	0	0	0	0	0	0	0
G2	284716	2371	0	0	3492824	3187	0	0
G3	0	0	0	0	0	0	0	0
G4	0	0	0	0	0	0	0	0
G5	0	0	0	0	0	0	0	0
G6	340300	1938	37	0	1276222	2232	0	0
G7	0	0	0	0	0	0	0	0
G8	678904	3849	0	0	1571019	3948	0	0
G9	0	0	0	0	0	0	0	0
G10	2224	29	11	0	338627	2654	0	0

2.3 Log

【Function Description】

On the "Log" page, you can view and download the system log.

【Operation path】

Information > Log

【Interface description】

Figure 2-3-1 Log interface

Index	System Time	Log Level	Type	Module	Param	Log Content
1	2021-05-13 09:35:15	event	Login	System	User	User admin login form ip [192.168.10.18]
2	2021-05-13 09:34:29	alert	Link	PORT	G6	Interface [G6] state change to up.
3	2021-05-13 09:32:44	alert	Link	PORT	G8	Interface [G8] state change to up.
4	2021-05-13 09:32:42	alert	Link	PORT	G2	Interface [G2] state change to down.
5	2021-05-13 09:32:42	alert	Link	PORT	G10	Interface [G10] state change to up.
6	2021-05-13 09:32:38	alert	Link	PORT	G10	Interface [G10] state change to down.
7	2021-05-13 09:31:57	event	Login	System	User	User admin login form ip [192.168.10.88]
8	2021-05-13 09:31:00	event	Login	System	User	User admin login form ip [192.168.10.88]
9	2021-05-13 09:30:53	alert	Link	PORT	G2	Interface [G2] state change to up.
10	2021-05-12 15:23:19	alert	Link	PORT	G10	Interface [G10] state change to up.

Showing 1 to 20 of 25 rows rows per page

3. Port Management

3.1 Port Config

【Function Description】

On the "Port Config" page, you can enable or disable ports, set port speed and flow control, or view basic information about all ports.

【Operation path】

Port > Port Config

【Interface description】

Figure 3-1 Port configuration interface

Name	State	Medium	Speed	Duplex	Flowctl State	Speed Config	Max Frame	Flowctl	Enable
Select All						Auto	1518	<input type="checkbox"/>	<input type="checkbox"/>
G1		COMBO	1000M	Half		Auto	1518	<input type="checkbox"/>	<input type="checkbox"/>
G2		COMBO	1000M	Half		Auto	1518	<input type="checkbox"/>	<input type="checkbox"/>
G3		COMBO	1000M	Half		Auto	1518	<input type="checkbox"/>	<input type="checkbox"/>
G4		COMBO	1000M	Half		Auto	1518	<input type="checkbox"/>	<input type="checkbox"/>
G5		COMBO	1000M	Half		Auto	1518	<input type="checkbox"/>	<input type="checkbox"/>
G6		COMBO	1000M	Full		Auto	1518	<input type="checkbox"/>	<input checked="" type="checkbox"/>
G7		COMBO	1000M	Half		Auto	1518	<input type="checkbox"/>	<input type="checkbox"/>
G8		COMBO	1000M	Full		Auto	1518	<input type="checkbox"/>	<input checked="" type="checkbox"/>
G9		COPPER	1000M	Half		Auto	1518	<input type="checkbox"/>	<input type="checkbox"/>
G10		COPPER	1000M	Full		Auto	1518	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Table 3-1 Main elements of the port configuration interface

Interface elements	Description
Name	Display the port name.
State	Display port status.
Medium	Displays the type of media that the port can use.
Speed	Display port speed.
Duplex	Displays the port duplex mode.
Speed Config	Configure the port speed and duplex mode.
Max Frame	Set the maximum frame.
Flowctrl	Select the "Flow Control" check box to enable the port flow control function.
Enable	Select the "Enable" check box to enable the corresponding port. Enabled by default.

3.2 Port Isolate

【Function Description】

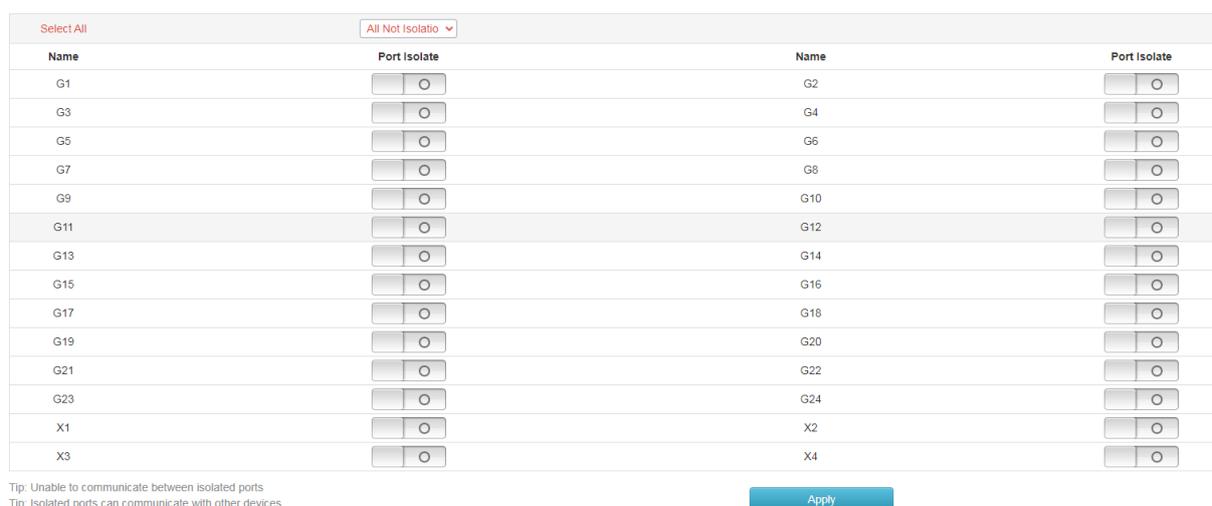
On the "Port Isolation" page, you can configure the port isolation.

【Operation path】

Port > Port Isolate

【Interface description】

Figure 3-2 Port Isolate interface



Communication between isolated ports is not possible, and isolated ports can communicate with other non-isolated ports.

3.3 Port Mirror

【Function Description】

Port mirroring is also called port monitoring. Port monitoring is a data packet acquisition technology. By configuring the switch, you can copy data packets of one/several ports (mirroring source port) to a specific port (mirroring destination port), and install one on the mirroring destination port. The host of the data packet analysis software analyzes the collected data packets, so as to achieve the purpose of network monitoring and troubleshooting.

【Operation path】

Port > Port Mirror

【Interface description】

Figure 3-3 Port mirror interface

Example: Mirror the message data sent from port 4 to port 1.

Mirror Destination Port	G1	Port Config	None Mirror
Port	Mirror Direction	Port	Mirror Direction
G1	None Mirror	G2	None Mirror
G3	None Mirror	G4	Both Mirror
G5	None Mirror	G6	None Mirror
G7	None Mirror	G8	None Mirror
G9	None Mirror	G10	None Mirror
G11	None Mirror	G12	None Mirror
G13	None Mirror	G14	None Mirror
G15	None Mirror	G16	None Mirror
G17	None Mirror	G18	None Mirror
G19	None Mirror	G20	None Mirror
G21	None Mirror	G22	None Mirror
G23	None Mirror	G24	None Mirror
X1	None Mirror	X2	None Mirror
X3	None Mirror	X4	None Mirror

3.4 Port Limit

【Function Description】

On the "Port Limit" page, you can configure the access rate of all ports.

【Operation path】

Port > Port Limit

【Interface description】

Figure 3-4 Port rate limit interface

Port	Ingress Rate(kbps)	Ingress Burst Size (Kbits)	Egress Rate(kbps)	Egress Burst Size (Kbits)
*	<input type="button" value="Global Config"/>			
G1	<input type="text" value="0"/>	<input type="text" value="2048"/>	<input type="text" value="0"/>	<input type="text" value="2048"/>
G2	<input type="text" value="0"/>	<input type="text" value="2048"/>	<input type="text" value="0"/>	<input type="text" value="2048"/>
G3	<input type="text" value="0"/>	<input type="text" value="2048"/>	<input type="text" value="0"/>	<input type="text" value="2048"/>
G4	<input type="text" value="0"/>	<input type="text" value="2048"/>	<input type="text" value="0"/>	<input type="text" value="2048"/>
G5	<input type="text" value="0"/>	<input type="text" value="2048"/>	<input type="text" value="0"/>	<input type="text" value="2048"/>
G6	<input type="text" value="0"/>	<input type="text" value="2048"/>	<input type="text" value="0"/>	<input type="text" value="2048"/>
G7	<input type="text" value="0"/>	<input type="text" value="2048"/>	<input type="text" value="0"/>	<input type="text" value="2048"/>
G8	<input type="text" value="0"/>	<input type="text" value="2048"/>	<input type="text" value="0"/>	<input type="text" value="2048"/>
G9	<input type="text" value="0"/>	<input type="text" value="2048"/>	<input type="text" value="0"/>	<input type="text" value="2048"/>
G10	<input type="text" value="0"/>	<input type="text" value="2048"/>	<input type="text" value="0"/>	<input type="text" value="2048"/>

Table 3-4 Main elements of the port rate limit interface

Interface elements	Description
Port	Display the port name.
Ingress rate	Configure the corresponding port ingress rate.
Ingress burst size	Configure burst packet size.
Egress rate	Configure the corresponding port export rate
Egress burst size	Configure burst packet size.

3.5 Storm Control

【Function Description】

On the "Storm Control" page, you can configure the rate of broadcast packets, multicast packets, and unknown unicast packets for each port to achieve port suppression.

【Operation path】

Port> Storm Control

【Interface description】

Figure 3-5 Storm control interface

Port	Broadcast(pps)	Multicast(pps)	Unknown Unicast(pps)
*	<input type="text" value="Global Config"/>	<input type="text" value="Global Config"/>	<input type="text" value="Global Config"/>
G1	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
G2	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
G3	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
G4	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
G5	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
G6	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
G7	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
G8	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
G9	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
G10	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

Table 3-5 Main elements of storm Control interface

Interface elements	Description
Port	Display the port name.
Broadcast	Configure the broadcast suppression rate of the corresponding port. Unit: pps
Multicast	Configure the multicast suppression rate of the corresponding port. Unit: pps
Unknown Unicast	Configure the unknown unicast suppression rate of the corresponding port. Unit: pps

3.6 EEE (Energy-Efficient-Ethernet)

【Function Description】

On the "EEE" page, you can configure EEE for each Ethernet port

【Operation path】

Port> EEE

【Interface description】

Figure 3-6 EEE Interface

Select All		EEE	
Name	EEE	Name	EEE
G1	<input type="checkbox"/>	G2	<input type="checkbox"/>
G3	<input type="checkbox"/>	G4	<input type="checkbox"/>
G5	<input type="checkbox"/>	G6	<input type="checkbox"/>
G7	<input type="checkbox"/>	G8	<input type="checkbox"/>
G9	<input type="checkbox"/>	G10	<input type="checkbox"/>
G11	<input type="checkbox"/>	G12	<input type="checkbox"/>
G13	<input type="checkbox"/>	G14	<input type="checkbox"/>
G15	<input type="checkbox"/>	G16	<input type="checkbox"/>
G17	<input type="checkbox"/>	G18	<input type="checkbox"/>
G19	<input type="checkbox"/>	G20	<input type="checkbox"/>
G21	<input type="checkbox"/>	G22	<input type="checkbox"/>
G23	<input type="checkbox"/>	G24	<input type="checkbox"/>

4. Basic(Layer 2 Management)

4.1 MAC Table

【Function Description】

On the "MAC Table" page, you can configure the aging time of the MAC address and view the MAC address information of the port.

【Operation path】

Basic > mac

【Interface description】

Figure 4-1 MAC Table interface

Add Del Expired Time(s):

<input type="checkbox"/>	Index	MAC Address	VLAN	Port	Type
<input type="checkbox"/>	1	00-00-00-00-61-35	1	G6	dynamic <input type="button" value="Bind"/>
<input type="checkbox"/>	2	4c-cc-6a-70-b4-60	1	G6	dynamic <input type="button" value="Bind"/>
<input type="checkbox"/>	3	00-26-9e-f6-93-f5	1	G8	dynamic <input type="button" value="Bind"/>

Total 3 records Total 1 pages Current 1 page First < Previous Next > Last

4.2 VLAN

【Function Description】

On the "VLAN" page, you can view VLAN status, set port VLAN, voice VLAN, and configure MAC-based VLAN and IP-based VLAN.

【Operation path】

Basic > VLAN

【Interface description】

The following figure shows the view of the VLAN status of the switch,

Vlan	Port																											
	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14	G15	G16	G17	G18	G19	G20	G21	G22	G23	G24	X1	X2	X3	X4
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U

Excluded
 Tagged
 Untagged

The following figure shows the configuration of port VLAN,

Port	Vlan Mode	PVID	vlan untag	vlan tag
Select All	hybrid			
G1	access	1	1	
G2	access	1	1	
G3	access	1	1	
G4	access	1	1	
G5	access	1	1	
G6	access	1	1	
G7	access	1	1	
G8	access	1	1	
G9	access	1	1	
G10	access	1	1	

Port properties that can be set:

Access:

The access port is usually used to connect to the terminal. The access port has the following characteristics:

- There is only one VLAN, port VLAN (also known as access VLAN), which is a member of 1 by default,
- Accept unmarked frames and C-marked frames,
- Discard all frames in the unclassified access VLAN,
- All frames on the egress are sent untagged.

Trunk:

Trunk ports can carry multiple VLAN traffic at the same time, and are usually used to connect to other switches. Trunk port has the following characteristics:

- By default, trunk ports are members of all existing VLANs. This can be limited by using allowed VLANs,
- Unless VLAN trunking is enabled on the port and divided into different VLANs, the

- frames of whether the port is a member or not will be discarded,
- By default, all frames but are classified into the port VLAN (also known
- As the native VLAN) frame tag gets on the egress. Frames that fall into the port VLAN do not get C-tagged egress,
- The exit marking can change all the marked frames, in this case, only the entrance of the marked frame is accepted,
- VLAN trunking may be enabled.

Hybrid:

Hybrid ports are similar to Trunk ports in many ways, but with additional port configuration capabilities. In addition to the features described for trunk ports, Hybrid ports have these capabilities:

- Can be configured as VLAN tag or unknown, C-tag all, S tag all, or S-custom tag all,
- Inlet filtering can be controlled,
- Enter the acceptance frame, the exit label and configuration can be configured independently.

Port VLAN:

The VLAN ID of the port (also called PVID). The allowed VLAN range is 1 to 4095, and the default is 1.

The following page is the voice VLAN config interface;

The screenshot shows a configuration interface with tabs for 'Vlan State', 'Vlan Config', 'Voice VLAN Config', 'MAC VLAN Config', and 'IP VLAN Config'. The 'Voice VLAN Config' tab is active. A message at the top states: 'The corresponding port untagged belongs to the vlan function to take effect; port receives the message, match the conditions set will enter the corresponding VLAN'. Below this, there are several configuration fields:

- 'Enable voice vlan' with a radio button set to 'O'.
- 'Vlan id' with a text input containing '1' and a range of '1-4094'.
- 'cos' with a text input containing '5' and a range of '0-7'.
- 'dscp' with a text input containing '46' and a range of '0-63'.

 A 'Set' button is located below these fields. Under the 'Voice vlan MAC' section, there are two text input fields:

- 'MAC' with a placeholder example '00-01-02-03-04-05'.
- 'MAC mask' with a placeholder example 'fc-ff-ff-00-00-00'.

 An 'Add' button is at the bottom of this section.

When the voice VLAN feature is enabled, the Access port can carry IP voice traffic from IP phones. When the switch is connected to a Cisco IP phone (such as a Cisco 7960 IP phone), the voice traffic sent by the IP phone has three layers of IP priority. And the CoS value of the second layer, both of these two values are set to 5 by default. For IEEE 802.1Q or IEEE 802.1p tagged traffic, the default COS value is untrusted. Configure MAC address-based VLAN,

Vlan State	Vlan Config	Voice VLAN Config	MAC VLAN Config	IP VLAN Config
<p>Vlan id <input type="text"/> range: 1-4094</p> <p>MAC <input type="text"/> For Example: 00-01-02-03-04-05</p> <p><input type="button" value="Add"/></p>				
No	VID	MAC	No matching records found	

Configure IP-based VLAN,

Vlan State	Vlan Config	Voice VLAN Config	MAC VLAN Config	IP VLAN Config
<p>Vlan id <input type="text"/> range: 1-4094</p> <p>IP <input type="text"/> For Example: 10.1.1.0/24</p> <p><input type="button" value="Add"/></p>				
No	VID	IP	No matching records found	

4.3 GVRP

【Function Description】

On the "GVRP" page, you can configure GVRP related functions.

【Operation path】

Basic > GVRP

【Interface description】

Enable or disable GVRP function;

Global Config	Port Config	GVRP Statistics
<p>Enable GVRP <input type="checkbox"/></p> <p>Create Dynamic VLAN <input type="checkbox"/></p> <p><input type="button" value="Apply"/></p>		

Apply the enabled GVRP function to the designated port and configure its timer;

Port	Enable GVRP	Registration Mode	Applicant State	Join Timer(cs)	Leave Timer(cs)	LeaveAll Timer(cs)
Select All	<input type="checkbox"/>	normal	normal			
G1	<input type="checkbox"/>	normal	normal	20	60	1000
G2	<input type="checkbox"/>	normal	normal	20	60	1000
G3	<input type="checkbox"/>	normal	normal	20	60	1000
G4	<input type="checkbox"/>	normal	normal	20	60	1000
G5	<input type="checkbox"/>	normal	normal	20	60	1000
G6	<input type="checkbox"/>	normal	normal	20	60	1000
G7	<input type="checkbox"/>	normal	normal	20	60	1000
G8	<input type="checkbox"/>	normal	normal	20	60	1000
G9	<input type="checkbox"/>	normal	normal	20	60	1000
G10	<input type="checkbox"/>	normal	normal	20	60	1000

View the operating information of GVRP;

Port	JoinEmpty Rx	JoinIn Rx	LeaveEmpty Rx	LeaveIn Rx	Empty Rx	JoinEmpty Tx	JoinIn Tx	LeaveEmpty Tx	LeaveIn Tx	Empty Tx
No matching records found										

4.4 Link aggregation

【Function Description】

Link aggregation is the formation of a logical port from multiple physical ports of the switch, and multiple links belonging to the same aggregation group can be regarded as a logical link with a larger bandwidth.

Link aggregation can realize the sharing of communication traffic among the member ports in the aggregation group to increase bandwidth. At the same time, each member port of the same aggregation group dynamically backs up each other, which improves the reliability of the link.

Member ports belonging to the same aggregation group must have consistent configurations. These configurations mainly include STP, QoS, VLAN, port attributes, MAC address learning, ERPS configuration, loop Protect configuration, mirroring, 802.1x, IP filtering, Mac filtering, Port isolation, etc.

Tip: It is not recommended to configure the ports and advanced functions for the ports used for link aggregation.

Link aggregation is divided into static aggregation and dynamic aggregation (LACP). The peer devices of link aggregation with switches are generally switches and NICs.

4.4.1 Static aggregation config

【Function Description】

Static aggregation requires manual configuration by the user and does not allow the system to automatically add or delete ports in the aggregation group. The static aggregation configuration logic is simple and easy to understand and use.

【Operation path】

Basic >Link Aggr

【Interface description】

Figure 4-4-1 Static aggregation interface

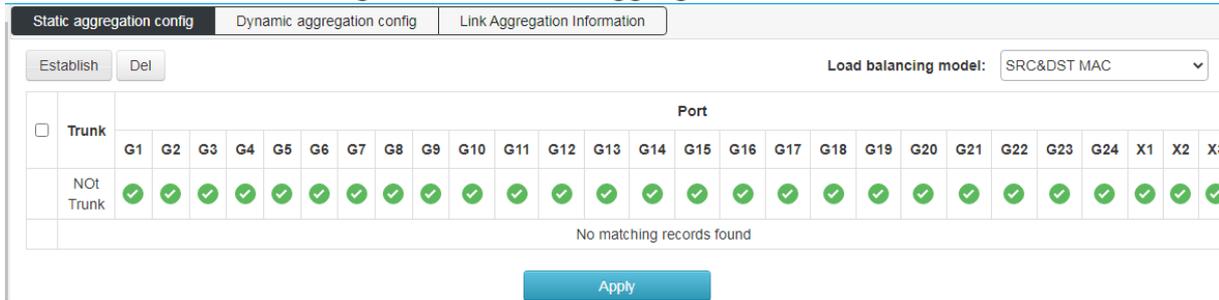


Table 4-4-1 Main elements of static aggregation interface

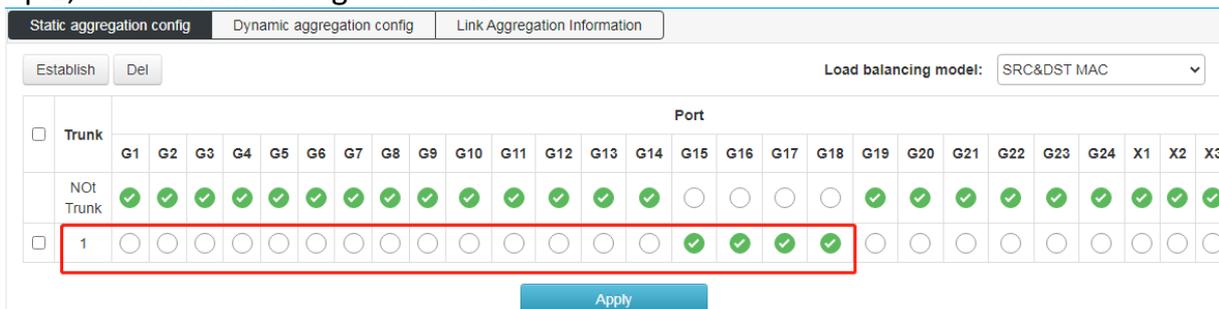
Interface elements	Description
Load balancing mode	Select the load balancing mode of the data stream. There are 6 types: 1.SRC MAC 2.DST MAC 3.SRC&DST MAC 4.SRC IP 5.DST IP 6.SRC&DST IP
Port member	Select the ports that need to be aggregated into a group. The switch has created all aggregation groups by default, and the port members are empty. To configure member ports for the aggregation group, click the port to the corresponding aggregation group, and the port can be added to the aggregation group.

Special Note:

1. The static aggregation of the same port cannot be configured at the same time as the dynamic LACP aggregation;
2. Please keep the configuration consistency of the member ports of the aggregation group;
3. The number of member ports in the aggregation group is 2-8.

【Example】

Select SMAC&DMAC for load balancing mode, and add ports 15, 16, 17, 18 to aggregation group 1, as shown in the figure below:



4.4.2 Dynamic aggregation config

【Function Description】

LACP (Link Aggregation Control Protocol, Link Aggregation Control Protocol) is a protocol based on the IEEE 802.3ad standard to realize dynamic link aggregation and disassembly. The two parties of the aggregation device exchange aggregation information through LACPDU messages, and aggregate the matching links together to send and receive data. The addition and deletion of ports in the aggregation group are automatically completed by the protocol, which has high flexibility and provides load balancing capabilities.

The configuration parameters of the LACP protocol mainly include: port LACP function enable, key value, port role (active/passive mode), and port priority.

Only the ports with the LACP protocol enabled will carry out LACP negotiation, which may form an aggregation link. The key is the basis of negotiation, and only ports with the same key can negotiate to form an aggregation link. The negotiation mode is "active/passive".

When "active" is selected, the device will actively initiate convergence negotiation; when "passive" is selected, the device passively accepts the convergence negotiation initiated by other devices. When two devices are interconnected, at least one or both ends need to be set to "active" mode to successfully negotiate.

【Operation path】

Basic > Link Aggr > Dynamic aggregation config

【Interface description】

Figure 4-4-2 LACP configuration interface

Name	Activity Mode	Send Mode	Port Priority	Key Value	Enabled
Select All	--	--	1-65535	0-65535	<input type="checkbox"/>
G1	--	--	32768	0	<input type="checkbox"/>
G2	--	--	32768	0	<input type="checkbox"/>
G3	--	--	32768	0	<input type="checkbox"/>
G4	--	--	32768	0	<input type="checkbox"/>
G5	--	--	32768	0	<input type="checkbox"/>
G6	--	--	32768	0	<input type="checkbox"/>
G7	--	--	32768	0	<input type="checkbox"/>
G8	--	--	32768	0	<input type="checkbox"/>
G9	--	--	32768	0	<input type="checkbox"/>
G10	--	--	32768	0	<input type="checkbox"/>

Link aggregation information: view switch aggregation port information;

This switch supports dynamic aggregation of ports. After the dynamic protocol is enabled on the ports, the devices of the two parties in the aggregation exchange information through the protocol. According to the parameters and status of the two parties, the matching links are automatically aggregated to send and receive data. After the convergence is formed, the switching equipment maintains the status of the convergence link, and automatically adjusts or disbands the convergence link when the configuration of both parties changes.

The configuration parameters of the dynamic protocol include the protocol switch state,

negotiated key, and active and passive mode selection. Only the ports with dynamic protocol enabled will carry out dynamic negotiation, thus it is possible to form an aggregation link. The key is the basis of negotiation, and only ports with the same key can negotiate to form an aggregation link. The negotiation mode is "active passive". When "active" is selected, the device will actively initiate convergence negotiation; when "passive" is selected, the device passively accepts the convergence negotiation initiated by other devices. If some ports have already undergone static port aggregation, LACP dynamic aggregation may not be achieved.

Note: Dynamic LACP aggregation on the same port cannot be configured at the same time as static aggregation

Static aggregation config		Dynamic aggregation config		Link Aggregation Information															
Trunk		Mode		Number Ports				Port List				Load Balancing							
		Local												Peer					
Trunk		Name	State	The Port Number	Priority	Key Value	Sign	Connection	The Port Number	Priority	Key Value	Sign	System ID	System Priority					

Flags: A -- LACP_Activity, B -- LACP_timeout, C -- Aggregation, D -- Synchronization, E -- Collecting, F -- Distributing, G -- Defaulted, H -- Expired

4.5 MSTP Configuration

【Function Description】

The Spanning Tree Protocol is established in accordance with the IEEE 802.1D standard and is used to eliminate physical loops at the data link layer in a local area network. Devices running this protocol discover loops in the network by exchanging information with each other, and selectively block certain ports, and finally trim the loop network structure into a loop-free tree network structure, thereby preventing packets from being looped. The continuous growth and infinite loop in the road network avoids the problem of reduced message processing capacity caused by the repeated reception of the same message. The configuration of the spanning tree function of this device is simple. After the spanning tree function is enabled, it can be used by selecting the relevant protocol (STP or RSTP). The MSTP of multiple spanning tree can be used only after enabling the configuration example.

【Operation path】

Basic > mstp

【Interface description】

Figure 4-5-1 Global configuration interface

Instance configuration: configure MSTP instance,
Set the mapping Vlan for multiple spanning trees

Configuration name: Identifies the name of the VLAN to MSTI mapping, the bridge must share the name and revision (see below), and the VLAN-to-MSTI mapping configuration in order to share the MSTI spanning tree. (In the area) The name can be up to 32 characters.

Configuration version: The revision of the above MSTI configuration. This must be an integer between 0 and 65535.

Mapping VLANs: A list of VLANs mapped to MSTI. VLANs must be separated by commas and/or spaces. VLAN can only be mapped to one MSTI. An unused MSTI should remain empty. (That is, there is no vlan mapped to it).

No	MSTI ID	Priority	Vlan Mapped	Bridge ID	Regional Root	Internal Path Cost	Time Since Topo-change	Topo-change Count	
1	0	32768	1-4094	8.000.AC:90:00:40:3D:00	8.000.AC:90:00:40:3D:00	0	0	0	Set

Interface instance configuration: configure the enablement of the instance on the port.

Global Config		Instance Config		Interface Instance Config		Interface		
MSTI ID:		0						
Interface	Ports List	Enable Status	MSTI ID	Priority	Admin Cost	Oper Cost	Role	State
Select All				<input type="text" value="128"/>	<input type="text" value="0"/>			
G1	G1		0	<input type="text" value="128"/>	<input type="text" value="0"/>	20000	Disabled	forwarding
G2	G2		0	<input type="text" value="128"/>	<input type="text" value="0"/>	20000	Disabled	forwarding
G3	G3		0	<input type="text" value="128"/>	<input type="text" value="0"/>	20000	Disabled	forwarding
G4	G4		0	<input type="text" value="128"/>	<input type="text" value="0"/>	20000	Disabled	forwarding
G5	G5		0	<input type="text" value="128"/>	<input type="text" value="0"/>	20000	Disabled	forwarding
G6	G6		0	<input type="text" value="128"/>	<input type="text" value="0"/>	20000	Disabled	forwarding
G7	G7		0	<input type="text" value="128"/>	<input type="text" value="0"/>	20000	Disabled	forwarding
G8	G8		0	<input type="text" value="128"/>	<input type="text" value="0"/>	20000	Disabled	forwarding
G9	G9		0	<input type="text" value="128"/>	<input type="text" value="0"/>	20000	Disabled	forwarding
G10	G10		0	<input type="text" value="128"/>	<input type="text" value="0"/>	20000	Disabled	forwarding

Interface configuration: Configure the ports enabled for spanning tree protocol and the enabled ports for BPDU packets;

Global Config		Instance Config		Interface Instance Config		Interface		
Interface	Ports List	Enable Spanning-Tree	Root Guard	BPDU Guard	Admin Edge	Oper Edge	Admin Point-to-Point	Oper Point-to-Point
Select All		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto		Auto	
G1	G1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	NO	Auto	NO
G2	G2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	NO	Auto	Yes
G3	G3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	NO	Auto	NO
G4	G4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	NO	Auto	NO
G5	G5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	NO	Auto	NO
G6	G6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	NO	Auto	Yes
G7	G7	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	NO	Auto	NO
G8	G8	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	NO	Auto	Yes
G9	G9	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	NO	Auto	NO
G10	G10	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto	NO	Auto	Yes

4.6 ERPS

【Function Description】

ERPS (Ethernet Ring Protection Switching): Ethernet multi-ring protection technology, the protocol standard is ITU-TG.8032 multi-ring standard. ERPS's pursuit of higher performance and more security is the eternal development direction of the network, and the Ethernet ring technology has become an important means of redundancy protection in the second-tier network.

In the two-layer network, the STP protocol is generally used for network reliability, as well as the loop protection protocol mentioned in the previous section. The STP protocol is a standard ring network protection protocol developed by IEEE and has been widely used. The application is limited by the size of the network, and the convergence time is affected by the network topology. STP generally takes a second to converge, and it takes longer when the network diameter is larger. Although RSTP/MSTP can reduce the convergence time to

milliseconds, it still cannot meet the requirements for services with high service quality requirements such as 3G/NGN voice. In order to further shorten the convergence time and eliminate the influence of network size, the ERPS protocol came into being.

ERPS is a link layer protocol specially applied to the Ethernet ring. It can prevent the broadcast storm caused by the data loop in the Ethernet ring; when a link on the Ethernet ring is disconnected, the backup link can be quickly activated to Restore communication between nodes on the ring network. Compared with the STP protocol, the ERPS protocol has the characteristics of fast topology convergence (less than 20ms) and the convergence time has nothing to do with the number of nodes on the ring network. The loop protection function is similar to STP and erps, but the loop protection does not have IEEE standards and belongs to a private protocol. The configuration is simple to use, and the convergence time is also in seconds. For simple ring network topologies and common network services, it has advantages in line backup It's also obvious.

【Operation path】

Basic > ERPS

【Interface description】

Figure 4-6-1 ERPS Global Config interface

Index	STG ID	Vlan Mapped
1	0	1-4094

Figure 4-6-2 ERPS Profile Config interface

Index	Profile Name	WTR Timer (minute)	Hold-off Timer (ms)	Guard Timer (ms)	WTB Timer (ms)	Revertive
1	Default	5	0	500	5500	<input type="checkbox"/>
2	test	1	0	500	5500	<input checked="" type="checkbox"/>

Figure 4-6-3 ERPS Ring Config interface

Index	Ring ID	East Interface	West Interface
1	1	X1	X2

Figure 4-6-4 ERPS Instance Config interface

Instance ID	Physical Ring ID	East Interface	West Interface	Node Role	Role Port	Profile Name	Ring Type	R-APS Channel	Data Reference STG	Data VLAN	R-APS Level	Protocol Version	Enable ERPS
1	1	-	-	Owner Node	East Interface	test	Major Ring	3001	0	7	V2	<input checked="" type="checkbox"/>	

Figure 4-6-5 ERPS Ring Instance Info interface

Instance ID	Physical Ring ID	Enable ERPS	Ring Type	Instance State	Node Role	Data VLAN List	Attached Sub-Ring Instances	Attached to Major Instance	Virtual ID(Vlan ID): Ring ID
1	None		Major Ring	Init	None	-	-	-	--

Interface Type	Interface name	Interface Role	Link State	Forced Switch	Manual Switch	Clear
East Interface	-	-	-	<input type="button" value="Forced Switch"/>	<input type="button" value="Manual Switch"/>	<input type="button" value="Clear"/>
West Interface	-	-	-	<input type="button" value="Forced Switch"/>	<input type="button" value="Manual Switch"/>	<input type="button" value="Clear"/>

4.7 Loop Protect

【Function Description】

The loop protection function is similar to STP in terms of functions, but the loop protection does not have the IEEE standard and is a private protocol. It is simple to configure and use. It has obvious advantages in line backup for simple ring network topologies and common network services.

On the "Loop Protection" page, you can enable or disable the loop protection function and set related parameters.

【Operation path】

Basic > Loop Protect

【Interface description】

Figure 4-7-1 Loop protection Global Config interface

Global Config | Port Config

Enable

Tx Interval range : 1-10 s

Port Auto-Recover Time s. Blocked port will recover if not received PDU while timer expires.

Apply

Figure 4-7-2 Loop protect port config interface

Port	Enabled	tx	State	Loop
Select All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
G1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Down	☀
G2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Down	☀
G3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Down	☀
G4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Down	☀
G5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Down	☀
G6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Forwarding	☀
G7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Down	☀
G8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Forwarding	☀
G9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Down	☀
G10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Forwarding	☀

4.8 PTP

PTP enable: enable PTP function globally;

The PTP protocol defines the following three types of basic clock nodes:

OC (Ordinary Clock): Only one PTP communication port clock is an ordinary clock.

BC (Boundary Clock): A clock with more than one PTP communication port.

TC (Transparent clock): Compared with BC/OC, BC/OC needs to keep time synchronization with other clock nodes, while TC does not keep time synchronization with other clock nodes.

TC has multiple PTP ports, but it only forwards PTP protocol packets between these ports and corrects the forwarding delay, and does not synchronize time through any one port.

Global Config | Port Config

PTP Enable

PTP Clock ordinary boundary transparent PTP Clock Type

Apply

Port configuration

Enable the PTP function of the designated port;

Port	Enabled	State
Select All	<input type="checkbox"/>	
G1	<input type="checkbox"/>	Down
G2	<input type="checkbox"/>	Down
G3	<input type="checkbox"/>	Down
G4	<input type="checkbox"/>	Down
G5	<input type="checkbox"/>	Down
G6	<input type="checkbox"/>	Forwarding
G7	<input type="checkbox"/>	Down
G8	<input type="checkbox"/>	Forwarding
G9	<input type="checkbox"/>	Down
G10	<input type="checkbox"/>	Forwarding

4.9 DHCP-snooping

Global configuration: enable DHCP monitoring function;

Global Config	Static Binding	Port Config
<p>Enable DHCP-Snooping <input type="checkbox"/></p> <p>Apply</p>		

Static Binding: configure static monitoring port

Global Config	Static Binding	Port Config			
<p>MAC <input type="text"/> For Example: 02-02-03-04-05-06</p> <p>IP Address <input type="text"/> For Example: 192.168.1.1</p> <p>Port <input type="text" value="G1"/></p> <p>Add</p>					
No	Port	MAC	IP Address	Type	Cycle
No matching records found					

Port configuration: enable the DHCP monitoring function on the port;

Port	Untrust	IPSG
Select All	<input type="checkbox"/> <input type="radio"/>	<input type="checkbox"/> <input type="radio"/>
G1	<input type="checkbox"/> <input type="radio"/>	<input type="checkbox"/> <input type="radio"/>
G2	<input type="checkbox"/> <input type="radio"/>	<input type="checkbox"/> <input type="radio"/>
G3	<input type="checkbox"/> <input type="radio"/>	<input type="checkbox"/> <input type="radio"/>
G4	<input type="checkbox"/> <input type="radio"/>	<input type="checkbox"/> <input type="radio"/>
G5	<input type="checkbox"/> <input type="radio"/>	<input type="checkbox"/> <input type="radio"/>
G6	<input type="checkbox"/> <input type="radio"/>	<input type="checkbox"/> <input type="radio"/>
G7	<input type="checkbox"/> <input type="radio"/>	<input type="checkbox"/> <input type="radio"/>
G8	<input type="checkbox"/> <input type="radio"/>	<input type="checkbox"/> <input type="radio"/>
G9	<input type="checkbox"/> <input type="radio"/>	<input type="checkbox"/> <input type="radio"/>
G10	<input type="checkbox"/> <input type="radio"/>	<input type="checkbox"/> <input type="radio"/>

4.10 802.1X

【Function Description】

The 802.1X protocol was proposed by the IEEE802 LAN/WAN committee to solve the problem of wireless LAN network security. Later, the protocol was applied to Ethernet as a common access control mechanism for LAN ports, and was mainly used to solve the problems of authentication and security in the Ethernet. At the port level of the LAN access device, the connected equipment Authentication and control.

【Operation path】

Basic > 802.1X

【Interface description】

On the "Global Configuration" page, you can enable or disable the relevant parameters of the 802.1x authentication function.

Figure 4-1-1 Global configuration interface

Global Config	RADIUS Server Config	Port-based Authentication	Authentication Host
802.1X Settings			
Enable 802.1X	<input type="checkbox"/> <input type="radio"/>		
Auth Method	Port-Auth <input type="button" value="v"/>		
RADIUS Client Address	<input type="text"/> For Example : 192.168.200.1		
RADIUS Client Port	<input type="text" value="1812"/> range : 0-65535 , Defaults 1812		
RADIUS Server Key	<input type="text"/> range : less than 64 characters		
RADIUS Server Retransmit	<input type="text" value="3"/> range : 1-100 , Defaults 3		
RADIUS Server Timeout	<input type="text" value="5"/> range : 1-1000 , Defaults 5		
RADIUS Server Dearthime	<input type="text" value="0"/> range : 0-1440 , Defaults 0		
<input type="button" value="Apply"/>			

Figure 4-10-2 RADIUS Server Config interface

Global Config **RADIUS Server Config** Port-based Authentication Authentication Host

Add RADIUS Server

IP Address	The Port Number	Server Key	Retransmit	Timeout
No matching records found				

Add RADIUS Server ✕

RADIUS Server Address For Example : 192.168.200.1

RADIUS Server Port range : 0-65535 , Defaults 1812

RADIUS Server Key range : less than 64 characters

RADIUS Server Retransmit range : 1-100 , Defaults 3

RADIUS Server Timeout range : 1-1000 , Defaults 5

Add

Figure 4-10-3 Port-based Authentication Interface

Global Config RADIUS Server Config **Port-based Authentication** Authentication Host

Port Name	Port Auth Enable	Port Auth Mode	Ctrl Direction	Version	Auth Status	Quiet Period	Reauth Max	EAP Tx Period	Reauth Period	Reauthentication	Key Transmit
Select All	<input type="checkbox"/>	Force Unauthorized	Both-dir	1						<input type="checkbox"/>	<input type="checkbox"/>
G1	<input type="checkbox"/>	Auto	In-dir	2	Uncontrolled	60	2	30	3600	<input type="checkbox"/>	<input type="checkbox"/>
G2	<input type="checkbox"/>	Auto	In-dir	2	Uncontrolled	60	2	30	3600	<input type="checkbox"/>	<input type="checkbox"/>
G3	<input type="checkbox"/>	Auto	In-dir	2	Uncontrolled	60	2	30	3600	<input type="checkbox"/>	<input type="checkbox"/>
G4	<input type="checkbox"/>	Auto	In-dir	2	Uncontrolled	60	2	30	3600	<input type="checkbox"/>	<input type="checkbox"/>
G5	<input type="checkbox"/>	Auto	In-dir	2	Uncontrolled	60	2	30	3600	<input type="checkbox"/>	<input type="checkbox"/>
G6	<input type="checkbox"/>	Auto	In-dir	2	Uncontrolled	60	2	30	3600	<input type="checkbox"/>	<input type="checkbox"/>
G7	<input type="checkbox"/>	Auto	In-dir	2	Uncontrolled	60	2	30	3600	<input type="checkbox"/>	<input type="checkbox"/>
G8	<input type="checkbox"/>	Auto	In-dir	2	Uncontrolled	60	2	30	3600	<input type="checkbox"/>	<input type="checkbox"/>
G9	<input type="checkbox"/>	Auto	In-dir	2	Uncontrolled	60	2	30	3600	<input type="checkbox"/>	<input type="checkbox"/>
G10	<input type="checkbox"/>	Auto	In-dir	2	Uncontrolled	60	2	30	3600	<input type="checkbox"/>	<input type="checkbox"/>

Figure 4-10-4 Authntication Host Interface

Global Config RADIUS Server Config Port-based Authentication **Authentication Host**

Port-Auth Information

User Name	Port	Session Time(s)	Authentication Method	MAC Address	Session State and Reason
No matching records found					

5. Layer 3 Config

5.1 Interface Config

【Function Description】

On the "Interface Configuration" page, you can configure interface parameters.

【Operation path】

Layer3 > Interface

【Interface description】

Figure 5-1 Interface Config Interface

【Example】

As shown in the figure: set the interface name to vlanif20 and the IP to 192.168.20.1/32.

The screenshot shows the 'Interface' configuration page. At the top, there are two 'Interface Name' dropdown menus, both set to 'vlanif20'. Below them are 'IPV4 Address' and 'IPV6 Address' input fields. The 'IPV4 Address' field contains '192.168.20.1/32'. There are 'AddIPV4' and 'AddIPV6' buttons. A 'Create Interface' button is highlighted with a red box. Below the form is a table with columns: Interface, State, Mode, IPV4 Address, IPV6 Address, MAC, and Enable. The table lists interfaces: eth0, lo, vlanif1, and vlanif20. The 'vlanif20' row is highlighted with a red box, showing its state as 'UP' and mode as 'Unknown'. Below the table is an 'Apply' button.

Table 5-1 Main elements of the interface configuration interface

Interface elements	Description
Interface	Set the name of the Layer 3 interface, the format is vlanifX (X range 1-4094).
Enable	Enable or disable the Layer 3 interface function. Enabled by default.
IPV4 Address	Set the IP address and mask.
Set	After modifying the IP, click the Set button and the modification will be applied.

5.2 Route Config

【Function Description】

Static routing refers to routing information manually configured by users or network administrators. When the network topology or link status changes, the network administrator needs to manually modify the related static routing information in the routing table. Static routing information is private by default and will not be passed to other routers. Of course, the network administrator can also configure the router to be shared. Static

routing is generally suitable for relatively simple network environments. In such an environment, network administrators can easily understand the network topology and set correct routing information.

【Operation path】

Layer3 > Route

【Interface description】

Figure 5-2-1 View IPv4 Route interface

The screenshot shows the 'View IPv4 Route' interface with a table of routes and a legend below it.

No	purpose	Mask	Sign	Gateway	Out Interface
1	127.0.0.0	8	C>*		lo
2	192.168.10.0	24	C>*		vlanif1
3	192.168.20.1	32	C>*		vlanif20

Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, N - NHRP, > - selected route, * - FIB route

Refresh

Figure 5.2.2 IPv4 Static Route Config interface

The screenshot shows the 'IPv4 Static Route Config' interface with input fields for configuration and a table of configured routes.

Destination prefix: / For Example: 10.1.1.0/24

Gateway: For Example: 10.0.0.1

distance: range: 1-255

Add

No	Destination prefix	Mask	Gateway	distance	
1	eg. 192.168.30.0	24	192.168.20.2	1	Del

Table 5-2-2 Main elements of static routing interface

Interface elements	Description
Destination Prefix	Fill in the destination network address.
Gateway	Fill in the address of the next hop.
distance	Fill in the management distance, the default is 1, and the range is 1-255.

Figure 5-2-3 View IPv6 Route Interface

No	purpose	Mask	Sign	Gateway	Out Interface
1	::1	128	C>*		lo
2	fe80::	64	C *		vlanif20
3	fe80::	64	C>*		vlanif1
4	fe80:fe00::	64	C>*		vlanif1
5	ff00::	8	K>*		vlanif20

Codes: K - kernel route, C - connected, S - static, R - RIPng, O - OSPFv3, I - IS-IS, B - BGP, A - Babel, N - NHRP, > - selected route, * - FIB route

[Refresh](#)

Figure 5.2.4 IPv6 Static Route Config Interface

No	Destination prefix	Mask	Gateway	distance
No matching records found				

5.3 ARP

【Function Description】

On the ARP configuration page, you can configure the arp aging time or statically bind IP+MAC. One of the IP or MAC is different from the IP or MAC in the binding entry. It cannot access the CPU but can be forwarded; IP+MAC are all different Or if they are all the same, they can access the CPU, and they can also be forwarded.

【Operation path】

Layer3 > arp

【Interface description】

Figure 5-3-1 View ARP interface

No	IP Address	MAC Address	Out Interface	Mode	ARP Aging Time
1	192.168.10.18	4c-cc-6a-70-b4-60	vlanif1	dynamic	14240
2	192.168.10.88	00-26-9e-f6-93-f5	vlanif1	dynamic	14240

Table 5-3-1 Main elements of the View ARP configuration interface

Interface elements	Description
No	Serial number.
IP Address	The IP address of the ARP entry.
MAC Address	The MAC address of the ARP entry.
Out Interface	Display the bound virtual interface.
Mode	Shows whether the arp entry is dynamic or static.
ARP Aging Time	Display Arp aging time, the default is 14400s.

Figure 5-3-2 Static ARP Config interface

Set the IP address and MAC address to be bound;

Figure 5-3-3 ARP Aging Time Config interface

No	Interface	State	Aging Time(s)
1	eth0	DOWN	14400
2	lo	UP	14400
3	vlanif1	UP	14400
4	vlanif20	UP	14400

5.4 ND Config

【Function Description】

On the ND configuration page, you can configure the ND aging time or statically bind IP+MAC. One of the IP or MAC is different from the IP or MAC in the binding entry. It cannot access the CPU but can be forwarded; IP+MAC are all different Or if they are all the same, they can access the CPU or forward them.

【Operation path】

Layer3 > ND

【Interface description】

Figure 5-4-1 View ND interface

No	IP Address	MAC Address	Out Interface	Mode	ND Aging Time
1	fe80::95a:6a30:7e0b:ae2c	00-26-9e-f6-93-f5	vlanif1	dynamic	14190
2	fe80::2156:41f4:8163:e630	4c-cc-6a-70-b4-60	vlanif1	dynamic	14190
3	fe80::5a41:20ff:fead:a6c4	58-41-20-ad-a6-c4	vlanif1	dynamic	11620

Figure 5-4-2 Static ND interface

ND View **Static ND** ND Aging Time

IP Address For Example : fe80:fe00::fe0e

MAC Address For Example : 00-01-02-03-04-05

Interface

No	IP Address	MAC	Interface
No matching records found			

Figure 5-4-3 ND Aging Time Config interface

ND View Static ND **ND Aging Time**

No	Interface	State	Aging Time(s)
1	eth0	DOWN	<input type="text" value="14400"/>
2	lo	UP	<input type="text" value="14400"/>
3	vlanif1	UP	<input type="text" value="14400"/>
4	vlanif20	UP	<input type="text" value="14400"/>

5.5 DHCP Server

【Function Description】

On the "DHCP Server" page, you can configure the address pool and static binding configuration.

【Operation path】

Layer3 > DHCP Server

【Interface description】

Figure 5-5-1 Global configuration interface

Address Pool Config **Client List** Static client config

Enable DHCP Server

Max Lease Num range : 2048-10240 , Defaults 4096

<input type="checkbox"/>	Address Pool Name	Subnet segment	Default Gateway	Begin IP	End IP	Lease time	DNS server 1	DNS server 2	Domain Name Service	NetBIOS server
No matching records found										

Figure 5-5-2 Address Pool Setting Interface

Address Pool Name	<input type="text"/>	Less than 32 Bytes
Subnet segment	<input type="text"/>	For Example: 192.168.0.0/24
Begin IP	<input type="text"/>	
End IP	<input type="text"/>	
Lease time	<input type="text"/>	Seconds
Default Gateway	<input type="text"/>	For Example: 192.168.0.1
DNS server 1	<input type="text"/>	For Example: 192.168.0.1
DNS server 2	<input type="text"/>	For Example: 192.168.0.1
Domain Name Service	<input type="text"/>	For Example: 192.168.0.1
NetBIOS server	<input type="text"/>	For Example: 192.168.0.1

[Add](#)

Table 5-5-2 Main elements of the address pool configuration interface

Interface elements	Description
Address Pool name	Fill in the name of the dhcp address pool.
Subnet Segment	Fill in the subnet segment
Begin IP	Fill in the starting address of the DHCP address pool
End IP	Fill in the end address of the DHCP address pool
Lease time	Fill in the lease time of the address.
Default gateway	Fill in the default gateway of the client. This will be the default gateway parameter assigned by the server to the client. The IP address of the default gateway must be on the same network as the IP address of the DHCP client.
DNS server 1	Fill in the primary DNS Server address
DNS server 2	Fill in the address of the standby DNS server
Domain Name Service	Fill in the server domain name
NetBIOS Server	Fill in NetBIOS Server

Figure 5-5-3 Client List interface;

Index	MAC Address	IP Address	User Name	Lease Time(s)	Expired Time(s)
No matching records found					

Figure 5-5-4 Static Client Config interface;

static DHCP Config

DHCP Pool:

IP Address: For Example: 192.168.0.1

MAC Address: For Example: 00-01-02-03-04-05

DHCP Pool	IP Address	MAC Address	
No matching records found			

Table 5-5-4 Main elements of Static Client Config interface

Interface elements	Description
DHCP Pool	Select the DHCP address pool.
IP Address	Fill in the IP address to be bound.
MAC Address	Fill in the MAC address to be bound.

5.6 DHCP Relay

【Function Description】

If the DHCP client and the DHCP server are on the same physical network segment, the client can correctly obtain the dynamically allocated ip address. If they are not in the same physical network segment, a DHCP Relay Agent is required. The DHCP Relay agent can eliminate the need for a DHCP server in each physical network segment. It can deliver messages to DHCP servers that are not on the same physical subnet, or send messages from the server back to those that are not on the same physical subnet. Net’s DHCP client.

【Operation path】

Layer3 > dhcp relay

【Interface description】

Figure 5-6 DHCP relay interface

The screenshot displays the DHCP Relay configuration page. At the top, there is a header 'DHCP Relay'. Below it, the 'Enable DHCP Relay' option is shown as a toggle switch that is currently turned off, with a 'Set' button to its right. Underneath, the 'Interface' is selected via a dropdown menu. The 'DHCP Server' field is a text input box with an 'Add' button below it; a note 'For Example: 192.168.1.1' is placed to the right of the input field. At the bottom, a table with columns 'Index', 'Interface', and 'DHCP Server' is shown, containing the text 'No matching records found'.

Table 5-6 Main elements of the DHCP relay interface

Interface elements	Description
Enable DHCP Relay	Enable the DHCP Relay function.
Interface	Select the corresponding Layer 3 interface.
DHCP Server	Configure the server IP address.

5.7 RIP

【Function Description】

RIP is a protocol based on the Distance-Vector algorithm. It exchanges routing information through UDP packets and uses a port number of 520.

RIP uses the number of hops to measure the distance to the destination address, and the number of hops is called the metric value. In RIP, the number of hops from a router to the network directly connected to it is 0, the number of hops to reach another network through the router connected to it is 1, and the rest can be deduced by analogy. To limit the convergence time, RIP specifies that the metric value is an integer between 0 and 15. The number of hops greater than or equal to 16 is defined as infinity that is, the destination network or host is unreachable. Due to this limitation, RIP is not suitable for large-scale networks.

【Operation path】

Layer3 > RIP

【Interface description】

Figure 5-7-1 RIP Global Config interface

The screenshot shows the 'RIP Global Config' interface with the following settings:

- Enable RIP:**
- RIP Version:** tx: v2, rx: v1&v2
- Send Update Time:** 30 (range: 1-86400, Defaults: 30)
- Route Timeout Time:** 180 (range: 1-86400, Defaults: 180)
- Garbage Collect Time:** 120 (range: 1-86400, Defaults: 120)
- Suppress Interface Route Update:**
- Allow Equal Cost MultiPath:**
- Redistribute Section:**
 - Default Metric:** 1 (range: 1-16, Defaults: 1)
 - Redistribute Default Route:**
 - Redistribute Connected Route:**

Figure 5-7-2 RIP Network Config interface

The screenshot shows the 'RIP Network Config' interface with a table for adding networks:

No	Network
No matching records found	

There is an 'Add' button and a text input field for the network address (e.g., 10.1.1.0/24).

Figure 5-7-3 RIP Interface Config interface

The screenshot shows the 'RIP Interface Config' interface with the following table:

Interface	Enable RIP	Split Horizon	Send Version	Receive Version	Type of Certification	Auth Length	Authentication Characters
Select All	<input type="checkbox"/>	None	auto	auto	no auth		
vlanif1	<input type="checkbox"/>	Split Horizon	auto	auto	no auth	RFC Compatible	
vlanif20	<input type="checkbox"/>	Split Horizon	auto	auto	no auth	RFC Compatible	

An 'Apply' button is located at the bottom of the table.

Figure 5-7-4 RIP Route Info interface

The screenshot shows the 'RIP Route Info' interface with a table for displaying route information:

No	Destination Network	Route Type	Route Sub-Type	Next Hop	Metric	From	External Metric	Route Tag	Route remain time
No matching records found									

5.8 OSPF

【Function Description】

The full English name of OSPF is Open Shortest Path First (Open Shortest Path First). It is a link state routing protocol that uses bandwidth-based metrics. OSPF uses the SPF algorithm to calculate routes, which guarantees no routing loops algorithmically, maintains routes through neighbor relationships, and avoids bandwidth consumption for periodic updates. OSPF has high routing update efficiency and fast network convergence, which is suitable for large and medium-sized networks. On the "OSPF" page, you can configure OSPF parameters.

【Operation path】

Layer3 > OSPF

【Interface description】

Figure 5-8-1 OSPF Global Config interface

The screenshot shows the OSPF Global Config interface with the following elements:

- Enable OSPF:** A toggle switch currently set to 'Off'.
- Router ID:** A text input field with a placeholder example: 'For Example : 192.168.1.1'.
- Suppress Interface Route Update:** A toggle switch currently set to 'Off'.
- Redistribute Section:** A shaded header for the redistribution options.
 - Default Metric:** A text input field with the value '1' and a range of '0-16777214'.
 - Redistribute Default Route:** A toggle switch (Off), Metric Type dropdown (External Type 1), and Metric input field (range: 0-16777214).
 - Redistribute Connected Route:** A toggle switch (Off), Metric Type dropdown (External Type 1), and Metric input field (range: 0-16777214).
 - Redistribute Static Route:** A toggle switch (Off), Metric Type dropdown (External Type 1), and Metric input field (range: 0-16777214).
 - Redistribute RIP Route:** A toggle switch (Off), Metric Type dropdown (External Type 1), and Metric input field (range: 0-16777214).
- Apply:** A blue button at the bottom center.

Table 5-8-1 Main elements of OSPF Global Config interface

Interface elements	Description
Enable OSPF	Enable or disable OSPF.
Route ID	Fill in the router ID number.
Suppress Interface Route Update	Enable/disable.
Default Metric	Set the cost of importing external routes (range: 0-16777214)
Redistribute Default Route	Redistribute Default Route (range: 0-16777214)
Redistribute Connected Route	(range: 0-16777214)
Redistribute Static Route	(range: 0-16777214)
Redistribute RIP Route	(range: 0-16777214)

Figure 5-8-2 OSPF Network Config interface

Table 5-8-2 Main elements of OSPF Network Config interface

Interface elements	Description
Network	Fill in the routing network segment address and mask.
Area	Fill in the area information.

Figure 5-8-3 OSPF Interface Config interface

Table 5-8-3 Main elements of OSPF Interface Config interface

Interface elements	Description
interface	Display the interface name.
Network Type	Select the type of OSPF: P2P: Hello packets are sent to the multicast address 224.0.0.5, neighbors can be discovered automatically, DR/BDR is not elected, the default Hello timer is 10 seconds, and the Dead timer is 40 seconds. Broadcast: Hello packets are sent to the multicast address 224.0.0.5, neighbors can be automatically discovered, DR/BDR elections, the default Hello timer is 10 seconds, and the Dead timer is 40 seconds. NBMA: Hello packets are sent by unicast. Neighbors need to be manually specified. DR/BDR is not elected. By default, the Hello timer is 30 seconds and the Dead timer is 120 seconds. P2MP: Hello packets are sent to the multicast address 224.0.0.5, neighbors can automatically discover that they do not elect DR/BDR, the default Hello timer is 30 seconds, and the Dead timer is 120 seconds.

Area	Area Name
Cost	Cost
Router Priority	Priority, the default is 1, the range (0-255).
Hello Interval	The interval for sending hello packets, the default is 10s
Dead Interval	The number of seconds to wait for the Hello packet sent by the router to declare that the OSPF router has disappeared (shut down) without being seen by the neighbor. The default is 40s.
Retransmit Interval	Retransmit after failure, the default interval is 5s
Authentication type	Area-based authentication types: 1. No authentication; 2. Simple password authentication; 3. MD5 authentication. No authentication by default.
key	Fill in the authentication key value.

Figure 5-8-4 OSPF Area Config interface

OSPF Global Config	OSPF Network Config	OSPF Interface Config	OSPF Area Config	OSPF Neighbor Info	OSPF Route Info	
Area ID	Area Type	Summary	Default Cost	Type of Certification	Shortcutting Mode	Virtual Link
No matching records found						

Figure 5-8-5 OSPF Neighbor Info interface

OSPF Global Config	OSPF Network Config	OSPF Interface Config	OSPF Area Config	OSPF Neighbor Info	OSPF Route Info					
No	Neighbor ID	Router Priority	Neighbor State	Interface State	Dead Time	Neighbor Address	Area	Interface	Designated Router	Backup Designated Router
No matching records found										

Figure 5-8-6 OSPF Route Info interface

OSPF Global Config	OSPF Network Config	OSPF Interface Config	OSPF Area Config	OSPF Neighbor Info	OSPF Route Info					
Network Route Info										
No	Destination Network	Destination Type	Path Type	Cost	Area ID	Next Hop	Out Interface			
Border Router Info										
No	Destination Network	Destination Type	Path Type	Cost	Area ID	LSA Flag	Next Hop	Out Interface		
LSA Flag: ABR -- Area Border Router, ASBR -- Autonomous System Boundary Router.										
External Route Info										
No	Destination Network	Destination Type	Path Type	Cost	Type2 Cost	Route Tag	Next Hop	Out Interface		

5.9 RIPng

Figure 5-9-1 RIPng Global Config interface

RIPng Global Config | RIPng Network Config | RIPng Interface Config | RIPng Route Info

Enable RIPng

Send Update Time range : 1-86400 , Defaults : 30

Route Timeout Time range : 1-86400 , Defaults : 180

Garbage Collect Time range : 1-86400 , Defaults : 120

Allow Equal Cost MultiPath

Redistribute

Default Metric range : 1-16 , Defaults : 1

Redistribute Default Route

Redistribute Connected Route

Redistribute Static Route

Redistribute OSPFv3 Route

Figure 5-9-2 RIPng Network Config interface

RIPng Global Config | RIPng Network Config | RIPng Interface Config | RIPng Route Info

RIPng Enable Network

Network / For Example: 2134:3e::/64

No	Network
No matching records found	

Figure 5-9-3 RIPng Interface Config interface

RIPng Global Config | RIPng Network Config | RIPng Interface Config | RIPng Route Info

Interface	Enable RIPng	Split Horizon	Suppress Interface Route Update
Select All	<input type="checkbox"/>	None	<input type="checkbox"/>
vlanif1	<input type="checkbox"/>	Split Horizon	<input type="checkbox"/>
vlanif20	<input type="checkbox"/>	Split Horizon	<input type="checkbox"/>

Figure 5-9-4 RIPng Route Info interface

RIPng Global Config | RIPng Network Config | RIPng Interface Config | RIPng Route Info

No	Destination Network	Route Type	Route Sub-Type	Next Hop	Metric	From	Route Tag	Route remain time
No matching records found								

5.8 OSPFv3

Figure 5-10-1 OSPFv3 Global Config interface

Figure 5-10-2 OSPFv3 Interface Config interface

Figure 5-10-2 OSPFv3 Neighbor Info interface

Figure 5-10-3 OSPFv3 Route Info interface

LSA Flag: ABR -- Area Border Router, ASBR -- Autonomous System Boundary Router.

6. Multicast Management

6.1 IGMP Snooping

【Function Description】

IGMP Snooping is the abbreviation of Internet Groupmanagement Protocol snooping (Internet Multicast Management Protocol Detection), which is a multicast restriction mechanism running on Layer 2 devices to manage and control multicast groups. The Layer 2 device running IGMP snooping analyzes the received IGMP messages, establishes a mapping relationship between ports and MAC multicast addresses, and forwards multicast data according to this mapping relationship.

On the "IGMP Snooping Config" page, you can perform global configuration and static multicast configuration.

【Operation path】

Multicast > IGMP Snooping

【Interface description】

Figure 6-1-1 IGMP Snooping Global Config interface

IGMP Snooping Global Config | IGMP Snooping VLAN Config | IPv4 Static Multicast

Enable

Member Port Aging Time range: 200-1000(Default: 300)

Router Port Aging time Unit: seconds Range: 1-1000 (Default: 105)

Index	Vlan Id	Multicast Source Address	Multicast Group Address	Static Member Ports	Dynamic Member Ports(Aging time)
No matching records found					

Figure 6-1-2 IGMP Snooping VLAN Config interface

IGMP Snooping Global Config | IGMP Snooping VLAN Config | IPv4 Static Multicast

Vlan Id

Port Fast Leave

Query Source Address For Example: 192.168.1.254

Query Interval Unit: seconds Range: 2-300

Max Response Time Unit: seconds Range: 1-25 (default: 10)

Last-Member Query Interval Unit: seconds Range: 1-5 (default: 1)

Index	Vlan Id	Port Fast Leave	Query Source Address	Query Interval	Max Response Time	Last-Member Query Interval
No matching records found						

Figure 6-1-3 IPv4 Static Multicast Config interface

The interface includes the following configuration options:

- Vlan Id:** 1
- Multicast Source Address:** [Empty] For Example: 192.168.1.1
- Multicast Group Address:** [Empty] For Example: 225.1.2.3
- Port List:** A grid of 24 ports (G1-G24 and X1-X4) with a "Select All" checkbox.

Index	Vlan Id	Multicast Source Address	Multicast Group Address	Static Member Ports
No matching records found				

6.2 MLD Snooping

MLD Snooping global configuration: configure MLD monitoring enable and set MLD function attributes;

The interface includes the following configuration options:

- Enable:** [Checked]
- Member Port Aging Time:** 300 (range: 200-1000(Defaults: 300))
- Router Port Aging time:** 105 (Unit: seconds Range: 1-1000 (Default: 105))

Index	Vlan Id	Multicast Source Address	Multicast Group Address	Static Member Ports	Dynamic Member Ports(Aging time)
No matching records found					

MLD Snooping VLAN configuration: Configure static multicast VLAN;

The interface includes the following configuration options:

- Vlan Id:** 1
- Port Fast Leave:** [Checked]
- Query Source Address:** [Empty] For Example : fe80:fe00::1
- Query Interval:** 10 (Unit: seconds Range: 2-300)
- Max Response Time:** 10 (Unit: seconds Range: 1-25 (default: 10))
- Last-Member Query Interval:** 1 (Unit: seconds Range: 1-5 (default: 1))

Index	Vlan Id	Port Fast Leave	Query Source Address	Query Interval	Max Response Time	Last-Member Query Interval
No matching records found						

IPv6 static multicast: configure static multicast function, and enable port static multicast function;

MLD Snooping Global Config
MLD Snooping VLAN Config
IPv6 Static Multicast

Vlan Id

Multicast Source Address For Example : fe80:fe00::1

Multicast Group Address For Example : ff1E::01

Port List Select All

G2

G4

G6

G8

G10

G12

G14

G16

G18

G20

G22

G24

X2

X4

G1

G3

G5

G7

G9

G11

G13

G15

G17

G19

G21

G23

X1

X3

Index	Vlan Id	Multicast Source Address	Multicast Group Address	Static Member Ports
No matching records found				

6.3 IP Multicast

IP multicast global configuration: multicast routing is enabled;

IP Multicast Global Config
IP Multicast Interface Config

Enable Multicast Routing

IP multicast interface configuration:

IP Multicast Global Config
IP Multicast Interface Config

VIF name	VIF index	Module Name	TTL threshold	Local Address	Remote Address	VIF Uptime
Select All			<input style="width: 50px;" type="text"/>			

6.4 IGMP

IGMP global configuration: Configure the maximum number of IGMP group records, the range is 0-2097152, the default is 0,

IGMP Global Config
IGMP Interface Config
IGMP Static Group Config
IGMP Group Info

Max Group Record Num range : 0-2097152 , Defaults : 0

IGMP interface configuration:

Interface name	Enable IGMP	IGMP Version	Last Member Query Count	Last Member Query Interval(ms)	Max Group Record Num	Other-Querier Interval(s)	Query Interval(s)	Query Response Time(s)	Startup Query Count	Startup Query Interval(s)	Robustness Variable	RA Option Validation
Select All	<input type="radio"/>	3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="radio"/>
vlanif1	<input type="radio"/>	3	2	1000	0	255	125	10	2	31	2	<input type="radio"/>
vlanif20	<input type="radio"/>	3	2	1000	0	255	125	10	2	31	2	<input type="radio"/>

[Apply](#)

IGMP static group configuration,

IGMP Global Config	IGMP Interface Config	IGMP Static Group Config	IGMP Group Info								
Static Group Config Interface name: <input type="text" value="vlanif1"/> Multicast Group Address: <input type="text"/> For Example: 225.1.2.3 ssm-map: <input type="checkbox"/> Multicast Source Address: <input type="text"/> For Example: 192.168.1.1 <input type="button" value="Add"/>		Join Group Config Interface name: <input type="text" value="vlanif1"/> Multicast Group Address: <input type="text"/> For Example: 225.1.2.3 Multicast Source Address: <input type="text"/> For Example: 192.168.1.1 <input type="button" value="Add"/>									
<input type="button" value="Del"/>											
<input type="checkbox"/> <table border="1" style="width: 100%;"> <thead> <tr> <th>Interface name</th> <th>Group Type</th> <th>Multicast Group Address</th> <th>Multicast Source Address</th> </tr> </thead> <tbody> <tr> <td colspan="4" style="text-align: center;">No matching records found</td> </tr> </tbody> </table>				Interface name	Group Type	Multicast Group Address	Multicast Source Address	No matching records found			
Interface name	Group Type	Multicast Group Address	Multicast Source Address								
No matching records found											

IGMP group information:

IGMP Global Config	IGMP Interface Config	IGMP Static Group Config	IGMP Group Info										
Interface name	Group Address	Group Mode	Group Record Uptime	Group Record Expires	Last Reporter	Include Source Count	Exclude Source Count	Source Mode	Source Address	Source Record Uptime	V3 Expires	Forward	Source Type
No matching records found													
Flags: R - Remote, M - SSM Mapping, S - Static, L - Local													
Refresh													

7. Advance

7.1 QoS

【Function Description】

QoS (Quality of Service) refers to a network that can use various basic technologies to provide better service capabilities for specified network communications. It is a technology used to solve problems such as network delay and congestion. When the network is overloaded or congested, QoS can ensure that important services are not delayed or discarded, while ensuring the efficient operation of the network.

【Operation path】

Advance > QoS

【Interface description】

Figure 7-1-1 Global Config interface

The screenshot shows the 'Global Config' interface for QoS. It includes the following sections:

- Policy:** Radio buttons for SP (selected), RR, WRR, and DRR.
- Weight:** Input fields for W0, W1, W2, W3, W4, W5, W6, and W7, all set to 0. A 'Set' button is below.
- CoS-Queue Map:** A dropdown for CoS (0) and a dropdown for Queue (0), with a 'Set' button.
- Current Map:** A list of mappings: 0->0, 1->1, 2->2, 3->3, 4->4, 5->5, 6->6, 7->7.
- DSCP-CoS Map:** A dropdown for DSCP (0), a dropdown for New DSCP (0), and a dropdown for CoS (0), with a 'Set' button.
- DSCP-CoS Map (Grid):** A grid of mappings from DSCP to CoS, including: 0->0, 1->1, 2->2, 3->3, 4->4, 5->5, 6->6, 7->7, 8->8, 9->9, 10->10, 11->11, 12->12, 13->13, 14->14, 15->15, 16->16, 17->17, 18->18, 19->19, 20->20, 21->21, 22->22, 23->23, 24->24, 25->25, 26->26, 27->27, 28->28, 29->29, 30->30, 31->31, 32->32, 33->33, 34->34, 35->35, 36->36, 37->37, 38->38, 39->39, 40->40, 41->41, 42->42, 43->43, 44->44, 45->45, 46->46, 47->47, 48->48, 49->49, 50->50, 51->51, 52->52, 53->53, 54->54, 55->55, 56->56, 57->57, 58->58, 59->59, 60->60, 61->61, 62->62, 63->63.

Figure 7-1-2 Port Config interface

Port	Default CoS	Trust Mode
Select All	0	Trust CoS
G1	0	Trust CoS
G2	0	Trust CoS
G3	0	Trust CoS
G4	0	Trust CoS
G5	0	Trust CoS
G6	0	Trust CoS
G7	0	Trust CoS
G8	0	Trust CoS
G9	0	Trust CoS
G10	0	Trust CoS

Table 7-1-2 Main elements of Port Config interface

Interface elements	Description
Port	Show port number
Default cos	Configure the default priority. The default is 0 (0-7). The larger the value, the higher the priority.
Trust Mode	1 Cos, 2 dscp, 3 all (when all is selected, dscp is effective, and dscp has a higher priority than cos).

7.2 ACL

【Function Description】

ACL, Access Control List, access control list. ACL is the function of packet filtering by configuring matching rules and processing operations on packets. The ACL rules applied on the port analyze the fields of the packet, and after identifying a specific packet, it is based on a preset operation (Allow/Prohibit Passing, Speed Limiting, Redirection, Port Closing, etc.) for corresponding processing. On the "ACL Configuration" page, you can match the protocol fields of the L2-L4 layer of the data packet. By defining the time period, you can set the effective time of ACL rules. Configure MAC ACL and IP ACL to process data packets that match ACL rules.

【Operation path】

Advance > ACL

【Interface description】

Figure 7-2-1 MAC ACL Config interface

The screenshot shows the 'MAC ACL CONFIG' interface with the following configuration fields:

- Entry ID:** Input field with a range of 0-31.
- Rule ID:** Input field with a range of 0-127.
- Action:** Dropdown menu set to 'deny'.
- Source MAC:** Input field with a hint: 'For example: 02-02-03-04-05-06, do not fill, that "any"'
- Source MAC MASK:** Input field with a hint: 'For example: fc-ff-ff-00-00-00, do not fill, that "any"'
- Destination MAC:** Input field with a hint: 'For example: 02-02-03-04-05-06, do not fill, that "any"'
- Destination MAC Mask:** Input field with a hint: 'For example: fc-ff-ff-00-00-00, do not fill, that "any"'
- Time-Range Name:** Dropdown menu with a hint: 'It is empty, indicating that it is effective anytime'

Below the configuration fields is an 'Add' button and a table with the following columns: Entry ID, Rule ID, Action, Source MAC, Destination MAC, and Time-Range. The table currently displays 'No matching records found'.

Table 7-2-1 Main elements of MAC ACL Config interface

Interface elements	Description
Entry ID	Enter the ACL group number to be configured, the value range is 1-99.
Rule ID	Enter the rule number, the value range is 1-127.
Action	Select how the switch handles data packets that meet the matching rules. Deny means discarding data packets, and permit means forwarding data packets.
Source MAC	Enter the source MAC address information included in the rule.
Source MAC MASK	Enter the source MAC address mask information included in the rule.
Destination MAC	Enter the destination MAC address information included in the rule.
Destination MAC Mask	Enter the destination MAC address mask information included in the rule.
Time-Range Name	

Figure 7-2-2 IP ACL Config interface

MAC ACL CONFIG
IP ACL CONFIG
Time Range Config
ACL GROUP CONFIG

Entry ID

Rule ID

Action

Protocol

Source IP

Source mask

Source Port

Destination IP

Purpose mask

Destination Port

Time-Range Name

range : 0-31

range : 0-127

For example: .xxx.xxx.xxx.xxx, do not fill, that "any"

For example: .xxx.xxx.xxx.xxx, do not fill, that "any"

Range: 0-65535, is empty, meaning any port

For example: .xxx.xxx.xxx.xxx, do not fill, that "any"

For example: .xxx.xxx.xxx.xxx, do not fill, that "any"

Range: 0-65535, is empty, meaning any port

It is empty, indicating that it is effective anytime

Entry ID	Rule ID	Action	Protocol	Source IP	Source mask	Source Port	Destination IP	Purpose mask	Destination Port	Time-Range
No matching records found										

Table 7-2-2 Main elements of IP ACL Config interface

Interface elements	Description
Entry ID	Enter the ACL group number to be configured, the value range is 100-999.
Rule ID	Enter the rule number, the value range is 1-127.
Action	Select how the switch handles data packets that meet the matching rules. Deny means discarding data packets, and permit means forwarding data packets.
Protocol	Select the switch data transmission rule.
Source IP	Enter the source IP address information.
Source mask	Enter the mask of the source IP address, the mask is set to 1 to indicate a strict match.
Source Port	Enter the TCP/UDP source port number.
Destination IP	Enter the destination IP address information.
Destination mask	Enter the mask of the destination IP address. Set the mask to 1 to indicate a strict match.
Destination Port	Enter the TCP/UDP destination port number.
Time-Range Name	

Figure 7-2-3 Time Range Config interface

The screenshot shows the 'Time Range Config' interface with the following elements:

- Navigation tabs: MAC ACL CONFIG, IP ACL CONFIG, **Time Range Config**, ACL GROUP CONFIG
- ADD Time Range** section:
 - Name: Input field with an 'Add' button.
- Config the time** section:
 - Time-Range Name: Dropdown menu with a 'Del' button.
 - Start Time: Input field with format 'yyyy-MM-dd HH:mm'.
 - End Time: Input field with format 'yyyy-MM-dd HH:mm'.
 - Time: Input field with format 'HH:mm - HH:mm'.
 - Week: Radio buttons for 'Absolute' (selected) and 'Periodic'. Below are checkboxes for days of the week: Sun, Mon, Tue, Wed, Thu, Fri, Sat.
 - 'Add' button at the bottom.
- Table below:

Name	State	Time
No matching records found		

Figure 7-2-4 ACL GROUP CONFIG interface

Port	MAC access list ID	IP access list ID
G1		
G2		
G3		
G4		
G5		
G6		
G7		
G8		
G9		
G10		

7.3 SNMP

【Function Description】

SNMP is currently the most widely used network management protocol in UDP/IP networks. It provides a management framework to monitor and maintain Internet devices.

SNMP network elements are divided into two types: NMS and Agent:

NMS (Network Management Station) is a workstation running SNMP client programs, which can provide a very friendly human-computer interaction interface to facilitate network administrators to complete most network management tasks.

Agent is a process that resides on the device and is responsible for receiving and processing request messages from NMS. In some emergency situations, such as interface status changes, the Agent will also notify the NMS.

NMS is the manager of SNMP network, and Agent is the managed person of SNMP network. NMS and Agent exchange management information through SNMP protocol.

SNMP provides four basic operations:

Get operation: NMS uses this operation to query the value of one or more objects of the Agent.

Set operation: NMS uses this operation to reset the value of one or more objects in the Agent database (MIB, Management Information Base).

Trap operation: The agent uses this operation to send alarm information to the NMS.

Inform operation: NMS uses this operation to send alarm information to other NMSs.

SNMP protocol version: Currently, the SNMP Agent of the device supports SNMP v2c version and is compatible with SNMP v1 version.

SNMP v1 uses community name (Community Name) authentication. The community name is used to define the relationship between SNMP NMS and SNMP Agent. If the community name carried in the SNMP packet is not recognized by the device, the packet will be discarded. The community name plays a role similar to a password and is used to restrict the SNMP NMS's access to the SNMP Agent.

SNMP v2c also uses community name authentication. It is compatible with SNMP v1 while expanding the functions of SNMP v1: it provides more operation types (GetBulk and

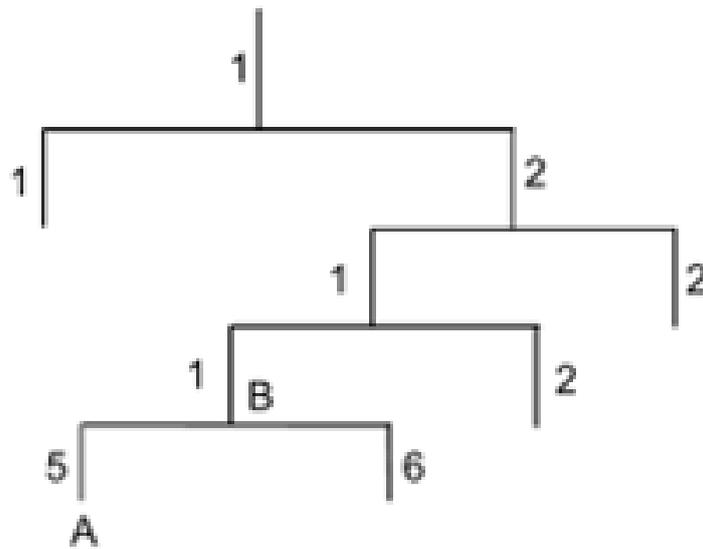
InformRequest); it supports more data types (Counter64, etc.); it provides richer error codes, Can distinguish errors in more detail.

Introduction to MIB:

Any managed resource is represented as an object, called a managed object. MIB (Management Information Base (Management Information Base) is a collection of managed objects. It defines a series of attributes of the managed object: the name of the object, the access rights of the object, and the data type of the object. Each agent has its own MIB. The NMS can perform read/write operations on the objects in the MIB according to the permissions. The relationship between NMS, Agent and MIB is shown in the figure below:



MIB is stored in a tree structure. The nodes of the tree represent managed objects, which can be uniquely identified (OID) by a path from the root. As shown in the figure below, the managed object B can be uniquely identified by a string of numbers {1.2.1.1}, which is the OID (Object Identifier) of the managed object.



【Operation path】

Advance > SNMP

【Interface description】

Figure 7-3-1 SNMP Global Config interface

The interface features a top navigation bar with four tabs: 'Information' (selected), 'Group', 'V3 User', and 'Alarm'. Below the tabs is a main configuration area with a header 'SNMP System'. The configuration includes: 'Enable' (a blue toggle switch), 'versions' (set to 'V1, V2C, V3'), 'System Name' (text input field), 'Location Information' (text input field), 'Contact Information' (text input field), 'Engine Number' (text input field), 'Trap Config' (a greyed-out section), and 'Start Up' (a greyed-out toggle switch). A blue 'Apply' button is located at the bottom right of the configuration area.

Figure 7-3-2 SNMP Group Config interface

The interface features a top navigation bar with four tabs: 'Information', 'Group' (selected), 'V3 User', and 'Alarm'. Below the tabs is a main configuration area with a header 'SNMP Community Config'. The configuration includes: 'Name' (text input field), 'Community Attributes' (dropdown menu showing 'rocommunity'), and an 'Add' button. Below the configuration area is a table with two columns: 'Name' and 'Community Attributes'. The table contains two rows: one for 'public' with 'rocommunity' and one for 'private' with 'rwcommunity'. Each row has a 'Del' button to its right.

Name	Community Attributes	
public	rocommunity	Del
private	rwcommunity	Del

Figure 7-3-3 SNMP v3 User Config

Information | Group | **V3 User** | Alarm

V3 User Config

Name:

User Attribute:

Certification Information:

Encrypt information:

Index	Name	User Attribute	Authentication Mode	Authentication password	Encryption mode	Encryption password
1	admin	rouser				
2	admin	rwuser				

Figure 7-3-4 SNMP Alarm Config interface

Configure the TRAP trap receiving address and the corresponding SNMP protocol version;

Information | Group | V3 User | **Alarm**

Trap Config

Address:

versions:

Address	versions
0.0.0.0	V1
0.0.0.0	V2C

7.4 RMON

Figure 7-4-1 Event Group Config interface

Event group: query and add event groups monitored remotely;

Event Group | Statistics Group | History Group | Alarm Group

Index: Event group number: 0-1024 (delete, just fill in this item)

Description:

Action:

Index	Description	Action	Recent Time
No matching records found			

Figure 7-4-2 Statistics Group Config interface

Statistics group: query the statistics information of a specific event after the interruption;

Event Group **Statistics Group** History Group Alarm Group

Index Event group number: 0-1024 (delete, just fill in this item)

Port

Add

Index	Name
No matching records found	

Figure 7-4-3 History Group Config interface

History group: Add to query the history records of specific events when they occur on the port;

Event Group Statistics Group **History Group** Alarm Group

Index Event group number: 0-1024 (delete, just fill in this item)

Sample Port

sampling Interval range : 5-65535(Seconds)

Max Sample Number Max Sample Number : 0-100

Add

Index	Sample Port	sampling Interval	Number Samples
No matching records found			

Figure 7-4-4 Alarm Group Config interface

Alarm group: add the attributes of the alarm event to be queried on the port;

Event Group Statistics Group History Group **Alarm Group**

Index Event group number: 0-1024 (delete, just fill in this item)

Sample Port

Alarm Parameters

sampling Interval range : 5-65535(Seconds)

Sampling Type

Rising Edge Threshold range : 0-4294967295

Falling Edge Threshold range : 0-4294967295

Rising Edge Event Event group index, when the alarm is triggered, the corresponding event of the event group will be activated, Range: 0-1024

Falling Event Event group index, when the alarm is triggered, the corresponding event of the event group will be activated, Range: 0-1024

Add

Index	Sample Port	Alarm Parameters	sampling Interval	Sampling Type	Rising Edge Threshold	Falling Edge Threshold	Rising Edge Event	Falling Event
No matching records found								

7.5 LLDP

Figure 7-5-1 LLDP Global Config interface

Global configuration: enable and configure the LLDP function;

Figure 7-5-2 Port Config interface

Port configuration: configure port LLDP function attributes;

Port	tx	rx
Select All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
G1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
G2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
G3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
G4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
G5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
G6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
G7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
G8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
G9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
G10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
G11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
G12	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 7-5-3 LLDP Neighbor Information Interface

LLDP neighbor: query LLDP neighbor information;

Index	Chassis-ID	PortID	Holdtime	Port Description	System Name	System Description	System Capability	Manage Address	Local Port	vlan id
1	MAC: 00:00:00:00:61:35	Locally Assigned - 4	120	Port #4		SMBStaX (standalone) 2019-09-02T13:11:58+08:00 R2.03 2019-09-02T13:11:58+08:00	Bridge/Switch (enabled)	192.168.10.200	G6	1

7.6 NTP

【Function Description】

On the "NTP Config" page, you can configure the NTP server address to synchronize the switch system time with the server.

【Operation path】

Advance > NTP

【Interface description】

Figure 7-6-1 NTP Global Config interface

Global configuration: configure NTP function enable, time zone selection and modification of check time interval;

The screenshot shows the 'NTP Global Config' interface. At the top, there are two tabs: 'NTP Global Config' (selected) and 'NTP Server Config'. The main area contains three settings: 'Mode' with a toggle switch currently turned off; 'Time Zone Settings' with a dropdown menu showing '(GMT+08:00) Irkutsk Ul'; and 'Time Interval' with a text input field containing '300'. To the right of the 'Time Interval' field, it says 'Second / time range: 5-65535 Defaults: 300'. At the bottom center, there is a blue 'Apply' button.

Figure 7-6-2 NTP Server Config interface

NTP server configuration: configure the NTP server address and view the NTP server status;

The screenshot shows the 'NTP Server Config' interface. At the top, there are two tabs: 'NTP Global Config' and 'NTP Server Config' (selected). The main area contains a 'Server' text input field, an 'Add Server' button, and a note 'For Example: 202.112.29.82'. Below this is a section titled 'Commonly used server' with a list of server names and their IP addresses:

Commonly used server	IP Address 1	IP Address 2
China	120.25.108.11	202.112.29.82
America	158.69.48.97	216.218.254.202
Singapore	202.73.57.107	218.186.3.36
Germany	46.4.106.197	141.82.25.203
India	162.159.200.1	157.119.108.165
Iran	77.104.104.100	194.225.150.25
Brazil	188.165.236.162	200.160.0.8

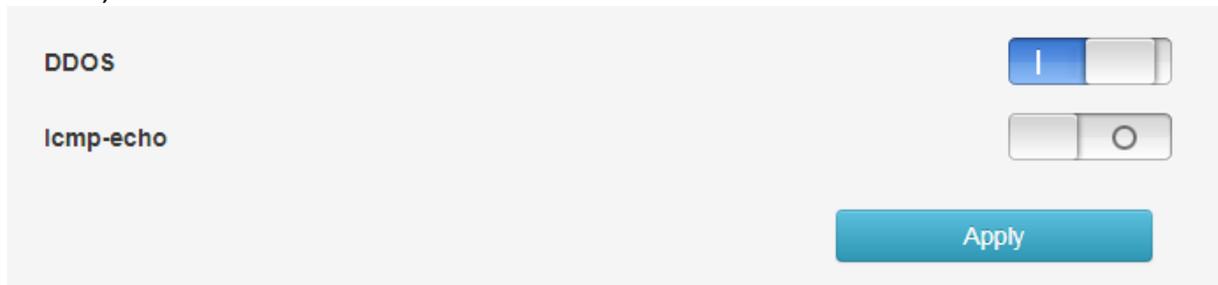
Below the list is a table with the following structure:

Index	Server	State
No matching records found		

7.7 Secure

Figure 7-7-1 Scure configuration interface

Distributed denial of service attack (DDOS) and anti-PING function (Icmp-echo) can be turned on;



The screenshot shows a configuration panel with two toggle switches. The first switch is labeled "DDOS" and is currently turned on (blue bar on the left). The second switch is labeled "Icmp-echo" and is currently turned off (white bar on the left). Below the switches is a blue "Apply" button.

8. System Management

8.1 User Config

【Function Description】

On the "User Config" page, you can configure the user name, password, and permissions for logging in to the switch's WEB interface.

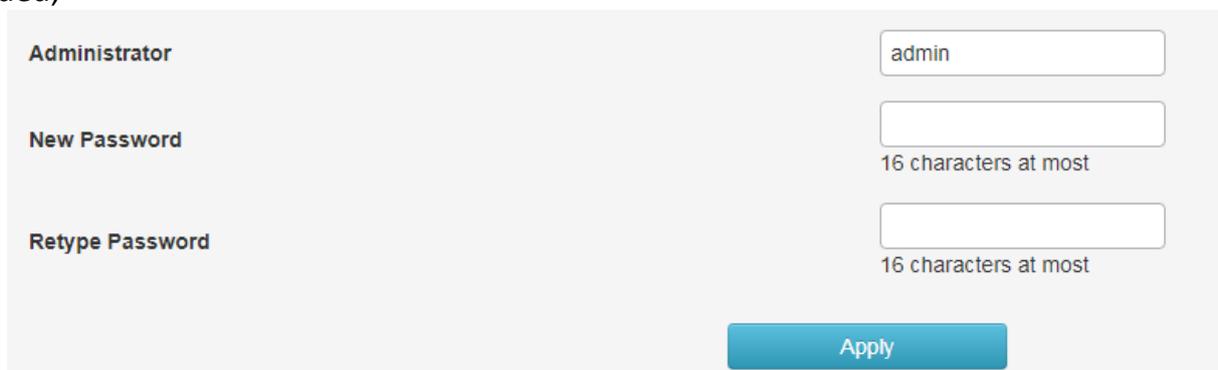
【Operation path】

System > User

【Interface description】

Figure 8-1 User Config interface

Modify the user's login password, the account name cannot be changed nor can the user be added;



The screenshot shows a configuration form with three input fields. The first field is labeled "Administrator" and contains the text "admin". The second field is labeled "New Password" and is empty, with the text "16 characters at most" below it. The third field is labeled "Retype Password" and is empty, with the text "16 characters at most" below it. Below the fields is a blue "Apply" button.

8.2 Network

【Function Description】

The management IP address of the switch can be configured on the "Network" page.

【Operation path】

System > Network

【Interface description】

Figure 8-2-1 IPv4 Config interface

IPV4 configuration: modify the IPV4 address of the switch, you cannot add an IP address;

IPv4 Config IPv6 Config

Manage Interface

IPv4 Address For Example : 10.0.0.2/24

Default Gateway For Example : 10.0.0.1

Preferred DNS Server For Example : 10.0.0.1

Alternative DNS Server For Example : 10.0.0.1

Apply

Figure 8-2-2 IPv6 Config interface

IPV6 configuration: Modify the IPV6 address of the switch, but also cannot add the IPV6 address;

IPv4 Config IPv6 Config

Manage Interface

IPv6 Address For Example : fe80:fe00::1/64

Default Gateway For Example : fe80:fe00::1

Apply

8.3 Service Config

Figure 8-3-1 Service Config interface

Configure the switch Telnet, SSH, HTTP version protocol and service port;

The Service Config interface includes the following fields and controls:

- Telnet Service:** A toggle switch that is currently turned on.
- TELNET Port:** A text input field containing the value 23.
- SSH Service:** A toggle switch that is currently turned on.
- SSH Port:** A text input field containing the value 22.
- HTTP Service:** A dropdown menu currently set to HTTP.
- HTTP Port:** A text input field containing the value 80.
- Apply:** A blue button at the bottom right to save the configuration.

8.4 Configuration management

Used to reset, upload and download switch configuration;

The Configuration management interface includes the following controls:

- Restore factory settings:** A blue button to reset the switch to its default state.
- Upload Config:** A section containing a "Choose File" button, the text "No file chosen", and an "Upload" button.
- Download Config:** A blue button to retrieve the current configuration from the switch.

8.5 Firmware Upgrade

Used to upgrade the firmware version currently used by the switch;

The Firmware Upgrade interface includes the following fields and controls:

- Product Model:** A text input field containing the value YH6824GST4-SFP.
- Hardware Version:** A text input field containing the value V1.
- Firmware Version:** A text input field containing the value V1.0.0.1-gd06e45122.
- New Firmware File:** A section containing a "Choose File" button and the text "No file chosen".
- Upload:** A blue button at the bottom right to initiate the firmware upgrade process.

8.6 Diagnostic

Ping detection: Use the ping function of the switch to detect whether the link between the switch itself and other IP devices is reachable;

Ping Detection Tracert Detection Cable Detection

IP Address

```
PING 192.168.10.200 (192.168.10.200): 56 data bytes
64 bytes from 192.168.10.200: seq=0 ttl=64 time=2.761 ms
64 bytes from 192.168.10.200: seq=1 ttl=64 time=0.797 ms
64 bytes from 192.168.10.200: seq=2 ttl=64 time=0.804 ms
64 bytes from 192.168.10.200: seq=3 ttl=64 time=0.807 ms

--- 192.168.10.200 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.797/1.292/2.761 ms
```

Tracert detection: Traceroute;

Ping Detection Tracert Detection Cable Detection

IP Address

```
traceroute to 192.168.10.200 (192.168.10.200), 30 hops max, 38 byte packets
 1  192.168.10.200 (192.168.10.200)  0.509 ms  0.347 ms  0.344 ms
```

Ethernet cable detection: detection of all network port cable properties of the switch

Ping Detection Tracert Detection Cable Detection

Cable Detection: ▼

8.7 Restart

Reboot the switch

Restart

This is a Class A product. In home environment, this product may cause radio interference. In this case, the user may be required to take appropriate measures.

Hereby Assmann Electronic GmbH, declares that the Declaration of Conformity is part of the shipping content. If the Declaration of Conformity is missing, you can request it by post under the below mentioned manufacturer address

www.assmann.com
ASSMANN Electronic GmbH
Auf dem Schüffel 3
58513 Lüdenscheid, Germany

