AVCOMM Technologies Inc.

7028GX12 Industrial Ethernet Managed Switch

User Manual

Contents

1 Summary

The Instructions mainly describe the simple configuration for WEB page operation of the switch, and users can manage the switch through the WEB page of the switch. The main features of WEB access are:

- Easy to access: users can easily access the switch anywhere from the network.
- Users can access WEB pages of the switch with their familiar browsers such as Microsoft Internet Explorer, etc., and WEB pages are presented to users in graphical and tabular forms.
- The switch provides rich WEB pages through which users can configure and manage most of the switch's functions.
- The classification and integration of the WEB page functions is convenient for users to find the relevant pages for configuration and management.

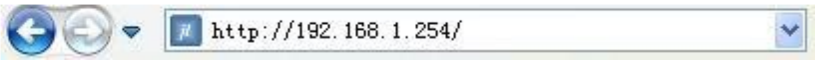
Explanation

1. Please use the Internet Explorer browser above version 8.0
2. When you log in the switch and set or change the Web page, you should pay attention to save and click the "save configuration" under the "system maintenance". Otherwise, your setup or change will not be saved after the switch is restarted.

2 Login the Web Page

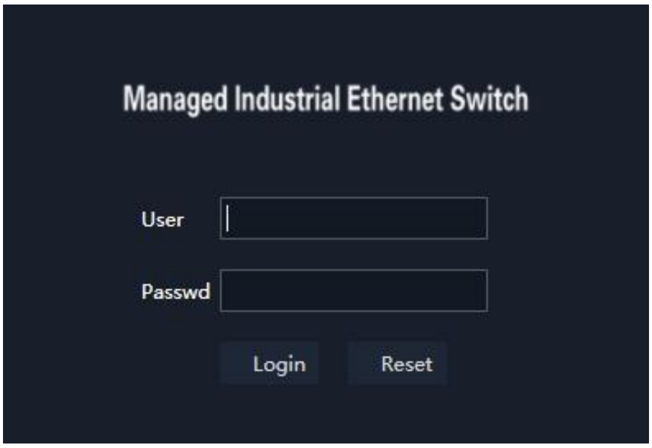
2.1 Login the Web network management client

By opening the Web browser, users can enter the default address of the switch in the address bar: http://192.168.1.254, and press the Enter key, as shown in the following figure:



http://192.168.1.254/

The login window is popped at this time, as shown in the following figure. Enter the default management username: admin and password admin, click the <login> button, you will see the switch's system information.

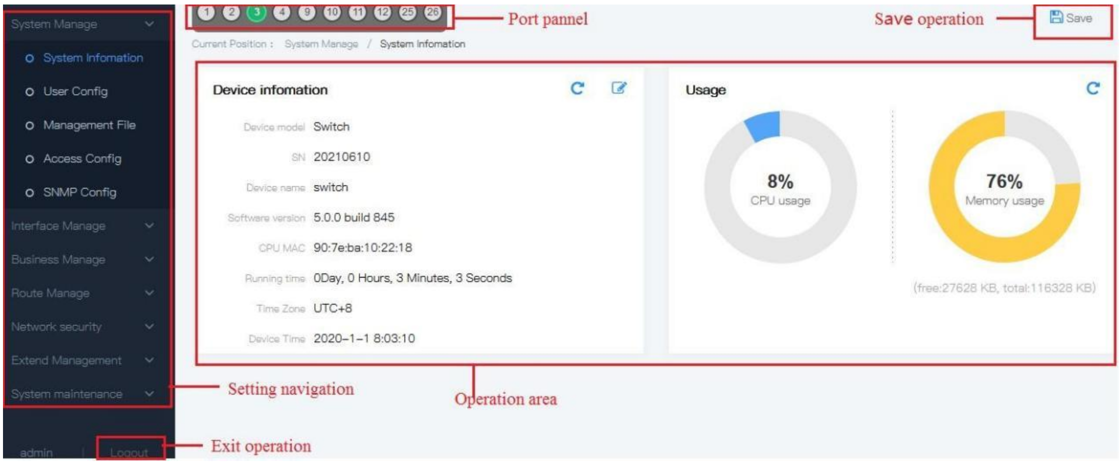


Explanation

1. When you log in a switch, the IP segment of the PC should be consistent with the switch network segment.
2. When you log in a switch for the first time, set the IP address of PC to be 192.168.1.x (x represents 1~254, except 254), the subnet mask to be 255.255.255.0, but the IP of PC can't be the same as that of the switch, that is, it cannot be 192.168.1.254.
3. The WebServer of the switch provides 5 times to enter username and password. If you enter incorrectly for 5 times, the browser will display "Bad passwords ,too many failures ,wait ten minuts" error information. The user need to wait ten minutes , and enter the correct username and password; after logging in the WebServer, it is recommended to modify the username and password.

2.2 Client interface composition

The client of the Web network management system is as shown in the following figure, which contains the setting navigation and operation areas.



Device infomation

Device model Switch
SN 20210610
Device name switch
Software version 5.0.0 build 845
CPU MAC 90:7e:ba:10:22:18
Running time 0Day, 0 Hours, 3 Minutes, 3 Seconds
Time Zone UTC+8
Device Time 2020–1–1 8:03:10

(free:27628 KB, total:116328 KB)

Area	**Explanation**
Port pannel	Port status
Setting navigation	The corresponding navigation can be selected for all operating functions
Exit operation	Click the icon to return to the login interface
Operation area	Specific settings and operations for all functional modules

2.3 Web interface navigation tree

The menu of Web network management mainly provides 6 menu items such as system manage, interface manage, business manage, route manage, network security, and system maintenance. There are submenus under each menu option, as shown in the following table.

Menu item	**Submenus**	**Explanation**
System manage	System information	Display product information & running information
	Management file	Save configuration, restore factory Settings and download and upload configuration files
	User config	Config user name, password, limitation
	Access config	Enable/disable TELNET service, configuration of HTTP/HTTPS service
	SNMP config	Provide configuration for SNMP
Interface manage	Port management	Configuration for port rate, flow control
	Storm contorl	Support the storm control of the broadcast, unknown multicast and unknown single broadcast, prevent the broadcast storm of these three types of messages
	Port-rate limit	Provide configuration for port rate
	Mirror	Provide configuration for port mirror
	LACP	Provide configuration for LACP
	Isolate-port config	Provide configuration for layer 2 port isolation

	Port statistics	Provide query port profiles and detailed statistics
Business manage	VLAN configuration	Provide the functions of configuring and querying VLAN, interface information
	MAC configuration	Provide the functions of configuring and querying the MAC address table information, MAC aging time, MAC learning and static MAC
	Spanning-tree configuration	Provide the functions of configuring and querying the device STP global configuration, instance configuration, instance configuration management and configuration management.
	ERPS-Ring Config	ERPS Ring Config
	RING Config	ring config
	IGMP-snooping config	Provide the functions of configuring and querying the IGMP Snooping configuration and static multicast
	MLD-snooping Config	IPv6 multicast address listening is provided
	QOS config	Provide the functions of configuring and querying QOS global configuration and configuration management
	LLDP config	Provide the functions of configuring and querying QOS global configuration, configuration management and LLDP neighbors
	UDLD Config	Single pass link detection function
	Link-flap-config	Link oscillation detection function
	DHCP Server config	Provides configuration for DHCP Server, address pool, client list, static client configuration, and port binding
Route manage	L3 interface	L3 interface configuration
	Check route	Check all the route information
	Static configuration	Provide the functions of static route configuration
	RIP configuration	Provide the functions of RIP route configuration
	OSPF configuration	Provide the functions of OSPF route configuration
	VRRP configuration	Provide the functions of VRRP route configuration
	ARP configuration	Provide the functions of ARP route configuration
	ND-config	
	NQA-config	
Network security	Access config	Provide filter rules and device access rules configuration
	Attack protection	Provide attack protection configuration function
	ACL config	Provide ACL config function
	Traffic monitor	Monitor data of each interface entry
	Alarm config	Configation for power, port alarm
	802.1X config	Provide configuration and query functions of global

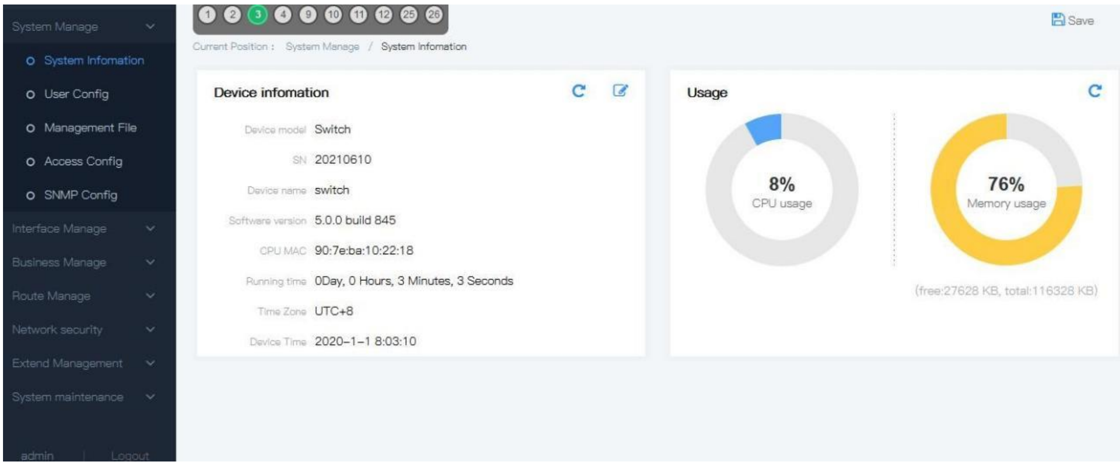
		802.1x authentication configuration and Radius server configuration
	onvif-config	Onvif device information display
	QINQ-config	QINQ function setting
	Time Range Config	Time period setting
	Devices-config	Connected device information display
	VOIP-config	Voip Connected device information display
System maintenance	NTP config	Provide configuration & NTP server checking function
	Log config	Display the log of the device
	diagnostic	Porvide Ping, Traceroute, port circuit function
	Reboot device	Reboot the switch
	Online upgrading	Upgrade the software version of the switch

3 System manage

3.1 System information

3.1.1Interface description

The panel display area of Web network management can display the product information of the switch very intuitively, according to the switch connected to it. Its display contents include ports quantity, ports condition, system information, version information and running status. The interface is shown as the following figure:



Device model Switch
SN 20210610
Device name switch
Software version 5.0.0 build 845
CPU MAC 90:7e:ba:10:22:18
Running time 0Day, 0 Hours, 3 Minutes, 3 Seconds
Time Zone UTC+8
Device Time 2020–1–1 8:03:10

Explanation

Click one of the ports, it shows the port number, type, transmission rate and status. You can modify "Device name", "Device time", and click "Submit" to complete the configuration

3.1.2Explanations

Configuration item	Meaning
Device model	Model number
Device name	Network identification used by devices to facilitate the judgment by integrated management tools
Hardware version	Display the hardware vesrsion of the device, pls pay attention on the hardware limitation from the software version
Software version	Display the version and release time of the current software
Running time	Current device running time
CPU usage	CPU running information
Memory usage	Memory running information
CPU MAC	MAC address of the device

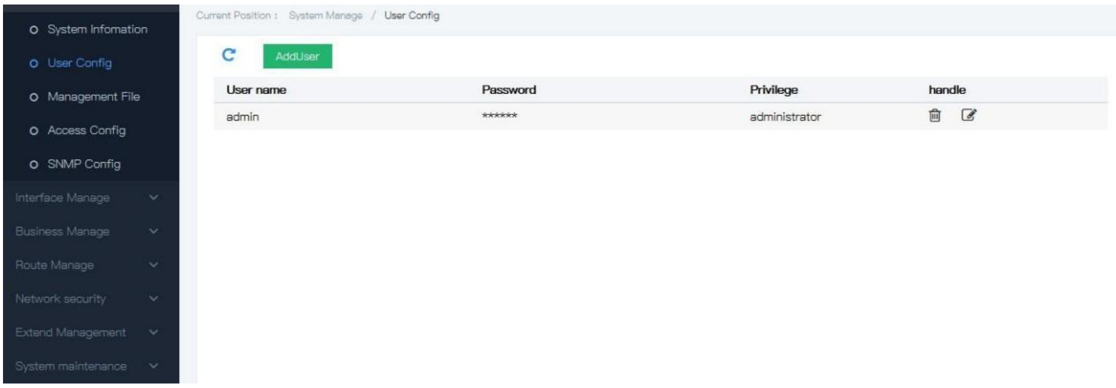
3.1.3Operation steps

Step 1	Click the "System configuration" menu in the navigation bar to enter the "System configuration" interface. Click "System information".
Step 2	You can carry out Device name, time related modification settings. Click "Submit" to complete settings after modification.
Step 3	If you need to make it as a startup configuration, you need to enter "System maintenance" and save it under "Save settings".

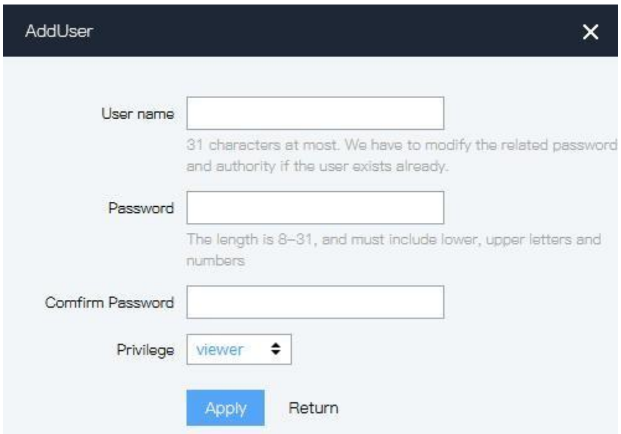
3.2 User management

3.2.1Interface description

The user can view the current username and permissions of the switch, and modify the username, password and permissions. The interface is shown as the following figure



User name	Password	Privilege	handle
admin	******	administrator	🗑 ✎



User name

31 characters at most. We have to modify the related password and authority if the user exists already.

Password

The length is 8–31, and must include lower, upper letters and numbers

Comfirm Password

Privilege: viewer

3.2.2Explanations

Configuration item	Meaning
User name	Display the username of the access system. The username can’t be empty or contain characters.
Password	The password to manage the user. The password can’t be empty or contain characters.
Permission	It divided into the administrator permission – Administrator, and the

	ordinary user permission – Viewer .

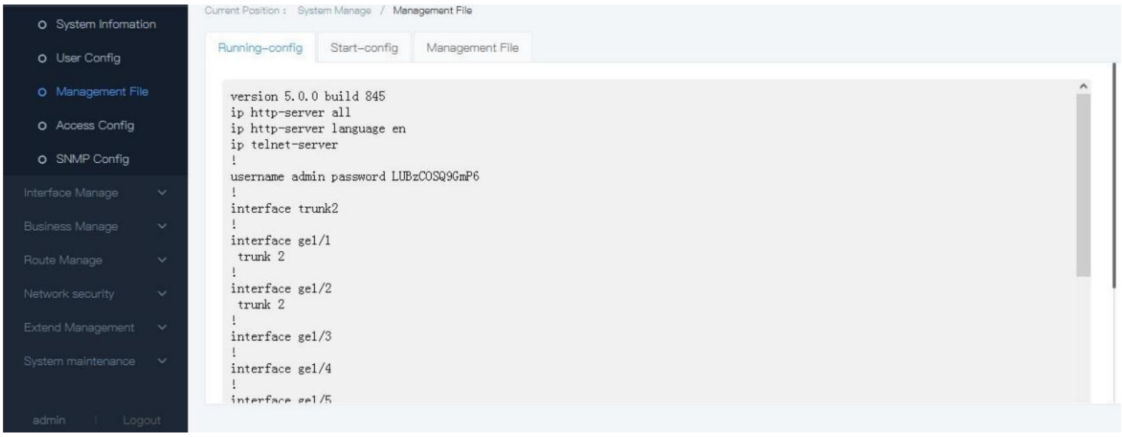
3.2.3Operation steps

Step 1	Click the "System configuration" menu in the navigation bar to enter the "System configuration" interface. Click the "User management" tab, and you can see the default username: admin, password: admin
Step 2	If a user needs to submit a new user, click "Add user". If a user needs to delete a username, click "Delete".
Step 3	If you need to make it as a startup configuration, you need to enter “System maintenance” and save it under “Save settings”.

3.3 Configuration Management

3.3.1 Management file

The user can view the current running configuration. Click the "System manage" menu in the navigation bar to enter the "System manage" interface. The interface is shown as the following figure

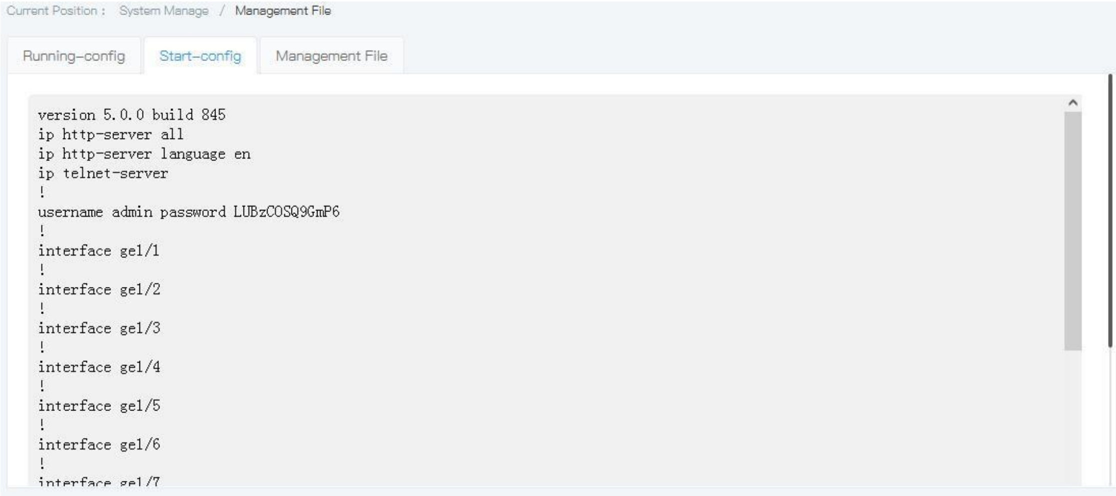


```
version 5.0.0 build 845
ip http-server all
ip http-server language en
ip telnet-server
!
username admin password LUBzCOSQ9GmP6
!
interface trunk2
!
interface gel/1
 trunk 2
!
interface gel/2
 trunk 2
!
interface gel/3
!
interface gel/4
!
interface gel/5
```

If you need to make it as a startup configuration, you need to save it under "Save settings"

3.3.2 The start config

If you need to make it as a startup configuration, click the "System manage" menu in the navigation bar to enter the "System manage" interface, and save it under “Save settings”. The interface is shown as the following figure

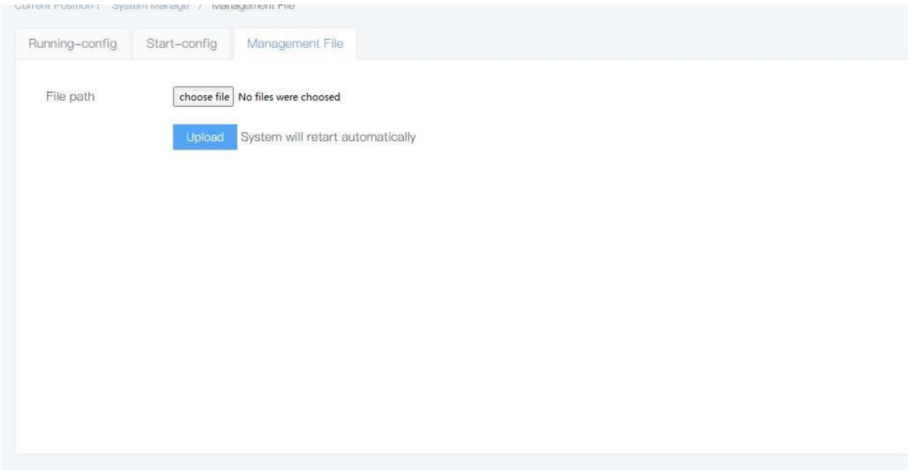


```
version 5.0.0 build 845
ip http-server all
ip http-server language en
ip telnet-server
!
username admin password LUBzCOSQ9GmP6
!
interface ge1/1
!
interface ge1/2
!
interface ge1/3
!
interface ge1/4
!
interface ge1/5
!
interface ge1/6
!
interface ge1/7
```

If you need to make the factory default as a startup configuration, you need to click restore, and then reboot the device. User also can download the startup configuration file by click “download” to get the “.con” file.

3.3.3 Management file

The user can view the current running configuration. Click the "Management file" menu in the navigation bar to enter the interface. The interface is shown as the following figure



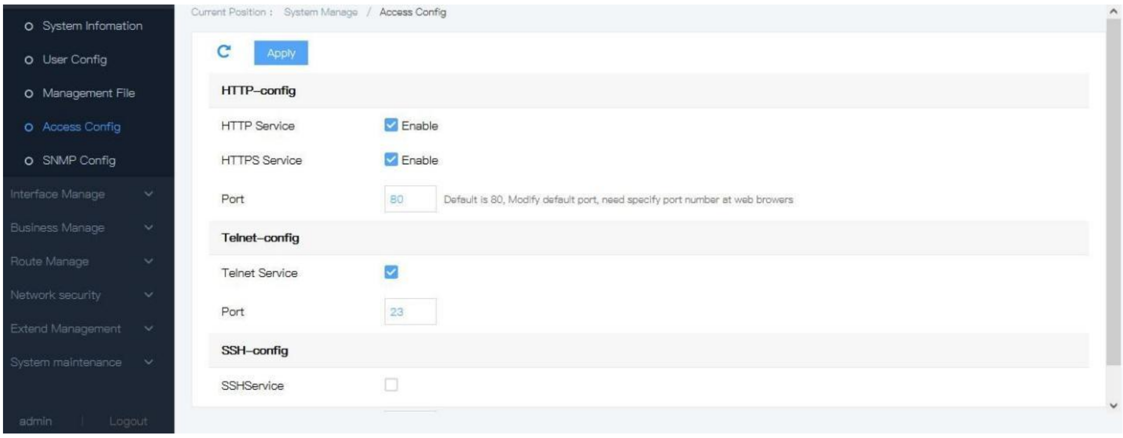
If you need to make it as a startup configuration, you need to click "choose file" and upload it.

3.4 Access config

3.4.1 Telnet config

1. Interface description

After enable TELNET service, TELNET terminal can connect with the switch by TELNET via PC, the interface is shown as the following figure:



HTTP-config

HTTP Service ☑ Enable

HTTPS Service ☑ Enable

Port 80 Default is 80, Modify default port, need specify port number at web browers

Telnet-config

Telnet Service ☑

Port 23

SSH-config

SSHService □

2. Operation steps

Step 1	Click the “System manage >Access configuration” menu in the navigation tree to enter the interface, tick the telnet service, set the port number, default port number is “23”, click “apply”.
Step 2	If it shall be used as start configuration, enter the “System manage>running configuration” for saving the settings.

Explanation

The terminal use TELNET to connect with the switch via PC should contain below condition:

1. Enable the TELNET service of the switch

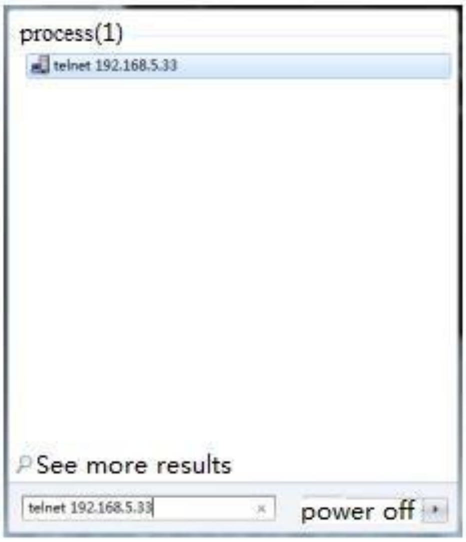
2. Should to know the IP address of the switch, and can be obtained by modifying(can use IP command)

3. If the port of the terminal PC which connects with the switch is under the same LAN, THE IP address should be set in the same network segment.

Once fulfill above condition, it can use TELNET to log in this switch, then config the switch.

3. E.G.

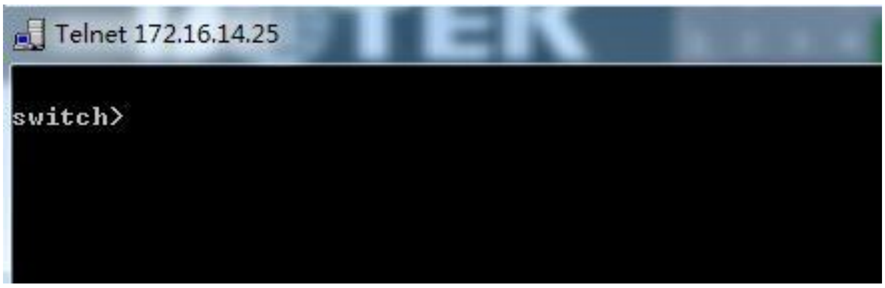
# Before log in the switch via TELNET, you have to input “TELNET+SPACE KEY+IP”, input “enter” in PC:


process(1)

telnet 192.168.5.33

See more results

telnet 192.168.5.33

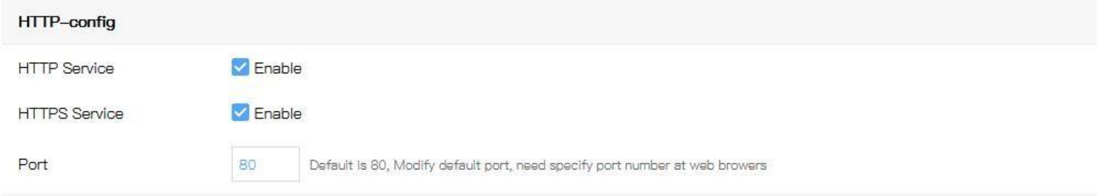

Telnet 172.16.14.25

```
switch>
```

3.4.2 HTTPS config

1. Interface description

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) is a HTTP channel that based on safety, it is the safety version of HTTP. HTTPS provides data encryption service. It prevents the transmitted message between web browser and website server from attacker's catch, so as to get any of important message, such as credit card number, password. User can modify the port number, and user also can close HTTP and HTTPS service.


HTTP–config

HTTP Service ☑ Enable

HTTPS Service ☑ Enable

Port 80 Default is 80, Modify default port, need specify port number at web browers

2. Explanations

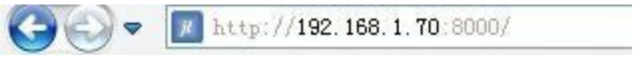
Configuration item	**Meaning**
HTTP	Visiting format: e.g. HTTP://192.168.1.254： port number
HTTPS	Visiting format: e.g. HTTPS://192.168.1.254。
Port number	Default is 80

3. Operation steps

Step 1	Click the “System manage >HTTP config” menu in the navigation tree to enter the interface, user can check the system default config.
Step 2	User can modify the default port number
Step 3	If it shall be used as start configuration, enter the “System manage>running configuration” for saving the settings.

4. E.G.

#Visit the IP address 192.168.1.70 from port number 8000, the IP setting in browser is as below:


http://192.168.1.70:8000/

Explanations

When modify the port as 8000, if need to log in again, please add port number while input the IP address. E.g.: http://192.168.1.254:8000

3.5 SNMP config

SNMP (Simple Network Management Protocol) is a network management standard protocol used for the TCP/IP network. It provides SNMP a method to manage the equipment through operating the central computer (i.e. network management workstation) of the network management software.

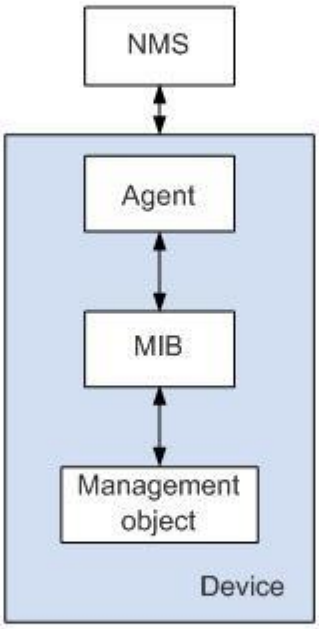
SNMP features：

Simple： SNMP adopts polling-driven, it provides the basic functions, which is suitable for small, fast and low price environment. And SNMP adopts UDP message, this is supported by most of the devices.

Strong: The target of SNMP is to make sure the managed information to be transmitted at any two different nodes, this is convenient for the administrator to check the information at any nodes of the network, so as to modify it or check the problems. There are 3 versions are widely used: SNMPv1、SNMPv2c and SNMPv3。SNMP system includes NMS （ Network Management System ） , Agent, Management object & MIB （Management Information Base）.

As the core of the network management, NMS manage the devices. Each managed devices include Agent, MIB & Management objects. NMS communicates with the running managed device Agent, and then Agent opertate it via MIB of the device, so as to NMS demand.

SNMP management mode



NMS

- NMS acts as administrator in the network, which is a system managing/ monitoring the network equipment using SNMP and works on the NMS server. It can send a request to Agent on the equipment and inquire or modify one or more specific parameter value(s). It can receive the Trap information proactively sent by Agent on the equipment to know the current state of the managed equipment.

Agent

- Agent is an agent in the managed equipment, which is used for maintaining the information data of the managed equipment, responding to the request of NMS and reporting the management data to NMS. After receiving the request information from NMS and completing the corresponding command through MIB, Agent responds to the operation result to NMS. When the equipment has a fault or other events, it will proactively send the information to NMS through Agent to report the change in its current state.

Management object

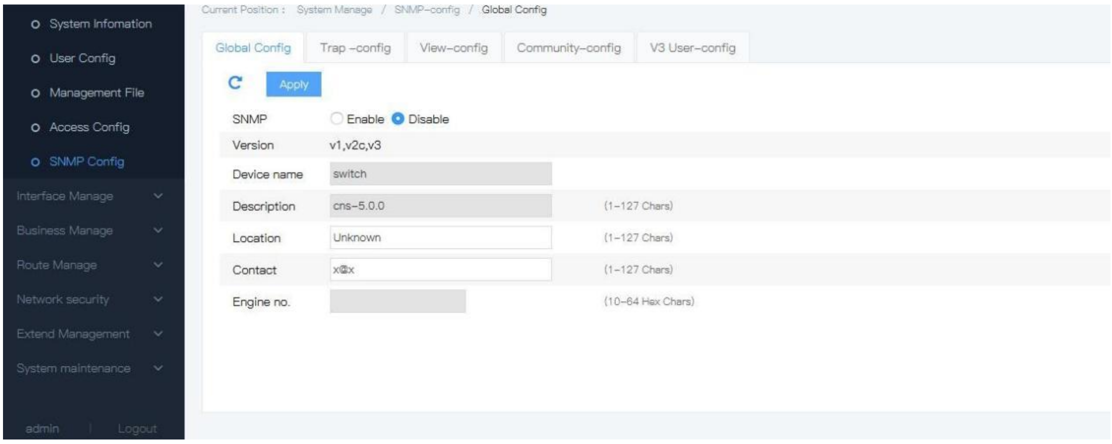
- Each set of equipment may contain several management objects. The management object may be a set of hardware (e.g. an interface board) in the equipment, or a set of hardware, software (e.g. routing protocol) and other configuration parameters.

MIB

- As a database, MIB defines the variable (i.e. information which can be inquired and set by Agent) maintained by the managed equipment. MIB defines a series of attributes of the managed equipment in the database, including object name, object state, object access permission and object data type. With MIB, the following functions can be served: By inquiring MIB, Agent can get the current state information of the equipment. By modifying MIB, it can set the equipment state parameter.

Operation steps

1. Click the “Advanced config> SNMP config” menu in the navigation tree to enter the “SNMP configuration” interface.



SNMP ○ Enable ● Disable

Version v1,v2c,v3

Device name switch

Description cns-5.0.0 (1-127 Chars)

Location Unknown (1-127 Chars)

Contact x@x (1-127 Chars)

Engine no. (10-64 Hex Chars)

Explanations

Configuration item	Sub item	Meaning
SNMP config	Mode	Enable or disable
	Version	Supports SNMPv1、SNMPv2c 和 SNMPv3
	Read/write area	No optional， the default is supported. It is used for authentification between Agent & NMS, character string, user can define it. The group name includes “readable” &”writeable”. When running GetRequest、GetNextRequest， it adopts “public”, when running “set”, it adopts “private”. If NMS needs to get the sysContact value of MIB node from the device be managed, it use readable group name “public”. If NMS needs to get the sysContact value of next MIB node from the device be managed, it use readable group name “public”. If NMS needs to set the sysName value of MIB node from the device be managed as “RUNDATA”, it use readable group name “Private”.
Trap config	Mode	Optional, enable or disable. Trap is the managed device send message to NMS actively without request. It is used for reporting emergent event. Please note that you should config SNMP basic function before Trapconfig.
	Trapv1 received	Necessary fill，set the address of Trap dest host
	Trapv2 received	Necessary fill，set the address of Trap dest host

User config	Read user	Set read user, the security level is authentication and encryption, the specified authentication protocol is MD5 & SHA, the specified encryption protocol is AES & DES
	Write user	Set write user, the security level is authentication and encryption, the specified authentication protocol is MD5 & SHA, the specified encryption protocol is AES & DES

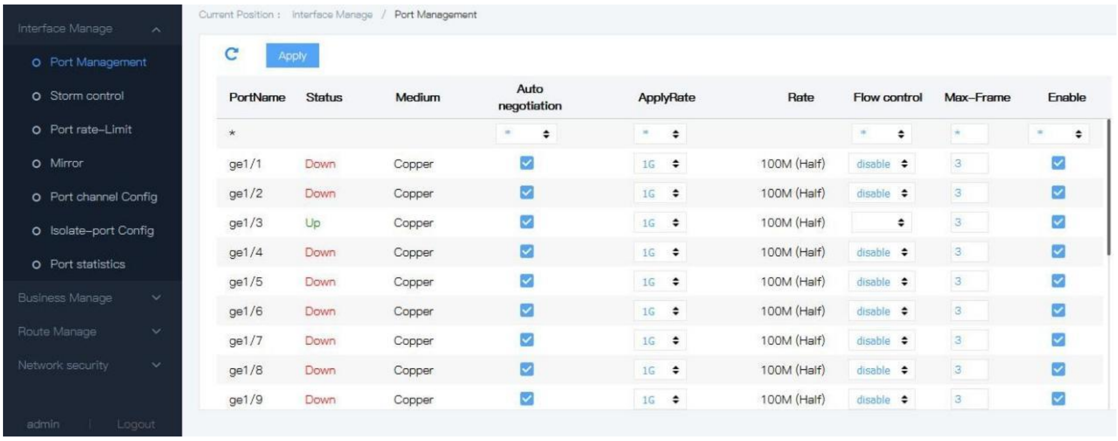
2. Fill in the corresponding configuration item and click "Submit"

4 Interface manage

4.1 Port management

1. Interface description

Port management page includes Medium(coper or fiber) information, applyrate, flow control function. It works only the port enables these functions. It supports auto negotiation. The interface is shown as the following figure:



PortName	Status	Medium	Auto negotiation	ApplyRate	Rate	Flow control	Max–Frame	Enable
*			*	*		*	*	*
ge1/1	Down	Copper	☑	1G	100M (Half)	disable	3	☑
ge1/2	Down	Copper	☑	1G	100M (Half)	disable	3	☑
ge1/3	Up	Copper	☑	1G	100M (Half)		3	☑
ge1/4	Down	Copper	☑	1G	100M (Half)	disable	3	☑
ge1/5	Down	Copper	☑	1G	100M (Half)	disable	3	☑
ge1/6	Down	Copper	☑	1G	100M (Half)	disable	3	☑
ge1/7	Down	Copper	☑	1G	100M (Half)	disable	3	☑
ge1/8	Down	Copper	☑	1G	100M (Half)	disable	3	☑
ge1/9	Down	Copper	☑	1G	100M (Half)	disable	3	☑

2.Explanations

Configuration item	Meaning
Port name	Relative port names, it is matched with the number on the switch panel.
Status	The port is connecting or not
Medium	Copper port or fiber port. 1000BaseSFP fiber port adopts Gigabit mini-GBIC for transmission.
Auto negotiation	Auto gegotiation, supports 0Mbits/s、100Mbits/s、1000Mbit/s
Apply rate	Port transmission rate

Flow control	When this terminal and the opposite terminal device enable the flow control, if there is block in this terminal device, it will send message to the opposite terminal device, inform the opposite terminal device stops to send message to it; The opposite device will stop to send message to this terminal device once receive the message. This prevents from message loss. Disable： Disable PAUSE frame receive & transmit rx（Rx PAUSE）： Enable PAUSE frame receive both（ Rx/Tx PAUSE）： Enable PAUSE frame receive & transmit tx（Tx PAUSE）： Enable PAUSE frame transmit
Max. frame	Display the max. frame of port transmission. Scope: 64-16356。
Enable	Display the port-forwarding data status, if the port is close, it means it can't forward.

3. Operation steps

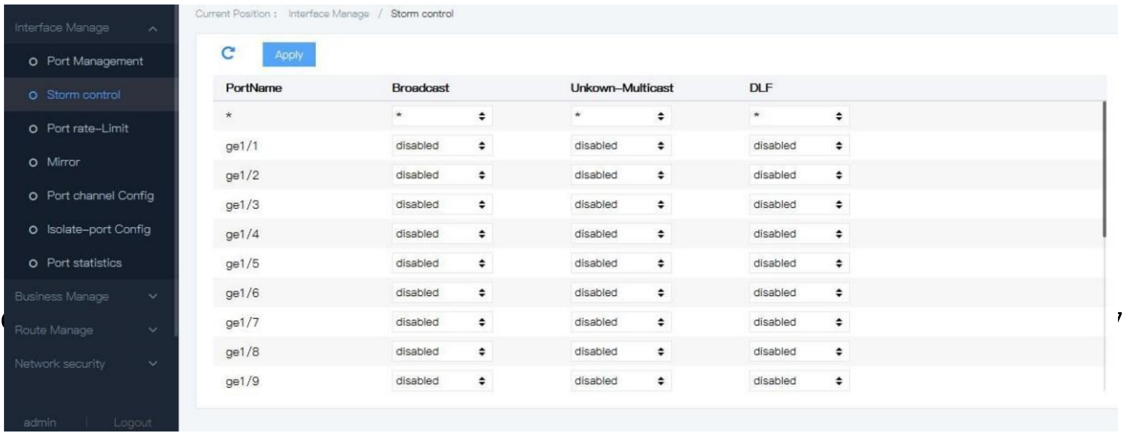
Step 1	Click the "Interface manage >port management" menu in the navigation tree to enter the interface, the interface is shown as the following figure:
Step 2	Configured the ports
Step 3	Save the setting
Step 4	If it shall be used as start configuration, enter the "System manage>running configuration" for saving the settings.

4.2 Storm control

1. Interface description

Storm control adopts below way to prevent broadcast, unknown multicast & unknown unicast from broadcast storm. The device supports port storm control under these 3 types by packet rate. During a detect time interval, compare the averate rate between these 3 type message and the max value, when the message rate over the max value, the device will start the storm control to the port.

When the layer 2 Ethernet port of the device receives broadcast, multicast or unknown unicast message, if the dest MAC address device can't understand the message ports according to this message, the device will forward this message to other layer 2 Ethernet ports which in the sam VLAN. This may cause broadcast storm, lower the forwarding performance of the device. AAdopts storm control function, these 3 types message flow can be controlled. The inferface is shown as below figure:



Current Position : Interface Manage / Storm control

PortName	Broadcast	Unkown-Multicast	DLF
*	*	*	*
ge1/1	disabled	disabled	disabled
ge1/2	disabled	disabled	disabled
ge1/3	disabled	disabled	disabled
ge1/4	disabled	disabled	disabled
ge1/5	disabled	disabled	disabled
ge1/6	disabled	disabled	disabled
ge1/7	disabled	disabled	disabled
ge1/8	disabled	disabled	disabled
ge1/9	disabled	disabled	disabled

2. Explanations

Configuration item	Meaning
Broadcast	Frame of FF-FF-FF-FF-FF-FF
Unknown-multicast	Frame of XX-XX-XX-XX-XX-XX，THE 2ND X is odd number
DLF	The MAC address of this frame is not in the device internal index table.

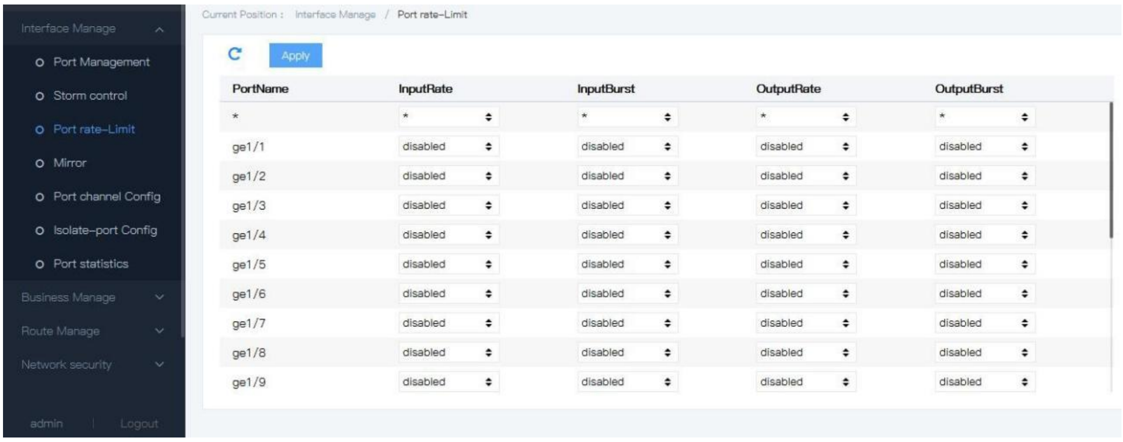
3. Operation steps

Step 1	Click the “Interface manage >storm control” menu in the navigation tree to enter the interface.
Step 2	Choose the port to be configured, set the value of broadcast, unknown-multicast, & DLF.
Step 3	Click “apply”.
Step 4	If it shall be used as start configuration, enter the “System manage>running configuration” for saving the settings.

4.3 Port rate-limit

1. Interface description

Port rate-Limit is to limit the rate of port data receiving. User can control the communication flow of each port, and fix the rate under certain value. The range is 0kbps~ 1000Mbps, the interface is shown as the following figure:



PortName	InputRate	InputBurst	OutputRate	OutputBurst
*	*	*	*	*
ge1/1	disabled	disabled	disabled	disabled
ge1/2	disabled	disabled	disabled	disabled
ge1/3	disabled	disabled	disabled	disabled
ge1/4	disabled	disabled	disabled	disabled
ge1/5	disabled	disabled	disabled	disabled
ge1/6	disabled	disabled	disabled	disabled
ge1/7	disabled	disabled	disabled	disabled
ge1/8	disabled	disabled	disabled	disabled
ge1/9	disabled	disabled	disabled	disabled

1. Set the output rate before the flow sending from the port
2. Set the input rate before the flow receiving from the port.

2. Explanations

Configuration item	Meaning

Input	Inputrate	Inputrate range 0-1000000。
	Burst	Burst range 0-1000000。
Output	Outputrate	Outputrate range 0-1000000。
	Burst	Burst range 0-1000000。

3. Operation steps

Step 1	Click the “Interface manage >Port rate -limit” menu in the navigation tree to enter the interface.
Step 2	Choose the port to be configured, set the value of the rate.
Step 3	Click “Apply”.
Step 4	If it shall be used as start configuration, enter the “System manage>running configuration” for saving the settings.

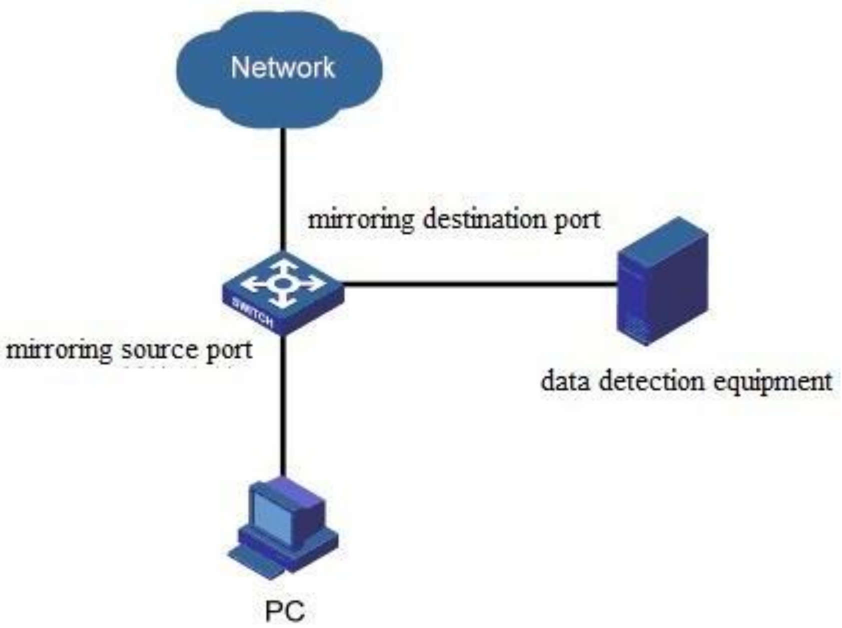
⚠ Attentions

Burst need to be set too, if the inputrate or ouputrate is set. The burst value should be less than the inputrate & outputrate

4.4 Mirror

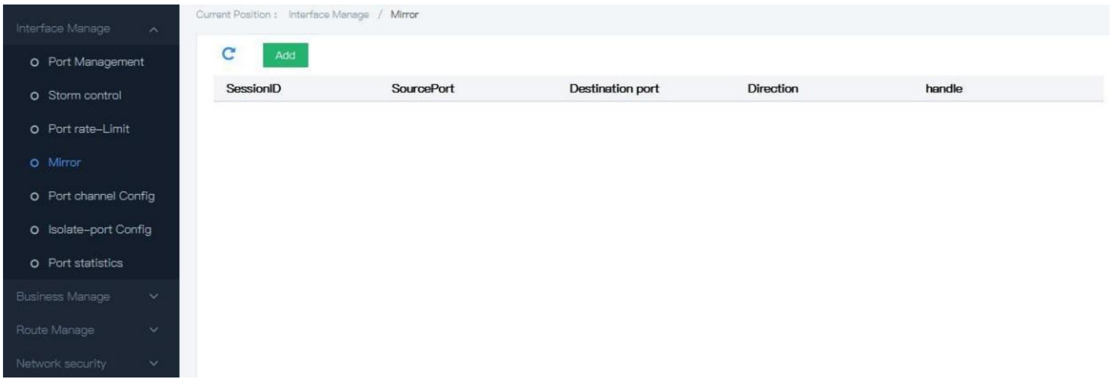
1. Interface description

Port mirroring is to copy the message of the specified port of the switch to the destination port, where the copied port is called the source port, and the copying port is called the destination port. The destination port will be connected to the data detection device, and the user uses these devices to analyze the message received by the destination port to monitor and troubleshoot the network, as shown in the following figure:

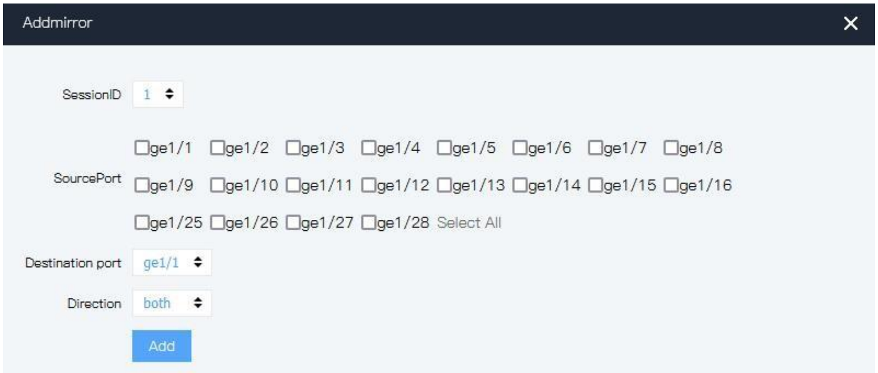


The device interface is shown as follows:

2. Explanations



SessionID	SourcePort	Destination port	Direction	handle



Addmirror

SessionID: 1

SourcePort:
□ge1/1 □ge1/2 □ge1/3 □ge1/4 □ge1/5 □ge1/6 □ge1/7 □ge1/8
□ge1/9 □ge1/10 □ge1/11 □ge1/12 □ge1/13 □ge1/14 □ge1/15 □ge1/16
□ge1/25 □ge1/26 □ge1/27 □ge1/28 Select All

Destination port: ge1/1

Direction: both

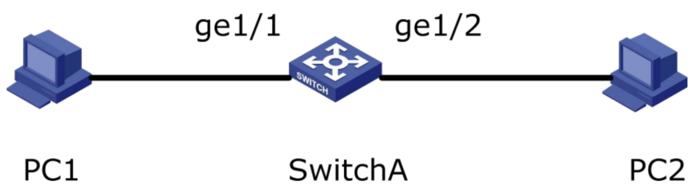
Configuration item	Meaning
Source port	This group defines the monitor ports. The device will collect data from this port. Mirror port can be 1 or more.
Destination port	This group defines a port for monitoring. The device will output the data with specified direction.
Direction	User can choose "ingress"， "egress"， "both" direction. ingress： import data， the received message of the port will be mirrored to the destination port. egress： Export data, the sent message of the port will be mirrored to the destination port. both： Both data. Sent & received message will be mirrored

3. Operation steps

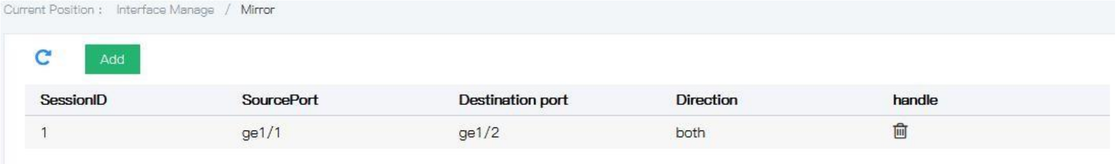
Step 1	Click the "Interface manage > mirror" menu in the navigation bar to enter the "mirror" interface, and select the corresponding ID.
Step 2	Check the source port and destination port and direction, click "Add"
Step 3	If it shall be used as start configuration, enter the “System manage>running configuration” for saving the settings.

4. E.G.

# Configuration requirements: the user wants to monitor the message sent by PC2 with the monitoring device PC1.
# The configuration diagram is as follows: PC1 accesses to SwitchA through the interface ge1/1. PC2 is directly connected to the ge1/2 interface of SwitchA.



# Settings: enable the mirroring function on the webpage, and check the source port ge1/2, choose the destination port ge1/1, choose the exit and entrance directions, click Submit. The page is shown as follows:


Current Position : Interface Manage / Mirror

Add

SessionID	SourcePort	Destination port	Direction	handle
1	ge1/1	ge1/2	both	🗑

4.5 Link Aggregation

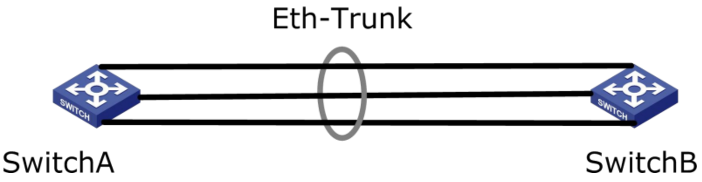
4.5.1 Introduction

1. Interface description

Link Aggregation is a way to bind a group of physical interfaces together as a logical interface to increase bandwidth and reliability.

- LAG (Link Aggregation Group) refers to a logical link that is formed by bindling a number of Ethernet links together, abbreviated as Eth-Trunk.
- With the continuous expansion of the network scale, the user demands more and more bandwidth and reliability of the link. In traditional technology, the way of replacing for high-speed interface boards or devices that support high-speed interface boards is commonly used to increase bandwidth, but this scheme needs to pay a high price and is not flexible enough.
- Link aggregation technology can be used to increase link bandwidth by binding multiple physical interfaces into a logical interface without upgrading hardware. The backup mechanism of link aggregation can effectively improve the reliability. At the same time, the load sharing of traffic on different physical links can be realized.

As shown below, between SwitchA and SwitchB is connected by three Ethernet physical links, and binding the three links together will make an Eth-Trunk logical link, which bandwidth equals to the sum of the bandwidth of original three Ethernet physical links, so as to increase the link bandwidth; at the same time, the three Ethernet physical links back up each other, which effectively improves the reliability of the link.



Link aggregation schematic diagram

The following requirements can be realized by configuring link aggregation:

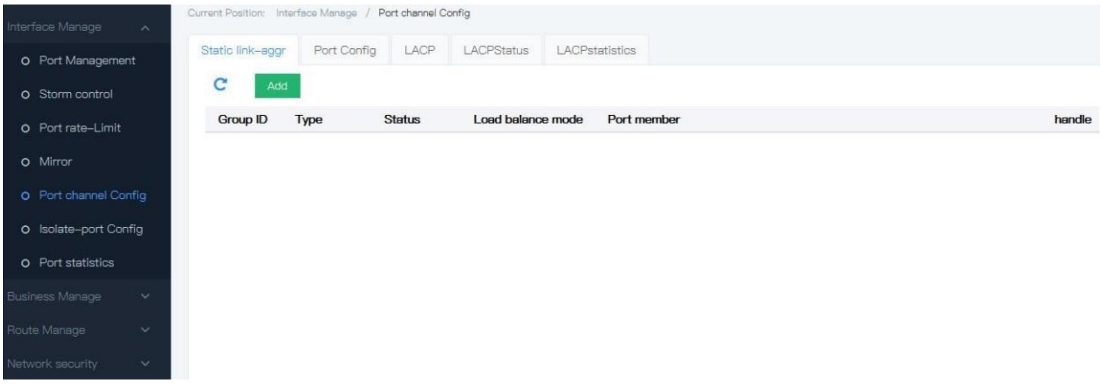
- When two switches are connected by one link, the bandwidth is not enough.
- When two switches are connected by one link, the reliability does not meet requirements.

Link aggregation is divided into manual load sharing mode and LACP mode based on whether link aggregation control protocol LACP is enabled.
Under the manual load sharing mode, the establishment of Eth-Trunk and the joining of member interface are manually configured without the participation of the link aggregation control protocol. Under this mode, all active links participate in the forwarding of data and the average sharing of traffic, so it is called the load sharing mode. If an active link fails, the link aggregation group will automatically share the traffic among the remaining active links. Manual load sharing mode can be used when a large link bandwidth is required between two direct connected devices while the device does not support the LACP protocol.

4.5.2 Static link-aggr

1. Interface descriptoin

Static link aggregation is manually configured by user. It is not allowed system automatically add or delete the ports in link aggregation group. It should be contain at least one port in the group. When there is only one port in the group, you only can delete the port by the way of deleting the group. The interface is shown as the following figure:



Group ID	Type	Status	Load balance mode	Port member	handle

2. Explanations

Configuration item	Meaning
Group ID	Link-aggr ID，1 ~ 16，total is 16
Src Mac	Load balance according to the source MAC address of the message. When the source MAC address is the same, the message go through the same port, otherwise, the message will go through the different ports.
Dst Mac	Load balance according to the destination MAC address of the message. When the destination MAC address is the same, the message go through the same port, otherwise, the message will go through the different ports.
Src&Dst Mac	Load balance according to the source & destination MAC address of the message. When the source & destination MAC address is the same, the message go through the same port, otherwise, the message will go through the different ports.

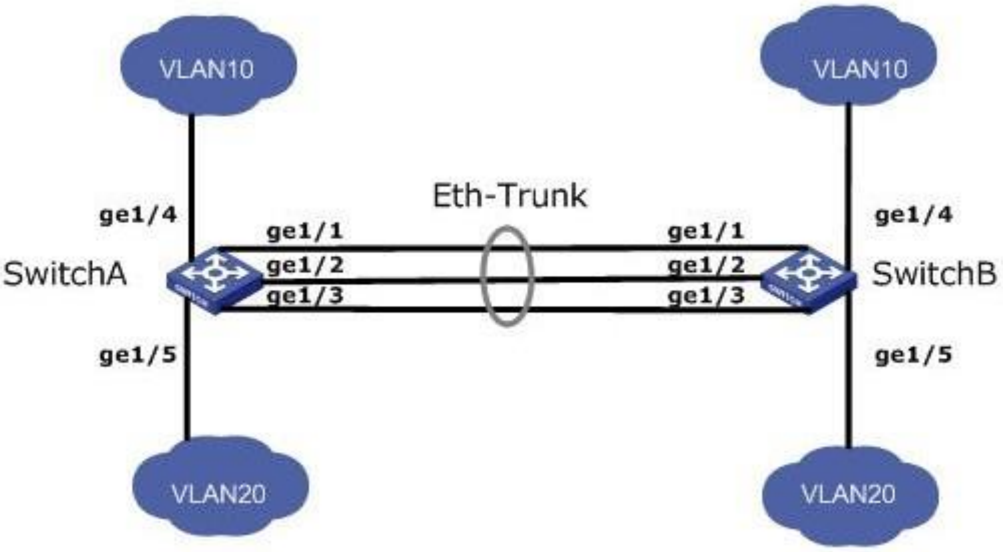
3. Operation steps

Step 1	Click the “Interface manage >Port channel config> Static link-aggr” menu in the navigation tree to enter the interface
Step 2	Choose group ID(1-16)， load balance mode: Src Mac,Dst Mac , Src& Dst Mac, choose the port, click “add”
Step 3	If it shall be used as start configuration, enter the “System manage>running configuration” for saving the settings.

4. E.G.

- # Requirement 1: The SwithcA & SwitchB connect with VLAN10 & VLAN20, and there are big data flow between SwitchA & SwitchB
- #Requirement 2: User want it can be provided with big link bandwidth between SwitchA & SwitchB, so as to make the same VLAN to communicate each other. At the same time, user wants crtain redundancy to be provided with, so as to make sure the reliability of the data transmission.

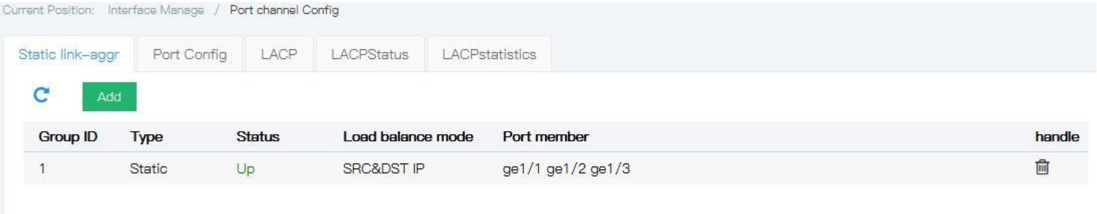
#the interface is shown as the following figure:



#Operation steps

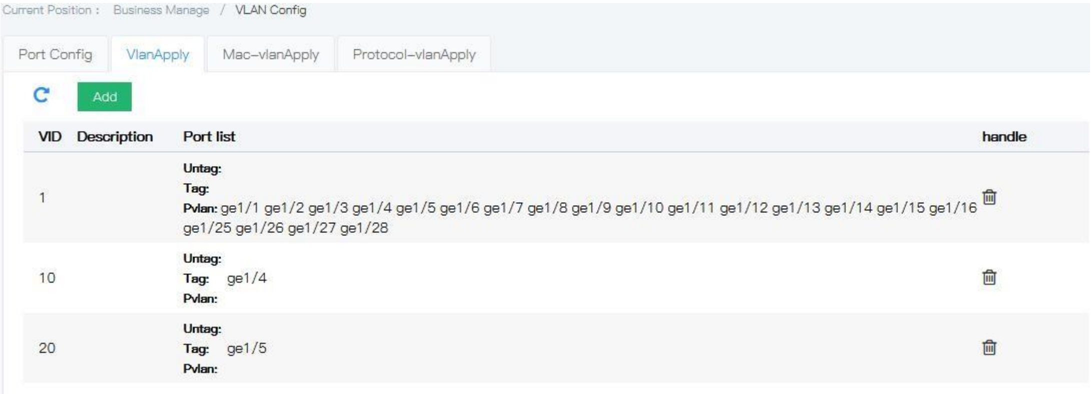
1） Create Eth-Trunk port of the switch, add in the port list(SwitchB is the same as SwitchA).

2） Click the "Inteface manage >Port-channel config >Static link-aggr" menu in the navigation tree to enter the interface, choose group ID "1", load balance mode "Src &Dst Mac" , and choose the port ge1/1, ge1/2 & ge1/3, click "add", the interface is shown as the following figure:



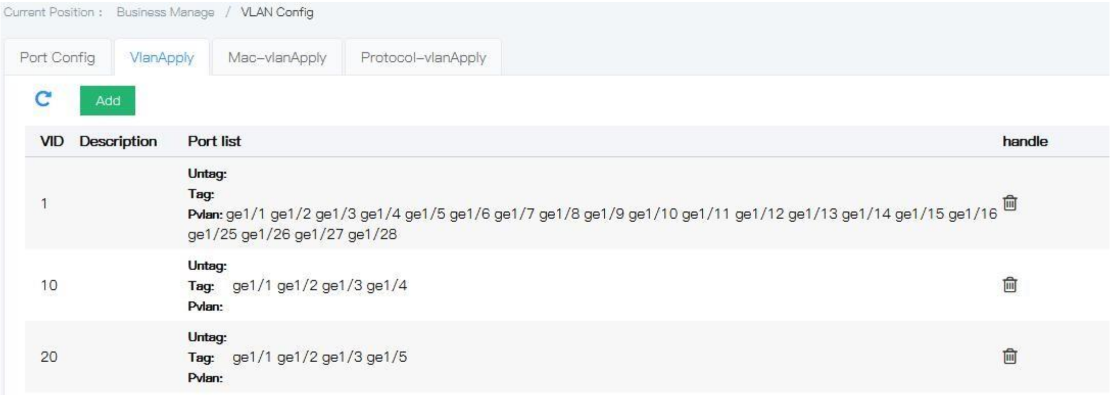
Group ID	Type	Status	Load balance mode	Port member	handle
1	Static	Up	SRC&DST IP	ge1/1 ge1/2 ge1/3	🗑

2) Configure ge1/4 port enable VLAN10 go through, ge1/5 port enable VLAN20 go through(SwitchB is the same as SwitchA). Click the "Business manage >VLAN config " menu in the navigation tree to enter the interface, input VLAN ID "10", check port list "ge1/4", click "add"; input VLAN ID "20", check port list "ge1/5", click "add", the interface is shown as the following figure:



VID	Description	Port list	handle
1		**Untag:** **Tag:** **Pvlan:** ge1/1 ge1/2 ge1/3 ge1/4 ge1/5 ge1/6 ge1/7 ge1/8 ge1/9 ge1/10 ge1/11 ge1/12 ge1/13 ge1/14 ge1/15 ge1/16 ge1/25 ge1/26 ge1/27 ge1/28	🗑
10		**Untag:** **Tag:** ge1/4 **Pvlan:**	🗑
20		**Untag:** **Tag:** ge1/5 **Pvlan:**	🗑

4）Configure port ge1/1, ge1/2 & ge1/3 enable VLAN10 & VLAN20 go through (SwitchB is the same as SwitchA). Click the "Business manage >VLAN config " menu in the navigation tree to enter the interface, input VLAN ID "10", check port list "ge1/1, ge1/2, ge1/3", click "add"; input VLAN ID "20", check port list "ge1/1, ge1/2, ge1/3", click "add", the interface is shown as the following figure:



VID	Description	Port list	handle
1		Untag: Tag: Pvlan: ge1/1 ge1/2 ge1/3 ge1/4 ge1/5 ge1/6 ge1/7 ge1/8 ge1/9 ge1/10 ge1/11 ge1/12 ge1/13 ge1/14 ge1/15 ge1/16 ge1/25 ge1/26 ge1/27 ge1/28	🗑
10		Untag: Tag: ge1/1 ge1/2 ge1/3 ge1/4 Pvlan:	🗑
20		Untag: Tag: ge1/1 ge1/2 ge1/3 ge1/5 Pvlan:	🗑

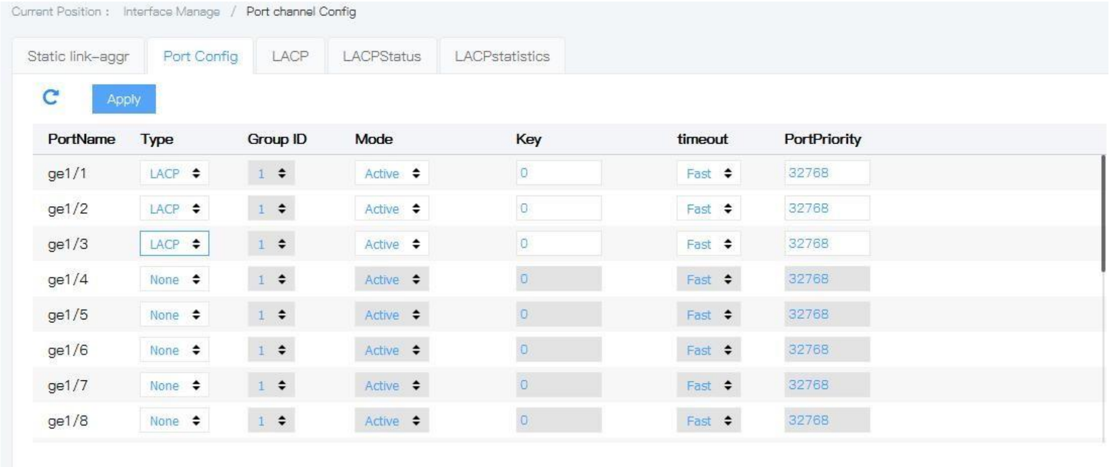
4.5.3 Add dynamic link aggregation

1. Interface description

LACP（Link Aggregation Control Protocol）is a protocol to realize dynamic link aggregation, and it is based on IEEE802.3ad standard. LACP communitate with the opposite terminal via LACPDU（Link Aggregation Control Protocol Data Unit）.

After enable LACP protocol for one of the port, this port will send LACPDU to the opposite terminal to tell its system priority, system MAC, port priority, port number, & operation key. When the opposite terminal receives this information, it will compare it with the saved information from the other ports, so as to choose the port can be aggregated. These entire make both ports reach an agreement to join or quip on certain dynamic link aggregation group.

： Dynamic LACP is an aggregation created or deleted by the system automatically. Dynamic LACP group port added and deleted is aumatically done by the protocol. Ports will be dynamic aggregated together under below condition: same rate and duplex, connect with the same device, with the same basic configuration. The interface is shown as the following figure:



PortName	Type	Group ID	Mode	Key	timeout	PortPriority
ge1/1	LACP	1	Active	0	Fast	32768
ge1/2	LACP	1	Active	0	Fast	32768
ge1/3	LACP	1	Active	0	Fast	32768
ge1/4	None	1	Active	0	Fast	32768
ge1/5	None	1	Active	0	Fast	32768
ge1/6	None	1	Active	0	Fast	32768
ge1/7	None	1	Active	0	Fast	32768
ge1/8	None	1	Active	0	Fast	32768

2. Explanations

Configuration item	Meaning
Type	Static & dynamic LACP Static mode: when need to increase the bandwidth or reliability between the two devices, and one of the device is not supported LACP, we can create static Link aggregation, and add member ports to increase the bandwidth and reliability between the devices. Dynamic LACP mode: Under dynamic LACP mode, there is redundant backup ability between the link of the two devices. When part of the link is breakdown, it adopts backup link to replace the breakdown link, keep the data transmission continued.
Mode	Passive: The port will not send LACP message automatically, it only response to the LACP message sent from the opposite terminal. Active: The port send LACP message automatically. One or two active LACP port link support dynamic LACP. If the two ports connecting each other are passive LACP ports, the LACP of these two ports will not working, they are waiting the LACP message from the opposite terminal.
Portpriority	When the LACP confirm the dynamic aggregation group members, it uses the device port ID priority to confirm. The device ID is made of two bytes system priority and 6 bytes system MAC. Device ID=System priority +system MAC address. When compare the ID, it compare the system priority first; if they are the same, it compare the system MAC address, the value smaller will be treated as priority. Scope: 0-65535, default: 32768

3. Operation steps

Step 1	Click the “Interface manage >port channel configuration > port configuration” menu in the navigation tree to enter the interface.
Step 2	Choose the ports to be configured, choose type(LACP), mode(Active or Passive), port priority(range: 0-65535, default: 32768), click “add”.
Step 3	If it shall be used as start configuration, enter the “System manage>running configuration” for saving the settings.

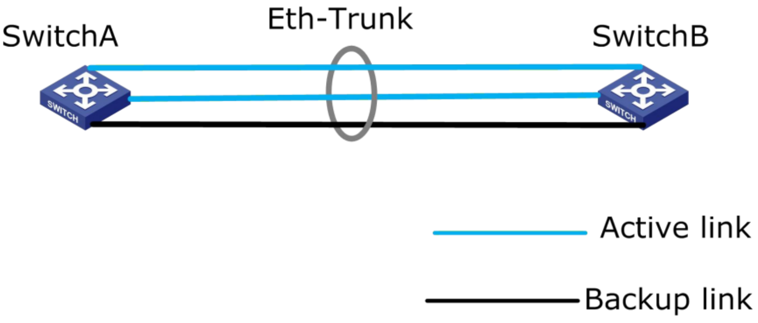
Explanation

1. Please make sure there is no other member ports in before change Eth-Trunk working mode, otherwise Eth-Trunk working mode can’t be changed.
2. The working mode in both side should be the same.

4. E.G.

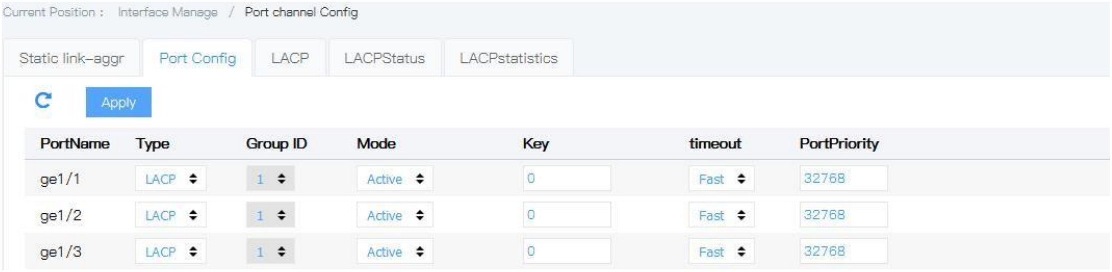
Configure LACP on two switches, so as to improve the bandwidth and reliability between these two devices, the requirements are as below:

- Both active links with load share ability
- One of the link between two devices are redundant backup link



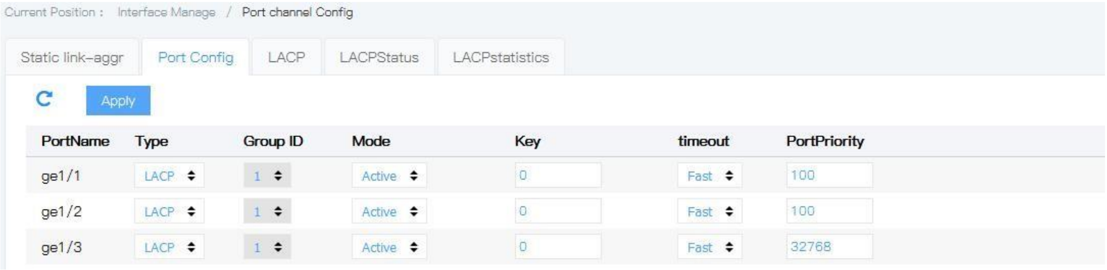
#Configuration steps

1) Configure LACP mode on SwitchA (SwitchB is the same as SwitchA). Click the "Interface manage >Port channel config> Port config" menu in the navigation tree to enter the interface, choose "ge1/1, ge1/2 & ge1/3>LACP>Active", the interface is shown as the following figure:



PortName	Type	Group ID	Mode	Key	timeout	PortPriority
ge1/1	LACP	1	Active	0	Fast	32768
ge1/2	LACP	1	Active	0	Fast	32768
ge1/3	LACP	1	Active	0	Fast	32768

3) Configure port priority on SwitchA. Click the "Interface manage >Port channel config> Port config" menu in the navigation tree to enter the interface, set the portpriority of ge1/1 & ge1/2 to 100, the interface is shown as the following figure:



PortName	Type	Group ID	Mode	Key	timeout	PortPriority
ge1/1	LACP	1	Active	0	Fast	100
ge1/2	LACP	1	Active	0	Fast	100
ge1/3	LACP	1	Active	0	Fast	32768

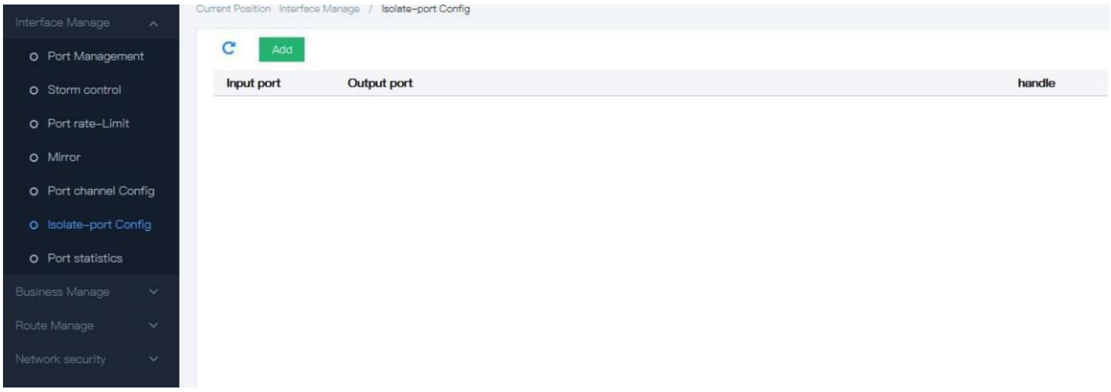
4.6 Isolated-port config

The ports in the same isolated-port group can be isolated each other; the ports in the different isolated-port group can't be isloted each other.

Operation steps

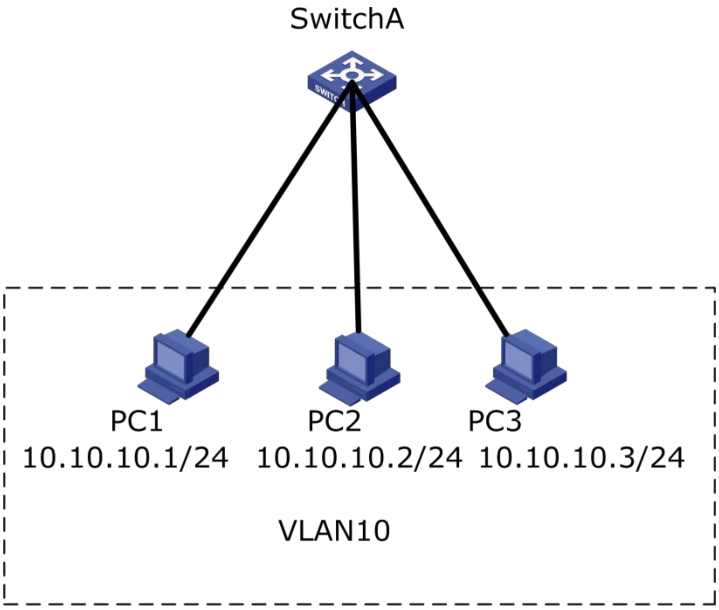
1. Click the "Business manage >Isolate-port configuration" menu in the navigation tree to

enter the interface, establish isolated group by ticking the ports, click “add”, the interface is shown as the following figure:



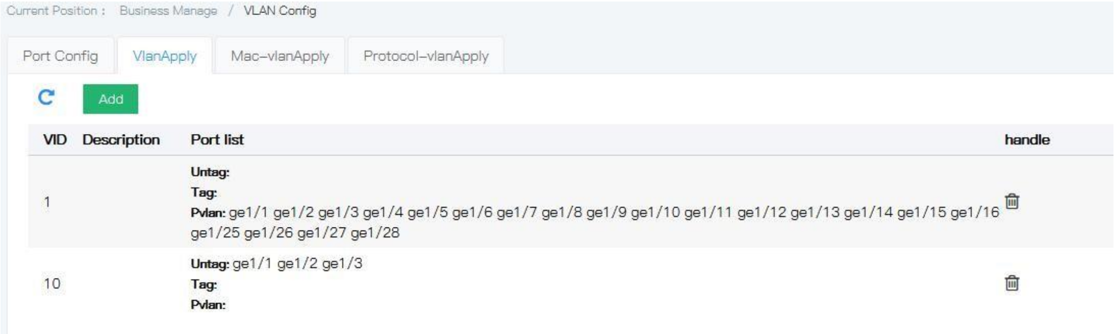
Input port	Output port	handle

#E.g.: It is shown as the following figure, PC1, PC2 & PC3 belong to VLAN10, user want PC1 & PC2 can’t access into each other in VLAN10, PC1 & PC3 can access into each other , PC2 & PC3 can access into each other.



Operation steps

1. Create VLAN, confirm the VLAN which PC are belong to. Click the “Business manage >VLAN configuration >VLAN APPLY” menu in the navigation tree to enter the interface, add VLAN0, tick ge1/1, ge1/2, ge1/3, click “add”, the interface is shown as the following figure:



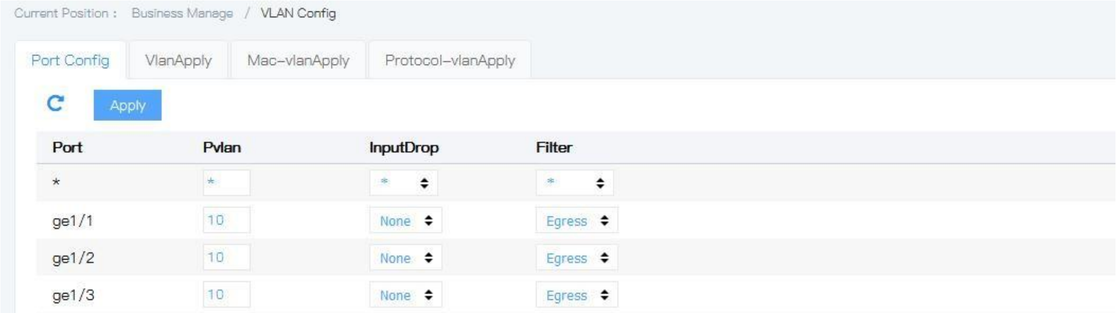
Current Position : Business Manage / VLAN Config

Port Config | VlanApply | Mac-vlanApply | Protocol-vlanApply

Add

VID	Description	Port list	handle
1		Untag: Tag: Pvlan: ge1/1 ge1/2 ge1/3 ge1/4 ge1/5 ge1/6 ge1/7 ge1/8 ge1/9 ge1/10 ge1/11 ge1/12 ge1/13 ge1/14 ge1/15 ge1/16 ge1/25 ge1/26 ge1/27 ge1/28	🗑
10		Untag: ge1/1 ge1/2 ge1/3 Tag: Pvlan:	🗑

2. Configure the Ethernet ports join the VLAN in the right way, so as to enable VLAN packet message get through. Click the "Business manage >VLAN configuration >Port configuration" menu in the navigation tree to enter the interface, tick ports ge1/1, ge1/2, ge1/3, change the value of PVID into 10, click "apply", the interface is shown as the following figure:



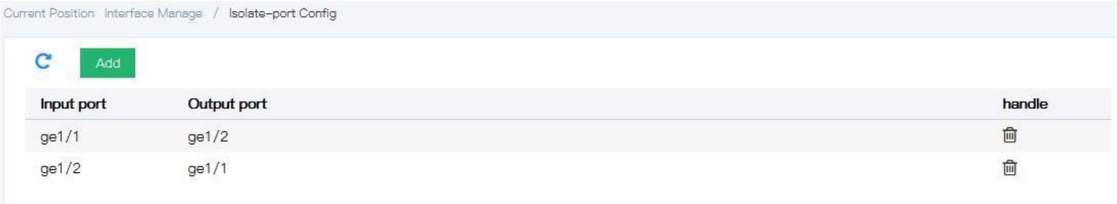
Current Position : Business Manage / VLAN Config

Port Config | VlanApply | Mac-vlanApply | Protocol-vlanApply

Apply

Port	Pvlan	InputDrop	Filter
*	*	*	*
ge1/1	10	None	Egress
ge1/2	10	None	Egress
ge1/3	10	None	Egress

3. Configure ge1/1, ge1/2 isolate-port function, click the "Business manage >IGMP-snooping config>IGMP-snooping config" menu in the navigation tree to enter the interface, check port ge1/1 & ge1/2 to establish isolated group, click "add", the interface is shown as the following figure:



Current Position Interface Manage / Isolate-port Config

Add

Input port	Output port	handle
ge1/1	ge1/2	🗑
ge1/2	ge1/1	🗑

4. Check the configuration result

# PC1 & PC2 can't be ping to each other

# PC1 & PC3 can be ping to each other

# PC2 & PC3 can be ping to each other

4.7 Port statistics

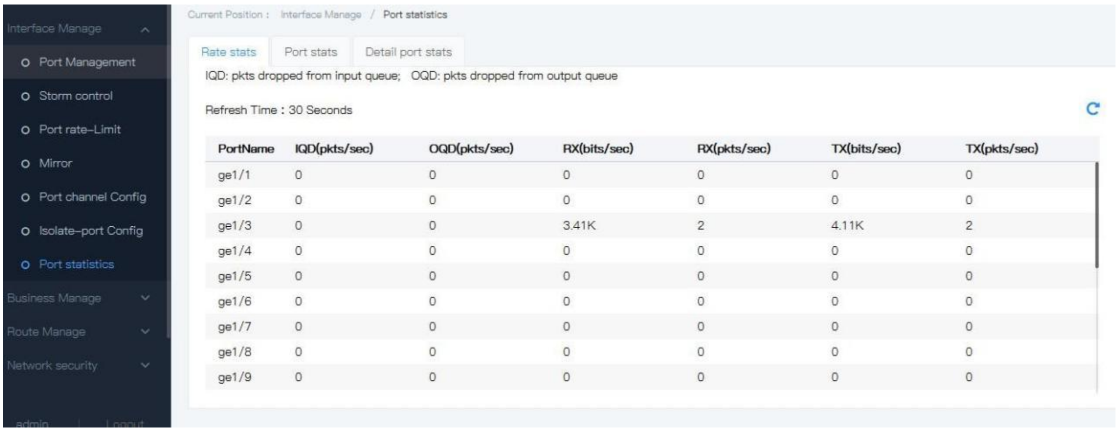
4.7.1 Interface description

Introduce all the port statistics, user can refresh or clear the statistics.

⚠ Attentions : It can't be recovered after statistics is clear. Please consider this before operating.

Operation steps

1. Click the “Interface manage >Port statistics >Port stats” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



IQD: pkts dropped from input queue; OQD: pkts dropped from output queue

Refresh Time : 30 Seconds

PortName	IQD(pkts/sec)	OQD(pkts/sec)	RX(bits/sec)	RX(pkts/sec)	TX(bits/sec)	TX(pkts/sec)
ge1/1	0	0	0	0	0	0
ge1/2	0	0	0	0	0	0
ge1/3	0	0	3.41K	2	4.11K	2
ge1/4	0	0	0	0	0	0
ge1/5	0	0	0	0	0	0
ge1/6	0	0	0	0	0	0
ge1/7	0	0	0	0	0	0
ge1/8	0	0	0	0	0	0
ge1/9	0	0	0	0	0	0

Explanation :

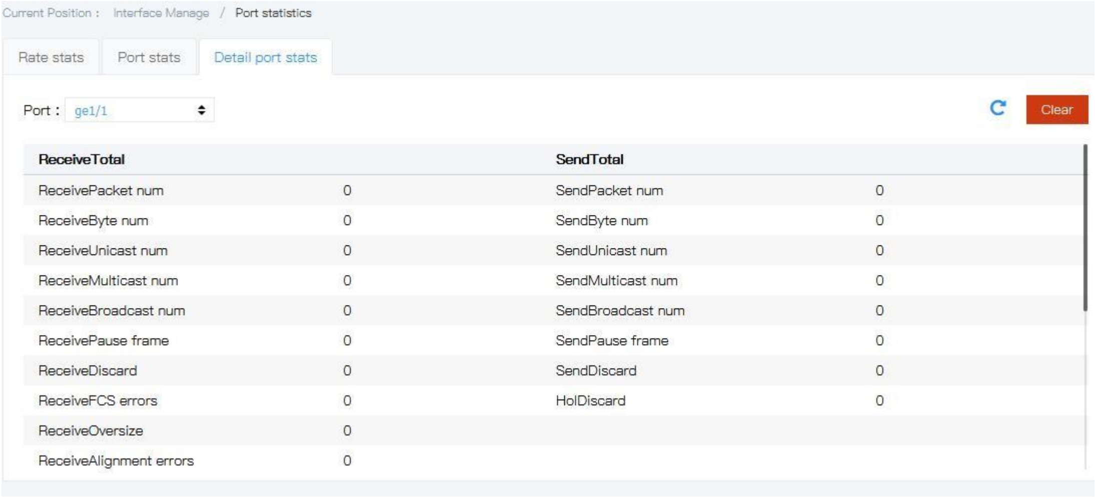
Click “Fresh” can get the latest statistics.

Click “Clear” can clear all the statistics.

4.7.2 Detail port stats

Introduce one of the ports statistics, user can refresh or clear the statistics.

1. Click the “Interface manage >Port statistics >Detail Port stats” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



Port : ge1/1

ReceiveTotal		SendTotal	
ReceivePacket num	0	SendPacket num	0
ReceiveByte num	0	SendByte num	0
ReceiveUnicast num	0	SendUnicast num	0
ReceiveMulticast num	0	SendMulticast num	0
ReceiveBroadcast num	0	SendBroadcast num	0
ReceivePause frame	0	SendPause frame	0
ReceiveDiscard	0	SendDiscard	0
ReceiveFCS errors	0	HolDiscard	0
ReceiveOversize	0		
ReceiveAlignment errors	0		

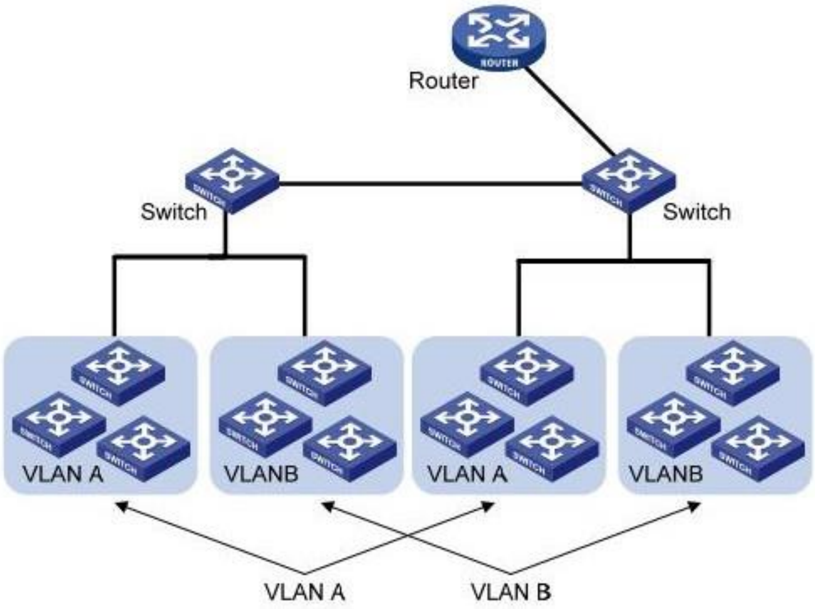
📖Explanation：

Click “Fresh” can get the latest statistics.
Click “Clear” can clear all the statistics.

5 Business manage

5 .1 VLAN config

VLAN (Virtual Local Area Network) is the virtual LAN. VLAN is a kind of data exchange technology that divides the LAN device logically (attention, not physically) into multiple network segments (or, smaller LANs), so as to realize the virtual workgroup. As shown in the following figure, VLAN divides a physical LAN into multiple logical LANs, each of which is a broadcast domain. Message interaction between hosts in VLAN can be carried out by traditional Ethernet communication mode. If communication is needed between hosts in different VLANs, it must be realized through network layer devices such as routers or three-layer switches and so on.



Compared with traditional Ethernet, VLAN has the following advantages:

- Scope of the broadcast domain controlled: the broadcast messages in the LAN are limited to a VLAN, saving the bandwidth and improving the network processing capability.
- The security of LAN is enhanced: because the message is isolated by the broadcast domain divided by VLAN at the data link layer, the hosts in each VLAN cannot communicate directly. It needs routers or three layer switches and other network layer devices for three-layer forwarding of the message.
- Flexible creation of virtual workgroup: you can create a virtual workgroup across physical network scope using VLAN. When user's physical location is moved within the scope of virtual workgroup, there is no need to change network configuration to access

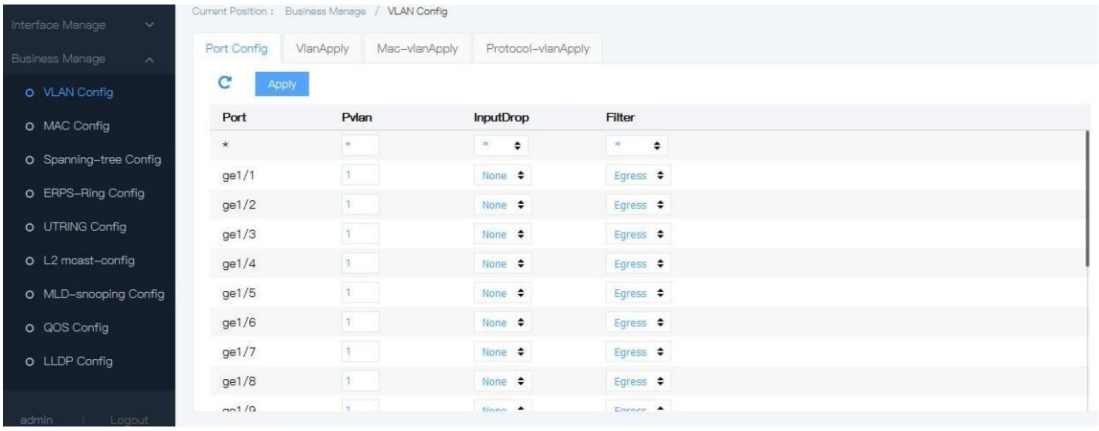
the network normally.

In other words, those in the same VLAN can communicate with each other, and those in the different VLAN cannot communicate with each other. A VLAN is identified by a VLAN ID, and those with the same VLAN ID belong to the same VLAN.

5.1.1 VLAN apply

a. Create new VLAN operation steps

1. Click the “Business manage >VLAN config > VLAN apply” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



Port	Pvlan	InputDrop	Filter
*	*	*	*
ge1/1	1	None	Egress
ge1/2	1	None	Egress
ge1/3	1	None	Egress
ge1/4	1	None	Egress
ge1/5	1	None	Egress
ge1/6	1	None	Egress
ge1/7	1	None	Egress
ge1/8	1	None	Egress
ge1/9	1	None	Egress

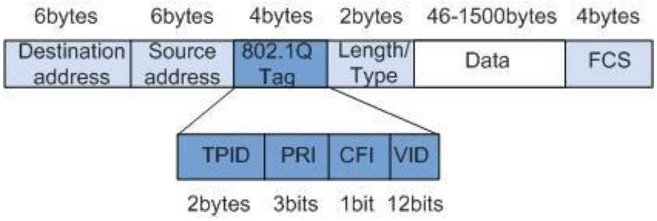
Explanations

Configuration item	Meaning
VLANID	Have to check， specified added VLAN ID， scope:1-4094. E.g. : 1-3， 5， 7， 9. Default is VLAN 1, when create new will not use VLAN1.
Untag	Untag
tag	Tag
Multicast	Have to check, specified multicast, default is Flood-unknown

802.1Q introduction

Trunk config: Trunk type ports are used for connecting with other switches. It is mainly connecting with the main line link. Trunk port enable frame from multiple VLAN to go through. The packing protocol of Trunk link is IEEE 802.1q. IEEE 802.1q is a formal standard of virtual bridged LAN. It makes some update on Ethernet frame format, which add 4 bytes 802.1q Tag between source MAD address field and protocol type field.

802.1q frame format



802.1Q Tag explanations

Field	Length	Item	Meaning
TPID	2bytes	Tag Protocol Identifier	When the value is 0x8100, it means 802.1q Tag frame. If the device not supported 802.1q receive the frame, it will discarded
PRI	3bits	Priority	Scope::0-7 ， the value is bigger, the priority is higher. When it is used as the block of the switch, it sends the higher priority frame first.
CFI	1bit	Canonical Format Indicator	”0” CFI means typical format; ”1” CFI means untypical format. It is compatible with Ethernet & token ring network. In Ethernet, the CFI is “0”.
VID	12bits	VLAN ID	VLAN ID scope:0-4095. 0 & 4095 are the retention value, the valid VLAN ID scope is : 1-4094

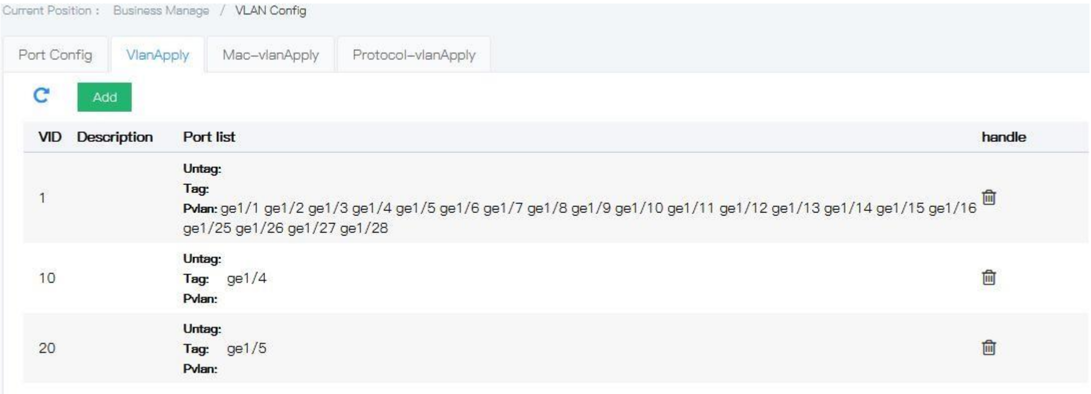
The sending data of each switch supports 802.1q contains VLAN ID, so as to indicate that the switch belongs to which VLAN. There are two styles for Ethernet frame in a VLAN network:

- Tagged frame : Added 4 bytes 802.1q Tag frame
- Untagged frame : Original, without adding 4 bytes 802.1q Tag frame

Trunk port is used for connecting other switches; it connects with the main link. Trunk port allows frame from different VLAN to go through.

2. Fill corresponding configuration items.

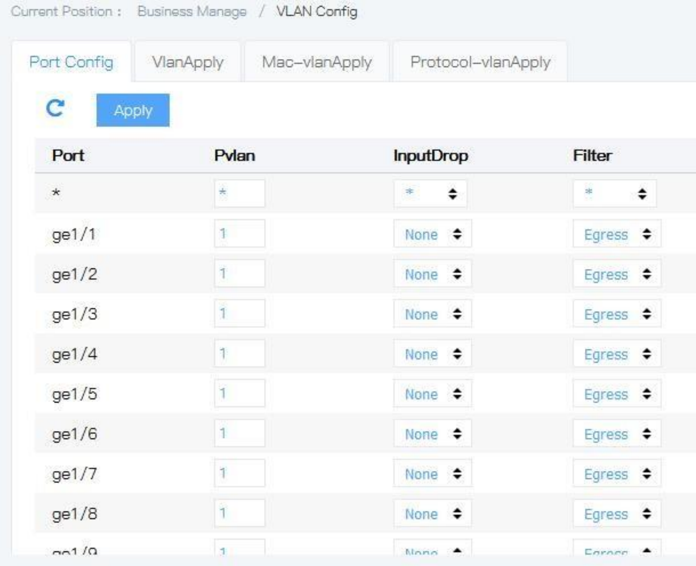
3. Click “add”, the interface is shown as the following figure:



VID	Description	Port list	handle
1		Untag: Tag: Pvlan: ge1/1 ge1/2 ge1/3 ge1/4 ge1/5 ge1/6 ge1/7 ge1/8 ge1/9 ge1/10 ge1/11 ge1/12 ge1/13 ge1/14 ge1/15 ge1/16 ge1/25 ge1/26 ge1/27 ge1/28	🗑
10		Untag: Tag: ge1/4 Pvlan:	🗑
20		Untag: Tag: ge1/5 Pvlan:	🗑

5.1.2 Port config

1. Click the “Business manage >VLAN config >Port config” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



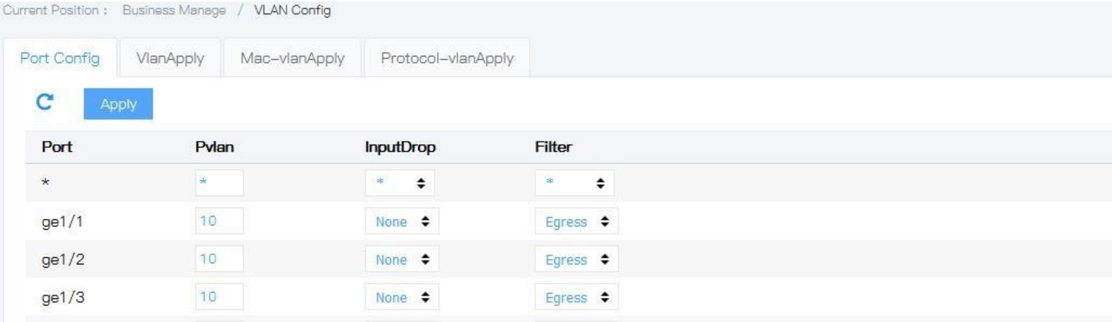
Port	Pvlan	InputDrop	Filter
*	*	*	*
ge1/1	1	None	Egress
ge1/2	1	None	Egress
ge1/3	1	None	Egress
ge1/4	1	None	Egress
ge1/5	1	None	Egress
ge1/6	1	None	Egress
ge1/7	1	None	Egress
ge1/8	1	None	Egress
ge1/9	1	None	Egress

Explanations

Configuration item	Meaning
PVID	Each port only can get one VLAN ID(PVID). When the untage Ethernet message packet were sent to the port, it will be marked with PVID VID tag. The default PVID of each port is 1.
Inputdrop	Mode： none （not drop）， untag(drop without tag message)， tag （drop all the tag message）， all （drop all lthe message）
Filter	Mode： egress， ingress， both， none

2. Fill corresponding configuration items.

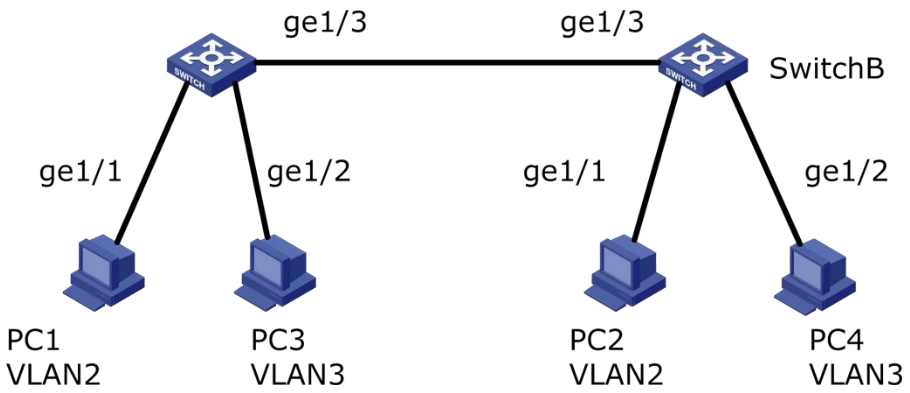
3. Click “add”, the interface is shown as the following figure:



Port	Pvlan	InputDrop	Filter
*	*	*	*
ge1/1	10	None	Egress
ge1/2	10	None	Egress
ge1/3	10	None	Egress

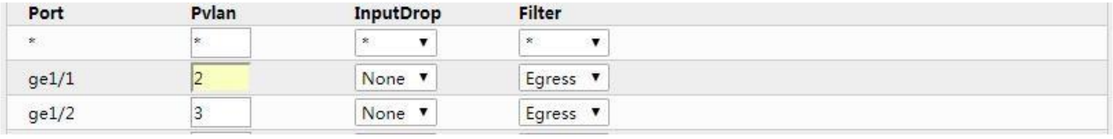
#E.G.

To make the link between SwitchA & SwitchB not only supports the communication for the users in VLAN2, but also supports the users in VLAN3, it needs to config the ports join these two VLAN at the same time: set the Ethernet port ge1/3 of SwitchA and the port ge1/3 of SwitchB join VLAN & VLAN3 at the same time.



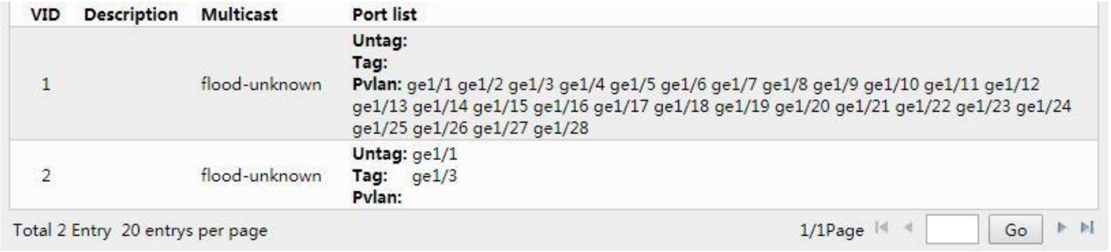
Operation steps:

1. Create VLAN2 & VLAN3 on SwitchA, and join the connecting ports into VLAN, set ge1/3 into Trunk mode. Click the “Business manage >VLAN config>Port config” menu in the navigation tree to enter the interface, fill the config items. The interface is shown as the following figure:



Port	Pvlan	InputDrop	Filter
*	*	* ▼	* ▼
ge1/1	2	None ▼	Egress ▼
ge1/2	3	None ▼	Egress ▼

2. Config SwitchA & SwitchB connecting port & VLAN. Click the “Business manage >VLAN config” menu in the navigation tree to enter the interface, fill the config items, click “add”(SwitchB is the same as SwitchA). Below figure is shown as how to add VLAN2:



VID	Description	Multicast	Port list
1		flood-unknown	**Untag:** **Tag:** **Pvlan:** ge1/1 ge1/2 ge1/3 ge1/4 ge1/5 ge1/6 ge1/7 ge1/8 ge1/9 ge1/10 ge1/11 ge1/12 ge1/13 ge1/14 ge1/15 ge1/16 ge1/17 ge1/18 ge1/19 ge1/20 ge1/21 ge1/22 ge1/23 ge1/24 ge1/25 ge1/26 ge1/27 ge1/28
2		flood-unknown	**Untag:** ge1/1 **Tag:** ge1/3 **Pvlan:**

Total 2 Entry 20 entrys per page 1/1Page Go

3. Result

Config User1 & User2 in the same network segment, e.g.: 192.168.100.0/24； config User3 & User4 in the same network segment, e.g.: 192.168.200.0/24

User1 & User2 can be ping each other ，but not for User3 & User4. User3 & User4 can be pin each other, but not for User1 & User2.

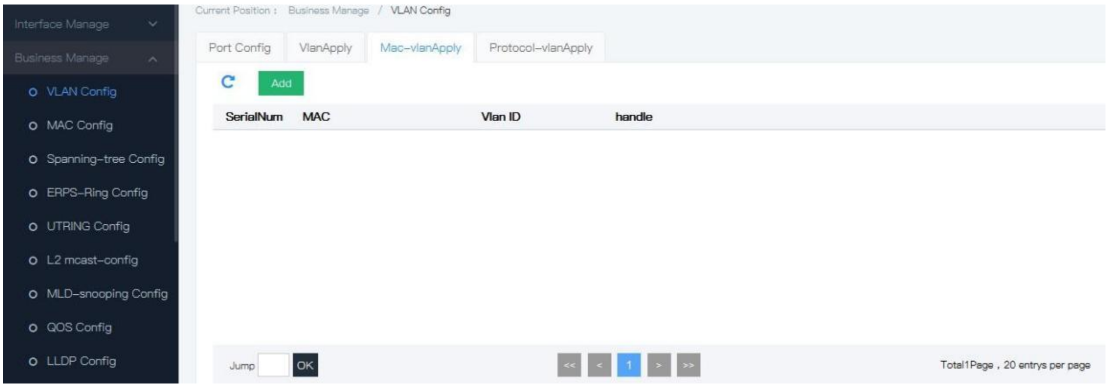
5.1.3 MAC-VLAN

VLAN based on MAC, it divides VLAN according to the MAD address of the PC network card. Administrator configures MAC address & VLAN ID mapping relationship table; if the frame which switch received is untagged, it add VLAN ID according to the table.

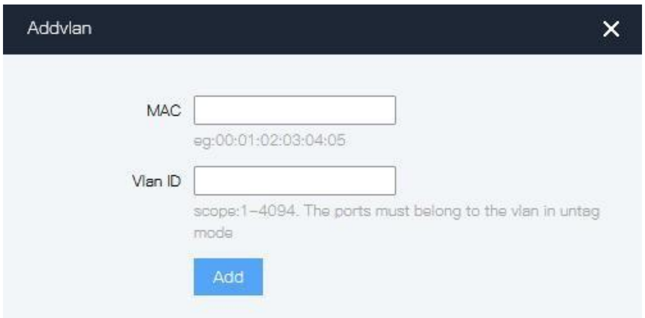
The advantage is: when the physical location of end user is changed, there is no need to relocate VLAN. This enhances the safety and access flexibility. The disadvantage is: It is suitable for the simple environment that there is no need to change the network card, and it has to define all the members in the network advanced.

Operation steps

1. Click the “Business manage >VLAN config>mac-vlan config” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



SerialNum	MAC	Vlan ID	handle



Addvlan

MAC
eg:00:01:02:03:04:05

Vlan ID
scope:1-4094. The ports must belong to the vlan in untag mode

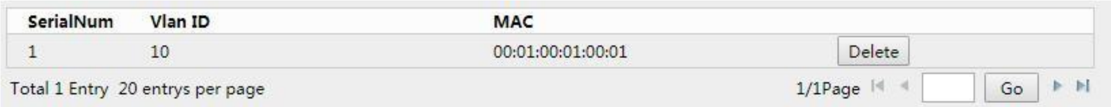
Add

Explanations

Configuration item	**Meaning**
VLAN ID	Necessary option, scope: 1-4094, e.g.: 1-3, 5, 7, 9.Default is VLAN 1. Other VLAN is necessary and add the link port under untag way.
MAC	Necessary option, input the MAC address of the PC network card.

2. Fill corresponding configuration items.

3. Click “add”, the interface is shown as the following figure:



SerialNum	Vlan ID	MAC	
1	10	00:01:00:01:00:01	Delete

Total 1 Entry 20 entrys per page 1/1Page Go

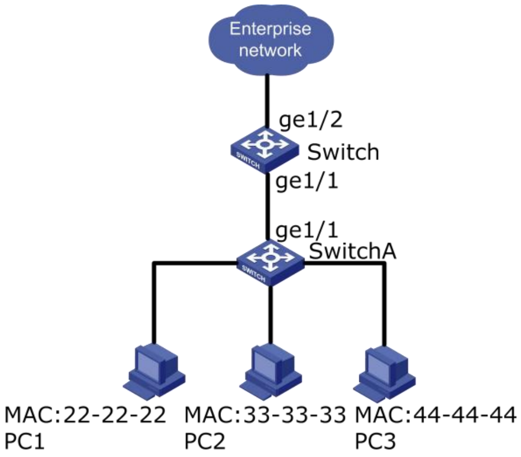
#E.G.

。 A company has high requirement on information security; it only allows PCs from its company can access to the company Internet. As shown in the figure, port ge1/1 of the switch connects with the uplink port of SwitchA. The downstream ports of SwitchA connect with PC1, PC2 & PC3 respectively. It allows PC1, PC2 & PC3 can access to the company Internet via SwitchA & Switch.

Configuration: It adopts below configuration which based on MAC address to devide VLAN:

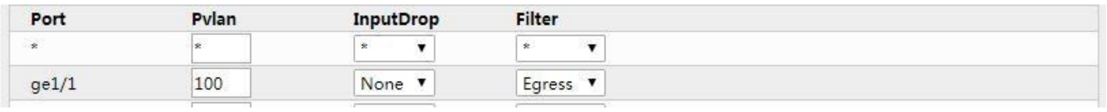
1. Create relative VLAN

2. Config each Ethernet ports to join VLAN in the right way.
3. Config the MAC address of PC1, PC2 & PC4 to connect with VLAN
Below data needs to be prepared:
Set port ge1/1 PVID of the switch as “100”
Set port ge1/1 of the switch join VLAN10 under “untagged” mode
Set port ge1/2 of the switch join VLAN10 under “tagged” mode
All the ports of the switchA join VLAN1 under “untagged” mode
Ge the MAC address of PC1, PC2 & PC3, config the MAC address connect with VLAN10



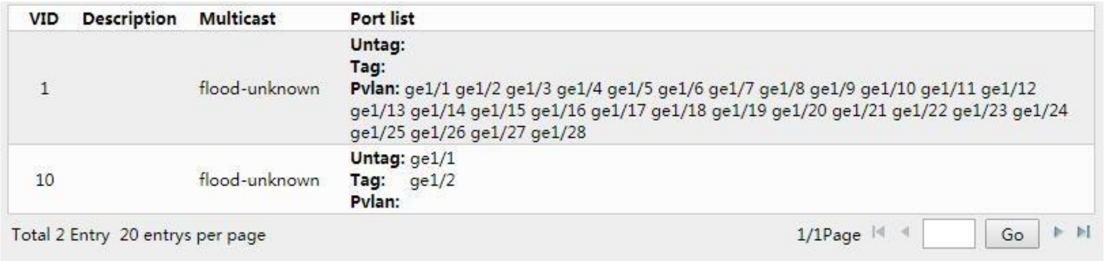
Operation steps

1. Click the “Business manage>VLAN config> Port config” menu in the navigation tree to enter the interface, choose ge1/1, input PVID “100”, the interface is shown as the following figure:



Port	Pvlan	InputDrop	Filter
*	*	* ▼	* ▼
ge1/1	100	None ▼	Egress ▼

2. Click the “Business manage>VLAN config> VLAN apply” menu in the navigation tree to enter the interface, input VLAN ID “10”, check port ge1/1 in untag port list, check ge1/2 in Tag port list, the interface is shown as the following figure:



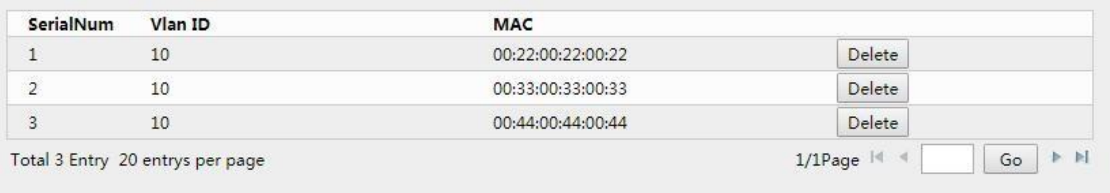
VID	Description	Multicast	Port list
1		flood-unknown	**Untag:** **Tag:** **Pvlan:** ge1/1 ge1/2 ge1/3 ge1/4 ge1/5 ge1/6 ge1/7 ge1/8 ge1/9 ge1/10 ge1/11 ge1/12 ge1/13 ge1/14 ge1/15 ge1/16 ge1/17 ge1/18 ge1/19 ge1/20 ge1/21 ge1/22 ge1/23 ge1/24 ge1/25 ge1/26 ge1/27 ge1/28
10		flood-unknown	**Untag:** ge1/1 **Tag:** ge1/2 **Pvlan:**

Total 2 Entry 20 entrys per page 1/1Page Go

3. Set all the ports of the SwitchA join VLAN under “untagged” mode. There is no need to operate this, the default setting of the switch is: all the ports join VLAN1 under “untagged” mode.

4. Set the MAC address of PC1, PC2 & PC3 to be connected with VLAN. Click the “Business manage >VLAN config >MAC-VLAN config” menu in the navigation tree to enter the interface, input the created VLAN ID with VLAN10, then input the MAC address of PC1

（0022-0022-0022）, PC2（0033-0033-0033）, PC3（0044-0044-0044）, click “add”, the interface is shown as the following figure:



SerialNum	Vlan ID	MAC	
1	10	00:22:00:22:00:22	Delete
2	10	00:33:00:33:00:33	Delete
3	10	00:44:00:44:00:44	Delete

Total 3 Entry 20 entrys per page 1/1Page Go

5. Check the result

PC1、PC2、PC3 are enable to access the company network, other PCs are no access to the network.

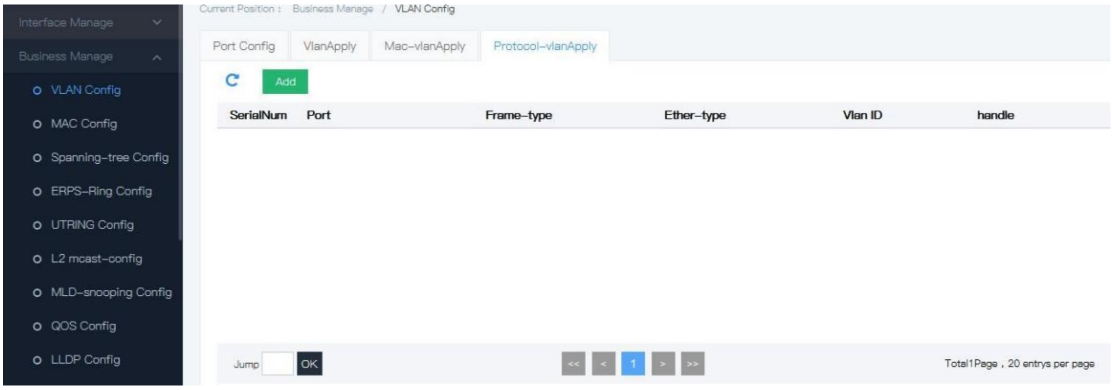
5.1.4 Protocol-VLAN

Divide VLAN based on protocol, it distributes different VLAN ID according to the packing format and the protocol which received message belongs to.

Administrator needs to configure the protocol field of the Ethernet frame & VLAN ID mapping relationship table. If the frame received is untagged, it adds VLAN ID according to the table. The advantage is: it divides VLAN based on protocol and binds the service type & VLAN from network. It is convenient for management. The disadvantage is: it needs to initial the configuration of the protocol type & VLAN ID; it needs to analyze the address format of each protocol, and makes relative conversion. This cost lots of resource of the switch, lower the speed.

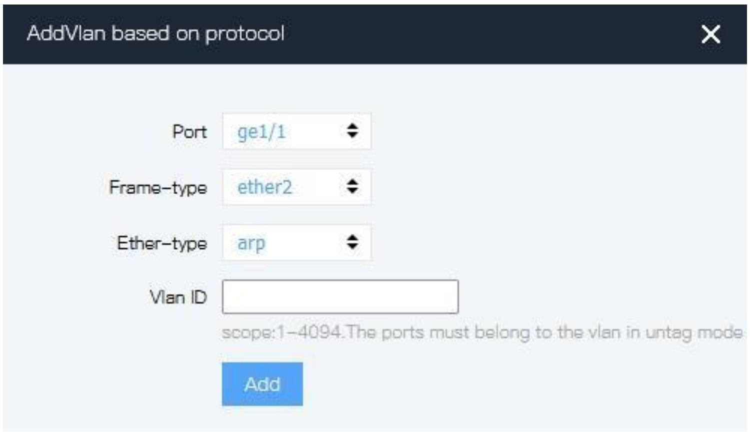
Operation steps

1. Click the “Business manage >VLAN config> protocol-vlan config” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



SerialNum	Port	Frame-type	Ether-type	Vlan ID	handle

Total1Page , 20 entrys per page



AddVlan based on protocol

Port: ge1/1

Frame-type: ether2

Ether-type: arp

Vlan ID:

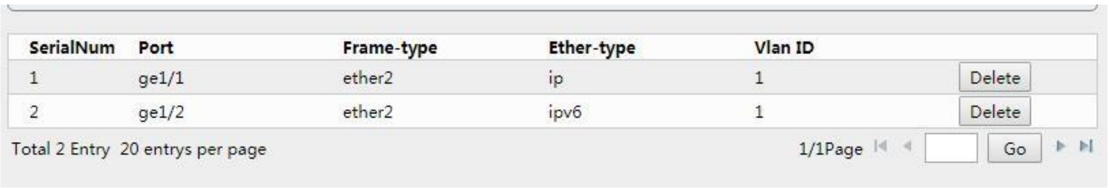
scope:1-4094.The ports must belong to the vlan in untag mode

Explanations

Configuration item	**Meaning**
Port	Choose port ge1/1- ge1/24， xe1/25- xe1/28
Frame-type	With optional, frame-type includes: ether2， 802.3， snap， llc， snap-priv
Ethernet-type	With optional, Ethernet-type:arp， ip,ipv6,802.1d.1q, 802.1d.1x
Vlan Id	Necessary option, join specified VLAN ID, scope: 1-4094. E.g.: 1-3， 5， 7， 9. Default is VLAN 1.

2. Fill corresponding configuration items.

3. Click “add”, the interface is shown as the following figure:

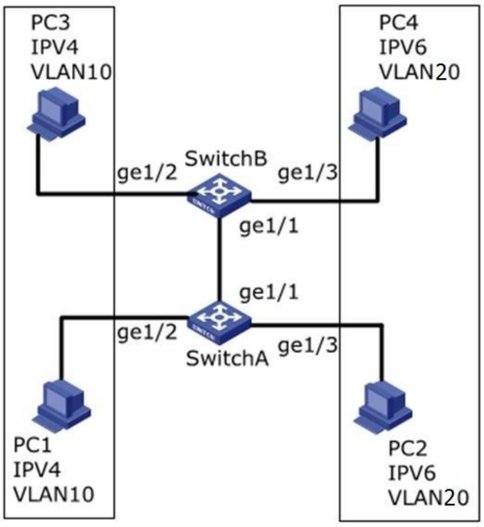


SerialNum	Port	Frame-type	Ether-type	Vlan ID	
1	ge1/1	ether2	ip	1	Delete
2	ge1/2	ether2	ipv6	1	Delete

Total 2 Entry 20 entrys per page 1/1Page

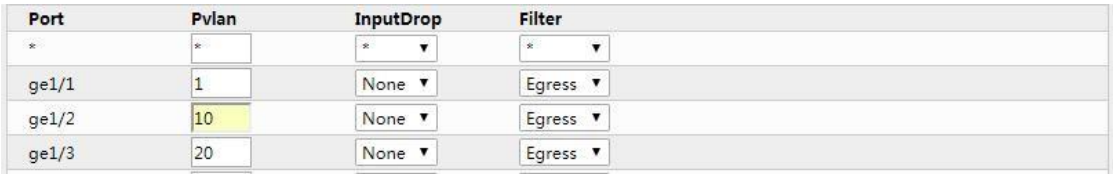
E.G.: PC1 & PC3 access to each other, the communication protocol is IPV4, bind IPV4 protocol with VLAN10. PC2 & PC4 access to each other, the communication is IPV6, bind IPV6 protocol with VLAN20.

VLAN diagram:



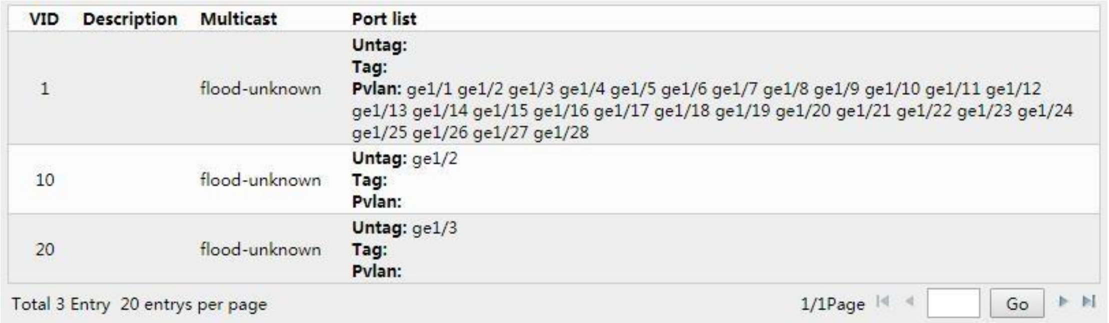
Operation steps

1. Create VLAN, confirm the VLAN every business belongs to. Click the "Business manage >VLAN config" menu in the navigation tree to enter the interface, modify the PVID value, the interface is shown as the following figure:



Port	Pvlan	InputDrop	Filter
*	*	* ▼	* ▼
ge1/1	1	None ▼	Egress ▼
ge1/2	10	None ▼	Egress ▼
ge1/3	20	None ▼	Egress ▼

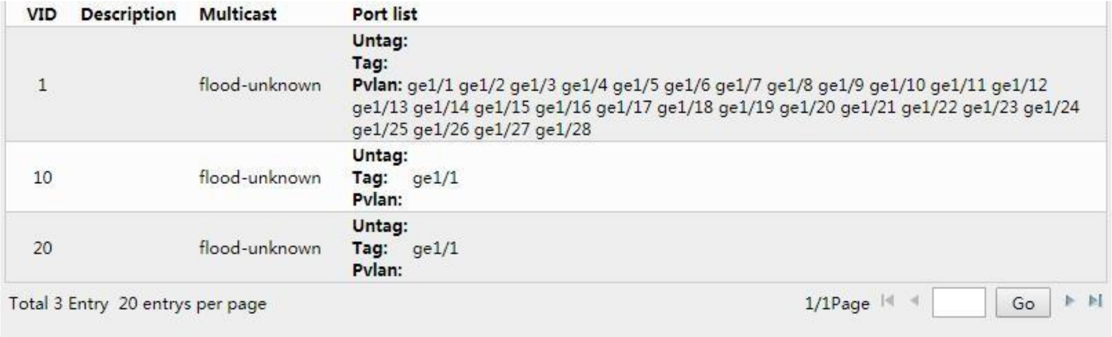
2. Config Ethernet port ge1/2 & ge1/3 of the SwitchA join the VLAN under "untag" mode. Click the "Business manage >VLAN config" menu in the navigation tree to enter the interface, input VLAN ID "10", choose ge1/2 in "Untag port list"; input VLAN ID "20", choose ge1/3 in "Untag port list". The interface is shown as the following figure:



VID	Description	Multicast	Port list
1		flood-unknown	**Untag:** **Tag:** **Pvlan:** ge1/1 ge1/2 ge1/3 ge1/4 ge1/5 ge1/6 ge1/7 ge1/8 ge1/9 ge1/10 ge1/11 ge1/12 ge1/13 ge1/14 ge1/15 ge1/16 ge1/17 ge1/18 ge1/19 ge1/20 ge1/21 ge1/22 ge1/23 ge1/24 ge1/25 ge1/26 ge1/27 ge1/28
10		flood-unknown	**Untag:** ge1/2 **Tag:** **Pvlan:**
20		flood-unknown	**Untag:** ge1/3 **Tag:** **Pvlan:**

Total 3 Entry 20 entrys per page

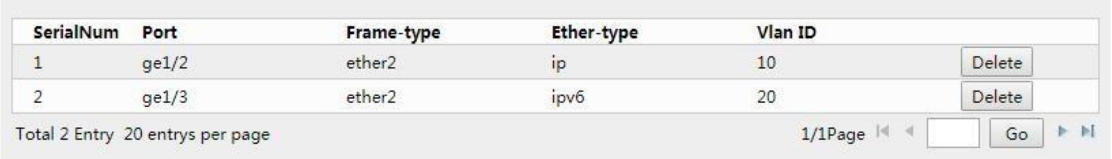
3. Config the Ethernet port ge1/2 & ge1/3 join VLAN under "untag" mode (The operation is the same as above).
4. Config port ge1/1 of the SwitchA join VLAN1- & VLAN20 under "tagged" mode. Click the "Business manage >VLAN config" menu in the navigation tree to enter the interface, input VLAN ID "10", choose ge1/1 in "tag port list", click "add"; input VLAN ID "20", choose ge1/1 in "tag port list", click "add". The interface is shown as the following figure:



VID	Description	Multicast	Port list
1		flood-unknown	**Untag:** **Tag:** **Pvlan:** ge1/1 ge1/2 ge1/3 ge1/4 ge1/5 ge1/6 ge1/7 ge1/8 ge1/9 ge1/10 ge1/11 ge1/12 ge1/13 ge1/14 ge1/15 ge1/16 ge1/17 ge1/18 ge1/19 ge1/20 ge1/21 ge1/22 ge1/23 ge1/24 ge1/25 ge1/26 ge1/27 ge1/28
10		flood-unknown	**Untag:** **Tag:** ge1/1 **Pvlan:**
20		flood-unknown	**Untag:** **Tag:** ge1/1 **Pvlan:**

Total 3 Entry 20 entrys per page 1/1Page Go

5. Click the “Business manage >VLAN config>protocol-vlan apply” menu in the navigation tree to enter the interface, input relative value, bind VLAN10 with ipv4, & bind VLAN20 with ipv6, click “add”. The interface is shown as the following figure:



SerialNum	Port	Frame-type	Ether-type	Vlan ID	
1	ge1/2	ether2	ip	10	Delete
2	ge1/3	ether2	ipv6	20	Delete

Total 2 Entry 20 entrys per page 1/1Page Go

5.2 MAC config

The main function of an Ethernet switch is to forward the message in the data link layer, that is, according to the destination MAC address of the message to output the message to the appropriate port. The MAC address forwarding list is a layer 2 forwarding list that contains the correspondence between the MAC address and the forwarding port. It is the basis of Ethernet switch to realize fast forwarding of layer 2 message.

The list of MAC address contains the following information:

- Destination MAC address
- VLAN ID which the port belongs to
- The forwarding port number of the device

When forwarding the message, Ethernet switch will adopt the following two forwarding modes according to the item information in the MAC address list:

- Unicast mode: when MAC address forwarding list contains corresponding items to the destination MAC address of the message, the switch sends the message directly from the forward port in the table entry.
- Broadcast mode: when the switch receives a message whose destination address is all F, or when the MAC address forwarding list is without an item of corresponding MAC address of the message, the switch will use broadcast mode to forward the message to all ports except the receiving port.

5.2.1 MAC config

In this page, you can set the MAC address aging time and view MAC address table information.

To accommodate network changes, the MAC address table needs to be updated constantly.The automatically generated table items in the MAC address table are not always valid. Each table item has a life cycle, and the table items that do not get refreshed after reaching the life cycle will be deleted. This life cycle is called aging time.If the record is refreshed before reaching the lifetime, the aging time of the table item is recalculated.

The MAC address aging function can be effectively implemented by setting the appropriate aging time.If the aging time set by the user is too short, it may cause the switch to broadcast a large number of data packets that cannot find the destination MAC address, and affect the performance of the switch.

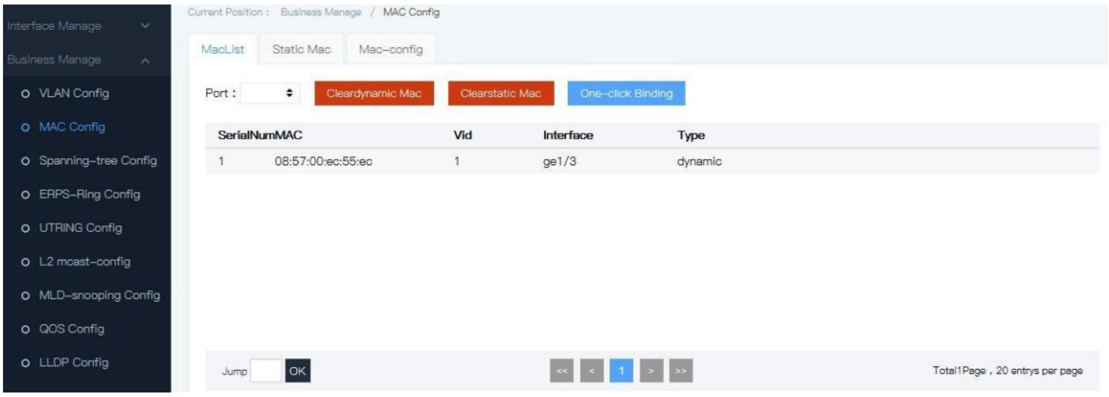
If the aging time set by the user is too long, the switch may save many outdated MAC address table entries, thus exhausting the MAC address forwarding resources, resulting in the switch being unable to update the MAC address forwarding as the network changes.

If the aging time set by the user is too short, the switch may remove a valid MAC address table entry, reducing forwarding efficiency.

In general, the recommended default of the aging time is 300 seconds

Operation steps:

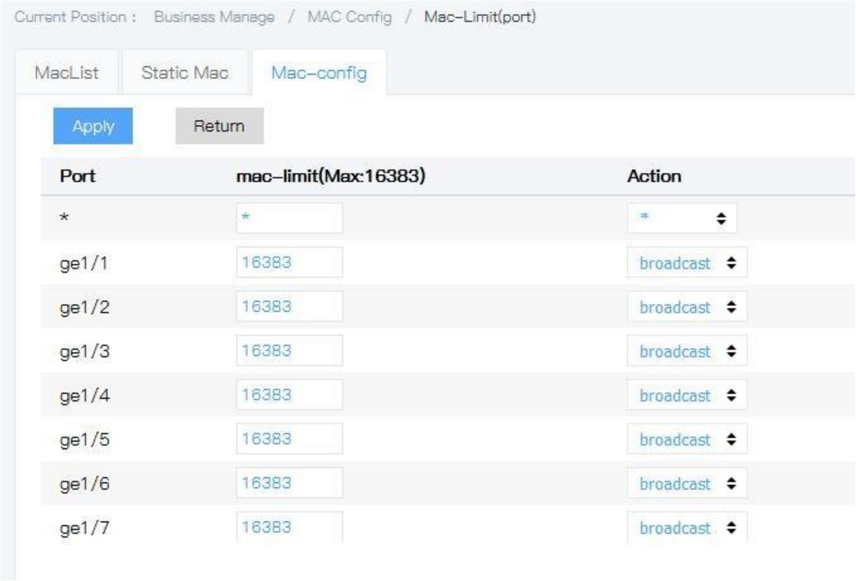
1. Click the "business manage > MAC config " menu in the navigation tree to enter the "MAC config" interface.



SerialNum	MAC	Vid	Interface	Type
1	08:57:00:ec:55:ec	1	ge1/3	dynamic

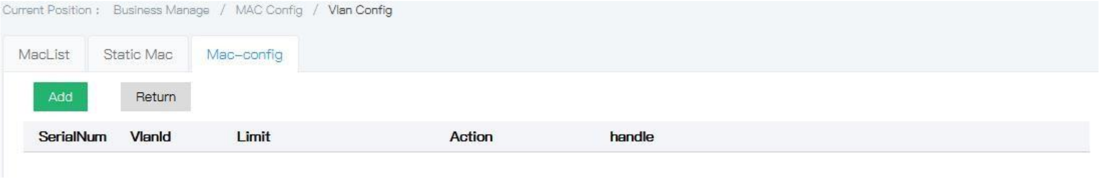
Total1Page , 20 entrys per page

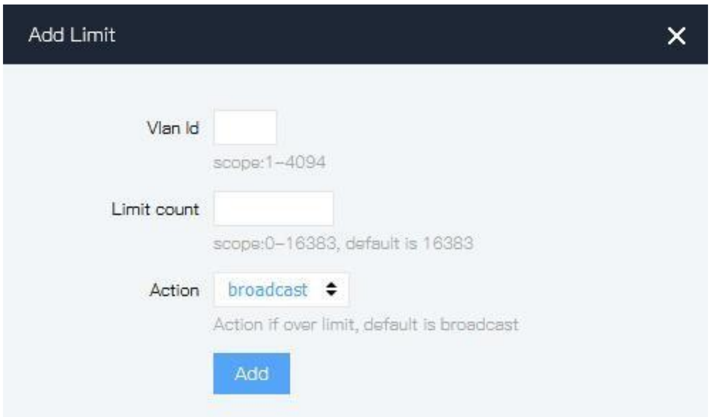
MAC limit(port):


Current Position : Business Manage / MAC Config / Mac-Limit(port)
MacList
Static Mac
Mac-config
Apply
Return

Port	mac-limit(Max:16383)	Action
*	*	*
ge1/1	16383	broadcast
ge1/2	16383	broadcast
ge1/3	16383	broadcast
ge1/4	16383	broadcast
ge1/5	16383	broadcast
ge1/6	16383	broadcast
ge1/7	16383	broadcast

MAC limit(vlan):




Add Limit
Vlan Id
scope:1-4094
Limit count
scope:0-16383, default is 16383
Action
broadcast
Action if over limit, default is broadcast
Add

Explanations

Configuration item	Meaning
MAC aging time	Input MAC aging time, default is 300s, scope: 10-1000000s
Mac-limit	Mac-limit, scope:0-16383， The setting value needs to be modified before the setting takes effect.

2. Fill corresponding configuration items.

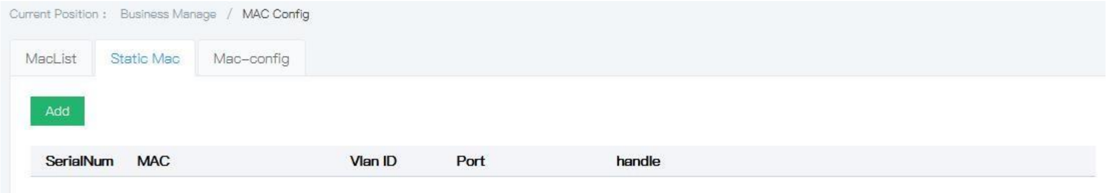
3. Click “add”

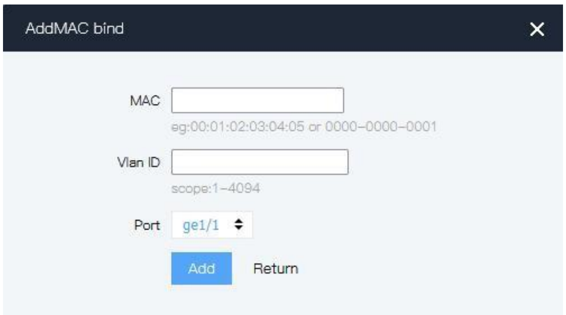
5.2.2 Static MAC

Static table items are manually configured by the user and sent to the interface board, table items do not age.

Operation steps

1. Click the "business management > MAC config > static MAC" menu in the navigation tree to enter the "static MAC" interface as shown below.





Explanations

Configuration item	**Meaning**
MAC	Necessary option, input new create MAC address, such as:H-H-H
Vlan ID	Necessary option, specified VLAN ID
Port	Necessary option, choose the port name, such as： ge1/3。 Remarks The ports should be the member ports of the VLAN

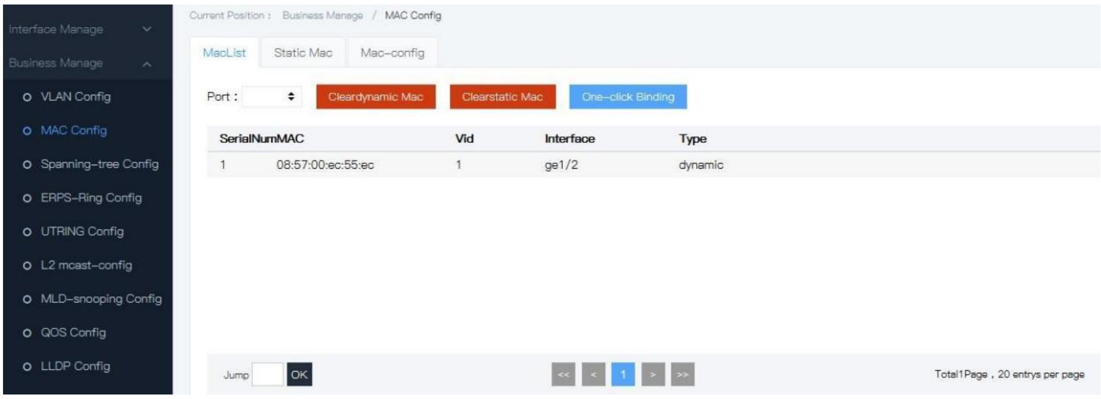
2. Fill corresponding configuration items.
3. Click “add”.

5.2.3 MAC List

The MAC table is used to store the MAC address, VLAN number, and output interface information of other devices learned by the switch. When forwarding the data, the MAC table is queried according to the destination MAC address and VLAN number in the Ethernet frame to quickly locate the outgoing interface of the device.

Operation steps

1. Click the “Business manage >MAC config >MAC LIST” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



SerialNum	MAC	Vid	Interface	Type
1	08:57:00:ec:55:ec	1	ge1/2	dynamic

Total1Page，20 entrys per page

Explanations

Item	**Meaning**
Serial num	Number
MAC	Destination MAC address
Vid	VLAN ID
Interface	Interface number
Type	Dynamic MAC address refers to the MAC address list item that can be aged according to the aging time configured by the user. Switch can add dynamic MAC address list item through MAC address learning mechanism or manually established by the user.

5.3 MSTP config

A switched network is divided into several regions through MSTP and several spanning trees are generated in each region, which are mutually independent. Each spanning tree is called an MSTI (Multiple Spanning Tree Instance) and each region is called an MST region (Multiple Spanning Tree Region).

MSTP is compatible with STP and RSTP and can make up their defects. It can converge quickly and make different VLAN traffics be forwarded along their respective paths, providing a better load sharing mechanism for the redundant links.

The comparison is shown in Figure below:

Protocol	**Feature**	**Application**
STP	Form a tree without loop, solve broadcast storm and realize redundant backup. Slow convergence.	Without differentiating user or business flow, all vlans share a tree.
RSTP	Form a tree without loop, solve broadcast storm and realize redundant backup. Fast convergence.	
MSTP	Form a tree without loop, solve broadcast storm and realize redundant backup. Fast convergence. Multiple spanning trees realize load balancing among vlans, and flow of different vlans is forwarded according to different paths.	Have to distinguish user or business flow, and implement load sharing. Different vlans forward flow through different trees, and each tree is independent from each other.

After deploying the spanning tree protocol in the Ethernet switching network, if a loop appears in the network, the spanning tree protocol can be implemented through topology calculation:

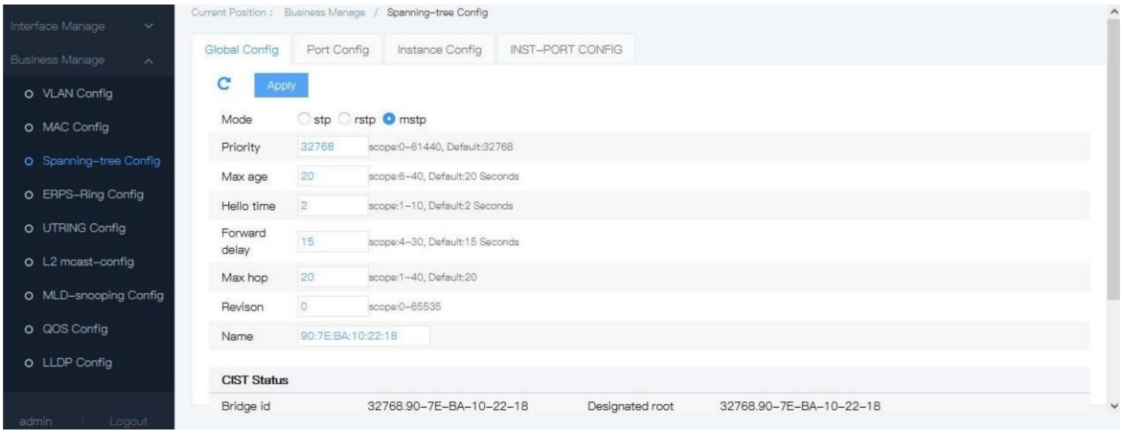
- Eliminate the loop: eliminate network communication loop by blocking redundant link
- Link backup: when the current active path failure occurs, it activates the redundancy backup link, so as to restore network connectivity.

5.3.1 Global config

Provides the ability to configure STP global parameters, and in some specific network environments, the STP parameters of some devices need to be adjusted for best results.

Operation steps

1. Click the “Business manage >Spanning-tree config> Global config” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



Current Position : Business Manage / Spanning-tree Config

Mode ○ stp ○ rstp ● mstp

Priority	32768	scope:0-61440, Default:32768
Max age	20	scope:6-40, Default:20 Seconds
Hello time	2	scope:1-10, Default:2 Seconds
Forward delay	15	scope:4-30, Default:15 Seconds
Max hop	20	scope:1-40, Default:20
Revison	0	scope:0-65535
Name	90:7E:BA:10:22:18	

CIST Status

Bridge id	32768.90-7E-BA-10-22-18	Designated root	32768.90-7E-BA-10-22-18

Explanations

Configuration item	**Meaning**
Enable Spanning-tree	Default is check, means the switch enable spanning-tree
Mode	Support STP, RSTP, MSTP mode
Priority	Scope 0-61440, Step order value is 4096。
Max age	Means the max age of the message, range: 6-40s, default is 20s
Hello time	Represents the period of message sending. The bridge sends hello message to the surrounding bridge at regular intervals to confirm whether there is a fault in the link. This interval is hello
Forward Delay	Represents the delay of port state migration, with a range of 4 to 30 seconds and a default of 15 seconds.
Max Hops	Select the maximum jump number. This value ranges from 1 to 20, with a default value of 20. The maximal jump number of trees in MST domain is used to limit the network size of trees in MST domain. Starting from the root bridge of the generation tree in the MST domain, the jump number is reduced by 1 for each configuration message in the domain forwarded by a switch. The switch will discard the configuration message with the jump number of 0, making the switch outside the maximum jump number unable to participate in the calculation of the generation tree, thus limiting the size of the MST domain.
Revision	MSTP revision level. The revision level of the MSTP is used in conjunction with the domain name and VLAN mapping table to determine the MST domain to which the switch belongs.
Name	MST domain name. The default value is the MAC address of the main control board of the switch. The domain name of the switch device is used together with the VLAN mapping table of the MST domain and the revision level of the MSTP to determine which domain the switch device can belong to.

2. Fill corresponding configuration items.

3. Click “add”.

E.G.

Through MSTP, a switched network is divided into multiple regions, and multiple spanning trees are formed in each region, and the spanning trees are independent of each other.Each Spanning Tree Instance is called a Multiple Spanning Tree Instance, and each domain is called an MST Region.

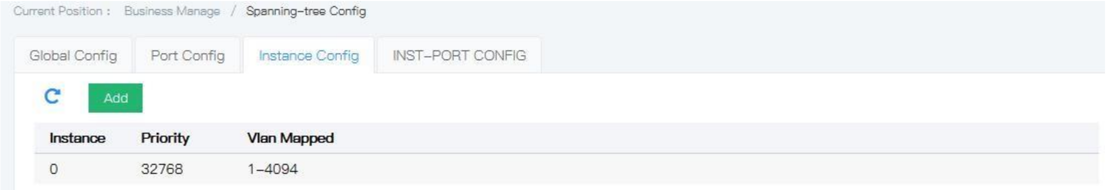
📖 Explanation：

An instance is a collection of multiple vlans. By binding multiple vlans to one instance, you can save communication overhead and resource occupancy. The calculation of each instance topology of MSTP is independent of each other, and load balancing can be achieved on these instances. Multiple vlans of the same topology can be mapped to an instance, and the forwarding state of these vlans on the port depends on the state of the port in the corresponding MSTP instance.

It is mapping of one or more vlans to the specified MST instance. One or more vlans can be assigned to one instance of the spanning tree at a time.

Operation steps：

1. Click the "business manage > MSTP config > instance config" menu in the navigation tree, the interface is shown as below.



Instance	Priority	Vlan Mapped
0	32768	1-4094

Explanations

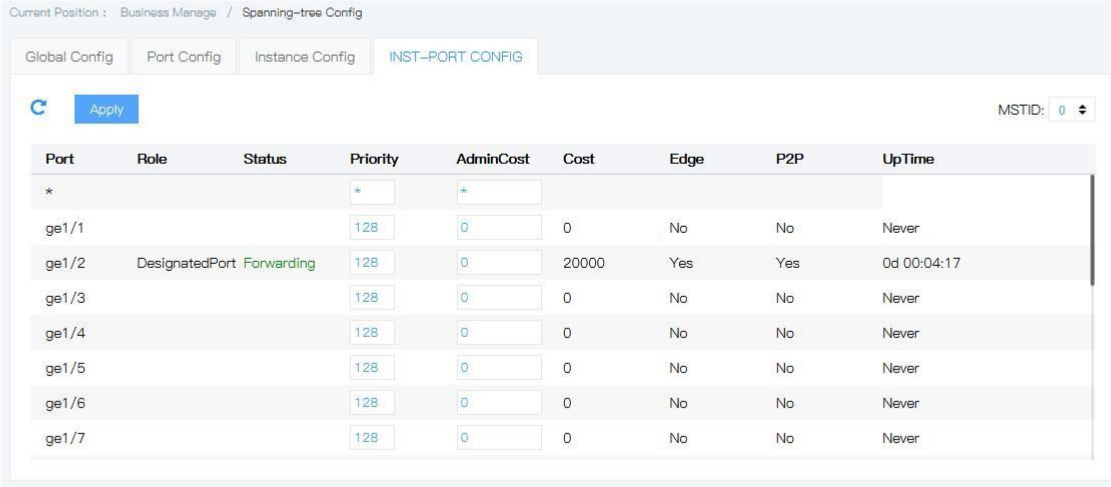
Configuration item	**Meaning**
MSTI ID	Scope: 1–63
Priority	Sets the priority of the specified instance, which must be a multiple of 4096. Scope: 0 to 65535, default value: 32768.
Vlan Mapped	Input VLAN to be mapped

2. Fill corresponding configuration items.

3. Click “add”.

5.3.2 Inst-port config

1. Click the "business manage > MSTP config > inst-port config" menu in the navigation tree, the interface is shown as below.



Current Position : Business Manage / Spanning-tree Config

Global Config | Port Config | Instance Config | INST-PORT CONFIG

Apply

MSTID: 0

Port	Role	Status	Priority	AdminCost	Cost	Edge	P2P	UpTime
*			*	*				
ge1/1			128	0	0	No	No	Never
ge1/2	DesignatedPort	Forwarding	128	0	20000	Yes	Yes	0d 00:04:17
ge1/3			128	0	0	No	No	Never
ge1/4			128	0	0	No	No	Never
ge1/5			128	0	0	No	No	Never
ge1/6			128	0	0	No	No	Never
ge1/7			128	0	0	No	No	Never

Explanations

Configuration item	Meaning
MSTID	Select the configured instance from the drop-down menu
Port	Fixed value, displayed according to user selection, do not support multiple selections.
Enable	Fixed value, displayed according to user selection, do not support multiple selections.
Instance	Up to 63 instances can be created
Priority	Select port priority. The smaller the value, the higher the priority. Interface priority can affect the role of the interface on the specified MSTI. Users can configure different priorities for the same interface on different MSTI, so that flow from different VLAN can be forwarded along different physical links, completing the function of sharing load by VLAN. Note: when interface priorities change, the MSTP recalculates the role of the interface and performs a state migration.
Admincost	Enter the path overhead value of the interface. The range of values under IEEE 802.1t standard is 1 ~ 200000000
Cost	The range of value under IEEE 802.1t standard is 1~200000000
Role	designated， alternated， Disabled
Status	Discarding or forwarding

2. Fill corresponding configuration items.

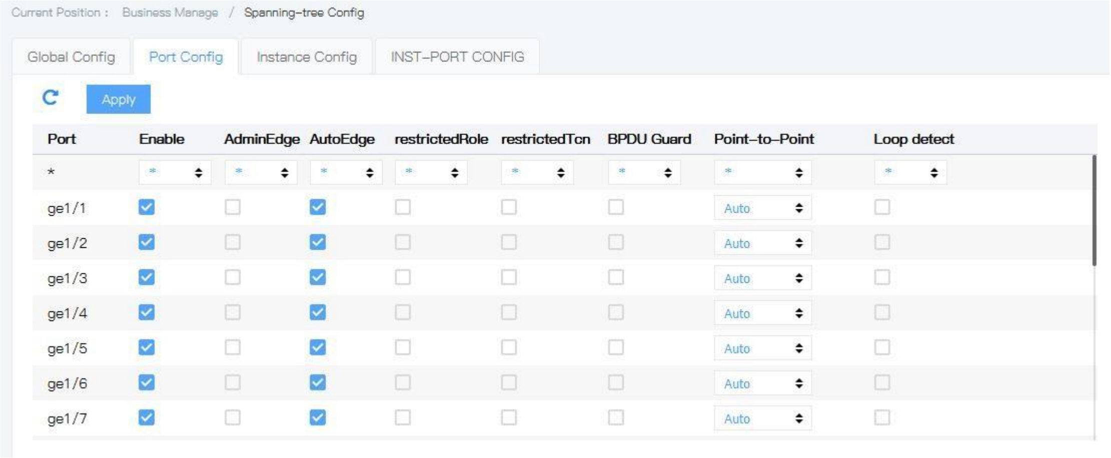
3. Click “add”.

5.3.3 Port config

In some specific network environments, the STP parameters of some switch device interfaces need to be adjusted for best results.

1. Click the “Business manage >MSTP config> port config” menu in the navigation tree to

enter the interface, the interface is shown as the following figure:



Port	Enable	AdminEdge	AutoEdge	restrictedRole	restrictedTcn	BPDU Guard	Point-to-Point	Loop detect
*	*	*	*	*	*	*	*	*
ge1/1	☑	□	☑	□	□	□	Auto	□
ge1/2	☑	□	☑	□	□	□	Auto	□
ge1/3	☑	□	☑	□	□	□	Auto	□
ge1/4	☑	□	☑	□	□	□	Auto	□
ge1/5	☑	□	☑	□	□	□	Auto	□
ge1/6	☑	□	☑	□	□	□	Auto	□
ge1/7	☑	□	☑	□	□	□	Auto	□

Explanations

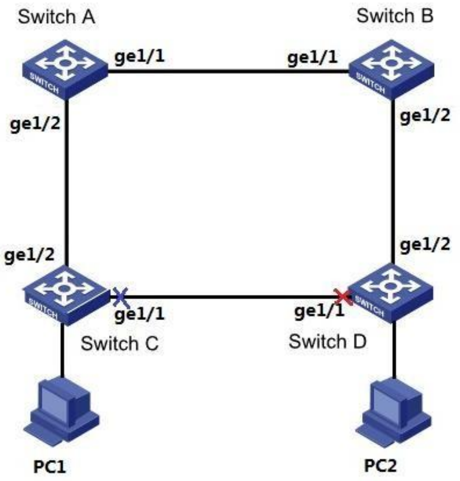
Configuration item	Meaning
Port	No option. Port list
Enable	Select enable opening port configuration or not. There are two choices of to check and not to check. The default is not to check.
BPDU Guard	Select whether to turn on the protection function of BPDU. There are two choices of to check and not to check. The default is not to check. When the BPDU protection function is enabled on the device, if the edge interface receives the BPDU, the device will close these interfaces and notify the network management system. The closed interfaces can only be restored manually by network administrators.
Edge	Edge ports should be directly connected to the user terminal, not another switch or network segment. Edge ports can quickly transit to a forward state, because on edge ports, changes in network topology do not create loops. By setting a port to an edge port, the spanning tree protocol allows it to transit quickly to the forward state. It is recommended that Ethernet ports connected directly to the user terminal be configured as edge ports so that they can quickly transit to the forward state. Choose Force True, Force False & automation
Point-to-Point	Choose Force True, Force False & automation Indicates the state that automatically detection which the port is set to default if connected to a point-to-point link Force-true Indicates that a particular port is connected to a point-to-point link.

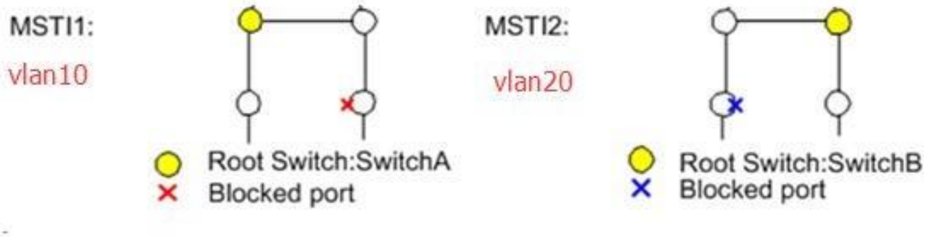
	Force-false Indicates that a particular port is not connected to a point-to-point link.

2. Fill corresponding configuration items.
3. Click “add”.

E.G.

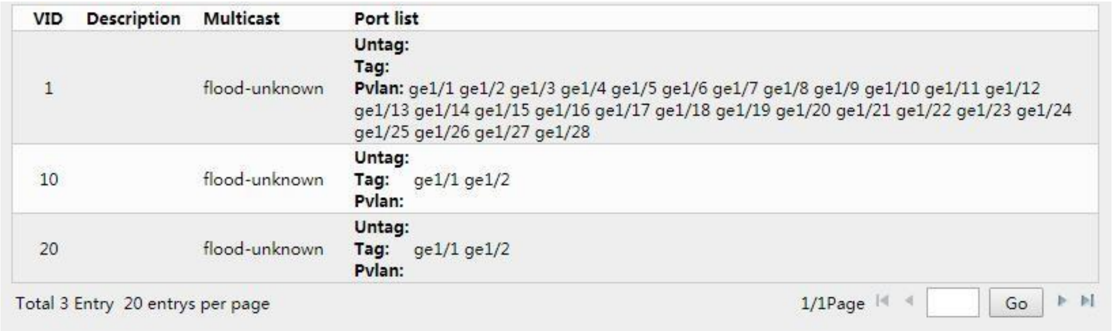
SwitchA, SwitchB, SwitchC, and SwitchD all run MSTP.MSTP introduces multiple instances for VLAN10 and VLAN20 flow load sharing. MSTP can set the VLAN mapping table to associate the VLAN with the generated tree instance, instance 1 mapping to VLAN10, and instance 2 mapping to VLAN20.





Operation steps

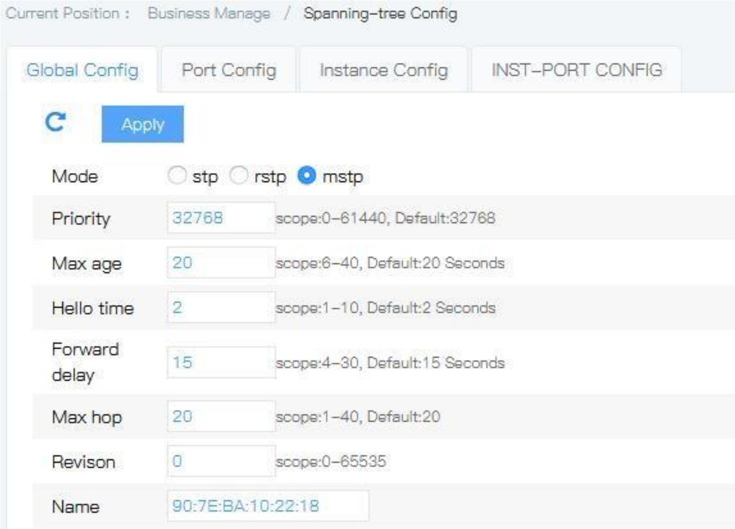
1. Add the ports which connect in the LINK into VLAN. Click the “Business manage >VLAN config >VLAN apply” menu in the navigation tree to enter the interface, allow VLAN10 & VLAN20 via Trunk, tick the Tag list “ge1/1、ge1/2”, click “add”, the interface is shown as the following figure:



VID	Description	Multicast	Port list
1		flood-unknown	**Untag:** **Tag:** **Pvlan:** ge1/1 ge1/2 ge1/3 ge1/4 ge1/5 ge1/6 ge1/7 ge1/8 ge1/9 ge1/10 ge1/11 ge1/12 ge1/13 ge1/14 ge1/15 ge1/16 ge1/17 ge1/18 ge1/19 ge1/20 ge1/21 ge1/22 ge1/23 ge1/24 ge1/25 ge1/26 ge1/27 ge1/28
10		flood-unknown	**Untag:** **Tag:** ge1/1 ge1/2 **Pvlan:**
20		flood-unknown	**Untag:** **Tag:** ge1/1 ge1/2 **Pvlan:**

Total 3 Entry 20 entrys per page 1/1Page Go

2. Configure SwitchA, SwitchB, SwitchC & SwitchD into the domain name RUNDATA. Click the “Business manage >MSTP config >Global config” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



Current Position : Business Manage / Spanning-tree Config

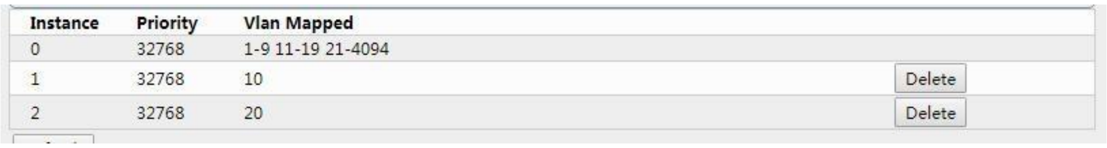
Global Config | Port Config | Instance Config | INST-PORT CONFIG

Apply

Mode ○ stp ○ rstp ● mstp

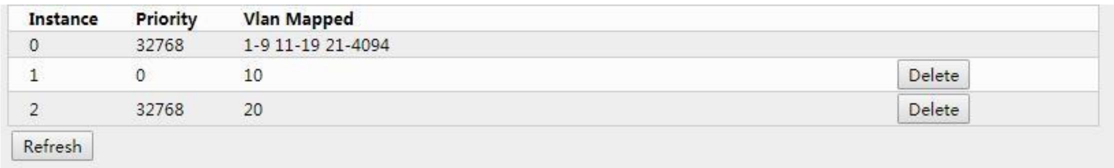
Priority	32768	scope:0-61440, Default:32768
Max age	20	scope:6-40, Default:20 Seconds
Hello time	2	scope:1-10, Default:2 Seconds
Forward delay	15	scope:4-30, Default:15 Seconds
Max hop	20	scope:1-40, Default:20
Revison	0	scope:0-65535
Name	90:7E:BA:10:22:18	

3. Create MSTI1 & MSTI2. Click the “Business manage >MSTP config >Instance config” menu in the navigation tree to enter the interface, input related data, click “add”, the interface is shown as the following figure:



Instance	Priority	Vlan Mapped	
0	32768	1-9 11-19 21-4094	
1	32768	10	Delete
2	32768	20	Delete

4. In RUNDATA, configure MSTI1 & MSTI2 root bridge & backup root bridge, configure switchA as the root bridge of MSTI1, SwitchA as the backup bridge of MSTI2. Click the “Business manage >MSTP config >Instance config” menu in the navigation tree to enter the interface, the interface is shown as the following figure



Instance	Priority	Vlan Mapped	
0	32768	1-9 11-19 21-4094	
1	0	10	Delete
2	32768	20	Delete

Refresh

⚠Attentions :

When configuring SwitchA, change the priority of MSTI1 to 0 and the priority of MSTI2 to 4096.

When configuring SwitchB, change the priority of MSTI1 to 4096 and the priority of MSTI2 to 0. The configuration method is the same as SwitchA and will not be repeated.

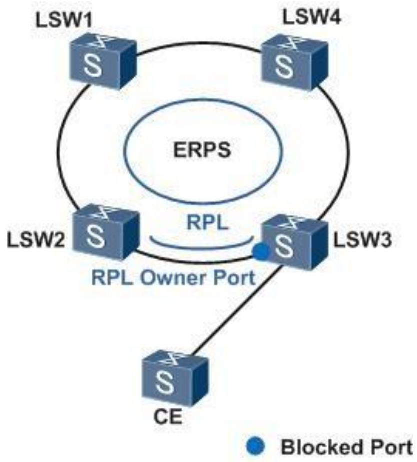
The priority must be a multiple of 4096

4. In the domain RUNDATA, configure the root bridge and backup root bridge of MSTI1 and MSTI2. Configure SwitchB as the root bridge of MSTI2, and the backup root bridge of MSTI1.
5. After above configuration, the network is pruned into tree, so as to eliminate the loop.

5.4 ERPS config

ERPS (Ethernet Ring Protection Switching) is a protocol for Ethernet link layer loop breaking. It takes the ERPS ring as the basic unit and contains several nodes. By blocking the RPL Owner port and controlling other normal ports, the port state can be switched between Forwarding and STP ding to eliminate the loop. At the same time, we use control VLAN, data VLAN and protection instance mechanism to better realize the function of ERPS.

As shown in the figure below, CE is connected to A-Ring network composed of LSW1 ~ LSW4.Such access mode can make the network have certain reliability, but in order to eliminate the loop in the network and effectively ensure the link connectivity, it needs to start a loop breaking mechanism.



Port role

There are three types of port roles in ERPS protocol: RPL owner port, RPL neighbor port and general port. RPL Neighbor is a port type supported by ERPSv2, but not by V1.

- RPL owner port

An ERPS ring has only one RPL Owner, as determined by user configuration. The RPL Owner port is blocked to prevent the creation of a loop in the ERPS ring.

When the device where the RPL owner is located receives a fault message and learns that other nodes or links on the ERPS ring fail, it will automatically open the RPL owner port, and this port will resume the receiving and sending of traffic to ensure that the traffic will not be interrupted.

The Link where the RPL Owner is located is known as the Ring Protection Link.

- RPL neighbor port

A RPL neighbor is a port directly connected to the RPL owner port.

Normally, both the RPL Owner port and the RPL Neighbor port are blocked to prevent the creation of a loop.

When the ERPS ring fails, both the RPL Owner port and the RPL Neighbor port are released.

The RPL neighbor port role is introduced to reduce the number of FDB entries flushed by the device that hosts the RPL neighbor port.

- Common Port

In the ERPS ring, all ports other than RPL Owner and RPL Neighbor are normal ports.

Common ports are responsible for monitoring the link state of their directly connected ERPS protocol and notifying other ports of changes in link state.

Control the VLAN

In the ERPS ring, the control VLAN is used to deliver ERPS protocol messages.

Each ERPS ring must be configured to control the VLAN. When a port joins the ERPS ring that has been configured to control the VLAN, the port will automatically join the control VLAN.

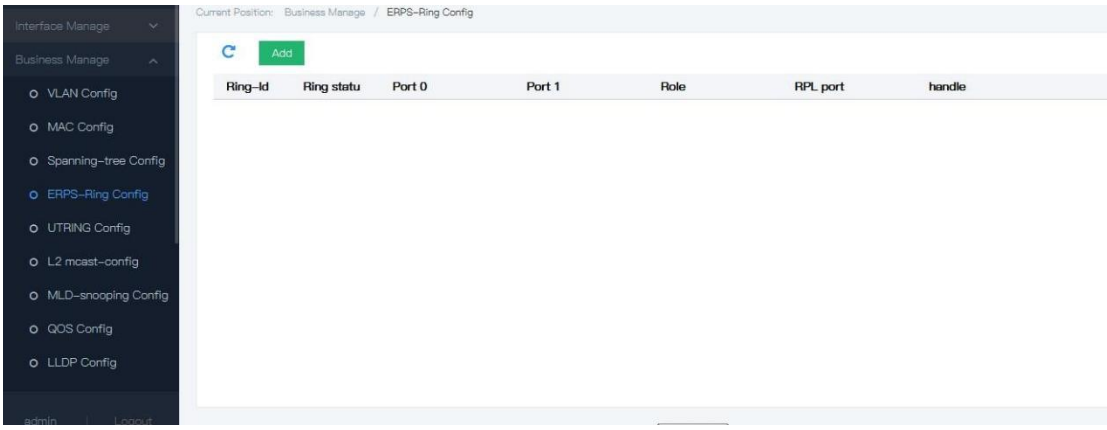
Different ERPS rings cannot use the same ID to control the VLAN.

In contrast to a control VLAN, a data VLAN is used to transmit data packets.

5.4.1 ERPS configuration information displayed

Operation steps

1. Click the "Business manage > ERPS config" menu in the navigation tree to enter the interface, the interface is shown as the following figure:



Ring-Id	Ring statu	Port 0	Port 1	Role	RPL port	handle

Explanations

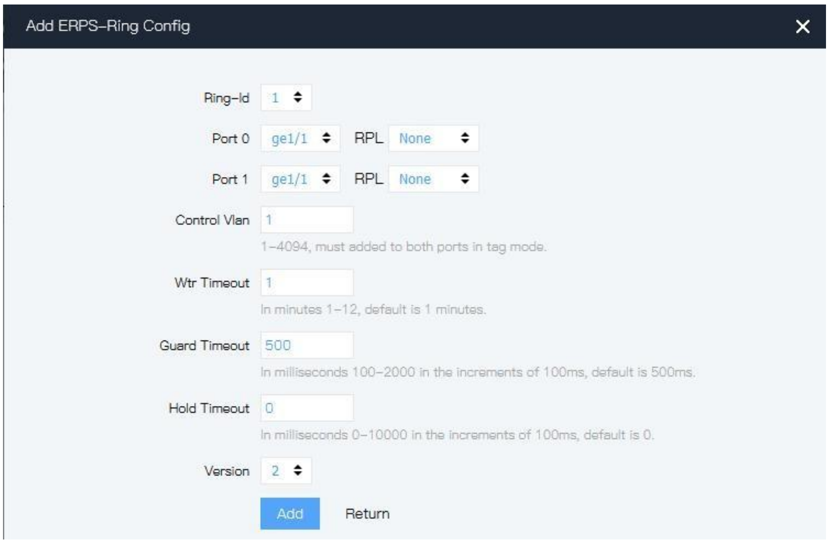
Configuration	Meaning

item	
Ring- Id	ERPS ring ID
Ring state	ERPS Ring state（protected,idle, PENDING）

5.4.2 Add ERPS

Operation steps

1. Click the “Business manage > ERPS config” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



Add ERPS-Ring Config ✕

Ring-Id 1

Port 0 ge1/1 RPL None

Port 1 ge1/1 RPL None

Control Vlan 1
1-4094, must added to both ports in tag mode.

Wtr Timeout 1
In minutes 1-12, default is 1 minutes.

Guard Timeout 500
In milliseconds 100-2000 in the increments of 100ms, default is 500ms.

Hold Timeout 0
In milliseconds 0-10000 in the increments of 100ms, default is 0.

Version 2

Add Return

Explanations

Configuration item	Meaning
Ring- Id	ERPS ring ID
Port role	RPL Neighbor\Owner\none
Control vlan	Control vlan
Wtr Timeout	When the RPL Owner port is released due to the fault of other devices or links, if the fault is restored, and some ports may not be changed from Down state to Up state, in order to prevent blocking the RPL Owner port immediately and causing blocking point shock, when the RPL Owner port receives the NR RAPS message of a certain port, Start the WTR Timer, and close the WTR Timer if it receives a SF RAPS message from another port before the Timer timeouts. If no SF RAPS message is received on any other port before the WTR Timer timeouts, the RPL Owner port is blocked and the NRRB RAPS message is sent after the WTR Timer timeouts. Other ports will set the Forwarding state of their ports to Forwarding state after receiving the article.
Guard Timeout	The device involved in a link or node failure sends NR RAPS

	packets to other devices after recovery or cleanup operation and starts Guard Timer at the same time. The purpose is to prevent the receipt of expired NR RAPS packets before the Timer timeout. If the NR message sent by other ports can be received after the timer timeout, the Forwarding state of this port will change to Forwarding state.
Hold Timeout	For the two-layer network running ERPS, the order of protection reversal may have different requirements. For example, in the application of multi-layer service, after the server failure, the user may want to recover the server failure for a period of time, but the client can not perceive the fault, that is, the protection reversal will not be carried out immediately. The appropriate Holdoff Timer can be set so that when a malfunction occurs, the malfunction is not immediately reported to the ERPS, and only if the malfunction fails to recover after the Holdoff Timer has timed out.
Version	Version V2、V1

5.5 A-Ring config

5.5.1 Overview

5.5.1.1 Node type

A-Ring ring physically corresponds to an Ethernet topology connected in A-Ring manner. The role of the A-Ring ring is decided by the user through configuration.

Master

Master is a main decision and control node on the A-Ring ring. There must be a Master on each A-Ring only.

Each switch on the Ethernet ring is called a node and there must be one Master on each A-Ring ring only. Master is an initiator of the Polling mechanism (automatic detection mechanism of the ring network state) and decider of operation execution after the network topology is changed.

Master periodically sends the HELLO message from its main port, which is spread on the ring through all Transfers. If the standby port can receive the HELLO message sent by the Master, it means that the ring network link is complete; if it does not receive the HELLO message within the specified time, the ring network link is deemed to be faulty. Master has the following two states:

- Complete State

When all links on the ring network are in an UP state, Master can receive the HELLO message sent by itself from the standby port, it means that Master is in a Complete state. The state of Master reflects the state of the A-Ring ring. Therefore, the A-Ring ring is also in a Complete state. At this moment, Master will block the standby port to prevent the data message from forming a broadcast loop on the ring topology.

- Failed State

When the link on the ring network is in a Down state, Master will be in a Failed state. At this moment, Master will open the standby port to ensure that the communication of all nodes on the ring network will not be interrupted.

Transfer

Except Master, all other nodes on the ring can be called transmission ports. There may be several Transfers or no Transfer (in fact, such networking is meaningless) on a A-Ring ring.

Each A-Ring ring physically corresponds to an Ethernet topology connected in A-Ring form and the A-Ring ring is identified with an ID expressed in an integer.

Except Master, all other nodes on the A-Ring ring are Transfers, which are responsible for monitoring the state of their directly connected A-Ring link and notifying the Master change in the link. Master will decide how to handle it. The Transfer has 3 states as follows:

- Link-Up State

When Master and standby port of the Transfer are in an UP state, it means that the Transfer is in a Link-Up state.

- Link-Down State

When Master or standby port of the Transfer is in a Down state, it means that the Transfer is in a Link-Down state.

- Preforwarding State

When Master or standby port of the Transfer is in a Preforwarding state, it means that the Transfer is in a Preforwarding state.

When the Transfer in an Link-Up state detects that the main port or standby port has link Down, it will move from an Link-Up state to an Link-Down state and send an Link-Down message to notify Master.

The Transfer will not directly move from the Link-Down state to the Link-Up state. When some port of the Transfer in the Link-Down state has link Up and the main port and standby port recover to the Up accordingly, the Transfer will move to the Preforwarding state and block the recovered port.

At the moment when the main and standby ports of the Transfer, Master cannot be informed of it immediately. Therefore, the standby port is still in an Up state. If the Transfer immediately moves to the Link-Up state immediately, it will necessarily cause the data message to form a broadcast loop on the ring network. Therefore, the

Transfer first moves from the Link-Down state to the Preforwarding state.

When the Transfer in a Preforwarding state receives the COMPLETE-FLUSH-FDB message sent by Master, it will move to the Link-Up state. If the COMPLETE-FLUSH-FDB message will not be lost during transmission, the A-Ring protocol also provides a backup mechanism to recover the temporarily blocked port and trigger state switching, i.e. if the Transfer cannot receive the COMPLETE-FLUSH-FDB message within the specified time, it will move to the Link-Up state automatically and open the temporarily blocked port.

5.5.1.2 Port role

Main port and standby port

Master and Transfer have access to the Ethernet ring through a main port and standby port and the port role is decided by the user's configuration.

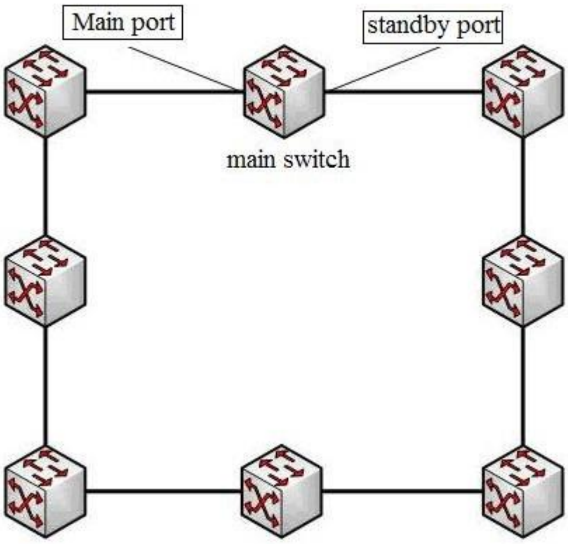
The main port and standby port of Master have different functions. Master sends the loop state detection message from its main port. If this message can be received by the standby port, it means that the A-Ring ring network of this node is complete. Therefore it is necessary to block the stand by port to prevent the data loop; on contrary, if the detection message cannot be received within the specified time, it means that the ring network is out of order. It is necessary to open the standby port to ensure normal communication of all nodes on the ring. The main port and standby port of the Transfer have the same function. The port role is also decided by the user's configuration.

5.5.1.3 Topology type

Single ring

Each A-Ring ring physically corresponds to an Ethernet topology connected in A-Ring form, in which there is a main switch only. This main switch is an initiator of the Polling mechanism (automatic detection mechanism of the ring network state) and decider of operation execution after the network topology is changed.

The typical topology diagram is shown below:

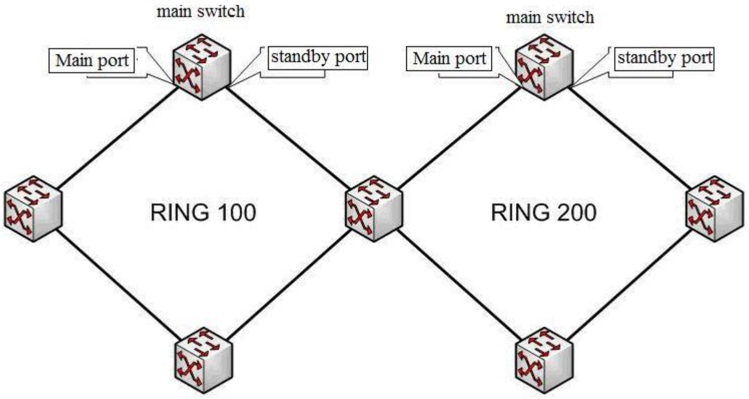


Single Ring

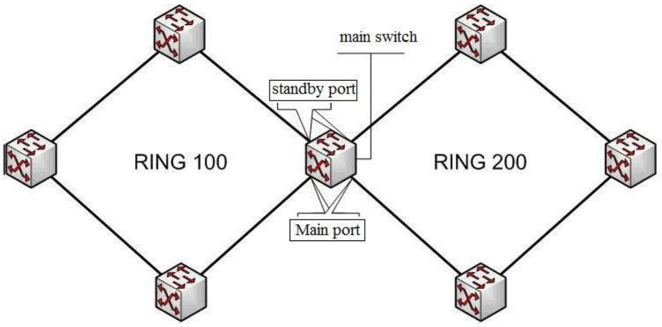
Tangent ring

Tangent ring means that two or more A-Rings share a common switch, without public ports. All A-Rings in the tangent ring follow the single ring mechanism, which will not affect each other. Its configuration is basically consistent with that of the single ring, but several A-Rings shall be configured for the public switch.

The typical topology diagram is shown below:



Tangent Ring with Tangency at Transfer

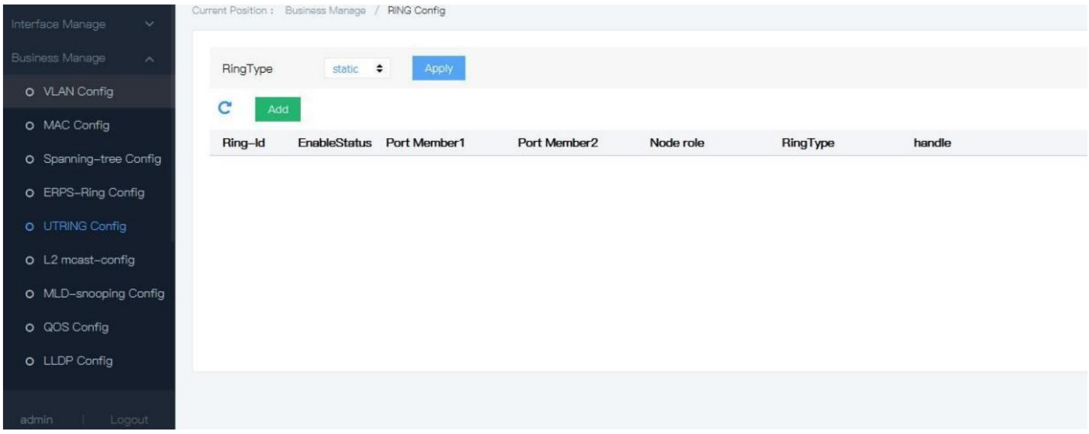


Tangent Ring with Tangency at Master

5.5.2 Port configuration

1. Panel description

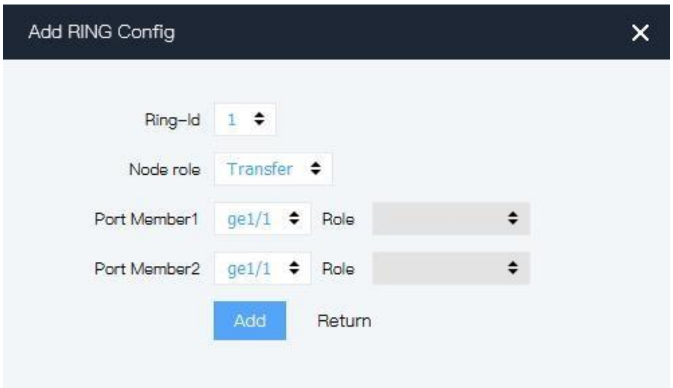
Set the basic parameters of the ring. The interface configuration is shown in Figure below:



Current Position : Business Manage / RING Config

RingType static

Ring-Id	EnableStatus	Port Member1	Port Member2	Node role	RingType	handle



Add RING Config

Ring-Id: 1

Node role: Transfer

Port Member1: ge1/1 Role:

Port Member2: ge1/1 Role:

2. Explanations of keywords

Configuration item	Meaning
Ring Type	Dynamic and static ring networks. Dynamic loop network indicates that the master switch is uncertain and changes with the change of topology. The main characteristic is that no convergence time is needed when the link is restored. The main characteristic of static ring network is that no matter how the topology changes, the main switch is fixed, but the convergence time is needed for link recovery.
ring ID	The number of the ring network can be distinguished according to the ring ID, which ranges from 1 to 16
The frist port member	The first port member of the ring network. Each member of the ring may contain at most two ports. Each switch may have more than one ring.
The second port member	The second port member of the ring network
system type	System types include Transfer (transmission node) and Master (Master node).
The node role	The type of a port member changes according to the system type. When the system is Master, the type of the member is Master and Subsidiary; When the system is Transfer, its member is of type None;

3. Operation steps

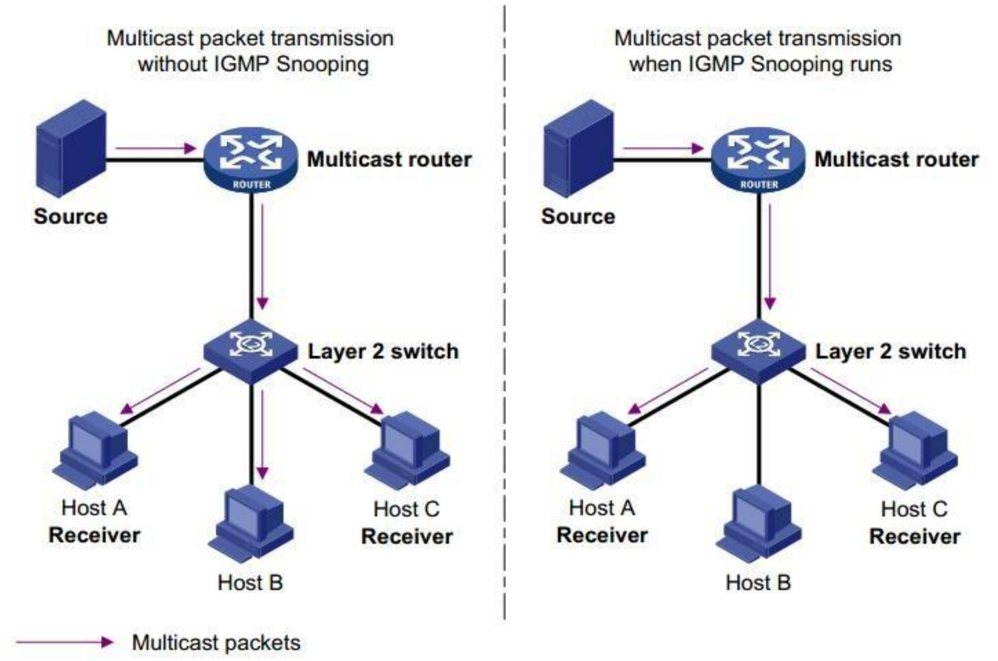
Step 1	Click the “Configuration management > UTRing configmenu in the navigation tree to enter the “UT Ring port configuration” interface.
Step 2	Fill in the corresponding configuration item and click “Submit”.
Step 3	If it shall be used as start configuration, enter the “System maintenance” and “Save settings” for save the settings.

5.6 L2-mcast config

The IGMP Snooping is Multicast constraint mechanism that deployed on the Layer 2 switch, it is used to manage & control the multicast group.

The layer 2 device which running IGMP detection will analyze the received IGMP messages, and establish the mapping relationship for the port & MAC multicast address; at the same time , it will forward the multicast data according to this mapping relationship.

As shown the following figure, when the IGMP detection is not running by layer 2 device, the multicast data is broadcasted on layer 2; when the IGMP detection is running by the layer 2 device, multicast data will not be broadcasted in layer 2, but broadcasted to specified one; unknown multicast data still will be broadcasted in layer 2.



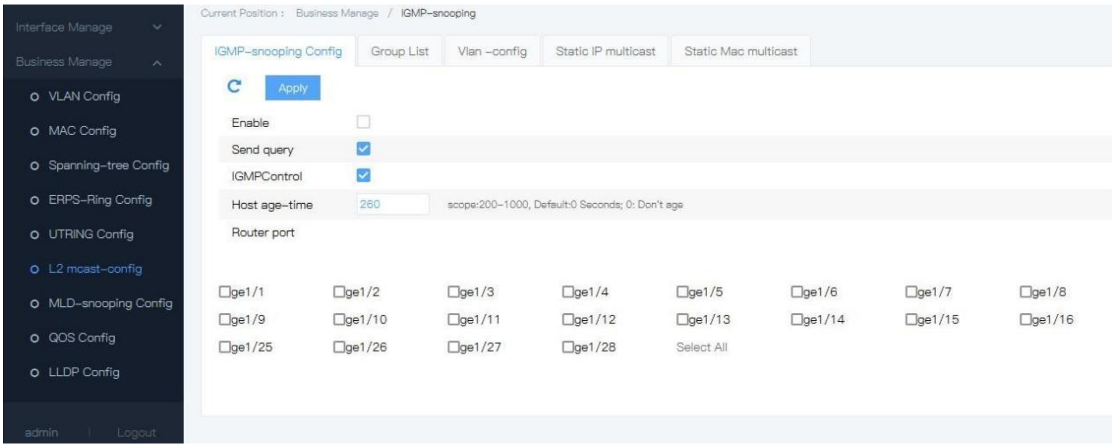
5.6.1 IGMP-snooping config

The IGMP Snooping is deployed on IPv4 network, to be more specific, on the Layer 2 switch between a multicast router and a user host, acting as a listener for IGMP/MLD messages transmitted between the router and the host and creating the forwarding table of multicast packet on Layer 2 switch to manage and control the forwarding of multicast packets on Layer 2 network.

By default, IGMP snooping on the switch is disabled. Therefore, you need to enable the global IGMP Snooping on the switch,

Operation steps

1. Click the “Business manage >L2-mcast-config >IGMP-snooping config” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



Enable ☐

Send query ☑

IGMPControl ☑

Host age-time 260 scope:200-1000, Default:0 Seconds; 0: Don't age

Router port

☐ge1/1 ☐ge1/2 ☐ge1/3 ☐ge1/4 ☐ge1/5 ☐ge1/6 ☐ge1/7 ☐ge1/8
☐ge1/9 ☐ge1/10 ☐ge1/11 ☐ge1/12 ☐ge1/13 ☐ge1/14 ☐ge1/15 ☐ge1/16
☐ge1/25 ☐ge1/26 ☐ge1/27 ☐ge1/28 Select All

Explanations

Configuration item	Description
Enable IGMP-snooping	Single check, enable or disable
Host-age time	When one port add in certain multicast group, the switch launch a timer for this port, the overtime is the host-age time. When overtime, the switch will delete the port in the multicast group far warding table. The scope is 200-1000s, default is 260s

2. Fill corresponding configuration items.

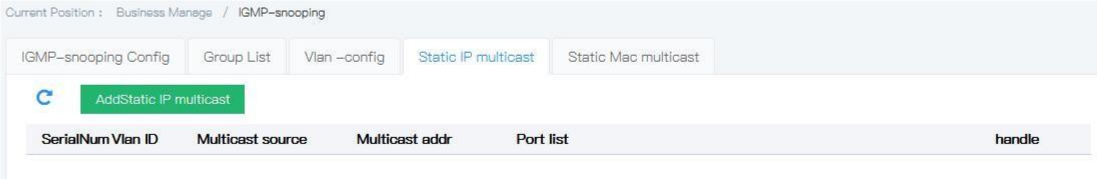
3. Click "add".

5.6.2 Static multicast

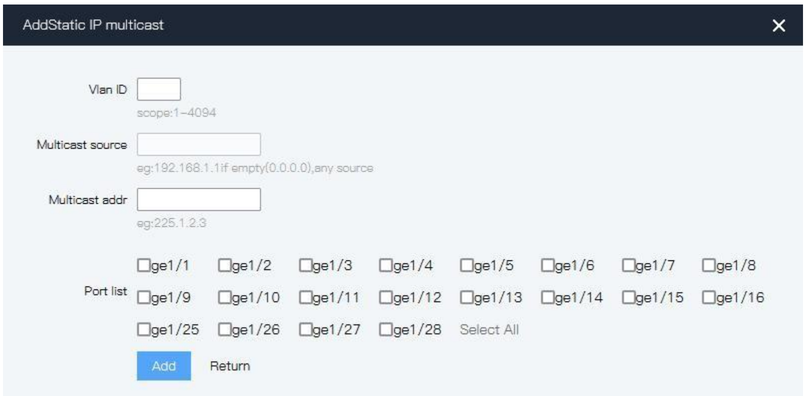
Based on the old multicast mode, when the users in the different VLAN ask for the same multicast, the data on the multicast router will copy and forward the VLAN for every recipient. This mode wastes lots of bandwidth. While enable IGMP Snooping function, the switch ports are added in the multicast VLAN through multicast group VLAN configuration mode. This makes the users in different VLAN share the same multicast VLAN to receive the multicast data; the multicast flow only be transmitted in the same multicast VLAN, this save the bandwidth. And the multicast VLAN is isolated with users VLAN, this ensure the safety and bandwidth stable.

Operation steps

1. Click the "Business manage >IGMP-snooping config >Static IP multicast" menu in the navigation tree to enter the interface, the interface is shown as the following figure:



SerialNum	Vlan ID	Multicast source	Multicast addr	Port list	handle



AddStatic IP multicast ✕

Vlan ID
scope:1–4094

Multicast source
eg:192.168.1.1if empty(0.0.0.0),any source

Multicast addr
eg:225.1.2.3

Port list
□ge1/1 □ge1/2 □ge1/3 □ge1/4 □ge1/5 □ge1/6 □ge1/7 □ge1/8
□ge1/9 □ge1/10 □ge1/11 □ge1/12 □ge1/13 □ge1/14 □ge1/15 □ge1/16
□ge1/25 □ge1/26 □ge1/27 □ge1/28 Select All

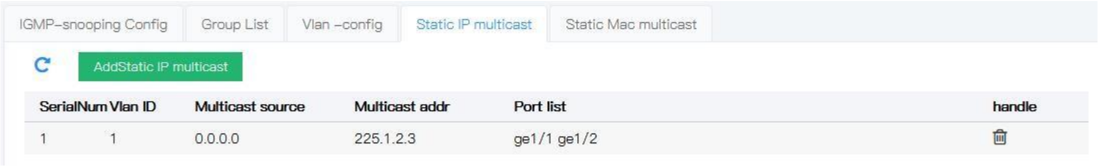
Add Return

Explanations

Configuration item	**Meaning**
Vlan Id	Fixed, it is fixed by the user options. Remarks: ensure the VLAN is created. Input a created VLAN
Source multicast	Input source multicast address
Multicast address	Input multicast address
Port list	Add multicast member

2. Fill corresponding configuration items.

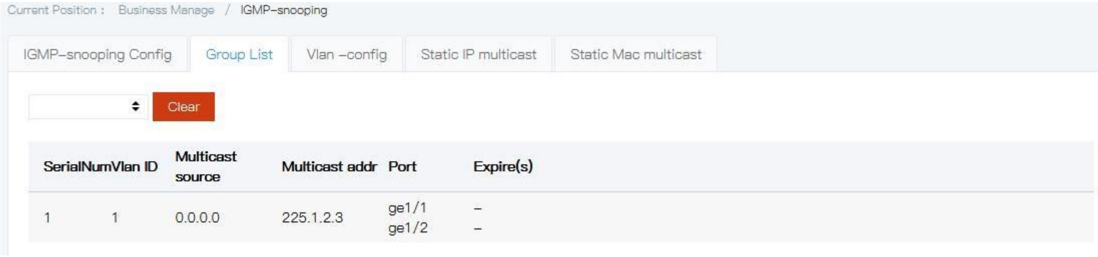
3. Click “add”, the interface is shown as the following figure:



SerialNum	Vlan ID	Multicast source	Multicast addr	Port list	handle
1	1	0.0.0.0	225.1.2.3	ge1/1 ge1/2	🗑

5.6.3 GROUP config

1. Click the “Business manage >L2-mcast-config>IGMP-snooping list” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



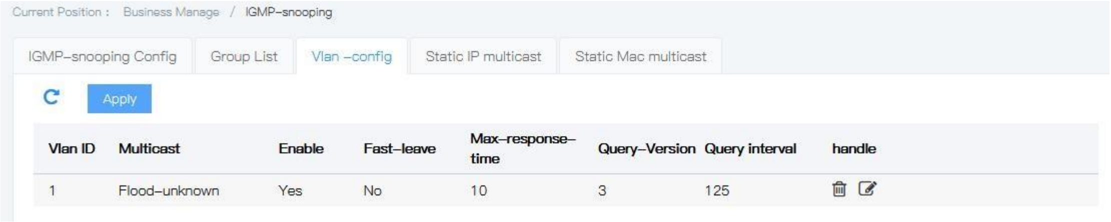
SerialNum	Vlan ID	Multicast source	Multicast addr	Port	Expire(s)
1	1	0.0.0.0	225.1.2.3	ge1/1 ge1/2	– –

2. Choose relative port, click “Clear”.

5.6.4 VLAN config

Operation steps

1. Click the “L2 mcast-config >L2-mcast-config >vlan config” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



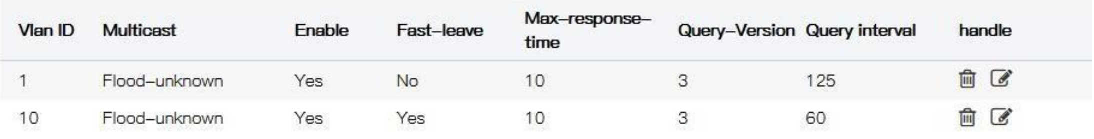
Vlan ID	Multicast	Enable	Fast-leave	Max-response-time	Query-Version	Query interval	handle
1	Flood-unknown	Yes	No	10	3	125	🗑 ✎

Explanations

Configuration item	**Meaning**
Vlan Id	Fixed Remarks: Ensure VLAN is created , input a created VLAN
Fast-leave	Enable/disable, enable is “1”, disable is “0”
Query interval	Scope: 2-1800s

2. Fill corresponding configuration items.

3. Click “add”, the interface is shown as the following figure:



Vlan ID	Multicast	Enable	Fast-leave	Max-response-time	Query-Version	Query interval	handle
1	Flood-unknown	Yes	No	10	3	125	🗑 ✎
10	Flood-unknown	Yes	Yes	10	3	60	🗑 ✎

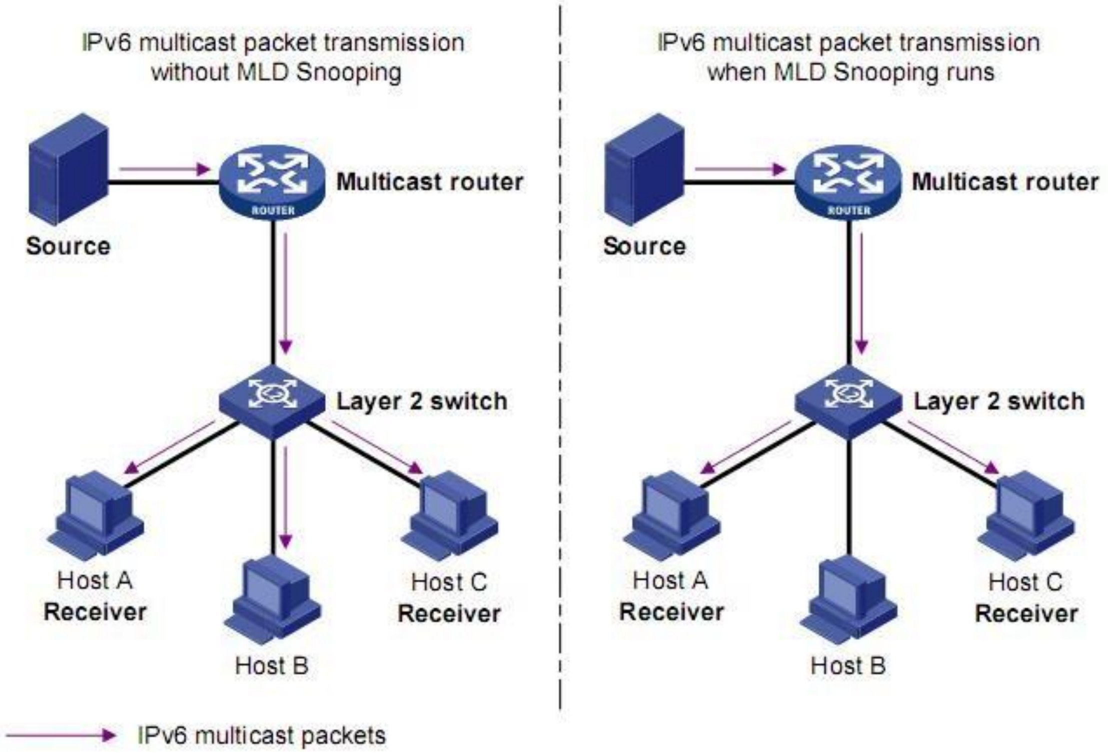
5.7 MLD-Snooping

MLD Snooping (Multicast Listener Discovery Snooping), It is an IPv6 multicast constraint mechanism that runs on Layer 2 devices and is used to manage and control IPv6 multicast groups.

5.7.1 MLD Snooping Principle

A Layer 2 device running MLD Snooping establishes a mapping for port and MAC multicast addresses by analyzing incoming MLD messages and forwards IPv6 multicast data based on such a mapping.

As shown in the figure below, when the Layer 2 device is not running MLD Snooping, IPv6 multicast data messages are broadcast at Layer 2; when the Layer 2 device is running MLD Snooping, multicast data messages of known IPv6 multicast groups are not broadcast at Layer 2, but are multicast to the specified receiver at Layer 2.



Comparison of Layer 2 devices before and after running MLD Snooping

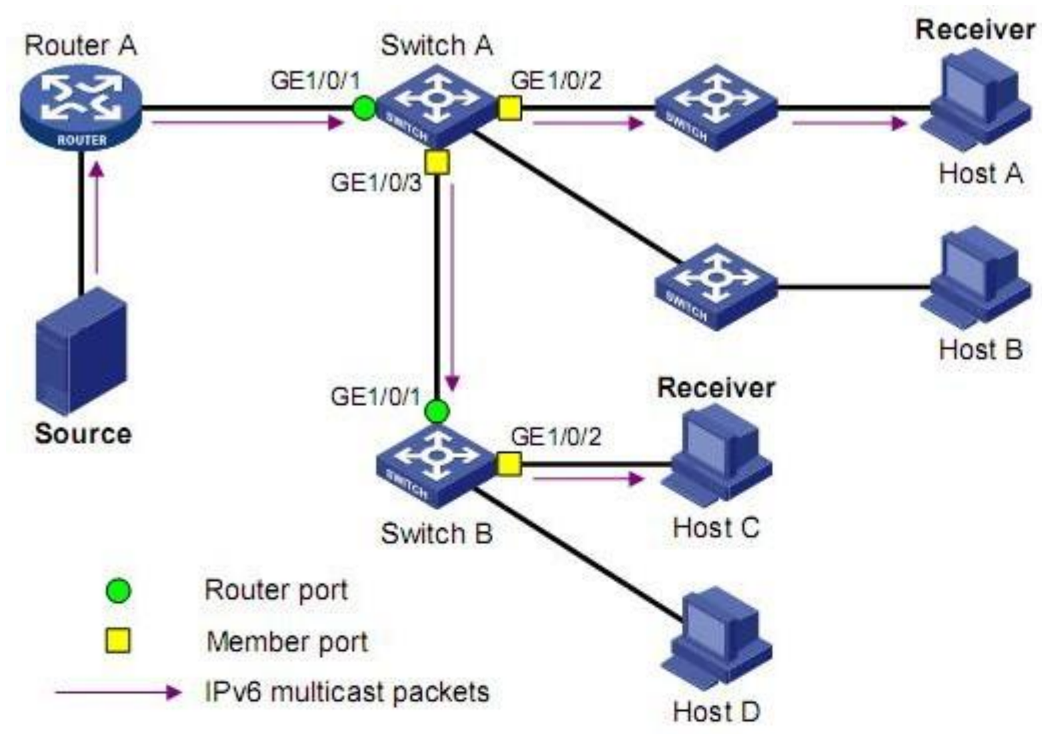
MLD Snooping forwards information via Layer 2 multicast to only those receivers who need it, providing the following benefits.

- Reduce broadcast messages in Layer 2 networks, saving network bandwidth.
- Enhance security of IPv6 multicast packet；
- Brings convenience to independent billing of each host.

5.7.2 MLD Snooping Basic Concept

1. MLD Snooping Related port

As shown in the figure below, Router A connects to the multicast source and runs MLD Snooping on Switch A and Switch B. Host A and Host C are the recipient hosts (i.e. IPv6 multicast group members).



In conjunction with the above diagram, introduce the port concepts associated with MLD Snooping.

Router Port: The port on the switch that faces the side of the Layer 3 multicast device (DR or MLD querier, such as the Gigabit Ethernet 1/0/1 port on each of Switch A and Switch B. The switch records all router ports on this device in the Routing Port list. The switch records all router ports on this device in the routing port list.

Member Port: Also known as IPv6 multicast group member port, it is the port on the switch facing the IPv6 multicast group member side， For example, GigabitEthernet1/0/2 and GigabitEthernet1/0/3 ports of Switch A, and GigabitEthernet1/0/2 port of Switch B.The switch records all member ports on this device in the MLD Snooping forwarding table.

5.7.3 MLD Snooping Working mechanism

A switch running MLD Snooping handles the different MLD actions in the following manner:

1. General query

The MLD querier periodically sends MLD universal group query messages to all hosts and routers (FF02::1) in the local network segment to query which IPv6 multicast groups are members of the segment.

- When an MLD universal group query message is received, the switch forwards it out through all ports in the VLAN except the receiving port and does the following actions for the receiving port of the message:
- If the dynamic router port is already included in the routing port list, reset its aging timer.
- If the dynamic router port is not included in the routing port list, add it to the routing port list and start its aging timer.

2. Report Member Relations

The host sends an MLD member relationship report message to the MLD querier in the following cases:

- When a member host of an IPv6 multicast group receives an MLD query message, it replies with an MLD member relationship report message.
- If a host wants to join an IPv6 multicast group, it proactively sends an MLD membership report message to the MLD querier to declare its membership in the IPv6 multicast group.

When an MLD membership report message is received, the switch forwards it out through all router ports in the VLAN, resolves the IPv6 multicast group address that the host wants to join from the message, and does the following for the receiving port of the message:

- If no forwarding table entry exists for this IPv6 multicast group, create a forwarding table entry, add the port as a dynamic member port to the outgoing port list, and start its aging timer.
- If the forwarding table entry corresponding to this IPv6 multicast group already exists, but the port is not included in its outgoing port list, add the port to the outgoing port list as a dynamic member port and start its aging timer.
- If there is already a forwarding table entry for this IPv6 multicast group and its outgoing port list already contains this dynamic member port, then reset its aging timer.

3. Leave multicast group

When a host leaves an IPv6 multicast group, it notifies the multicast router that it has left an IPv6 multicast group by sending an MLD leave group message. When the switch receives an MLD leave group message from a dynamic member port, it first determines whether the forwarding table entry corresponding to the IPv6 multicast group to be left exists and whether the receiving port is included in the list of outgoing ports of the forwarding table entry corresponding to the IPv6 multicast group:

- If no forwarding table entry exists for the IPv6 multicast group, or if the outgoing port list for the corresponding forwarding table entry for the IPv6 multicast group does not contain the port, the switch does not forward the message to any port, but discards it directly.
- If there is a forwarding table for the IPv6 multicast group and the outgoing port list of the corresponding forwarding table for the IPv6 multicast group contains this port, the switch forwards the message through all router ports in the VLAN. At the same time, since it is not known whether there are other members of the IPv6 multicast group under the receiving port, the switch does not immediately remove the port from the outgoing port list of the corresponding forwarding table for the IPv6 multicast group, but resets its aging timer.

When the MLD querier receives an MLD leave group message, it resolves the address of the IPv6 multicast group that the host wants to leave and sends an MLD specific group query message to that IPv6 multicast group through the receive port. After receiving the MLD group-specific query message, the switch forwards it out through all router ports in the VLAN and all member ports of the IPv6 multicast group. For the receiving port of an MLD leave group message (assumed to be a dynamic member port), the switch, during its aging time:

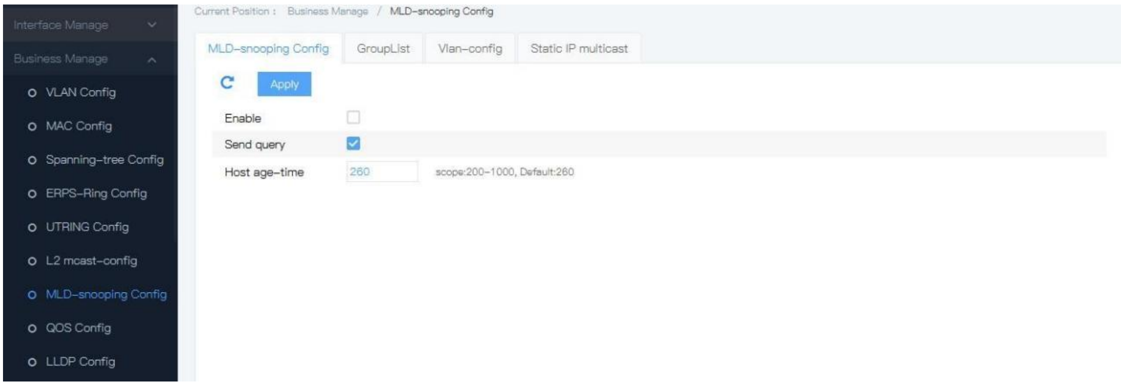
- If an MLD membership relationship report message is received from that port from a host in response to a query for that particular group, it indicates that there are still members of that IPv6 multicast group under that port and resets its aging timer.

- If no MLD membership relationship report message is received from this port from a host in response to this group-specific query, it means that there are no more members of this IPv6 multicast group under this port, and then it is removed from the outgoing port list of the forwarding table entry corresponding to this IPv6 multicast group after its aging time has expired.

5.7.4 MLD-Snooping Configuration

Operation step

1.Click "Service Management" in the navigation bar> MLD-Snooping Configuration” Menu, Enter the "MLD-Snooping Configuration" interface, as shown in the following figure.



Enable □
Send query ☑
Host age–time 260 scope:200–1000, Default:260

The meaning of the interface information is shown in the following table

Configuration item	**Description**
Enable MLD-Snooping Configuration	If MLD-Snooping is globally disabled, it is not possible to configure MLD-Snooping under VLAN. Single option, divided into two states(enable and disable), the default is disable.
Host aging time	When a port joins a multicast group, the switch starts a timer for the port with a timeout that is the host port aging time. After the timeout, the switch removes the port from the forwarding table of the multicast group. The value ranges from 200 ~ 1000 seconds, and the default value is 260 seconds.

2.Fill in the appropriate configuration items.

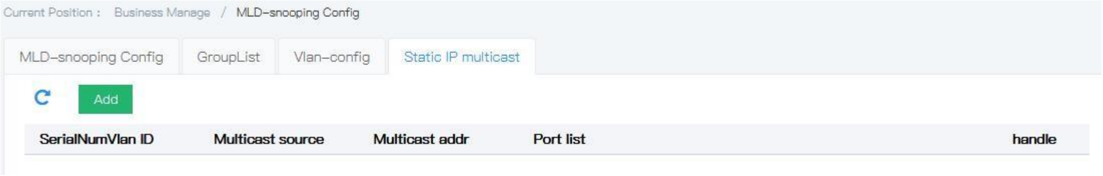
3.Click "Setting" to complete the configuration.

5.7.5 Static Multicast

Based on the previous multicast on-demand approach, when users in different VLANs demand the same multicast group, the data is replicated and forwarded on the multicast router for each VLAN including the recipient. Such a multicast on-demand approach wastes a lot of bandwidth. After the MLD-Snooping function is activated, the switch ports are added to the multicast VLAN by configuring the multicast VLAN, so that users in different VLANs share one multicast VLAN to receive multicast data, and multicast streams are transmitted only in one multicast VLAN, thus saving bandwidth. And because multicast VLANs are completely isolated from users, both security and bandwidth are guaranteed.

Operation step

1.Click "Service Management" in the navigation > MLD-Snooping > Static IP Multicast" menu, enter the "Static IP Multicast" interface as shown in the following figure.



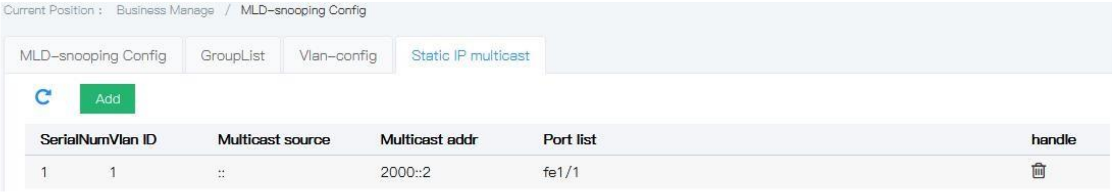
The meaning of the interface information is shown in the table below.

Configuration item	Description
Vlan Id	Fixed according to the data selected by user Description: Enter a VLAN that has been created
Multicast Source	Enter the multicast source address
Multicast address	Enter the multicast address
Port list	Add multicast member, you can select more than one

The meaning of the interface information is shown in the table below.

2.Click "Add" to fill in the appropriate configuration items.

3.Click "Setting" to complete the configuration, as shown below.

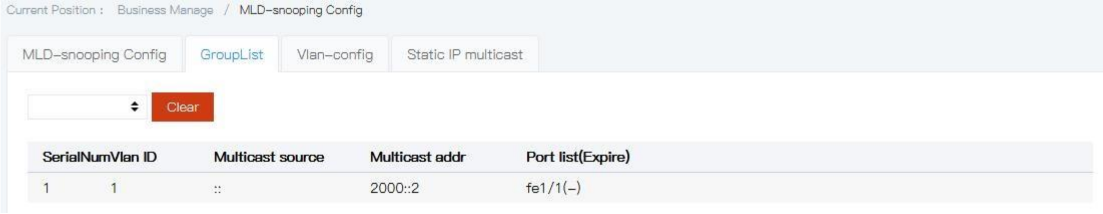


SerialNum	Vlan ID	Multicast source	Multicast addr	Port list	handle
1	1	::	2000::2	fe1/1	🗑

5.7.6 group list

Operation step

1.Click "Service Management" in the navigation > MLD-Snooping Configuration > Group List" menu, enter the "Group List" interface as shown in the figure below.



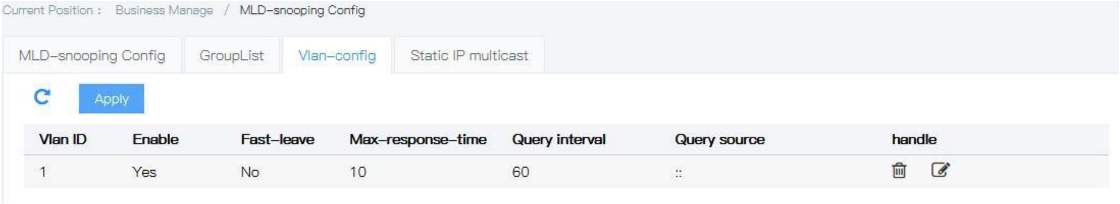
SerialNum	Vlan ID	Multicast source	Multicast addr	Port list(Expire)
1	1	::	2000::2	fe1/1(–)

2.Select the appropriate interface and click "Clear".

5.7.7 VLAN Setting

Operation step

1.Click "Service Management" in the navigation > MLD-Snooping Configuration > VLAN setting"menu， enter the "VLAN setting"interface as shown in the figure below.


Current Position : Business Manage / MLD-snooping Config

MLD-snooping Config | GroupList | Vlan-config | Static IP multicast

Apply

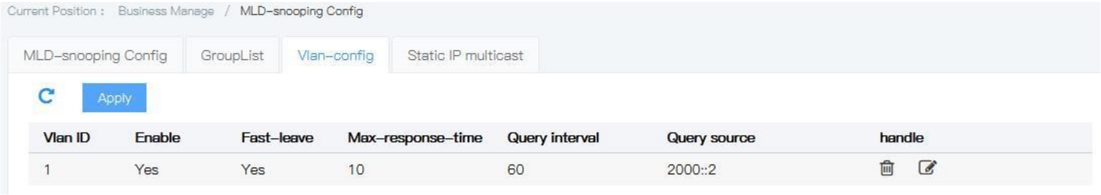
Vlan ID	Enable	Fast-leave	Max-response-time	Query interval	Query source	handle
1	Yes	No	10	60	::	

The meaning of the interface information is shown in the table below.

Configuration item	**Description**
Vlan Id	Fixed according to the data selected by user Description: Enter a VLAN that has been created
Fast leave multicast	Enable/disable fast leave multicast. Enable to show 1, Disable to show 0
Query message interval	Range: 2-1800 seconds

2.Click "Add" to fill in the appropriate configuration items.

3.Click "Setting" to complete the configuration, as shown below.


Current Position : Business Manage / MLD-snooping Config

MLD-snooping Config | GroupList | Vlan-config | Static IP multicast

Apply

Vlan ID	Enable	Fast-leave	Max-response-time	Query interval	Query source	handle
1	Yes	Yes	10	60	2000::2	

5.8 QOS config

In network services, the Quality of Service (QoS) includes the transmission bandwidth, transmission delay and packet loss rate. In the network, the QoS can be improved by ensuring the transmission bandwidth, reducing the transmission delay, minimizing the data packet loss rate and delay jitter.

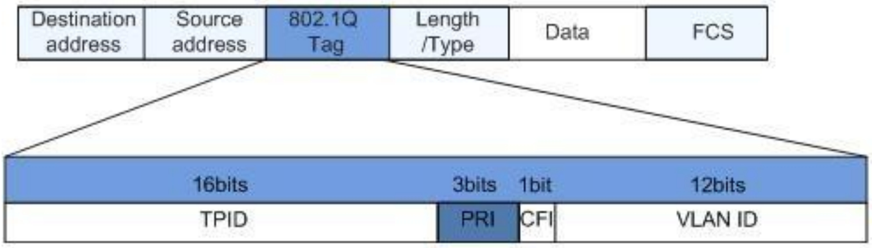
QoS can be used to regulate network traffic, avoid and manage network congestion, and reduce packet loss rate, which also supports provision of dedicated bandwidth to users, different service quality for different services, improve the network service capabilities.

Different packets are assigned different QoS precedence. For example, VLAN packets are assigned the 802.1p or Class of Service (CoS) field and IP packets are assigned the DSCP. When packets are transmitted through different networks, in order to maintain the precedence of the packets, you need to configure the mappings between these precedence fields at the gateways connecting different networks.

802.1p precedence in VLAN header

The VLAN frames are usually transmitted between Layer 2 devices. According to the definition of IEEE 802.1Q, the PRI (802.1p precedence) field or the CoS (Class of Service) field in the VLAN header identifies theQoS requirement.

802.1p precedence in VLAN frames

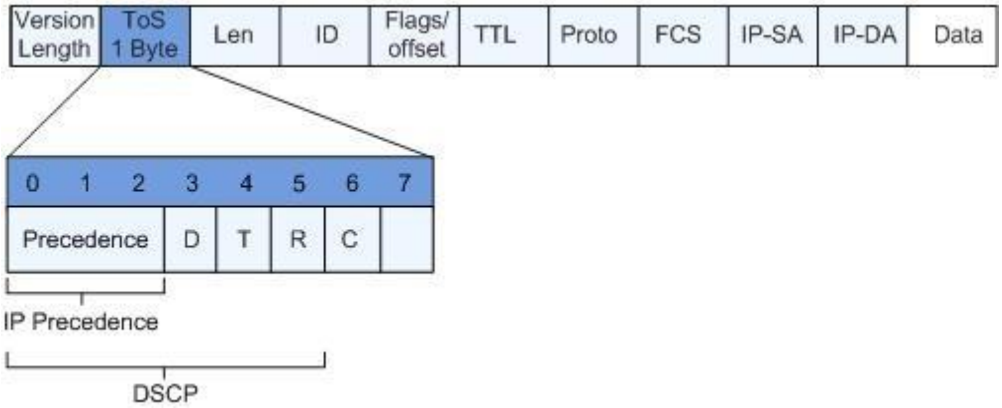


The 802.1Q header contains a 3-bit long PRI field, which defines eight types of business precedence CoS, i.e. 7,6, ..., 1 and 0 in descending order of precedence.

IP Precedence/DSCP field

According to the definition of RFC791, the ToS（Type of Service）field of an IP packet header is composed of 8 bits, of which the 3-bit Precedence field identifies the precedence of the IP packet. The location of the Precedence in the packet is shown in the figure below.

IP Precedence/DSCP field



The bits from 0 to 2are the Precedence field, which represents the eight precedence levels of packet transmission,i.e. 7,6, ..., 1, and 0 in descending order of precedence. 7 or 6 represents the highest precedence, which is often reserved for routing or updating network control traffic. The user-level applications can only take the precedence from 0 to5.

In addition to the Precedence field, the ToS field also includes three bits, i.e. D, T and R, of which Indicates the delay requirement (0 stands for normal delay and 1 stands for low delay). T represents throughput (0 stands for normal throughput and 1 stands for high throughput). R indicates reliability (0 stands for normal reliability and 1 stands for high reliability). The 6th and 7th bits in the ToS field are reserved.

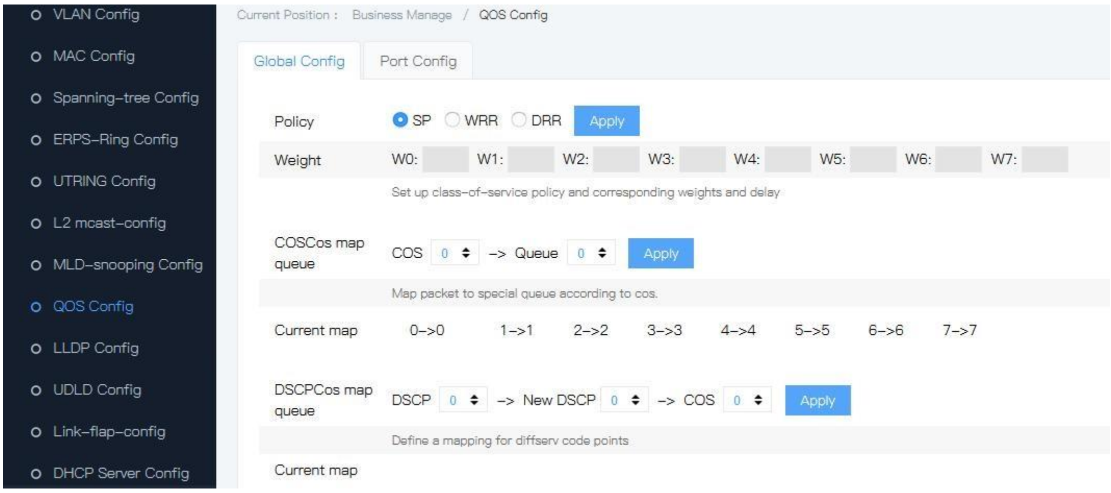
As specified in DiffServ system, each message will be classified into different categories in the network. The classified information is contained in the IP packet header. The DiffServ system uses the first 6 bits of Type of Service (TOS) in the IP packet header to carry the packet classification information. This definition is valid only for the lower 6bits and is a number less than 63. This definition supports both IPv4 (ToS fields) and IPv6 (Traffic Class fields). There are 64 DSCP precedence values(0-63).

5.8.1 QOS Global config

In the case of network congestion, it is necessary to solve the problem of multiple messages competing for resources at the same time. Congestion management usually adopts queue scheduling technology to avoid intermittent congestion in network. Queue scheduling technologies include: SP (Strict Priority), WRR (Weighted Round Robin), DRR scheduling (DRR (Deficit Round Robin) scheduling is also an extension of RR).

Operation steps

1. Click the “Business manage >QOS config >Global config” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



Policy ● SP ○ WRR ○ DRR

Weight W0: W1: W2: W3: W4: W5: W6: W7:

Set up class-of-service policy and corresponding weights and delay

COSCos map queue COS 0 -> Queue 0

Map packet to special queue according to cos.

Current map 0->0 1->1 2->2 3->3 4->4 5->5 6->6 7->7

DSCPCos map queue DSCP 0 -> New DSCP 0 -> COS 0

Define a mapping for diffserv code points

Current map

Explanations

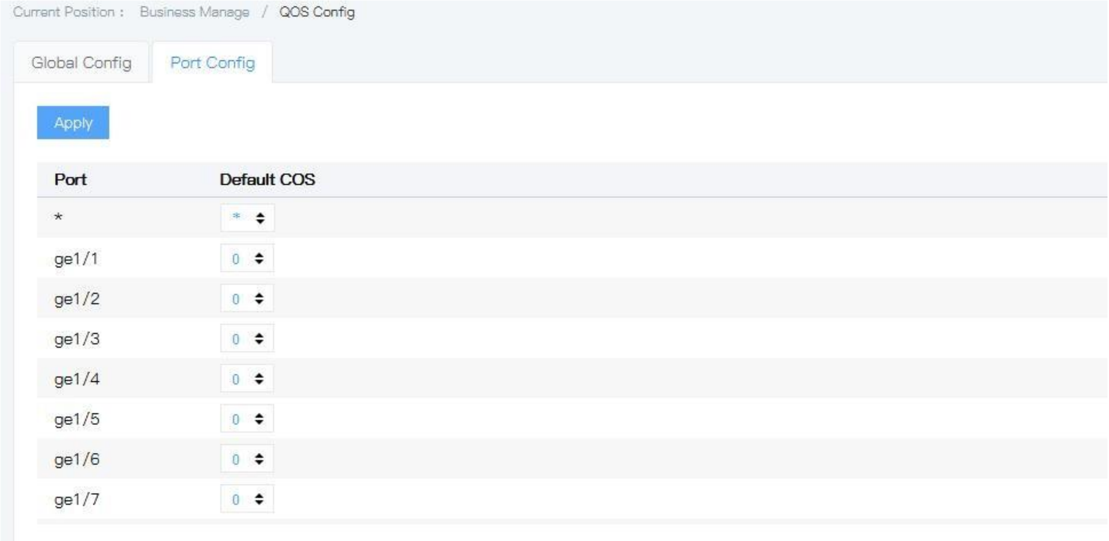
Configuration item	Meaning
SP	SP queue scheduling algorithm is designed for key business applications. A key feature of critical business is the requirement that services be given priority in the event of congestion to reduce latency in response. Taking 8 output queues of ports as an example, the priority queue divides 8 output queues of ports into 8 classes, which are successively 7, 6, 5, 4, 3, 2, 1 and 0 queues. Their priorities are lowered in turn.
WRR	WRR queue scheduling algorithm takes turns among the queues to ensure that each queue gets a certain service time. For example, if there are 8 output queues on the port, WRR can configure a weighting value for each queue (w7, w6, w5, w4, w3, w2, w1, w0 are the corresponding weighted values in order).
DRR	DRR (Defict Round Robin) scheduling is also an extension of RR. Compared with WRR, WRR only cares about messages, and the actual bandwidth obtained by big size messages is greater than that obtained by small size messages under the same scheduling opportunity. The packet length factor is taken into account in the scheduling process, so as to achieve the scheduling rate equity.
DSCP	Range 0-63

New DSCP	Range 0-63
Cos	Range 0-7
Queue	Range 0-7
Weight	Weighted value, range:0-100， used in WRR & DRR

5.8.2 QOS port config

Operation steps

1. Click the “Business manage >QOS config >Port config” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



Port	Default COS
*	*
ge1/1	0
ge1/2	0
ge1/3	0
ge1/4	0
ge1/5	0
ge1/6	0
ge1/7	0

Explanations

Configuration item	**Meaning**
Port	With optional multiple ports
Default cos	Scope:0-7

5.9 LLDP config

5.9.1 Working Mode of LLDP

LLDP has the following four working modes:

- TxRx: Send and receive LLDP packet.
- Tx: Send but not receive LLDP packet.
- Rx: Receive but not sent LLDP packet.
- Disable: Neither send nor receive LLDP packet.

When LLDP working mode of the port changes, the port will initialize the protocol state machine. In order to avoid frequent changes in the working mode of a port and cause the port to constantly perform an initialization operation, the port initialization delay time can be configured. When the working mode of the port changes, the initialization operation is delayed for a period of time.

5.9.2 Sending Mechanism of LLDP Message

When a port works in TxRx or Tx mode, the device periodically sends LLDP packet to its neighbors. If the local configuration of a device changes, a LLDP packet is sent immediately to notify the neighboring devices of the local information changes as soon as possible. However, in order to prevent a large number of LLDP packets from being sent due to frequent local changes, every LLDP packet sent must be delayed for a period of time before sending the next packet.

When the working mode of the device is changed from Disable/Rx to TxRx/Tx or a new neighbor device is found (that is, a new LLDP packet will be received and information about the sending device of the packet is not saved locally), the device will automatically enable the fast sending mechanism, to reduce the sending cycle of LLDP packet to 1 second, and will continuously send specified number of LLDP packet before resume normal sending cycle.

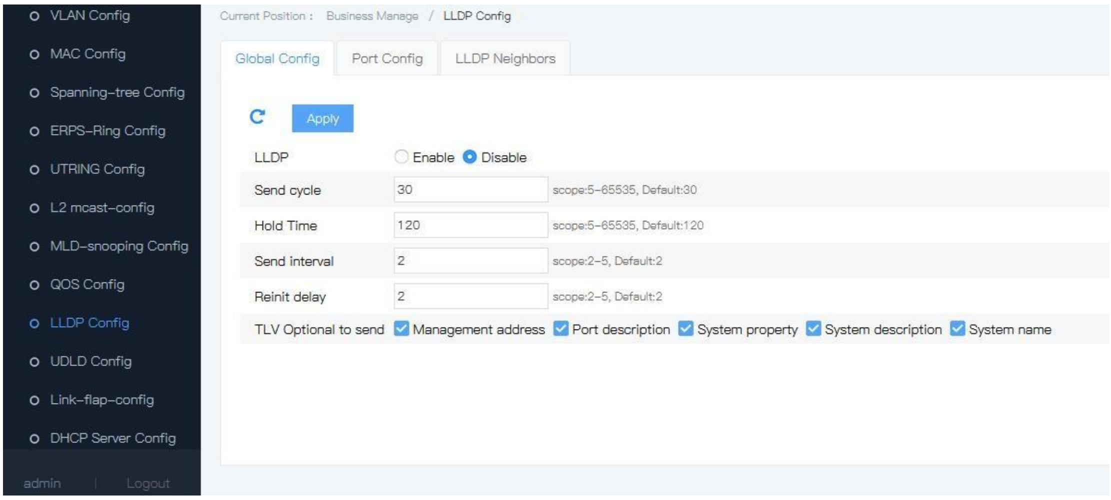
5.9.3 Receiving Mechanism of LLDP Message

When a port works in TxRx or Rx mode, the device will check the validity of received LLDP packets and carried TLVs. After passing the check, the device will save the neighbor information to the local area and set the aging time of neighbor information on the local device based on the Time To Live (TTL) value in TLV. If the value is zero, the neighbor information is aged immediately.

5.9.4 LLDP global config

Operation steps :

1. Click the “Business manage >LLDP config >Global config” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



LLDP ○ Enable ● Disable

Send cycle 30 scope:5-65535, Default:30

Hold Time 120 scope:5-65535, Default:120

Send interval 2 scope:2-5, Default:2

Reinit delay 2 scope:2-5, Default:2

TLV Optional to send ☑ Management address ☑ Port description ☑ System property ☑ System description ☑ System name

Explanations

Configuration item	Description
LLDP	Single opton, enable or disable LLDP
Send cycle	Default is 30s， scope： 5-65535s

Hold time	The amount of time that device information is held in a neighbor device. Default is 120s，scope：5-65535s
Send interval	Default is 2s，scope：2-5s
Reinit delay	Default is 2s，scope：2-5s
TLV option to send	Management address, port description, system property, system description, system name

Ethernet messages that encapsulate LLDP Data Unit are called LLDP messages. TLV is the unit that constitutes LLDPDU, and each TLV represents a message.

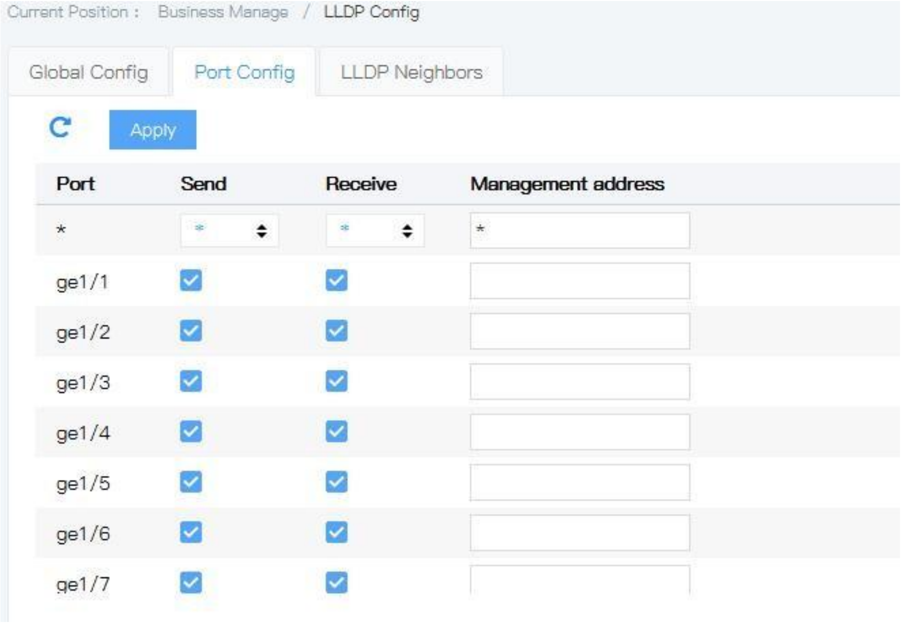
2. Fill corresponding configuration items.

3. Click “add”.

5.9.5 Port config

Operation steps

1. Click the “Business manage >LLDP config >Port config” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



Port	Send	Receive	Management address
*	*	*	*
ge1/1	☑	☑	
ge1/2	☑	☑	
ge1/3	☑	☑	
ge1/4	☑	☑	
ge1/5	☑	☑	
ge1/6	☑	☑	
ge1/7	☑	☑	

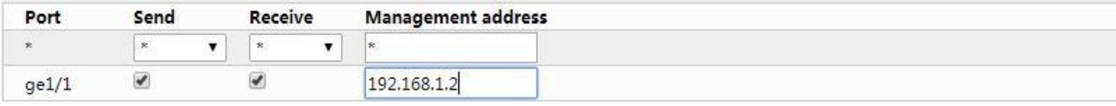
Explanations

Configuration item	**Meaning**
Port	Supports to configure ports
Send	Send LLDP message
Receive	Receive LLDP message
Managed address	Input this terminal switch IP address, e.g. 192.168.1.254

There are 2 working mode of LLDP. TxRx: Transmit and receive LLDP message. Disable: neither transmit nor receive LLDP message.

2. Configure send & receive LLDP pack message, click the “Business manage >LLDP config >Port config” menu in the navigation tree to enter the interface, tick send & receive in ge1/1 , input the IP address of this switch, e.g 192.168.1.254, click “save” , the

interface is shown as the following figure:

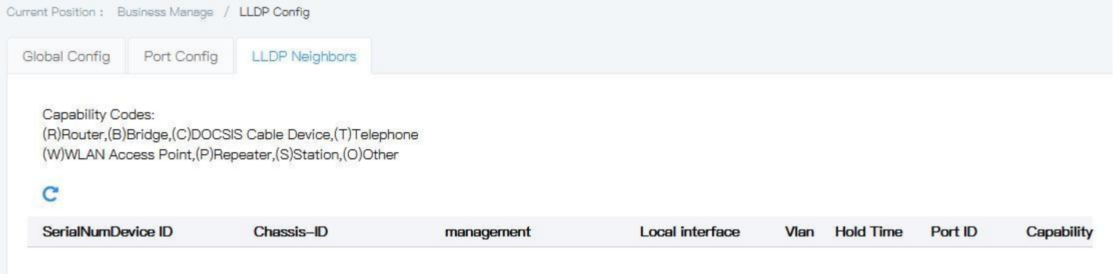


Port	Send	Receive	Management address
*	* ▾	* ▾	*
ge1/1	☑	☑	192.168.1.2

5.9.6 LLDP neighbors

LLDP neighbors display operation steps

Click the “Business manage >LLDP config >LLDP neighbor” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



Capability Codes:
(R)Router,(B)Bridge,(C)DOCSIS Cable Device,(T)Telephone
(W)WLAN Access Point,(P)Repeater,(S)Station,(O)Other

SerialNumDevice ID	Chassis–ID	management	Local interface	Vlan	Hold Time	Port ID	Capability

Explanations

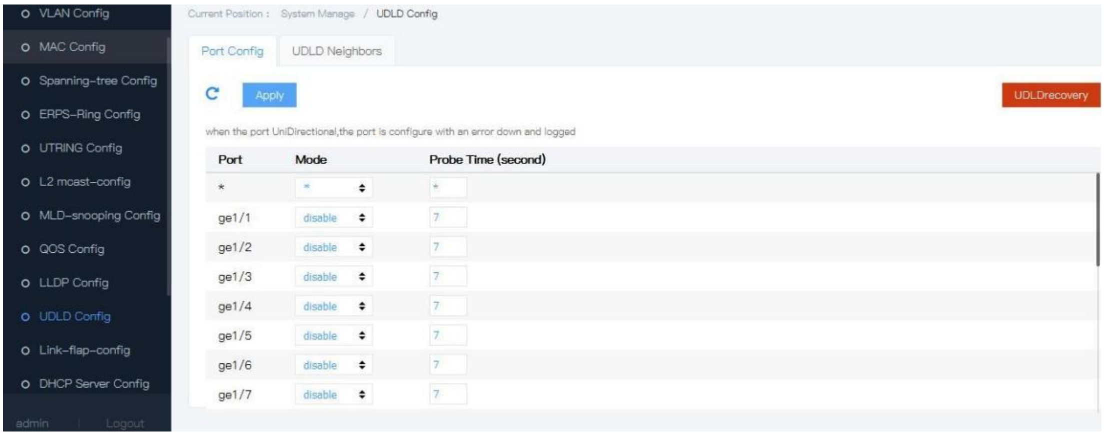
Configuration item	Meaning
Device-ID	Equipment Model Name
Chassis-ID	Equipment mac address
Mgm-IP	Device Management IP
Local-Intf	Local port number
Hldtme	The amount of time that device information is held in a neighbor device
Port-ID	Neighbor port number

5.10 UDLD config

UDLD (UniDirectional Link Detection):Layer 2 protocol for monitoring the physical management of Ethernet links using fiber optic or twisted-pair connections. When a one-way link (which can only be transmitted in one direction) occurs, the UDLD can detect the condition, close the corresponding interface and send a warning message。

UDLD supports two working modes; Normal (default) and Aggressive (default) modes。

Click the "Business Management >UDLD Management" menu in the navigation tree to enter the "UDLD Management" interface, as shown in the figure below。



when the port UniDirectional,the port is configure with an error down and logged

Port	Mode	Probe Time (second)
*	*	*
ge1/1	disable	7
ge1/2	disable	7
ge1/3	disable	7
ge1/4	disable	7
ge1/5	disable	7
ge1/6	disable	7
ge1/7	disable	7

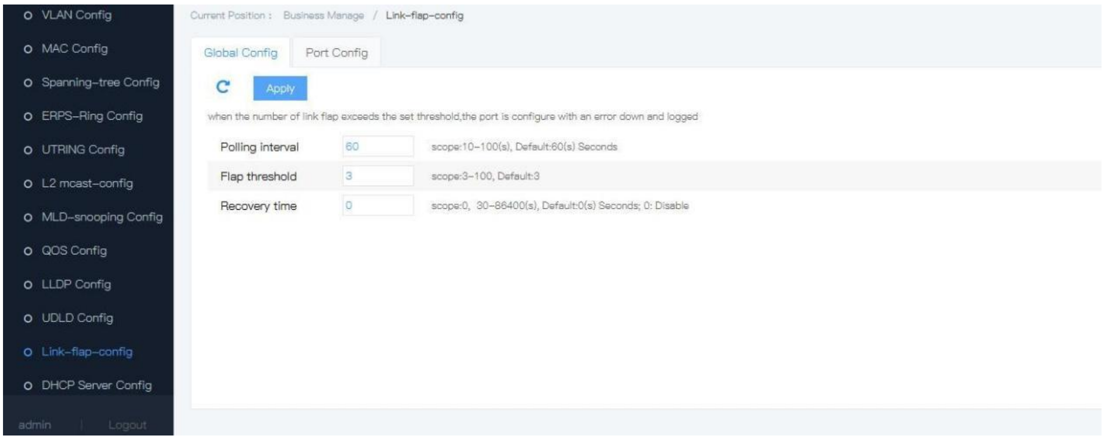
Explanations

Configuration item	Meaning
normal	UDLD can detect unidirectional links and mark ports as undetermined to produce system logs
aggressive	UDLD can detect by unidirectional links.An attempt to rebuild the link is made to send a UDLD message probe packet every 7 seconds. If there are no UDLD echo replies, the port is placed in the ErrDisable state
Probe	Detection time

5.11 Link-flap config

Link oscillation is to close the interface whose physical state frequently changes Up/Down and make it in the state of Down, so that the network topology will stop changing frequently back and forth. When the number of times the link has wobbled over the polling interval exceeds the set threshold, alarm logs are generated and the port is set to Err-Disable state。

Click the "Business Management > Link-Flap" menu in the navigation tree to enter the "Link-Flap Management" interface, as shown in the figure below.



when the number of link flap exceeds the set threshold,the port is configure with an error down and logged

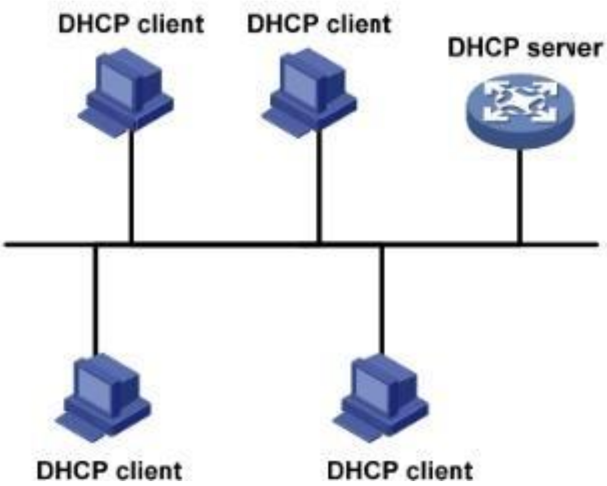
Polling interval	60	scope:10-100(s), Default:60(s) Seconds
Flap threshold	3	scope:3-100, Default:3
Recovery time	0	scope:0, 30-86400(s), Default:0(s) Seconds; 0: Disable

Explanations

Configuration item	Meaning
polling interval	The system needs to count the number of link oscillations in unit time, which is recorded as the link oscillation time interval
Instability threshold	The Up/Down switch of interface state is recorded as one link oscillation
recovery time	Interface down after the set recovery time can be UP, 0 is disabled

5.12 DHCP Server config

DHCP (Dynamic Host Configuration Protocol) is usually applied in large local area network environments. Its main role is to centrally manage and assign IP addresses, so that hosts in the network environment can dynamically obtain IP addresses, Gateway addresses, DNS server addresses and other information, and improve the utilization rate of addresses.



5.12.1 DHCP IP address allocation

5.12.1.1 IP address allocation strategies

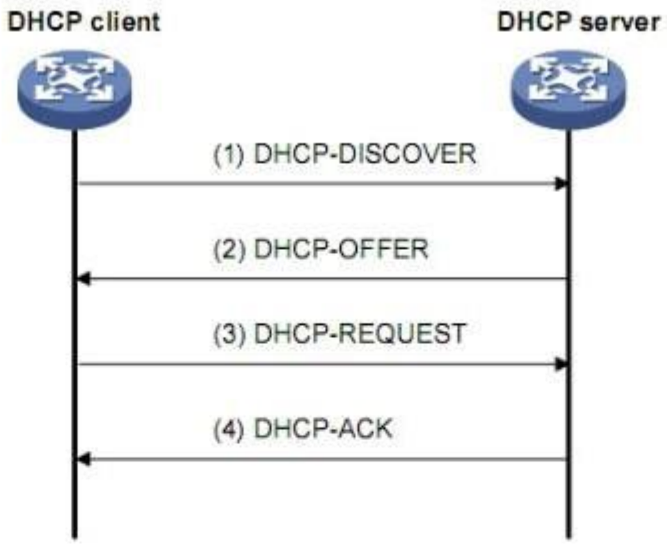
According to different demands of clients, DHCP provides three IP address allocation strategies:

Manually assigned addresses: static bound fixed IP addresses set by the administrator for a few specific clients (such as the WWW server).Send the configured fixed IP address to the client via DHCP.

Automatic allocation of addresses: DHCP assigns clients an IP address with an unlimited lease period.

Dynamic allocation address: DHCP assigns the IP address with a certain validity period to the clients. After reaching the validity period, the client needs to re-apply for the address. Most clients get this dynamically assigned address.

5.12.1.2 IP address dynamic acquisition



IP address Dynamic acquisition process

As shown in the figure above, the DHCP client dynamically obtains the IP address from the DHCP server, mainly through four stages:

(1) Discovery stage is where the DHCP client looks for the DHCP server. The client sends the DHCP-DISCOVER message by broadcasting.

(2) Provide stage, that is, the stage where DHCP server provides IP address. After receiving the DHCP-DISCOVER message from the client, the DHCP server selects an IP address according to the priority assigned by the IP address and sends it to the client with other parameters through the DHCP-OFFER message. The way of sending the DHCP-OFFER message is determined by the flag field in the DHCP-DISCOVER message.

(3) Selection stage, that is, the stage where the DHCP client selects the IP address. If multiple DHCP-OFFER messages are sent to this client by DHCP server, the client only accepts the first received DHCP-OFFER message, and then sends the DHCP-REQUEST message through broadcasting, which contains the IP address assigned by the DHCP server in the DHCP-OFFER message.

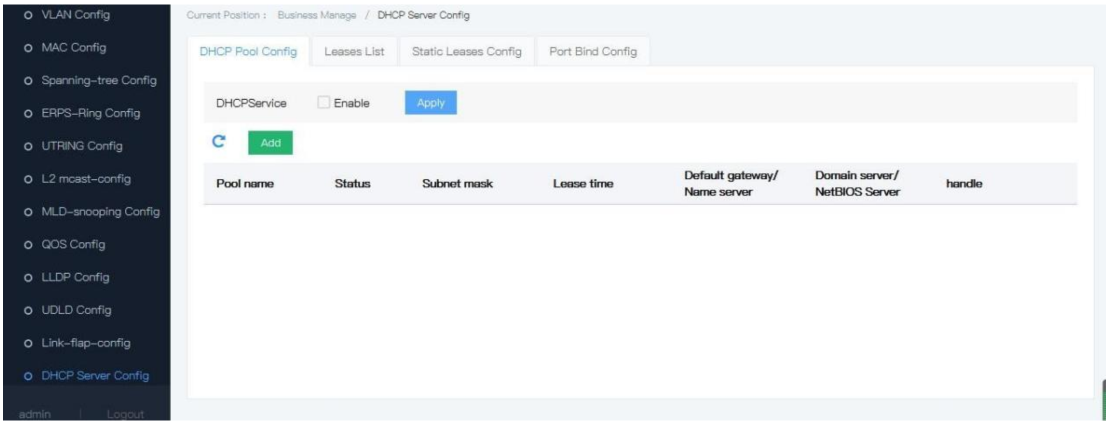
(4) confirmation stage, that is, the stage where DHCP server confirms the IP address. After the DHCP-REQUEST message sent by the DHCP client is received by the DHCP server, only the server selected by the DHCP client will perform the following operations: if the address is confirmed to be assigned to the client, the DHCP-ACK message will be returned; Otherwise, return the DHCP-NAK message this indicates that the address cannot be assigned to the client.

5.12.2 DHCP pool config

Enable DHCP-snooping

Operation steps

1. Click the "Business manage >DHCP server config >DHCP pool config" menu in the navigation tree to enter the interface, the interface is shown as the following figure:

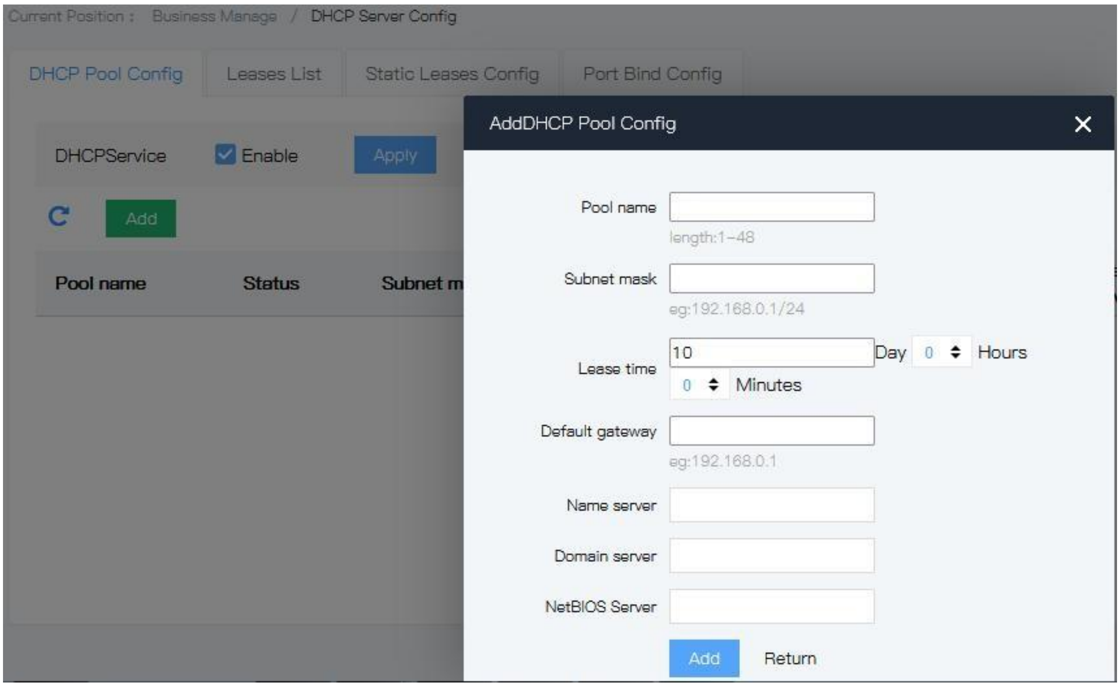


Pool name	Status	Subnet mask	Lease time	Default gateway/ Name server	Domain server/ NetBIOS Server	handle

Explanations

Configuration item	**Meaning**
Pool name	Length of the DHCP Server pool name is 1~48
Subnet mask	DHCP client can automatically obtain the IP
Lease time	DHCP client can automatically obtain the lease time of the address, the scope is 0-999 days
Default gateway	DHCP client can automatically obtain the gateway
DNS address	DHCP client can automatically obtain the DNS address
Domain service	DHCP client can automatically obtain the domain
NetBIOS server	DHCP client can automatically obtain NetBIOS server address

2. Fill corresponding configuration items.
3. Click "add".



Current Position : Business Manage / DHCP Server Config

DHCP Pool Config | Leases List | Static Leases Config | Port Bind Config

DHCPService ☑ Enable Apply

Add

AddDHCP Pool Config

Pool name: (length:1~48)

Subnet mask: (eg:192.168.0.1/24)

Lease time: 10 Day 0 Hours 0 Minutes

Default gateway: (eg:192.168.0.1)

Name server:

Domain server:

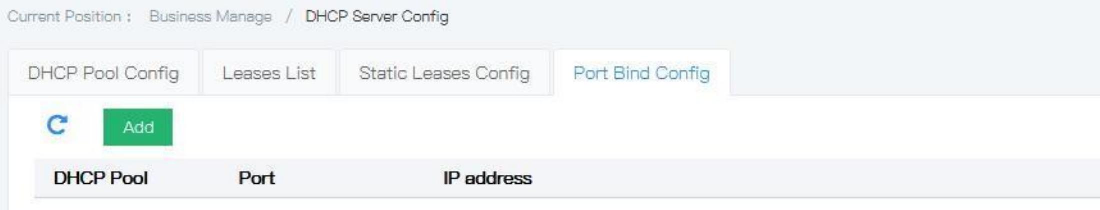
NetBIOS Server:

Add Return

5.12.3 Port bind

Operation steps

1. Click the “Business manage >DHCP-snooping config >Port bind config” menu in the navigation tree to enter the interface, the interface is shown as the following figure:

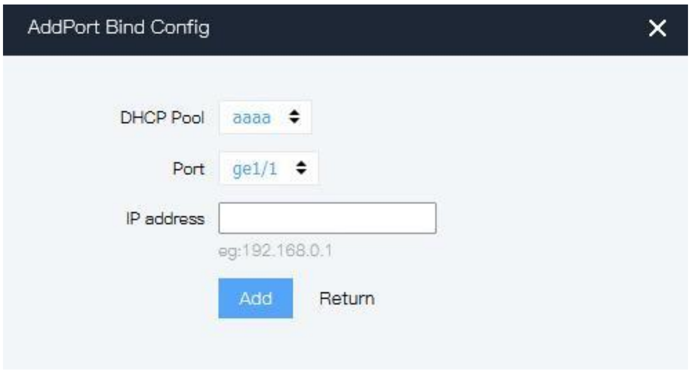


Current Position : Business Manage / DHCP Server Config

DHCP Pool Config | Leases List | Static Leases Config | Port Bind Config

Add

DHCP Pool	Port	IP address



AddPort Bind Config

DHCP Pool: aaaa

Port: ge1/1

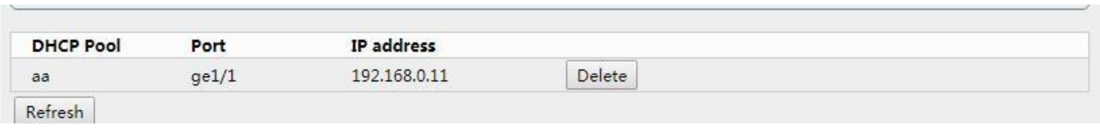
IP address: (eg:192.168.0.1)

Add Return

Explanations

Configuration item	**Meaning**
DHCP Pool	Fixed value, created address pool
IP address	Static IP address of the user
Port	Matching switch port

2. Fill corresponding configuration items.
3. Click “add”.



DHCP Pool	Port	IP address	
aa	ge1/1	192.168.0.11	Delete

5.12.4 Static client config

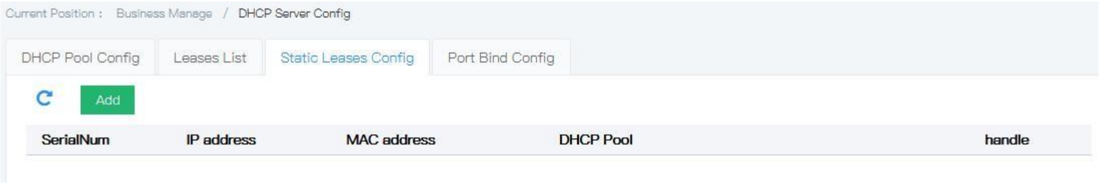
In the DHCP network, users who obtain IP addresses statically (non-DHCP users) may have various attacks on the network, such as imitating DHCP Server and constructing false DHCP Request messages. This will bring some security risks for legitimate DHCP users to use the network normally.

In order to effectively prevent non-DHCP user attacks, the device can be enabled to generate static MAC table entry functions based on the DHCP Snooping binding table. After that, the device will automatically execute commands to generate static MAC table entries for all the DHCP user's corresponding DHCP Snooping bound table items under the interface, and at the same time shut down the interface's ability to learn dynamic MAC table items. At this point, only the source MAC and static MAC table item matching message can pass through the interface, otherwise the message will be discarded. Therefore, for non-DHCP users under this interface, only if the administrator manually configures the static MAC table items of such users, their messages can pass, otherwise the messages will be discarded.

Static client configuration can be used to satisfy specific devices (such as servers) that require a fixed IP address.

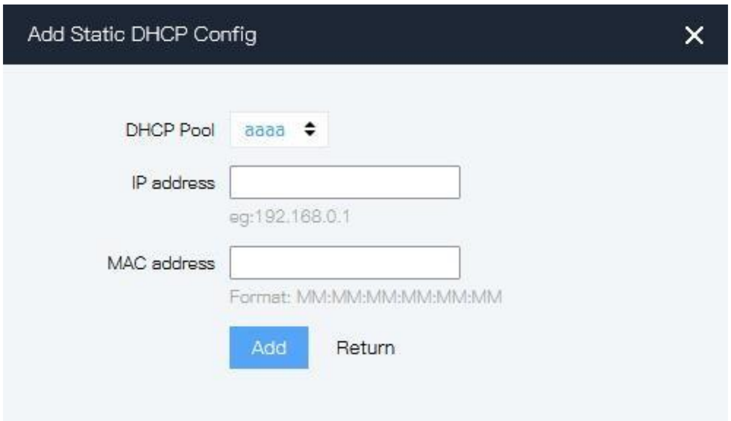
Operation steps:

1. Click the “Business manage >DHCP Server config >Static leases config” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



Current Position : Business Manage / DHCP Server Config

SerialNum	IP address	MAC address	DHCP Pool	handle



Add Static DHCP Config

DHCP Pool: aaaa
IP address: eg:192.168.0.1
MAC address: Format: MM:MM:MM:MM:MM:MM

Explanations

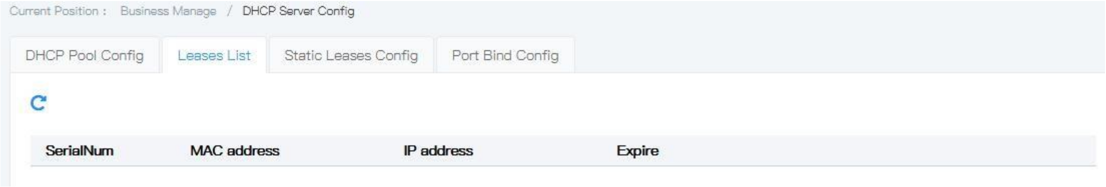
Configuration item	Meaning
DHCP Pool	Fixed value, created address pool

IP address	Input the IP address needs to be banded
MAC address	Input the MAC address needs to be banded

5.12.5 Leases list

Operation steps

1. Click the “Business manage >DHCP Server config >LEASES list” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



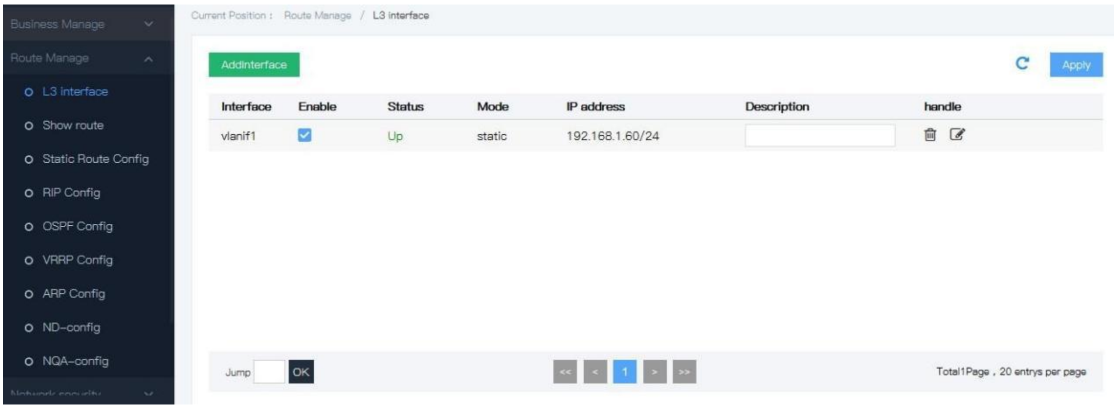
SerialNum	MAC address	IP address	Expire

6 Route manage

6.1 L3 interface config

1. Interface description

L3 interface is mainly for device IP address setting. On Web of this device, it only supports manual IPV4 setting.



Interface	Enable	Status	Mode	IP address	Description	handle
vlanif1	☑	Up	static	192.168.1.60/24		

2. Explanations

Configuration item	Meaning
IPV4	IP address adopts Dotted Decimal Notation, e.g. 10.110.50.101

3. Operation steps

Step 1	Click the “Route manage >L3 interface” menu in the navigation tree to enter the interface, the default IPV4 address is: 192.168.1.254/24

Step 2	If user needs to change the IP, choose “Modify” , fill relative address and gateway, click “Add”.
Step 3	If it shall be used as start configuration, enter the “System manage>running config” for saving the settings.

Explanation

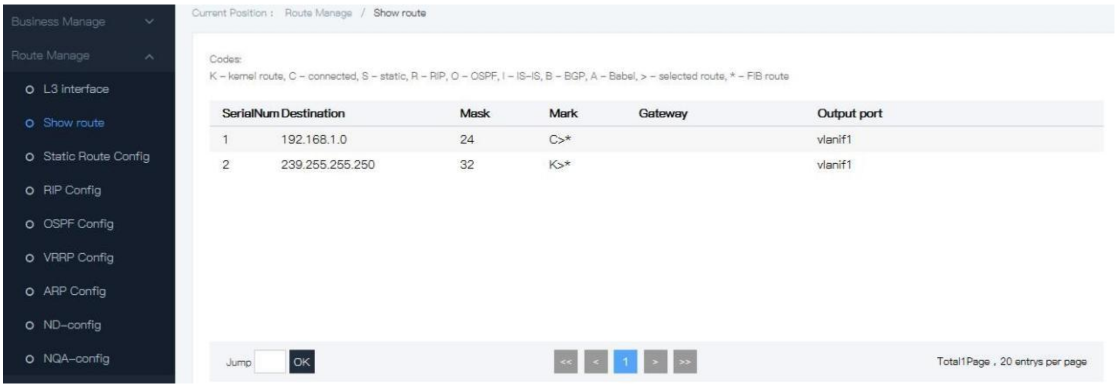
After change IP, you need to login with the new IP address to enter the Web interface.

6.2 Show route

User can check the route information

Operation steps

1. Click the “Route manage > Show route” menu in the navigation tree to enter the interface, The interface is shown as the following figure:



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

SerialNum	Destination	Mask	Mark	Gateway	Output port
1	192.168.1.0	24	C>*		vlanif1
2	239.255.255.250	32	K>*		vlanif1

Explanations

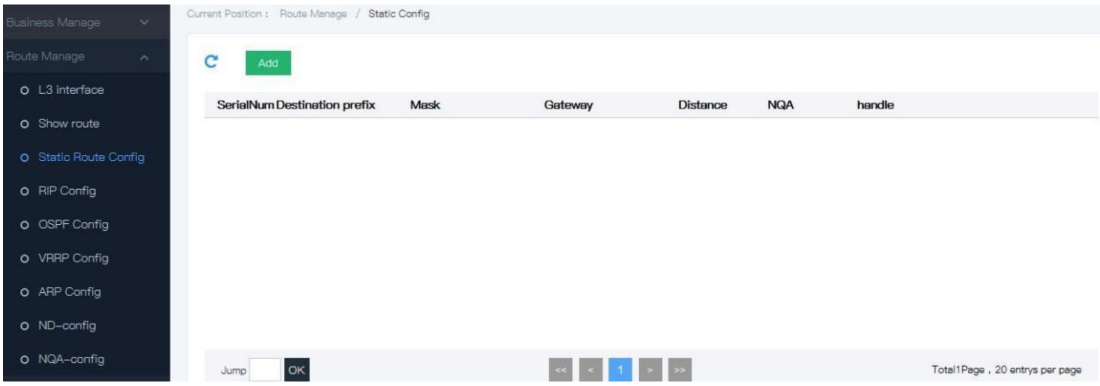
Configuration item	**Meaning**
Gateway	
Destination	Destination network IP address & Subnet mask

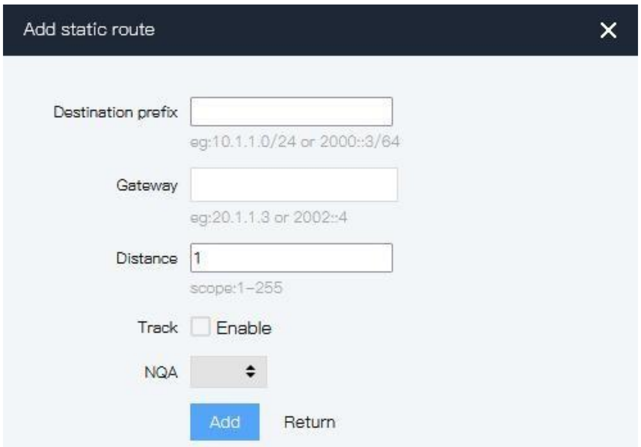
6.3 Static config

Static route is manually set by the network administrator. In a network with a relatively simple network structure, the network administrator only needs to manually configure the static route to achieve network interoperation. Static route is typically configured in a small network with a fixed topology. Using appropriate static route in the network can reduce route selection problems and overload of route selection data flow, and improve the forwarding speed of packets. When the network changed, the network administrator needs to modify the configuration parameters again to ensure normal network communication.

Operation steps

1. Click the “Route manage > Static config” menu in the navigation tree to enter the interface, The interface is shown as the following figure:





Destination prefix
eg:10.1.1.0/24 or 2000::3/64

Gateway
eg:20.1.1.3 or 2002::4

Distance 1
scope:1-255

Track □ Enable

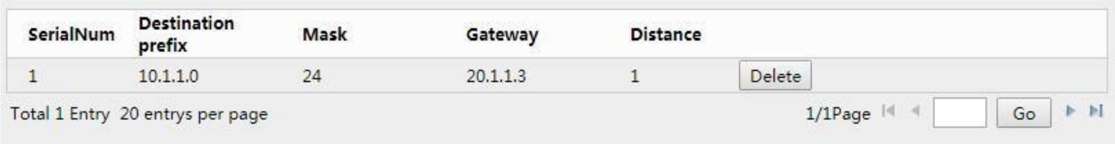
NQA

Explanations

Configuration item	Meaning
Destination prefix	Set dest network of the route
Gateway	Set IP address of dest network route path previous and next nodes
Distance	Specified route managed distance. The distance shorter,the priority higher

2. Fill corresponding configuration items.

3. Click “add”, the interface is shown as the following figure:



SerialNum	Destination prefix	Mask	Gateway	Distance	
1	10.1.1.0	24	20.1.1.3	1	Delete

6.4 RIP config

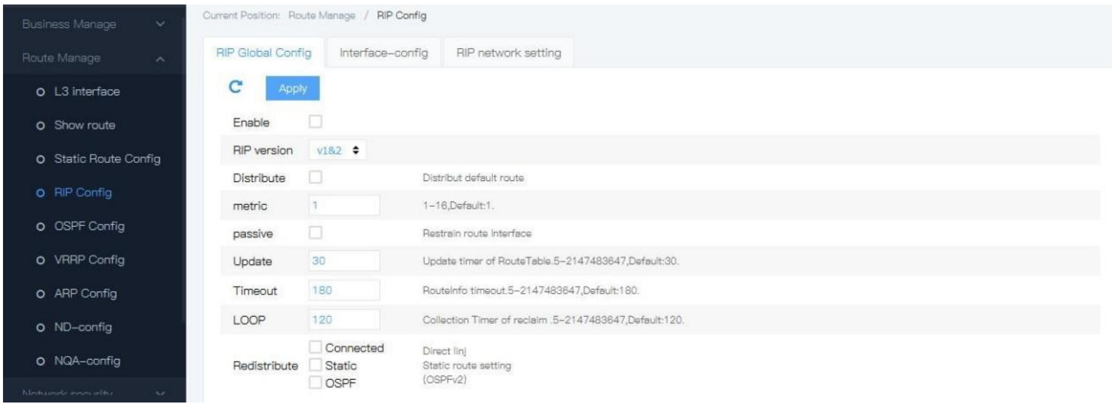
RIP (Routing Information Protocol) is a relatively simple dynamic Routing Protocol, which is mainly used in small networks, such as campus network and simple regional network. RIP is generally not used for complex environments and large networks. As one of the earliest Interior Gateway Protocol (IGP), RIP IS still widely used today because of its simpler implementation and easier configuration and maintenance management than OSPF and is-is. RIP currently has both versions of RIPv1 and RIPv2.

RIP adopts the distance-vector algorithm, it uses the number of hops to measure the distance to the destination address, and defines the path with the least number of hops as the optimal path. The number of hops from a router to a network directly connected to it is zero, and each hop is incremented by one. The number of jumps is called a metric. In order to limit the convergence time, RIP stipulates that the value range of measured value is integer between 0 and 15, and the value 16 represents infinity, that is, the destination network is unreachable. Because of this limitation, RIP is not suitable for large networks.

6.4.1 RIP global config

Operation steps

1. Click the "Route manage > RIP global config" menu in the navigation tree to enter the interface, The interface is shown as the following figure:



Enable □

RIP version v1&2

Distribute □ Distribut default route

metric 1 1-16,Default:1.

passive □ Restrain route Interface

Update 30 Update timer of RouteTable.5-2147483647,Default:30.

Timeout 180 RouteInfo timeout.5-2147483647,Default:180.

LOOP 120 Collection Timer of reclaim .5-2147483647,Default:120.

Redistribute □ Connected Direct linj
□ Static Static route setting
□ OSPF (OSPFv2)

Explanations

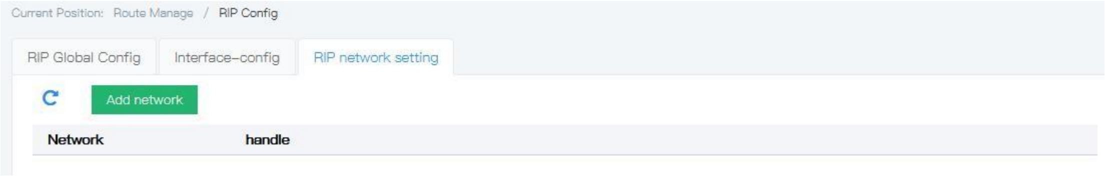
Configuration item	**Meaning**
Enable RIP	Choose enable or disable RIP, default is "disable"
RIP version	Choose RIP version, with optional RIPv1 & RIPv2。 Default : RIPv1&v2， transmit & receive RIPv1 & RIPv2 message. RIPv1 ： only transmit & receive RIPv1 message, adopts broadcast way when transmit RIPv2 ： only transmit & receive RIPv2 message, adopts multicast way when transmit
Distribute	Choose enable or disable, default is "disable"
Passive	Restrain the port to transmit route update message.
Metric	。 Setthe default value, range: 1-16, default is "1"
Redistribute	Choose enable or disable external route(Static/ospf/bgp/connected) in RIP protocol, default is "disable"
Update timer	Fill time interval of RIP task sending update message, range: 5-2147483647s
Overtime timer	Fill the valid date of the route. If no updated, then this route path will be set unreach automatically, range: 5-2147483647s. Recommend setting: "180s"(6 update periods)

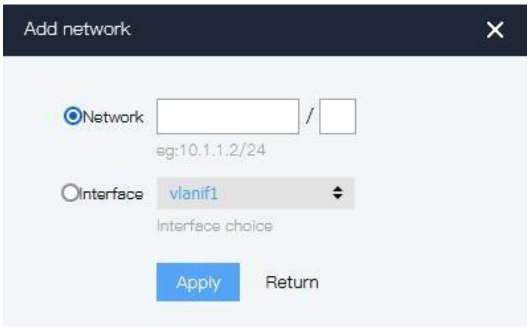
Trash timer	Trash timer is the time that route from unreach to final deleted. If the route past become unreach, and there is no update during this period, this
	route will be deleted automatically, range: 5-2147483647, recommend setting “120s”

6.4.2 RIP config

Operation steps

1. Click the “Route manage > RIP network setting” menu in the navigation tree to enter the interface, The interface is shown as the following figure:





Explanations

Configuration item	Meaning
RIP send version	Choose the RIP version of sending message Auto： Auto format v1： Adopts RIPv1 format to send message v2： Adopts RIPv2 format to send message v1&2： Compatible with 2 formats
RIP receive version	Choose the RIP version of receiving message Auto： Auto format v1： Adopts RIPv1 format to receve message v2： Adopts RIPv2 format to receive message v1&2： Compatible with 2 formats
Auth type	Enable or disable the authentication of the the port when sending & receiving message, default is “no auth”. Only the devices adopt the same auth type and password can be exchange RIP message; and only RIPv2 supports message authentication function.
Auth ID	Auth ID should be input when set MD5 keys, the ID is a number between 1-255
Keys	Set the keys, the key is a character string

Horizen	Coose if enable horizen function. Once enable, the device will not send back the route message which study from certain port, default is
	“enable”

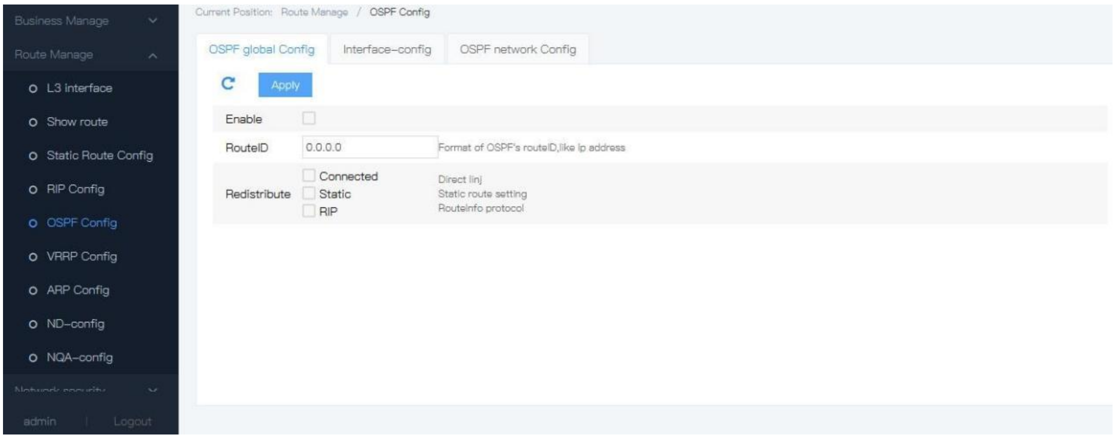
6.5 OSPF config

OSPF(Open Shortest Path First) IS an interior gateway protocol(IGP). It is used for single autonomous system route control. It belongs to IGP.

OSPF is an IGP route protocol which developed by IETF OSPF group. It is designed for IP network, and it supports IP subnet and external route information mark. It allows message authentication and IP multicast.

6.5.1 OSPF global config

Click the “Route manage > OSPF global config” menu in the navigation tree to enter the interface, The interface is shown as the following figure:



Enable □

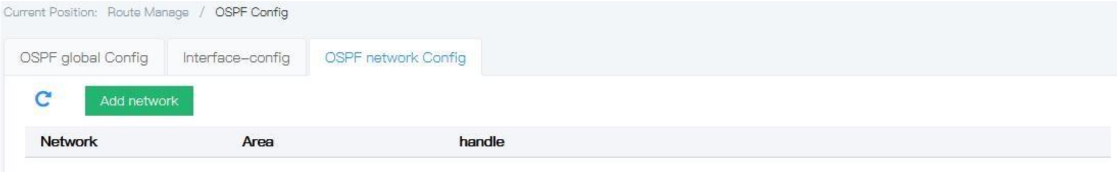
RouteID 0.0.0.0 Format of OSPF's routeID,like Ip address

Redistribute
□ Connected Direct linj
□ Static Static route setting
□ RIP RouteInfo protocol

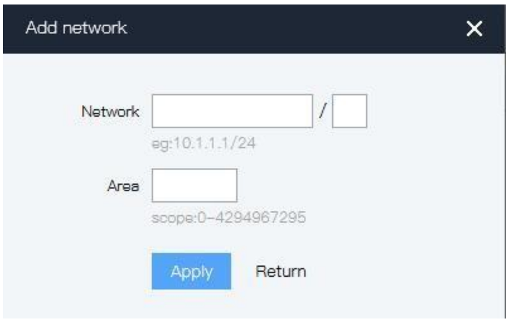
Explanations

Configuration item	**Meaning**
Route ID	Force ASBR to generate a default route into the OSPF routing domain
Redistribute	Reassign routing metrics
Spf timer	Sets the time delay for routing calculation in a domain, the initial time interval, and the maximum time interval
Passive mode	The passive mode of the interface is configured. When configured as a passive mode, the corresponding interface does not establish an adjacency relationship with other routers. The router will publish the network directly connected to the passive interface in the router LSA in the manner of the peripheral network. By default, the interface does not enable passive mode.

1. Click the "Route manage > OSPF config" menu in the navigation tree to enter the interface, The interface is shown as the following figure:



Network	Area	handle



Explanations

Configuration item	**Meaning**
Interface	Current configured interface list
Router priority	Configure router priority, range: 0-255, 0 means in corresponding network, the router can't be chosen as specified router. The bigger of the value, the higher of the priority. Resend interval: the resend interval of the interface, it is used for resend message between LSA & DD
Hello interval	Configure the time interval of the interface sending "hello". In the same network, only the hellow interval is the same will reach neighbor connection relationship. Please make sure the Hello interval of all the interfaces are the same. Default value is 10s.
Dead interval	Configure the dead interval of router neighbor relationship failure. Within the specified time, if there is no Hello message from the neighbor, so the neighbor relationship is failed. Default value is 40s.
Cost	Configure the interface path cost. OSPF calculate the shortest route forwarding data path from the interface which based on port cost value. If do not manual configure it, OSPF will calculate interface path cost automatically; if auto calculate cost feature is disable, then will adopts default value as interface path cost. Default value is 1.
Network	Configure the network type of the interface, the default type of Ethernet is broadcast.

Auth type	Configure the interface auth type. Only the interfaces with the same auth type and password can reach neighbor relationship and synchronize LSA. It includes below type: null： No auth simple: Simple password auth. md5： Md5 auth Simple password: Input simple auth password MD5 password ID： Input password ID for md5 auth MD5 password： Input password for md5 auth

6.6 VRRP config

VRRP (Virtual Router Redundancy Protocol) adds a set of routers that can assume gateway functions to the backup group to form a Virtual Router. VRRP's election mechanism determines which Router takes on forwarding tasks. Hosts in the LAN only need to configure the Virtual Router as the default gateway.

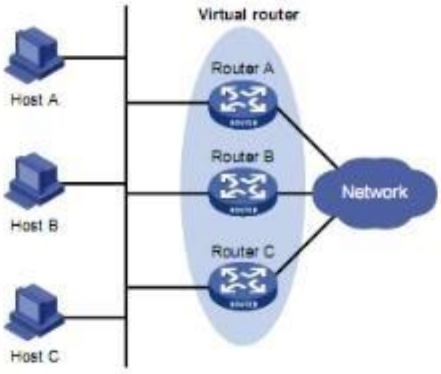
VRRP divides up a group of routers in a LAN, called a backup group. The Backup group consists of a Master router and multiple Backup routers that function as a virtual router.

VRRP backup group has the following characteristics:

Virtual routers have IP addresses, called virtual IP addresses. Hosts in the LAN only need to know the IP address of the virtual router and set it to the next hop of the default route.

Hosts in the network communicate with external networks via this virtual router.

The router in the backup group selects the Master router according to the priority, which assumes the gateway function. Other routers serve as Backup routers. When the Master router fails, it replaces Master to continue to perform the gateway responsibility, so as to guarantee the host in the network to continuously communicate with the external network.



VRRP Network schematic

As shown above, Router A, Router B and Router C make up a virtual Router. This virtual router has its own IP address. Hosts in the LAN set the virtual router as default gateway. The highest-priority routers in Router A, Router B and Router C act as Master routers, taking on the functions of gateways.The remaining two routers serve as Backup routers.

Explanation:

The IP address of the virtual router can be the unassigned IP address of the network segment where the backup group is located, or it can be the same as the interface IP address of a router in the backup group. The router whose interface IP address is the same as the virtual IP address is called the "IP address owner”.

In the same VRRP backup group, only one IP address owner is allowed to be configured.

The status of the router in the Backup group can be Master, Backup and Initialize.

1. The priority of the router in the backup group

VRRP determines the role of each router (Master router or Backup router) in the Backup group based on priority. The higher the priority, the more likely to become the Master router.

The value range of the priority of VRRP is 0 to 255 (the higher value indicates higher priority), the configurable range is 1 to 254, the priority 0 is reserved for special purposes for the system, and 255 is reserved for IP address owners. When the router is the owner of the IP address, its priority is always 255.Therefore, when there is an IP address owner in the backup group, it is the Master router as long as it is working properly.

2. The working mode of the router in the backup group

Routers in a backup group work in two modes:

Non-preemptive mode: if the router in the Backup group works in non-preemptive mode, the Backup router will not become the Master router as long as the Master router does not fail, even if it is subsequently configured with higher priority.

Preemption: if the router in the backup group works in preemption mode, it will send a VRRP notification message to the public once it finds that its priority is higher than the current Master router. This causes the routers in the backup group to re-elect the Master router, and eventually replace the original Master router. Accordingly, the original Master router will become the Backup router.

3. The authentication mode of the router in the backup group

In order to prevent illegal users constructing message attack backup groups, VRRP verifies received VRRP messages by adding authentication words to VRRP messages. VRRP offers two authentication options:

Simple: simple character authentication. The router sending the VRRP message fills the authentication word in the VRRP message, while the router receiving the VRRP message compares the authentication word in the received VRRP message with the locally configured authentication word. If the authentication word is the same, the received message is considered to be true and legitimate VRRP message; otherwise, the received message is considered an illegal message.

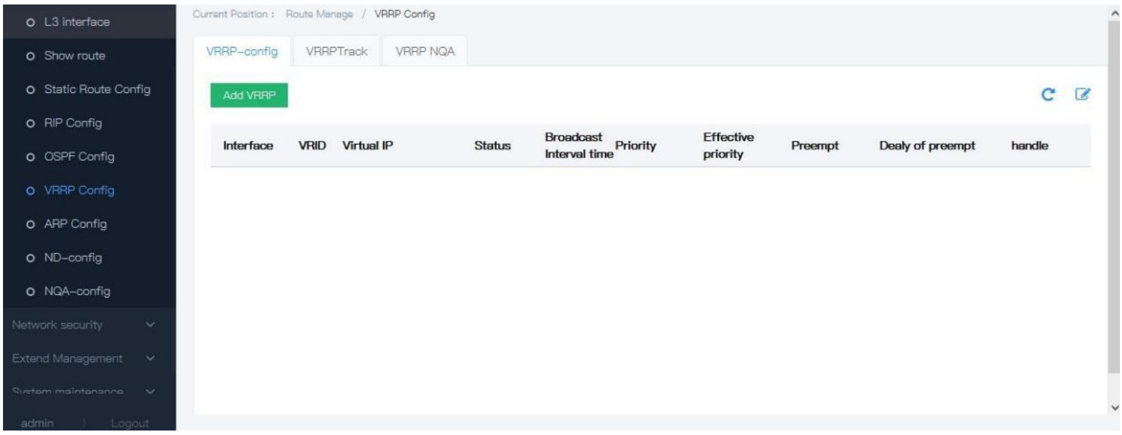
Md5: md5 authentication. The router sending the VRRP message USES the Authentication word and MD5 algorithm to abstract the VRRP message, and the result is saved in the Authentication Header. Routers receiving VRRP messages perform the same calculations using the authentication word and MD5 algorithm and compare the results with the content of the authentication header. If it is the same, the received message is considered to be true and legitimate VRRP message; otherwise, the received message is considered an illegal message.

In a secure network, users can also not set authentication mode.

6.6.1 VRRP config

Operation steps：

Click the "Route manage > VRRP config" menu in the navigation tree to enter the interface, The interface is shown as the following figure:



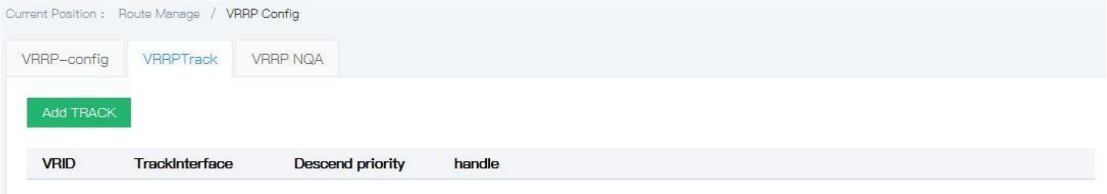
Explanations

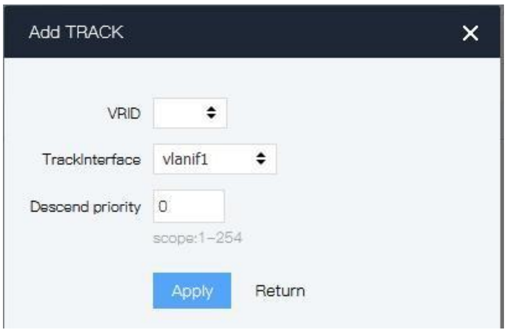
Configuration item	**Meaning**
Interface	Current config list
VRID	Virtual route ID, scope: 1-255
Virtual IP	Virtual route IP
Broadcast interval	VRRP message broadcast interval,scope:1-10, default:1
Priority	Virtual route priority, scope: 1-254, default:100
Preempt	Enable/disable preempt
Delay of preempt	Scope: 0-1000, default: 0

6.6.2 VRRP track

Operation steps :

Click the "Route manage > VRRP config > VRRP track" menu in the navigation tree to enter the interface, The interface is shown as the following figure:





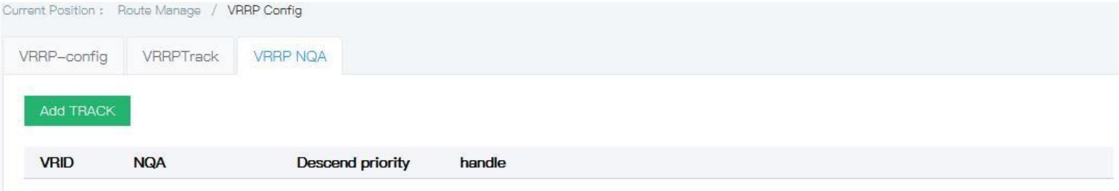
Explanations

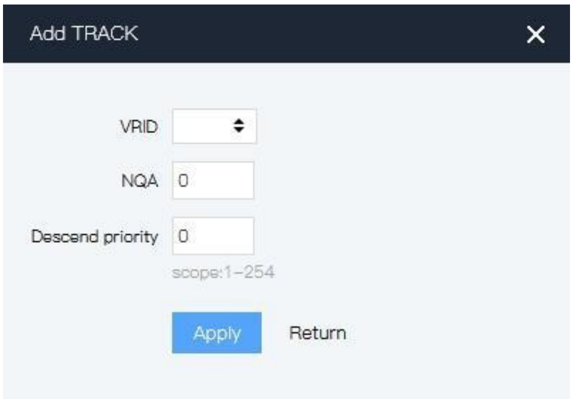
Configuration item	Meaning
track Interface	Current config track Interface
VRID	Virtual route ID， scope: 1-255
Priority	Virtual route priority， scope: 1-254， default:0

6.6.3 VRRP nqa

Operation steps：

Click the "Route manage > VRRP config> VRRP nqa" menu in the navigation tree to enter the interface, The interface is shown as the following figure:





Explanations

Configuration item	Meaning
VRID	Virtual route ID， scope: 1-255
NQA	scope:1-254
Priority	Virtual route priority， scope: 1-254， default:0

6.7 ARP config

ARP (Address Resolution Protocol) is the Protocol for resolving IP addresses to Ethernet MAC addresses(or physical addresses).

In a LAN, when a host or other network device has data to send to another host or device, it must know the other's network layer address (IP address). But having an IP address is not enough, because IP datagram must be encapsulated in frames to be sent over the physical network, so the sending station must also have the physical address of the receiving station, a mapping from the IP address to the physical address is required. ARP is the protocol for implementing this functionality.

After the device parses to the destination MAC address through ARP, it will add an IP address to MAC address mapping entry in its ARP table for subsequent forwarding of messages to the same destination.

ARP table items are divided into dynamic ARP table items and static ARP table items.

1. Dynamic ARP table items

Dynamic ARP table items are automatically generated and maintained by ARP protocol through ARP messages, which can be aged, updated by new ARP messages, and covered by static ARP table items. When reach the aging time or interface down, corresponding dynamic ARP table entries will be deleted.

2. **S**tatic ARP table items

Static ARP table entries are manually configured and maintained without aging or being covered by dynamic ARP table entries.

Configuring static ARP table entries increases communication security. The static ARP table entry can only use the specified MAC address when communicating with the device with specified IP address. The attack message cannot change the mapping relation between the IP address and MAC address of this table entry, thus protecting the normal communication between this device and the specified device.

Static ARP table entries are divided into long static ARP table entries, short static ARP table entries and multi-port ARP table entries.

When configuring a long static ARP table entry, in addition to the IP address and MAC address entries, you must configure the VLAN and outgoing interface for the ARP table entry. Long static ARP table entries can be used directly for message forwarding.

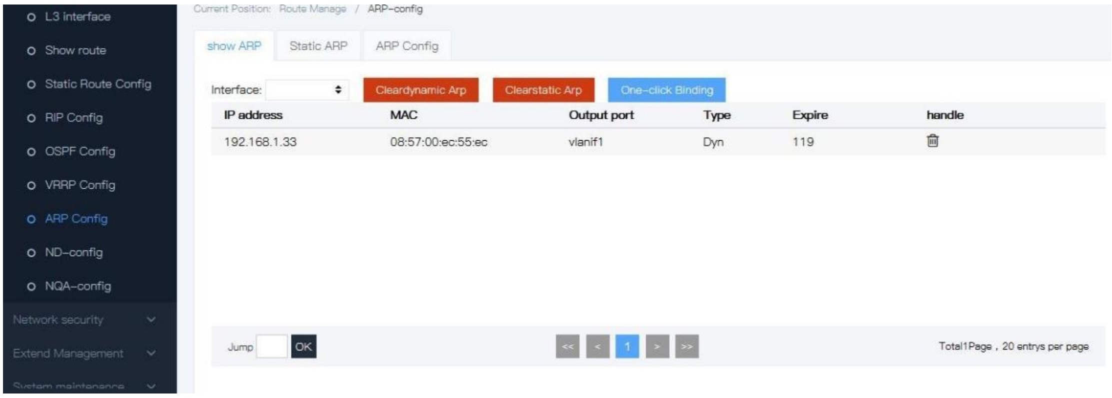
When configuring a short static ARP table entry, you only need to configure the IP address and MAC address entries. If the outgoing interface is a layer 3 Ethernet port, the short static ARP table item can be directly used for message forwarding. If the outgoing interface is a VLAN interface, short static ARP table entries cannot be directly used for message forwarding. When needs to send the IP packets, it needs to send ARP request packet first, if the received response message in the source IP address and source MAC address is the same as configured IP address and MAC address, it will add the interface of received ARP response message into the static ARP table entries, after this, it can be used for forwarding IP packets.

The multi-port ARP table entry is formed by configuring the short static ARP table entry and the multicast MAC address table entry. If the MAC address in the short static ARP table entry is the same as the MAC address in the multicast MAC address table entry, the multi-port ARP table entry will be generated. If the device is sending IP packets, the multi-port ARP table entry guides IP packets to be sent from multiple outgoing ports.

6.7.1 Show ARP

Operation steps：

2. Click the “Route manage > ARP config” menu in the navigation tree to enter the “Show ARP”interface, The interface is shown as the following figure:

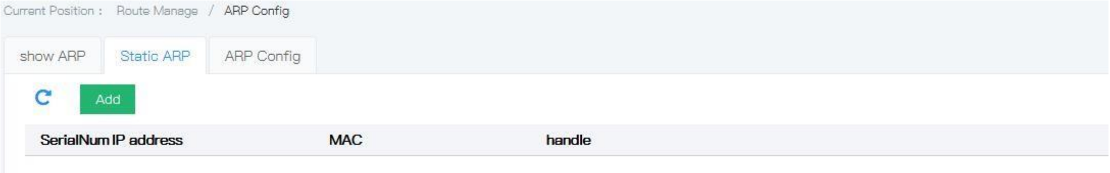


IP address	MAC	Output port	Type	Expire	handle
192.168.1.33	08:57:00:ec:55:ec	vlanif1	Dyn	119	🗑

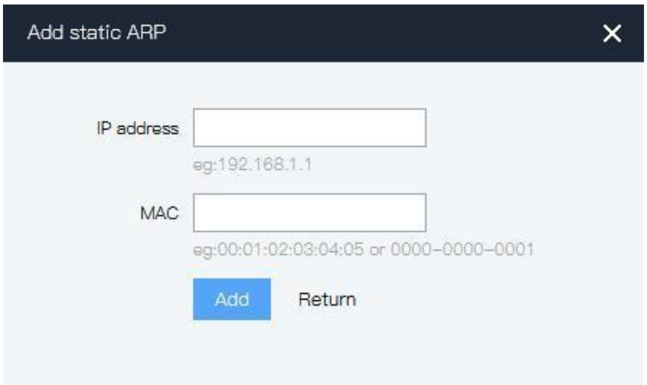
6.7.2 Static ARP

Operation steps：

Click the “Route manage > ARP config” menu in the navigation tree to enter the “Static ARP ”interface, The interface is shown as the following figure:



SerialNum	IP address	MAC	handle



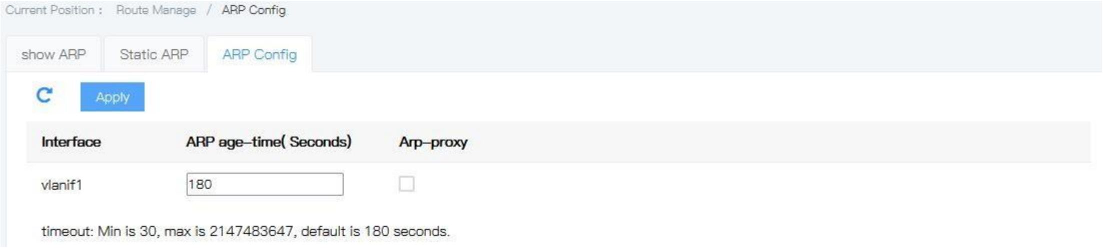
Explanations

Configuration item	Meaning
IP address	Added static IP
Mac	Mac address which matched with IP address which

6.7.3 ARP age-time

Operation steps:

1. Click the “Route manage > ARP config” menu in the navigation tree to enter the “ARP age-time”interface, The interface is shown as the following figure:



Interface	ARP age–time(Seconds)	Arp–proxy
vlanif1	180	□

timeout: Min is 30, max is 2147483647, default is 180 seconds.

Explanations

Configuration item	Meaning
AGE-TIME	Range: 1-2147483647s， default is 600s

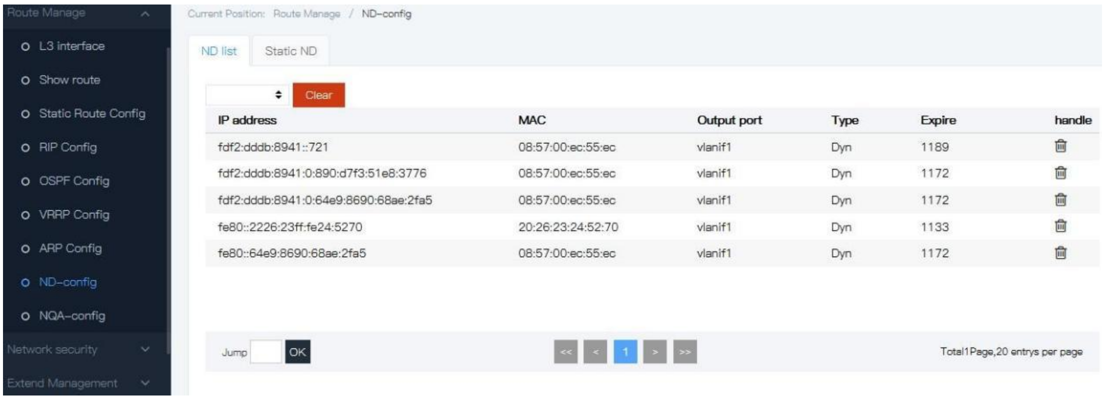
6.8 ND config

ND Snooping is a security feature for IPv6 ND (Neighbor Discovery) for use in two-layer switched network environments. By listening to the Neighbor request message NS (Neighbor Solicitation) in the DAD (Duplicate Address Detection) process of the user to establish ND Snooping dynamic binding table. Thus, the source IPv6 address, source MAC address, VLAN, entry port and other information of the message are recorded to prevent subsequent ND message attacks by impersonating users and impersonating gateways.

6.8.1 ND list

Operation steps:

1. Click the “Route manage >ND config >ND list” menu in the navigation tree to enter the “ARP age-time”interface, The interface is shown as the following figure:



IP address	MAC	Output port	Type	Expire	handle
fdf2:dddb:8941::721	08:57:00:ec:55:ec	vlanif1	Dyn	1189	🗑
fdf2:dddb:8941:0:890:d7f3:51e8:3776	08:57:00:ec:55:ec	vlanif1	Dyn	1172	🗑
fdf2:dddb:8941:0:64e9:8690:68ae:2fa5	08:57:00:ec:55:ec	vlanif1	Dyn	1172	🗑
fe80::2226:23ff:fe24:5270	20:26:23:24:52:70	vlanif1	Dyn	1133	🗑
fe80::64e9:8690:68ae:2fa5	08:57:00:ec:55:ec	vlanif1	Dyn	1172	🗑

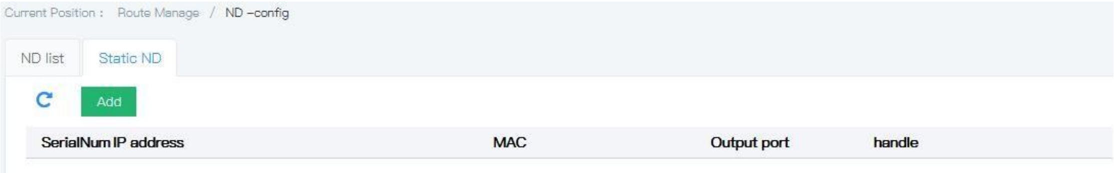
Explanations

Configuration item	Meaning
IP address	Snooping IPv6 address
mac	Local mac
Output port	Output port
type	Both static and dynamic
Expire	Age time

6.8.2 Static ND

Operation steps:

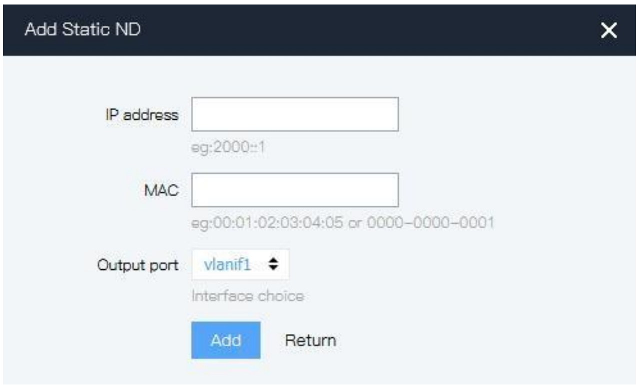
1. Click the "Route manage >ND config >Static ND" menu in the navigation tree to enter the interface, The interface is shown as the following figure:


Current Position : Route Manage / ND –config

ND list | Static ND

Add

SerialNum	IP address	MAC	Output port	handle


Add Static ND

IP address
eg:2000::1

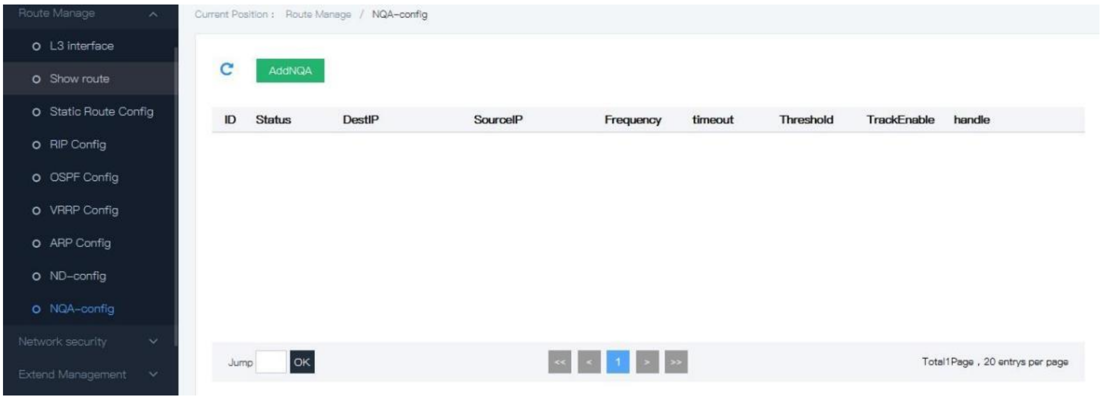
MAC
eg:00:01:02:03:04:05 or 0000-0000-0001

Output port: vlanif1
Interface choice

Add Return

6.9 NQA config

Network Quality Analysis (NQA) is a real-time Network performance detection and statistics technology, which can calculate Network information such as response time, Network jitter, packet loss rate and so on.NQA can monitor network QoS in real time, and diagnose and locate network failure effectively.



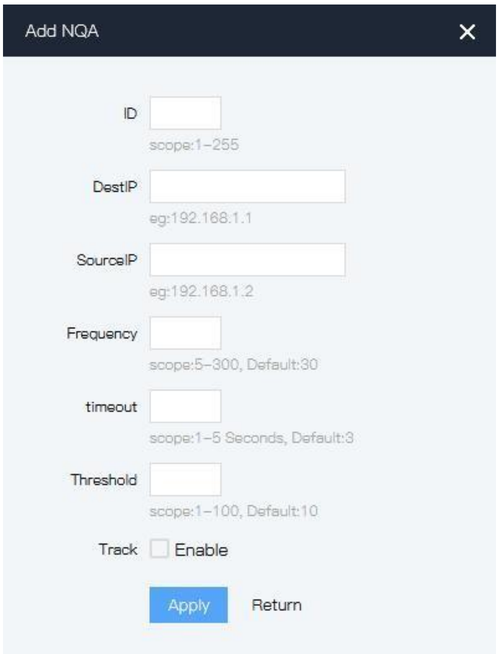
Current Position : Route Manage / NQA-config

AddNQA

ID	Status	DestIP	SourceIP	Frequency	timeout	Threshold	TrackEnable	handle

Jump OK

Total1Page , 20 entrys per page


Add NQA

ID
scope:1–255

DestIP
eg:192.168.1.1

SourceIP
eg:192.168.1.2

Frequency
scope:5–300, Default:30

timeout
scope:1–5 Seconds, Default:3

Threshold
scope:1–100, Default:10

Track □ Enable

Apply Return

Explanations

Configuration item	Meaning
ID	Test group number
Dest IP	Destination access IP address
Source IP	Source IP address
Frequency	The time interval at which NQA test cases automatically execute tests
timeout	Number of probes per test
Threshold	The timeout of a probe
track	Track enable\disable

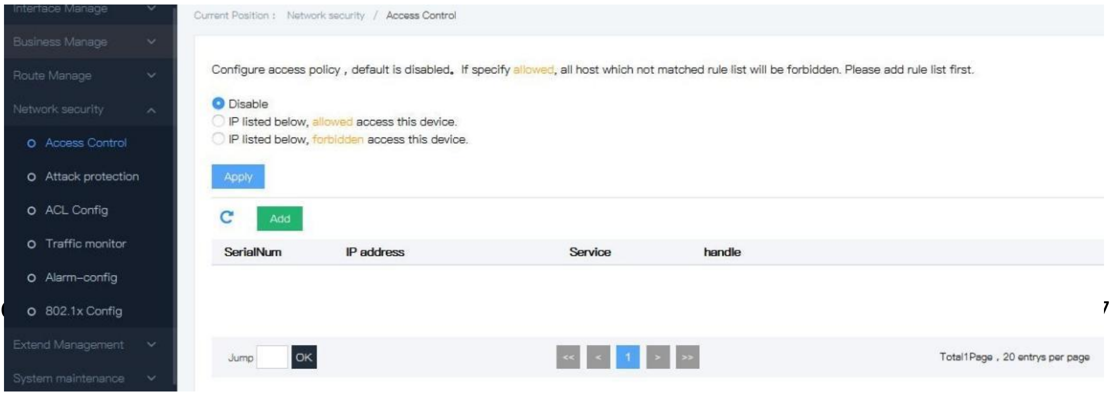
7 Network security

7.1 Access control

As the network size and flow data enlarge, control the network security and distribute the bandwidth become very important. It can prevent unlegal user to access the network by data packets filtering. At the same time, it can save the data flow. ACL adopts matched messages rules to filter the data packets.

Operation steps

1. Click the “network security >Access control” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



Configure access policy , default is disabled。 If specify allowed, all host which not matched rule list will be forbidden. Please add rule list first.

● Disable
○ IP listed below, allowed access this device.
○ IP listed below, forbidden access this device.

Apply

Add

SerialNum	IP address	Service	handle

Jump OK

<< < 1 > >>

Total1Page , 20 entrys per page

Explanations

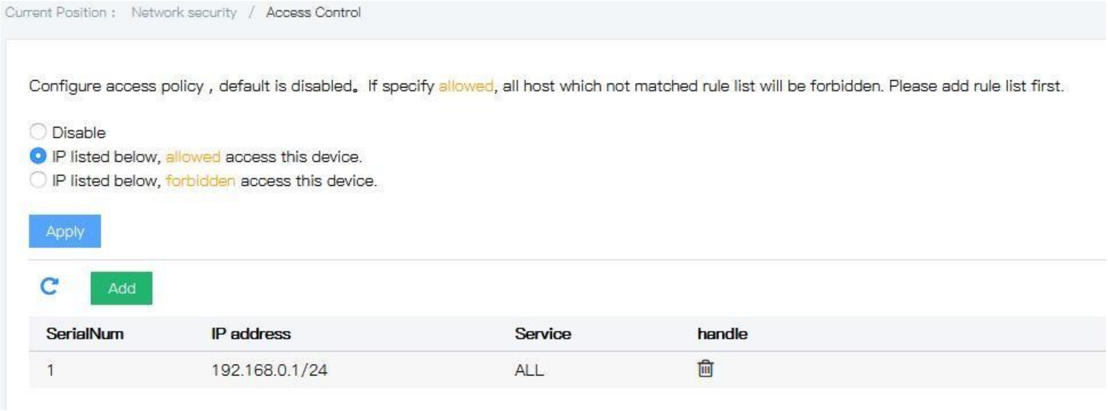
Configuration item	Submenu	meaning
Set the filter rules	Disable	Default is disable
	Meet the rules, allowed access this device	
	Meet the rules, forbidden access this device	
Set the access rule	IP address	Input IP address
	Service	All include both: http， telnet

⚠Attentions

Default is “disable”. If specify, Allowed, all host which not matched rule list will be forbidden, please add rule list first.

2.

Please add the device access rule first. Click the “Network security >Access control >configure access rule for system” menu in the navigation tree to enter the interface, 192.168.0.11/24, select “all” service, click “add”, check “IP listed below, allowed access this device”, click “Apply”, the interface is shown as the following figure:



Current Position : Network security / Access Control

Configure access policy , default is disabled。 If specify allowed, all host which not matched rule list will be forbidden. Please add rule list first.

○ Disable
● IP listed below, allowed access this device.
○ IP listed below, forbidden access this device.

Apply

Add

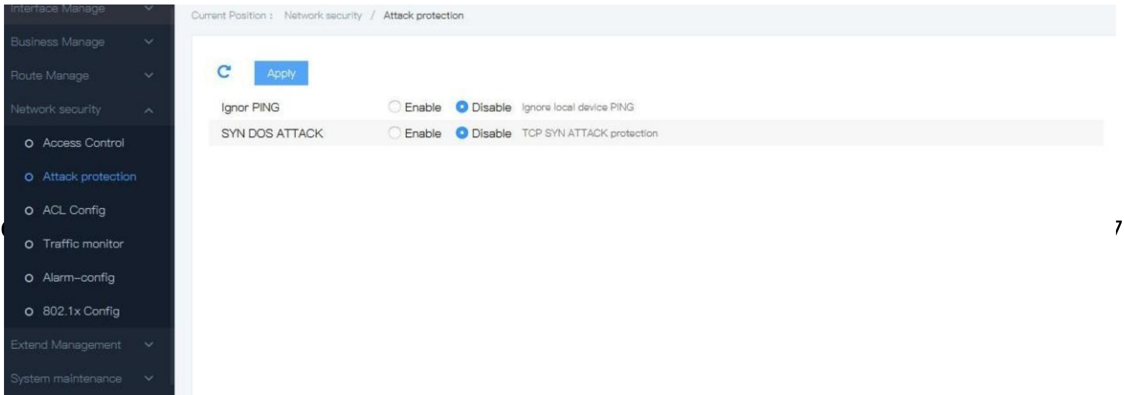
SerialNum	IP address	Service	handle
1	192.168.0.1/24	ALL	🗑

7.2 Attack protection config

To enhance the security of the switch, it is enable to open attack protection.

Operation steps

1. Click the “Network security >Attack protection ” menu in the navigation tree to enter the



Current Position : Network security / Attack protection

Apply

Ignor PING	○ Enable	● Disable	Ignore local device PING
SYN DOS ATTACK	○ Enable	● Disable	TCP SYN ATTACK protection

interface, enable “Ignore local device PING” & “TCP SYN ATTACK protection”, set the value of “CPU receive threshold”, click apply, the interface is shown as the following figure:

Explanations

Configuration item	Meaning
Ignore ping packet	Ignore ping packet’s attack
SYN DOS attack protection	TCP SYN attack protection
CPU receive threshold	Scope：0-100000（defaul:0，means no rate limit），超 if over the scope, no rate receive

7.3 ACL config

The Access Control List (ACL) can realize the packet filtering via configuration of matching rules and processing operations on packets.

After the port of switch receives a packet, it analyzes the fields in the packet based on the ACL rules applied on the current port. After identifying a specific packet, the switch allows or blocks the corresponding packet from passing through according to a preset policy.

The packet matching rules defined by the ACLs can also be referenced by other functions that need to distinguish traffic, such as the definition of traffic classification rules in QoS.

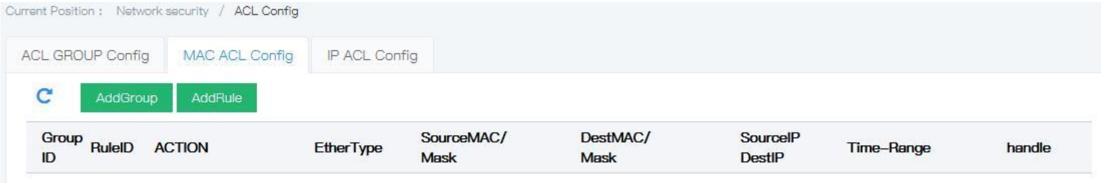
The ACL is a collection of permission and denial conditions that apply to packets. When receiving a packet on an interface, the switch compares the packet field with the ACL used, and judges whether the packet is allowed to be forwarded based on the criteria specified in the access control list. The ACL can classify the packets with a series of matching conditions, which can be the source MAC address, destination MAC address, VLAN, etc. of the packet.

7.3.1 MAC ACL config

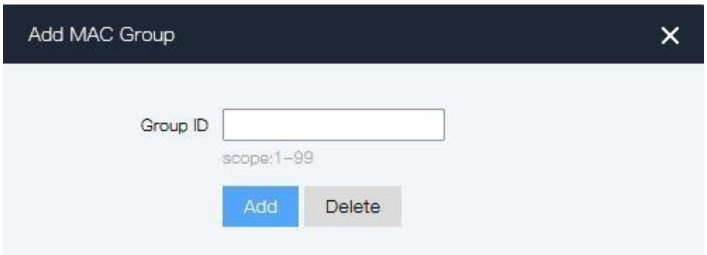
Layer 2 ACL: Set the rules according to source MAC address, Dest MAC address, VLAN priority, layer 2 protocols, etc.

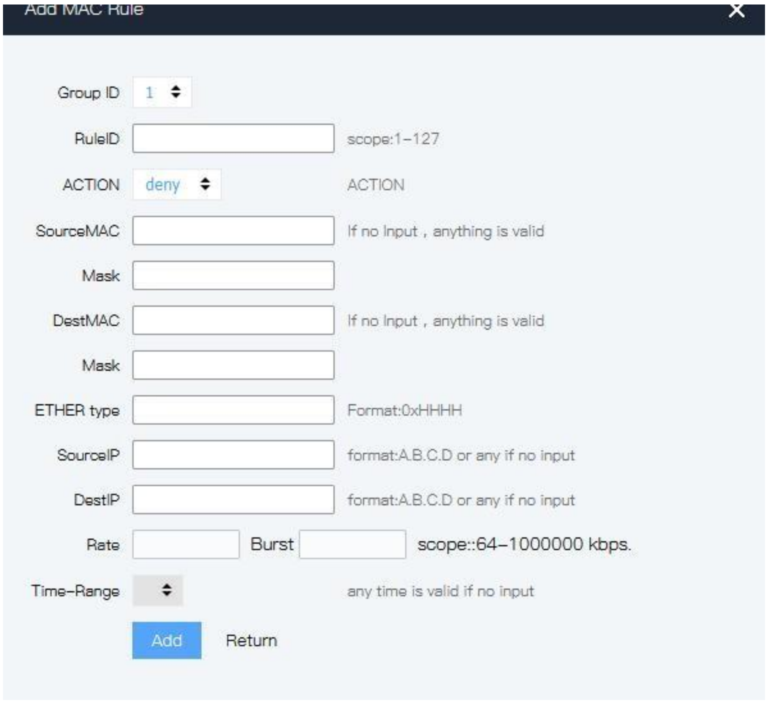
Operation steps

1. Click the “Network security >ACL config > MAC ACL config” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



Group ID	RuleID	ACTION	EtherType	SourceMAC/ Mask	DestMAC/ Mask	SourceIP DestIP	Time-Range	handle





Add MAC Rule

Group ID: 1

RuleID: scope:1–127

ACTION: deny — ACTION

SourceMAC: If no Input , anything is valid

Mask:

DestMAC: If no Input , anything is valid

Mask:

ETHER type: Format:0xHHHH

SourceIP: format:A.B.C.D or any if no input

DestIP: format:A.B.C.D or any if no input

Rate: Burst: scope::64–1000000 kbps.

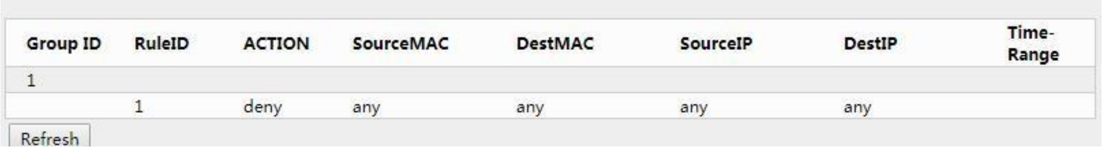
Time-Range: any time is valid if no input

Explanations

Configuration item	Meaning
Group ID	Layer 2 ACL range:1-99
Rule	Scope： 1-127
Action	ACL rules:“permit” or“deny”
Source MAC	Input ACL rule source MAC address. Format: H-H-H。
Dest MAC	Input ACL rule dest MAC address. Format:H-H-H。
Time-Range name	Input the time-Range name

2. Fill corresponding configuration items.

3. Click “add”, the interface is shown as the following figure:



Group ID	RuleID	ACTION	SourceMAC	DestMAC	SourceIP	DestIP	Time-Range
1							
	1	deny	any	any	any	any	

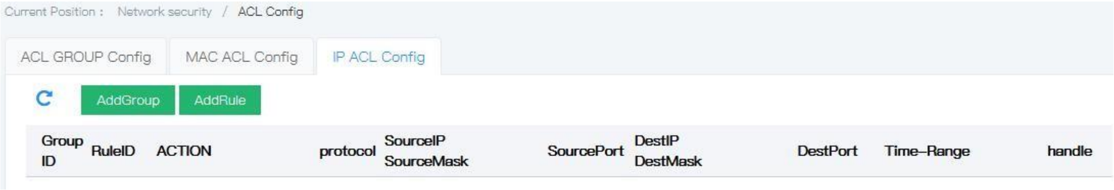
7.3.2 IP ACL config

Based on IP ACL（Basic IP ACL）：Setthe rules based on the source IP address of the packet, ACL ID range： 100~999。

Senior IP ACL（Advanced IP ACL）：Set the rules based on the source IP address, dest IP address, IP’s protocols, etc. ACL ID range： 100~999

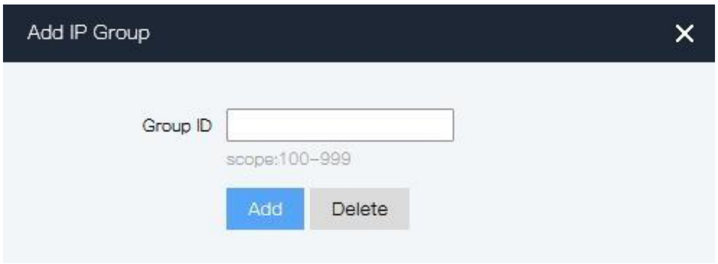
Operation steps

1. Click the “Network security >ACL config > IP ACL config” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



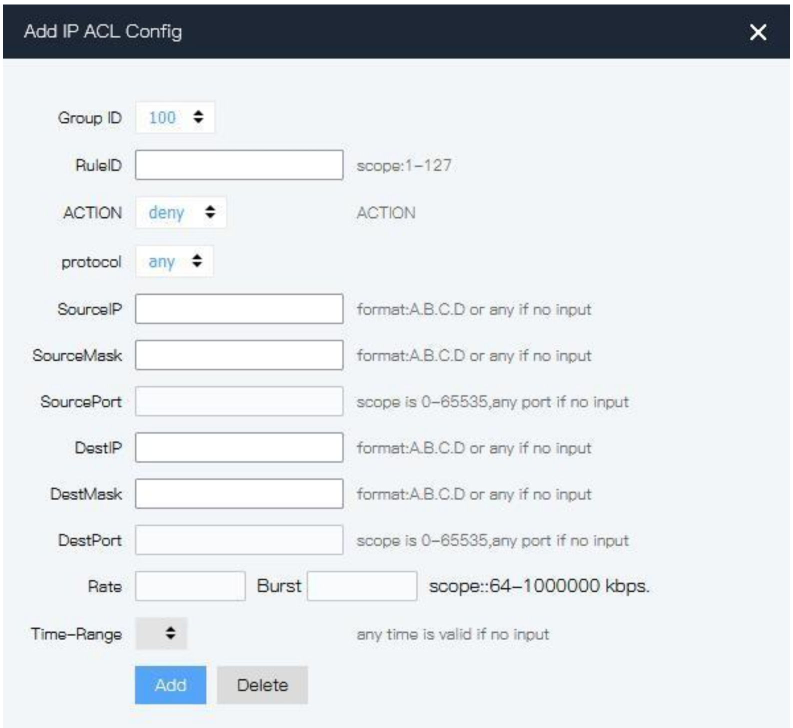
Current Position : Network security / ACL Config

Group ID	RuleID	ACTION	protocol	SourceIP SourceMask	SourcePort	DestIP DestMask	DestPort	Time-Range	handle



Add IP Group

Group ID
scope:100-999



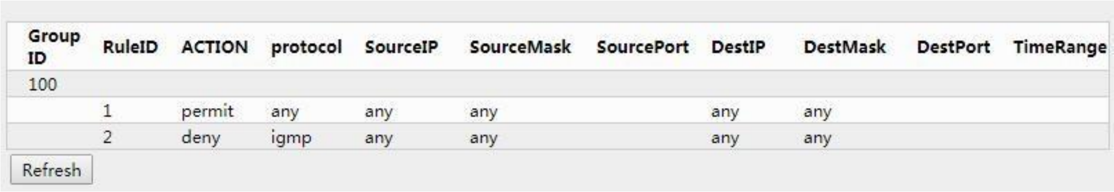
Add IP ACL Config

Group ID	100	
RuleID		scope:1-127
ACTION	deny	ACTION
protocol	any	
SourceIP		format:A.B.C.D or any if no input
SourceMask		format:A.B.C.D or any if no input
SourcePort		scope is 0-65535,any port if no input
DestIP		format:A.B.C.D or any if no input
DestMask		format:A.B.C.D or any if no input
DestPort		scope is 0-65535,any port if no input
Rate	Burst	scope::64-1000000 kbps.
Time-Range		any time is valid if no input

Explanations

Configuration item	Meaning
Group ID	Layer 2 ACL range:100-999
Rule	Scope： 1-127
Action	ACL rules:“permit” or“deny”
Protocol	Type: Any, icmp, igmp, ip, tcp, udp
Source IP	Input ACL rule source IP
Source Mask	Input ACL rule source Mask
Source port	Input ACL rule source port
Dest IP	Input ACL rule dest IP
Dest Mask	Input ACL rule dest Mask
Dest port	Input ACL rule dest port
Time-Range name	Input time-range name

2. Fill corresponding configuration items.
3. Click "add", the interface is shown as the following figure:



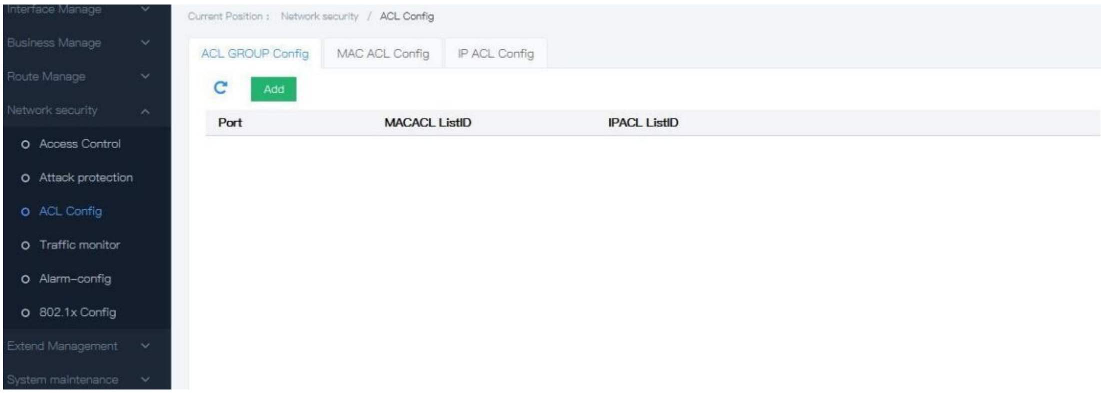
Group ID	RuleID	ACTION	protocol	SourceIP	SourceMask	SourcePort	DestIP	DestMask	DestPort	TimeRange
100										
	1	permit	any	any	any		any	any		
	2	deny	igmp	any	any		any	any		

7.3.3 ACL GROUP config

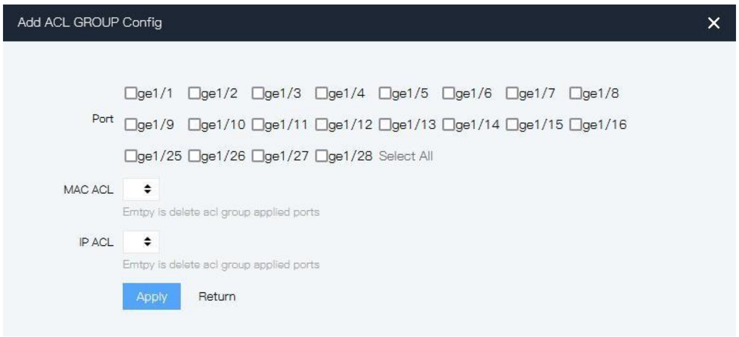
After creating the list, it has to be applicated to the ports that you need to set.

Operation steps：

Click the "Network security >ACL config > ACL GROUP config" menu in the navigation tree to enter the interface, the interface is shown as the following figure:



Port	MACACL ListID	IPACL ListID

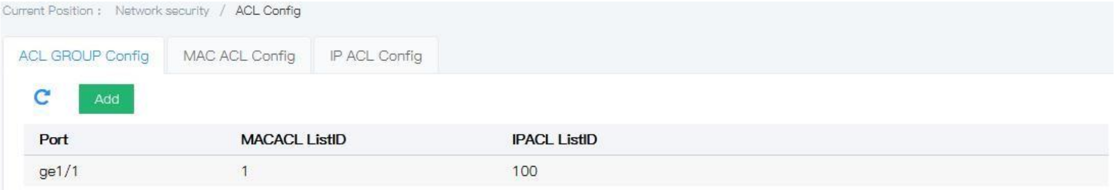


Add ACL GROUP Config

Port ☐ge1/1 ☐ge1/2 ☐ge1/3 ☐ge1/4 ☐ge1/5 ☐ge1/6 ☐ge1/7 ☐ge1/8
☐ge1/9 ☐ge1/10 ☐ge1/11 ☐ge1/12 ☐ge1/13 ☐ge1/14 ☐ge1/15 ☐ge1/16
☐ge1/25 ☐ge1/26 ☐ge1/27 ☐ge1/28 Select All

MAC ACL
Emtpy is delete acl group applied ports

IP ACL
Emtpy is delete acl group applied ports

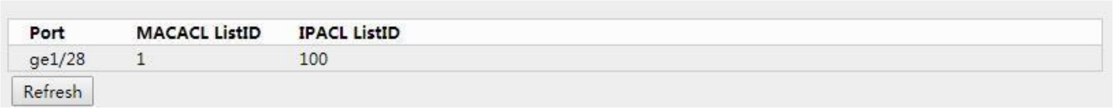


Port	MACACL ListID	IPACL ListID
ge1/1	1	100

Explanations

Configuration item	Meaning
MAC ACL ID	The created MAC ACL ID to be applicated on the ports
IP ACL ID	The created IP ACL ID to be applicated on the ports

2. Fill corresponding configuration items.
3. Click "add", the interface is shown as the following figure:



Port	MACACL ListID	IPACL ListID
ge1/28	1	100

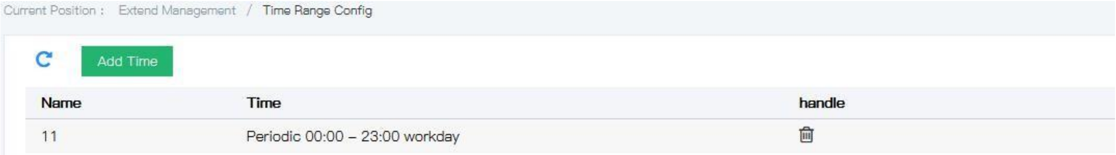
#E.G.

Definition method of time - based ACL.

Suppose an organization wants to use a time based ACL implementation on the switch: Monday to Friday (weekday) mornings from 8:00 to 12:00, afternoons from 13:30 to 17:30, allow for email only, and non-work hours allow for all access.

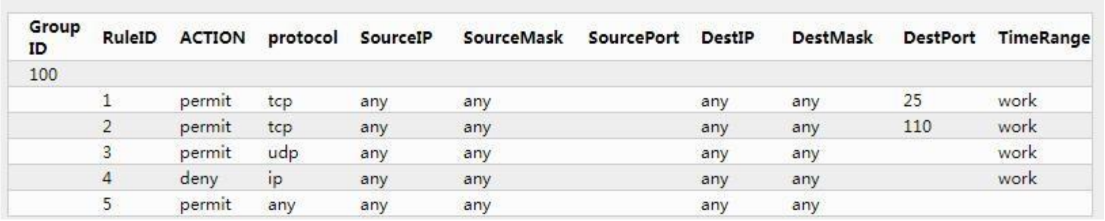
Steps

1. Define time range. Click the "network security > TIME RANGE config" menu in the navigation tree, enter the "TIME RANGE config" interface, select create "Add TIME", and enter the morning of Monday to Friday (working day) from 8:00 to 12:00, and from 13:30 to 17:30, respectively, as shown in the figure below.



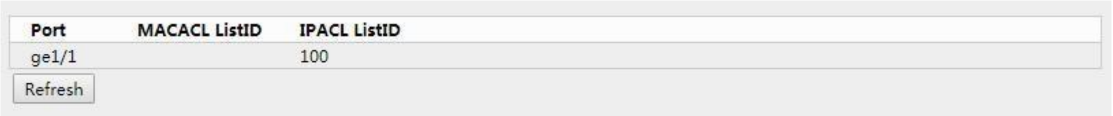
Name	Time	handle
11	Periodic 00:00 – 23:00 workday	🗑

2. Adit ACL. Click the “Network security >ACL config > IP ACL config” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



Group ID	RuleID	ACTION	protocol	SourceIP	SourceMask	SourcePort	DestIP	DestMask	DestPort	TimeRange
100										
	1	permit	tcp	any	any		any	any	25	work
	2	permit	tcp	any	any		any	any	110	work
	3	permit	udp	any	any		any	any		work
	4	deny	ip	any	any		any	any		work
	5	permit	any	any	any		any	any		

3. ACL100 to be applicated on ge1/1. Click the “Network security >ACL config >ACL GROUP config” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



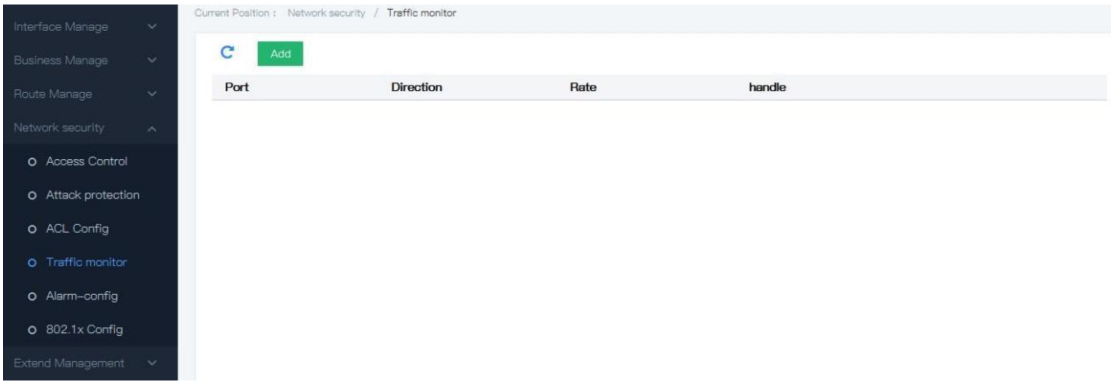
Port	MACACL ListID	IPACL ListID
ge1/1		100

7.4 Traffic monitor

Monitor the port rate

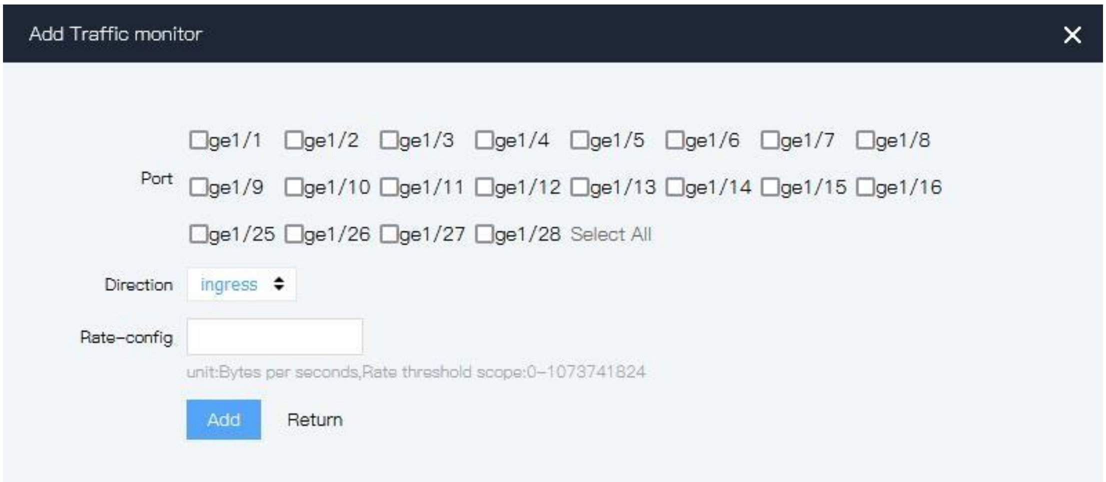
Operation steps

1. Click the “Network security >Traffic monitor” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



Current Position : Network security / Traffic monitor

Port	Direction	Rate	handle



Port ☐ge1/1 ☐ge1/2 ☐ge1/3 ☐ge1/4 ☐ge1/5 ☐ge1/6 ☐ge1/7 ☐ge1/8 ☐ge1/9 ☐ge1/10 ☐ge1/11 ☐ge1/12 ☐ge1/13 ☐ge1/14 ☐ge1/15 ☐ge1/16 ☐ge1/25 ☐ge1/26 ☐ge1/27 ☐ge1/28 Select All

Direction: ingress

Rate-config:

unit:Bytes per seconds,Rate threshold scope:0-1073741824

Explanations

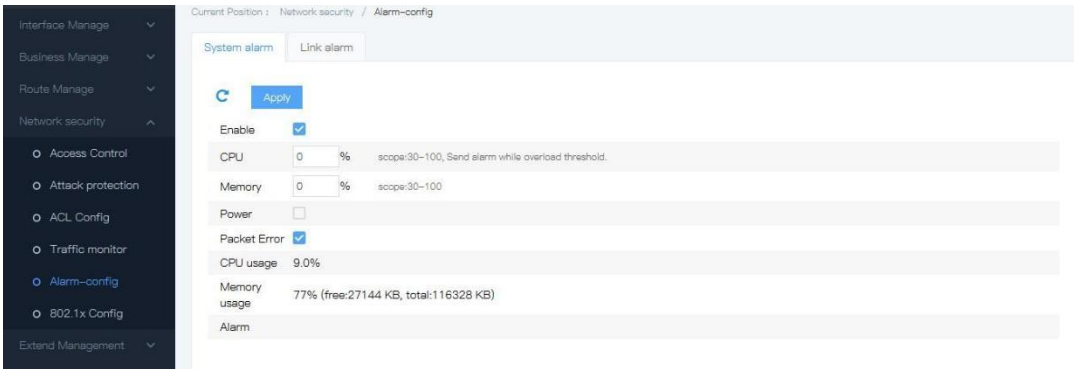
Configuration item	meaning
Direction	Ingress or egress
Rate -config	Scope： 0-1073741824 byte/s

7.5 Alarm config

7.5.1 System alarm

The device supports power alarm, user can configure it according.

1. Click the “Network security > Alarm config” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



Current Position : Network security / Alarm-config

Enable	☑		
CPU	0	%	scope:30-100, Send alarm while overload threshold.
Memory	0	%	scope:30-100
Power	☐		
Packet Error	☑		
CPU usage	9.0%		
Memory usage	77% (free:27144 KB, total:116328 KB)		
Alarm			

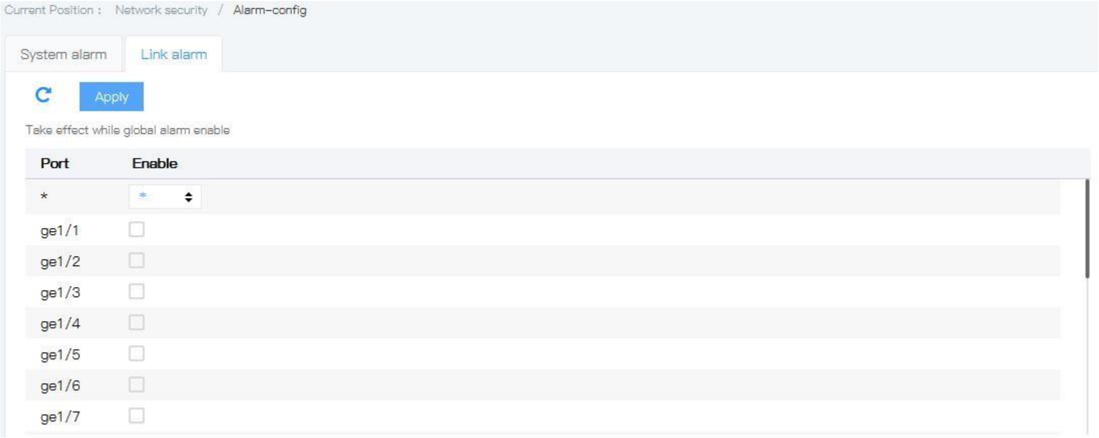
Explanations

Configuration item	Meaning
Enable	Alarm setting
Power	Enable/disable power alarm

7.5.2 Link alarm

User can configure Link alarm according.

1. Click the “Network security > Alarm config >Link alarm” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



Current Position : Network security / Alarm-config

Take effect while global alarm enable

Port	Enable
*	*
ge1/1	□
ge1/2	□
ge1/3	□
ge1/4	□
ge1/5	□
ge1/6	□
ge1/7	□

Explanations

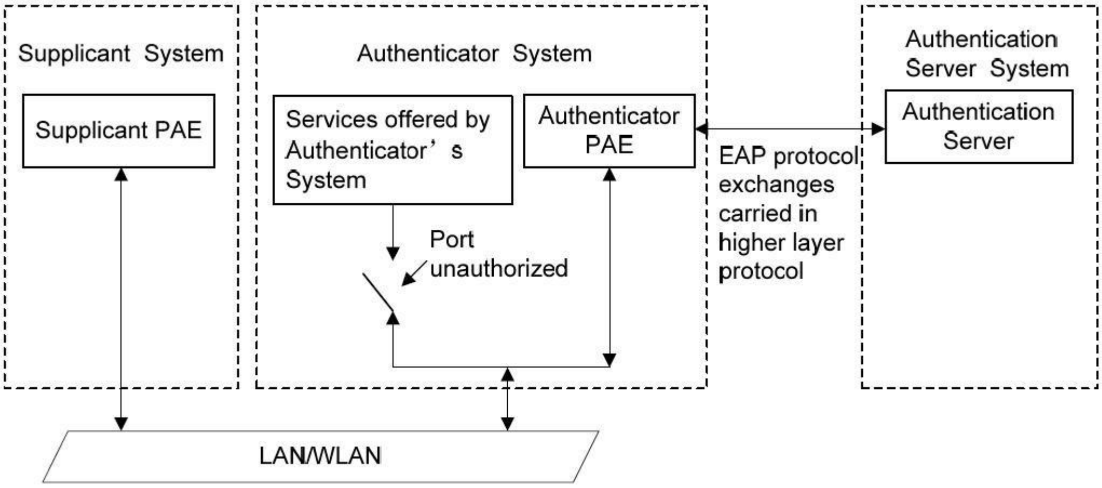
Configuration item	Meaning
Port	Enable or not

7.6 802.1x config

The 802.1X protocol is a port-based network access control protocol that addresses the authentication and security issues in Ethernet, which can authenticate the accessed client devices on the port of the LAN where the devices access, so as to control the access of client devices to network resources.

The 802.1X system consists of three entities: Client, Device, and Authentication server as shown in the figure below.

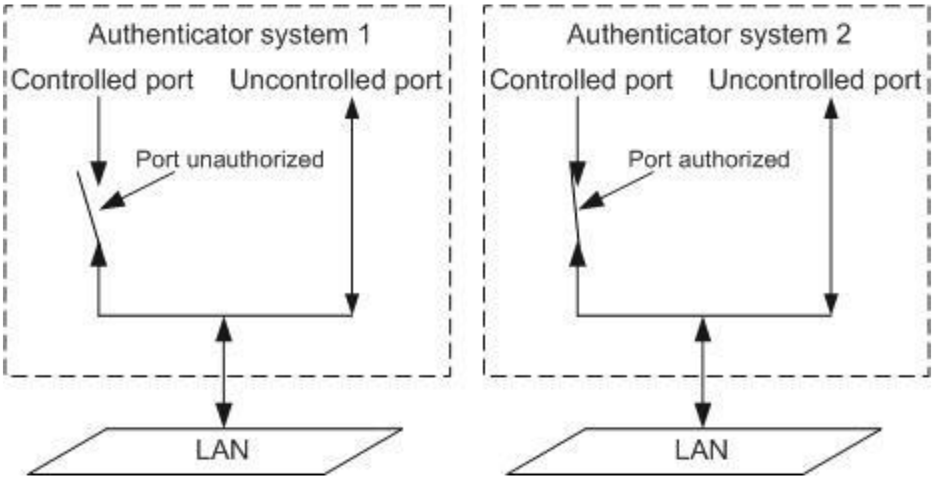
The system used 802.1x is a typical Client/Server structure, it includes Supplicant System（Client）, Authenticator System（Terminal Device） & Authentication Server System（Authentication server）. It is shown as the following figure


Supplicant System
Supplicant PAE
Authenticator System
Services offered by Authenticator’ s System
Authenticator PAE
Port unauthorized
EAP protocol exchanges carried in higher layer protocol
Authentication Server System
Authentication Server
LAN/WLAN

The client is a user terminal device that requests to access the LAN, which shall be authenticated by the device in the LAN. The client shall have the software that supports 802.1X authentication.

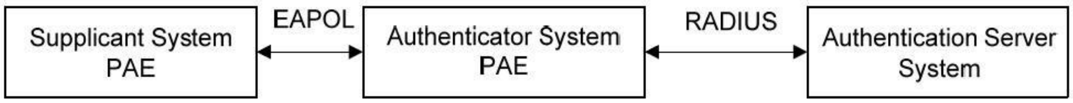
The device is a network device to control the client’s access to the LAN, which is located between the client and the authentication server, provides the client with the port (physical or logical) for accessing the LAN, and authenticate the client connected through the interaction with the server.

The authentication server is used to authenticate, authorize, and charge clients, which is usually a Remote Authentication Dial-In User Service (RADIUS) server. The authentication server verifies the validity of the client based on the client authentication information sent from the device, and transmit the authentication result to the device, which judges whether the client is allowed to access the LAN. In some small-scale networks, the device may also take place of the role of the authentication server, that is, the device locally authenticates, authorizes, and charges the client.



802.1x working mode

IEEE 802.1x authenticator system adopts EAP(Extensible Authentication Protocol) to exchange the authenticator information between the client and authenticator server.



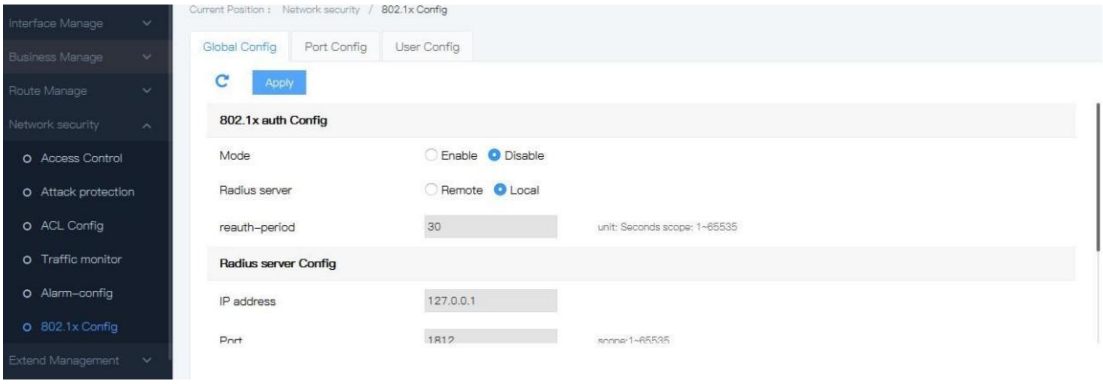
- Between client PAE and device PAE, EAP protocol message uses EAPOL encapsulation format, it is directly hosted in a LAN environment.
- Between PAE on the device end and RADIUS server, EAP protocol messages can use EAPOR (EAP Over RADIUS) packaging format, which is hosted in RADIUS protocol; It can also be terminated by PAE on the device end, and PAP protocol or CHAP protocol messages are transmitted between PAE on the device end and RADIUS server
- When the user is authenticated, the authentication server passes the user's relevant information to the device end, where PAE determines the authorization/unauthorization status of the controlled port according to the instructions of the RADIUS server (Accept or Reject).

7.6.1 Global config

Network access control based on 802.1X access control: Auth & control to the access devices which connect with the interface of LAN.

Operation steps：

1. Click the “Network security >802.1x config > global config” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



802.1x auth Config

Mode ○ Enable ● Disable

Radius server ○ Remote ● Local

reauth-period 30 unit: Seconds scope: 1~65535

Radius server Config

IP address 127.0.0.1

Port 1812 scope:1~65535

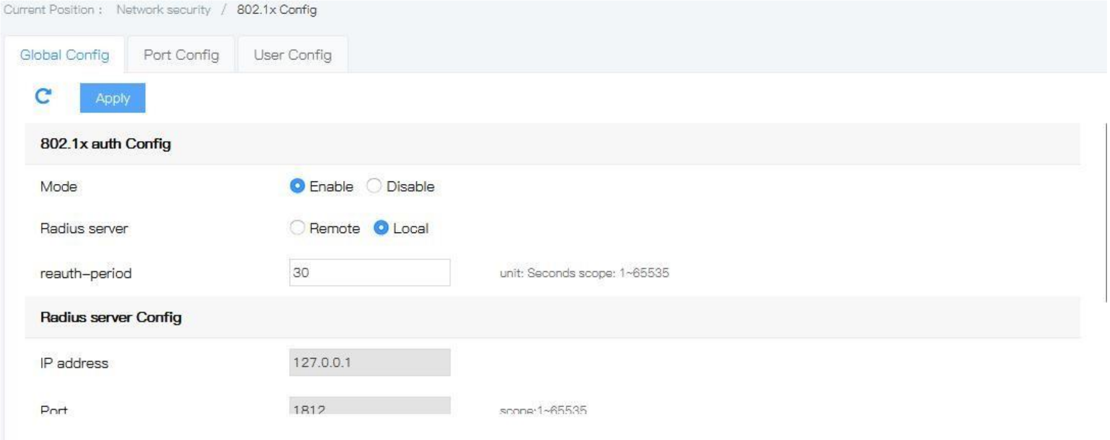
Explanations

Configuration item	Meaning
Mode	Single option. With enable & disable option, default is disable
Radius server	Single option.　With remote & local option, default is local
Reauth-period	Authentication update interval, default is 30 seconds, range: 1~65535. After the successful authentication of 802.1x, the user shall be re-authenticated at a certain interval, which shall be controlled by a re-authentication timer.
IP address	Enter the Radius server to configure the IP address
Port	Enter the Radius server to configure the IP port. Scope: 1 ~ 65535
Auth password	Consistent with Radius server authentication password

Maximum reauthenticate	Number of certification retries. Scope: 1 ~ 10 After the switch sends the authentication request frame to the user for the first time, no response from the user is received within the specified time, and the switch will send the authentication request to the user again. The switch no longer sends the authentication request to the user repeatedly when the sending number reaches its maximum.

2. Fill corresponding configuration items.

3. Click "Apply", the interface is shown as the following figure:



Current Position : Network security / 802.1x Config

Global Config | Port Config | User Config

Apply

802.1x auth Config

Mode: ● Enable ○ Disable

Radius server: ○ Remote ● Local

reauth-period: 30 unit: Seconds scope: 1~65535

Radius server Config

IP address: 127.0.0.1

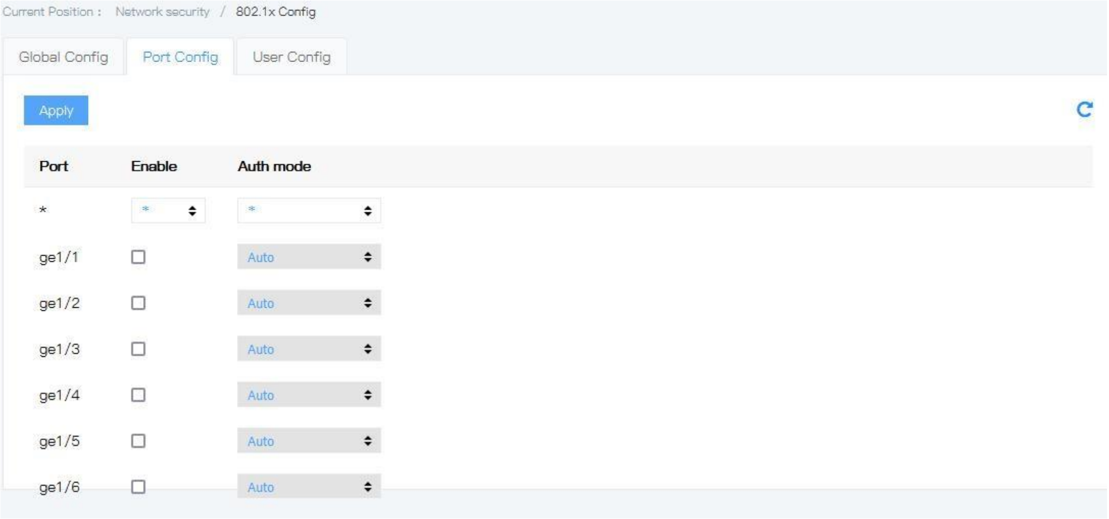
Port: 1812 scope:1~65535

7.6.2 Port config

Network access control based on 802.1X access control: Auth & control to the access devices which connect with the interface of LAN.

Operation steps :

1. Click the "Network security >802.1x config > port config" menu in the navigation tree to enter the interface, the interface is shown as the following figure:



Current Position : Network security / 802.1x Config

Global Config | Port Config | User Config

Apply

Port	Enable	Auth mode
*	*	*
ge1/1	□	Auto
ge1/2	□	Auto
ge1/3	□	Auto
ge1/4	□	Auto
ge1/5	□	Auto
ge1/6	□	Auto

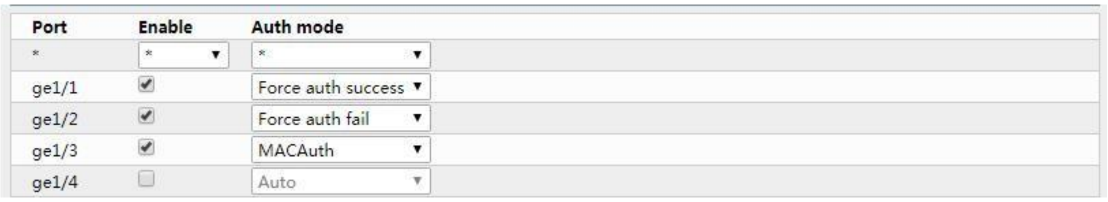
Explanations

Configuration item	Meaning
Port	Single choice, fixed value
Auth mode	Choose the port auth mode:

	Auto mode Force auth success Force auth fail Mac auth Default is auto mode

2. Fill corresponding configuration items.

3. Click “add”, the interface is shown as the following figure:



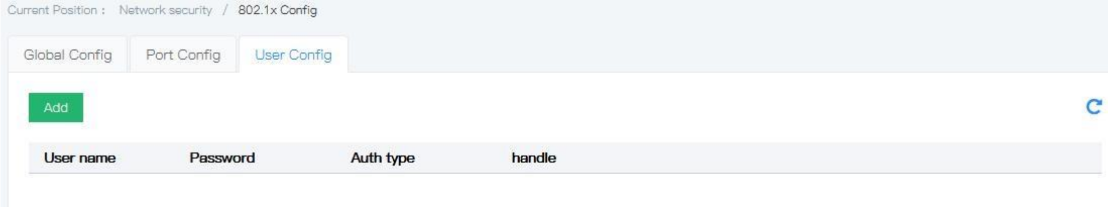
Port	Enable	Auth mode
*	* ▾	* ▾
ge1/1	☑	Force auth success ▾
ge1/2	☑	Force auth fail ▾
ge1/3	☑	MACAuth ▾
ge1/4	☐	Auto ▾

7.6.3 User config

Network access control based on 802.1X access control: Auth & control to the access devices which connect with the interface of LAN.

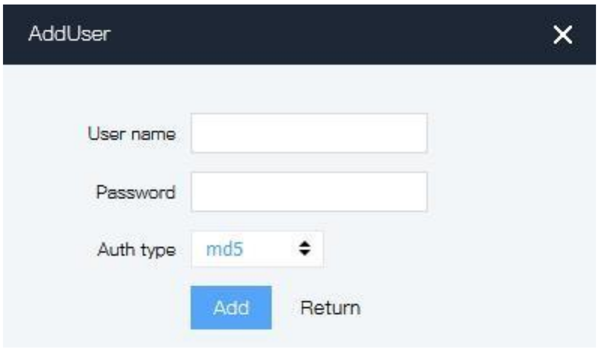
Operation steps :

1. Click the “Network security >802.1x config > user config” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



Current Position : Network security / 802.1x Config

User name	Password	Auth type	handle



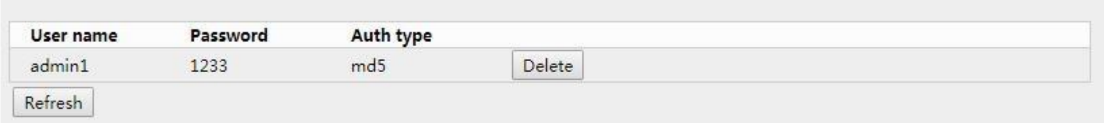
Auth type: md5

Explanations

Configuration item	Meaning
User	User name
Password	Password
Authentication	It includes MD5, TLS, MSCHAPV2, PEAP, TTLS, TLV, GTC, SIM

2. Fill corresponding configuration items.

3. Click “add”, the interface is shown as the following figure:



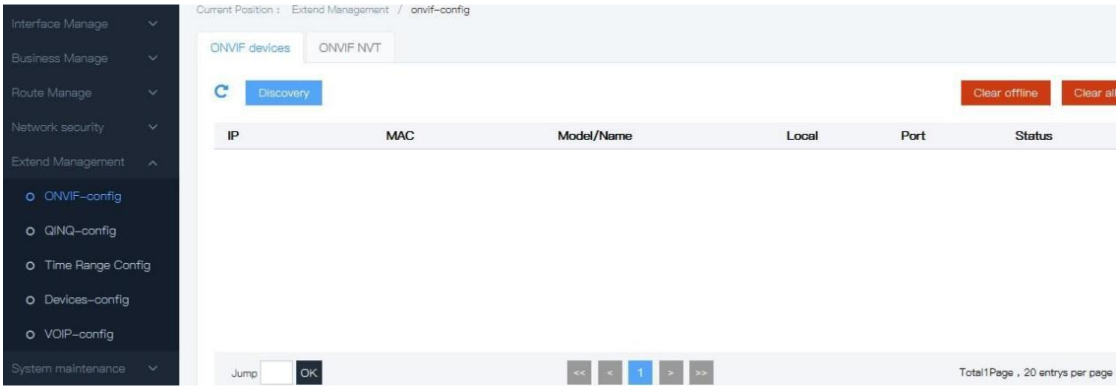
User name	Password	Auth type	
admin1	1233	md5	Delete

Refresh

8 Extend management

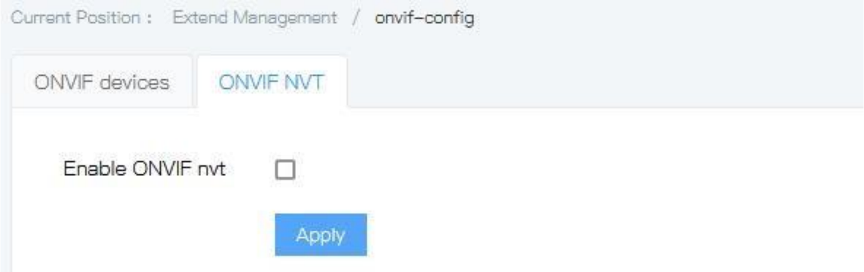
8.1 onvif-config

Click the "Extended Manage >onvif-config" menu in the navigation tree to enter the interface, as shown in the figure below.



IP	MAC	Model/Name	Local	Port	Status

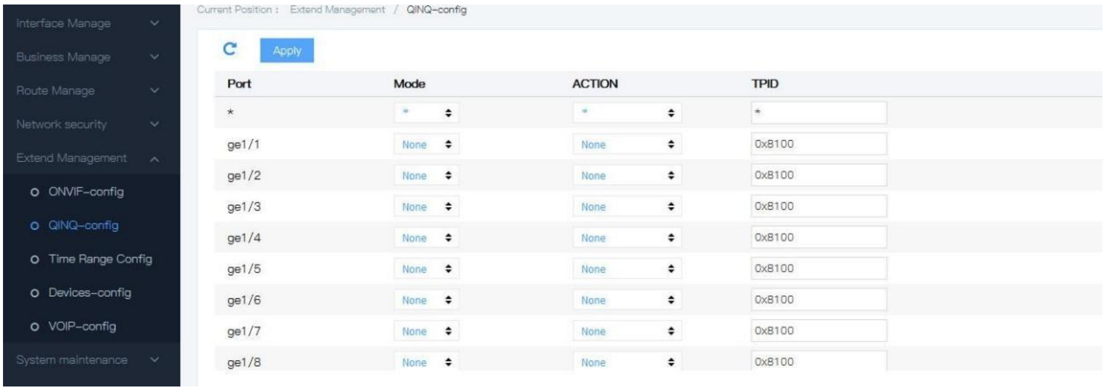
Total1Page , 20 entrys per page



Enable ONVIF nvt □

8.2 QINQ-config

Click the "Extended Manage >qinq-config" menu in the navigation tree to enter the interface, as shown in the figure below.



Port	Mode	ACTION	TPID
*	*	*	*
ge1/1	None	None	0x8100
ge1/2	None	None	0x8100
ge1/3	None	None	0x8100
ge1/4	None	None	0x8100
ge1/5	None	None	0x8100
ge1/6	None	None	0x8100
ge1/7	None	None	0x8100
ge1/8	None	None	0x8100

8.3 TIME RANGE config

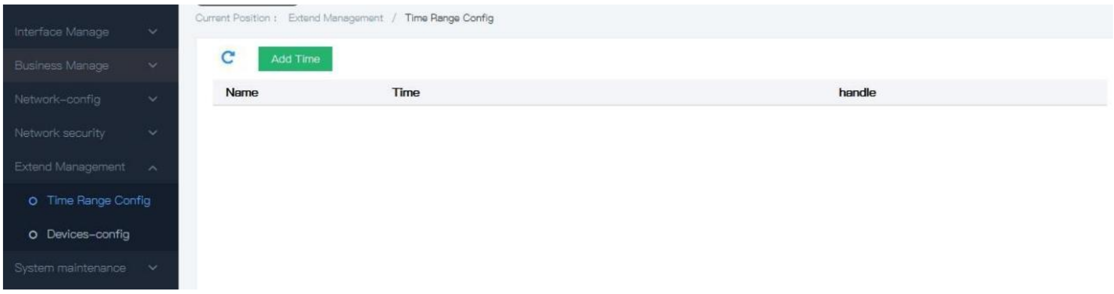
Configuration of effective time periods enables the user to make ACL setting of the message for time periods distinguish.

Time periods are used to describe a particular time range.Users may have requirements that some ACL rules need to be enforced at some time or other, and that they are not used for packet filtering during other time periods, commonly referred to as time period filtering. At this point, the user can configure one or more time periods and then reference that time period when the ACL rules are configured to implement time-based ACL filtering.

The configuration for time periods is as follows: configure period time periods and absolute time periods. The configuration cycle time period takes the form of the weekly days. Configuring absolute time periods takes the form of start time to end time

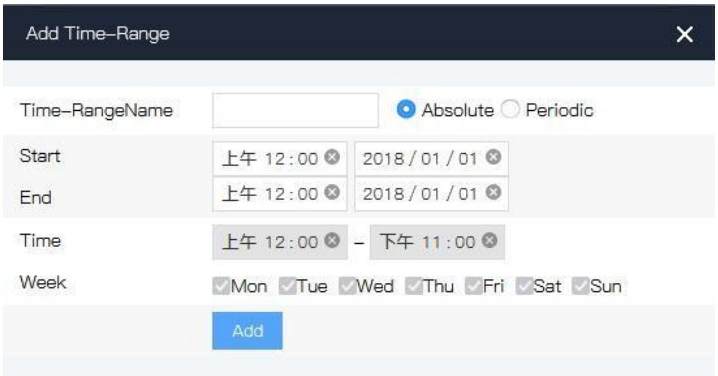
Operation steps

Click the "Business manage > time range config" menu in the navigation tree to enter the interface, the interface is shown as the following figure:



Current Position : Extend Management / Time Range Config

Name	Time	handle



Time-RangeName ● Absolute ○ Periodic

Start 上午 12:00 2018 / 01 / 01

End 上午 12:00 2018 / 01 / 01

Time 上午 12:00 – 下午 11:00

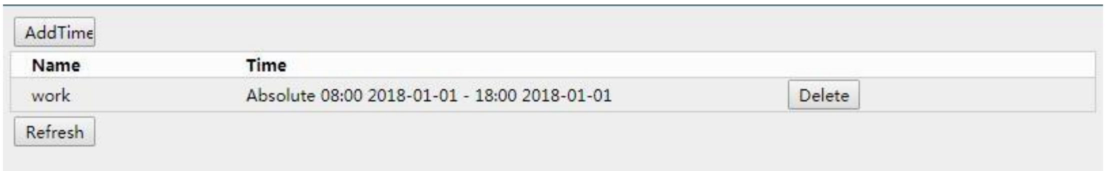
Week ☑Mon ☑Tue ☑Wed ☑Thu ☑Fri ☑Sat ☑Sun

Explanations

Configuration item	meaning
Time-Range name	Input Time-Range name， with optional absolute time & period time
Absolute time	Set the beginning time to end time, different absolute time segment can be set, or not set absolute time
Period time	Set the day fo the week(Mon,Tue…Sun), different period time segment can be set, or not set period time.

2. Fill corresponding configuration items.

3. Click "add", the interface is shown as the following figure:

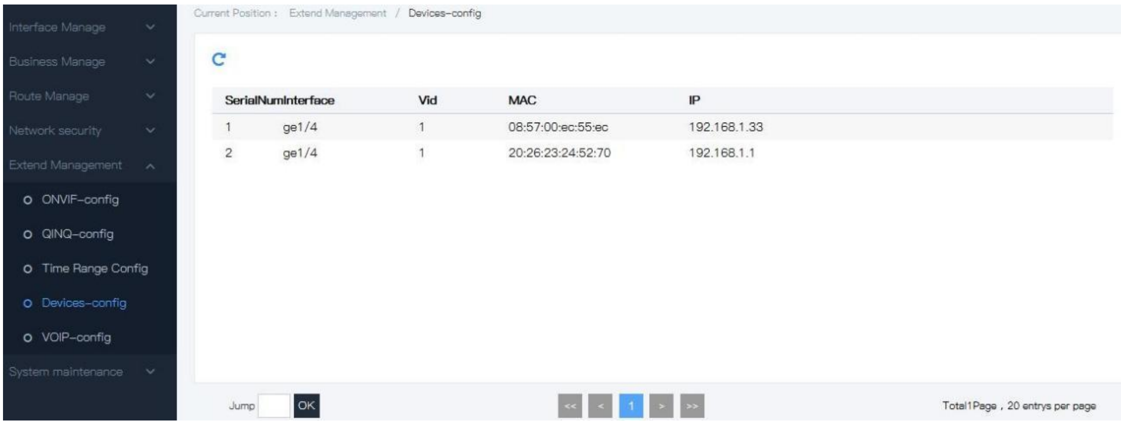


Name	Time	
work	Absolute 08:00 2018-01-01 - 18:00 2018-01-01	Delete

8.4 Devices config

To facilitate the user to view the device interface connected to the device related information.

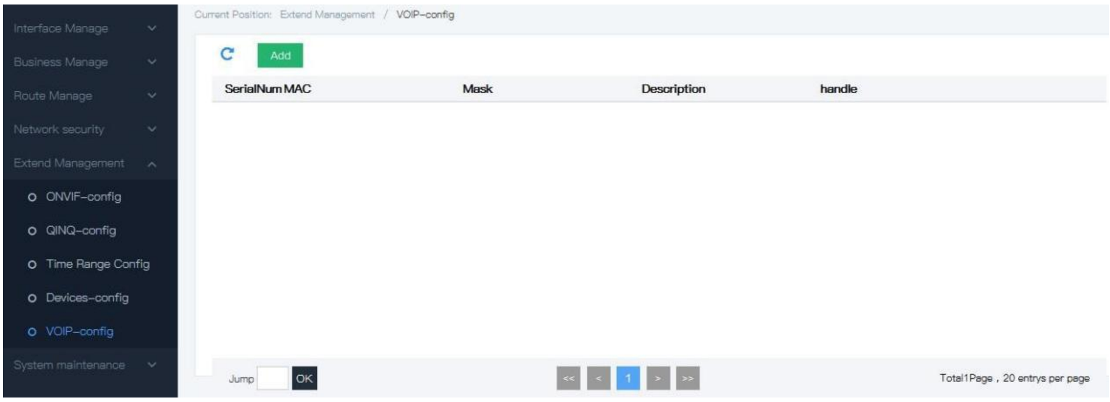
Click the "Extended Manage >Devices Configuration" menu in the navigation tree to enter the interface, as shown in the figure below.



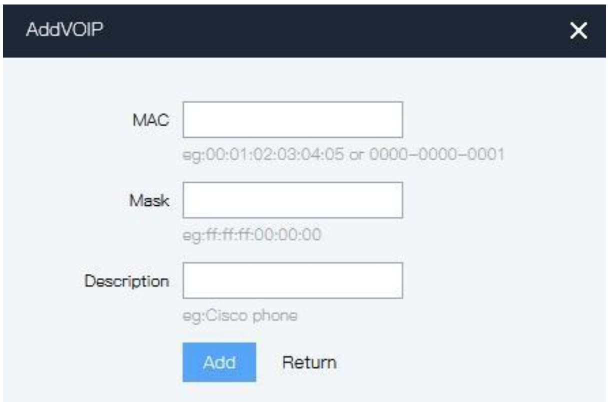
SerialNum	Interface	Vid	MAC	IP
1	ge1/4	1	08:57:00:ec:55:ec	192.168.1.33
2	ge1/4	1	20:26:23:24:52:70	192.168.1.1

8.5 VOIP-config

Click the "Extended Manage >VOIP-config" menu in the navigation tree to enter the interface, as shown in the figure below.



SerialNum	MAC	Mask	Description	handle

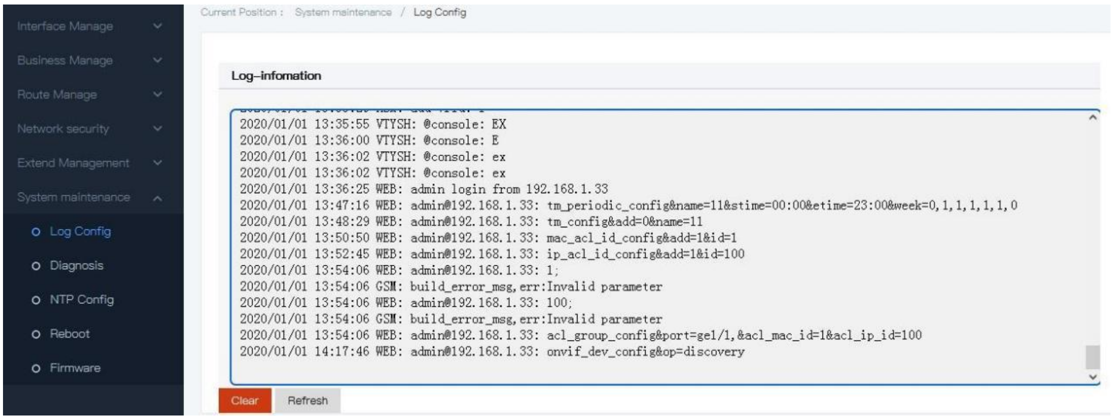


9 system maintenance

9.1 Log config

1. Interface description

Function: Check the device log information(history record), upload device log to tftp server, the interface is shown as the following figure:



```
2020/01/01 13:35:55 VTYSH: @console: EX
2020/01/01 13:36:00 VTYSH: @console: E
2020/01/01 13:36:02 VTYSH: @console: ex
2020/01/01 13:36:02 VTYSH: @console: ex
2020/01/01 13:36:25 WEB: admin login from 192.168.1.33
2020/01/01 13:47:16 WEB: admin@192.168.1.33: tm_periodic_config&name=11&stime=00:00&etime=23:00&week=0,1,1,1,1,1,0
2020/01/01 13:48:29 WEB: admin@192.168.1.33: tm_config&add=0&name=11
2020/01/01 13:50:50 WEB: admin@192.168.1.33: mac_acl_id_config&add=1&id=1
2020/01/01 13:52:45 WEB: admin@192.168.1.33: ip_acl_id_config&add=1&id=100
2020/01/01 13:54:06 WEB: admin@192.168.1.33: 1;
2020/01/01 13:54:06 GSM: build_error_msg,err:Invalid parameter
2020/01/01 13:54:06 WEB: admin@192.168.1.33: 100;
2020/01/01 13:54:06 GSM: build_error_msg,err:Invalid parameter
2020/01/01 13:54:06 WEB: admin@192.168.1.33: acl_group_config&port=ge1/1,&acl_mac_id=1&acl_ip_id=100
2020/01/01 14:17:46 WEB: admin@192.168.1.33: onvif_dev_config&op=discovery
```

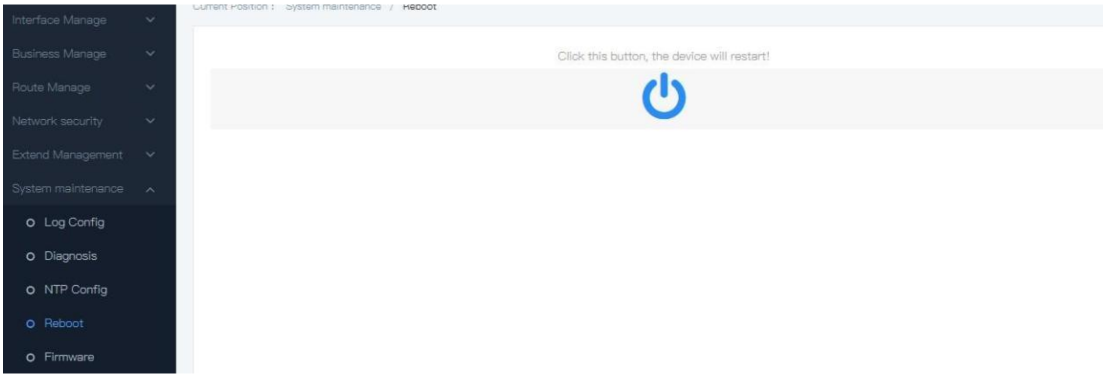
2.Operation steps

Step 1	Click the "System maintenance> log config" menu in the navigation tree to enter the interface, input the TFTP server address: e.g 192.169.1.125, file name "diary", click "Upload".
Step 2	If it shall be used as start configuration, enter the "System manage>running config" for saving the settings.

9.2 Reboot

Operation steps:

1. Click the "System maintenance> reboot" menu in the navigation tree to enter the "Reboot" interface, click "Reboot", The interface is shown as the following figure:



Current Position： System maintenance / Reboot

Click this button, the device will restart!

9.3 NTP config

Network Time Protocol (NTP) is an application layer Protocol in TCP/IP Protocol family. NTP is used to synchronize the clock between a series of distributed time servers and clients. The implementation of NTP is based on IP and UDP. NTP messages are transmitted through UDP, and the port number is 123. With the complexity of network topology, clock synchronization of devices in the whole network becomes very important. If you rely on the administrator to manually modify the system clock, not only lots of work to do, but also the accuracy of the clock can not be guaranteed. NTP is to solve the synchronization problem of the system clock in the network.

NTP basic principle: NTP implementation process as shown below. RouterA and RouterB are connected through the WAN, and both of them have their own independent system clocks, which can be automatically synchronized through NTP.

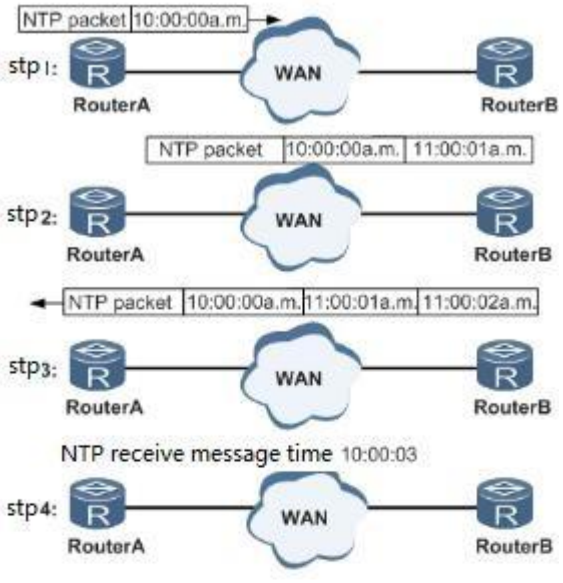
Make the following assumptions:

Before RouterA and RouterB's system clock synchronization, RouterA's clock was set to 10:00:00a.m. And RouterB's clock was set to 11:00:00a.m.

As an NTP time server, RouterB's clock is synchronized with RouterB's clock.

The time for one-way transmission between RouterA and RouterB is 1 second.

The time for both RouterA and RouterB process NTP messages is 1 second.



System clock setting:

RouterA sends NTP message to RouterB, this message includes the time mark that it leaves RouterA 10:00:00a.m.（T1）

When the NTP message reach RouterB, RouterB add the reach time mark 11:00:01a.m.（T2）

When the NTP message leaves RouterB, RouterB add the leave time mark 11:00:02a.m.（T3）

RouterA receives this response message, adds new time mark 10:00:03a.m.（T4）

After this, RouterA get enough information to calculate below data:

The delay time that NTP message leave and back in one period： Delay= (T4 - T1) - (T3 – T2)。

Time difference for RouterA to RouterB： Offset= ((T2- T1) + (T3 – T4)) / 2。

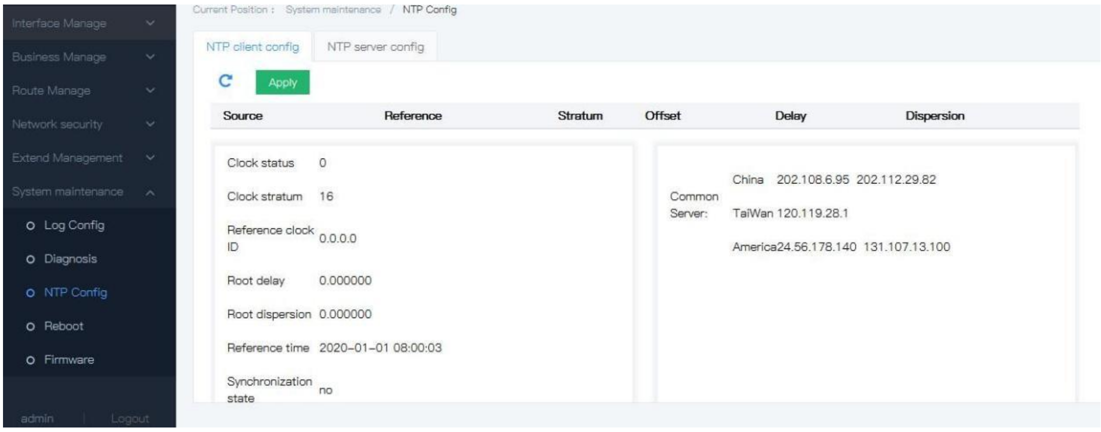
The delay time of RouterA after calculation is 2s ， Offset is 1h. RouterA set its time according to this information, so as to synchronize with RouterB.

📖 Explanation：

Above is the simple description of NTP, RFC1305 defines the calculation of NTP.

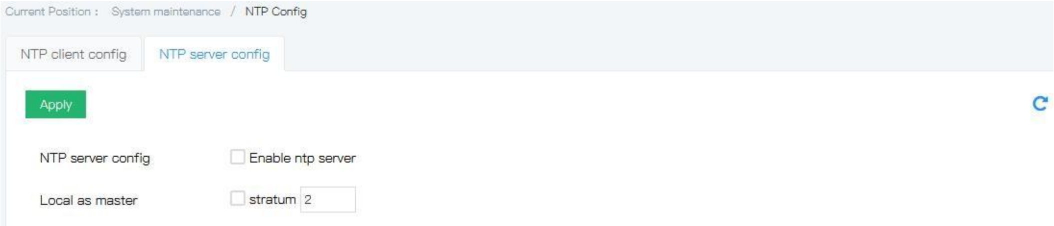
Operation steps

1. Click the “System manage >NTP config” menu in the navigation tree to enter the interface, the interface is shown as the following figure:



Clock status 0
Clock stratum 16
Reference clock ID 0.0.0.0
Root delay 0.000000
Root dispersion 0.000000
Reference time 2020-01-01 08:00:03
Synchronization state no

Common Server: China 202.108.6.95 202.112.29.82
TaiWan 120.119.28.1
America24.56.178.140 131.107.13.100



NTP server config ☐ Enable ntp server
Local as master ☐ stratum 2

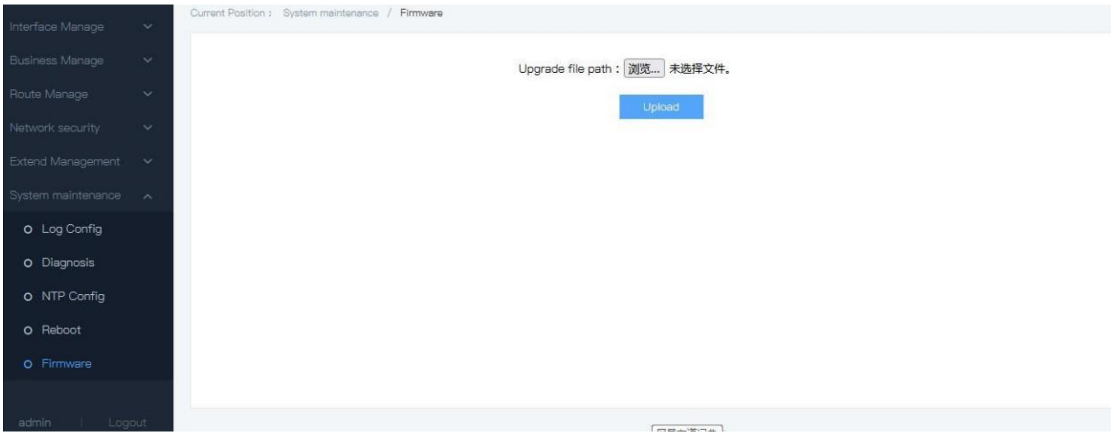
Explanations

Configuration item	Meaning
Mode	Enable or disable NTP Auto clock
Interval	Range： 5-65535 default： 300
Server	Max. support 5 server IP address

9.4 Online Upgrading

Operation steps

Click the “System maintenance> firmware” menu in the navigation tree to enter the “Firmware” interface, click “choose file>upload”, The interface is shown as the following figure:



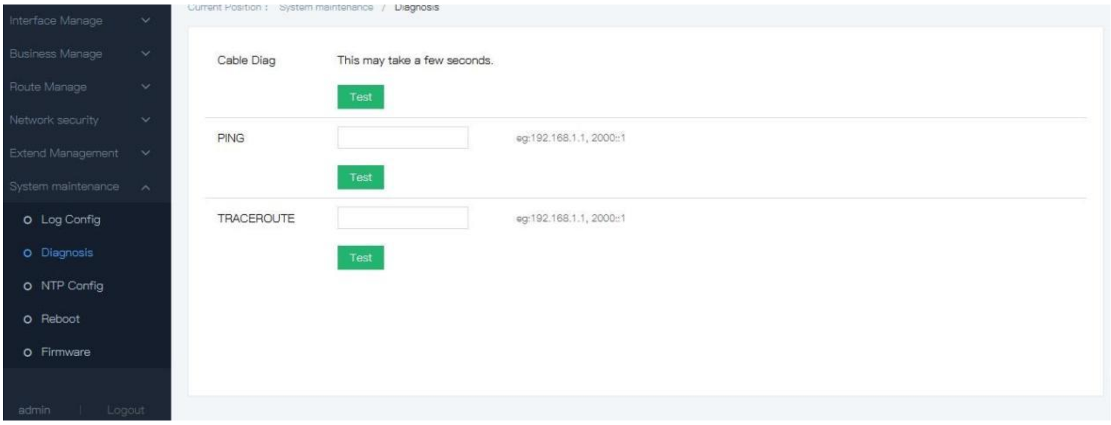
Upgrade file path : 浏览... 未选择文件。

9.5 Diagnosis test

9.5.1 ping

1. Interface description

PING is a command for checking the network connection and rate. The IP address is unique, one of the device will send a packet to the dest IP address, and request it to send back the same packet. With this, it can be confirmed that if these two devices are connecting, what the time delay is.



Cable Diag — This may take a few seconds.

PING — eg:192.168.1.1, 2000::1

TRACEROUTE — eg:192.168.1.1, 2000::1

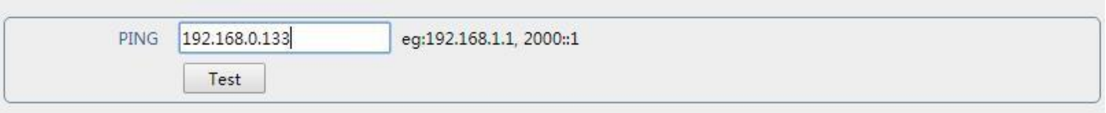
2. Operation steps

Step 1	Click the "System config" menu in the navigation bar to enter the "System config" interface, click “Diagnosis”, input the IP address in “PING”
Step 2	Click “test” to get the result.

3. E.G.

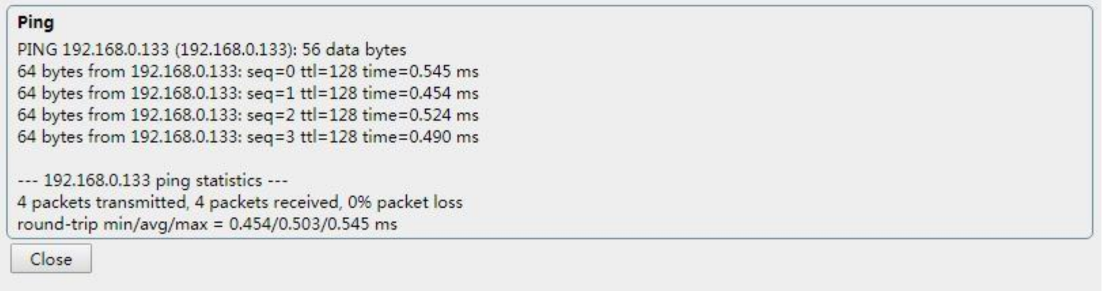
#ping test IP address is 172.16.14.25

1） IP address input： 172.16.14.25， Click “test”.



PING 192.168.0.133 eg:192.168.1.1, 2000::1

2） Test result is shown as the following figure:



Ping

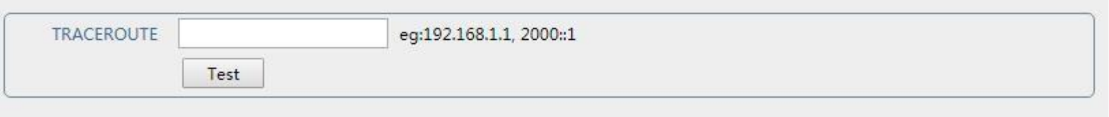
```
PING 192.168.0.133 (192.168.0.133): 56 data bytes
64 bytes from 192.168.0.133: seq=0 ttl=128 time=0.545 ms
64 bytes from 192.168.0.133: seq=1 ttl=128 time=0.454 ms
64 bytes from 192.168.0.133: seq=2 ttl=128 time=0.524 ms
64 bytes from 192.168.0.133: seq=3 ttl=128 time=0.490 ms

--- 192.168.0.133 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.454/0.503/0.545 ms
```

9.5.2 Traceroute

1. Interface description

Traceroute test how long time by sending a small data packet to target device until the data packet are back from the target device. Port circuit includes PHY layer circuit & MAC circuit. The interface is shown as the following figure:



2. Operation steps

Step 1	Click the "Diagnosis" menu in the navigation bar to enter the interface, click "traceroute", input the IP address.
Step 2	Click "test" to get the result.