Layer 3 Ethernet Switch

User's manual

28th/May/2020

Version: V3.0

Revision History

Date	Version	Description
28/10/2016	V 1.0	First Edition
10/3/2020	V 2.0	Refresh according to new version UI
28/5/2020	V 3.0	Refresh according to the company's new brand requirements

0 Foreword

0.1 Target reader

This manual applies for installers and system administrators who are responsible for installing, configuring, or maintaining the network. This manual assumes that you understand the transport and management protocols used by all networks.
This manual also assumes that you are familiar with the technical terms, theoretical principles, practical skills, and specific expertise of network devices, protocols and interfaces related to networking. At the same time, you must have a graphical user interface, command line interface, simple network management protocol and Web browser work experience.

0.2 Conventions

This manual comply with the following conventions

GUI Conventions	Description
✍ illustrate	Description of the operation content, make the necessary additions and explanations.
⚠ Notice	Remind the operator should pay attention to matters, improper operation may cause data loss or damage to equipment.

1 Managed Software Specifications

1.Layer2 function			
1.1	Port Management	Enable / disable ports	
		speed、duplex、MTU Settings	
		flow-control settings	
		View port information	
1.2	Port Mirroring	Support port in/out direction, Vlan mirroring	vlan mirroring only supports command line configuration
1.3	Port Speed	Supports port speed limit, the rate-limiting is determined by the chip	
1.4	Port Isolation	Support port isolation settings	
1.5	Suppression	Support unknown unicast, unknown multicast, broadcast storm suppression	
1.6	Link Aggregation	Support Static aggregation	
		Support LACP Dynamic aggregation	
1.7	VLAN	access	
		trunk	
		hybrid	replaced by trunk
		Support based on port, protocol, MAC VLAN classification	
		Support GVRP dynamic VLAN registration	Only supports command line configuration
1.8	MAC	Support Static add, delete	
		Limit the number of MAC address learning	
		Supports dynamic aging time	
1.9	Spanning Tree	Support 802.1d (STP)	
		Support 802.1w (RSTP)	
		Support 802.1s (MSTP)	
1.10	IGMP-snooping	Support Static add, delete	
		Support v1 / 2/3 Dynamic Multicast Listening	
2.Layer3 and Routing function			
2.1	Port configuration	Support SVI port	

2.2	ARP	Support Statics ARP	
		Support set ARP aging time	
2.3	VRRP	Support VRRP routing backup	
2.4	ND	Support IPv6_ND configuration	
2.5	Routing function	Statics routing	
		RIP（V1/V2）	
		OSPF(V2)	
		RIP/OSPF support routing authentication function	
		RIP/OSPF support routing lead-in and filtering function	
3.Extensions			
3.1	ACL	Based on source MAC, the purpose of MAC, protocol type, source IP, destination IP, L4 port number	
		Support time-range time management	
3.2	QOS	Based 802.1p (COS) Category	
		Based DSCP Category	
		Based on source IP, destination IP, port number classification	
		Support SP, WRR, DRR scheduling policy	
		Support flow rate-limiting CAR	
3.3	LLDP	Support LLDP link discovery protocol	
3.4	User settings	Add / remove users	
3.5	Journal	User login, operation, status, event logging	
3.6	Attack prevention	DOS defense	
		Support CPU protection Limit the rate of sending cpu packets	
		ARP bindings (IP, MAC, PORT Binding)	
3.7	Network Diagnostics	Support ping、telnet、trace	
3.8	System Management	Device reset, configuration save / restore, upgrade management, time settings, etc.	
4 Management Function			
4.1	CLI	Supports Serial Command Line Management	
4.2	TELNET	Support telnet remote management	

4.3	WEB	Support Layer2 Settings	
5.Other functions			
5.1	Support DHCP Server		
5.2	Ring protection - This feature is ERPS		
5.3	SNMPV1/V2C/V3		

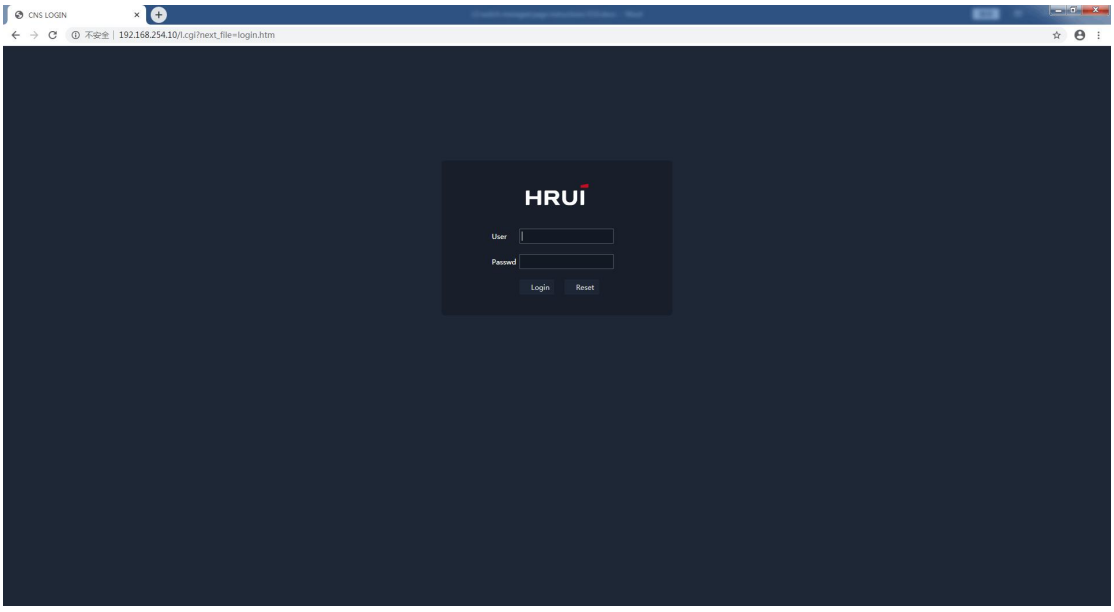
2 Login Web page

2.1 Login Web system client

Users can open a Web browser and enter the default address of switch: http://192.168.254.1,press Enter.

✍ illustrate：When logging into the switch, the switch network segment should be same as IP network segment of the PC.The first time you log in, set the PC's IP address to 192.168.254.x（x represents 1 to 254, except1,set Subnet mask to 255.255.255.0,But PC IP Can't be the same as switch,that can not be 192.168.254.1.

Login window appears, as shown below. Input the default user name: admin and password admin. Click <Login> button, you will see the switch system information



2.2 Web Interface navigation tree

Web NMS menu mainly provides system configuration, port configuration, layer 2

configuration, network security, network configuration, system maintenance, six menu items. There are submenus under each menu option, as shown in Table.

Menu Item	Sub-menu	Explanation
Device Brief		Display port status and product information
System Management	Config Management	Provide query equipment current running configuration, start configuration and configuration management
	Reboot	Reboots the switch
	Upgrade Software	Upgrade Switch's Software Version
	User	Setting users information, including user name, password, permissions (1-15)
	Log	Display log information on the device
	Access	Enable / disable TELNET services Enable / disable HTTP service, modify the port number, the default port number 80
	SNMP	Configures and queries SNMP system configuration, Trap Configuration and User Configuration
	LLDP	Configures and queries global QOS configuration, port configuration and functions of LLDP Neighbor
Interface Management	Port Management	Set the port speed (auto-negotiation, 10M, 100M, 1000M), set the flow control (disable, tx, rx, both), enable or disable the maximum Frame
	L3 interface	Configures VLANIF port
	Link-aggregation	Provide configuring and querying static and dynamic LACP function
	Mirror	Provide configuring and querying port mirroring
	Port Statistics	Provide querying port summary and detailed statistics function
	Bandwidth Chart	Query port bandwidth trend statistics and support downloading
Business Management	VLAN	Provide configuring and querying VLAN, interface information function
	MAC	Provide configuring and querying MAC address table information, MAC aging time, MAC learning, static MAC functions
	Spanning-tree	Provide configuring and querying device's STP global configuration, instance configuration, the instance port configuration and port configurations function.
	ERPS	Provide configuring and querying ERPS-Ring global configuration and node configuration features
	QINQ	Configures QINQ VLAN
	NTP	configures and queries the NTP server
	DHCP Server	Configures and queries DHCP Server configuration, address pool configuration, client lists configuration, client static configuration, port binding function
	ARP	Configures statics ARP and view ARP
	ND	Support IPV6 Statics ND binding

Route	Show route	View routing table, including direct, static and dynamic routing table
	Static Route	Support statics routing configuration
	RIP	Support RIP vision V1/V2 configuration
	OSPF	OSPF routing function configuration
	VRRP	Configures and view VRRP
Multicast	MulticastMAC	Provide static multicast MAC configuration
	IGMP-snooping Configuration	Provide configuring and querying IGMP Snooping configurations and static multicast function
	IGMP	Provide configuration of interface multicast properties
	PIM	Provide global configuration of PIM protocol
	Multicast Route	Provide multicast routing static configuration
Network Security	Isolate-port	Provide configuring and querying Layer 2 port isolation function
	802.1x	Provide 802.1X function
	Storm Control	The device supports Suppression control at broadcast, unknown multicast and unknown unicast message of port by pack rate to to prevent these three types of messages from broadcasting storms
	ACL	Configures and queries ACL information
	Access control	Configures and queries filtering rules and accessing device rules
	Anti-attack settings	Configures and queries anti-attack function
	Alarm	Provide system alarm and interface alarm settings
QOS	Traffic management	Provide traffic policy function
	Port Rate-Limit	Provide the function of configuring and querying the speed limit of the interface
	Traffic shaping	Provide flow shaping function
	Congestion management	Provide QoS congestion scheduling strategy
	Default priority	Provide port priority function
	Priority map	Provide priority mapping function
Extend Management	ONVIF	Provide ONVIF discovery function
	Time Range Config	Configuring effective period of time allows the user to distinguish packets ACL.
	Devices	Provide Mac and IP information table item functions
	VOIP	Provide VoIP function
	Diagnosis	Provides Ping, Traceroute, port loopback function

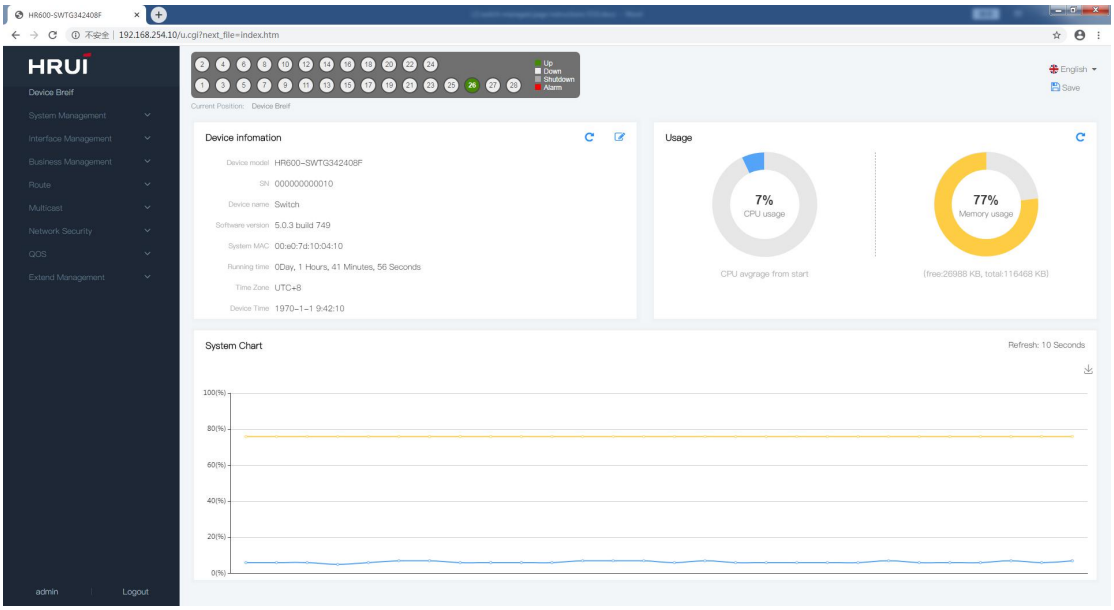
3 Device Breif

Web NMS panel display area according to the connected switch, can be very intuitive display information and product information of each port of this switch on the front panel, the display includes:

Number of ports, each port working status, product information, device status

Steps:

Click the navigation bar "Device Breif" menu, enter the " Device Breif" interface. It is shown as below.



✍ **illustrate：**

Place the cursor on a port, click the left mouse button, there will display port number, type, speed, and status information.

You can modify the "Device Name", "Device Time", click "Save" to complete the configuration.

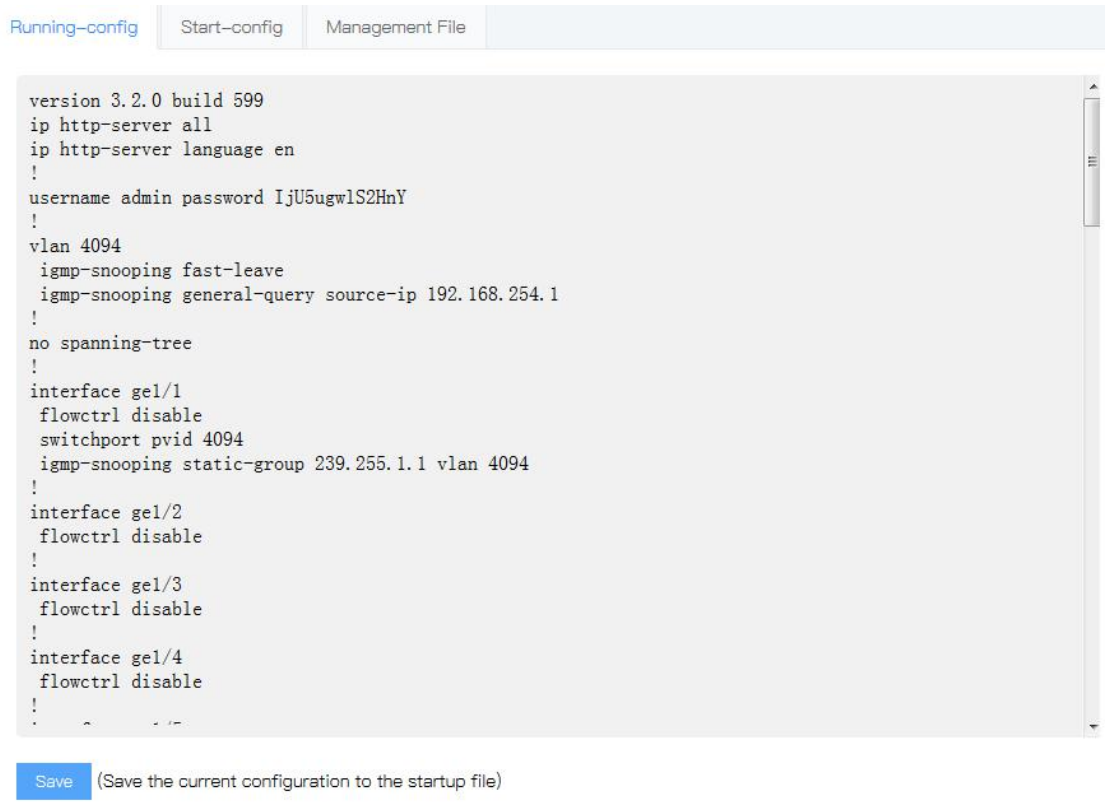
---

4 System Management

4.1 Config Management

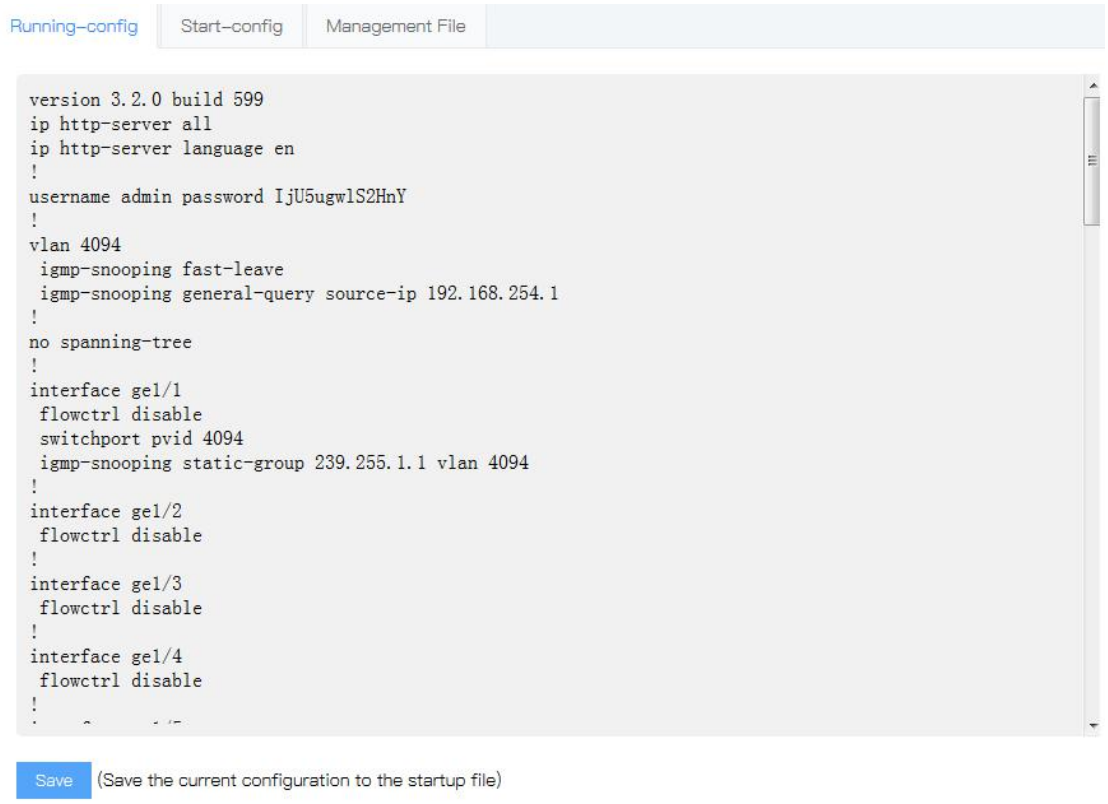
a. See the running-config steps

1.Click the Navigation tree " System Management > Config Management > Running-config" menu, go to " Running-config " screen, as shown below.



b. Save Configuration Steps:

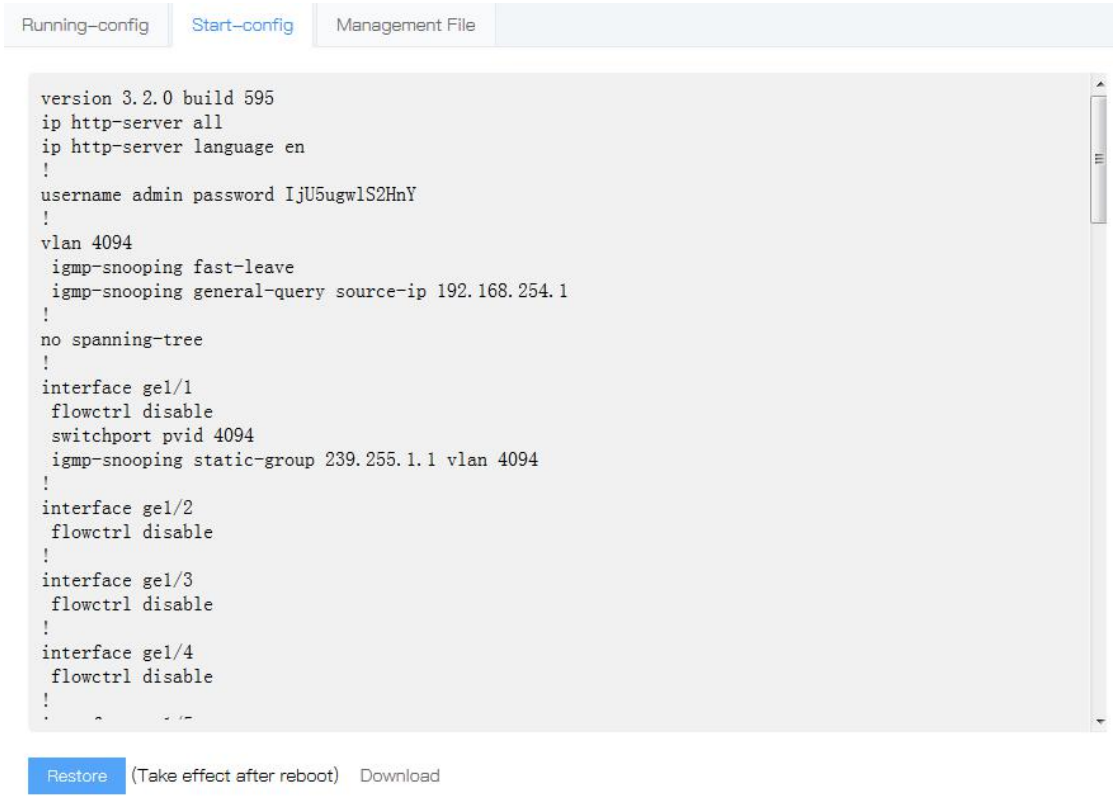
Choose the " System Management > Config Management > Running-config " menu, go to " Running-config " screen, click "Save ", as shown below.



C. See the startup configuration steps

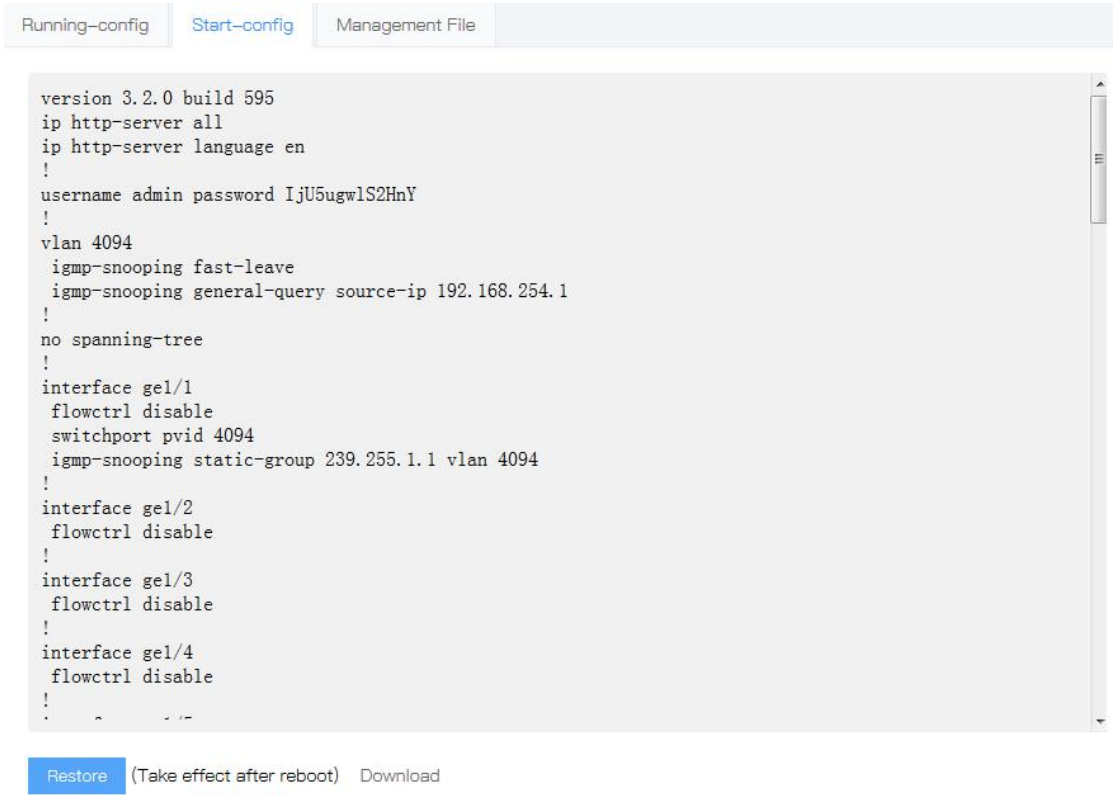
1.Click the Navigation tree " System Management > Config Management >Start-config"

menu, go to " Start-config " screen, as shown below.

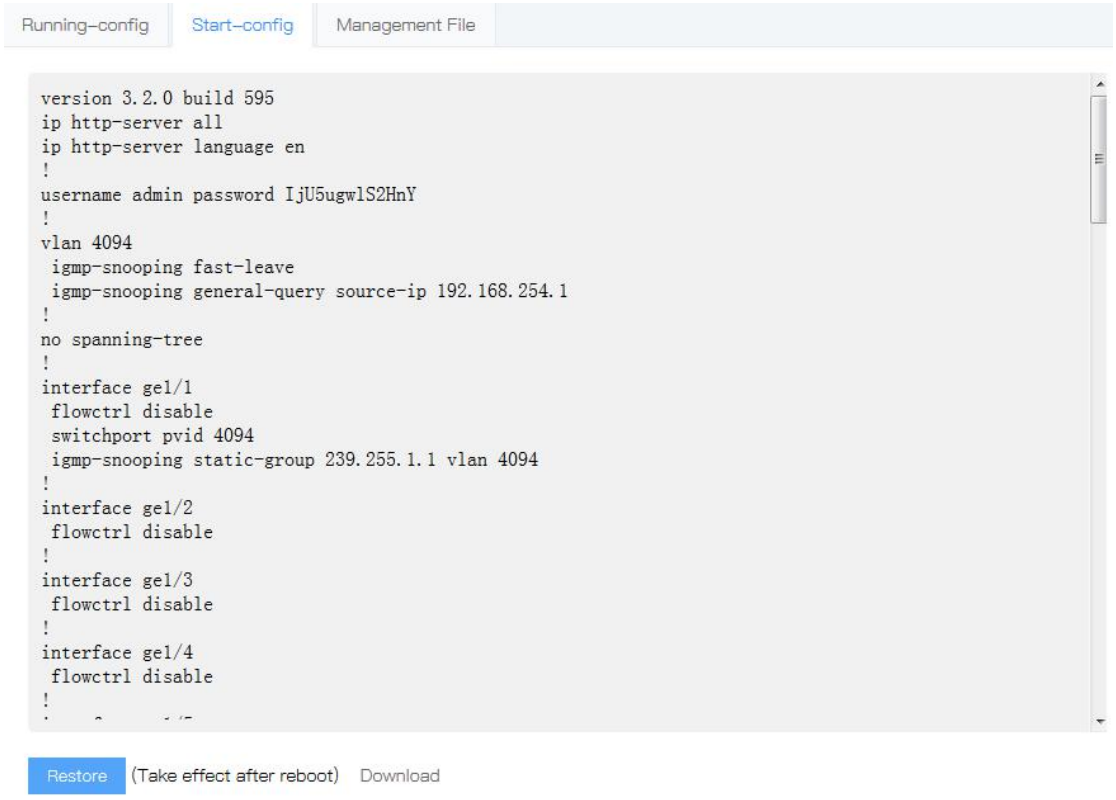


d. Download the configuration file Procedure

Navigation tree " System Management > Config Management > Start-config " menu, go to " Start-config " screen, as shown below.

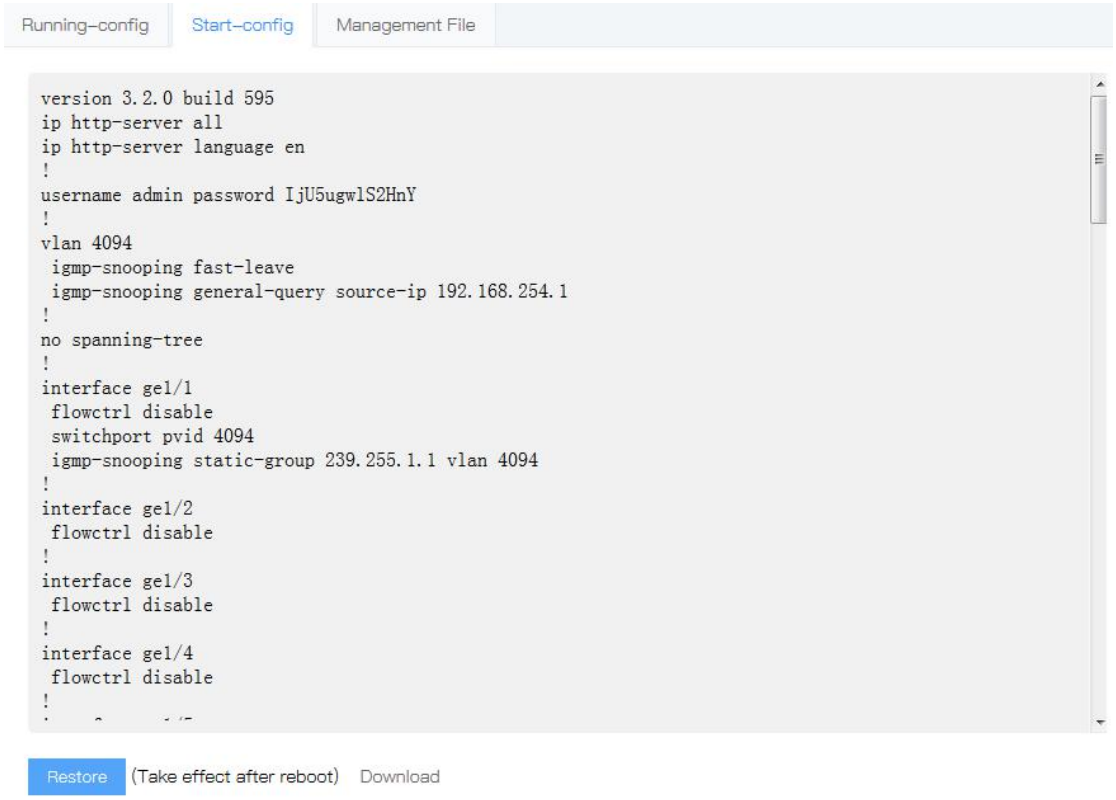


Click on "download", as shown below.



e. Restore factory settings Procedure

Navigation tree " System Management > Config Management > Start-config " menu, go to " Start-config " screen, click "Restore", as shown below.



f. Upload profile Procedure

1.Click Navigation tree " System Management > Config Management > Config Management

" menu, go to " Config Management" screen, click "File path", choose the configuration that has been created, as shown below.

2.Click "Upload" to complete the configuration.

4.2 Reboot

Steps:

1. Choose the " System Management > Reboot " menu, go to "reboot" screen, click "Reboot", as shown below.

4.3 Upgrade Software

Steps:

1.Click Navigation tree "System Management > Upgrade Software" menu, go to " Upgrade Software " interface, click the "Upgrade file path", click "Upload" to complete the configuration. As shown below.

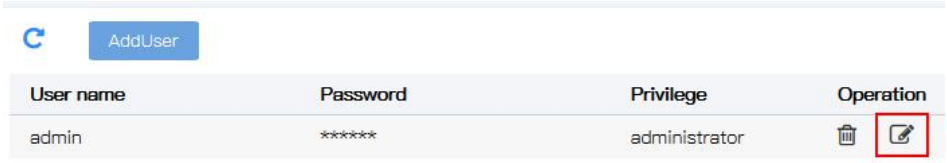
4.4 User

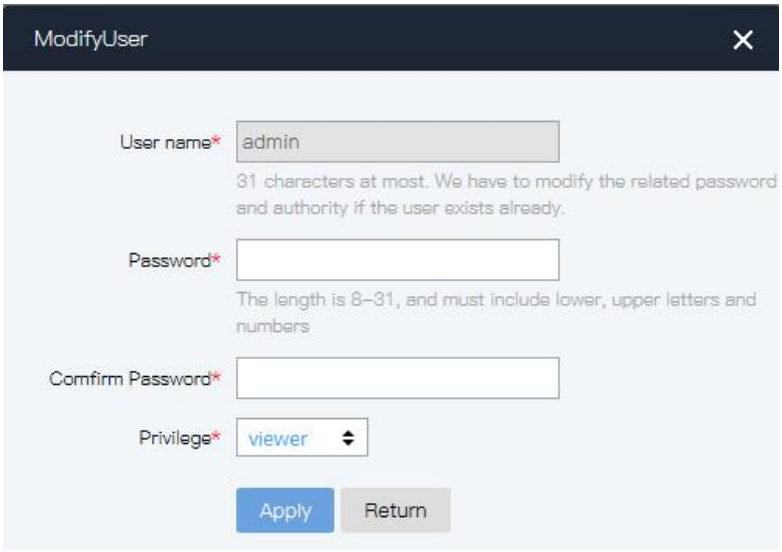
Users can view and modify the switch's user name, password and permission.

Steps:

1.Click the navigation bar " System Management > User " menu, enter " User " screen. Click "Modify", you can see the default user name: admin, password: admin, permissions:

15. It's shown as below.



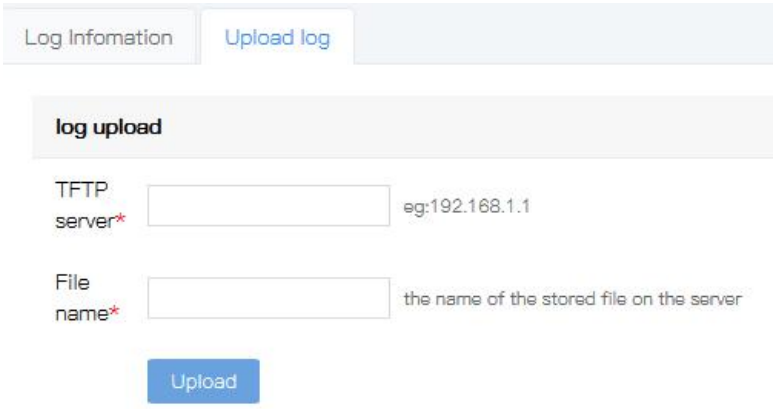


4.5 Log

Switch diary can be uploaded to the FTP server.

Steps:

Click the navigation bar "System Management > Log > Upload log" menu, enter " Upload log ", input the TFTP server address: "192.168.254.253", the file name, "diary", click "Upload", It's shown as below.



4.6 Telnet Config

The user can enable the telnet service.

Steps:

Click the navigation bar "System Management > Access" menu, enter "Telnet" page, select "Enable", the default port number "23", click "Apply", It's shown as below.

4.7 SSH Config

The user can enable the telnet service.

Steps:

Click the navigation bar "System Management > Access" menu, enter "SSH" page, select " Enable ", the default port number "22", click "Apply", It's shown as below.

4.8 HTTP&HTTPS Config

Users can modify the port number, turn off HTTP and HTTPS service.

Steps:

1.Click the navigation bar " System Management > Access " menu, enter "Access", the user can see the system default configuration, It's shown as below.

✍ **illustrate：**

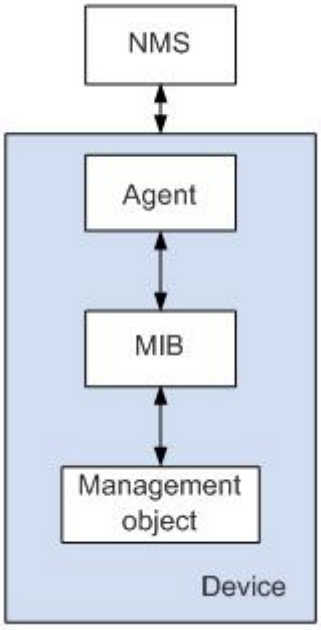
When the port is changed to 8081, Logging in to the switch again, should input the IP address plus port number, so input on web: http://192.168.254.1:8081

3. When Closing HTTP and HTTPS services, you can cancel "check", click "Apply". It's shown as below.

4.9 SNMP

SNMP (Simple Network Management Protocol) is a widely used network management standard protocol TCP / IP network. SNMP provides a method to manage the device through the center of the computer running network management software (ie network management workstation) method. SNMP features are as follows:
Simple: SNMP adopts the polling mechanism and provides the basic feature set, suitable for small, fast, low-cost environment, and SNMP UDP packets to carry, which is supported by the vast majority of devices. Powerful: SNMP goal is to ensure the transfer of management information between any two points in order to retrieve information administrator any node on the network, make changes, and troubleshooting. SNMP protocol used widely mainly in three versions, namely SNMPv1, SNMPv2c and SNMPv3. SNMP system includes a network management system NMS (Network Management System), agent process Agent, four components managed objects Management object and MIB MIB (Management Information Base).
NMS network management as the center of the entire network, the device management. Each managed device contains Agent program on the device, MIB and a plurality of managed objects. By interacting with the NMS Agent running on the managed device by the end of the device through the Agent MIB operation to complete NMS instructions.

SNMP Management Model



NMS

- NMS managers play a role in the network, using SNMP is a protocol for network equipment management / monitoring systems, running on the NMS server. NMS can send a request to the Agent on the device, query or modify one or more of the specific parameter values. NMS can receive information Trap Agent on the active device sent to learn the current status of the managed devices.

Agent

- Agent is a management proxy process equipment for maintenance of the managed devices data and information in response to requests from the NMS to report to management data transmission request NMS. Agent after receiving a request for information on NMS, after completion of the corresponding instruction through the MIB table, and the result of the operation in response to the NMS. When equipment failure or other event occurs, the device sends information to the Agent by NMS, NMS report to the current state of the device changes.

Management object

- Management object refers to the managed object. Each device may include a plurality of managed objects, the managed object can be a hardware device (such as an interface board), it can also be a collection of some of the hardware, software (such as routing protocol) and configuration parameters.

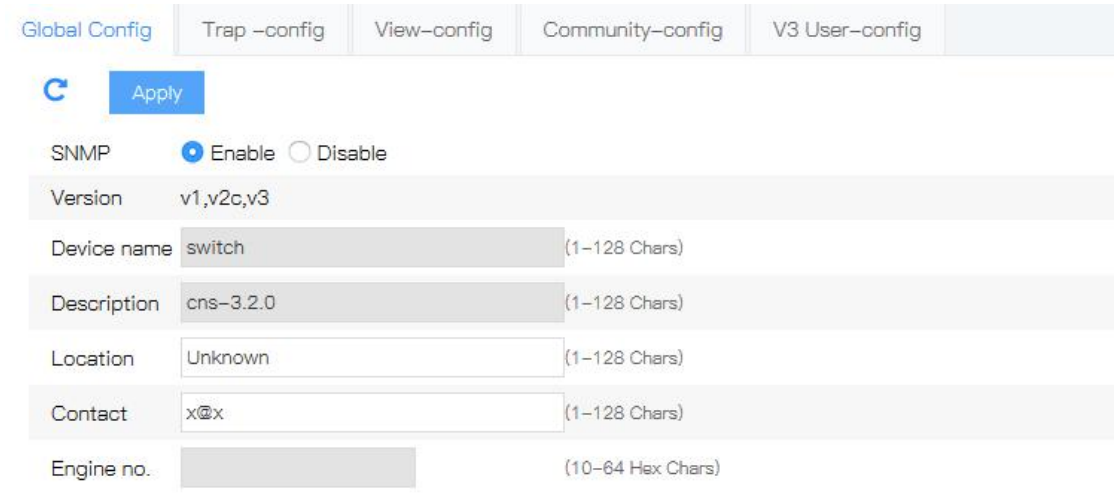
MIB

- MIB is a database that indicates the managed devices maintained variable (ie, capable of being Agent query and set information). MIB defines the managed device is a series of attributes in the database: name of the object, the state of the object, and the object access object data types. By MIB, you can perform the following functions: Agent by querying the MIB, the device can be informed of the current status information. Agent by modifying the MIB, you can set the parameters of the device status.

a. Users can set the basic management information and select the desired switch to crawl trap event.

Steps:

1.Click the navigation tree " System Management > SNMP > Global Config" menu, enter " Global Config " screen, as shown below.



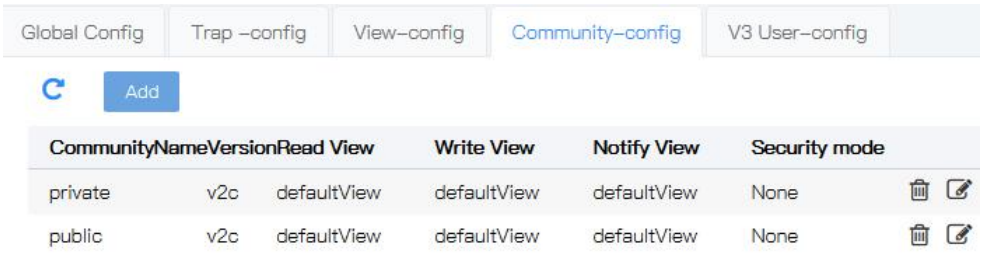
Interface information meaning as followings

Config Item	Sub-Config	Description
Global Config	Model	Optional, enable or disable
	Version	Not Optional, The device Support 3 kind of version by default,SNMPv1、SNMPv2c 和 SNMPv3
Community-config	Read / write area	Not Optional, the device Default supporting used in completing the certification between the Agent and NMS, character string, the user can defining. The group name includes "readable" and "writable", the implementation of “GetRequest, GetNextReques”t operation, use "public" for certification; the implementation of “Set” operation, use "private" for certification. Assuming that NMS wants to get the value of device being managed MIB node sysContact, use a readable group named public. Assuming that NMS wants to get the next node sysName value of device being managed MIB node sysContact, use the readable group named public Assuming that NMS wants to set the value of device being managed MIB node

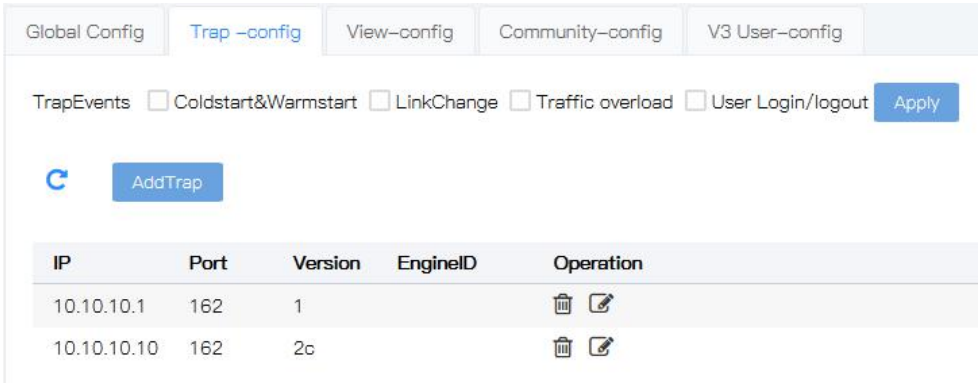
		sysName to Hong, use the writable group named private
Trap Config	TrapEvents	Optional, report event messages to NMS
	IP	Required, set Trap destination host address
	Port	Required, set Setting the Receive Port Number of Trap Target Host, default is 162
	Version	Required, report Trap message version number, support V1 and V2C
User's config	Read user	Set reading user, security grade is needing certificate and encryption, specifying the authentication protocol MD5 and SHA, specify the encryption protocol as AES and DES
	Write user	Set writing user, security grade is needing certificate and encryption, specifying the authentication protocol MD5 and SHA, specify the encryption protocol as AES and DES

2.Fill in the appropriate configuration items.
3.Click "Apply" to complete the configuration.
For example: NMS and SwitchA connected by Ethernet, NMS IP address is 10.10.10.1,configure Switch A:set group name and access right, administrator signs, contact and location information of switch, allow switch send Trap message to make NMS get access right to switch, and receive Trap message sent by switch.

Steps:
1.Enable SNMP Agent service and set SNMP V1, V2, V3 version's group name. Click the navigation tree " System Management > SNMP > Community-config" menu, enter " Community-config " interface, as shown below.



2.Allow the switch to send traps message to the network management station 10.10.10.1, click the" System Management > SNMP > Trap -config" menu enter the" Trap -config" interface. Input 10.10.10.1in the Trapv1 Receiver, input 10.10.10.10 in "Trapv1 receiver", as shown below.

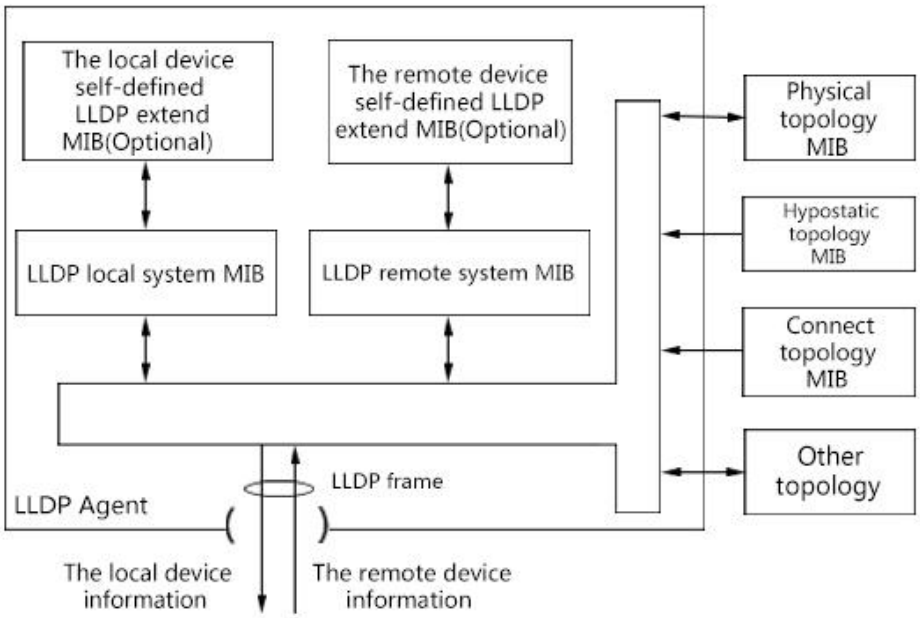


4.10 LLDP

LLDP (Link Layer Discovery Protocol) is defined in IEEE 802.1ab Link Layer Discovery Protocol. LLDP is a standard Layer find a way, you can manage the address, device ID, the interface identification information such as the local device to organize and distribute it to their neighbors equipment, after its neighbor device to receive this information in a standard save MIB (Management Information Base) form up for NMS queries and determining that the communications link status.

LLDP information may be a local device to organize and publish to their remote device, the remote device information received from the local device will be saved in the form of a standard MIB. It works as shown below.

LLDP schematic diagram



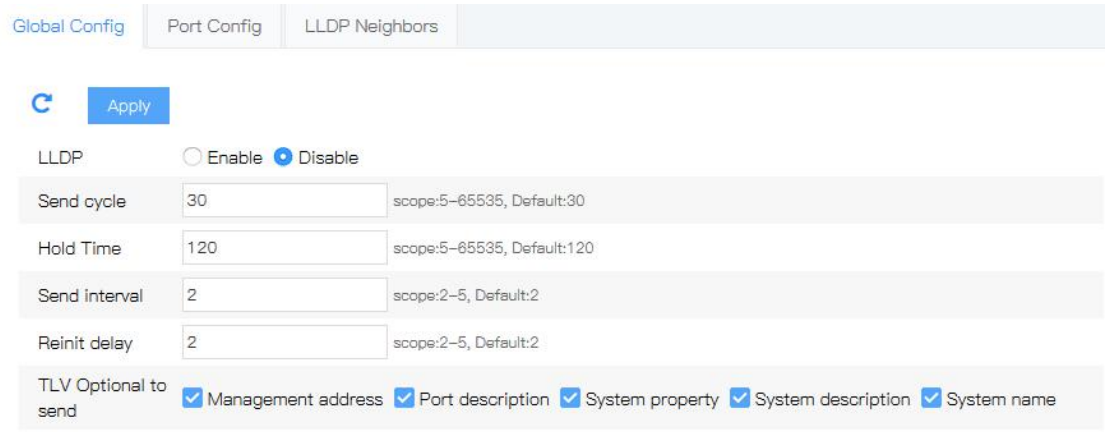
LLDP basic principle is:

- LLDP module LLDP agent on the physical topology and device interfaces MIB entities interact, as well as other types of MIB to update their local system MIB LLDP and LLDP MIB extensions local custom equipment.
- Encapsulated information into the local device LLDP frames are sent to the remote device.
- Receiving remote device sent from the LLDP frames to update their LLDP remote system MIB, as well as remote device custom extensions LLDP MIB.
- LLDP frame, it is clear that the device LLDP agent transmits and receives information via a remote device, including the connection of the interface, MAC address which the remote device remote device information.
- LLDP local system MIB is used to save a local device information. Including the device ID, port ID, system name, system description, interface description, address and other network management information.
- LLDP remote system MIB information used to save the remote device. Including the device ID, port ID, system name, system description, interface description, address and other network management information.

4.10.1 LLDP Global Config

Steps:

1.Click the navigation tree " System Management > LLDP > Global Config" menu, enter the "Global Config" screen, as shown below.



Interface information meaning as followings.

Config item	Description
LLDP	Radio. Enable or disable the UDP protocol
Hold time	120 seconds by Default, Scope: 5-65535s
Send interval	2 seconds by Default, Scope: 2-5s
Reinit delay	2 seconds by Default, Scope: 2-5s
TLV optional to send	Management address, port description, system properties, system description, system name

Encapsulated LLDP data unit LLDP DU (LLDP Data Unit) Ethernet packets called LLDP packets. TLV is LLDPDU units, each represents a TLV information.

2.Fill in the appropriate configuration items.

3.Click "Apply" to complete the configuration.

4.10.2 Port configuration

Steps

1. Choose the " System Management > LLDP > Port" menu, enter the "Port" screen, as shown below.

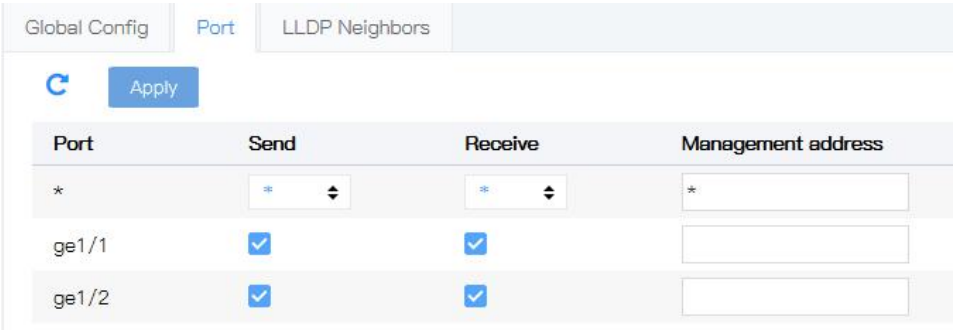
Interface information meaning as followings

Config item	Description
port	Support for configuring multiple ports
Send	Send LLDP
Receive	Received LLDP

Management address	Enter the IP address of the local switch. Such as 192.168.1.254

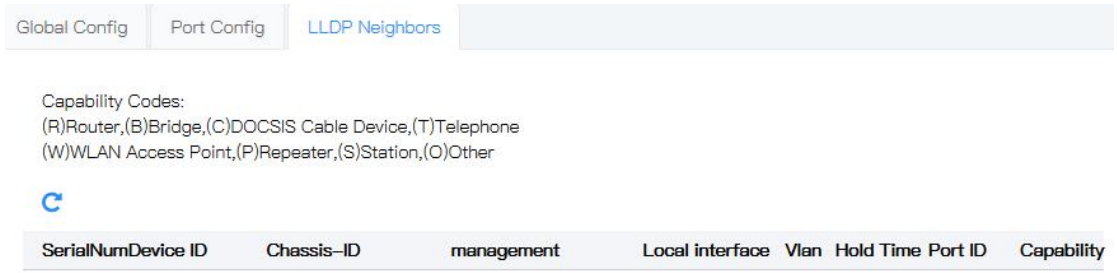
LLDP There are two modes of operation. Tx Rx: can send and receive LLDP packets. Disable: not send or receive LLDP s.

2. Configuration can send and receive LLDP packets, click the navigation tree " System Management > LLDP > Port " menu, enter the "Port" interface, ge1 / 1 tick the "send", "receive", enter this IP address of the end of the switch, such as 192.168.1.254. Click "Apply" to complete the configuration, as shown below.



4.10.3 LLDP Neighbors

LLDP neighbor displayed Procedure
Click the navigation tree " Business Manage> LLDP Config> LLDP Neighbor" menu, enter "LLDP Neighbor" screen, as shown below.



5 Interface Management

5.1 Port Management

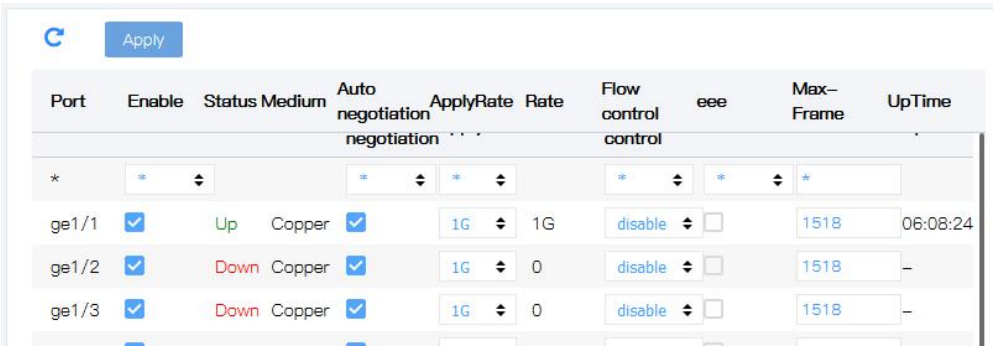
For easier identification port, configure port's marked description information. Users can query and configure the Ethernet interface as needed.

Steps:

1.Click the navigation bar "Interface Management > Port Management " enter " Port Management " interface.

2.Select the desired configuration data, select configurable items "Auto-negotiation",

"Flow control", "maximum frame ", as shown below.



Configurable items meaning as below

Configurable items	**Description**
Auto-negotiation	Can be configured to auto-negotiation, forced10M,forced Fast, forced Gigabit, Gigabit Ethernet interfaces support 10Mbits / s, 100Mbits / s, 1000Mbit / s three rates, you can select the appropriate interface rate as required.
Flow Control	When the local and remote devices are turned on flow control, congestion occurs if the local device, it will send a message to the remote device to notify the remote device to temporarily stop sending packets; and the peer device receiving the message to this end will temporarily stop sending packets to avoid packet loss occurrence Disable - Disable PAUSE frame receipt and transmission rx (Rx PAUSE) - is enabled to receive PAUSE frames both (Rx / Tx PAUSE) - is enabled to receive and transmit PAUSE frames tx (Tx PAUSE) - PAUSE frame transmission is enabled
The maximum frame	Support Max9216
Enabled	Port can be turned on and off

Attention

This switch chip don’t support forced 1G pattern

5.2 L3 interface

Supported interface types:

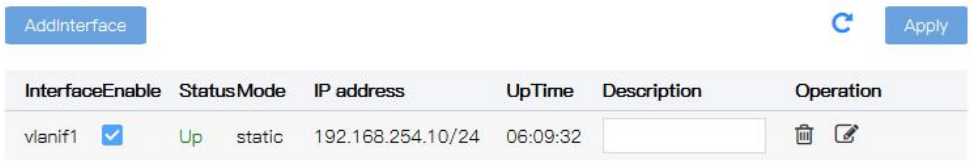
Supports interfaces: logical interface. Logical interface is an interface that does not exist corresponding to a physical device and is created manually by the user.

Currently, the logical interfaces supported by UNOS including:

- Loopback interface
- Empty interface
- Aggregate interface
- VLAN interface

Add the VLAN interface step

1. Click the navigation tree “Interface Management > L3 interface “menu. Interface is shown below



2.Click “Add”.

📖 illustrate:

The interface name needs to be created first.

5.3 Link-aggregation

5.3.1 Link-aggregation

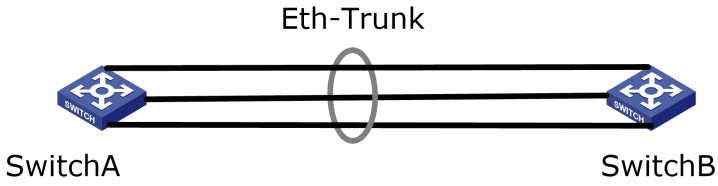
Port Channel Config is method of binding a group of physical interfaces as a logical interface to increase the bandwidth and reliability. Link aggregation group (LAG) refers to logical link formed by multiple Ethernet links binding, abbreviated as Eth-Trunk. As networks have been expanding, the users have more and more high requirement to linking bandwidth and reliability. Under the conventional technique, commonly replace the high-rate interface board or replace device supporting the high-rate interface board to increase bandwidth, but this solution needs to pay the high costs and is inflexible.

Link aggregation technology under no hardware upgrades condition

combine multiple physical interfaces together as a logical interface to achieve the purpose of increasing the link bandwidth. Link Aggregation backup mechanism can effectively improve the reliability, meanwhile, may also be implemented on different physical link load balancing.

Shown as below, Switch A and Switch B are connected through three Ethernet physical links, binding these three links, which becomes a Eth-Trunk logical link. This logical link bandwidth is equal to the sum of original three Ethernet physical link bandwidth, thus achieving the purpose of increasing the link bandwidth; at the same time, the three Ethernet physical links back up each another, effectively improve the reliability of the link.

Link Aggregation schematic:

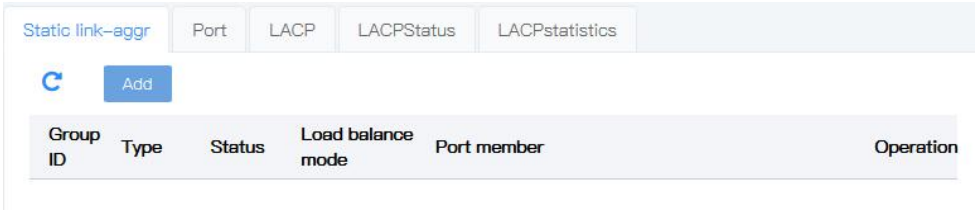


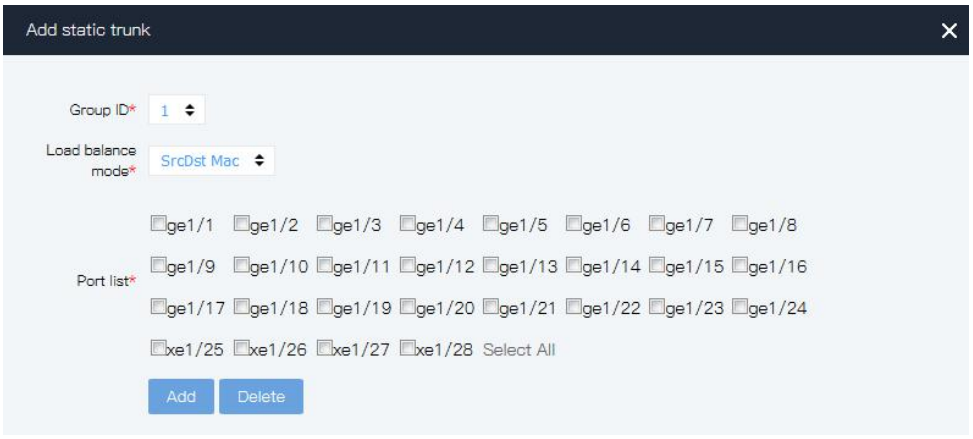
When there is a demand as followings, you can achieve by configure link aggregation
When two switches connected through a link bandwidth is not enough.
When two switches connected through a link reliability does not meet the requirements.
When the bandwidth of two switch devices through a link connection is not enough.
When the reliability of the two switches through a link connection does not meet the requirements.

Depending on whether enable the Link Aggregation Control Protocol LACP, Link aggregation is divided into manual load balance mode and LACP mode.
In manual load sharing mode, the Eth-Trunk establishment and member port participation is made by manual configuration, but LACP is no involvement. In this mode all active links are involved in forwarding data, averagely share traffic, so called load balancing mode.
If an active link fails, the link aggregation group automatically balance the traffic on the remaining active links. When you need to provide a large link bandwidth between two directly connected devices and the device does not support the LACP protocol, you can use the manual load balancing mode.

5.3.2 Add static link aggregation

Adding static link aggregation (ie, manual load sharing mode) Procedure:
Click the navigation bar " Interface Manage> Port channel Config> Static link-aggr" menu, enter "Static link-aggr" interface, select the “Group ID” (1-20), select “load balancing” (Src Mac, Dst Mac, Src & Dst Mac), select the port needed aggregation, click "Add", shown as below.





Port information means as below:

Configuration Item	Description
Group ID	Link aggregation group ID, a total of 1 to 20, 20 aggregation groups
Load balancing	Src Mac (based on the source MAC address for load balancing), Dst Mac (based on the destination MAC address for load balancing), Src & Dst Mac (based on heterologous MAC address and destination MAC address, or load balancing), the default is based on the source MAC address for load balancing
Port list	You can select multiple ports, Max support 8 ports

5.3.3 LACP

Dynamic Link Aggregation

LACP (Link Aggregation Control Protocol) Based IEEE802.3ad standard is a protocol implementation of dynamic link aggregation and unlock-aggregation. LACP protocol and opposite end interact information by LACPDU (Link Aggregation Control Protocol Data Unit)

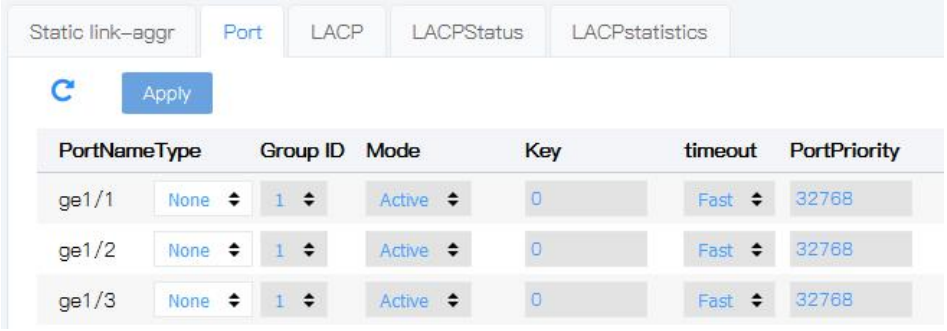
After opening a port LACP protocol, the port will inform opposite end own system priority, system MAC port priority, port number and operation key to by sending LACPDU. After receiving this message,

the opposite end will compare this message with other port stored information and select a port can make link aggregation, so two parties can agree on joining or exiting a dynamic aggregation group.

Dynamic LACP aggregation is an automatically created or deleted aggregation, port adding and deleting in dynamic aggregation group is done automatically by protocol. Only having the same rate and duplex properties, connected to the same device, the same basic configuration port can be dynamically aggregated.

Adding dynamic link aggregation procedure:

1.Click the navigation bar "Interface Management > Link-aggregation > Port" menu, select the port, choose the port type you want to configure (select the “dynamic LACP”), select the ”mode”(Active or Passive),select the “port priority” (range: 0-65535, default: 32768), click "Apply", shown as below:



Interface information means as followings:

Configuration Item	Description
Type	Static and dynamic LACP, Static mode When the need to increase the bandwidth or the reliability of two devices, one device of two devices does not support LACP, creating on a static link aggregation on device, and add multi member interfaces to increase the bandwidth and reliability. Dynamic LACP mode In the dynamic LACP mode links between two devices can implement redundancy backup, replace the faulty link to keep data transmission uninterrupted when a part of a link failure.
Mode	Active (active state), Passive (passive) Passive ports do not automatically send LACP protocol packets; only responds to LACP protocol packets sent by the remote device. Active port automatically sends LACP protocol packets. There are one or two active LACP link ports can be dynamic LACP aggregation. If the two ports connected to each other are passive LACP port, this two will not be dynamic LACP aggregation, because both two ports are waiting for the end device's LACP protocol packets.
Port Priority	When determining the dynamic LACP aggregation group members, LACP will determine according to the superior device ID's priority of end port ID. Device ID consisted by a two-byte system priority and six-byte MAC system, namely the device ID = system priority + system MAC address. When comparing the device ID, the first systematic priority, if it's the same, comparing the system MAC address, smaller value one would be considered excellent. Range: 0-65535 Default: 32768.

✍ **illustrate：**

Before changing Eth-Trunk working mode, the first is make sure that the Eth-Trunk does not add any member port, or cannot modify the Eth-Trunk working mode.

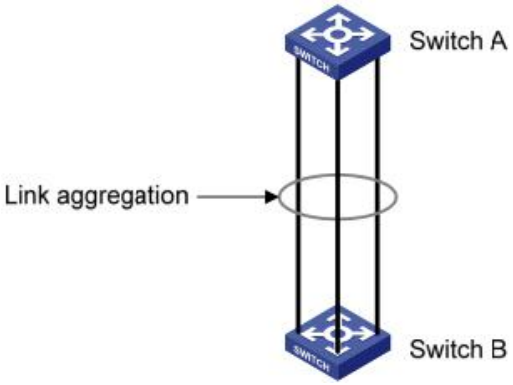
The local and opposite end configuration mode should be consistent.

For example

Ethernet Switch “Switch A” aggregated with three ports (GE1 ~ GE3)

Access Ethernet Switch” Switch B”, to achieve flows load balancing among the member ports.

Here is the dynamic aggregation mode as an example.

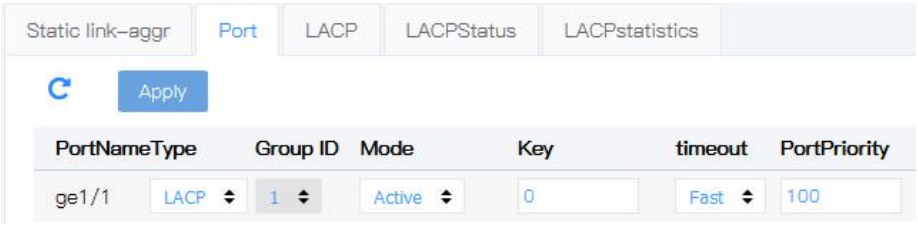


✍ **illustrate:**

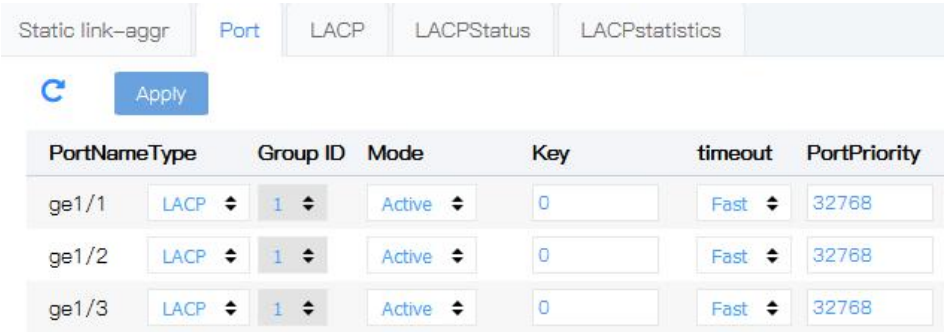
The following just list the configuration on Switch A, Switch B also need to make the same configuration to achieved port aggregation.

Steps:

1. Set the system priority of Switch A to “100”, making it be the active side of LACP .Click the navigation bar " Interface Management > Link-aggregation > Port" menu, enter the " Port”, the LACP is set to "100", click "Apply" to complete the configuration.



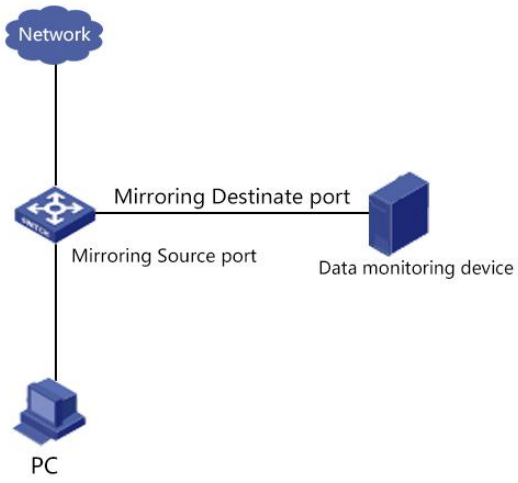
2. Create Eth-Trunk and configure LACP mode on Switch A. Configuring B is similar with configuring Switch A. Click the navigation bar " Interface Management > Link-aggregation > Port" menu, enter the "Port", Select the ports need configured ge1/1, ge1/2,ge1/3,Select the type "Dynamic LACP", select the mode "Active", click "Apply" to complete the configuration .Show as below.



5.4 Mirror

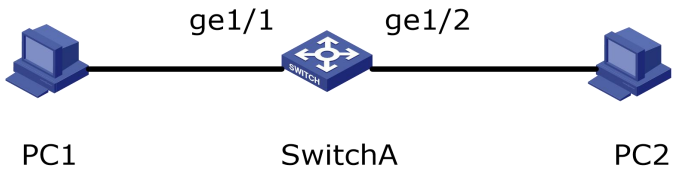
Port mirroring means coping the switch’s specified port packets to the destination port; The

port to be copied is called the source port, and the copied port is called the destination port. Destination port can access data detection device, users use these devices to analyze the destination port received message for network monitoring and troubleshooting, shown as below:



Configuration Example:

PC1 via the port ge1 / 1 access SwitchA. PC2 is directly connected to SwitchA ge1 / 2 port. Users hope that through monitoring devices PC2, monitor PC1 messages sent



Steps：

1.Click the navigation bar " Interface Management > Mirror", enter "Mirror" screen, select the session ID.

2.Select the source port ge1 / 1, select the destination port ge1 / 2, choose the direction" both", click "Add", shown as below.

Interface information means as below:

Configuration Item	Description
Session ID	Switch default have 4 session ID
Source Port	You can select multiple port
Destination port	Can't be a link aggregation port, only select a port as the destination port, the port can't be selected as the source port
Direction	ingress "Mirroring ingress port": that is, any message received on this port are mirrored to the destination port. egress "Mirroring egress port": that is, any messages sent to the port are mirrored to the destination port. both "Access Port Mirroring" the receiving and sending messages of the port are mirrored to the destination port.

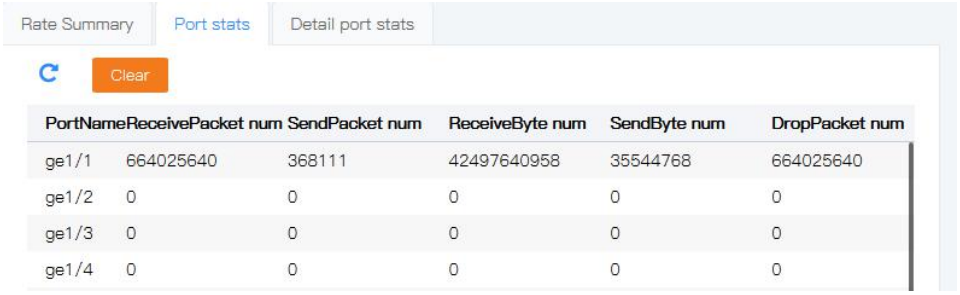
5.5 Port statistics

a. Introduce all interface traffic statistics information in details and the user can manually refresh or clear statistical information.

⚠Notice: After the traffic statistics is cleared, they can't be restored. Please confirm carefully before operation.

Steps:

1.Click the navigation bar " Interface Management > Port statistics > Port Stats" menu, enter " Port Stats ", shown as below.



✍illustrate：

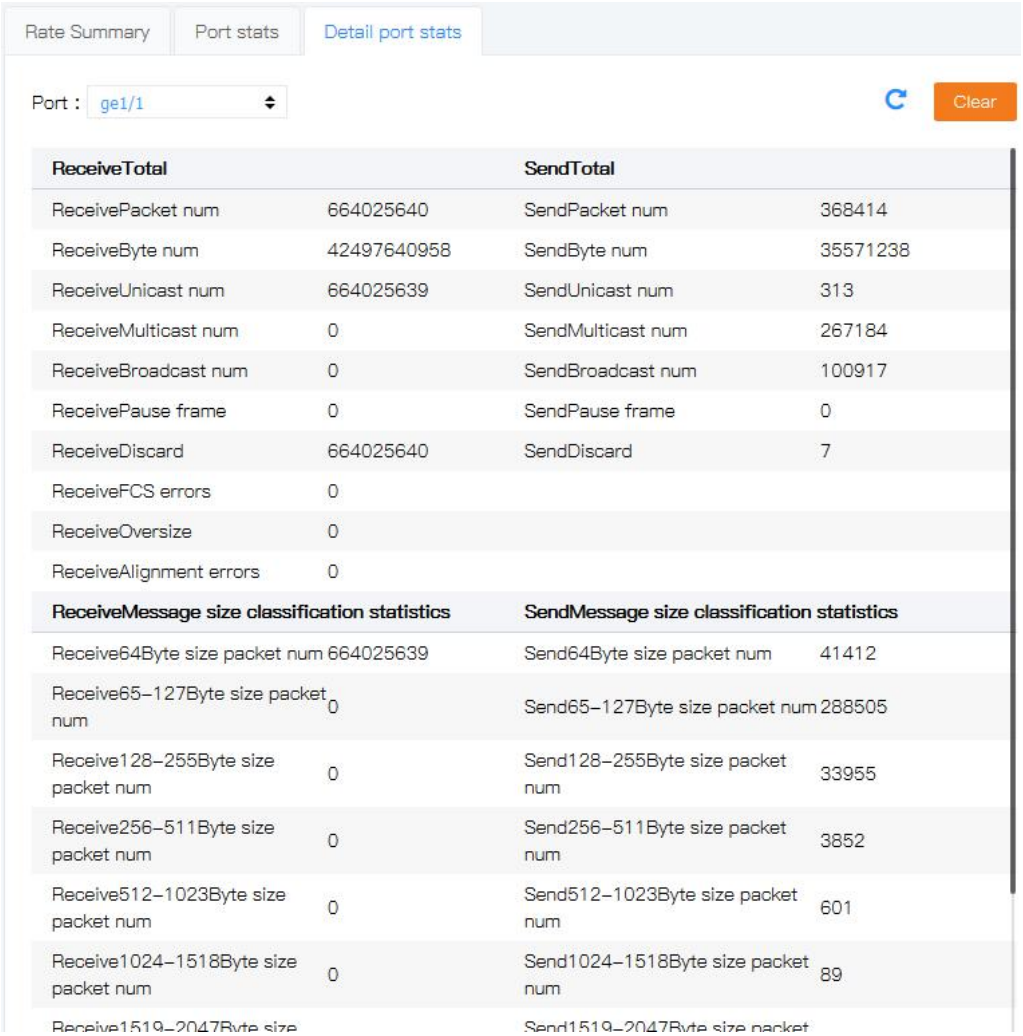
Click "Refresh" the page get the latest traffic statistics.

Click "Clear", traffic statistics of all the ports is cleared, and refresh the page.

---

b. Introduce an interface traffic statistics' detailed information and the user can manually refresh or clear statistical information.

1.Click the navigation bar " Interface Management > Port statistics> Detail Port Stats" menu, Enter " Detail Port Stats ", shown as below:



ReceiveTotal		SendTotal	
ReceivePacket num	664025640	SendPacket num	368414
ReceiveByte num	42497640958	SendByte num	35571238
ReceiveUnicast num	664025639	SendUnicast num	313
ReceiveMulticast num	0	SendMulticast num	267184
ReceiveBroadcast num	0	SendBroadcast num	100917
ReceivePause frame	0	SendPause frame	0
ReceiveDiscard	664025640	SendDiscard	7
ReceiveFCS errors	0		
ReceiveOversize	0		
ReceiveAlignment errors	0		
ReceiveMessage size classification statistics		**SendMessage size classification statistics**	
Receive64Byte size packet num	664025639	Send64Byte size packet num	41412
Receive65–127Byte size packet num	0	Send65–127Byte size packet num	288505
Receive128–255Byte size packet num	0	Send128–255Byte size packet num	33955
Receive256–511Byte size packet num	0	Send256–511Byte size packet num	3852
Receive512–1023Byte size packet num	0	Send512–1023Byte size packet num	601
Receive1024–1518Byte size packet num	0	Send1024–1518Byte size packet num	89
Receive1519–2047Byte size		Send1519–2047Byte size packet	

✍illustrate：

Click the "Refresh" the page get the latest traffic statistics.

Click "Clear", traffic statistics of all the ports is cleared, and refresh the page.

5.6 Bandwidth Chart

Query the interface bandwidth utilization information based on the interface.

Steps:

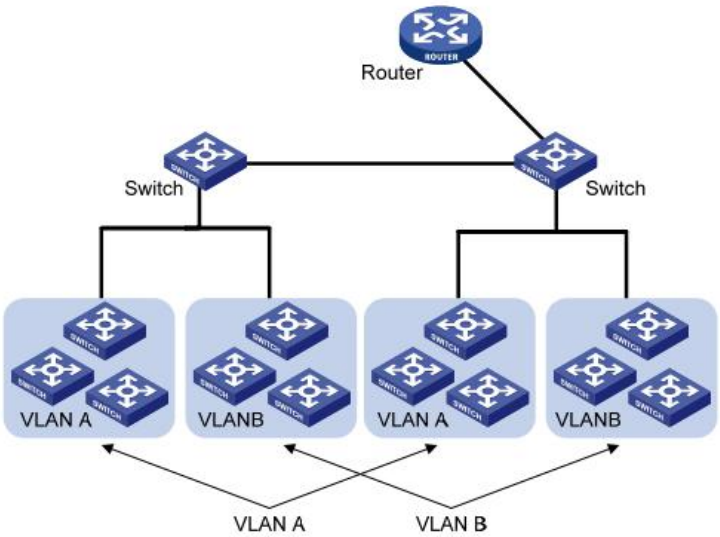
1.Click the navigation bar "Interface Management > Bandwidth Chart ", enter " Bandwidth Chart " interface.

6 Business Management

6.1 VLAN

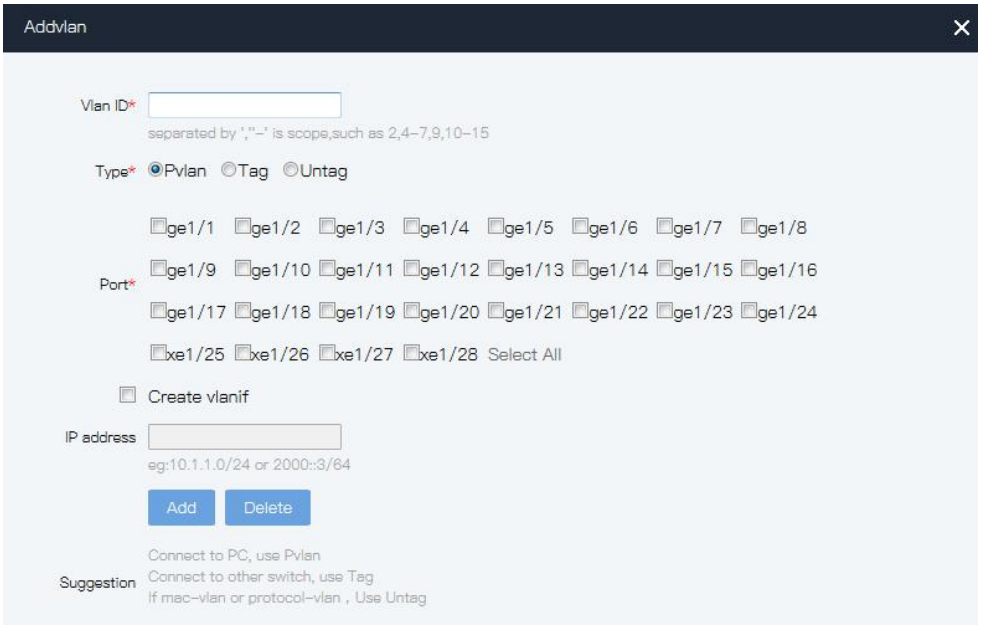
6.1.1 VLAN Configuration

A VLAN is not controlled by physical locations, so hosts in one VLAN no need be placed in the same physical space. As following pic shows, VLAN divides a physical LAN into multiple logical LAN, each VLAN is a broadcast domain. Hosts in a VLAN packets can interact each other through conventional Ethernet communication, while hosts in different VLAN need communication, it must have a router or Layer 3 switch or other network layer devices.



Compared with the traditional Ethernet, VLAN have the following advantages:
Control the broadcast domain range: LAN broadcast message are restricted in one VLAN, reducing bandwidth and improving network performance.
Improving LAN security: As the message is isolated by the broadcast domain divided by VLAN at the data link layer, so the hosts within each VLAN can't communicate directly, need forwarding through a router or Layer 3 switches and other network equipment layer packets Layer 3.
Flexibility to create virtual working groups: using VLAN to create virtual working groups across physical network range, when the physical location of the user moves within the virtual working group range without changing the network configuration that is able to access the network.
The managed switch supports 802.1Q VLAN, protocol-based VLAN, MAC-based VLAN and port-based VLAN. In the default configuration, VLAN is the 802.1Q VLAN mode.
Port-based VLAN, the principle is dividing VLAN based on switching device interface number. The network administrator configures different PVID for each interface of switch, that is VLAN belonged to port default. When a data frame enters the switch interface, if no VLAN tag, and the PVID configured on the interface, then the data frame will be marked with port 's PVID. If the entering frame has a VLAN tag, the switch will not add VLAN tag, even if the interface has been configured PVID.
VLAN frame is determined by the type of interface. The advantage is the simple definition of a member. The disadvantage is moving member need reconfigure VLAN.

a. Create VLAN Procedure
1.Click the navigation tree "Business Management > VLAN > Port-vlan" menu, enter the " Port-vlan "screen, shown as below.

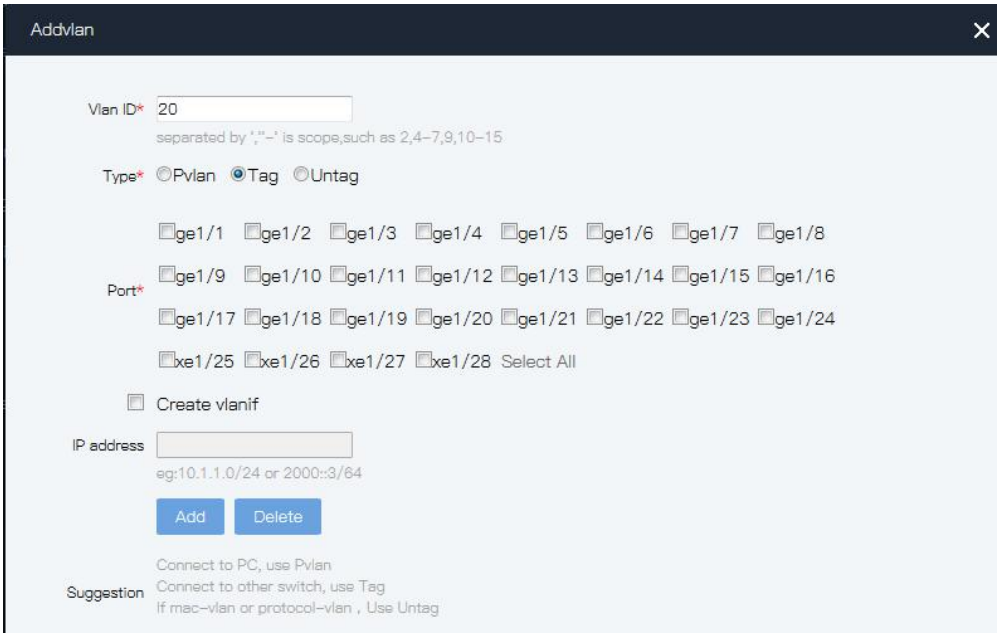


Interface information means as followings:

Configure item	Description
VLAN ID	Must select. Required, Add Vlan ID, range from 1~4094.such as: 1-3,5,7,9. VLAN 1 is the default, not re-create VLAN 1. when creating
Type	Select Pvlan、Tag and Untag according to application scenarios
Port	Port list
Create vlanif	Create a L3 VLAN interface
IP address	Valid when vlanif is selected, it is the IP address of the VLAN three-layer interface

2.Fill in the appropriate configuration items.

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

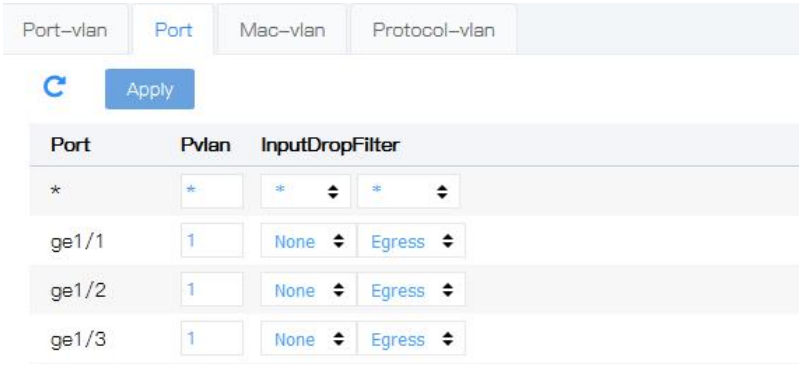


🕮 illustrate：

Configuring VLAN is the way to specify the multicast, there are three ways to deal with, respectively, flooding all, flooding unknown multicast, directly discarded.

b. The current port to the specified VLAN Procedure

1.Click the navigation tree " Business Management > VLAN > Port" menu, enter " Port" interface, show as pic.

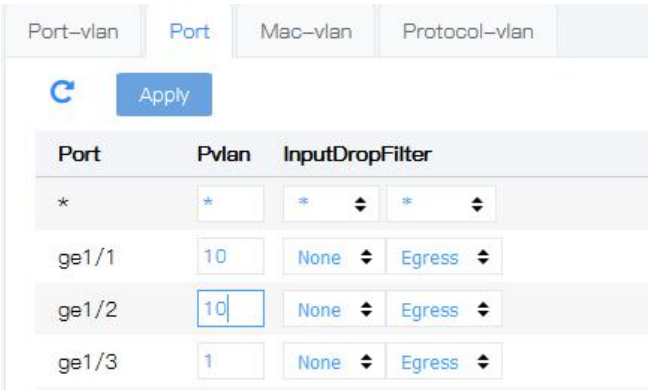


Interface information means as followings.

Config-item	Description
PVLAN	Pvlan for default VLAN, default is 1, also known as Native vlan. Usually set up with the VLAN settings, the port to join the untag vlan. Port receive message discard attribute: none- does not discard; untag-discards without tag message; tag-discards with tag message; all- discards all.

2.Fill in the appropriate configuration items.

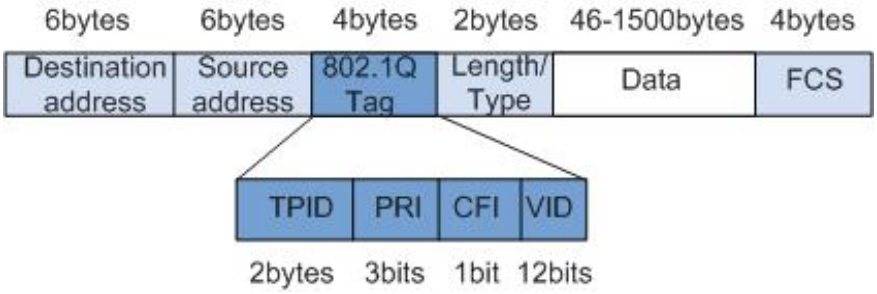
3.Click "Apply" to complete the configuration, show as following pic



c.802.1Q introduction

Trunk configuration, Trunk interface is used to connect other types of switching equipment, it is mainly connected to the trunk link. Trunk interface allows multiple VLAN frames to pass through. Trunk link encapsulation protocol is IEEE 802.1q, IEEE 802.1q is the official standard virtual bridged LAN for Ethernet frame format has been modified between the source MAC address field and the protocol type field is added 4-byte 802.1q Tag

802.1q Frame format

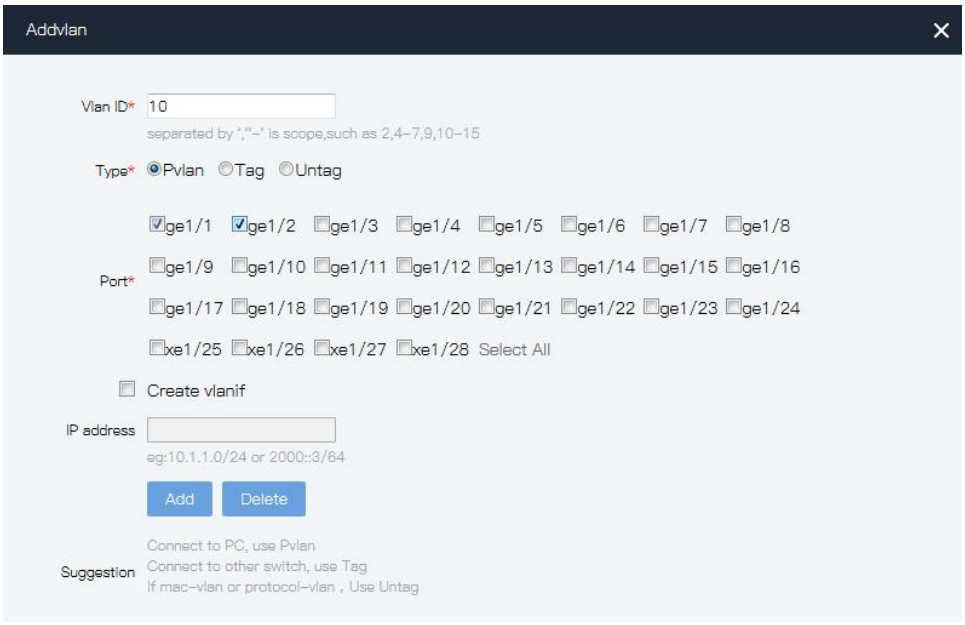


802.1Q Tag meanings

Field	length	Name	Analysis
TPID	2bytes	Tag Protocol Identifier (Tag Protocol Identifier), the frame type.	Value of 0x8100, said 802.1q Tag frames. If the device does not support 802.1q receives such a frame will be discarded.
PRI	3bits	Priority, it indicates the priority of the frame.	In the range of 0 to 7. The higher the value, the greater the priority. When the switch for blocking, the high priority transmission priority of the data frame.
CFI	1bit	Canonical Format Indicator (Standard format indication bit) indicates whether the MAC address is a classic	CFI is 0 Description classic format; CFI 1 indicates that the non-canonical format. Compatible for Ethernet and Token Ring. In Ethernet, CFI

		format.	is 0.
VID	12bits	VLAN ID, it indicates that the frame VLAN belongs to.	VLAN ID ranges from 0 to 4095. 0 and 4,095 for the agreement to retain value, so the range of valid VLAN ID is 1 to 4094.

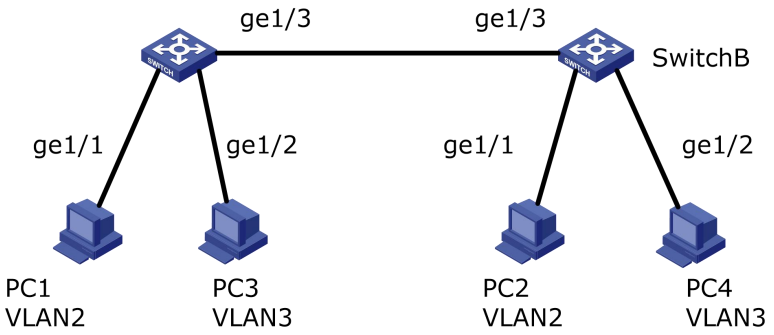
Each switch supports 802.1q protocol packets sent will include VLAN ID, to indicate the switch belongs to which VLAN. Thus, in one VLAN switching network, the Ethernet frame has two forms:
tagged frame: Join the 4-byte 802.1q Tag frames
untagged frame: Original, without adding 4-byte 802.1q Tag frames
Trunk interface is used to connect to other types of switching equipment, it is mainly connected to the trunk link. Trunk interface allows multiple VLAN frames to pass through.
d. Trunk port configuration procedure
1.Click the navigation tree " Business Management > VLAN > Port-vlan", switch port default configuration is trunk port configuration. Shown as below.



2.Permitted VLAN pass through Trunk port. Click the navigation tree "Business Management > VLAN > Port-vlan" menu, input VLAN ID of VLAN which is allowed pass through Trunk port, select the appropriate interface among Tag port list, click "add" to complete the configuration

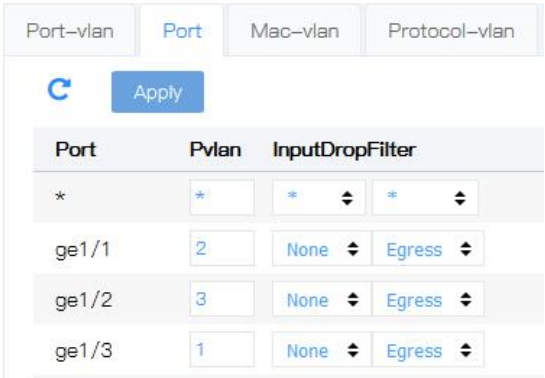
E.g.

To make the link between SwitchA and SwitchB supports both user and support communication within VLAN2 user communication within VLAN3, you need to configure the connection interface while adding two VLAN. That should be configured SwitchA Ethernet interface ge1 / 3 and SwitchB Ethernet interface ge1 / 3 while adding VLAN2 and VLAN3.

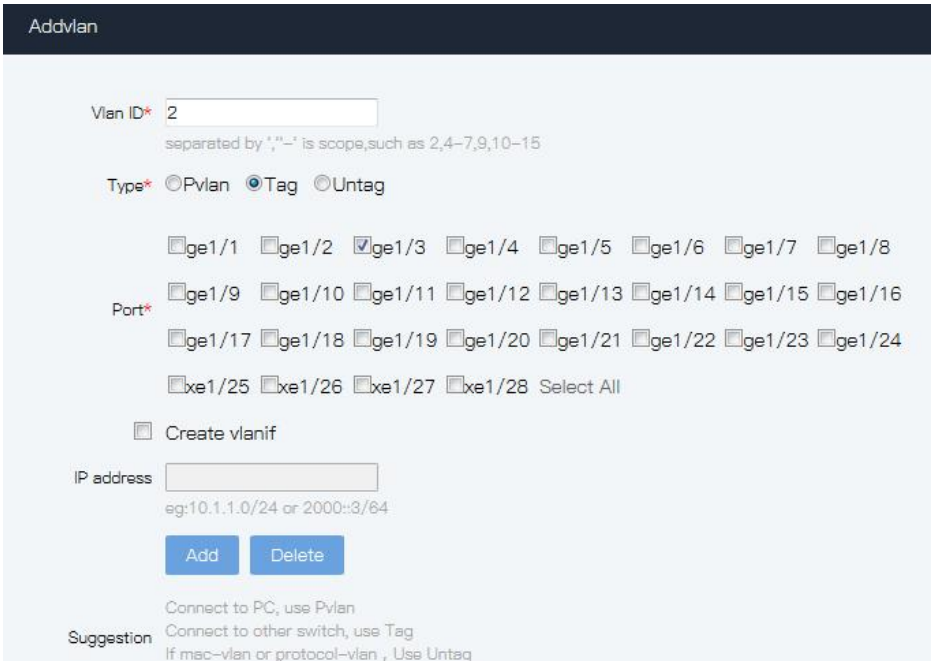


Steps:

1.Create VLAN2 and VLAN3 in SwitchA, and connect the user interface to a VLAN, respectively, will ge1 / 3 is set to trunk mode. Click the navigation tree " Business Manage > VLAN Config> Port Config" menu, enter " Port Config " page, fill in the appropriate configuration items, click the "Apply" to complete the configuration, SwitchB configuration similar to SwitchA, shown as below.



2.Configure types of interfaces on SwitchA and SwitchB connected and VLAN pass. Click the navigation tree "Business Management > VLAN > Port-vlan" menu, enter " Port-vlan " page, fill in the appropriate parameters and click "Add" to complete the configuration, SwitchB configuration similar to SwitchA. The following figure is added through VLAN2 steps, by adding VLAN3 similar to Vlan2.



3.Verify the configuration.

User1 and User2 will be configured in a network, such as 192.168.100.0/24; User4 will User3 and arranged in a network segment, such as 192.168.200.0/24.

User1 and User2 can ping each other, but both fail to ping User3 and User4. User3 and User4 can ping each other, but both fail to ping User1 and User2.

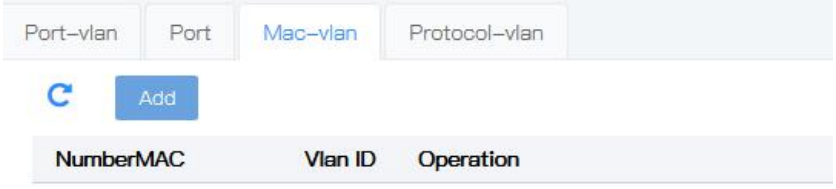
6.1.2 MAC-VLAN

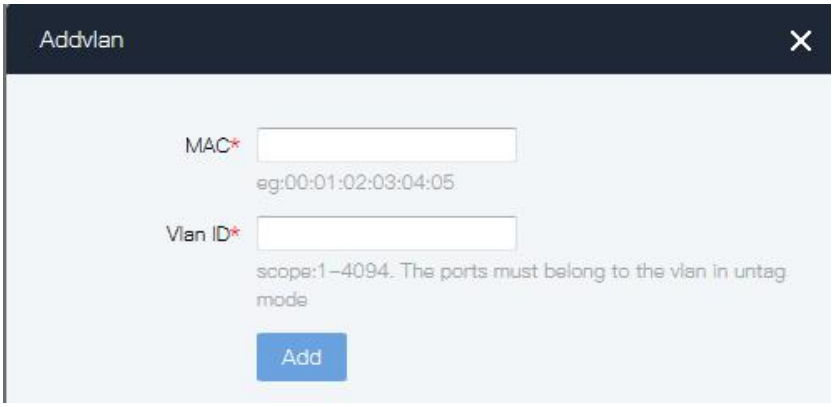
MAC-based VLAN, its principle is based on the computer's MAC address to divide VLAN. Network administrators to successfully configure MAC address and VLAN ID mapping table, if the switch is received untagged (without VLAN tags) frame, according to the table to add VLAN ID.

The advantages are: the physical location of the end user when changes do not need to reconfigure the VLAN. Increase the flexibility of end-user security and access. The disadvantage is: only applicable to the card are not changed frequently, the network environment relatively simple scenario, it is necessary to define in advance all the members of the network.

Steps:

1.Click the navigation tree " Business Management > VLAN > Mac-vlan " menu, enter " Mac-vlan " interface, shown as below.

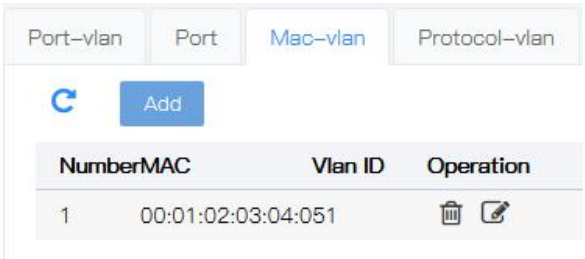




Interface information meaning as followings

configuration	Description
VLAN ID	Required, add VlanID, range from1~4094.such as: 1-3,5,7,9. Where VLAN 1 is the default. Other VLAN must exist and need to un-tag joins link ports.
MAC	Required, input computer's MAC address

2. Fill in the appropriate configuration items.
3. Click "Add" to complete the configuration.

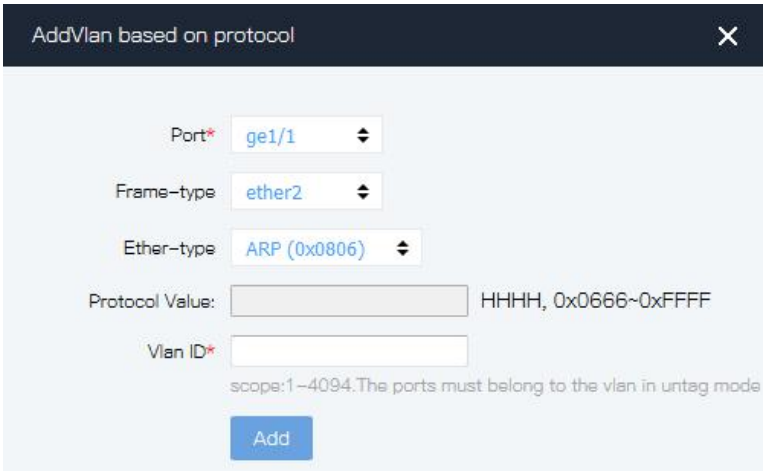


6.1.3 Protocol-vlan

Protocol-based VLAN, the principle is (suite) and encapsulation format packets assign different VLAN ID according to the protocol interface received the packet belongs. Network administrators need to configure the Ethernet frame protocol field mapping table and VLAN ID, and if you receive the untagged (without VLAN tags) frame, according to the table to add VLAN ID. The advantages are: protocol-based VLAN, and VLAN network service type provided in the binding phase, ease of management and maintenance. Disadvantages are: the need for all of the network protocol type mapping table and VLAN ID of the initial configuration. Need to analyze various protocols and the corresponding address format conversion, the switch consumes more resources, slightly inferior speed.

Steps:

1. Choose the " Business Management > VLAN > Protocol-vlan" menu, enter " Protocol-vlan " interface, shown as below.



Interface information meaning as followings

Configuration item	description
ports	Select Port from pull-down menu（ge1/1-ge1/24,xe1/25- xe1/28）
Frame Type	Optional, ether2802.3,snap,lc,snap-priv
Ether-type	Optional, arp, ip, ipv6, 802.1d.1q, 802.1d.1x
Protocol Value	Protocol value
VlanID	Required, add VLAN ID, range from 1~4094,such as 1-3,5,7,9.VLAN 1is default.VLAN must exist and must untag way to join the port to be connected.

2. Fill in the appropriate configuration items.
3.Click "Add" to complete the configuration.

✍ **illustrate:**
Set match protocol IPV4 and IPV6, need to match the settings ARP protocol.

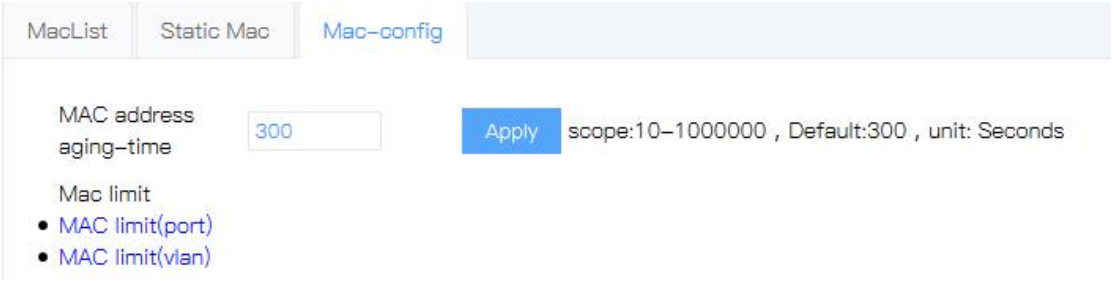
6.2 MAC

The main function of the Ethernet switch is at the data link layer packet forwarding is based on the purpose of the packet
MAC address of the packet to the appropriate output port. MAC address forwarding table contains the MAC address is a forwarding and port forwarding correspondence between the two-story, is the basis of Ethernet switch forwarding packets quickly.
MAC address forwarding table entry contains the following information:

- Destination MAC address
- VLAN ID belonged to the ports
- Forwarding egress port number
- Ethernet switch forwarding packets based on the MAC address table, take the following two forwarding modes:
- Unicast mode: If the MAC address forwarding table contains the destination MAC address corresponding table entry, Switch directly to the packet sent from the entry port to send in turn.
- Broadcast mode: If the switch receives the destination address of the packet to all F, or MAC address forwarding table does not that contains entries for the destination MAC address, the switch broadcasts the packet in addition to access to closing all ports outside the port forwarding.

6.2.1 MAC Configuration

On this page, you can set the MAC address aging time, and view the MAC address table,
In order to adapt to network changes, MAC address table must be constantly updated. MAC address table entries automatically generated are not always valid, each entry has a life cycle, its lifecycle is not updated entries will be deleted and the lifecycle is called the aging time. If the record before reaching the lifetime is refreshed, the aging time of the entry recalculated. Set the appropriate aging time can effectively implement the MAC address aging. The aging time is too short, the switch may lead to a large number of broadcast packets with unknown destination MAC address, affecting performance of the switch.
If the aging time is too long, the switch may retain outdated MAC address entries MAC address table so that the depletion of resources, resulting in the switch forwarding tables can’t be updated according to changes in the network's MAC address.
If the aging time is set too short, the switch may remove valid MAC address entries. This decreases the forwarding efficiency.
In general, we recommend using the default aging time of 300 seconds。
Set the MAC address aging time of Procedure
1.Click the navigation tree "Business Management > MAC Config > MAC-config" menu, enter "MAC-config "interface.



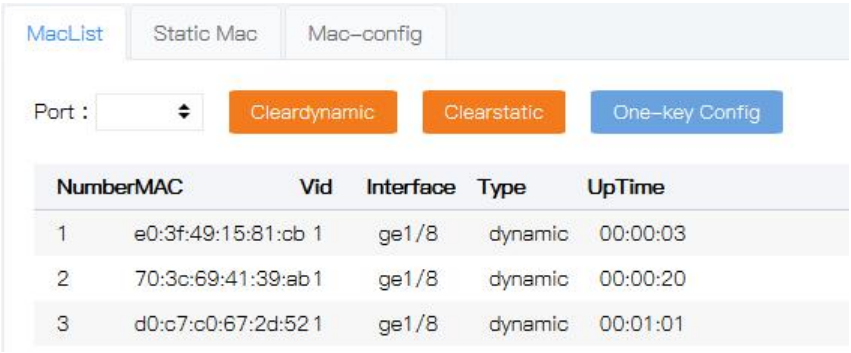
Interface information meaning as followings

Configuration item	Description
MAC aging time	Enter the MAC aging time

2. Fill in the appropriate configuration items.
3.Click "Apply" to complete the configuration.

MAC address table stores the switch learned by other devices, VLAN IDs, and outbound interface information and so on. Before forwarding the data, based on the Ethernet frame destination MAC address and VLAN ID query MAC table for the outbound interface of the device.

Check MAC address table Procedure
1.Click the navigation tree " Business Management > MAC Config > MacList" menu, enter " MacList " interface, shown as below.



Interface information meaning as followings

Item	Description
Number	Sort No.
MAC	Destination MAC address
Vid	VLAN ID port belongs to
Interface	Forwarding egress port number
Type	Dynamic MAC addresses that can be configured by the user according to the aging time and aging out MAC address table, the switch can add dynamic MAC address entry by MAC address learning mechanism or manner established by the user manual.

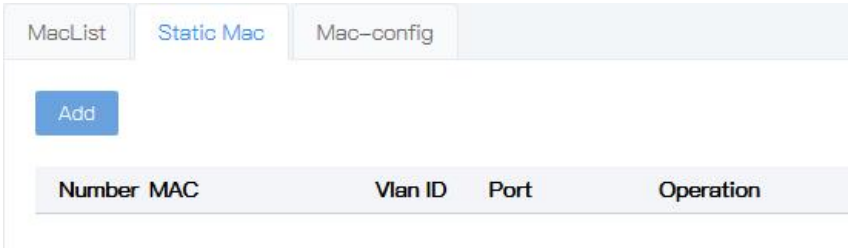
6.2.2 Static state MAC

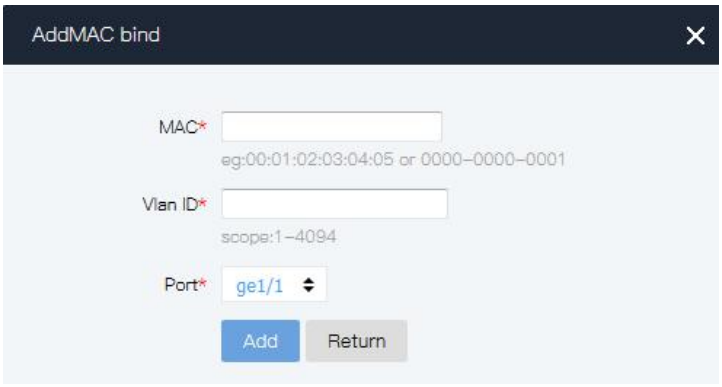
Static entry

manually configured by the user, and delivered to each interface board entries do not age.

Create Static MAC Address Step

1. Click the " Business Management > MAC Config> Static Mac" menu, enter " Static Mac" interface as shown below.





Interface information meaning as followings

Configuration item	Description
MAC	Required, Enter the new MAC address. Such as: H-H-H.
Vlan ID	Required, specified VLAN ID
Port	Required, select the port type and enter the name. such as:ge1/3. Note: The interface must be a member of a VLAN configured port.

2.Fill in the appropriate configuration items.

3.Click "Add" to complete the configuration.

6.3 Spanning-tree

Ethernet switching network to link backup and enhance network reliability, often redundant links. However, the use of redundant links is created on the exchange network loops and broadcast storms caused by MAC address table instability and other symptoms, resulting in poor quality of user communication, even communication interruption. To solve the switched network loop problem, Spanning Tree Protocol STP (Spanning Tree Protocol) developing process like many other protocols, STP evolves as the network constantly updated, STP definition from the original IEEE 802.1D is defined in the IEEE 802.1W Rapid Spanning Tree Protocol RSTP (Rapid Spanning Tree Protocol) , to the latest IEEE 802.1S

defined in the multiple spanning Tree protocol MSTP (multiple spanning Tree protocol). Spanning Tree protocol, MSTP is compatible with STP RSTP, MSTP is compatible with STP. Comparison of Three STP shown in the table.

Comparison of Three Spanning Tree Protocol

Spanning Tree Protocol	specifications	Scenarios
STP	Forming a loop-free tree, broadcast storms and resolve to achieve redundancy. Slow convergence.	Without distinction or user traffic, all VLAN spanning tree.
RSTP	Forming a loop-free tree, broadcast storms and resolve to achieve redundancy. Fast convergence.	
MSTP	Forming a loop-free tree, broadcast storms and resolve to achieve redundancy. Fast convergence. Multiple spanning trees to achieve load balancing among VLAN, VLAN traffic flows to be forwarded along different paths.	We need to distinguish between users or traffic, and load balancing. Different VLAN spanning tree forwarding traffic through different, independent of each other and each of them spanning tree.

After the deployment of Spanning Tree Protocol in Ethernet switching network, if the loop, the spanning tree protocol through a network topology calculation can be realized:

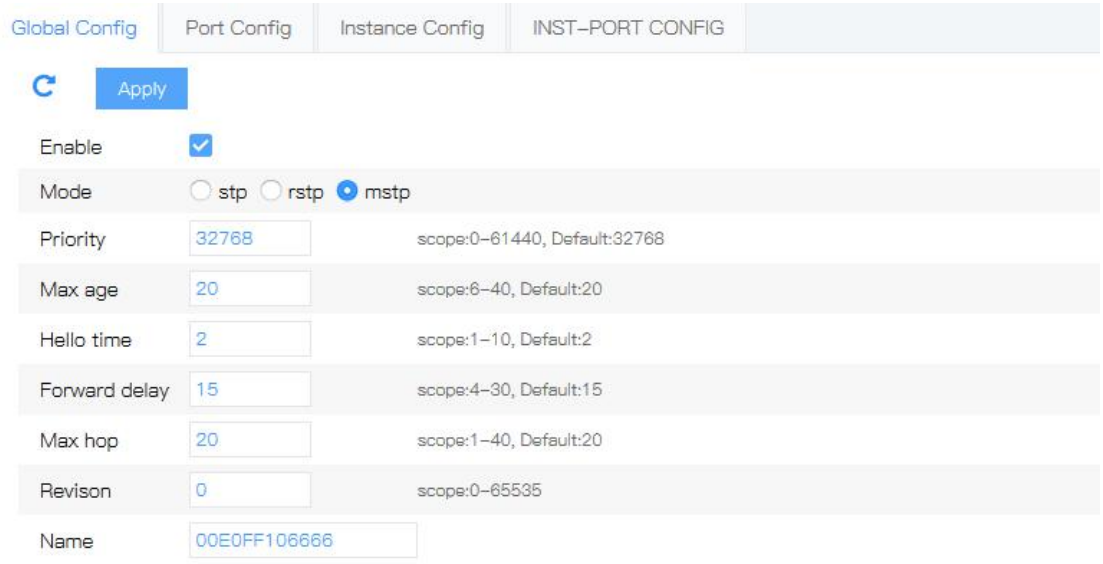
- Eliminate the loop: eliminate possible network communications loop network by blocking redundant links
- Link Backup: when the currently active path fails, the activation link redundancy, restore the network connectivity.

6.3.1 Global Configuration

STP global parameters provide configuration functions in certain networks, you need to adjust the parameters STP portion of the device, in order to achieve the best results.

Steps:

1.Click the navigation tree " Business Management > Spanning-tree > Global Config" menu, enter the " Global Config " screen, shownas below.



Interface information meaning as below

Configuration Item	Description
Start Using Spanning-tree	Ticked by default, assure that the switch start using Spanning-tree
Mode	Support 3 kind of STP mode, that's STP, RSTP and MSTP.
Max age	indicating this message's maximum survival, range for this value is 6-40 seconds, default is 20 seconds.
Hello time	Indicating the periodic of messages sent, Bridge will send "Hello" to intervals around at regular, to check whether any link is faulty, this time named" Hello time
Forward Delay	The port state transition delay, range from 4~30s,15s by default
Max Hops	Choose the Max Hops, range from 1 ~20, 20 by default. The maximum number of hops in an MST region spanning tree used to limit the size of the MST region spanning tree network. Starting from the root bridge of the MST region configuration BPDU passes a switch hop count is decreased by 1; switch discards the hop count is zero configuration message, so that the maximum hop switches that are beyond spanning tree calculation, and thus limits the size of the MST region.
Revision	MSTP revision level. MSTP revision level for the same domain name, VLAN mapping table together determine the MST region the device belongs.
Name	MST domain. The default is the main control

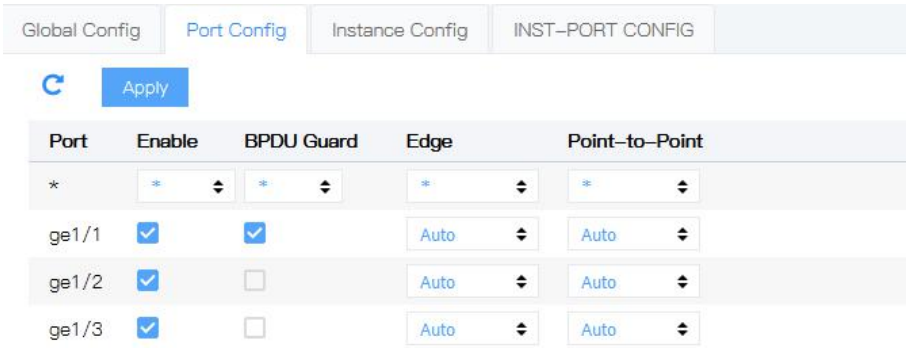
	board switch device MAC address. Switch device used in conjunction with domain VLAN mapping table of MST region, MSTP revision level, determines the switch belongs to which domain.

2. Fill in the appropriate configuration items.
3. Click “Apply”, to complete the configuration.

6.3.2 Port configuration

On certain networks, you need to adjust some parameters STP switch device interface, in order to achieve the best results.

1.Click the navigation tree " Business Management > Spanning-tree > Port" menu, enter the "Port" screen, shown as below.



Interface information meaning as followings.

Configuration Item	Description
Port	Not optional. Port list
Enable	Radio. Choose whether to open the port configuration. Selection and not selection. The default is not selection.
BPDU Guard	Radio. Choose whether to open the BPDU protection function. Selection and not selection. The default is not selection. When BPDU protection is enabled on the device, if the interface received a BPDU, the device will shut down these interfaces, and informs the NMS. Interfaces can only be closed manually by the network administrator.
Edge	Edge port should be connected directly to the user terminal instead of another switch or network segments. Edge ports can rapidly transition to the forwarding state because the edge ports, network topology changes do not produce loops. By setting a port as an edge port, the spanning tree protocol allowing it to quickly transition to forwarding state. It proposed to connect directly to the

	user terminal Ethernet ports configured as an edge port, so that they can quickly transition to forwarding state. Select Force True, Force False and automatic.
Point-to-Point	Select Force True, Force False and automatic。 Automatic State whether the port is set to the default automatic detection point link connected. Force-true The interface is connected point link. Force-false The interface is not connected to point link.

2.Fill in the appropriate configuration items.
3.Click “Apply”, to complete the configuration.

6.3.3 Instance Configuration

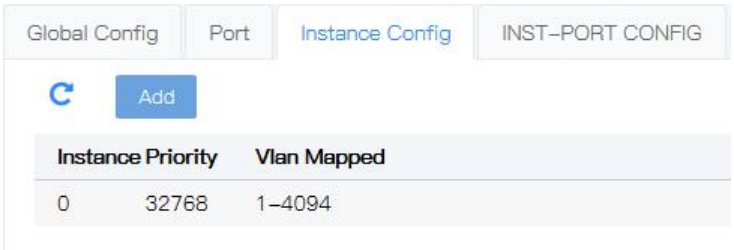
By MSTP divides a switched network into multiple regions, each of which has multiple trees spanning independent of one another. Each spanning tree is called an MSTI MSTI (Multiple Spanning Tree Instance), each region is called an MST region (MST Region: Multiple Spanning Tree Region).

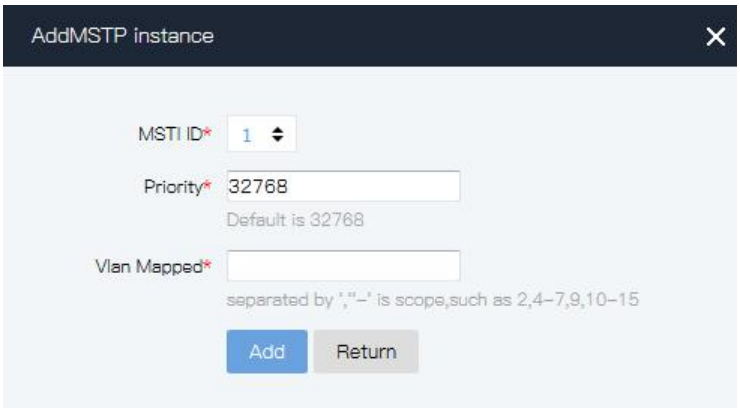
illustrate:

The so-called instance is a collection of multiple VLAN's. By bundling multiple VLAN to an instance, you can save communication overheads and resource usage. MSTP topology each instance calculated independently, in these instances can achieve load balancing. The same VLAN can be mapped to the topology of a plurality of instances, these VLAN forwarding state on a port depends on the port corresponding to the MSTP instance state. Simply put, that is, one or more of the specified VLAN mapping MST instance. One can assign one or more VLAN to a spanning tree instance.

Steps:

1.Click the navigation tree " Business Management > Spanning-tree > Instance Config" menu, enter " Instance Config " interface, shown as below.



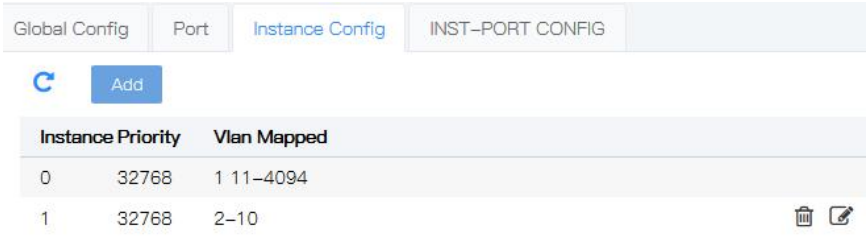


Interface information meaning as followings.

Configuration Item	Description
MSTI ID	Enter any instance number during 1-63.
Priority	Setting specifies the priority of the instance, it must be a multiple of 4096. Its range is 0 to 65535. The default value is 32768.
Vlan Mapped	Enter the desired VLAN mapping

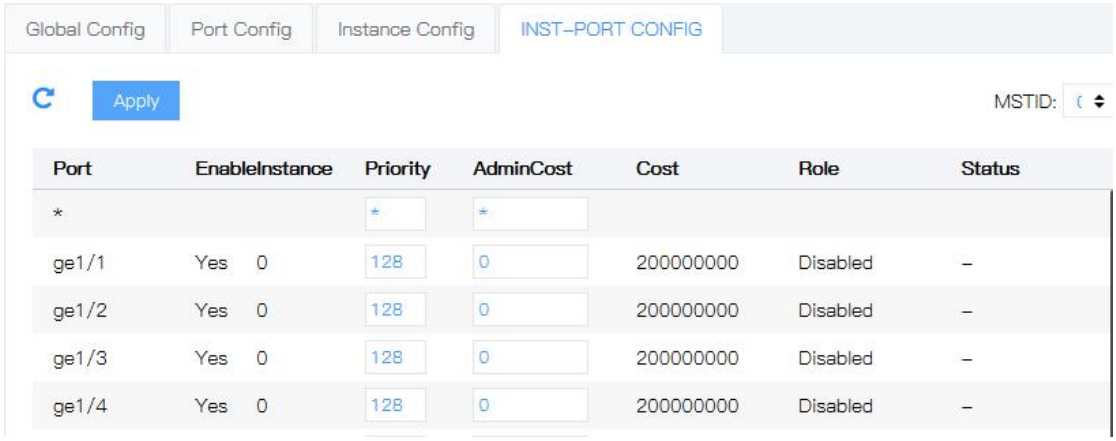
2.Fill in the appropriate configuration items.

3.Click “Apply”, to complete the configuration.



6.3.3 Examples port configuration

1.Click the navigation tree " Business Management > Spanning-tree > INST-PORT CONFIG" menu, enter "INST-PORT CONFIG" screen, shown as below.



Interface information meaning as followings:

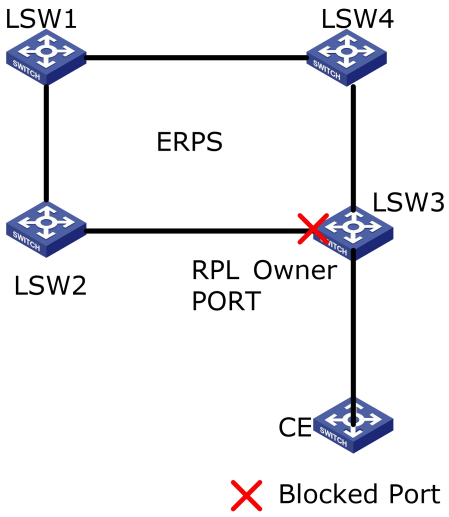
2. Fill in the

Configuration Item	Description
MSTID	Elect the configured instance from drop-down menu
Port	Fixed value, display according to the user's select, does not support multiple selections.
Enable	Fixed value, display according to the user's selection, don't support multiple selections.
Instance	You can create maximum 63 instances
Priority	Select the priority of the port. A lower value indicates a higher priority. Interface priority can affect the interface role in the MSTI. Users can be on the same interface to configure different MSTI different priorities, so that the different VLAN traffic along different physical links, thereby implementing the VLAN-based load balancing. Note: The priority of an interface is changed, MSTP will re-compute the role of the interface and a state transition.
Admin cost	Enter the path cost of the interface. When using the IEEE 802.1t standard method in the range from 1 to 200 000 000
cost	When using the IEEE 802.1x standard method in the range from 1 to 200 000 000
role	Divided into three categories root port, designated port, alternate port, Disabled
status	Including 2 status, discarding and forwarding

appropriate configuration items.
3.Click "Apply" to complete the configuration.

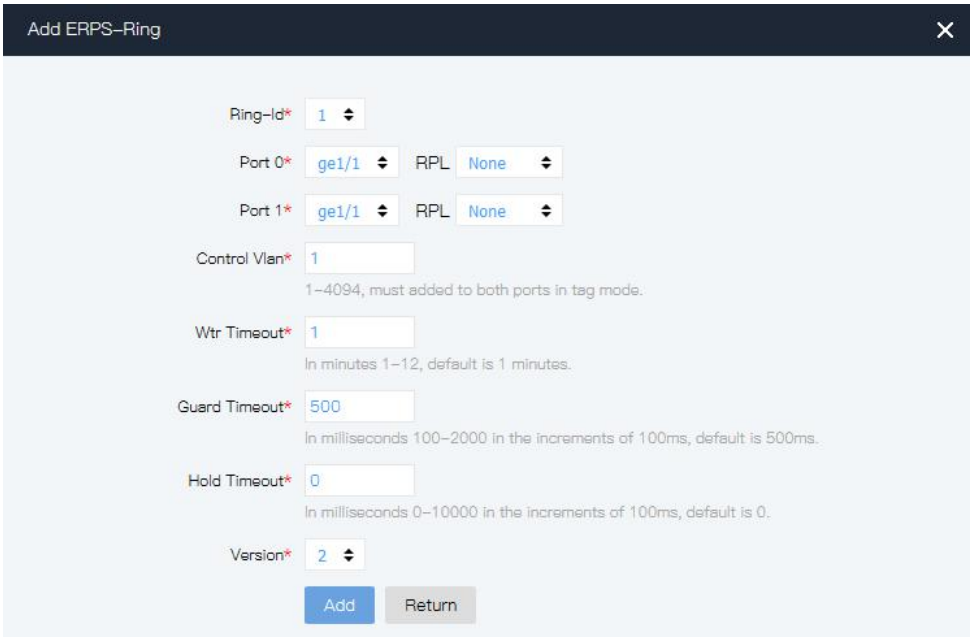
6.4 ERPS-Ring

ERPS (Ethernet Ring Protection Switching), namely Ethernet multi-ring protection technology, is a two-story ITU-T standard protocol defined by broken ring, the standard number of ITU-T G.8032 / Y1344, so-called G.8032。It defines the RAPS (Ring Auto Protection Switching) protocol packets and protection switching mechanisms. ERPS is an Ethernet link-layer protocol used to get rid of the loop. It ERPS ring as the basic unit, comprising a plurality of nodes, by blocking RPL Owner port and other common control port, so the port state switching between the Forwarding and Discarding, the purpose of eliminating loops. We use control mechanisms VLAN, VLAN and data protection instance, in order to better achieve ERPS function.
As shown below, CE ring network access LSW1 ~ LSW4 thereof. Such access allows the network to have some reliability, but in order to eliminate loops in the network, effectively ensure the link connectivity, you need to activate a mechanism to break the loop.



ERPS ring, that is, by a group configured with the same control VLAN Layer 2 switching equipment constituted, is the basic unit ERPS agreement to join the second floor ERPS ring switching device called a node. Each node can not join more than two ports with a ERPS ring, join node needs to be configured to add.

1.Click the navigation tree "Business Management > ERPS-Ring Config " menu, enter the " ERPS-Ring Config ", after ticked, click the "Add". interface as shown below.



Interface information meaning as followings.

Configuration item	Description
Ring-id	ERPS-Ring (1-16 instances Optional)
Port 0	Port List

Port 1	Port List
RPL	Port role，None/Owner/Neighbor
Control Vlan	ERPs protocol management VLAN
Wtr Timeout	WTR Timer
Guard Timeout	Guard Timer
Hold Timeout	Hold Timer
Version	Support Version 1 and 2

2.Fill in the appropriate configuration items.

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

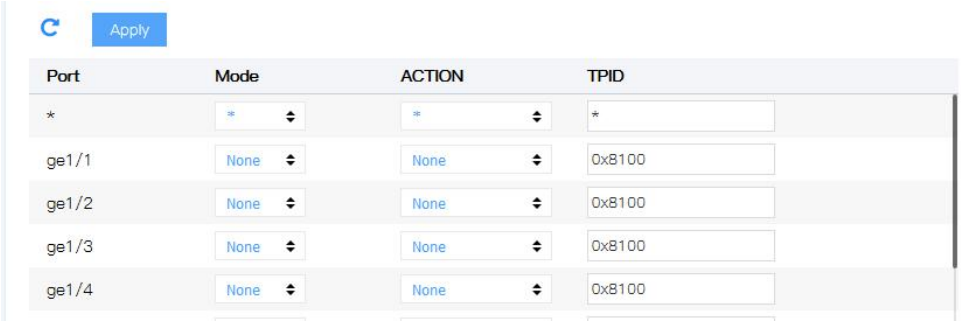
6.5 QINQ

QinQ Technology (also known as stacked VLAN or double VLAN). The standard comes from IEEE 802.1ad, which encapsulates the user private network VLAN tag in the public network VLAN tag, so that the message passes through the operator's backbone network (public network) with two layers of VLAN tag.

QinQ technology effectively expands the number of VLANs by stacking two 802.1Q headers in the Ethernet frame, making the maximum number of VLANs up to 4094x4094. At the same time, multiple VLANs can be multiplexed into a core VLAN. MSP usually establishes a VLAN model for each customer, uses the general attribute registration protocol / general VLAN registration protocol (GARP / GVRP) to automatically monitor the VLAN of the whole backbone network, and speeds up the network convergence speed by expanding the spanning tree protocol (STP), so as to provide flexibility for the network. Svlan technology as the initial solution is good, but with the increase of the number of users, svlan model will also bring scalability problems. Because some users may want to carry their own VLAN ID when data transmission between branches, MSP using QinQ technology faces the following two problems: first, VLAN identification of the first customer may conflict with other customers; second, service providers will be severely limited by the number of IDs that customers can use. If users are allowed to use their VLAN ID space in their own way, there is still a limit of 4096 VLANs in the core network.

Steps:

1.Click in the navigation tree "Business Management > QINQ " menu, enter " QINQ" screen as shown in the following figure.

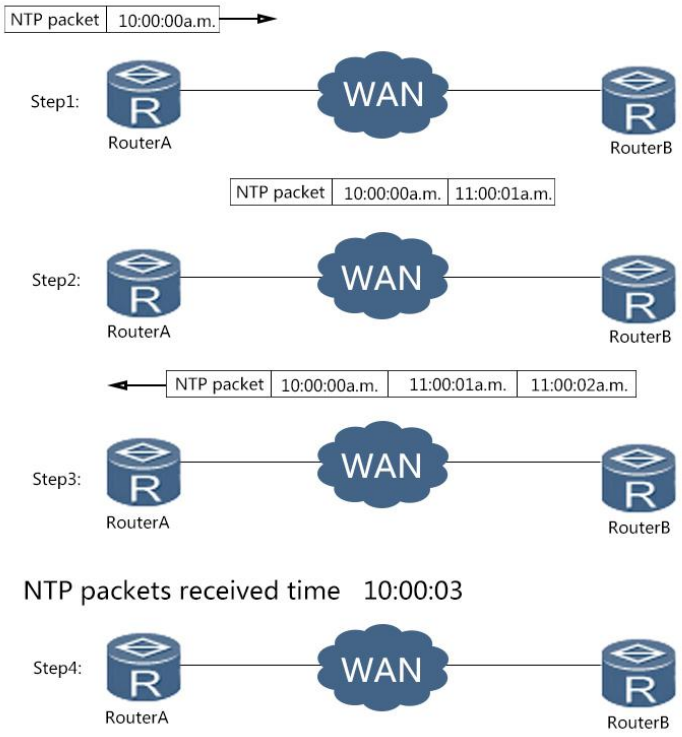


2.Fill in the corresponding configuration items and click "Apply" to complete the configuration.

6.6 NTP

Network Time Protocol NTP (Network Time Protocol) is a TCP / IP protocol suite, which is an application layer protocol. NTP is used across a range of distributed time server and client to synchronize clocks. NTP implementation based on IP and UDP. NTP packets transmitted over UDP port number is 123. With the increasing complexity of the network topology, the entire network equipment clock synchronization will become very important. If you rely on an administrator to manually change the system clock is not only a huge amount of work, and the accuracy of the clock cannot be guaranteed. NTP appears to solve the problem of synchronization within the network equipment system clock.
The basic principle of NTP, NTP implementation process as shown below. RouterA and RouterB through a wide area network WAN (Wide Area Network). They have their own independent system clock; the system clock is automatically synchronized through NTP.
Make the following assumptions:
In RouterA and RouterB system clock synchronization before, RouterA's clock is set to 10:00:00 a.m., RouterB clock set 11:00:00 a.m.
RouterB as the NTP time server, RouterA and RouterB clock to synchronize the clocks.
Packets between RouterA and RouterB-way transmission takes one second.
RouterA and RouterB process NTP packets is 1 second.

NTP Implementation Figure



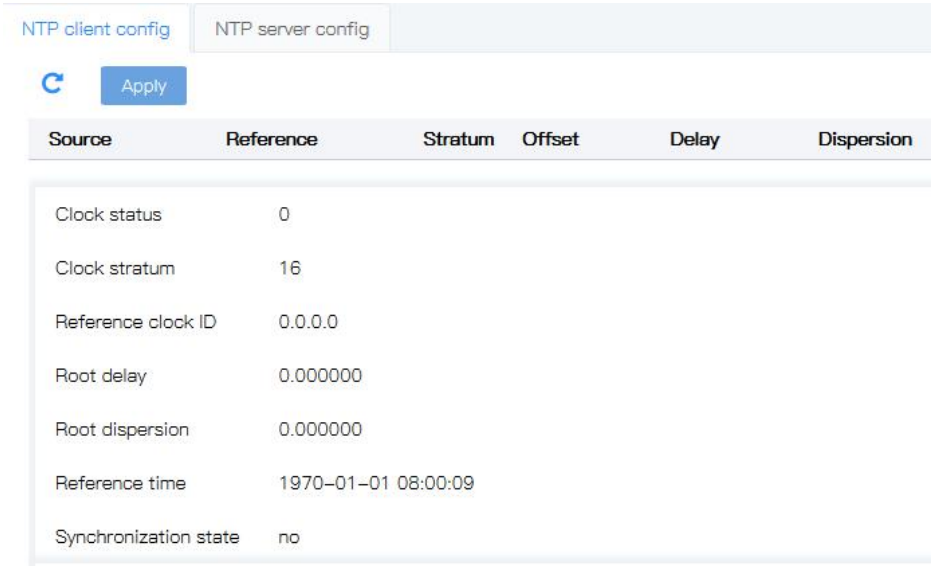
System clock synchronization process is as follows:
RouterA sends an RTP packet to RouterB, the packet with a time stamp 10:00:00 a.m. when it leaves RouterA. (T1).
When this NTP message arrives RouterB, RouterB adds its receiving timestamp 11:00:01 a.m. (T2).
When this NTP message leaves RouterB, RouterB on leave plus timestamp 11:00:02 a.m. (T3).

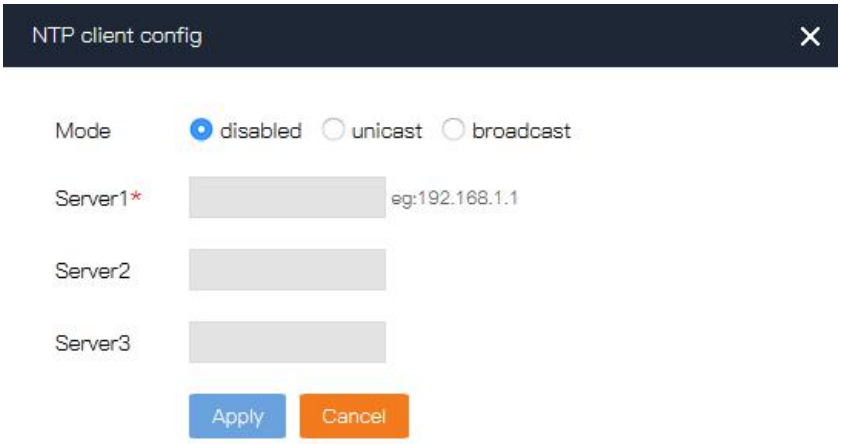
When Router A receives the response packet, it adds a new timestamp 10:00:03 a.m. (T4).
So far, RouterA get enough information to calculate the following two important parameters:
NTP back and forth a period of latency: Delay= (T4 - T1) - (T3 – T2)。
RouterA and RouterB relative time difference: Offset= ((T2- T1) + (T3 – T4)) / 2。
Router OS get calculated Delay 2 seconds, Offset 1 hour. RouterA this information to set its own clock, clock synchronization and RouterB.

✍ illustrate：
The above is a brief description of the NTP operating principle, RFC1305 defines the NTP complex algorithm to ensure clock synchronization accuracy.

Steps

1.Click the navigation tree " Business Management > NTP > NTP client config" menu, enter " NTP client config " screen, as shown below.



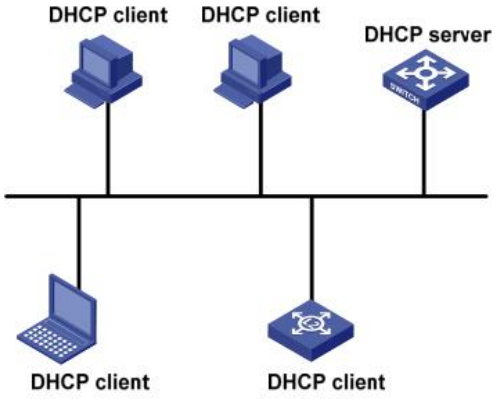


Interface information meaning as followings

Configuration item	Description
Mode	Enable or disable NTP automatically
The servers	Maximum support 3 server IP address

6.7 DHCP Server

With the continuous expansion of network size and increase in network complexity, the situation is more than the number of computers available IP addresses often. And with the widespread use of portable computers and wireless networks are constantly changing location of the computer, the corresponding IP address must be updated frequently, resulting in more complex network configurations. DHCP (Dynamic Host Configuration Protocol, Dynamic Host Configuration Protocol) is to solve these problems and develop. DHCP uses "client / server" model, where the client configuration request to the server, the server returns the configuration information for the client's IP addresses to implement dynamic allocation of network resources. In a typical DHCP application, it includes a DHCP server and multiple clients (such as PC and laptops), as shown in FIG.



It offers three IP address assignment policies for the different needs of the client, DHCP:

- Manual allocation: The network administrator to a client (such as WWW servers, etc.) static binding
- IP address. Fixed IP address by the DHCP server assigns to the client.
- Automatic allocation: DHCP client assigns a permanent IP address infinitely long.
- Dynamic allocation: DHCP assigns the client has a valid IP address period, when the lease expires, the client needs to reapply address. Most clients obtain this address is dynamically allocated.

DHCP client obtains an IP address from a DHCP server via four stages:
(1) Discovery phase, the DHCP client to locate a DHCP server. Client broadcasts a DHCP-DISCOVER.
(2) Offer stage where DHCP server offers an IP address. After the DHCP server receives the DHCP-DISCOVER message sent by the client, according to the priorities assigned IP address is an IP address selected from the address pool, along with other parameters via DHCP-OFFER message is sent to the client (transmission mode according to DHCP-DISCOVER packets in the flag field sent by the client's decision, refer to section 1.3 DHCP packet format).
(3) Selection phase, the DHCP client IP address selection phase. If you have more than one DHCP server to the client sent to the DHCP-OFFER message, the client accepts the first received DHCP-OFFER packets, and broadcasts a DHCP-REQUEST packet, the packet contains DHCP server DHCP-OFFER packets assigned IP address.
(4) Confirmation phase, the DHCP server acknowledges the IP address. After the DHCP server receives a DHCP client to DHCP-REQUEST packet, only the DHCP server chosen by the client will proceed as follows: If the confirmation address assigned to the client, it returns DHCP-ACK packet; otherwise, it returns DHCP -NAK packets of the IP address assigned to the client. If a dynamic address allocation strategy, the DHCP server assigned to the client's IP address has a lease period, when the lease expires server withdraws the IP address. If the DHCP client wants to use the address period, the need to update the IP address lease. When DHCP client's IP address lease duration half-time, DHCP client to the DHCP server a DHCP-REQUEST unicast packets, to update IP lease. If the IP address is valid, the DHCP server to respond to unicast DHCP-ACK packet to notify the DHCP client of the new IP lease; If the IP address cannot be assigned to the client, the DHCP server responds DHCP-NAK packets notify the DHCP client cannot obtain a new lease. If you

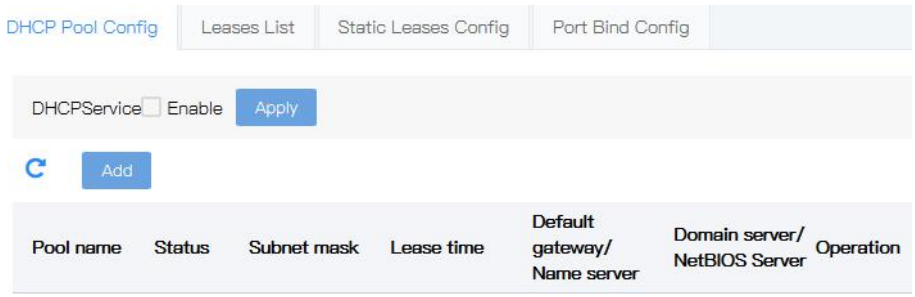
operate in half the time to renew the lease were failures, DHCP client in 7/8 lease duration, the DHCP-REQUEST broadcast retransmission packet renewed. Processing Ibid DHCP server, not repeat them.

6.7.1 DHCP Server Configuration

Enable DHCP server

Steps:

1.Click the navigation tree "Business Management > DHCP Server > DHCP Pool Config" menu, enter "DHCP Pool Config" screen, select Enabled, click "Apply", as shown below.

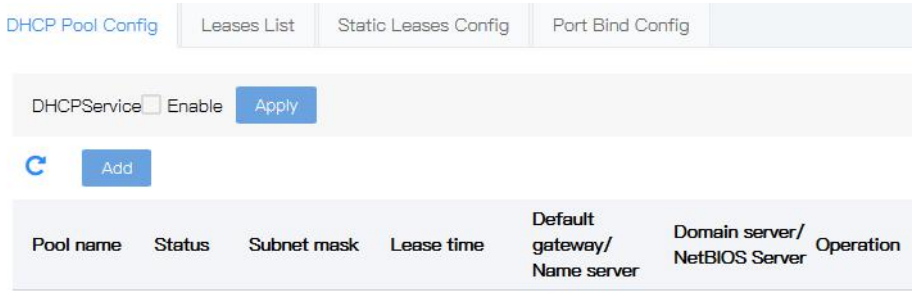


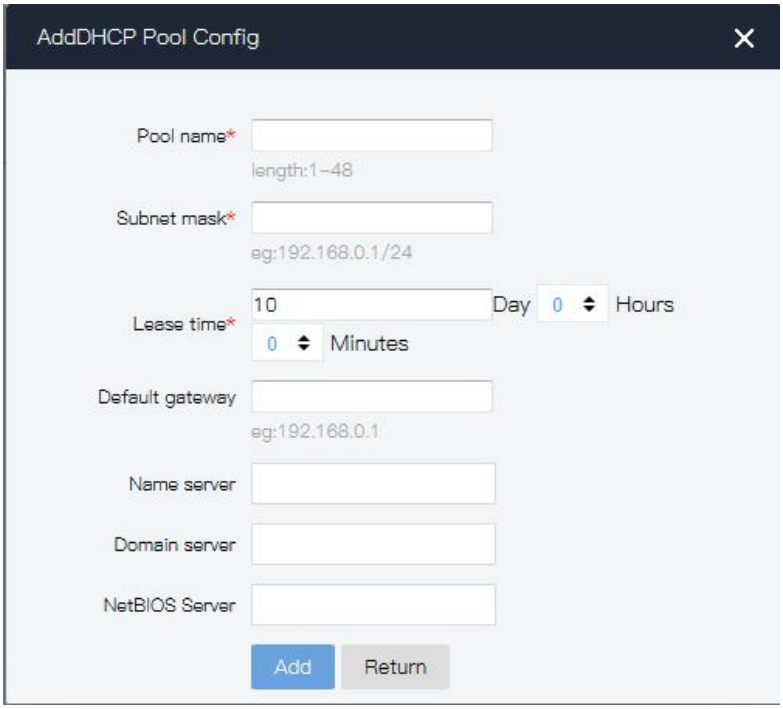
6.7.2 Address pool configuration

Configuring the DHCP server based on the global address pool, select a server from the address pool a free IP address assigned to the client. In order to obtain a dynamic IP address from your computer switches you need to configure a DHCP server based on the global address pool.

Steps:

1.Click the navigation tree " Business Management > DHCP Server > DHCP Pool Config " menu, go to " DHCP Pool Config " interface, as shown below.

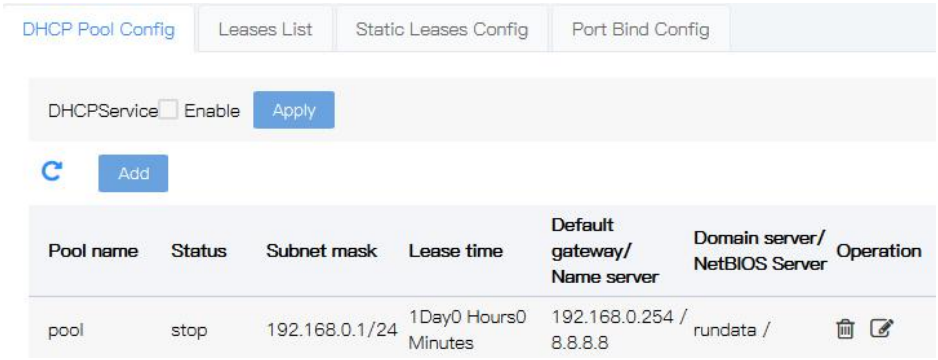




Interface information meaning as followings.

Config item	Description
Pool name	Enter the poor name
Subnet mask	Enter the IP address pool address and subnet mask.
Lease time	The lease of dynamic IP addresses. The default is 1 day. The range: Day: an integer ranging from 0 to 999. Hours: integer ranging from 0 to 23. Score: integer ranging from 0 to 59.
Default gateway	Enter the gateway IP add
DNS server	Enter DNS IP ADD
Domain server	Enter the DHCP server assigned to the client's domain name.
NetBIOS server	Enter the NetBIOS server IP address

2. Fill in the appropriate configuration items.
3. Click "Add" to complete the configuration, as shown below.



6.7.3 Leases list

View leases IP Address List Procedure

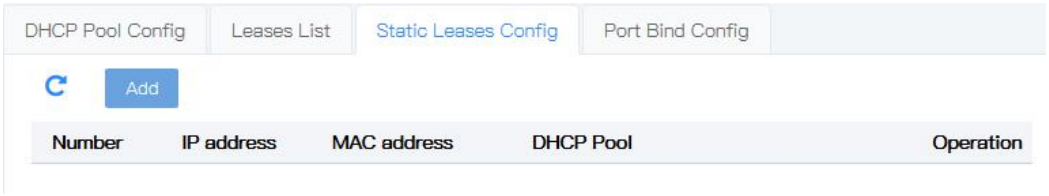
1. Choose the " Business Management > DHCP Server > Leases List" menu, go to " Leases List" screen, as shown below.

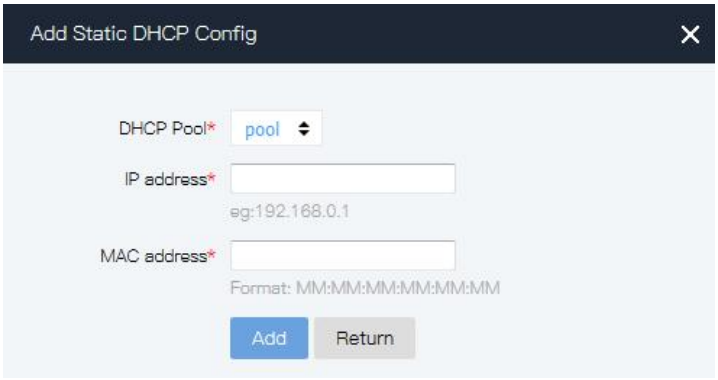
6.7.4 Static Leases configuration

To meet the specific device (such as a server) needs a fixed IP address, you can take a static client configuration.

Steps:

1.Click in the navigation tree " Business Management > DHCP Server > Static leases Config" menu, go to "static leases configuration" screen, as shown below.

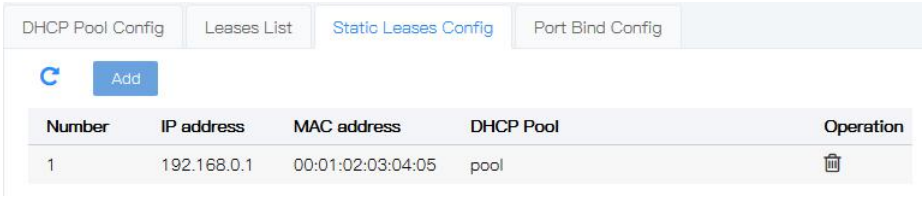




Interface information meaning as followings

Config item	Description
DHCP Pool	Fixed value. Already created address pool.
IP address	Input the IP address to be bound.
MAC address	Input the MAC address to be bound

2. Fill in the appropriate configuration items.
3. Click "Add" to complete the configuration, as shown below.

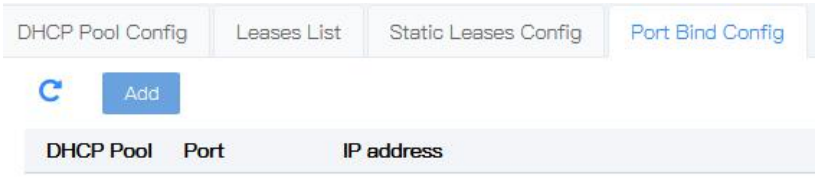


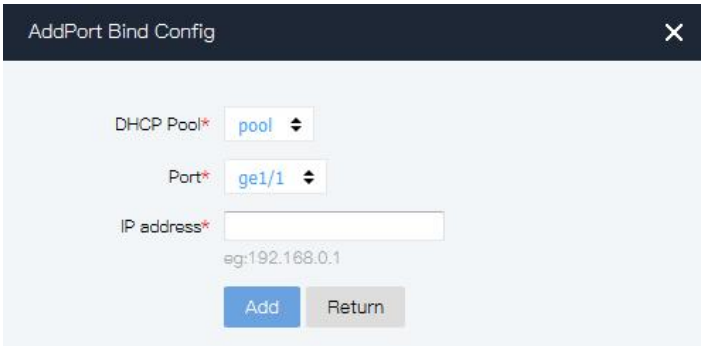
6.7.5 Port Binding

To meet the switch ports, have a fixed IP address, you can use the IP address of the switch port binding

Steps:

1.Click the navigation tree " Business Management > DHCP Server > Port Bind config" menu, go to " Port Bind config " screen, as shown below.





Interface information meaning as followings

Config item	Description
DHCP Pool	Fixed value. Already created address pool.
port	Radio. It indicates the interface name selected by the user, creating multiple support.
IP address	Enter the IP address to be bound.

2. Fill in the appropriate configuration items.
3. Click "Add" to complete the configuration, as shown below.

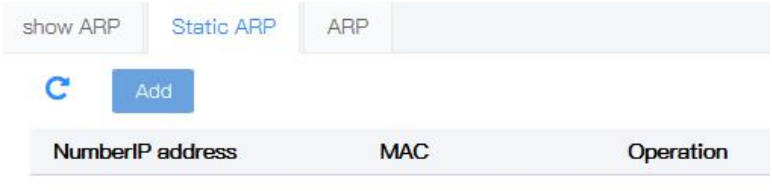
6.8 ARP

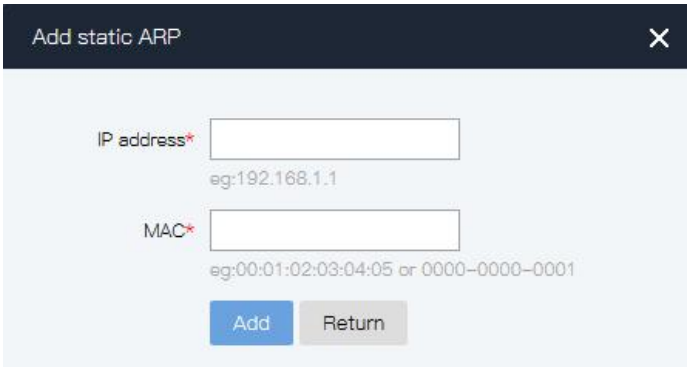
Address Resolution Protocol (ARP) is a protocol which determines its physical address when only know the IP address of the host. Because of the extensive application of IPv4 and Ethernet. Its main role is obtaining corresponding physical address through a known IP address. But it can also be used in ATM (Asynchronous Transfer Mode) and FDDIIP (Fiber Distributed Data Interface). There are two ways to map IP addresses to physical addresses: table and non-tabular. ARP specifically refers to the network layer (IP layer, which is equivalent to the third layer of OSI) address resolved to the MAC address of data link layer (MAC layer, which is equivalent to the second layer of OSI)

OSI mode divide network work into seven layers, IP address in the third layer, .MAC address in the second layer. When protocol send the packet, it should encapsulate the header of the third layer (IP address) and the second layer (MAC address), but protocol only know the destination node's IP address, do not know its MAC address, and can't cross the second, the third layer, so here have to use ARP services.

A Configure static ARP steps:

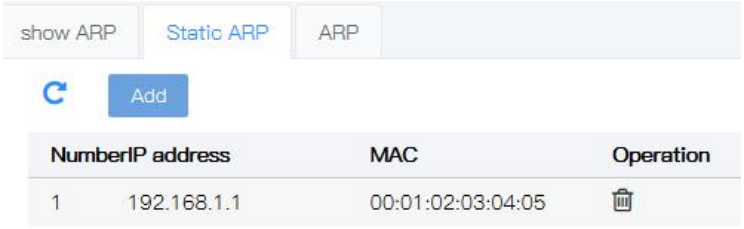
1. Click the navigation tree "Business Management > ARP > Static ARP" menu. The interface is shown below.





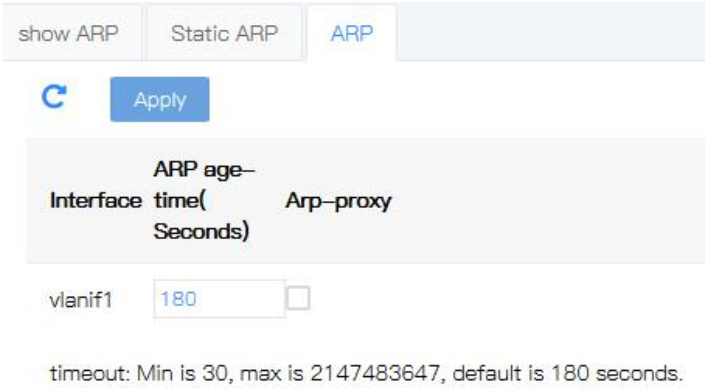
2.Input IP address

3.Click "Add", page is shown below



B Configure ARP aging time steps：

1.Click the navigation tree “Business Management > ARP > ARP” menu. The interface is shown below.



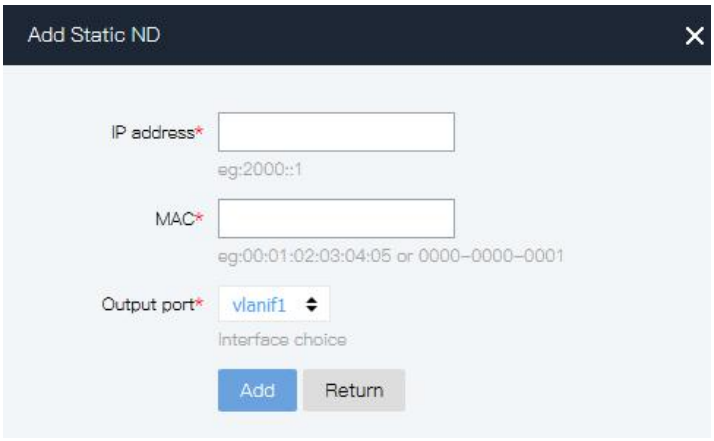
Input aging time, click “Apply”.

6.9 ND

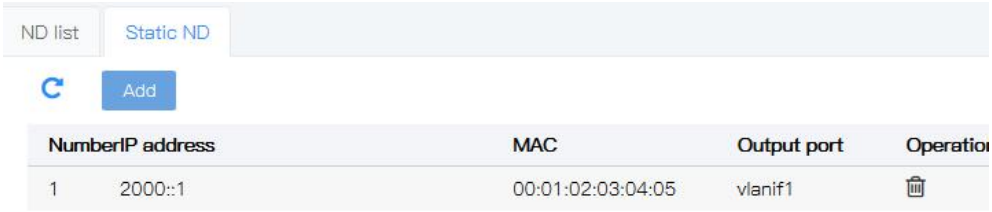
Address resolution plays an important role in packet forwarding. When a node needs to get the link layer address of another node on the same link, it needs to resolve the address. ARP is used in IPv4 and NS and Na messages in Nd (neighbor discover) are used in IPv6

A Configure static ND steps:

1.Click the navigation tree “Business Management > ND > Static ND” menu. The interface is shown below.



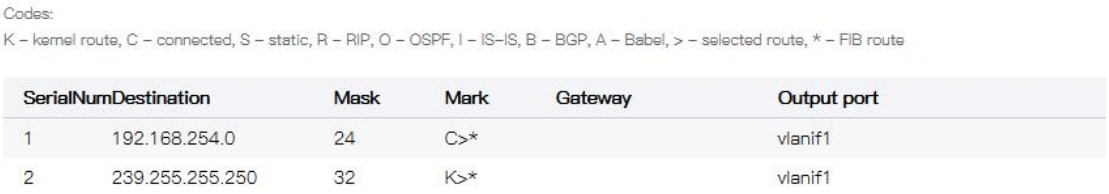
2.Input IP address、MAC and VLANIF
3.Click “Add”, page is shown below



7 Route

7.1 Show route

Used to view routing in the switch
Steps
1. Click the navigation tree " Route > Show route". The interface is as follows.



7.2 Static Route

Static routing is a special route that is manually configured by the administrator. The following table lists the contents of this chapter. When the network structure is relatively simple, just configuring the static route can make the network work properly. Carefully set and using
Static routing can improve network performance and ensure bandwidth for critical applications.

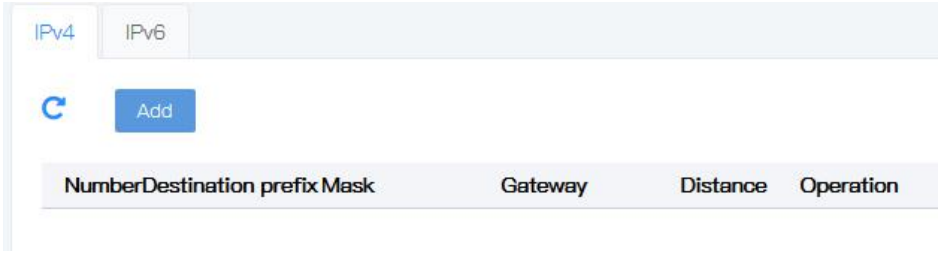
The disadvantage of static routing is that when the network fails or the topology changes, the static route does not change automatically, and the administrator must be involved. The default route is another special route. In general, administrators can configure default routes manually, but in some cases, dynamic routing protocols can also generate by default routes such as OSPF and IS-IS. In a nutshell, the default route use when can't find matching routing table entry. In the routing table, the default route appears as routing form of network 0.0.0.0 (mask is 0.0.0.0) Check whether the default route is set by order "Display ip routing table" .If the destination address of message can't match any entry of the routing table, the message will select the default route. If there is no default route and the destination address of the message is not in the routing table, then the message is discarded and an ICMP message which is destination address or network unreachable returned to the source port. When configuring a static route, you can specify the interface-type interface-name, or specify the next hop-address. Specifying the sending interface or the next hop address, it depends on the specific situation. In fact, all routing entries must have a clear next hop-address. When sending a message, it firstly searches the matching route in the routing table based on the destination address of the message. Only specify the next hop-address, the link layer can find the corresponding link layer address and forward the message.

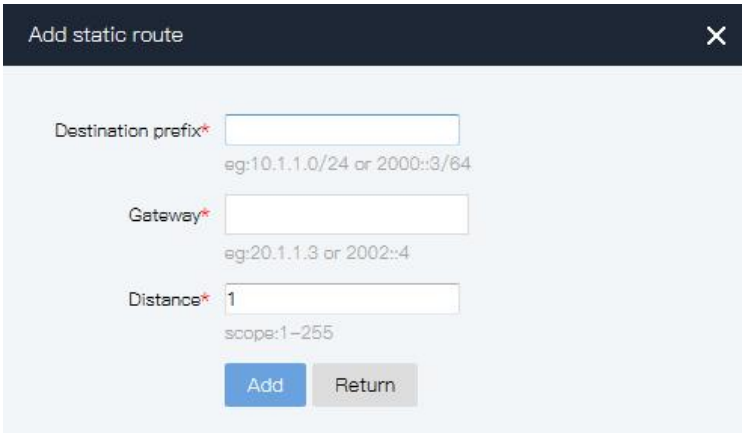
⚠ Attention

Recommend not specifying Ethernet interface. Because the Ethernet interface is the interface of the broadcast type, it will result in a number of next hop and cannot uniquely determine the next hop. In the application, If the broadcast interface (such as Ethernet interface) must be specified as the sending interface, the corresponding next hop-address should be specified at the same time.

Static route configuration steps

1 click the navigation tree " Route > Static Route", the interface is as follows.





2.View Static route configured, click "Show route"

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	10.1.1.0	24	S	20.1.1.3	
2	192.168.254.0	24	C>*		vlanif1
3	239.255.255.250	32	K>*		vlanif1

7.3 RIP

The routing information protocol (RIP) is a relatively outdated but still widely used internal gateway protocol (IGP), which is mainly used in the smaller homogeneous networks. RIP is a classical distance vector routing protocol, which appears in RFC 1058, and presents an improved RIP-2 among RFC1388, and was revised in RFC 1723 and RFC 2453.
RIP uses Bellman-For algorithm currently RIP IPv4 has two versions, RIPv1 and RIPv2. RIP has the following main features:
RIP is a typical distance vector routing protocol.
RIP messages sent by the broadcast address 255.255.255.255, RIPv2 send messages by using multicast address 224.0.0.9, both using the port 520 of UDP
RIP takes the minimum hop count to the destination network as the routing metric, rather than the bandwidth and delay of the link.
RIP is designed for small networks. The number of hops is limited to 15 hops, and the 16 hop is not reachable.
RIP-1 is a kind of class routing protocol, does not supporting discontinuous subnet design.
RIP-2 support CIDR and VLSM variable subnet mask, which make it supports the discontinuous subnet mask design
RIP periodic full routing updating, make the routing table broadcast to the neighbor router, broadcast cycle default 30 seconds.
RIP protocol management distance is 120.

For small networks, in terms of occupied bandwidth, RIP is small cost and easy to configure, manage, and implement, and RIP is still in use. But RIP also has obvious shortcomings. When there is more than one network will appear loop problem. In order to solve the loop problem, IETF proposed a split-Horizon method, the routing information received at this interface will no longer go out from the interface. The scope of the division solves the routing loop problem between two routers, but can't prevent the problem which is the loop mainly formed by delay factor because of large scale network. The trigger update requires the router to transmit its routing table immediately when the link changes. These speeds up the convergence of the network, but prone to broadcast flooding. In short, the solution of the loop problem needs to consume a certain amount of time and bandwidth. If the RIP protocol is adopted, the number of links in the network can't exceed 15, which makes the RIP protocol is not suitable for large networks.

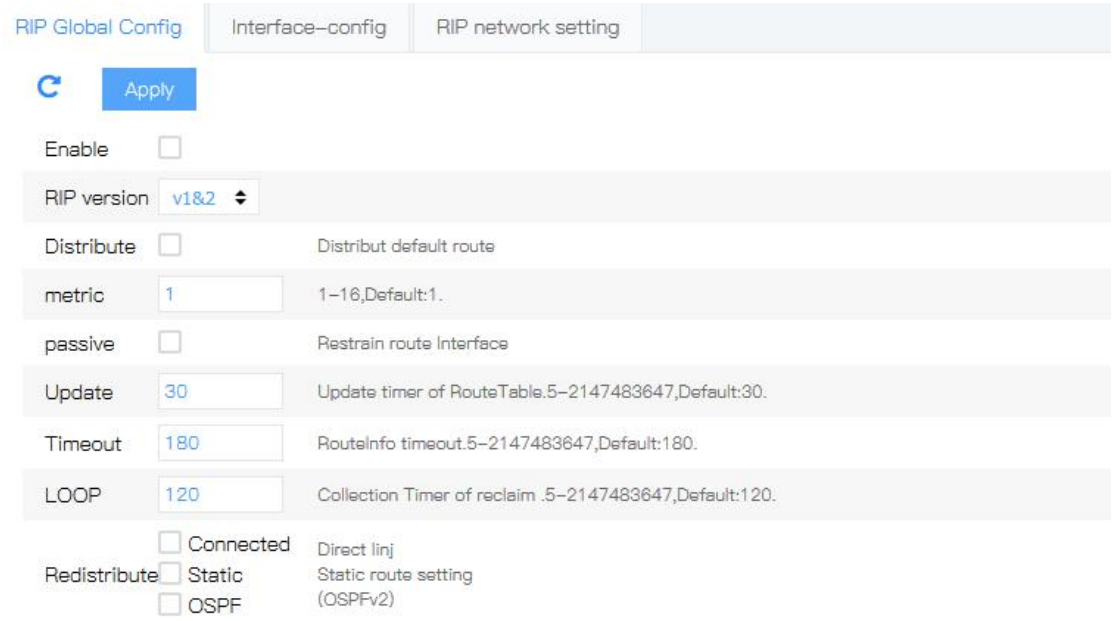
RIP Working principle

RIP is a distributed type routing protocol based on distance vector, which is the standard protocol of the Internet. Its biggest advantage is simple. The RIP protocol requires that each router in the network maintain a distance record from itself to each other destination network. The RIP protocol defines "distance" as: the distance of a router directly connected network defines as 1.the distance of a router not directly connected network defines as pass each router plus 1. "Distance" is also called "hops". RIP allows one path contain up to 15 routers, so distance equal to 16 is unreachable. So RIP protocol only applies to small Internet.

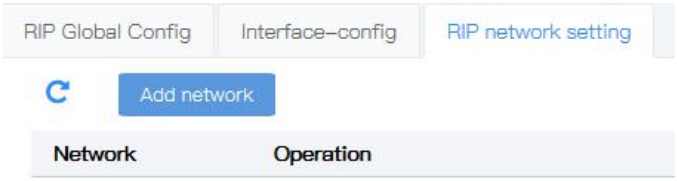
RIP 2 comes from RIP and is a supplementary protocol for RIP. It is mainly used to increase the number of loaded useful information and increase its security performance. RIPv1 and RIPv2 are UDP-based protocols. Under RIP2, each host or router sends and receives packets from UDP port 520 through the routing select process. The default routing update period for RIP protocol is 30S.

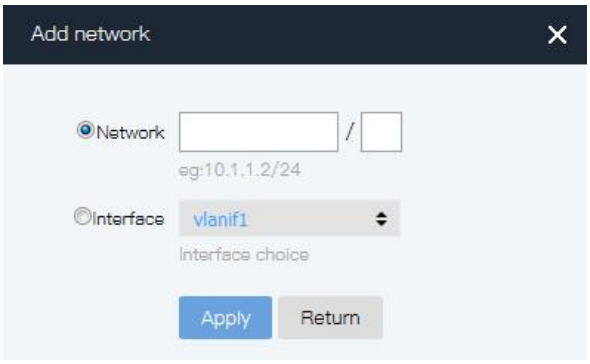
RIP Configuration steps:

1.Open RIP and click the navigation tree “Route > RIP Config > RIP Global Config”. The interface is as follows.

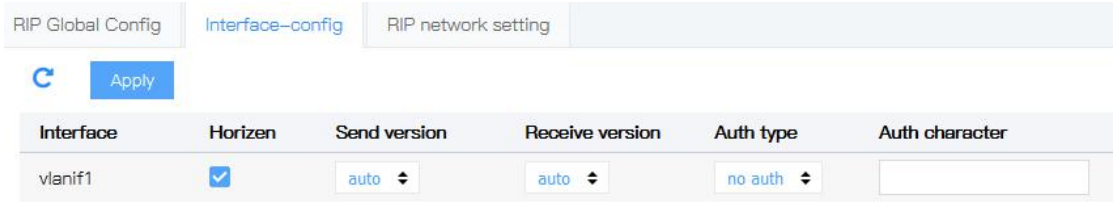


2.Declare the network segment, click the navigation tree “Route > RIP Config > RIP network setting", the interface is as follows.





Configure RIP authentication, click the navigation tree" Route > RIP Config >Interface-config". The interface is as follows.



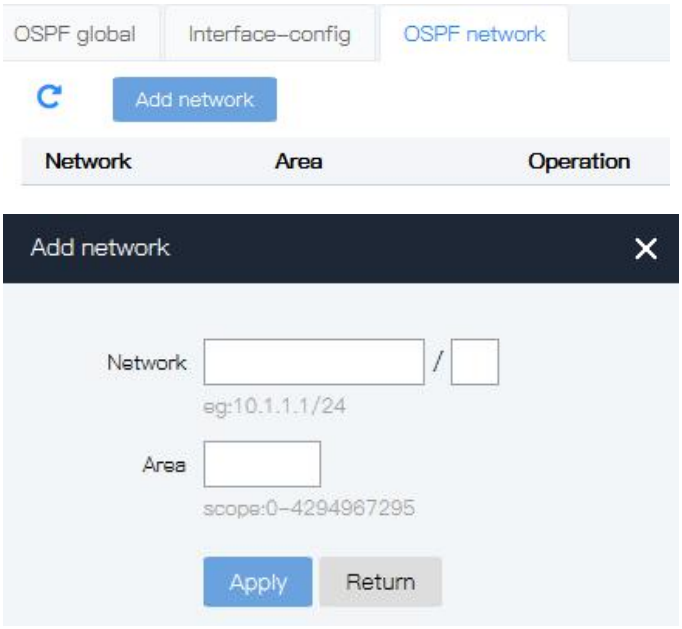
7.4 OSPF

OSPF (Open Shortest Path First) is an Interior Gateway Protocol (IGP) for routing decisions within a single autonomous system (AS). It is an implementation of the link state routing protocol, under the internal gateway protocol (IGP). It is operating within the autonomous system. The shortest path is calculated using the Dixdale algorithm.

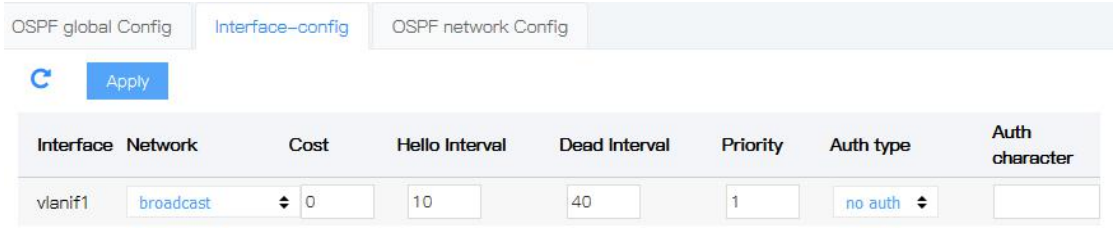
OSPF is IGP routing protocols developed by IETF's OSPF workgroup OSPF designed for IP networks support IP subnet and external routing information marking, also allows authentication of message and supports IP multicast

1.Enable OSPF. Click the navigation tree "Route > OSPF > OSPF global Config" The interface is shown in the following figure.

2.Declare the OSPF network segment, Click the navigation tree" Route > OSPF > OSPF network", the interface as shown below.



3.Configure OSPF authentication, click the navigation tree" Route > OSPF > Interface-config", the interface as shown below.



7.5 VRRP

VRRP (Virtual Router Redundancy Protocol) is a fault-tolerant protocol. Generally, all the hosts in network are set up with a default route so the message of host sent which destination address is not in this network segment will be sent to Router A through Default route then realizing the communication between the host and the external network. When Router A is broken, in this network segment, all host which the Router A as the default route will be disconnected from the external network, then appearing single point fault. VRRP is proposed to solve these problems, it is design for LAN (like Ethernet) with multicast broadcast function. VRRP organizes a set of routers (including a Master as an active router and several Backup routers) of the LAN into a virtual router, called a backup group. This virtual router has its own IP address 10.100.10.1 (the IP address can be the same as the address of a router in the backup group, the same is called the ip owner), the router within the backup group also has its own IP address (If the master's IP address is 10.100.10.2 and the backup's IP address of is 10.100.10.3). The host in the LAN only knows the IP address 10.100.10.1 of the virtual router and does not know the IP address 10.100.10.2 of the specific master router and the IP address 10.100.10.3 of the backup router. [1] They set their default routing next hop address to the virtual router's IP address 10.100.10.1. As a result, the host within the network through this virtual router to communicate with other networks. If the master in the backup group is broken, the backup

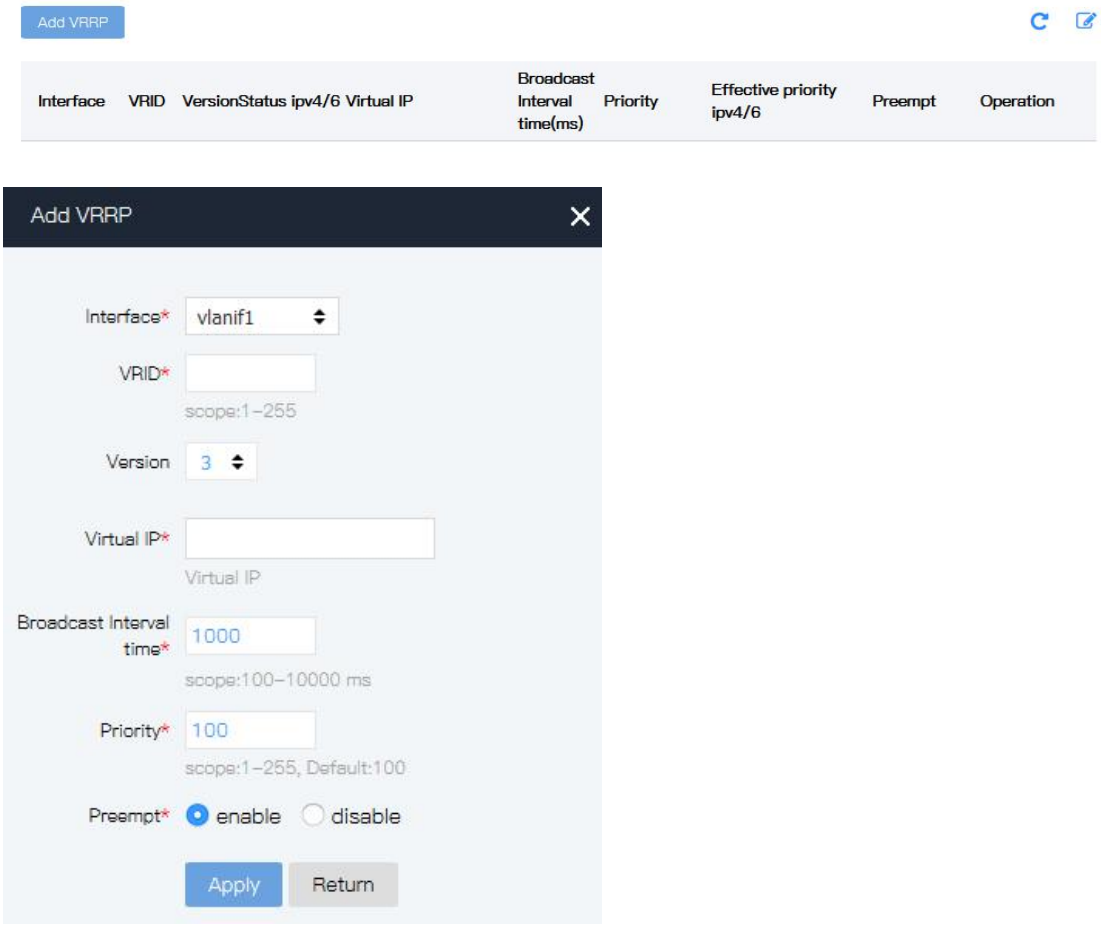
router will select a new master through the election policy and the new route continue to provide the routing service to the hosts in the network. Thereby enabling the hosts within the network to communicate with the external network without interruption.

The working mechanism of the VRRP protocol has many similarities with CISCO's HSRP (Hot Standby Routing Protocol). But the main difference between the two is in the HSRP of CISCO the need to configure a separate IP address as a virtual router external address, this address can't be interface address of any member of the group.

The use of VRRP protocol, not modifying the network structure, maximize the protection of investment. With minimal management costs, but greatly enhance the network performance, with significant application value.

Configuration steps

1. Click in the navigation tree "Route > VRRP" menu. The interface is shown in the following figure.

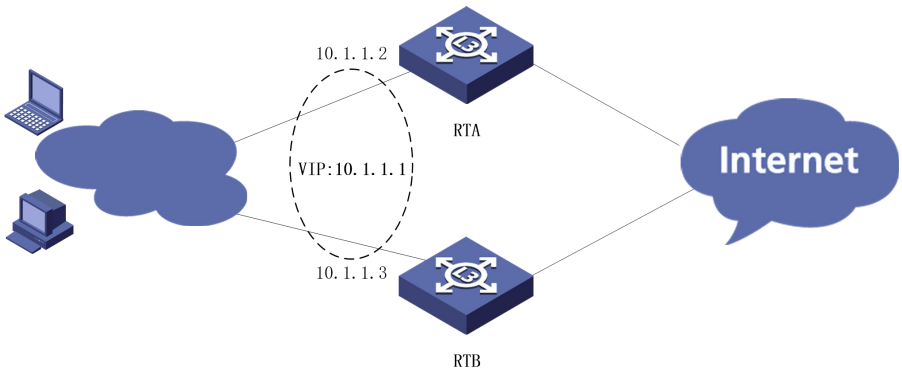


The most typical VRRP application: RTA, RTB constitute a VRRP router group, assuming RTB processing capacity is higher than the RTA, the RTB will be configured as IP address owner, H1, H2, H3 default gateway is set to RTB. RTB becomes the master router, responsible for ICMP redirection, ARP reply and IP message forwarding; Once RTB fails, RTA immediately start switching, become the master, thus ensuring a transparent security switch to customers.

In VRRP applications, RTB is online when RTA is only as a backup, does not participate in forwarding work, idle router RTA and link L1. By a reasonable network design, you can achieve the dual effects of backup and load sharing. Let RTA and RTB belong to two VRRP groups that are each other backed up at the same time: RTA in group 1 is the IP address

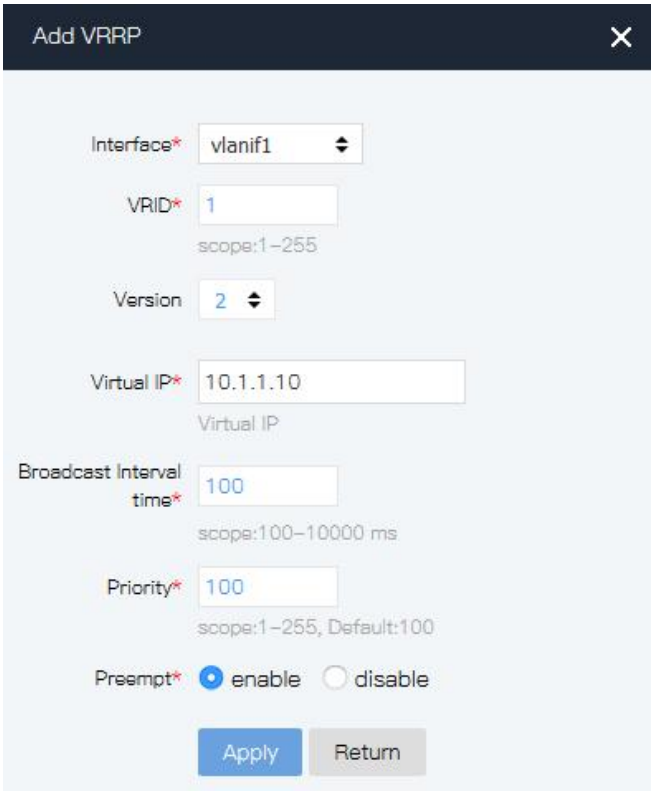
owner; RTB in group 2 is the IP address owner. Set the default gateway of H1 to RTA; the default gateway for H2, H3 is set to RTB. In this way, sharing the equipment load and network traffic, but also improving the network reliability.

The sample diagram is shown below:

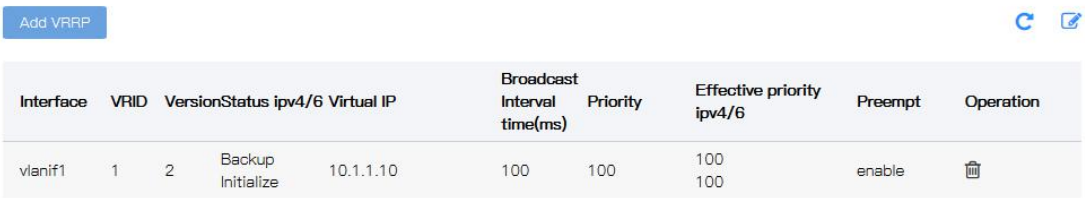


Steps

RTA settings, click the navigation tree "Route > VRRP" menu, the interface as shown below.



2.Click “Apply”.



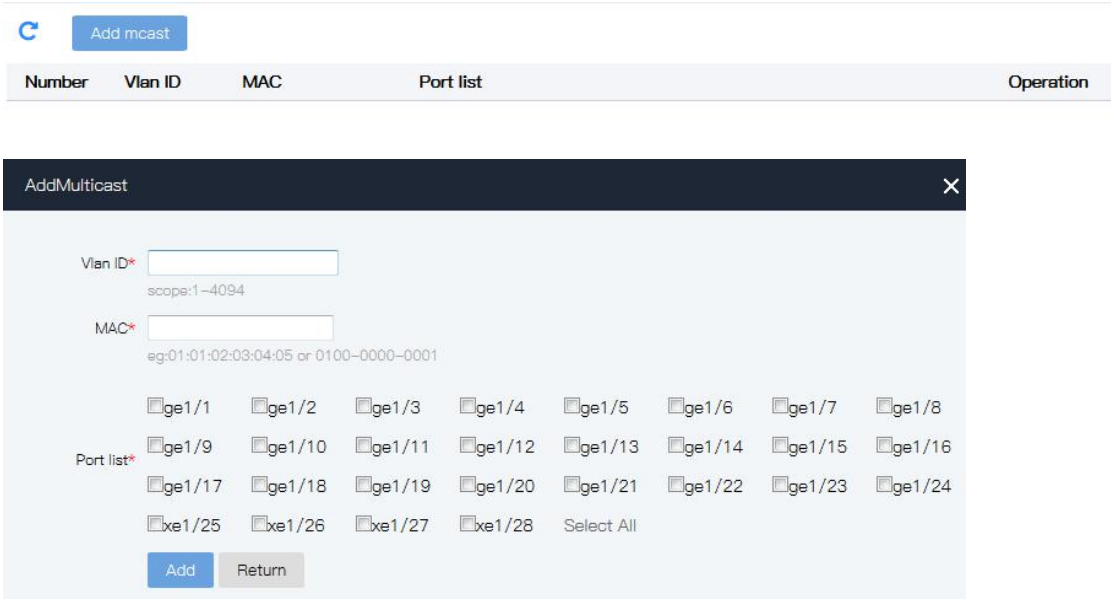
8 Multicast

8.1 Multicast MAC

Configure multicast program according to static multicast MAC

Steps

Click the navigation tree " Multicast > MulticastMAC " menu, enter " MulticastMAC" screen as shown below.



Interface information meaning as followings.

Configuration item	Description
Vlan ID	Fixed, depend on the selected data. Description: The VLAN has been created. Enter a VLAN that has been created
MAC	Enter the multicast MAC address
Port list	Joins the multicast members, you can multi-selection

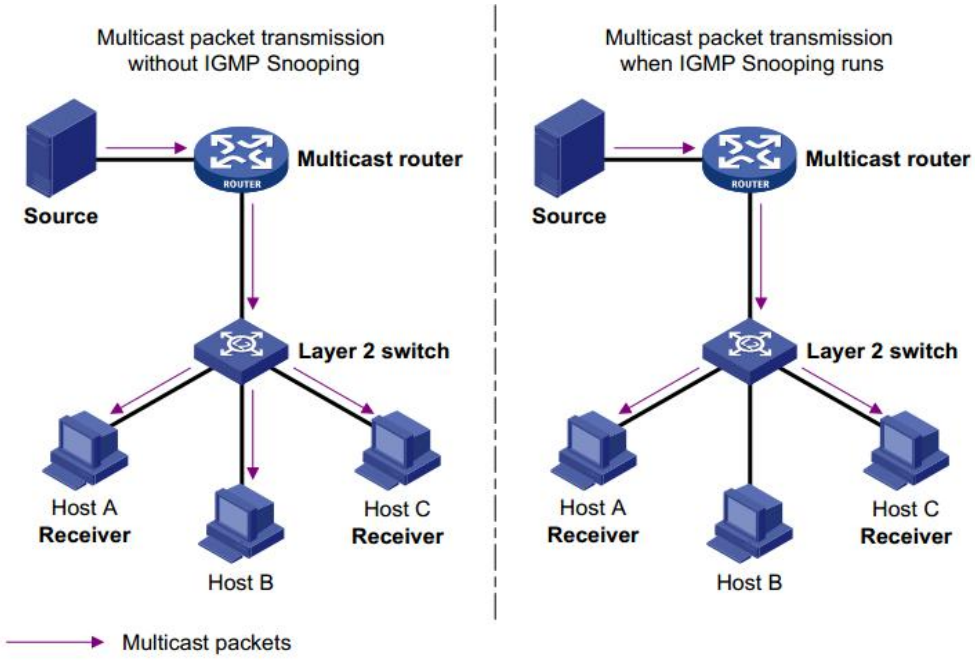
8.2 IGMP-snooping

IGMP Snooping (Internet Group Management Protocol Snooping) is a multicast control mechanism running on Layer 2 devices to manage and control multicast groups.

Layer 2 device IGMP Snooping By analyzing received IGMP messages, analyze, ports and multicast MAC addresses to establish a mapping relationship, and forwards multicast data based on these mappings.

As shown below, when the floor is not running IGMP snooping, multicast packets are broadcast on the second floor; the second floor when the device running IGMP snooping, multicast packets for known multicast groups on the second floor It is broadcast, while the

second floor is multicast to the receivers, but the unknown multicast data will still be broadcast in the second floor.

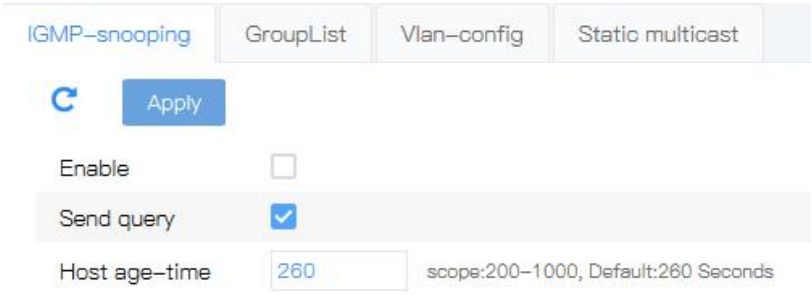


8.2.1 IGMP-snooping

IGMP Snooping, for IPv4 networks, deployed on the switcher position between multicast routers and hosts, arranged in a VLAN, IGMP sent between the role of listener routers and hosts / MLD multicast data packets establish the two-story forwarding, manages and controls the forwarding of multicast data in a Layer 2 network.
By default, the IGMP Snooping function of the switch is to enable the state, we need to be able to switch the global IGMP Snooping feature.

Steps

1.Click the navigation tree " Multicast > IGMP-snooping > IGMP-snooping" menu, enter " IGMP-snooping" screen as shown below.



Interface information meaning as followings.

Configuration Item	Description

Enable IGMP-snooping Config	To globally enable IGMP Snooping situation is not configured IGMP Snooping in the VLAN. Radio, and go into enable two states. The default is to enable.
Host age-time	When a port joins a multicast group, the switch starts a timer for the port, the timeout is host port aging time. After a timeout, the switch removes the port from the multicast group forwarding table. The value is in the range of 200 to 1,000 seconds and defaults to 260 seconds.

2.Fill in the appropriate configuration items.
3.Click “Apply”, to complete the configuration.

8.2.2 Group List

It is used to view dynamically generated multicast table entries, which takes effect when IGMP snooping is enabled globally.

Steps

Click the navigation tree " Multicast > IGMP-snooping > GroupList" menu, enter " GroupList " screen as shown below.

8.2.3 VLAN-config

Multicast VLAN configuration, configure the multicast related properties of VLAN

Steps

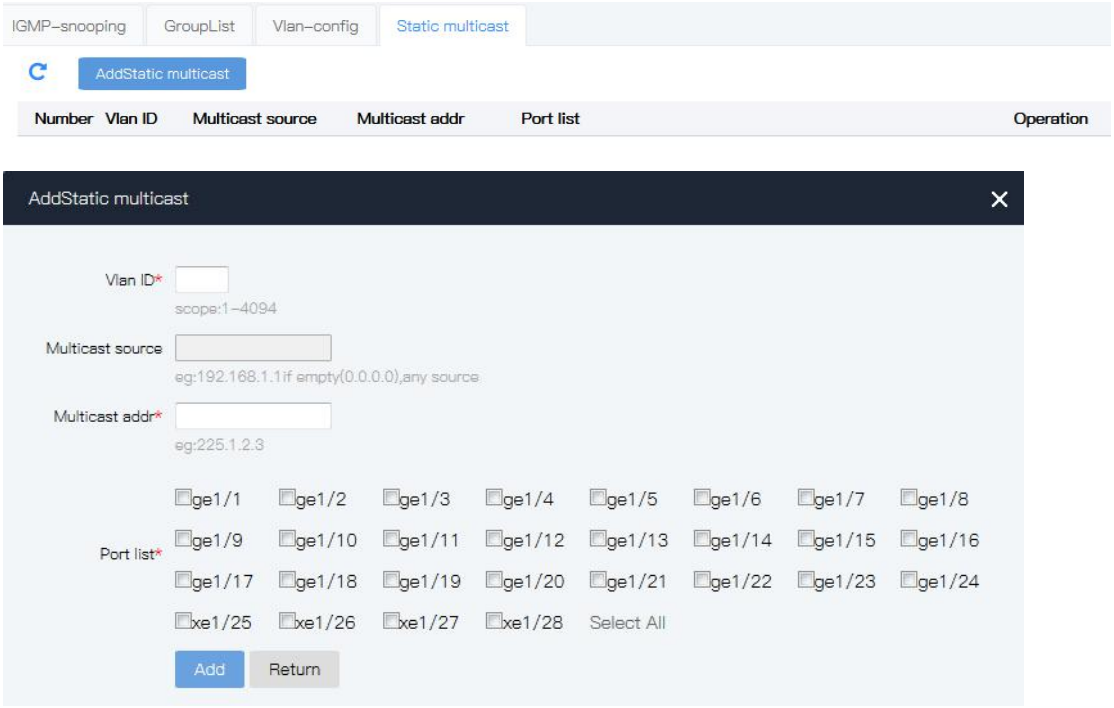
Click the navigation tree " Multicast > IGMP-snooping > VLAN-config" menu, enter " VLAN-config " screen as shown below.

8.2.4 Static IP Multicast

In traditional multicast implementations, when users in different VLAN to the same multicast group, the data on the multicast router will be copied and forwarded for each VLAN that contains receivers. Such multicast implementations, wasting a lot of bandwidth. After starting an IGMP Snooping, the multicast VLAN way that will add switch ports to the multicast VLAN, so that users in different VLAN to share the same multicast VLAN receive the multicast, multicast streams in a multicast only VLAN in the transmission, thus saving bandwidth. And because the multicast VLAN users. VLAN security isolation, security, and bandwidth can be guaranteed.

Steps

1.Click the navigation tree "Multicast > IGMP-snooping > Static multicast" menu, enter " Static multicast " interface as shown below.

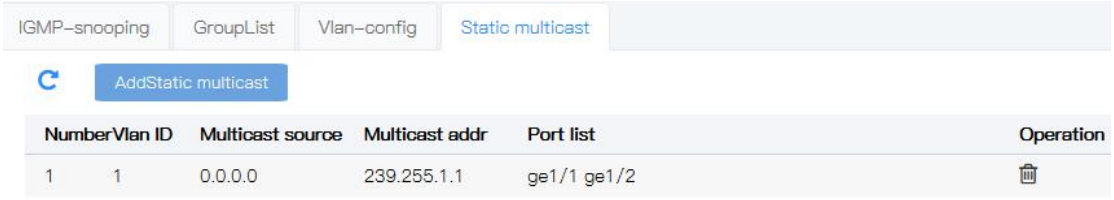


Interface information meaning as followings.

Configuration item	Description
Vlan Id	Fixed, depend on the selected data. Description: The VLAN has been created. Enter a VLAN that has been created
Multicast source	Enter the multicast source address
Multicast address	Enter the multicast address
Port list	Joins the multicast members, you can multi-selection

2.Fill in the appropriate configuration items.

3.Click “Apply”, to complete the configuration.

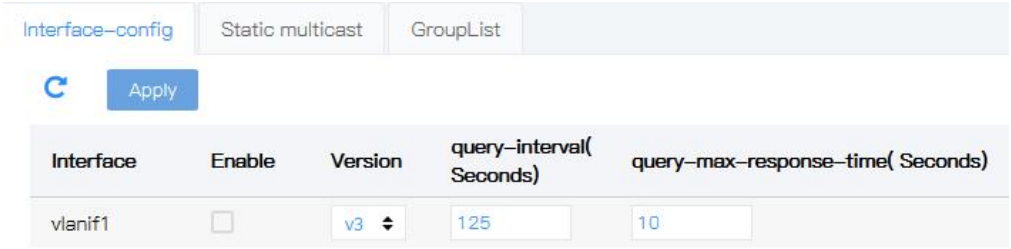


8.3 IGMP

8.3.1 Interface-config

Steps

1.Click the navigation tree "Multicast > IGMP > Interface-config" menu, enter " Interface-config " interface as shown below.



Interface information meaning as followings.

Configuration item	Description
Interface	VLANIF interface
Enable	Enable IGMP attribute of VLANIF interface
Version	IGMP version
query-interval	Query interval, default is 125s
query-max-response-time	Query max response time, default is 10s

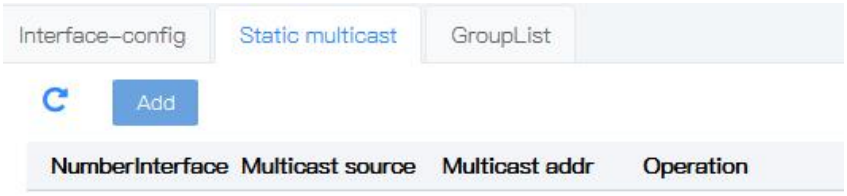
2.Fill in the appropriate configuration items.

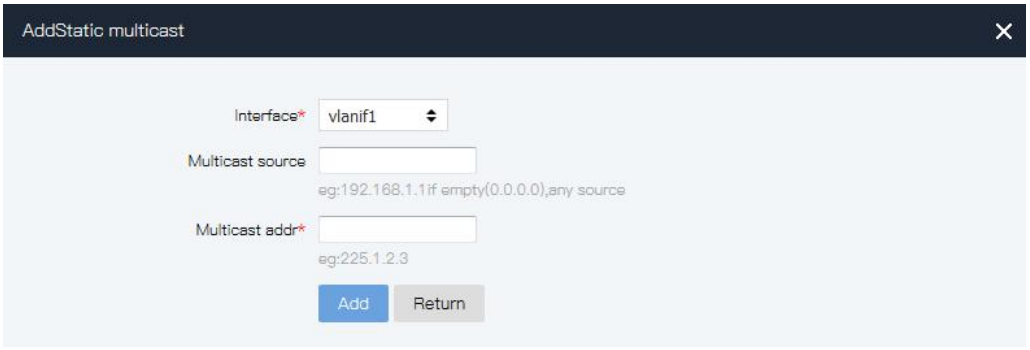
3.Click “Apply”, to complete the configuration.

8.3.2 Static multicast

Steps

1.Click the navigation tree "Multicast > IGMP > Static multicast" menu, enter " Static multicast " interface as shown below.





Interface information meaning as followings.

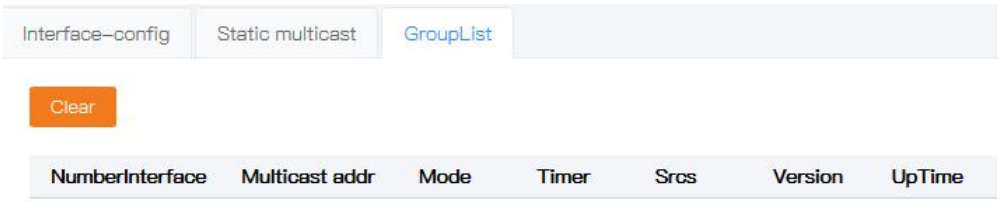
Configuration item	Description
Interface	VLANIF interface
Multicast source	Enter the multicast source address
Multicast address	Enter the multicast address

2.Fill in the appropriate configuration items.
3.Click “Add”, to complete the configuration.

8.3.3 Group List

Steps

1.Click the navigation tree "Multicast > IGMP > GroupList" menu, enter " GroupList " interface as shown below.



8.4 PIM

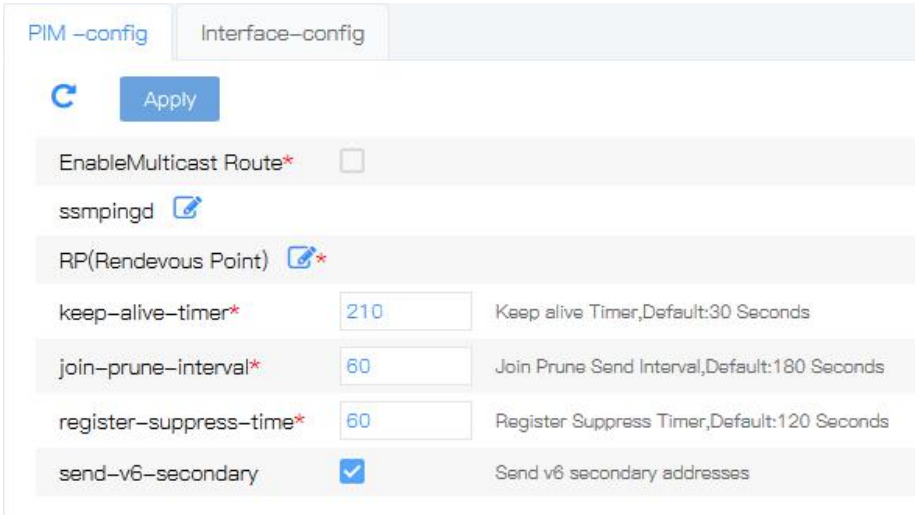
PIM (Protocol Independent Multicast) is a multicast routing protocol. PIM does not depend on a specific unicast routing protocol. It can use the unicast routing table established by any unicast routing protocol to complete the RPF check function, so as to establish multicast routing.

Because PIM does not need to receive and send multicast routing updates, compared with other multicast routing protocols, PIM overhead reduces a lot.

PIM defines two modes: Dense Mode and sparse mode. PIM-DM (Protocol Independent Multicast Dense Mode), which is the dense mode of PIM, is suitable for the situation of small network scale and relatively concentrated multicast members. PIM-DM is defined in RFC 3973.

Steps

1.Click the navigation tree "Multicast > PIM > PIM-config" menu, enter " PIM-config " interface as shown below.



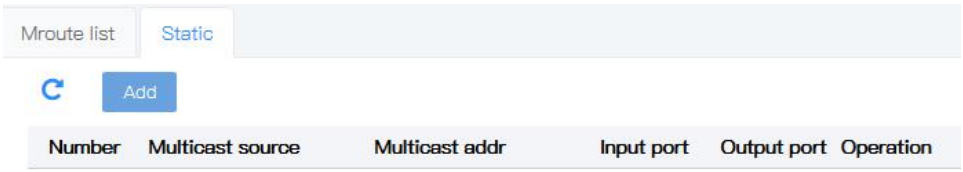
2.Fill in the appropriate configuration items.

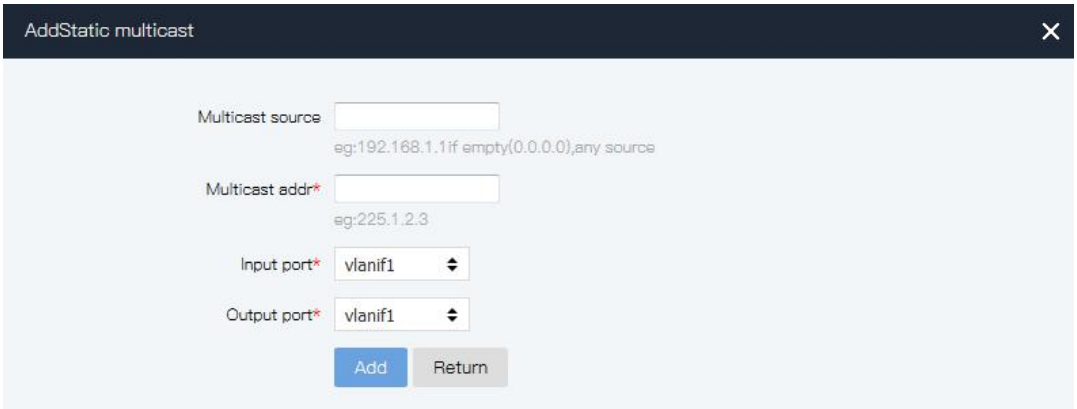
3.Click “Apply”, to complete the configuration.

8.5 Multicast Route

Steps

1.Click the navigation tree "Multicast > Multicast Route > Static, enter " Static " interface as shown below.





Interface information meaning as followings.

Configuration item	Description
Multicast source	Enter the multicast source address
Multicast address	Enter the multicast address
Input port	Multicast source input VLANIF interface
Output port	Multicast stream forwarding output VLANIF interface

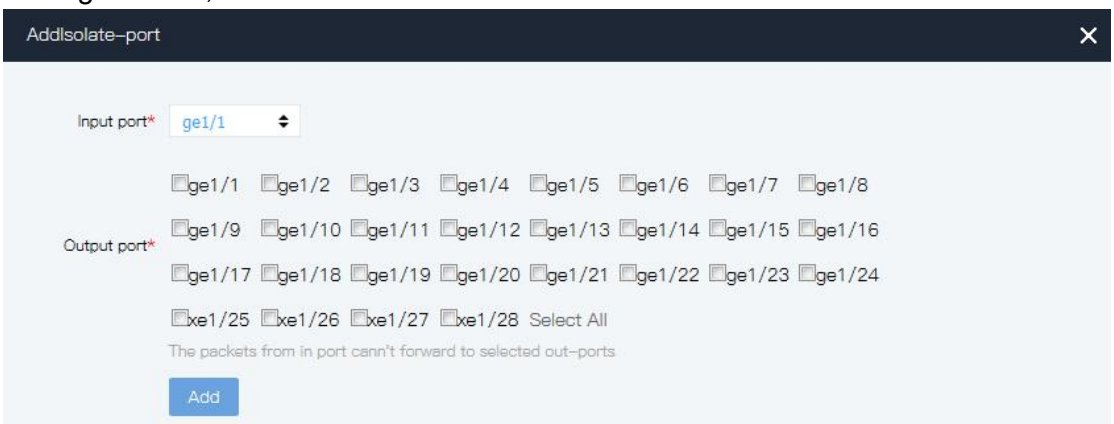
2.Fill in the appropriate configuration items.
3.Click “Add”, to complete the configuration.

9 Network security

9.1 Isolate-port

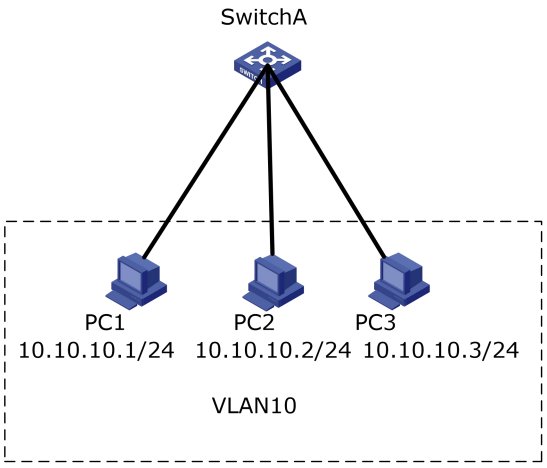
It’s isolated each other between ports in the same isolation group, not isolated between ports in different isolation groups.

Steps:
1.Click the navigation bar "Network security> Isolate-port" menu, enter " Isolate-port", established isolation group by checking the port, click the "Add" to complete the configuration, show as below.



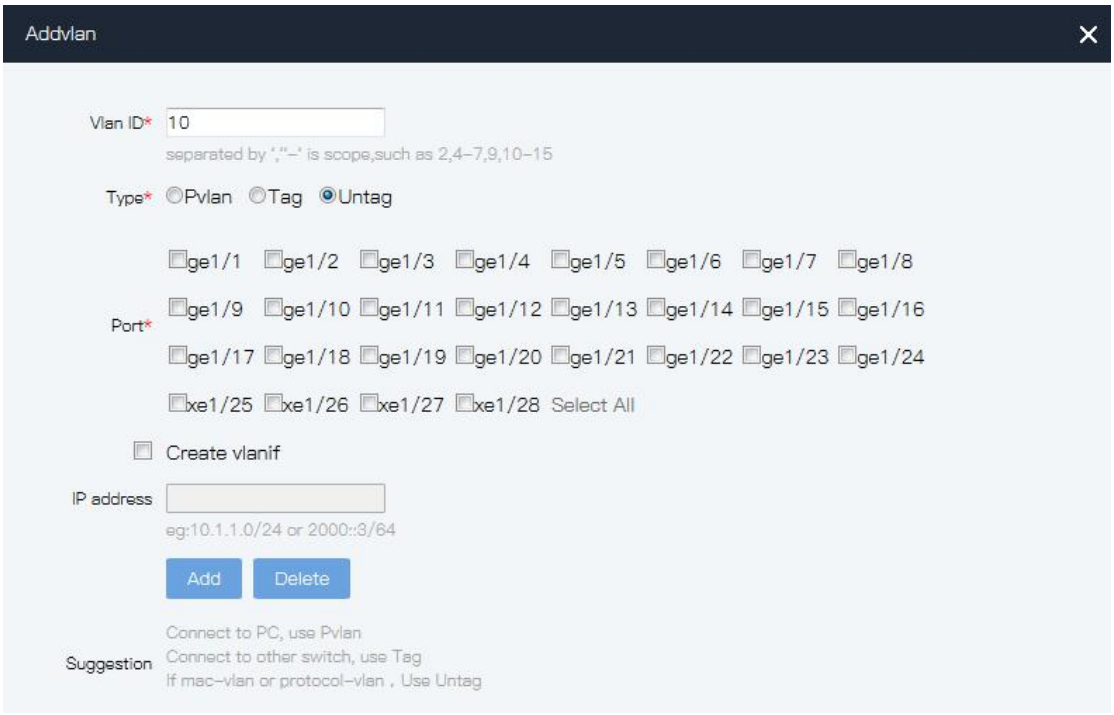
For example, show in following pic, PC1, PC2 and PC3 belong to VLAN 10, User wants PC1 and PC2 cannot access to each other in VLAN 10, PC1 and PC3 can visit each other, PC2 and PC3 can visit each other .

Configured port isolation network diagram

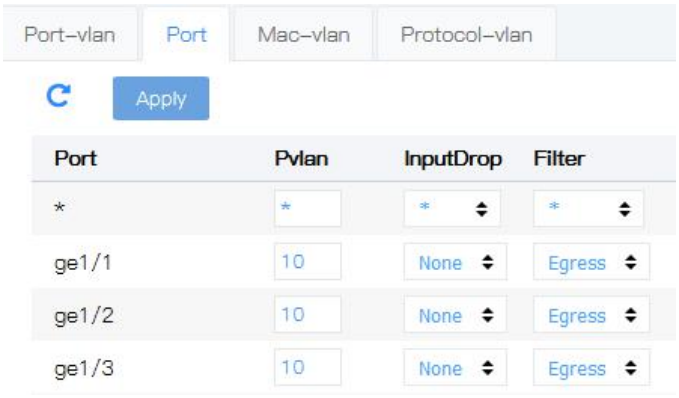


Steps:

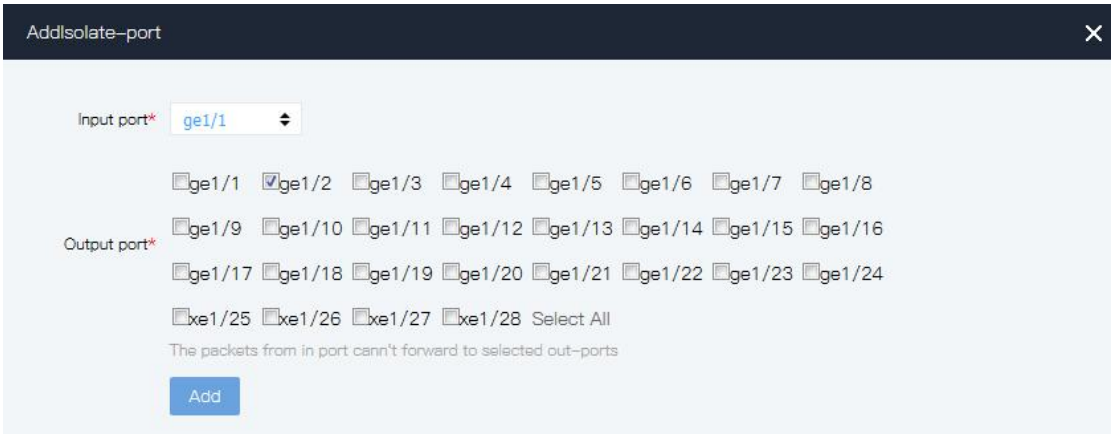
1.Creating VLAN, ensure the Vlans that belongs to PC. Click the navigation tree " Business Management > VLAN > Port-vlan" menu, enter the "Port-vlan" interface, “Vlan ID” Input”10”, Click "Add" to complete the configuration, show as below:



2.Configure Ethernet interface to join VLAN in the right way. Implement that interface allows VLAN message to pass. Click the navigation tree " Business Management > VLAN > Port" menu, enter " Port" interface, select “ge1/1, ge1/2, ge1/3”, change the number in the “PVID” to”10”, click “Apply" to complete the configuration, shown as below.



3.Configure port ge1 / 1, ge1 / 2 isolation function, Click the navigation bar "Network security > Isolate-port Config" menu, enter "Isolate-port Config ", Tick port ge1/1, ge1/2 to establish isolation group, click “Add” to complete the configuration, show as below



4.Verify the configuration.
PC1 & PC2 can’t ping each other.
PC1 & PC3can ping each other.
PC2 & PC3 can ping each other

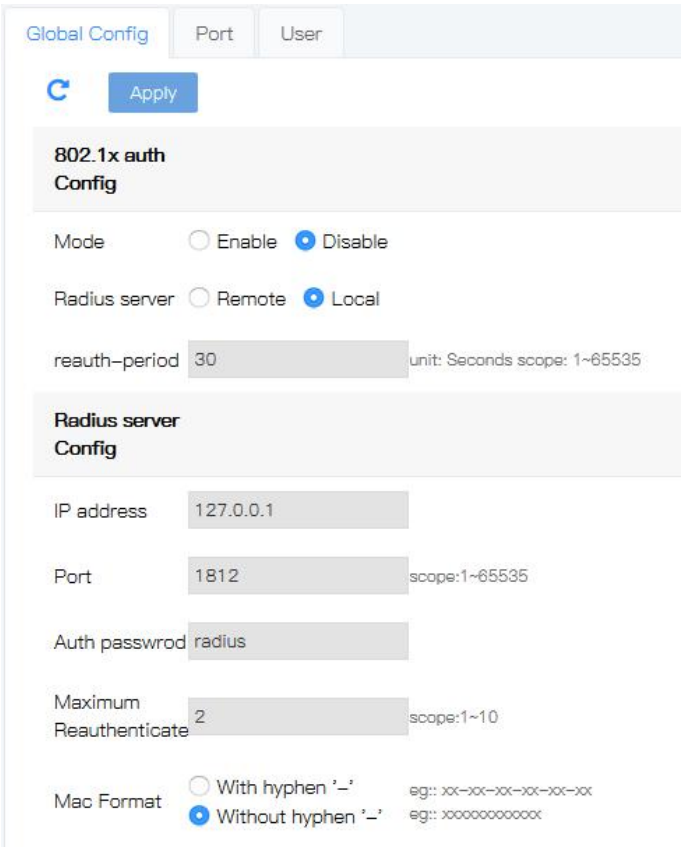
9.2 802.1X

802.1x protocol is an access control and authentication protocol based on client / server. It can restrict unauthorized users / devices from accessing LAN / WLAN through access port. 802.1x authenticates users / devices connected to switch ports before acquiring various services provided by switches or LANs. Before passing the authentication, 802.1x only allows eapol (extended authentication protocol based on LAN) data to pass through the switch port connected by the device; after passing the authentication, normal data can pass through the Ethernet port smoothly.

9.2.1 Global Config

Steps:

1.Click in the navigation tree "Network Security > 802.1x > Global Config" menu, enter " Global Config " screen as shown in the following figure.

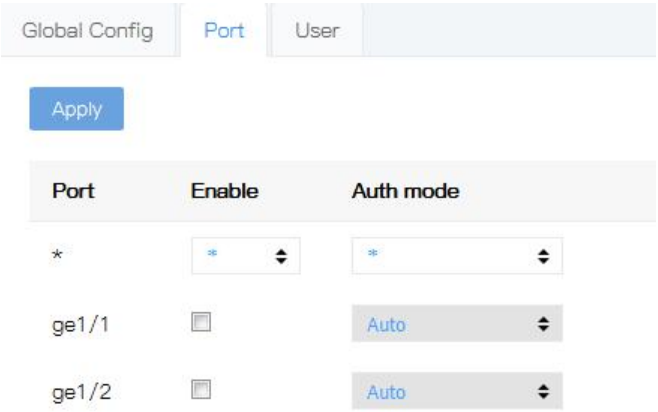


2.Fill in the corresponding configuration items and click "Apply" to complete the configuration.

9.2.2 Port Config

Steps:

1.Click in the navigation tree "Network Security > 802.1x > Port" menu, enter " Port" screen as shown in the following figure.

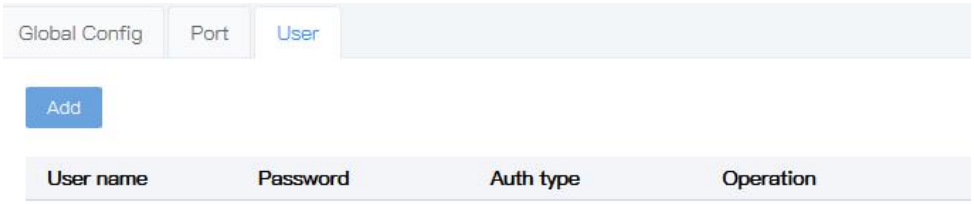


2.Fill in the corresponding configuration items and click "Apply" to complete the configuration.

9.2.3 User Config

Steps:

1.Click in the navigation tree "Network Security > 802.1x> User" menu, enter " User" screen as shown in the following figure.



2.Fill in the corresponding configuration items and click "Add" to complete the configuration.

9.3 Storm control

The basic principle of Storm control:

Storm Control prevent the broadcast, unknown multicast and unknown unicast broadcast storm by following form. The device supports storm control at these three types of messages up port by packet rate. Within a detection interval, comparing the average rate of three message of the equipment monitored interface with maximum threshold configuration, when the message rate is bigger than the configured maximum threshold, the device will storm control at this port, perform configured storm control action.

When a device's Layer 2 Ethernet interface receives the broadcast, multicast or unknown unicast message, if the device can not clear the outgoing interface of message according to the destination MAC address of the packets, the device forwards the message to other Layer 2 Ethernet interfaces in the same VLAN (Virtual Local Area Network)

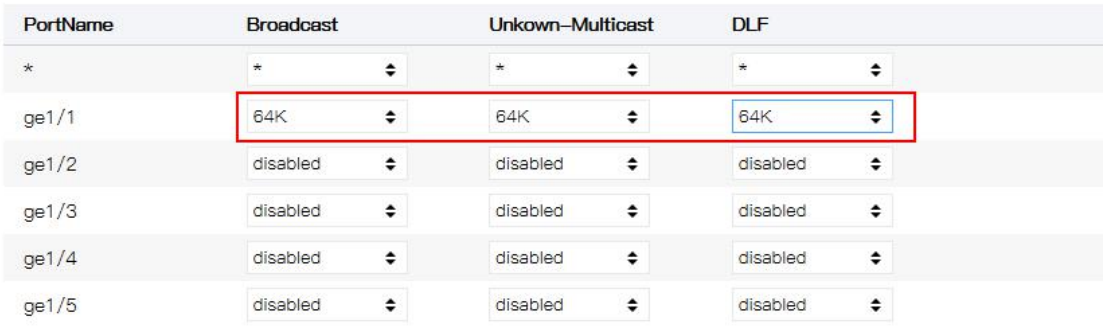
, which may cause broadcast storms, reduce the device performance.

With storm control characteristics can control three types of message flow, preventing broadcast storms.

Steps:

1.Click the navigation bar "Network security > Storm control" menu, enter the "Storm control" interface.

Configure storm control rate of Broadcast, unknow multicast, and unicast, assuming they all are 64kbps, shown as below.



9.4 ACL

With the increase of network scale and traffic control and distribution of network security has become an important part of the bandwidth for network management. Through the packet filter effectively prevents unauthorized users from accessing the network, but also can control the traffic and save network resources. ACL (Access Control List, ACL) that is configured by packets matching rules and processing operations to achieve the packet filtering function.

When a switch port receives packets of the ACL rule applied on the current port of packet fields, after identifying a message, according to preset policies permit or deny packets through.

Defined by the ACL packet matching rule it may also be required for other traffic classification function reference, such as QoS classification rules.

By setting the matching rules and processing operations, the access control list (ACL) can be realized packet filtering. ACL is applied to a collection of a series of packets permit and deny conditions. When receiving a packet on the interface, so that the switch packet fields as compared with that used in ACL, specified in the standard access list based on the determined packet is forwarded license. ACL through a series of conditions to classify packets, these conditions may be the packet's source MAC address, destination MAC address, source IP address, destination IP address and port number. ACL through a series of conditions to classify packets, these conditions can be the source address of the packet, destination address, and port number. Depending on the application purpose, it can be divided into the following ACL:

IP ACL: Rules are based on source IP address of the packet. ACL ID range: 100 to 999.

MAC ACL: rules based on the source MAC address of the packet, the destination MAC address, 802.1p priority, and link layer protocol type 2 information. ACL ID range: 1 to 99.

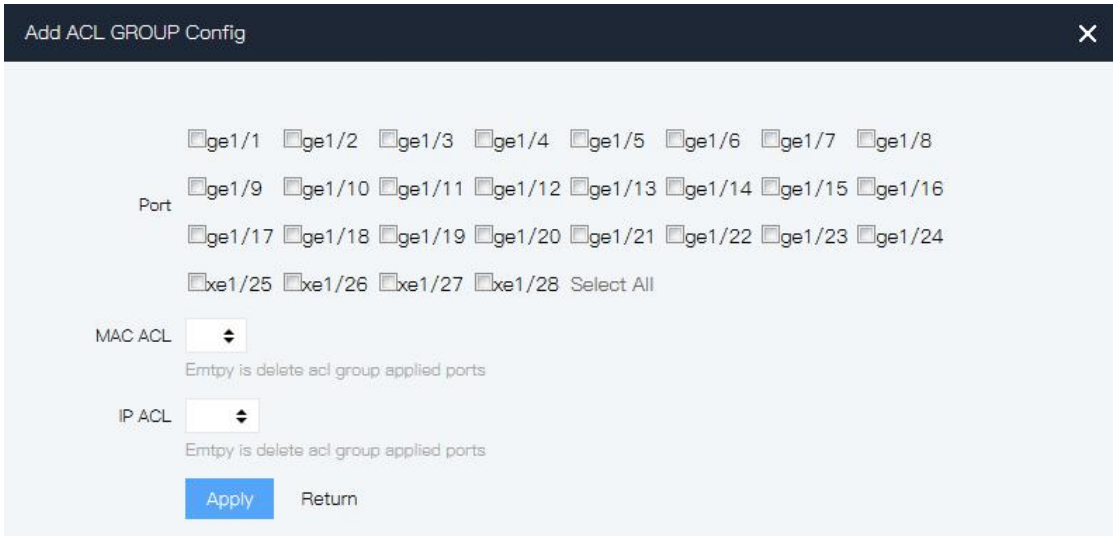
9.5.1 ACL GROUP Config

After the table is created, then it must also apply it to everyone who wants to use it on the interface

Steps:

1.Click in the navigation tree "Network Security > ACL Config> ACL GROUP Config" menu,

enter "ACL GROUP Config" screen as shown below.

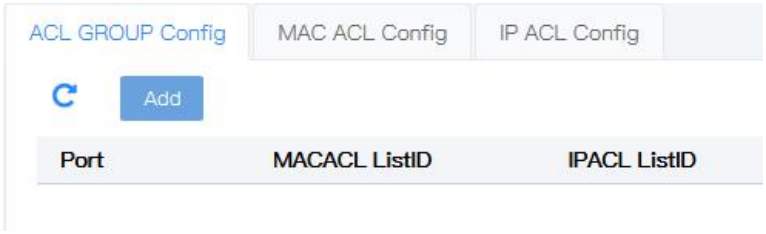


Interface information meaning as followings.

Configuration item	Description
MACACL list ID	Already created MAC access list applied to the port ID
IPACL list ID	Already created IP access list applied to the port ID

2.Fill in the appropriate configuration items to create good acl 1 and acl 100 as an example, are applied to the ge1 / 1 and ge1 /

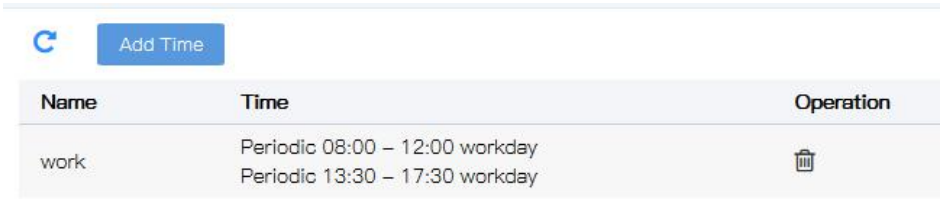
3.Click "Apply" to complete the configuration, as shown in FIG.



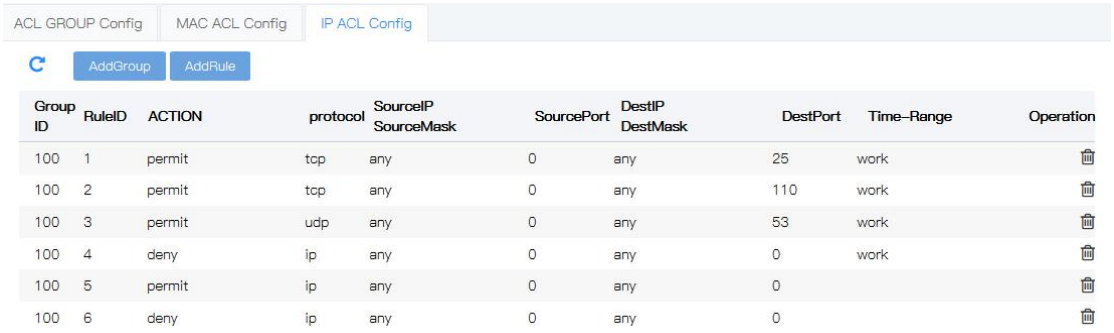
Here is an example to illustrate the definition of the method of time-based ACL. If you want to use a unit-based ACL on the switch in time to achieve: Monday to Friday (working days) from 8:00 am to 12:00 pm from 13:30 to 17:30 only allow users to receive and send mail, non-working time allowed all access.

Steps:

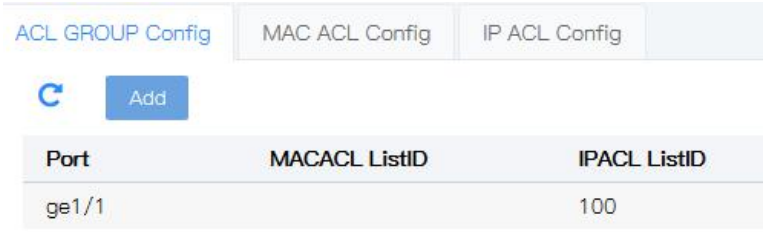
1. Define the time range. Click in the navigation tree "Extend Management > TIME RANGE Config" menu, enter "TIME RANGE Config" screen, choose to create a "cycle time", respectively, enter Monday to Friday (working days) from 8:00 am to 12:00 pm from 13:30 to 17:30, as shown below.



2. Edit the ACL. Click in the navigation tree "Network Security> ACL Config> IP ACL Config" menu, enter "IP ACL Config" screen, respectively, create the following five ACL, as shown below.



3. Call an ACL, ACL100 applied to ge1 / 1. Click in the navigation tree "Network Security> ACL Config> ACL GROUP Config" menu, enter "ACL GROUP Config" screen, as shown below.

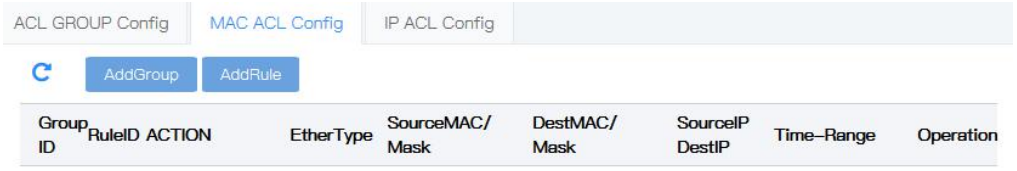


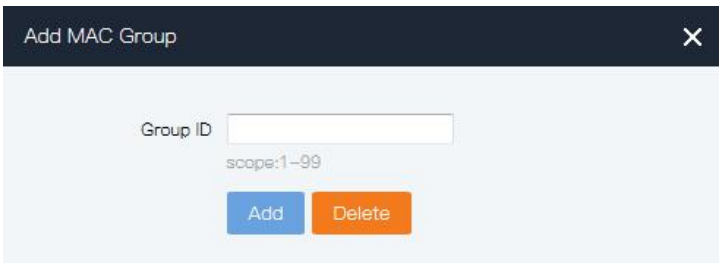
9.5.2 MAC ALC Config

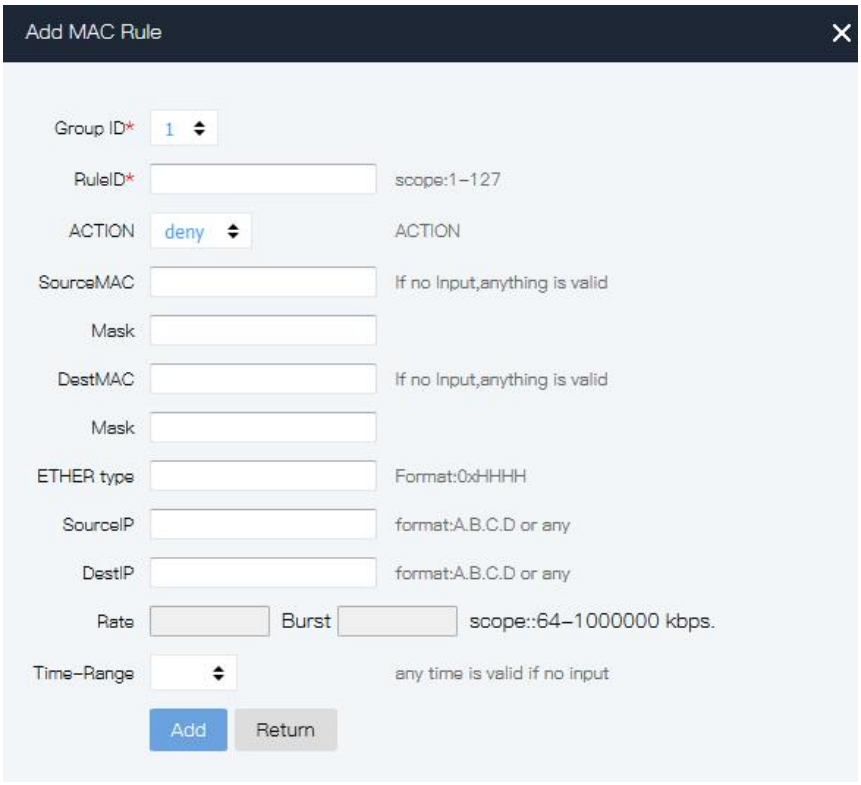
MAC ACL: rules based on source MAC address, destination MAC address, VLAN priority, and link layer protocol type 2 information.

Steps:

1.Click in the navigation tree "Network Security > ACL Config> MAC ACL Config" menu, enter "MAC ACL Config" screen as shown in the following figure.





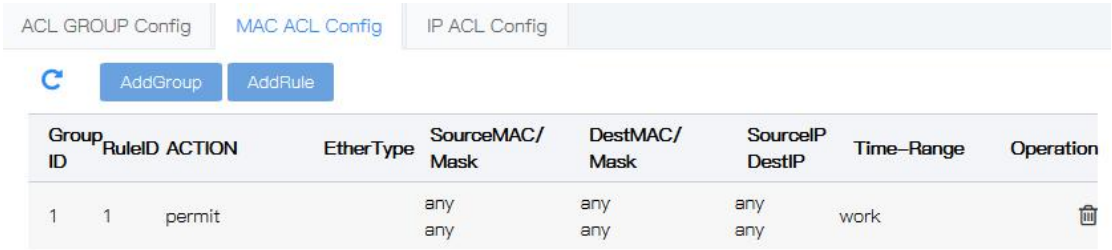


Interface information meaning as followings.

Configuration item	Description
Group ID	MAC ACL ranges: 1-99
Rule	Each rule represents the number range is: 1-127
Action	ACL rules are divided into "permit" (allow) the rules or "deny" (reject) rules.
Source MAC	ACL rule source MAC address. Format for the H-H.
Dest MAC	ACL rule destination MAC address. Format for the H-H.
Time-Range name	Enter the configured time range name.

2.Fill in the appropriate configuration items.

3.Click "Add" to complete the configuration, as shown in FIG.



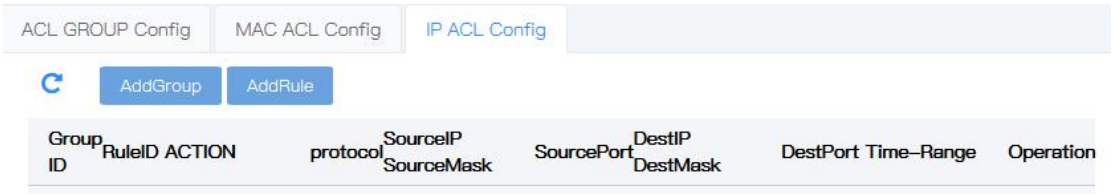
9.5.3 IP ALC Config

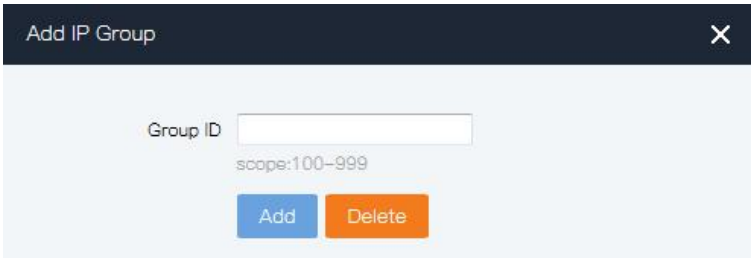
IP ACL (Basic IP ACL): Rules are based on source IP address of the packet. ACL ID range:

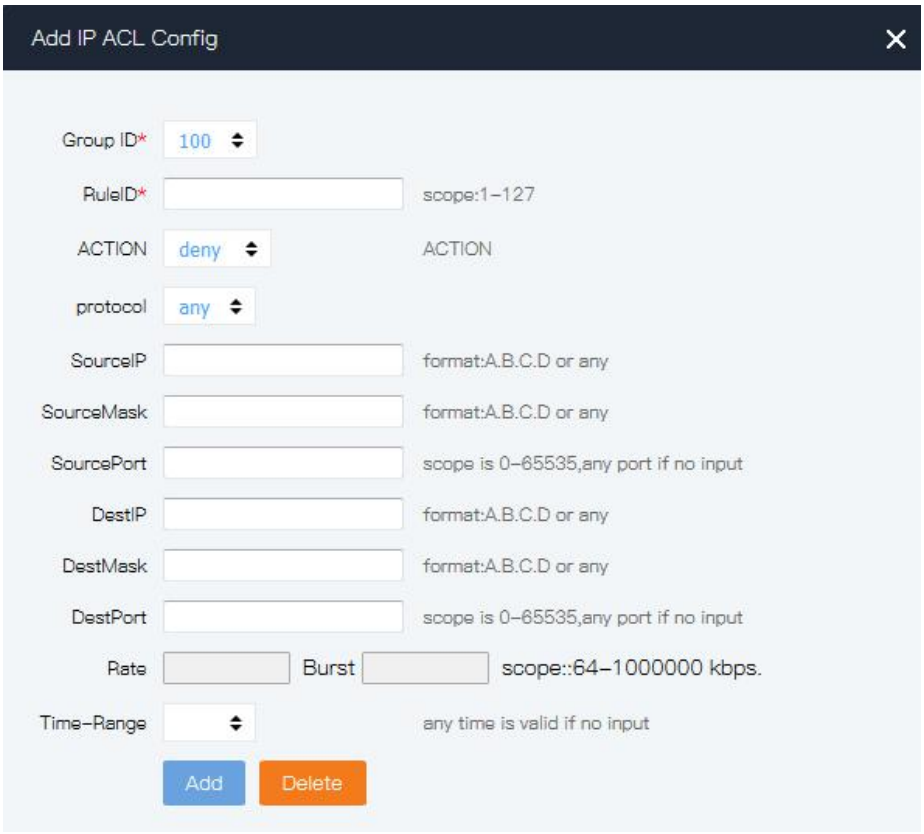
100 to 999.

Steps:

1.Click in the navigation tree "Network Security > ACL Config> IP ACL Config" menu, enter "IP ACL Config" screen as shown in the following figure.





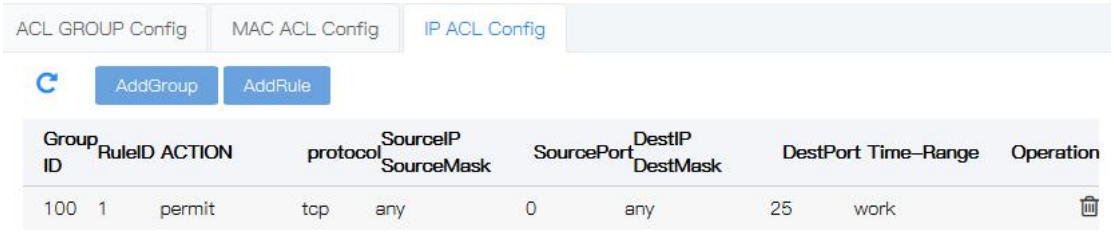


Interface information meaning as followings.

Config item	description
Group ID	IP ACL ranges: 100-999
Rule ID	Each rule represents the number range is: 1-127
Action	ACL rules are divided into "permit" (allow) the rules or "deny" (reject) rules.
protocol	Required, select the type of protocol. Any, icmp,

	icmp, ip, tcp, udp
Source IP	Enter the source IP ACL rule
Source mask	ACL rule source mask
Source port	Enter the source port of ACL rule
Destination IP	Enter Destination IP of ACL rule
Destination mask	Enter the destination mask of ACL rule
Destination port	Enter the destination port ACL rule
Time-Range name	Enter the configured time range name.

2.Fill in the appropriate configuration items.
3.Click "Add" to complete the configuration, as shown in FIG.

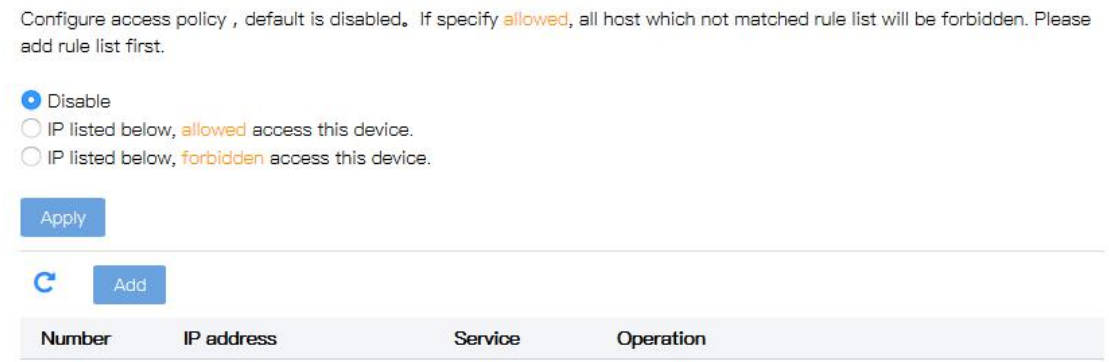


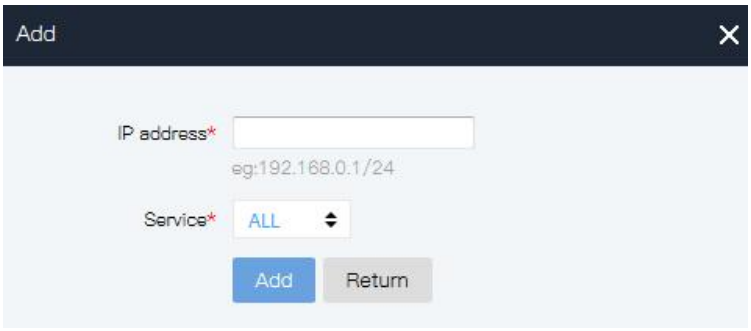
9.5 Access control

With the increase of network scale and traffic control and distribution of network security has become an important part of the bandwidth for network management. Through the packet filter effectively prevents unauthorized users from accessing the network, but also can control the traffic and save network resources. ACL (Access Control List, ACL) that is configured by packets matching rules and processing operations to achieve the packet filtering function.
Next, switch the filtering rules and access rules

Steps

1. Click the navigation tree "Network Security > Access Control" menu, enter "Access Control" interface as shown below.





Interface information meaning as following.

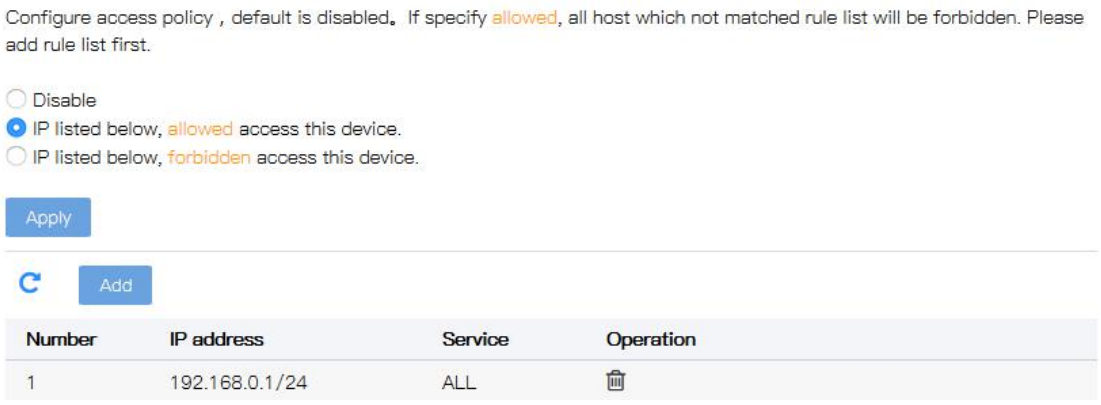
Configuration item	Sub-Option	Description
Configure access policy	Disable	Disable by default
	Host who meet the following rules to allow access to the corresponding service equipment	
	Host who meet the following rules to prohibit access to the corresponding service equipment	
Configure access rule for system	IP address	Enter the IP address
	serve	All inculding http and telnet

Attention

Disabled by default. If set to allow, not in the list of rules would prohibit all access. Please add the rule, and then set access rules, or it may cause the current cannot access the web.

2. First set up the device access rules, click the navigation tree "Network Security > Access Control " menu, enter the IP address 192.168.1.10/24, service options all, click "Add" As shown below:

3. then setting filter rules, click the navigation tree "Network security > Access Control" menu, select here "where the hosts meet the following rules to allow the device to access the appropriate services," click " Apply "to complete the configuration, as shown below:



9.6 Attack protection

To improve the security of the switch, you can turn the switch attack prevention options

Steps

1. Choose the "Network Security > Attack protection" menu, enter " Attack protection ", respectively, to enable "ignore ping ", "SYN DOS ATTACK", click" Apply "to complete the configuration interface as shown below.

Interface information meaning as followings.

Configuration item	Description
Ignore ping	Ignore ping attacks
SYN DOS attack	TCP SYN attack prevention

9.7 Alarm

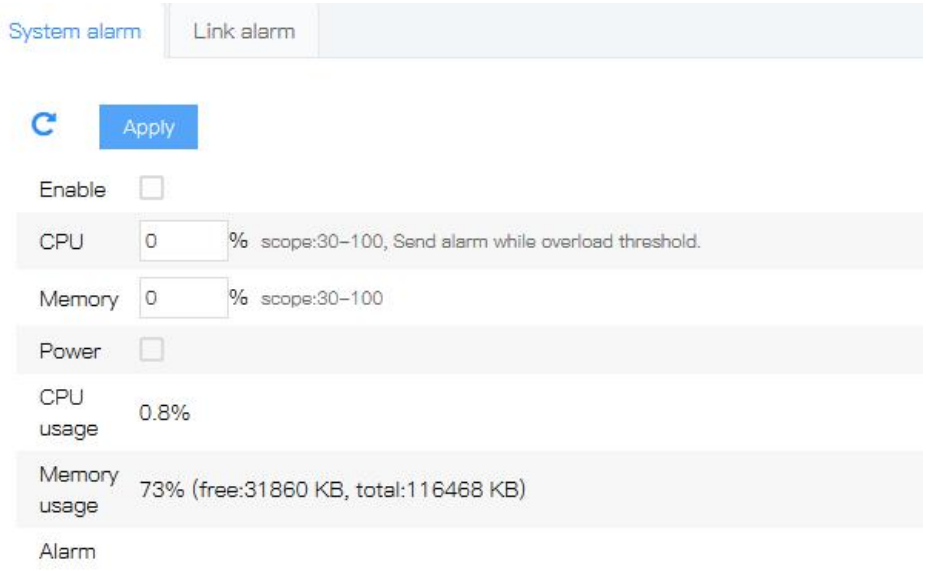
The system provides two alarm configurations of system alarm and link alarm to simplify operation and maintenance.

9.7.1 System alarm

System alarm includes CPU and memory over threshold alarm

Steps:

1.Click in the navigation tree "Network Security > Alarm > System alarm" menu, enter " System alarm " screen as shown in the following figure.



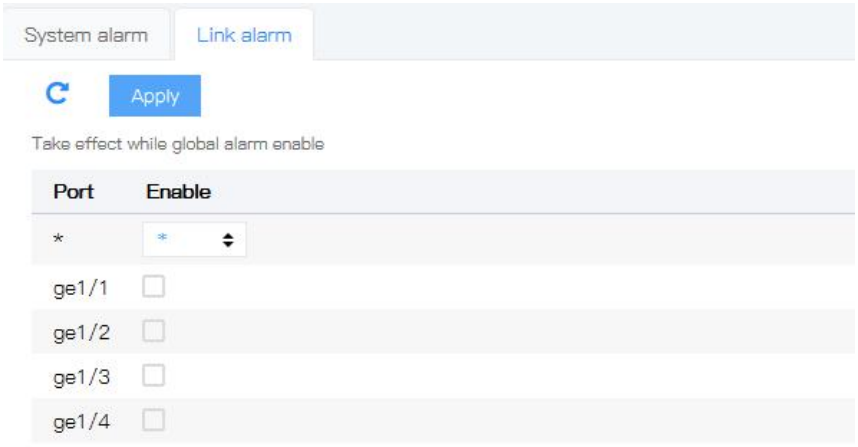
2.Fill in the corresponding configuration items and click "Apply" to complete the configuration.

9.7.2 Link alarm

The system alarm is enabled and effective. When the link is down, an alarm is generated and an alarm icon is displayed at the top

Steps:

1.Click in the navigation tree "Network Security > Alarm > Link alarm" menu, enter " Link alarm " screen as shown in the following figure.



2.Fill in the corresponding configuration items and click "Apply" to complete the configuration.

10 QoS

QoS (Quality of Service) is used to assess the ability to meet customer demand for services in the Internet, QoS is used to assess the ability of the service network to transmit

packets. The network provides are diverse, and therefore can be evaluated based on different aspects. Commonly referred to as QoS, is the evaluation of packet delivery process can provide support for the bandwidth, delay, jitter, packet loss and other core demand service capabilities. Bandwidth, also called throughput represents the average rate of traffic flow within a certain period of time, usually expressed kbit/s. Delay, represents the average time when traffic across the network requires. For a network device, the requirements will generally be understood to several delay classes. For example, it is divided into two grades delay, so that high-priority traffic by priority queue scheduling method as fast as possible to get the service, and the low priority traffic is no need to wait for high-priority traffic to get service. Jitter, showing changes in traffic flow across the network time. Packet loss rate, indicating traffic flow in the course of transmission loss ratio. Because modern transport system with high reliability, loss of information tends to occur when the network is congested. The most common cause is queue overflow packet loss.

In the traditional IP network, all packets are treated equally without priority difference, each network device for all the packets are made of first-in first-out strategy to process its utmost efforts (Best-Effort) will be reported message to the destination, but the reliability of packet transmission, transmission delay, and so does not provide any guarantee.

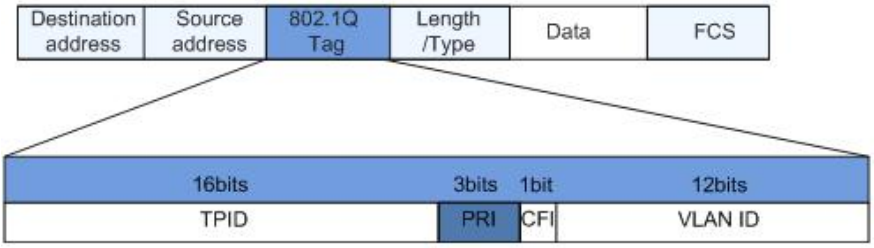
The rapid development of the network, the IP network with new applications emerging, service quality IP network also made new demands. Such as VoIP and video transmission delay for delay-sensitive traffic packets put forward higher requirements. If the packet transfer delay is too long, it will be unacceptable to the user. In order to support voice, video and data services with different service requirements, it requires the network can distinguish different types of business, and then to provide them with appropriate services. Traditional IP network services impossible to identify and try to distinguish between the various network traffic types, and have the ability to distinguish what type of business to provide differentiated services for different business premise, so the traditional network model can not meet the best service applications. QoS technologies will emerge to address this problem. QoS can regulate network traffic, manage network congestion and to avoid, reduce packet loss rate. At the same time as providing dedicated bandwidth, provide different services for different quality of services, etc., to improve the service capacity of the network.

Different packets using different QoS priorities, such as VLAN packets using 802.1p, or called CoS (Class of Service) field, IP packets DSCP. When the packets pass through different networks, in order to maintain the priority of the packets, you need to configure the mapping between these priorities in the fields connected to different network gateway.

VLAN frame header 802.1p priority

Typically the interaction between the two-story frame VLAN devices. Defined according to IEEE 802.1Q, VLAN header PRI field (ie, 802.1p priority), also known as CoS (Class of Service) field that identifies the quality of service requirements.

VLAN frame 802.1p priority

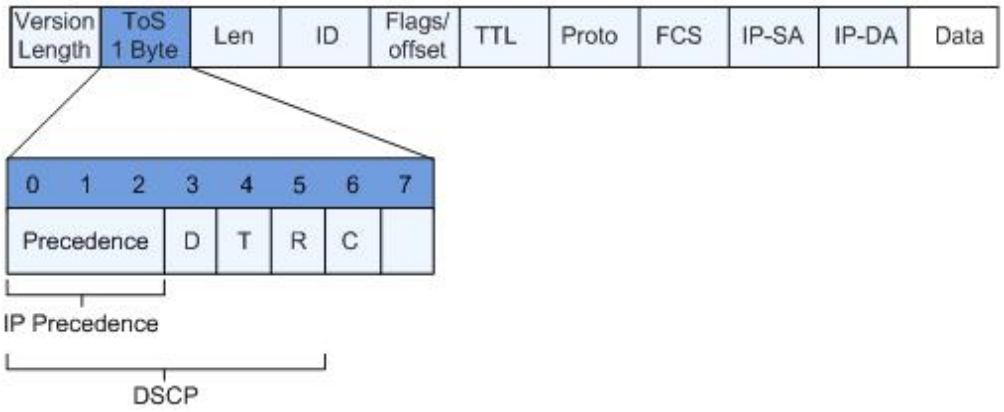


PRI field contains 3 bits long in the 802.1Q header. PRI field defines eight business priorities CoS, in priority order from highest to lowest value of 7,6, ..., 1 and 0.

IP Precedence / DSCP field

791 according to the definition of RFC, IP header ToS (Type of Service) field consists of eight bits, of which three-bit Precedence field identifies priorities, as shown in IP packets Precedence position telegram.

IP Precedence/DSCP field



Bit 0-2 expressed Precedence field, on behalf of packets transmitted eight priorities, in descending order of priority value of 7,6, ..., 1 and 0. The highest priority is 6 or 7, often choose or update the network routing control communication reserved, user-level application can only use level 0 to 5.

Precedence field in addition to outside, ToS field also includes D, T, R three bits: D bits represents delay requirements (Delay, 0 represents a normal delay, 1 represents a low latency). T bit represents throughput (Throughput, 0 represents a normal throughput, represents a high throughput). R represents a bit reliability (Reliability, 0 represents normal reliability, represents high reliability). ToS field bit 6 and 7 reserved.

RFC1349 redefines the IP packets in the ToS field, an increase of C bits indicating transport overhead (Monetary Cost). After, IETF DiffServ working group in RFC2474 bit IPv4 packet header ToS field 0-5 redefined as DSCP, ToS field and renamed DS (Differentiated Service) bytes. DSCP location in the message as shown above.

Before 6 DS field (0 ~ 5) is used as Differentiated Services Code Point DSCP (DS Code Point), high 2 (6, 7) are reserved. Low DS field 3 (0 ~ 2) is a class selector code points CSCP (Class Selector Code Point), the same CSCP value represents a class of DSCP. DS node selects PHB (Per-Hop Behavior) according to the DSCP value.

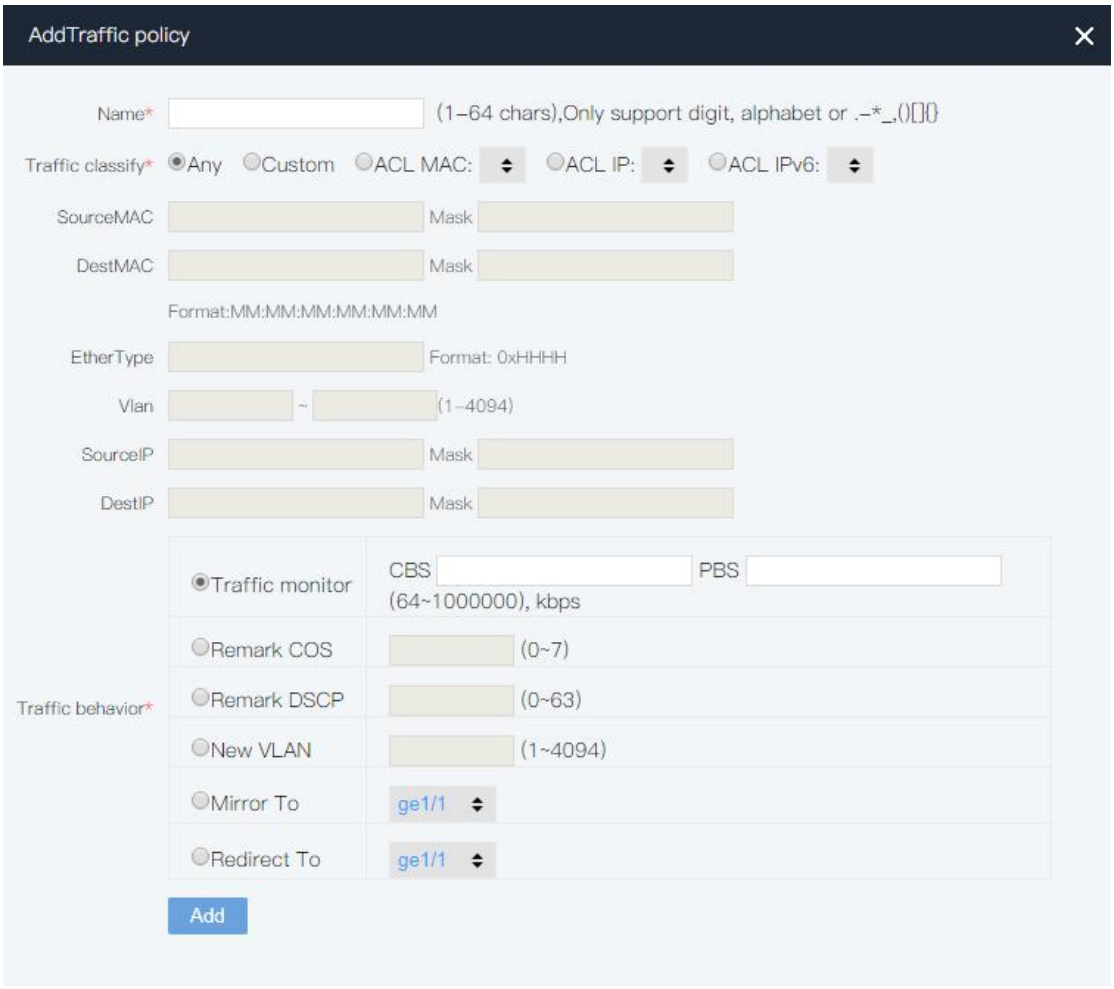
10.1 Traffic management

Based on the flow policy, the matching rules of the fields related to the flow information are

formulated, and the priority, VLAN and DSCP equivalent of the interface flow are retagged based on the interface binding to realize the flow redirection and forwarding

Steps:

1. Choose the " QOS > Traffic management > Traffic policy" menu, go to " Traffic policy " screen, as shown below.



1.Fill in the corresponding configuration items and click "Add" to complete the configuration.

10.2 Port rate-Limit

Configuring the interface speed is that limiting the rate of physical interface sending

outward or receiving data inward.

Background Information

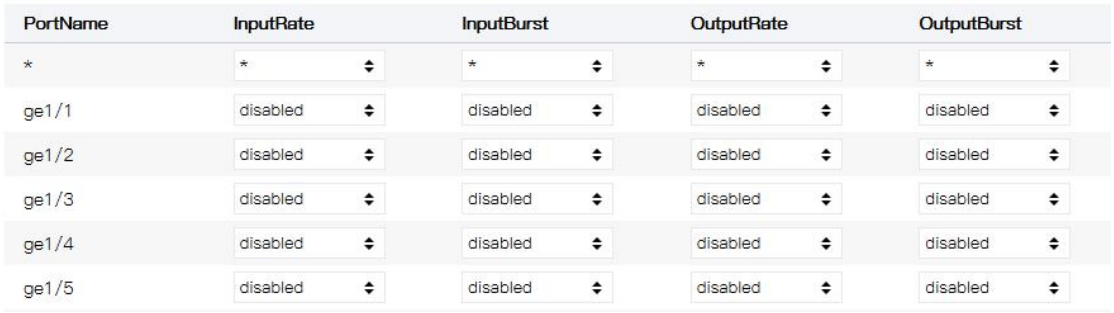
Before the flow sent out from port, Configuring the speed limit in the export direction of interface to control all flowing out message flows.

Before the flow received from port, Configuring the speed limit in entrance direction of interface to control all flowing out message flows.

Steps

1.Click the navigation bar "QOS > Port rate-Limit" menu, enter "Port rate-Limit" interface.

2.Input the value of port rate-limit configuration, and then click the "Apply", shown as below.



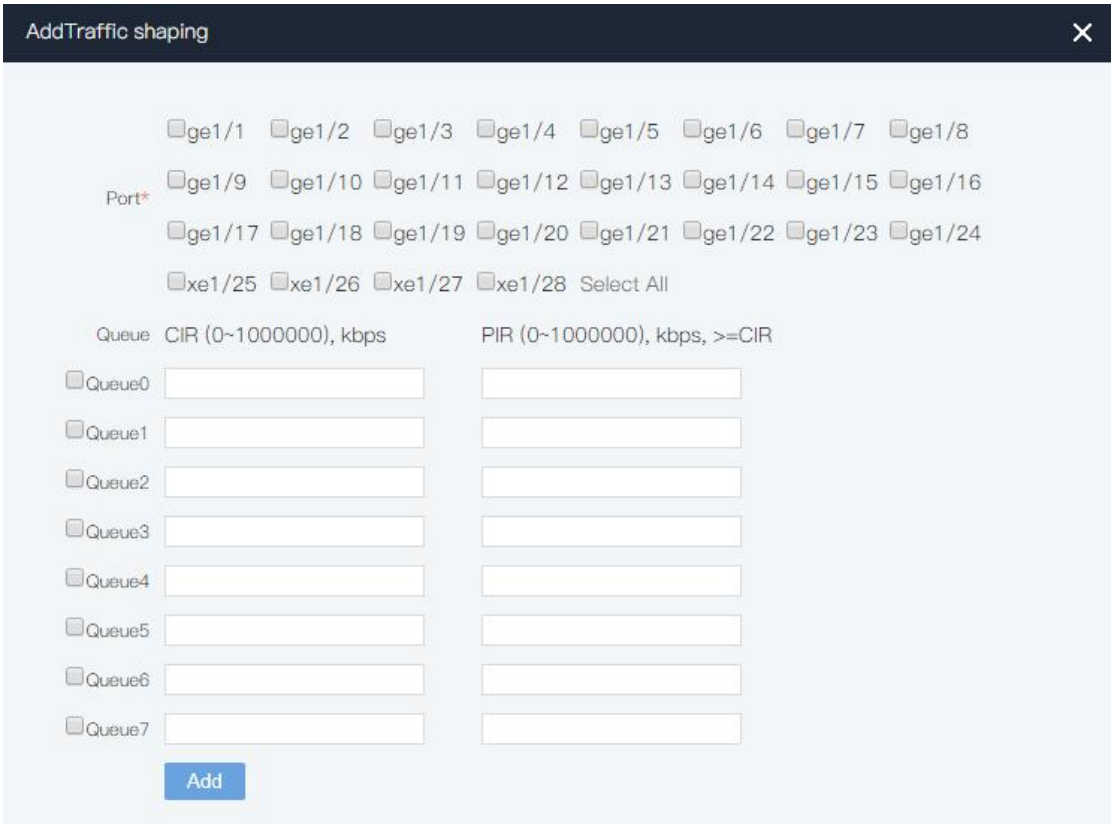
Configuration Parameter Description

Configuration Item		Description
Entrance direction of port	Entrance direction Rate	Input CIR of entrance direction. The range is disable,64kbps-800Mbps.
	Entrance direction Burst	Input CBS of entrance direction. The range is disable,64kbps-800Mbps.
Export direction of port	Export direction rate	Input CIR of export direction. The range is disable,64kbps-800Mbps.
	Export direction Burst	Input CBS of export direction. The range is disable,64kbps-800Mbps.

10.3 Traffic shaping

Steps:

2. Choose the " QOS > Traffic shaping " menu, go to " Traffic shaping " screen, as shown below.



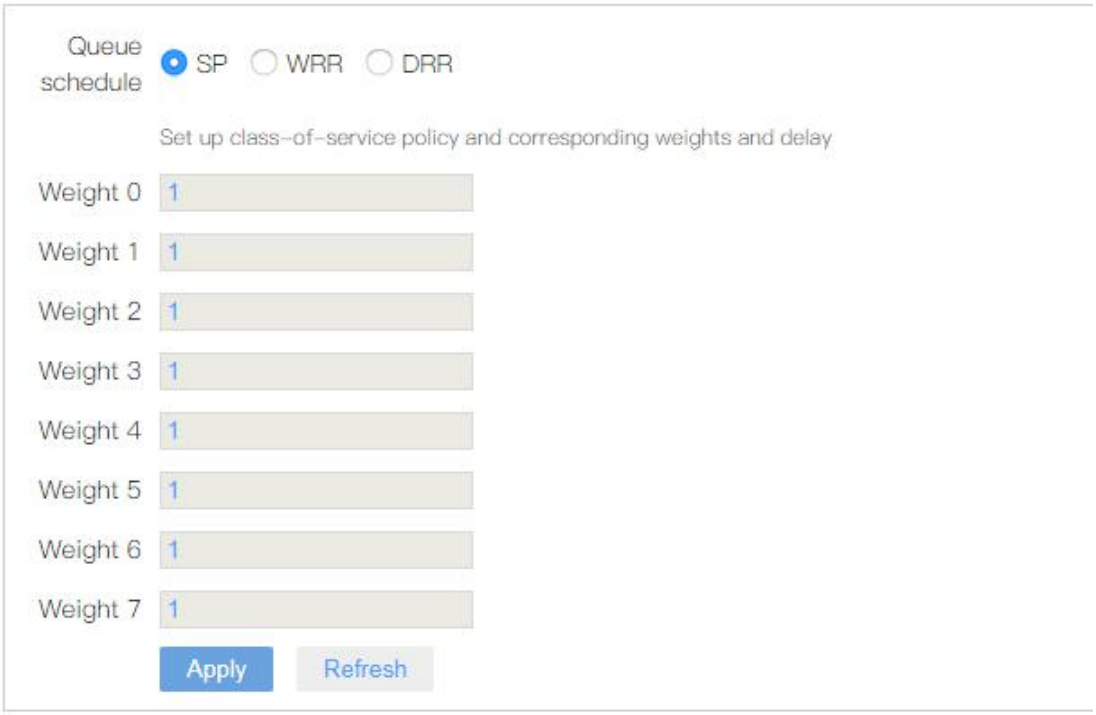
2.Fill in the corresponding configuration items and click "Add" to complete the configuration.

10.4 Congestion management

When congestion occurs, several packets compete for resources issues, usually through queue scheduling to be addressed. Congestion management uses the queue scheduling techniques to avoid network congestion occurs intermittently. Queue scheduling technologies include: SP (Strict-Priority, strict priority queue) and WRR (Weighted Round Robin, WRR queue), DRR scheduling (DRR (Deficit Round Robin) scheduling RR is also extended).

Steps:

1. Choose the " QOS > Congestion management" menu, go to " Congestion management " screen, as shown below.



Interface information meaning as following.

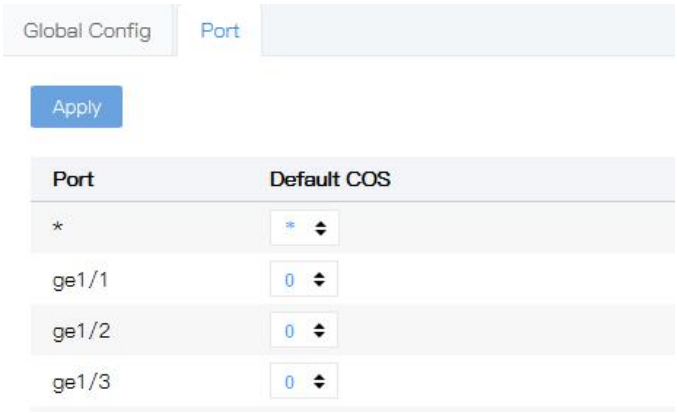
Config item	Description
SP	SP queue scheduling algorithm, for mission-critical application design. There is an important business-critical features, that is, when congestion occurs require preferential service to reduce the response delay. In the port there are eight output queues on the priority queue 8 output port queue into eight classes, followed 7,6,5,4,3,2,1,0 queue, Their priority in Descending order.
WRR	WRR queue scheduling algorithm scheduling queues in turn to ensure that every queue can be served for a certain time. In the port there are eight output queues, WRR can configure a weighted value (queue7 ~ queue0 corresponding weights were w7, w6, w5, w4, w3, w2, w1, w0) for each queue
DRR	DRR DRR (Deficit Round Robin) scheduling is also extended RR, relative to the WRR to words, to solve the WRR concerned only with packets, the actual bandwidth equal scheduling chance of large-size packets are greater than the bandwidth of the small size of the packets obtained problem by scheduling process takes into account factors packet length to achieve the rate scheduling fairness.

2. Fill in the corresponding configuration items and click "Apply" to complete the configuration.

10.5 Default Priority

QOS port configuration Procedure

1.Click in the navigation tree " QOS > Default Priority" menu, enter the " Default Priority " screen, and click "Apply" to complete the configuration, as shown below.



Interface information meaning as followings

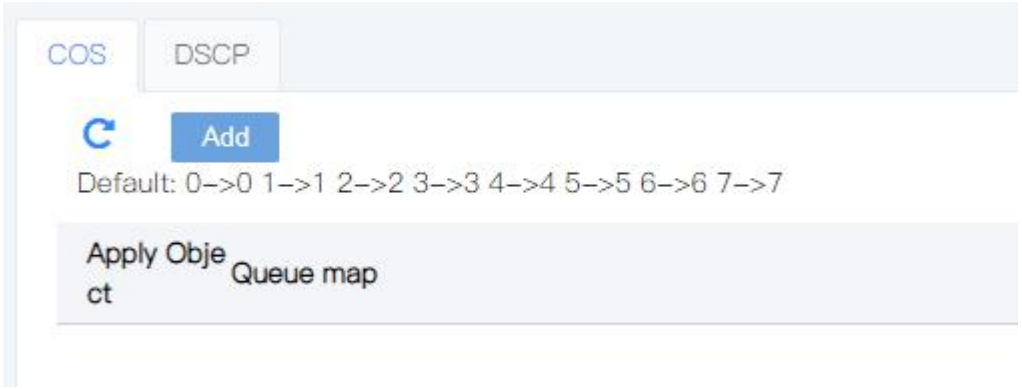
Config item	Description
Port	You can choose multiple ports
Default cos	Range from0-7

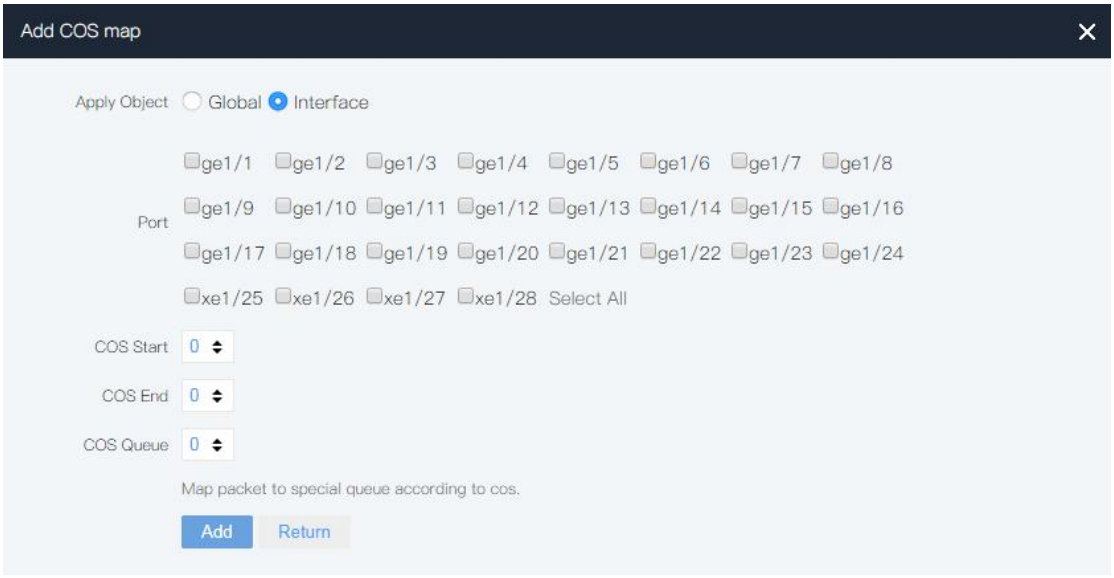
2. Fill in the corresponding configuration items and click "Apply" to complete the configuration.

10.6 Priority map

Steps:

1.Click in the navigation tree " QOS > Priority map" menu, enter the " Priority map " screen, and click "Add" to complete the configuration, as shown below.





2. Fill in the corresponding configuration items and click "Add" to complete the configuration.

11 Extend Management

11.1 ONVIF

ONVIF (open network video interface Forum) is a global open industry forum, whose goal is to promote the development and use of global open standards for physical IP based security product interfaces. ONVIF creates a standard for how IP products in video surveillance and other physical security fields communicate with each other. ONVIF was founded in 2008 by axis communications, Bosch Security Systems and Sony.

Advantages of open standards

- **Interoperability**

Products from different manufacturers can be used in the same system and in the same language;

- **Flexibility**

End users and integrators can use technologies and solutions from different manufacturers;

- **Forward looking**

No matter how the market develops, ensure to provide products with interoperability.

Steps

Click in the navigation tree "Extend Management > ONVIF " menu, enter " ONVIF " screen,

as shown below.

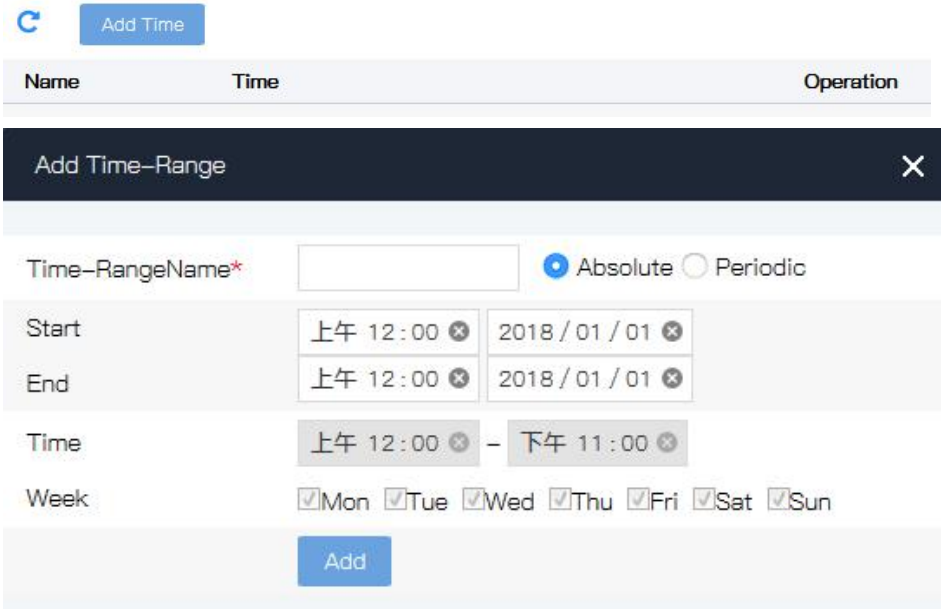
2. Click "discovery" to automatically discover IP cameras.

11.2 Time Range Config

Configuring effective period of time allows the user to distinguish packets ACL.
It is used to describe a particular period of time. Users may have such a demand: Some ACL rules to take effect within a certain time or while at other times they are not for packet filtering, known as filtered by time period use. In this case, the user can configure one or more time periods, and then refer to the time period when configuring ACL rules to implement filtering based on ACL period.
Time ranges are the following: periodic time ranges and absolute time period. Periodic time range is in the form of days of the week; absolute time range using the start time and the end time.

Steps

Click in the navigation tree "Extend Management > Time Range Config" menu, enter "Time Range Config " screen, as shown below.

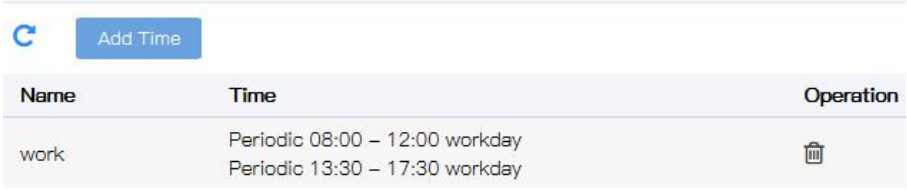


Interface information meaning as following.

Configuration	Description
Time-Range name	Enter the Time-Range name, an optional (absolute time and cycle time)

Start-end	Absolute time range using the start time and the end time. You can configure multiple absolute time period may not be an absolute time range.
Time week	Periodic time range is in the form of the week every week. You can configure multiple cycle periods may not configure the cycle time period

2.Fill in the appropriate configuration items.
3.Click "Add" to complete the configuration, as shown in FIG.

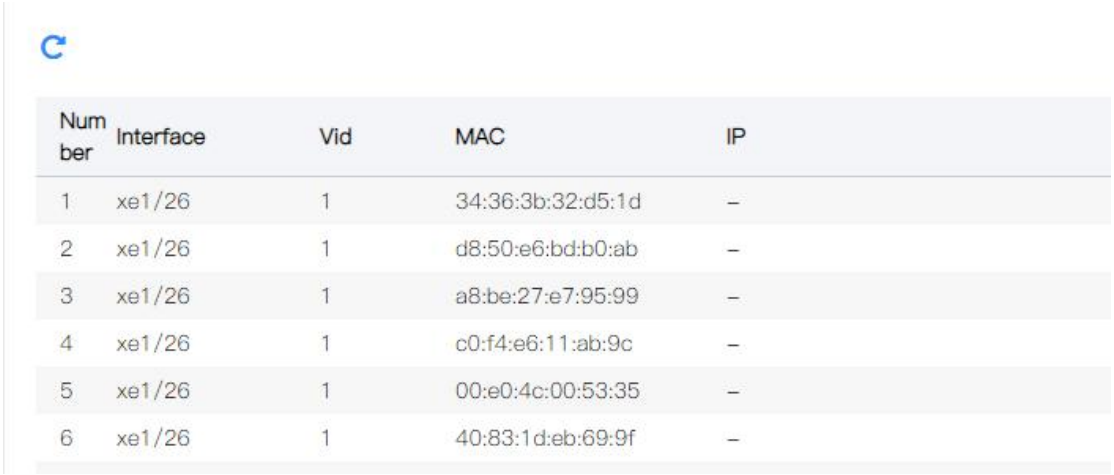


11.3 Devices

Used to query system Mac and IP corresponding table entries

Steps

Click in the navigation tree "Extend Management > Devices" menu, enter " Devices " screen, as shown below.

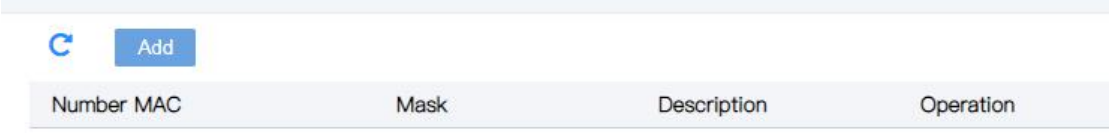


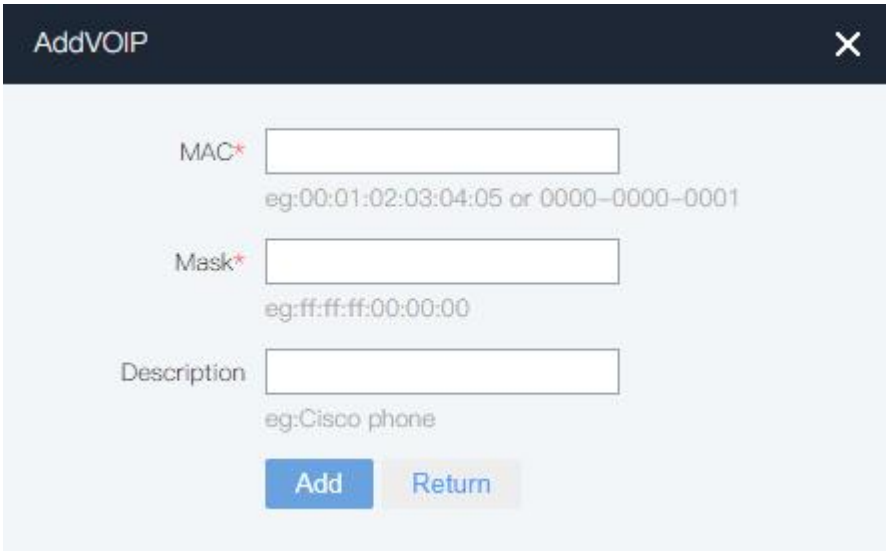
Number	Interface	Vid	MAC	IP
1	xe1/26	1	34:36:3b:32:d5:1d	–
2	xe1/26	1	d8:50:e6:bd:b0:ab	–
3	xe1/26	1	a8:be:27:e7:95:99	–
4	xe1/26	1	c0:f4:e6:11:ab:9c	–
5	xe1/26	1	00:e0:4c:00:53:35	–
6	xe1/26	1	40:83:1d:eb:69:9f	–

11.4 VOIP

Steps

Click in the navigation tree "Extend Management > VOIP" menu, enter " VOIP " screen, as shown below.





2. Fill in the corresponding configuration items and click "Add" to complete the configuration.

11.5 Diagnosis

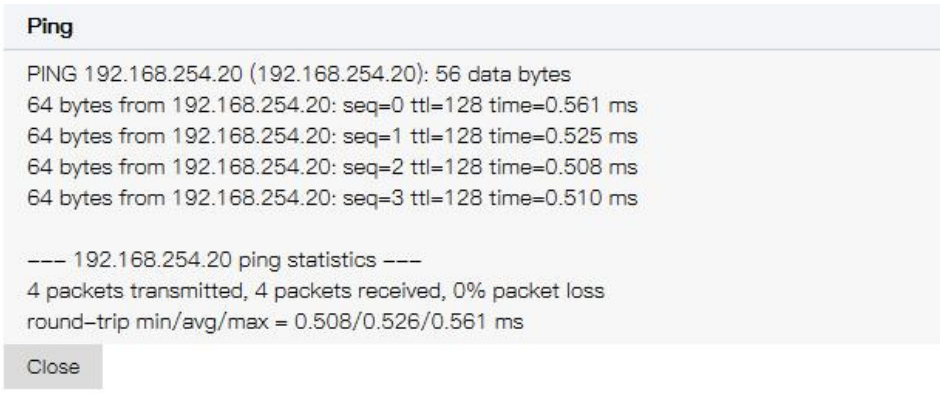
11.5.1 Ping

ping command is used for check the IPv4 address is reachable or not, and output the corresponding statistics information.

Steps:

1.Click the navigation bar "Extend Management > Diagnosis" menu, enter " Diagnosis " screen. click the "ping", input the IP address. It's shown as below.

2.Click "Test", the user can see, shown as below.



11.5.2 Traceroute

Traceroute send small packets to the destination device until it returns to measure how long it takes. Port Loopback include PHY and MAC loopback.

Steps:

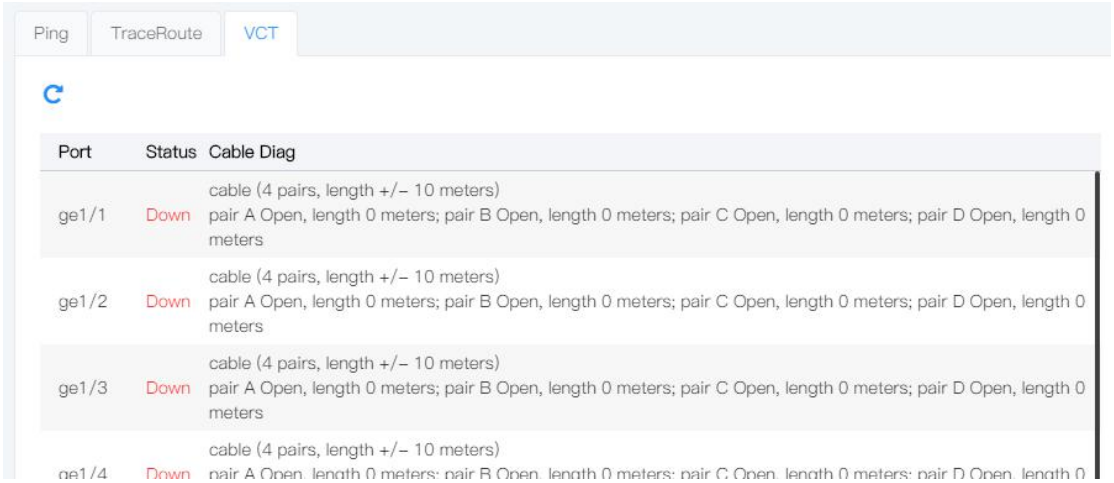
1.Click the navigation bar "Extend Management > Diagnosis" menu, enter "Diagnosis" interface, select "Traceroute", input the IP address. It's shown as below.

2.Click "Test", the user can see, as shown below

11.5.3 VCT

Steps:

1.Click the navigation bar "Extend Management > Diagnosis" menu, enter " Diagnosis " screen. click the "VCT", input the IP address. It's shown as below.


Ping
TraceRoute
VCT
Port
Status
Cable Diag
ge1/1
Down
cable (4 pairs, length +/– 10 meters)
pair A Open, length 0 meters; pair B Open, length 0 meters; pair C Open, length 0 meters; pair D Open, length 0 meters
ge1/2
Down
cable (4 pairs, length +/– 10 meters)
pair A Open, length 0 meters; pair B Open, length 0 meters; pair C Open, length 0 meters; pair D Open, length 0 meters
ge1/3
Down
cable (4 pairs, length +/– 10 meters)
pair A Open, length 0 meters; pair B Open, length 0 meters; pair C Open, length 0 meters; pair D Open, length 0 meters
ge1/4
Down
cable (4 pairs, length +/– 10 meters)