Managed Industrial Ethernet Switch User mannual

6th/Jul/2016

Version：V1.0

Revision History

Date	Version	Description
06/07/2016	V 1.0	First Edition

0 Foreword

0.1 Target reader

This manual is intended to be responsible for installing, configuring, or maintaining a network of installers and system administrators. This manual assumes that you understand all the transport and management protocols used by the network.

This manual also assumes that you are familiar with networking-related network devices, protocols and interfaces jargon, theoretical principles, practical skills and specific expertise. You also must have a graphical user interface, work experience, command line interface, SNMP and Web browser.

0.2 Conventions

This manual comply with the following conventions。

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

1.Management Software Specifications

1.Layer2 function			
1.1	Port Management	Enable / disable ports	
		speed、duplex、MTU Settings	
		flow-control settings	
		Port View	
1.2	Port Mirroring	Support port access direction, vlan mirror	vlan mirroring only supports command line configuration
1.3	Port Speed	Supports port speed limit, the speed limit is determined by the chip size	
1.4	Port Isolation	Support port isolation settings	
1.5	Suppression	It supports 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
		translate	This device does not support
		Support based on port, protocol, MAC VLAN classification	
		Support GVRP dynamic VLAN registration	Only supports command line configuration
		Voice VLAN	
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)	It also supports ERPS (proprietary protocol)
		Support 802.1w (RSTP)	
		Support 802.1s (MSTP)	
1.10	IGMP-snooping	Support Static add, delete	
		Support v1 / 2/3 Dynamic	

		Multicast Listener	
2.Eextensions			
2.1	ACL	Based on source MAC, the purpose of MAC, protocol type, source IP, destination IP, L4 port number	
		Support time-range time management	
2.2	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 rate limit CAR	
2.3	LLDP	Support LLDP link discovery protocol	
2.4	User settings	Add / remove users	
2.5	Journal	User login, operation, status, event logging	
2.6	Attack prevention	DOS defense	
		Support for CPU protection, limiting the rate of packets sent cpu	
		ARP bindings (IP, MAC, PORT Binding)	
2.7	Network Diagnostics	Support ping、telnet、trace	
2.8	System Management	Device reset, configuration save / restore, upgrade management, time settings, etc.	
3 Management Function			
3.1	CLI	Supports Serial Command Line Management	
3.2	TELNET	Support telnet remote management	
3.3	WEB	Support Layer2 Settings	
4.DHCP Server			
5.Other functions			
5.1	DHCP Snooping		
5.2	Ring protection - This feature is a list of top ERPS		
5.3	SNMPV1V2V3		

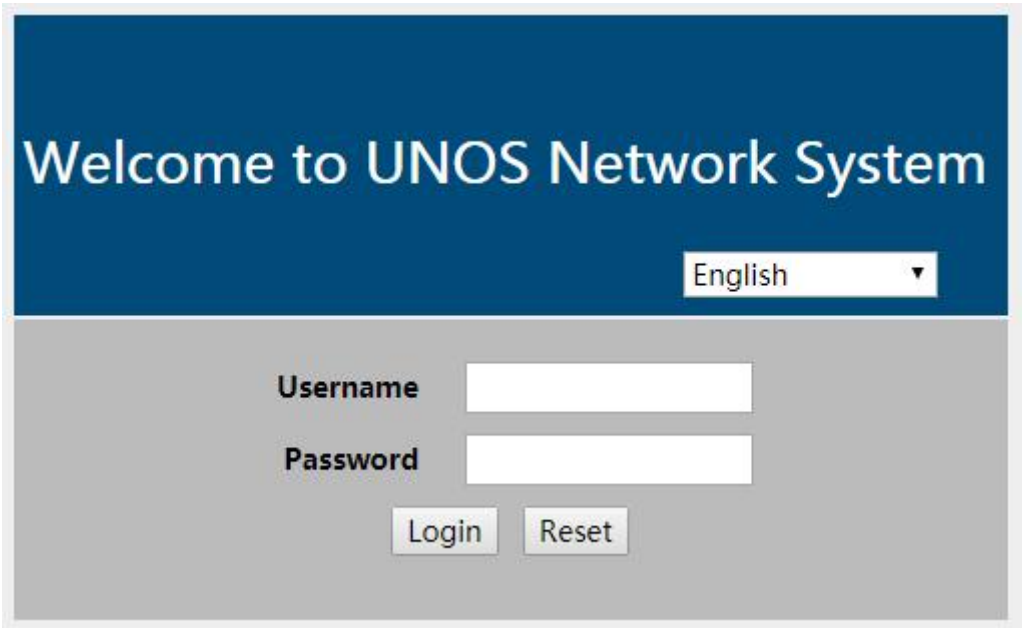
2 Login Web page

2.1 Login Web system client

Users can open a Web browser and enter the address of the default switch: http://192.168.1.253,press Enter.

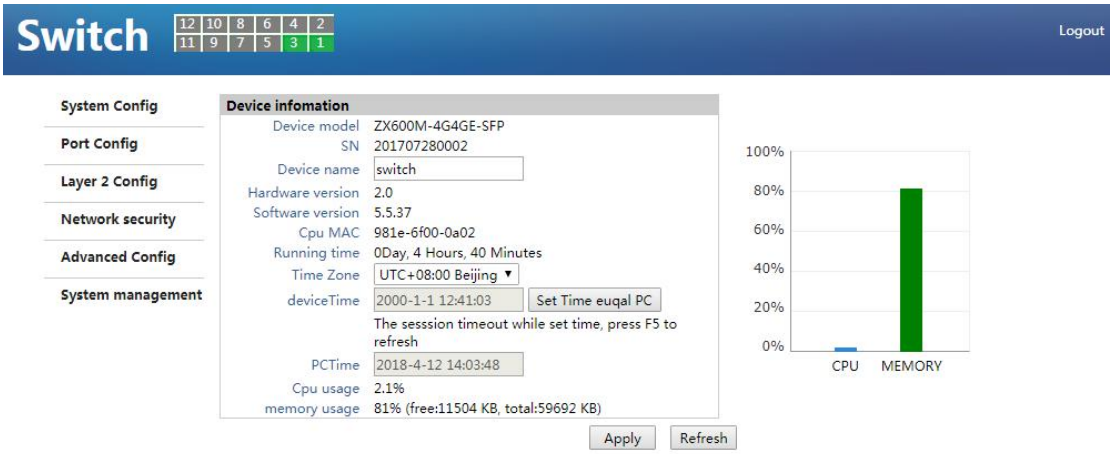
✍ illustrate：When logging into the switch, the switch should be IP network segment of the PC is consistent.The first time you log in, set the PC's IP address 192.168.1.x（x represents 1 to 254, except253,Subnet mask set 255.255.255.0,But PC IP Can't be the same as switch,that can not be 192.168.1.253.

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



2.2 Client interface composition

It describes the typical user interface of the Web system, shown as below.



2.3 Web Interface navigation tree

Web NMS menu mainly provides system configuration, port configuration, two-story configuration, network security, network configuration, system maintenance, six menu items. Each menu option under another sub-menu, as shown in Table.

Menu Item	Sub-menu	Explanation
System Configuration	system information	Display port status and product information
	Network Settings	Set the management IP address and gateway
	User Configuration	Setting users, including user name, password, permissions (1-15)
	Logging Configuration	Disply log information on the device
	TELNETConfiguration	Enable / disable TELNET services
	HTTPS Configuration	Enable / disable HTTP service, change the port number, the default port number 80
	Diagnostic Test	Provides Ping, Traceroute, port loopback function
Port Configuration	Physical port	Set the port speed (auto-negotiation, 10M, 100M, 1000M), set the flow control (disable, tx, rx, both), to enable the maximum frame Close
	Suppression	The device supports broadcast interface for unknown multicast and unknown unicast packet rate respectively storm control to prevent these three packets broadcast storm
	Port speed	Port speed limit query interface provides configuration and function.
	Port Mirroring	Configures and queries port mirroring
	Link Aggregation	Configure and query static and dynamic LACP function

	Port Isolation	Configures and queries Layer 2 port isolation
	Port Statistics	Provide access to port summary and detailed statistics
Layer2 Configuration	VLAN Configuration	Provide query and configure VLAN, interface information
	MAC Configuration	Configures and queries MAC address table information, MAC aging time, MAC learning, static MAC functions
	MSTP Configuration	Configures and queries global STP device configuration, instance configuration, the instance port configuration and port configurations.
	IGMP-snoopingConfiguration	Query and configure IGMP Snooping configuration and static multicast function
	DHCP-snoopingConfiguration	Configures and queries DHCP-snooping global configuration, and static port configuration features BINDING
	ERPS-Ring Configuration	Configures and queries ERPS-Ring global configuration and node configuration features
	GMRP Configuration	Function Configures and queries global configuration GVRP, GVRP port settings and view GMRP groups
Network security	Access control	Configure and query filtering device access rules and rules function
	Attack prevention settings	Configures and queries Guard function
	ACLConfiguration	It configures and queries the ACL function
	802.1X Configuration	Configures and queries global 802.1X authentication configuration, Radius server configuration function
Network Configuration	QOS Configuration	Configures and queries global QOS configuration and port configuration features
	LLDP Configuration	Configures and queries global QOS configuration, port configuration and functions of LLDP Neighbor
	SNMP Configuration	Configures and queries SNMP system configuration, Trap Configuration and User Configuration features
	RMONConfiguration	Configures and queries RMON configuration features
	DHCP Server Configuration	Configures and queries DHCP Server configuration, address pool, client lists, client static configuration, port binding function
	DNS Settings	Configures and queries DNS functions
	NTP Settings	It configures and queries the NTP server functions
system maintenance	Configuration File Management	Provide access to device current startup configuration, and users can upload files to the switch configuration, or you can download the configuration file from the switch
	Keep the	save the configuration

	configuration	
	Reboot the device	Reboots the switch
	Reset	The switch will restore the device to factory configuration.
	Online upgrade	Upgrade Switch's Software Version

3 System Configuration

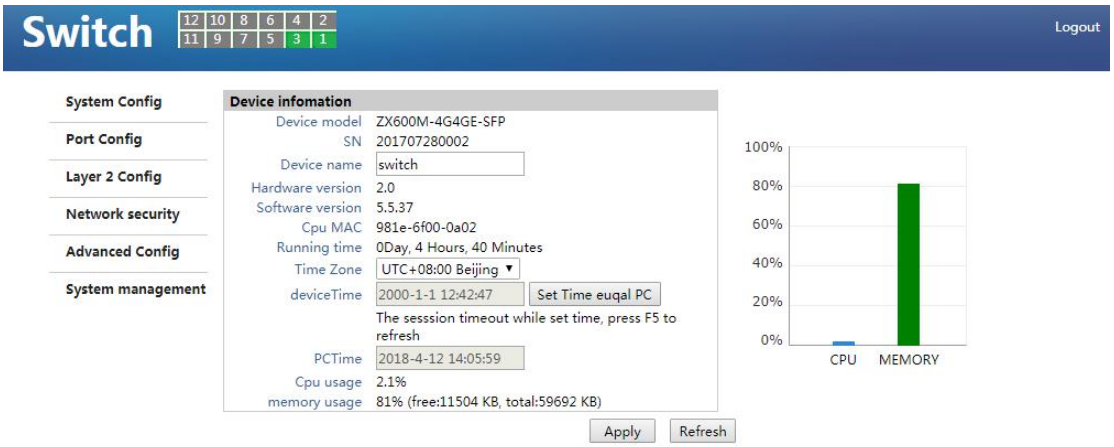
3.1 system information

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 "System Configuration" menu, go to "System Configuration" screen. Click "System Information", shown as below.



✍ **illustrate：**

In the product information, you can modify the "Device Name", "Device Time", click "Settings" to complete the configuration.

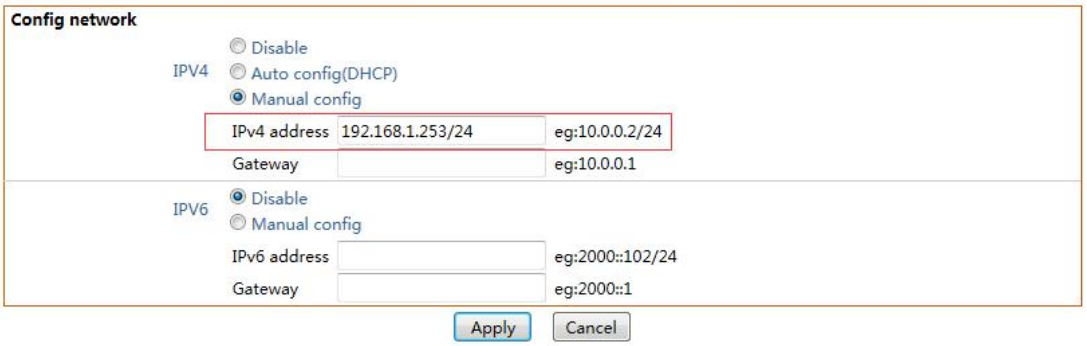
3.2 Network Settings

You can change the switch into the web interface management IP address

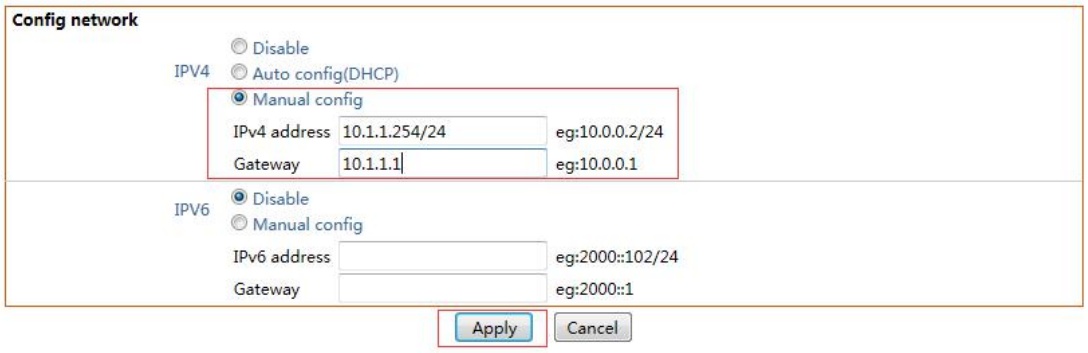
Steps:

1.Click the navigation bar "System Configuration" menu, go to "System Configuration" screen. Click "Network Settings" tab, you can see the default IPV4 address is

192.168.1.253/24, shown as below.



2.If users need to change the IPV4 address 10.1.1.254/24, gateway 10.1.1.1, navigation bar, click the "System Configuration" menu, go to "System Configuration" screen. Click "Network Settings" tab, select "Set", enter IPV4 address 192.168.1.254/24, gateway 10.1.1.1, click the "Settings", shown as below.

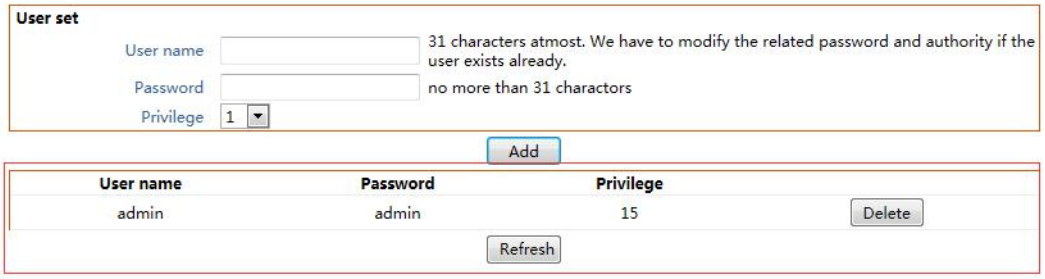


3.3 User Configuration

Users can view the switch current user name, password,and permission users can modify the user name, password, and permissions

Steps:

1.Click the navigation bar "System Configuration" menu, go to "System Configuration" screen. Click "User Configuration" tab, you can see the default user name: admin, password: admin, permissions: 15. shown as below.



3.4 Logging Configuration

Switch diary can be uploaded to the FTP server.

Steps:

1. Click the navigation bar "System> Journaling Configuration" menu, go to "upload log", enter the TFTP server address: "192.168.1.254", the file name, "diary", click "Upload", the interface is as follows.

3.5 Telnet Configuration

The user can start the telnet service.

Steps:

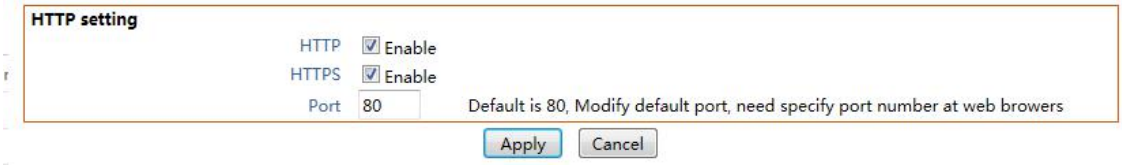
Click the navigation bar "System Configuration" menu, go to "System Configuration" screen. Click " AccessConfiguration", enter "TELNET Configuration" page, select "Enable", the default port number "23", click "Settings", shown as below.

3.6 HTTPS Configuration

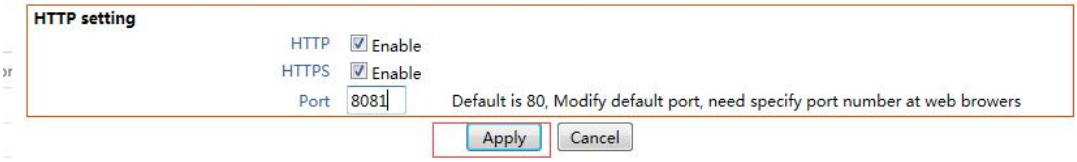
Users can modify the port number, the user can turn off HTTP and HTTPS service.

Steps:

1.Click the navigation bar "System Configuration" menu, go to "System Configuration" screen. Click the "Access Configuration",Enter "HTTP Settings" page, the user can see the system default configuration, shown as below.



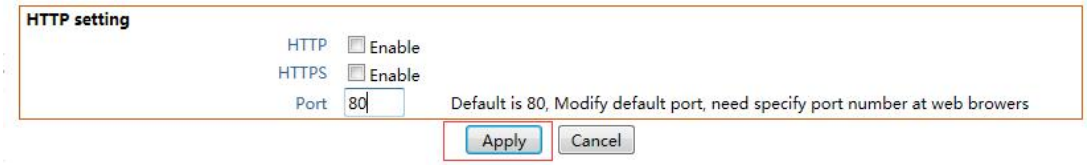
2.By entering the port number: 8081, click the "Settings", shown as below.



✍ **illustrate：**

When the port is changed to 8081, the re-log into the switch, enter the IP address should be added to the port number that is entered on the web http://192.168.1.253:8081

3. Close HTTP and HTTPS services, the abolition of "check", click "Apply", shown as below.

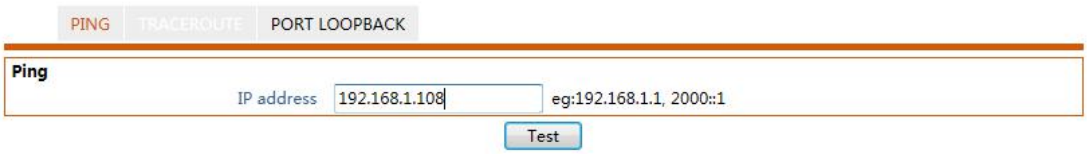


3.7 Diagnostic Test

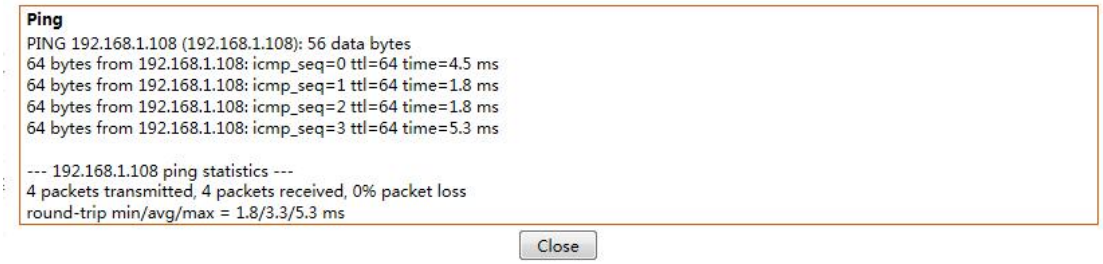
ping command to verify the IPv4 address is reachable, and display the corresponding statistics.

Steps:

1.Click the navigation bar "System Configuration" menu, go to "System Configuration" screen. Click "diagnostic test", click the "ping", enter the IP address, shown as below.



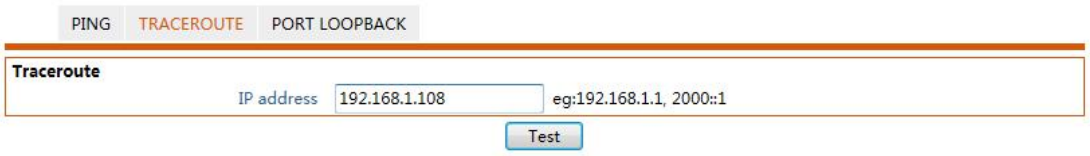
2.Click "Test", the user can see, shown as below.



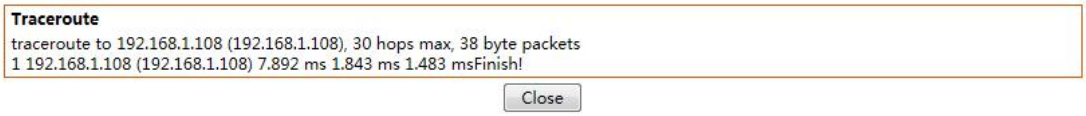
Traceroute sends small packets to the destination device until it returns to its measuring how long it takes.Loopback include PHY and MAC layers loopback.

Steps:

1.Click the navigation bar "System Configuration" menu, go to "System Configuration" screen. Click "diagnostic test", click "Traceroute", enter the IP address, shown as below.



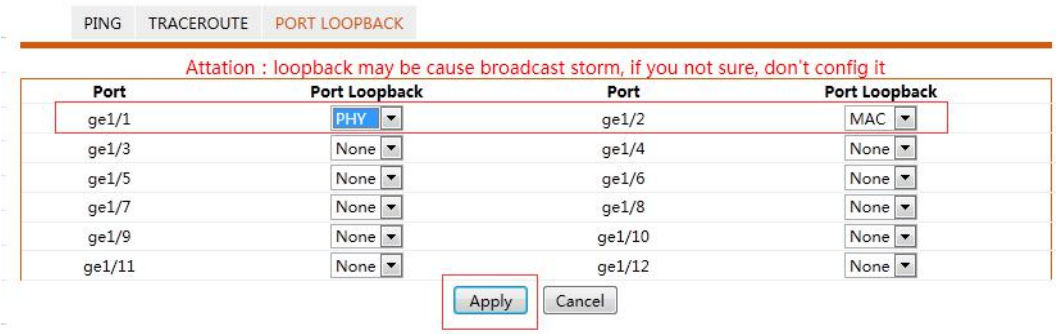
2.Click "Test", the user can see, shown as below .



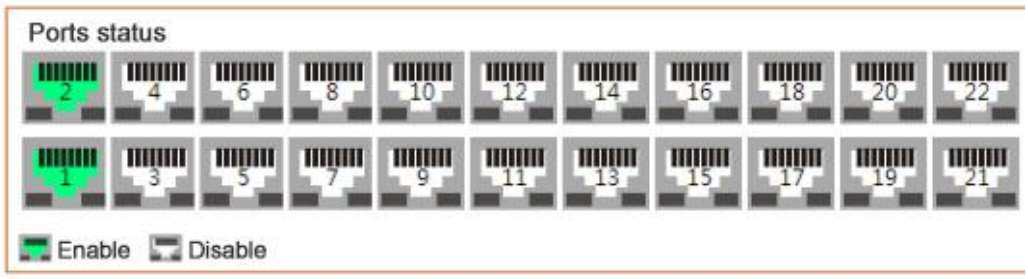
Open Ethernet interface loopback testing, inspection Ethernet interface is working. When the test interface can be forwarded packets. This feature is present for positioning within the chip associated with the interface module failures.

Steps:

1.Click the navigation bar "System Configuration - System configuration - Diagnostic Test - Port loopback", ge1 / 1 select "PHY", ge1 / 2 to select "MAC" shown as below.



2.Check loopback status, navigation bar, click "System Configuration - System Configuration - System Information", the user can see port1 and port2 have been opened, shown as below.


Ports status
2
4
6
8
10
12
14
16
18
20
22
1
3
5
7
9
11
13
15
17
19
21
Enable
Disable

4 Port Configuration

4.1 Physical port

For ease of identification interface configured to identify it to the interface description. Users can query and configure the Ethernet interface as needed

Steps:

1."Port Configuration> physical port" in the navigation bar, click the menu, go to "physical port" screen.

2.Select the desired configuration data, select configurable items "Auto-negotiation", "Flow control", "maximum frame ", as shown in FIG.

PortName	Status	Medium	Auto negotiation	ApplyRate	Rate	Flow control	Max-Frame	Enable
ge1/1		RJ45	☑	Force 1G	100M	both	1518	☑
ge1/2		RJ45	☑	Force 1G	0	both	1518	☑
ge1/3		RJ45	☑	Force 1G	1G	both	1518	☑
ge1/4		RJ45	☑	Force 1G	0	both	1518	☑
ge1/5		RJ45	☑	Force 1G	0	both	1518	☑
ge1/6		RJ45	☑	Force 1G	0	both	1518	☑
ge1/7		RJ45	☑	Force 1G	0	both	1518	☑
ge1/8		RJ45	☑	Force 1G	0	both	1518	☑
ge1/9		SFP	☑	Force 1G	0	both	1518	☑
ge1/10		SFP	☑	Force 1G	0	both	1518	☑
ge1/11		SFP	☑	Force 1G	0	both	1518	☑
ge1/12		SFP	☑	Force 1G	0	both	1518	☑

Apply Cancel

Configurable items meaning as below

Configurable items	Description
Auto-negotiation	Can be configured to auto-negotiation, forced Shizhao 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. Optical port can not be configured.

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

4.2 Suppression

The basic principle of suppression:

Storm Control in the following form to prevent the broadcast unknown multicast and unknown unicast broadcast storm. This device supports three types of packets on the interface respectively storm control packet rate. Within a detection interval, the average rate of three packets of the equipment is monitored interface receiving and and maximum threshold configuration compared to when the packet rate is greater than the configured maximum threshold, the device of the interface storm control, perform configured storm control action.

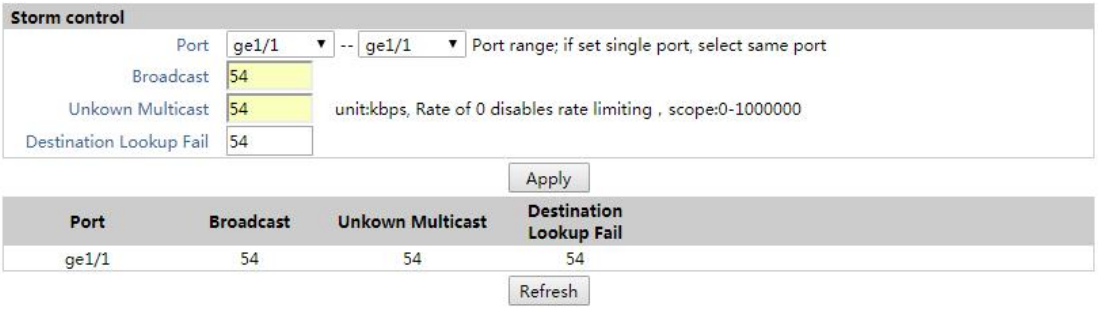
When the device is a Layer 2 Ethernet interface receives the broadcast, multicast or unknown unicast packets, if (Virtual Local Area Network) within the same VLAN packets based on the destination MAC address of the device does not clear the message interface, the device other Layer 2 Ethernet interface to forward these messages, which may cause broadcast storms, reducing the device performance.

Introducing suppression characteristics can be controlled by three types of packet traffic to prevent broadcast storms.

Steps:

1.Click the navigation bar "Port Configuration> Storm Control" menu, enter the "Storm Control" interface.

Broadcast, unknow multicast, and unicast storm control rate, it is assumed are 54kbps, shown as below.



4.3 Port Speed

Configure the interface speed is limited by physical interface to send or receive rate data inward outward.

Background Information

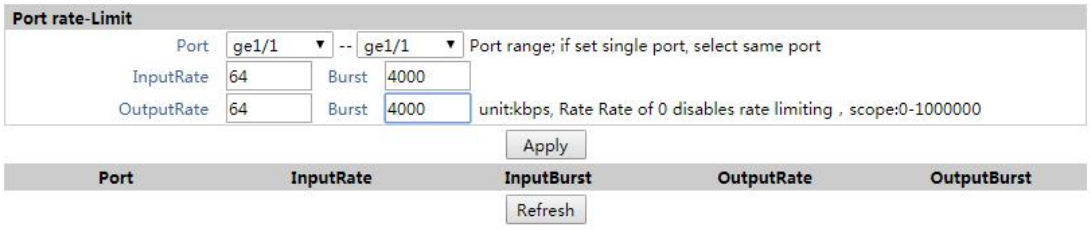
Before the flow send out from port,Configuring the speed limit in the outbound direction of an interface,to control all packets flows.

Before the flow received from port ,Configuring the speed limit in the outbound direction of an interface,to control all packets flows.

Steps

1.Click the navigation bar "Port Configuration> Portrate Limit" menu, enter "Portrate Limit" interface.

2.Enter the desired port speed configuration values, and then click the "Settings", shown as below.



Configuration Parameter Description

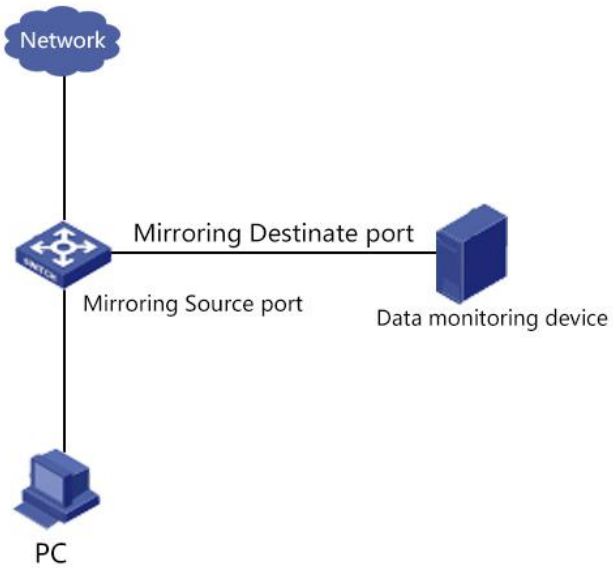
Configuration Item		Description
Interface entering direction	Input Rate	Enter the direction of the entrance CIR.The range 0-1000000.
	Input Burst	Enter the entrance direction of CBS.The range 0-1000000.
Interface out direction	Output Rate	Enter the direction of the entrance CIR.The range 0-1000000.
	Output Burst	Enter the exit direction of CBS.The range 0-1000000.

4.4 Port Mirroring

Port mirroring is to copy the specified port switch packets to the destination port; where the port is duplicated port is called the source port, destination port called replication.

Destination port can access data detection device, users use these devices to analyze the destination port to receive packets for network monitoring and troubleshooting. shown as

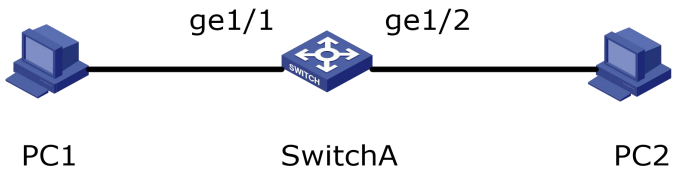
below:



Configuration Example:

PC1 via the interface ge1 / 1 access SwitchA. PC2 is directly connected to SwitchA ge1 / 2 interfaces.

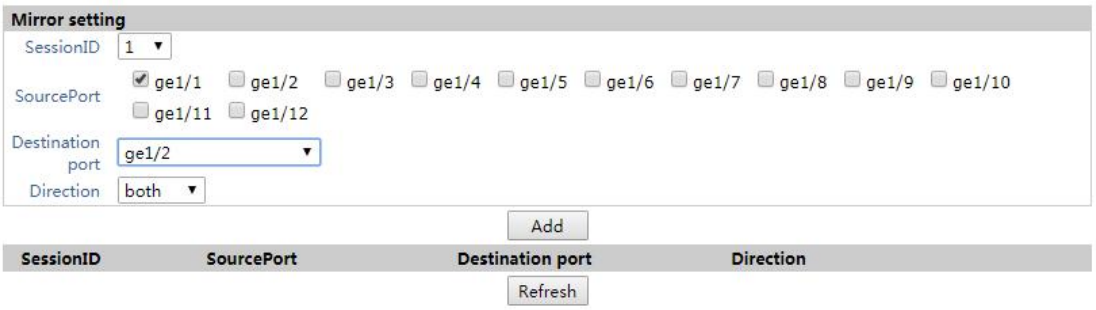
Users hope that through monitoring devices PC2 PC1 packets sent to monitor.



Steps：

1."Port Configuration> Mirror" in the navigation bar, click the menu, go to "port mirroring" screen, select the session ID.

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



Interface information means as below:

Configuration Item	Description
Session ID	There are four switches, the default session ID
Source Port	You can select multiple port
Destination port	Can not be a link aggregation port, only select a port as the destination port, the port can not be selected as the source
Direction	ingress "Mirroring ingress port": that is, any packets 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" that receive and send messages to any of the port are mirrored to the destination port.

4.5 Link Aggregation

4.5.1 This section describes link aggregation

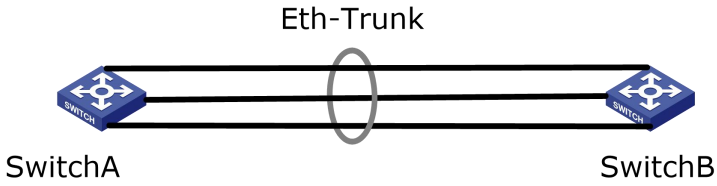
Link Aggregation (Link Aggregation) is - a group of physical interfaces are bundled together as a logical interface to increase the bandwidth and reliability of a method.

Link aggregation group LAG (Link Aggregation Group) refers to several pieces of Ethernet links bundled together in a logical link is formed, abbreviated as Eth-Trunk.As networks have been expanding, the user link bandwidth and reliability raised higher and higher requirements.In the conventional technique, commonly used to replace the high-rate interface board or replace the high-rate interface board supports devices way to increase bandwidth, but this solution needs to pay the high costs and inflexible.

Link aggregation technology without hardware upgrades conditions by combining 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 traffic load balancing.

Shown as below, between SwitchA and SwitchB are connected by three physical Ethernet links, these three links bundled together, it becomes a logical Eth-Trunk link, this logical link bandwidth is equal to the original three Ethernet total net physical link bandwidth, so as to achieve the purpose of increasing the link bandwidth; at the same time, the three Ethernet physical links back up one another, effectively improve the reliability of the link.

Link Aggregation schematic:



When there is a demand as followings, you can configure link aggregation to achieve:

When two switches are connected through a link bandwidth is not enough.

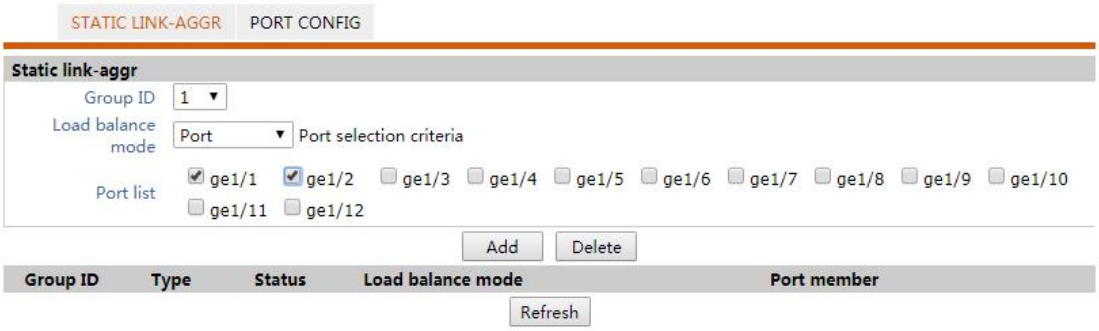
When two switches are connected through a link reliability does not meet the requirements.

Depending on whether the Link Aggregation Control Protocol LACP, link aggregation in manual load balancing mode and into LACP mode is enabled.

In manual load balancing mode, the establishment of the Eth-Trunk and add an interface by manual configuration, Link Aggregation Control Protocol no involvement. In this mode all active links are involved in forwarding data, the average share traffic, so called load balancing mode. If a strip active link fails, the link aggregation group automatically average remaining active links share the traffic. When you need to provide a direct connection between the devices in two large link bandwidth and the device does not support LACP protocol, you can use the manual load balancing mode.

4.5.2 Add a static LACP

Adding static LACP (ie, manual load balancing mode) Procedure:
1.Click the navigation bar "Port Configuration> Port channel config> STATIC LINK-AGGR" menu, go to "add a static LACP interface, select the “Group ID” (1-16), select “load balancing” (Src Mac, Dst Mac, Src & Dst Mac), select the “port”, click "Add", shown as below.



Interface information means as below:

Configuration Item	Description
Group ID	Link aggregation group ID, a total of 1 to 16, 16

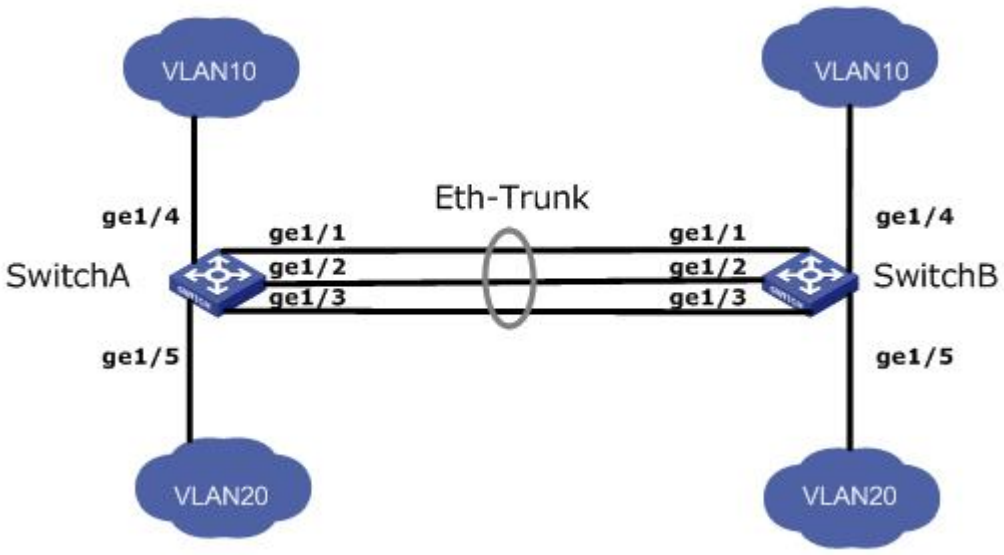
	aggregation groups, per group support up to four ports.
Load balancing	Src Mac (based on the source MAC address for load balancing), Dst Mac (based on the destination MAC address for load balancing), Src & Dst Mac (based on heterologous MAC address and destination MAC address, or load balancing), the default is based on the source MAC address load balancing
Port list	You can select multiple ports

The following is an exsample (By manual load balancing mode)

As the following pic shows,SwitchA and SwitchB are connected VLAN10 and VLAN20 of networks through an Ethernet link, and there is a greater flow of data between SwitchA and SwitchB.

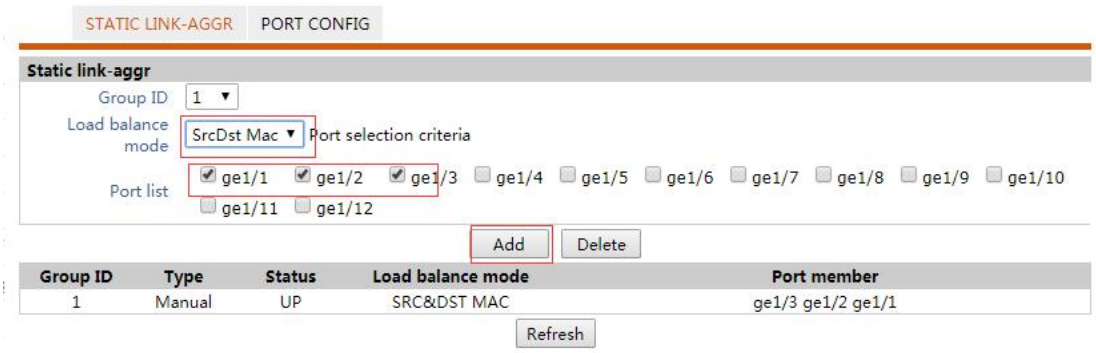
Users want to be able to provide greater bandwidth of the link between SwitchA and SwitchB to make the same inter-VLAN communicate with each other. And we also want to be able to provide some redundancy to ensure reliability of data transmission and links.

Manual load balancing mode Link Aggregation Network diagram

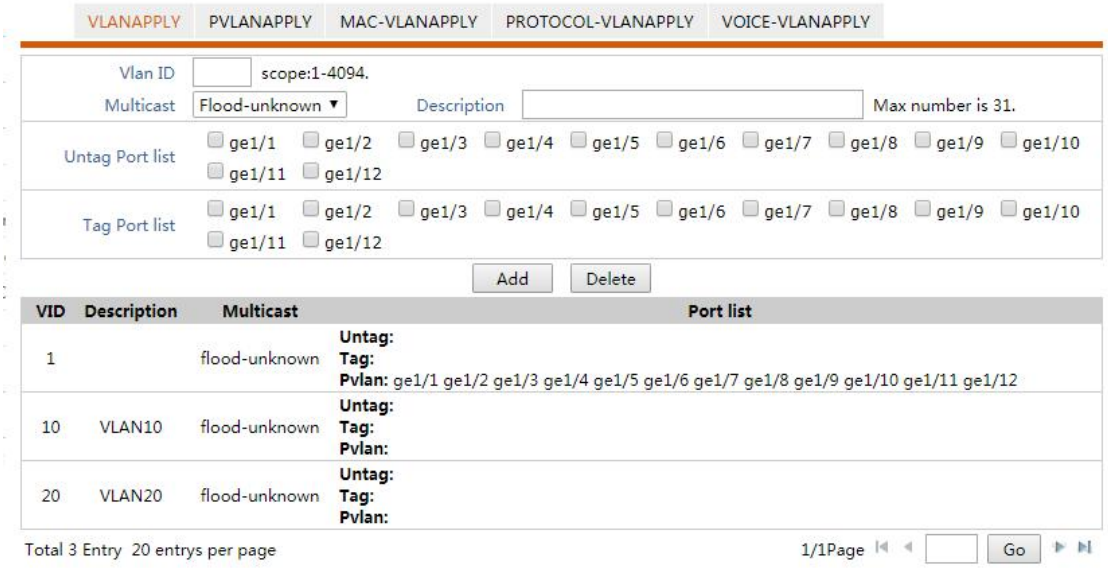


Steps：

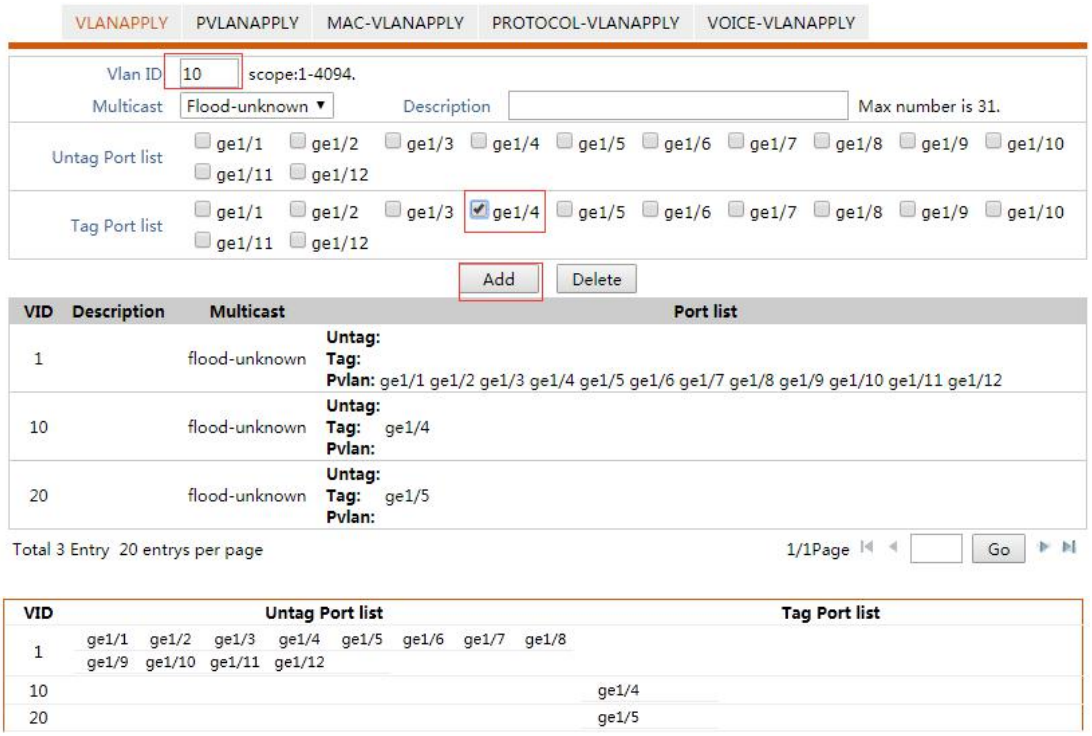
1. Create interfaces Eth-Trunk on SwitchA and add member interfaces, to increase link bandwidth,SwitchB configuration similar with SwitchA,Not repeat.Click the navigation bar "Port Configuration> Port channel config> Global Configuration" menu,Enter the "Add Static LACP interface,Select “Group ID “ 1 ,Select the “load balancing mode”(Src Mac),Select the “ ports “ge1/1、ge1/2、ge1/3,Click "Add",Show as below:



2. Creat Vlan on SwitchA.SwitchB configuration similar with Switch A,Not repeat.Click the navigation tree "Layer Configuration> VLAN Configuration>VLAN Configuration" menu,Enter the "VLAN Config uration" interface,Vlan' ID Input "10",Description Input "vlan10",Seletc "Flood-unknown",Click "Settings",Vlan' ID Input "20",Description Input vlan"20",Select "Flood-unknown",Click "Settings",Complete the configuration, shown as below.

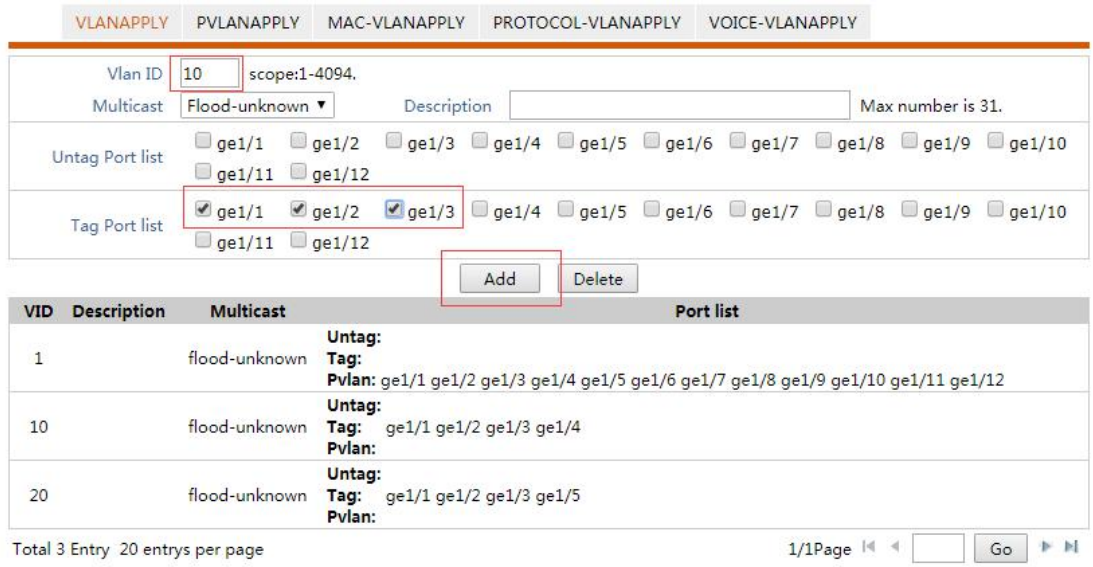


3. In SwitchA, Configuration ge1 / 4 port allows VLAN 10 through,Configuration ge1/5 port allow VLAN20 through.SwitchB configuration similar with SwitchA. Click the navigation tree "Layer Configuration> VLAN Configuration> TRUNK Configuration" menu, enter "TRUNK-CONFIG" interface,Under the "Vlan setting" is "Vlan ID", Input "10",Tick "ge1/4"from the Tag port list,Click "Add",Under the "Vlan setting " is VLan ID input "20",tick"ge1/5"in the Tag ports list,Click " Add",Show as below



VID	Untag Port list	Tag Port list
1	ge1/1 ge1/2 ge1/3 ge1/4 ge1/5 ge1/6 ge1/7 ge1/8 ge1/9 ge1/10 ge1/11 ge1/12	
10		ge1/4
20		ge1/5

4. In the configuration of SwitchA aggregated ports ge1 / 1, ge1 / 2, ge1 / 3 allows VLAN10 and VLAN20 through.SwitchB configuration similar with SwitchA.Click the navigation tree "Layer Configuration> VLAN Configuration> TRUNK Configurat"Vlan setting" is "Vlan ID" Input"10", Tick"ge1/1,ge1/2,ge1/3" in the Tag ports list,Click " Add",Under the "Vlan setting" is "Vlan ID" Input"20"Tick"ge1/1,ge1/2,ge1/3" in the Tag ports list,Click " Add",show as below.



4.5.3 Add a Dynamic LACP

Dynamic Link Aggregation

Based IEEE802.3ad standard LACP (Link Aggregation Control Protocol, Link Aggregation

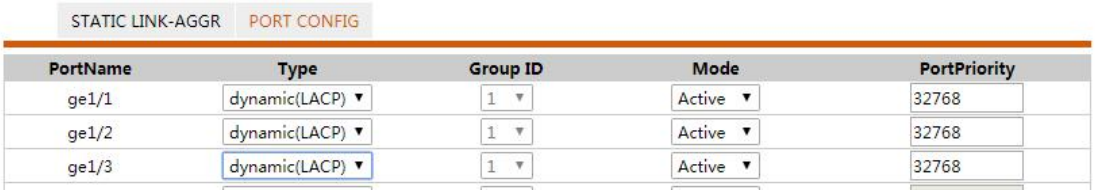
Control Protocol) is an implementation of dynamic link aggregation and de-aggregation of the agreement. LACP protocol LACPDU (Link Aggregation Control Protocol Data Unit, Link Aggregation Control Protocol Data Unit) and peer interaction information.

After opening a port LACP protocol, the port will advertise itself to the remote system priority, system MAC by sending LACPDU, port priority, port number, and operational Key. After receiving this information termination information with the other ports of the stored information can compare to select the ports to be aggregated so that the two sides can join or leave a port of a dynamic aggregation group consensus.

Dynamic LACP aggregation is an automatically created or deleted aggregation, add and delete a dynamic aggregation group port protocol is done automatically. Only the same speed and duplex properties, connected to the same equipment, the same basic configuration port can be dynamically come together.

Adding dynamic link aggregation procedure:

1.Click the navigation bar "Port Configuration> Port channel config> Port Configuration" menu, enter the "Port Name", select the port, choose the 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 "Add", 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, two devices in one does not support LACP, the device can be created on a static link aggregation, and add bandwidth of member interfaces between devices and reliable sex. Dynamic LACP mode In the dynamic mode LACP links between two devices can implement redundancy backup, backup links 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 are connected to each other are passive LACP port, this will not be a two-port dynamic LACP polymerization, because both ports are waiting for the end device LACP protocol packets.
Port Priority	In determining the dynamic LACP aggregation group members, the priority will be determined according to the device ID superior end port ID. Wherein the device ID 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 the same, compare the system MAC address value smaller one would be considered excellent. Range: 0-65535 Default: 32768.

✍ **illustrate：**

Before changing Eth-Trunk working mode first make sure that the Eth-Trunk does not contain any member interface, or can not modify the Eth-Trunk working mode.

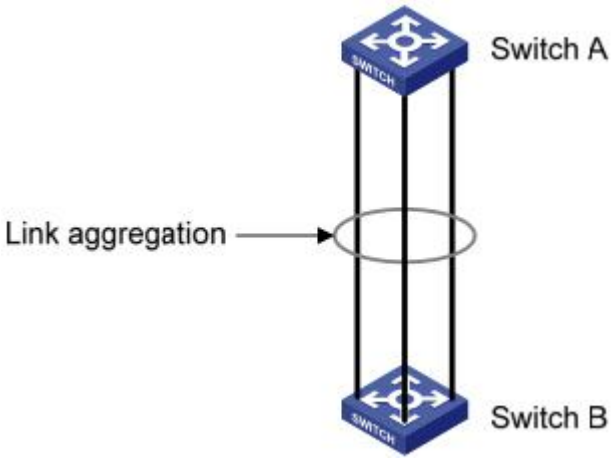
The local and remote configuration mode should be consistent.

For exsample

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

Access Ethernet Switch” SwitchB” ,to acheive flows load balancing among the member ports .

Here is The dynamic aggregation mode as an example.



✍ **illustrate:**

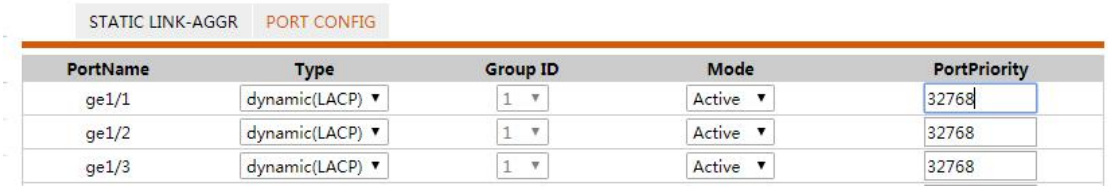
The following just list the configuration on Switch A, Switch B also need to make the same

configuration can be achieved port Aggregation.

Steps:

1. Set the system priority is “100”, making it the active side and LACP on SwitchA.Click the navigation bar "Port Configuration> Link Aggregation> PORT Configuration" menu, enter the "PORT Configuration", the LACP is set to "100", click "Apply" to complete the configuration.

2. Create Eth-Trunk on SwitchA and configure LACP mode.SwitchB configurated similar SwitchA.Click the navigation bar "Port Configuration> Link Aggregation> Port Configuration" menu, enter the "Port configuration",Select the ports need configurate ge1/1, ge1/2,ge1/3,Select the type "Dynamic LACP", select the mode "Active", click "Apply" to complete the configuration.Show as below.

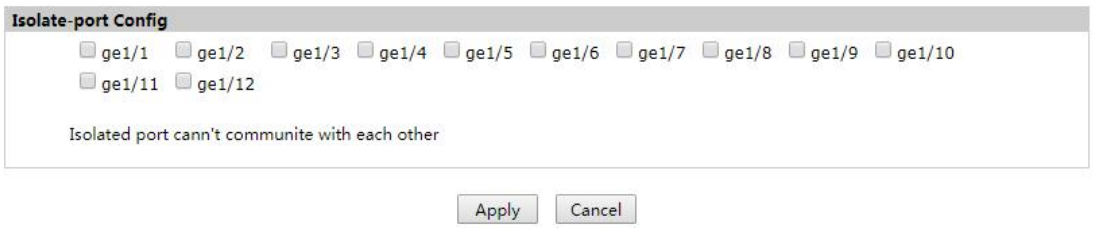


4.6 Port Isolation

Isolated with each other between ports in the same ports isolation group,not isolation between ports in different port isolation groups.

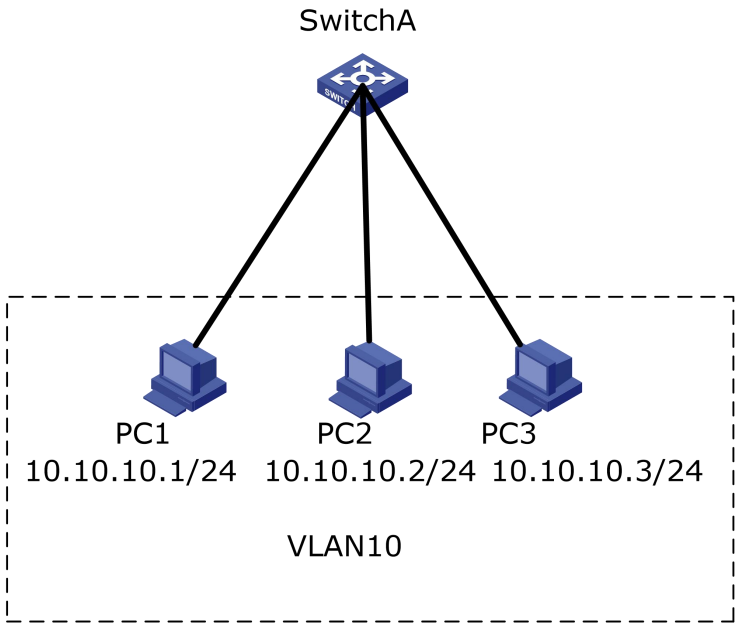
Steps:

1.Click the navigation bar "Port Configuration> Link Aggregation> Port isolation" menu, enter "port isolation", established by checking the port isolation group, click the "Apply" to complete the configuration,show as below.



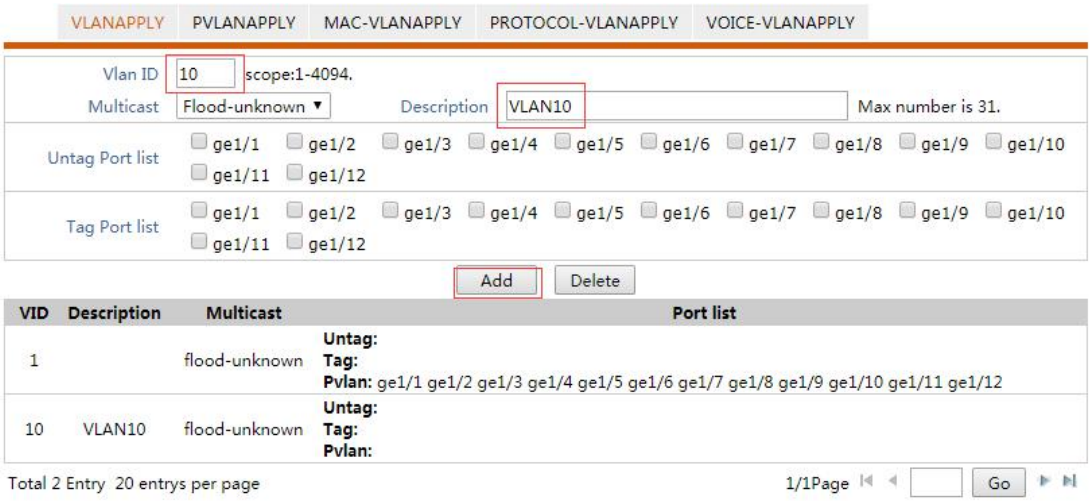
For exsample,show in following pic,PC1, PC2 and PC3 belong to VLAN 10,User wants between PC1 and PC2 in VLAN 10 can not access each other, can visit each other between PC1 and PC3, can visit each other between PC2 and PC3.

Configured port isolation network diagram

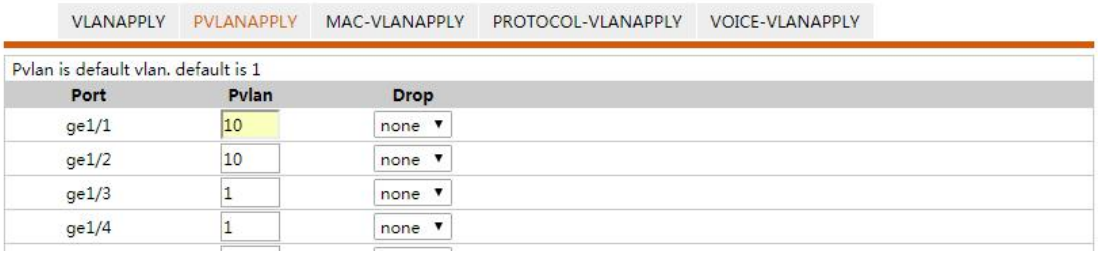


Steps:

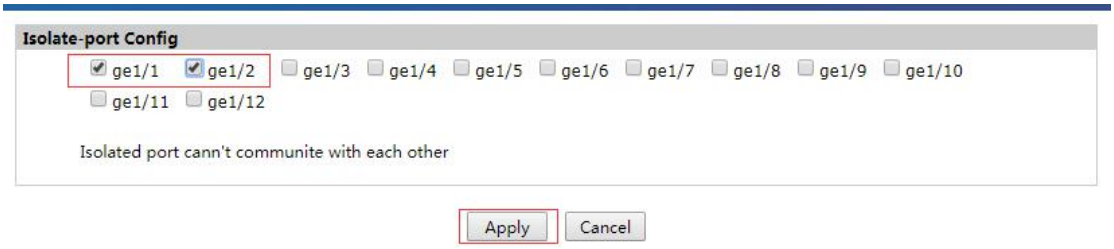
1.Creat VLAN,assure the Vlan PC belongs to.Click the navigation tree "Layer Config> VLAN Config> VLAN Conig" menu, enter the "VLAN Config"interface,"VlanID" Input"10","Description" input"Vlan10", select "Flood-unknown",Click "Add" to complete the configuration,show as belows:



2.Configurate Ethernet portjoin Vlanas correct ways,Implement interface allows VLAN packets to pass.Click the navigation tree "Layer Config> VLAN Config> PVLAN Config" menu, enter "PVLAN Config" 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 fuction,Click the navigation bar "Port Configuration> Link Aggregation> Port isolation" menu, enter "port isolation",Tick port ge1/1,ge1/2 establish isolation group,click “Apply”complete the configuration, show as below



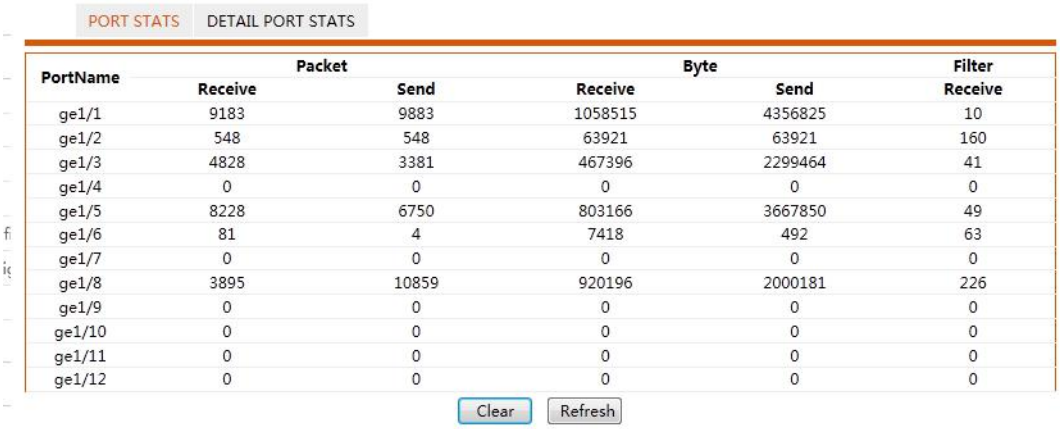
4.Verify the configuration.
PC1 & PC2 can’t ping each other.
PC1 & PC3can ping each other.
PC2 & PC3 can ping each other

4.7 Port Statistics

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

Noted:After the traffic statistics emptied can not be restored. Please confirm carefully before operation.

Steps:
1.Click the navigation bar "Port Configuration> Port Statistics> Summary Port Statistics" menu, enter "Port Stats", shown as below.



PORT STATS | DETAIL PORT STATS

PortName	Packet		Byte		Filter
	Receive	Send	Receive	Send	Receive
ge1/1	9183	9883	1058515	4356825	10
ge1/2	548	548	63921	63921	160
ge1/3	4828	3381	467396	2299464	41
ge1/4	0	0	0	0	0
ge1/5	8228	6750	803166	3667850	49
ge1/6	81	4	7418	492	63
ge1/7	0	0	0	0	0
ge1/8	3895	10859	920196	2000181	226
ge1/9	0	0	0	0	0
ge1/10	0	0	0	0	0
ge1/11	0	0	0	0	0
ge1/12	0	0	0	0	0

Clear Refresh

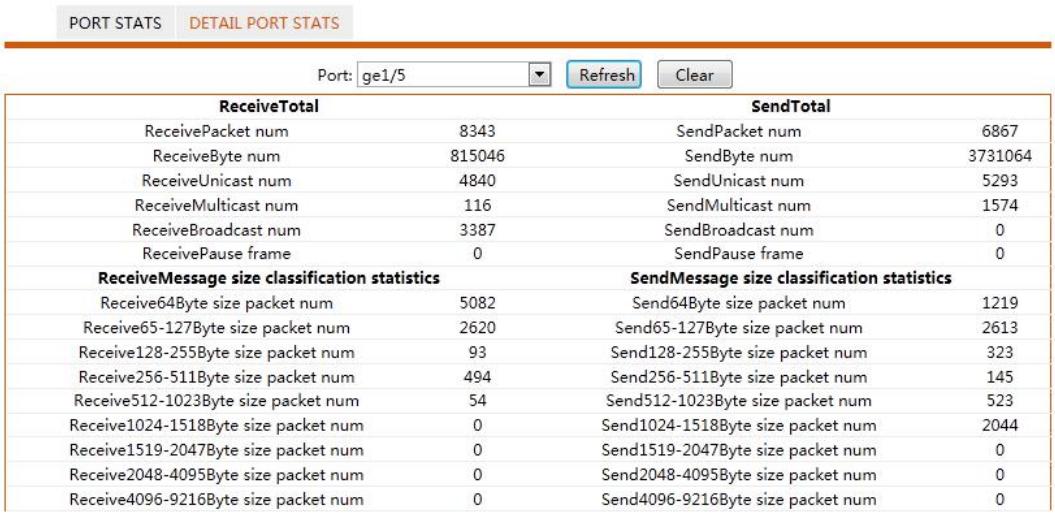
✍illustrate:

Click the "Refresh" the page for 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 "Port Configuration> Port Statistics> Detail Port Stats" menu, Enter "port Detailed stats ",show as below:



PORT STATS | DETAIL PORT STATS

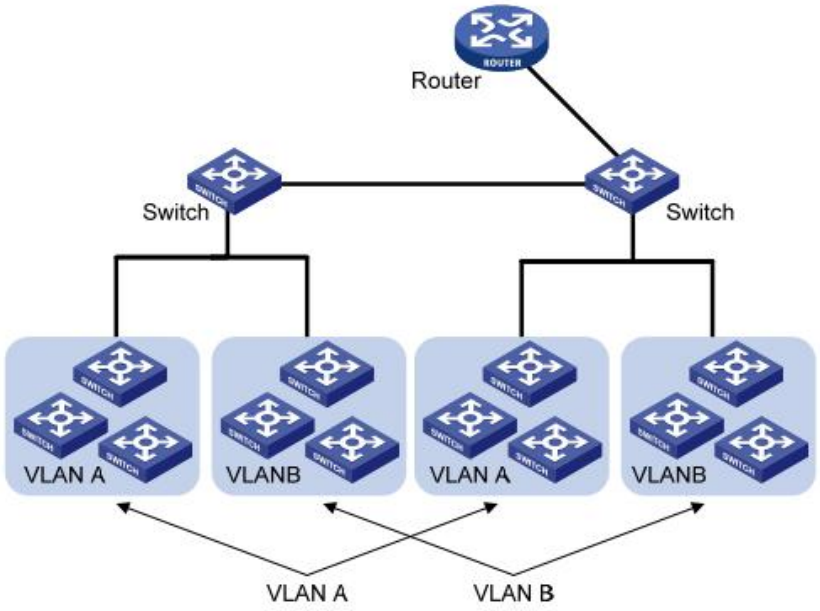
Port: ge1/5 Refresh Clear

ReceiveTotal		SendTotal	
ReceivePacket num	8343	SendPacket num	6867
ReceiveByte num	815046	SendByte num	3731064
ReceiveUnicast num	4840	SendUnicast num	5293
ReceiveMulticast num	116	SendMulticast num	1574
ReceiveBroadcast num	3387	SendBroadcast num	0
ReceivePause frame	0	SendPause frame	0
ReceiveMessage size classification statistics		**SendMessage size classification statistics**	
Receive64Byte size packet num	5082	Send64Byte size packet num	1219
Receive65-127Byte size packet num	2620	Send65-127Byte size packet num	2613
Receive128-255Byte size packet num	93	Send128-255Byte size packet num	323
Receive256-511Byte size packet num	494	Send256-511Byte size packet num	145
Receive512-1023Byte size packet num	54	Send512-1023Byte size packet num	523
Receive1024-1518Byte size packet num	0	Send1024-1518Byte size packet num	2044
Receive1519-2047Byte size packet num	0	Send1519-2047Byte size packet num	0
Receive2048-4095Byte size packet num	0	Send2048-4095Byte size packet num	0
Receive4096-9216Byte size packet num	0	Send4096-9216Byte size packet num	0

5. Layer2 Configuration

5 .1 VLAN configuration

A VLAN is not restricted by physical locations, so hosts in a VLAN to be located in the same physical space.as following pic shows,VLAN divides a physical LAN into multiple logical LAN ,each VLAN is a broadcast domain.Between hosts in a VLAN packets can interact through a conventional Ethernet communication, while hosts in different VLAN if needed within the communication, it must be able to achieve through a router or Layer 3 switch network layer devices.



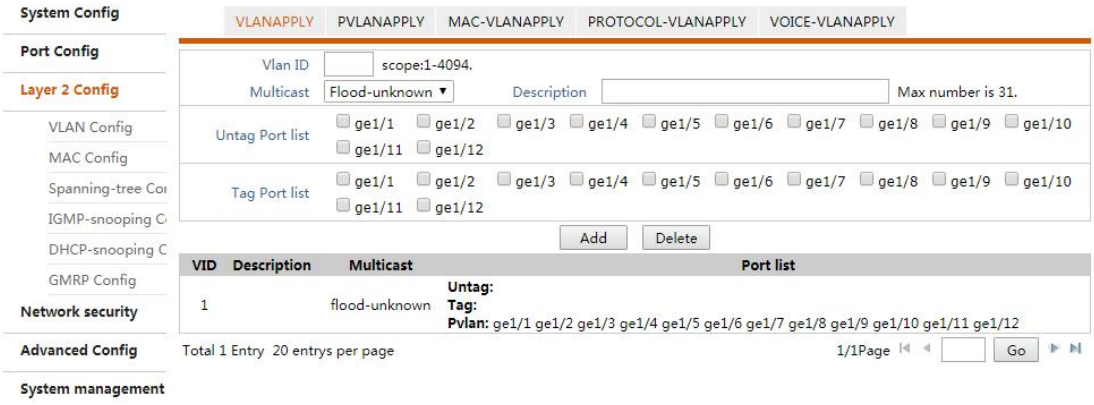
Compared with the traditional Ethernet, VLAN enjoys the following advantages:
Control the broadcast domain range: LAN broadcast packets are restricted in one VLAN, reducing bandwidth and improve network performance.
Improving LAN security: As the packets at the data link layer is divided by the quarantine VLAN broadcast domain, so the hosts within each VLAN can not communicate directly, through a router or Layer 3 switches and other network equipment layer packets Layer 3 forwarding.
Flexibility to create virtual working groups: VLAN can be used to create a physical network across a range of virtual working groups, 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.
This managed switch supports 802.1Q VLAN, protocol-based VLAN, MAC-based VLAN and port-based VLAN. In the default configuration, VLAN for the 802.1Q VLAN mode.
Port-based VLAN, the principle is based on the principle of switching device interface number to divide VLAN. The network administrator to configure each interface switch different PVID, namely VLAN interface to a default it belongs. When a data frame into the switch interface, if no VLAN tag, and the PVID configured on the interface, then the data

frame will be marked with PVID interface. If the incoming frame has a VLAN tag, the switch will not add VLAN tag, even if the interface has been configured PVID.

VLAN frame for treatment is determined by the type of interface. The advantage is the simple definition of a member. The disadvantage is a member of the mobile reconfigure VLAN.

a. Create VLAN Procedure

1.Click the navigation tree "Layer Configuration> VLAN Configuration> VLAN Configuration" menu, enter the "VLAN Config"screen, shown as below.

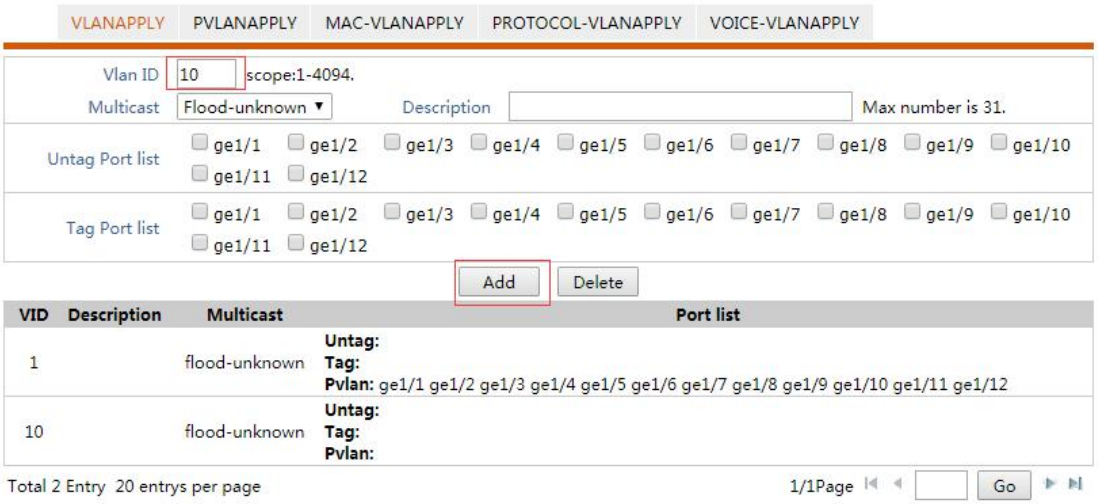


Interface information means as followings:

Configurateitem	**Description**
VLAN ID	Required,Add Vlan ID, range from 1~4094.such as: 1-3,5,7,9VLAN 1 is the default which, when not re-create VLAN 1.
Description	Optional,Detailed description of VLAN information. When creating a new batch, the description must be empty.
Multicast	Required,Multicas thandled,"Flood-unknown"by default,Flood-all optional,discard.

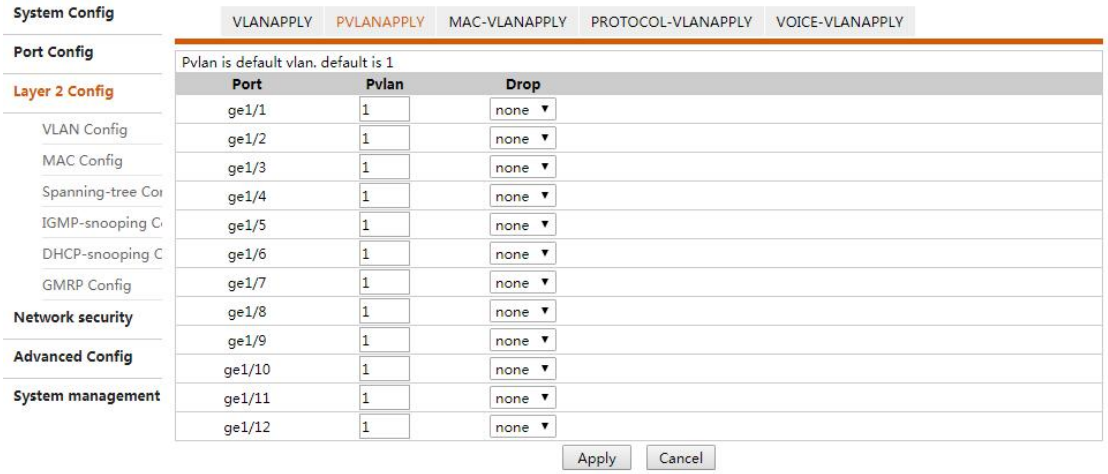
2.Fill in the appropriate configuration items.

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



b.The current port to the specified VLAN Procedure

1.Click the navigation tree "Layer Configuration> VLAN Configuration> PVLAN Configuration" menu, enter "PVLAN Config" interface, show as pic.



Interface information means as followings.

Config-item	Description
PVLAN	PVLAN acquiescence VLAN, the default is 1, also known as the local VLAN. The VLAN setting is usually set, and the port is added to the VLAN tag. Port receives message discarding property: not discarding; abandoning label free tag information; label and tag message discard; discard all.

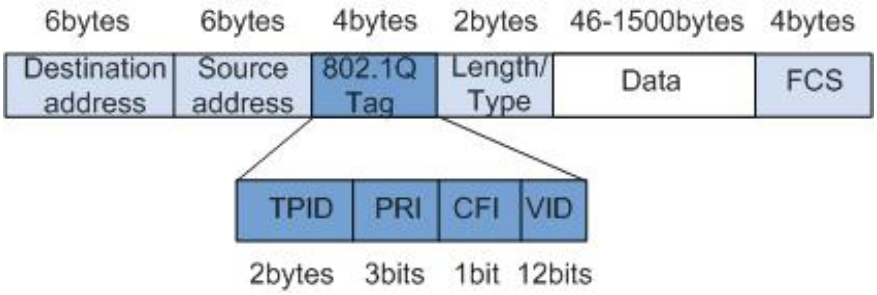
2.Fill in the appropriate configuration items.

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

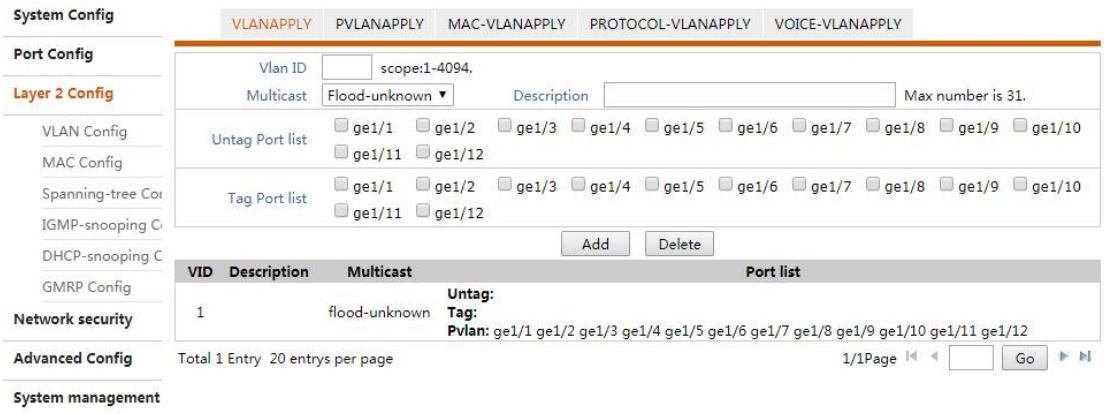


802.1Q Tag meanings

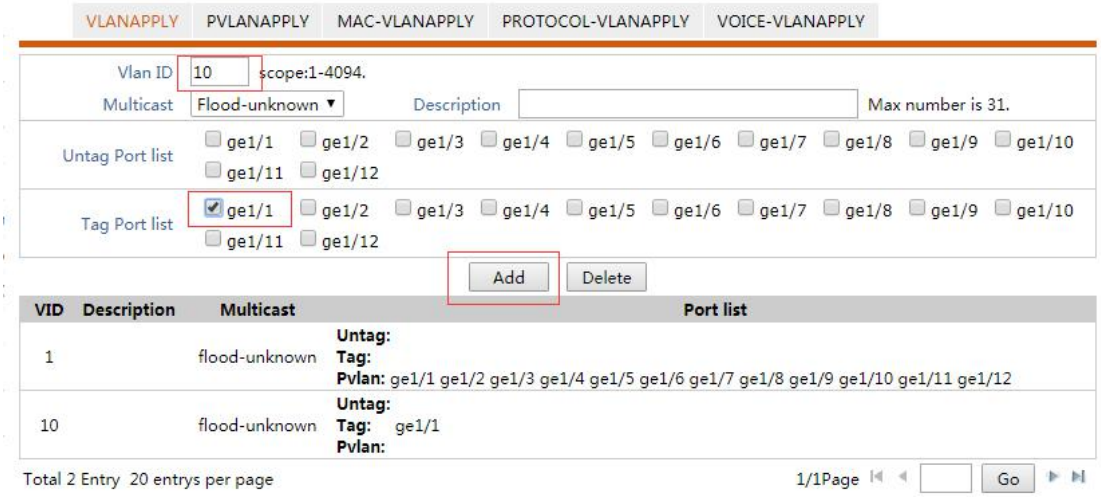
Field	length	Name	Analysis
TPID	2bytes	Tag Protocol Identifier(Tag Protocol Identifier), the frame type.	Value of 0x8100, said 802.1q Tag frames. If the device does not support 802.1q receives such a frame will be discarded.
PRI	3bits	Priority,It indicates the priority of the frame.	In the range of 0 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 format.	CFI is 0 Description classic format, CFI 1 indicates that the non-canonical format. Compatible for Ethernet and Token Ring. In Ethernet, CFI 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 configurationprocedure
1.Click the navigation tree "Layer Configuration> VLAN Configuration> VLAN Configuration" menu, enter "VLAN Configuration" interface, The default configuration of the switch port is the trunk port. As shown in the following figure.

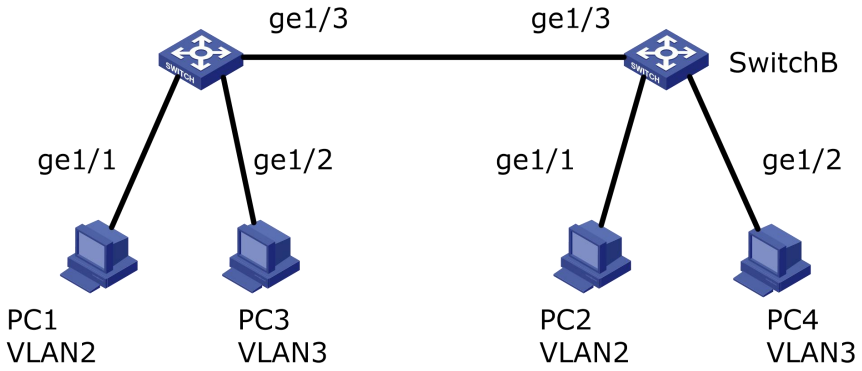


2.Permitted VLAN Trunk port. Click the navigation tree "Layer Configuration> VLAN Configuration> VLAN Configuration" menu, enter "VLAN Configuration" interface, input the VLAN ID that allows VLAN through the Trunk port, select the corresponding interface in the Tag port list, click "add" to complete the configuration.



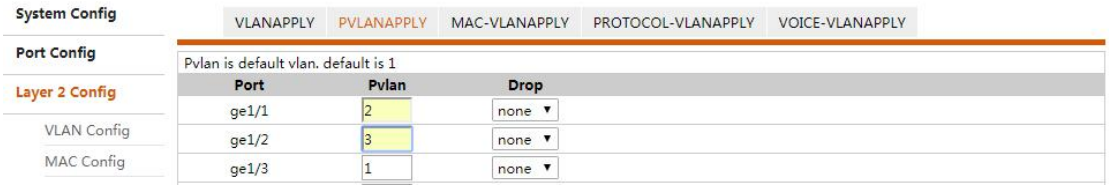
E.g

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.



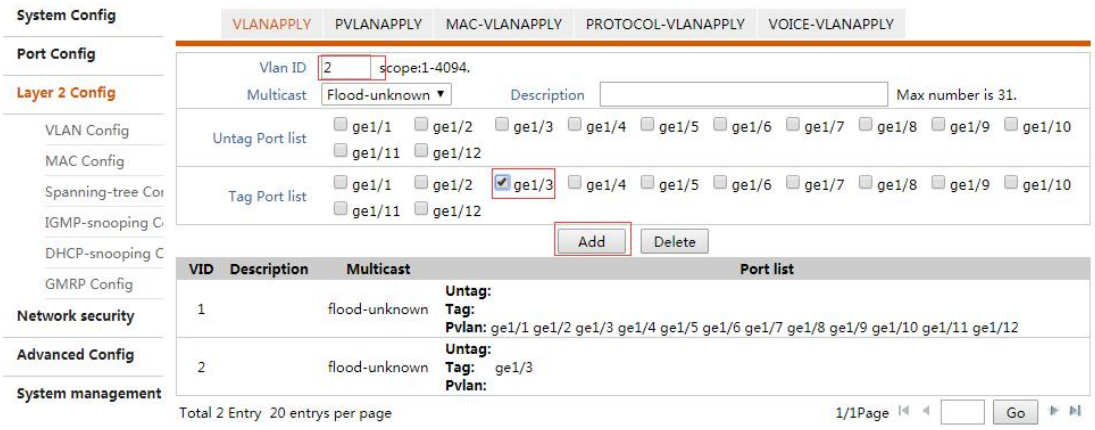
Steps:

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 "Layer Configuration> VLAN Configuration> PVLAN Configuration" menu, enter "PVLAN Configuration" screen, 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 "Layer Configuration> VLAN Configuration> VLAN Configuration" menu, enter "VLANConfiguration" screen, 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.

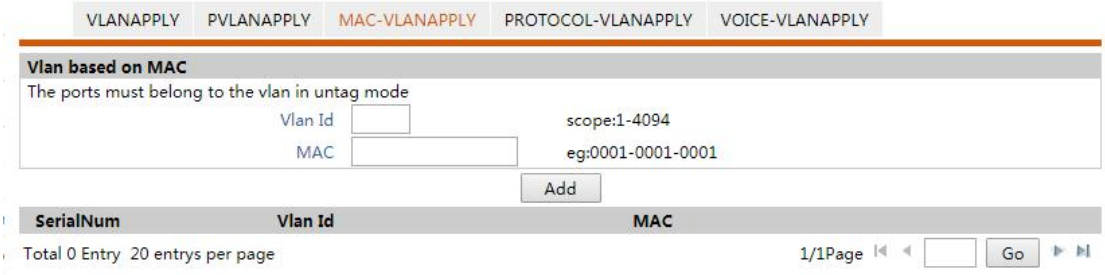
5.2 mac-vlan

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:

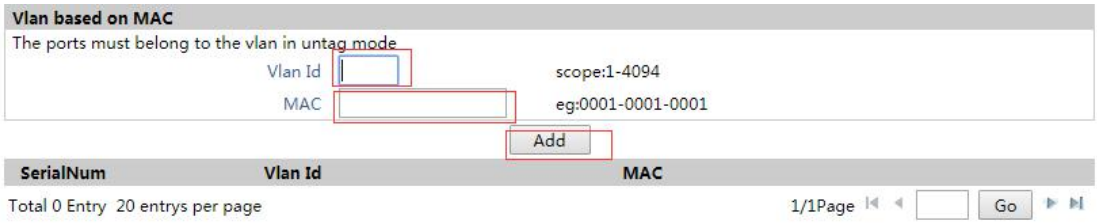
1.Click the navigation tree "Layer Configuration> Vlan Config" menu, enter "Vlan based on MAC" interface, shown as below.



Interface informatio 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 untag joins link ports.
MAC	Required ,input computer's MAC address

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

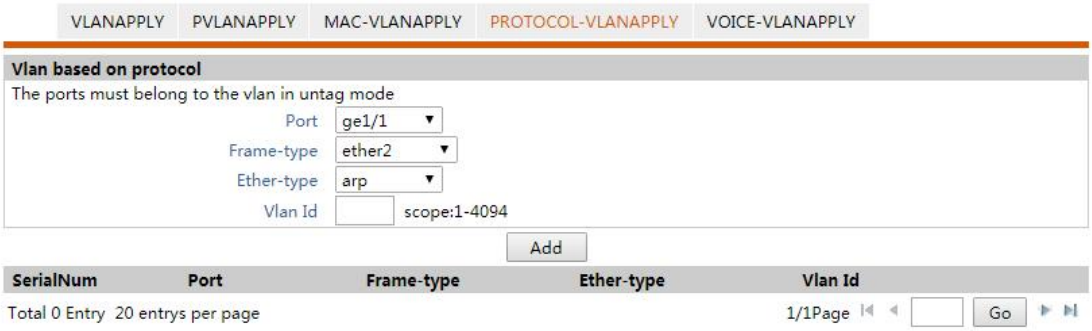


5.3 protocol-vlan

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:

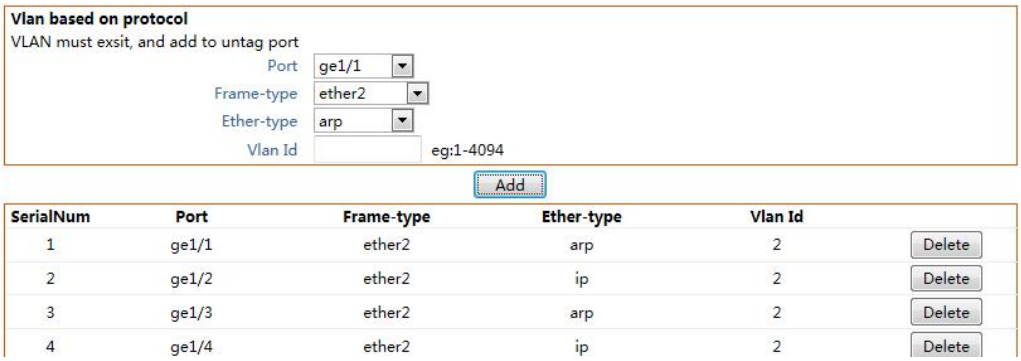
1. Choose the "Configuring Layer> Vlan based on protocol" menu, enter "Vlan based on protocol" interface, shown as below.



Interface information meaning as followings

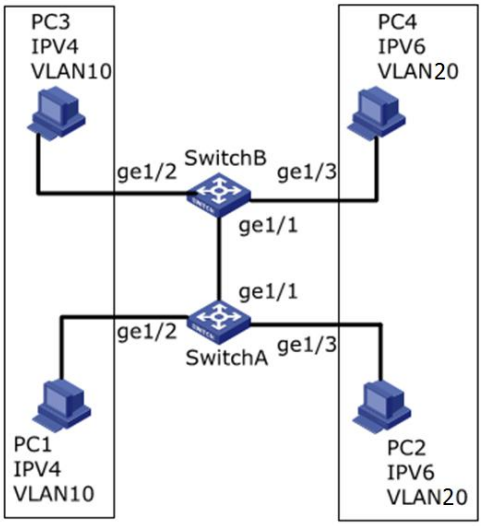
Configuration item	description
ports	Select Port from pull-down menu（ge1/1-ge1/24,xe1/25- xe1/28）
Frame Type	Optiona, ether2802.3,snap,lc,snap-priv
Ether-type	Optiona,arp,ip,ipv6,802.1d.1q, 802.1d.1x
VlanID	Required,add VLAN ID,range from 1~4094,such as 1-3,5,7,9.VLAN 1is default.VLAN must exist and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

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



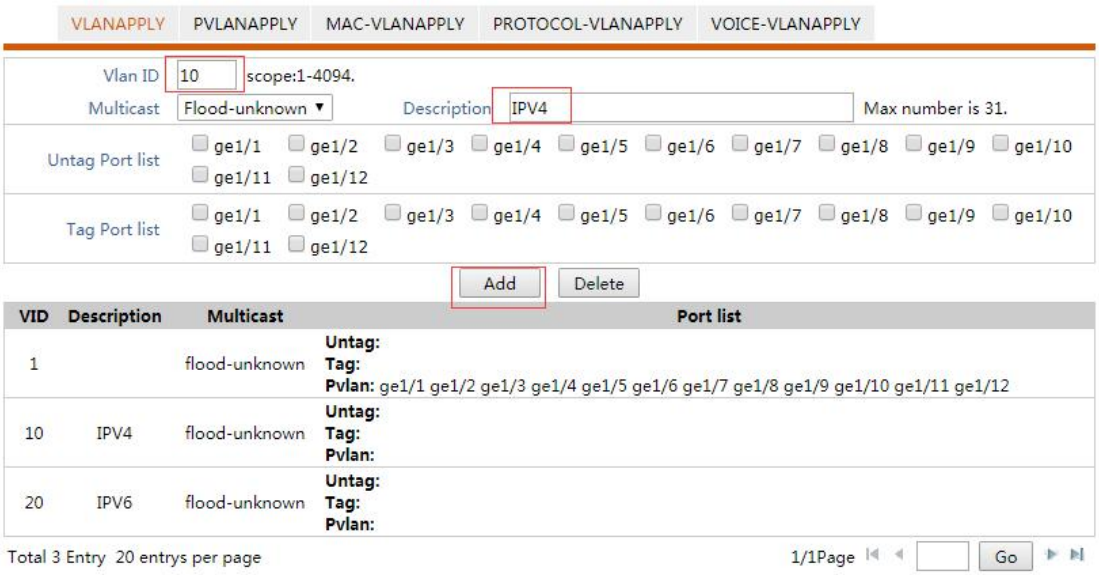
✍ **illustrate:**
Set match protocol IPV4 and IPV6, need to match the settings ARP protocol.

The following is an exsample,As shown between PC3 and PC1 can communicate, using IPV4 protocol, IPV4 protocol will bind to VLAN10 in. PC2 and PC4 can exchange visits between the communication protocol using IPV6, IPV6 protocol will bind to VLAN20 in.
Protocol-based VLAN network diagram

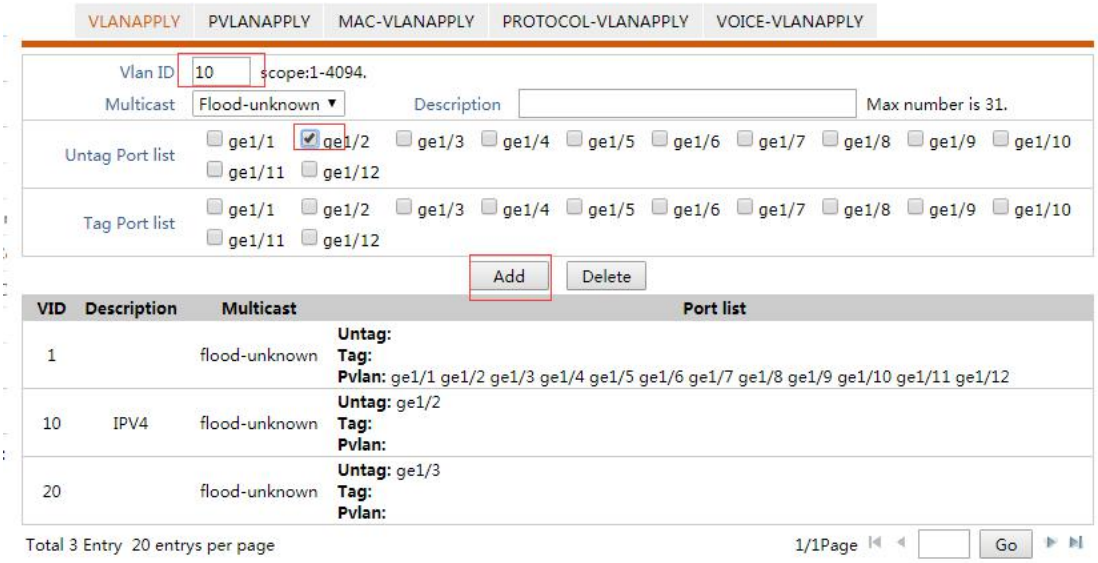


Steps:
1. Create VLAN,assure VLAN each service belongs to .Click the navigation tree "Layer

Configuration> VLAN Configuration> VLAN Configuration" menu, enter the "VLAN Configuration" screen, create vlan10, Vlan 'ID input value of 10, type a description IPV4. Create vlan20, Vlan 'ID input values 20, type a description IPV6. Select Flood-unknown, click "Add" to complete the configuration, shown as below.



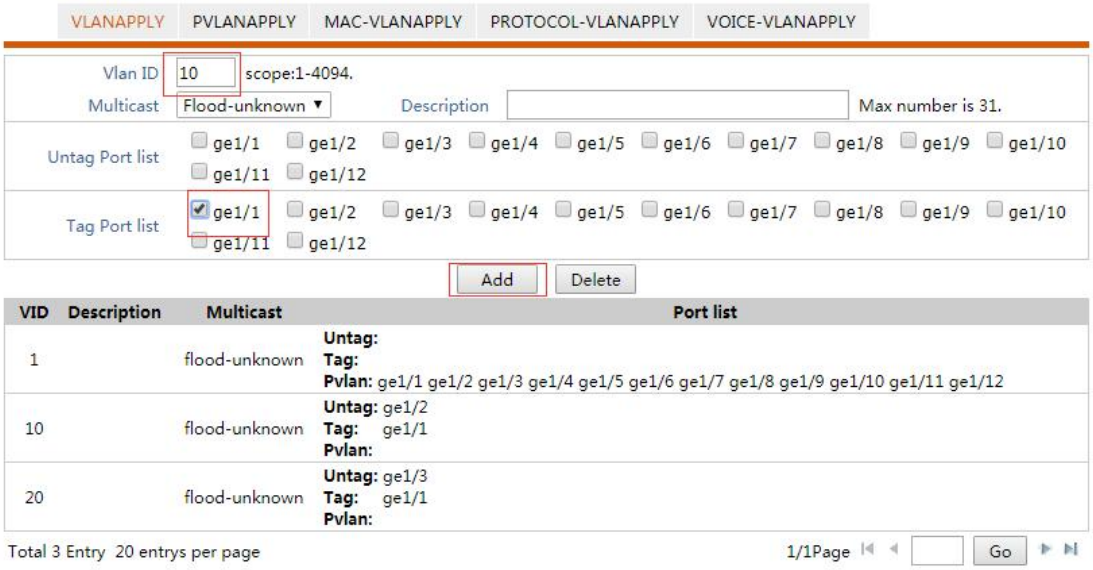
2. Configure SwitchA Ethernet interface ge1 / 2 and ge1 / 3 need to untag joins link port joins VLAN. Click the navigation tree "Layer Configuration> VLAN Configuration> VLANConfiguration" menu, enter "VLAN Configuration" screen, enter Vlan ID "10", in the "Untag port list" Select Port ge1 / 2. Similarly, enter "TRUNK Configuration" screen, enter Vlan ID "20", the "Untag port list" select the port ge1 / 3. Click "Add" to complete the configuration, shown as below.



3. Configure SwitcB Ethernet interface ge1 / 2 and ge1 / 3 need to untag joins link port joins VLAN. Operation with 2, not repeat them.

4. Configure ge1 on SwitchA / 1 VLAN10 tagged mode and VLAN 20. Click the navigation tree "Layer Configuration> VLAN Configuration> VLAN Configuration" menu, enter "VLAN

Configuration" screen, enter Vlan ID "10", in the "Tag port list" Select Port ge1 / 1, click the "Add" . Similarly, enter "TRUNK Configuration" screen, enter Vlan ID "20", in the "Tag port list" Select Port ge1 / 1, click "Add" to complete the configuration, shown as below.



5. The agreements and associated VLAN, to implement the interface protocol to receive the packet belongs (family) type packets to assign different VLAN ID, according to the navigation tree, click the "Configuring Layer> protocol-vlan" menu and enter " protocol-vlan "screen, enter the appropriate value, the vlan10 bind ipv4, vlan20 bind ipv6, click" Add. " Complete the configuration, shown as below.

SerialNum	Port	Frame-type	Ether-type	Vlan Id	
1	ge1/2	ether2	arp	10	Delete
2	ge1/2	ether2	ip	10	Delete
3	ge1/3	ether2	arp	20	Delete
4	ge1/3	ether2	ip	20	Delete

5.4 Voice vlan

Voice data transmission priority of the traditional approach is to use the ACL (Access Control List) to distinguish between voice and data, and using QoS (Quality of Service) guarantee the transmission quality. To simplify user configuration and more convenient transport voice traffic management proposed Voice VLAN feature. Enable Voice VLAN function interface based on the interface into the data stream source MAC address field to determine whether the data stream for the voice data stream. Source MAC address complies with the voice device OUI (Organizationally Unique Identifier) address of packets that the voice traffic. Receiving voice data stream to the interface will automatically be added to Voice VLAN for transmission. Thereby simplifying the user configuration to achieve the user to easily manage voice data.

Voice VLAN OUI address

OUI address represents a MAC address segment. The 48-bit MAC address and the corresponding mask bit AND operation to determine the OUI. MAC address and OUI address bits match the access device, it is determined by the mask of all "1" in length. For

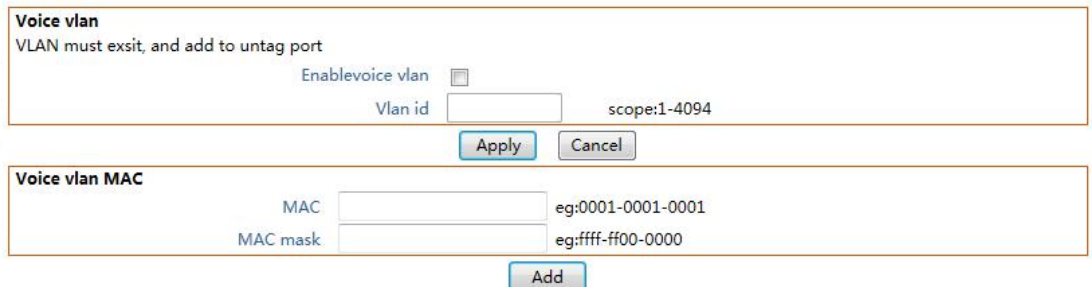
example, MAC address is 1-1-1, mask FFFF-FF00-0000, then the result will be the MAC address and its corresponding mask bits to perform operations that OUI address 0001-0000-0000.

Just before 24 match the first MAC address of the access device 24 and the OUI, then enable the Voice VLAN-enabled interface will find this data stream as voice traffic, access equipment is a voice device.

Voice VLAN for voice data stream into the user's VLAN. You can create a Voice VLAN and add the interface connected to a voice device to the Voice VLAN. Then voice data flows can be transmitted on the Voice VLAN.

Networks often exist voice data and non-voice data simultaneously two types of traffic. Voice data transmission is required to have a higher priority than other data traffic to reduce the delay and packet loss may occur during transmission.

1.Click the navigation tree "Layer Configuration> Voice vlan" menu, enter "Voice vlan" interface, shown as below.

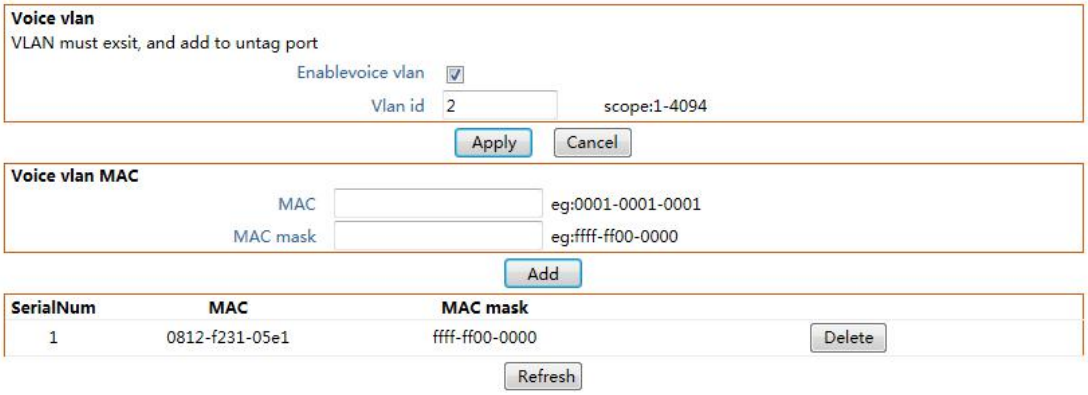


Interface information meaning as followings

2.Fill in the appropriate configuration items.

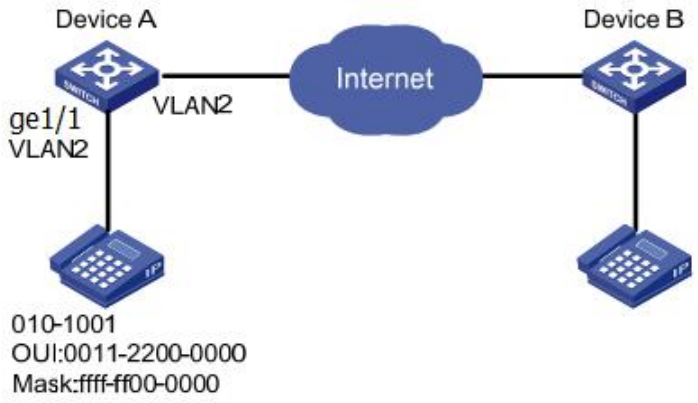
Configuration item	description
voice vlan	Check voice vlan
Vlan id	Required,add VLAN ID,range from 1~4094,such as 1-3,5,7,9. VLAN 1 is default,Other VLAN must exist and need to untag joins link ports.
MAC	Required.tEnter the specified OUI address voice messages.such as:0812-f231-05e1。
MAC mask	Required .Input mask. Such as: ffff-ff00-0000.

3.First click the "apply", then click "Add" to complete the configuration, shown as below.



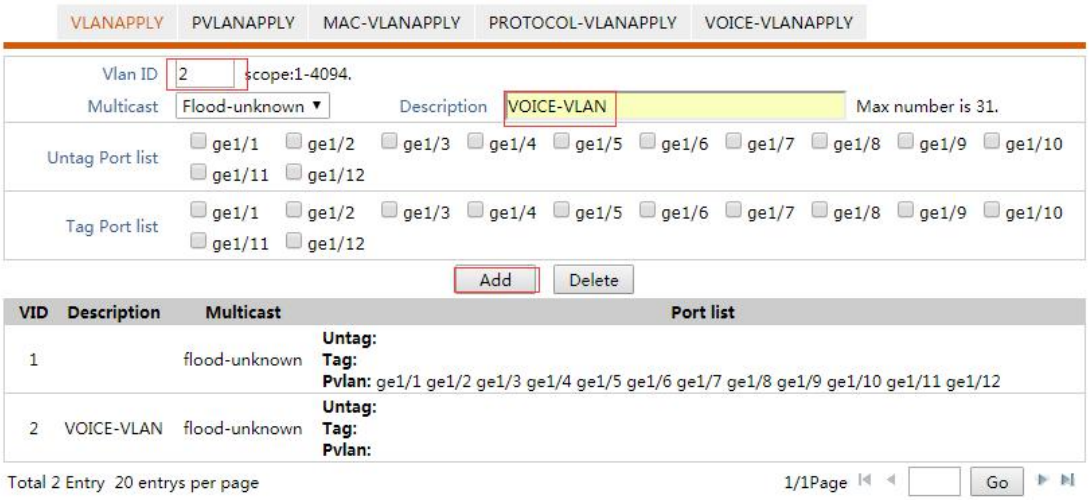
The following is an exsample:By configuring Voice VLAN in manual mode, so that access to IP telephony ports controlled by artificially join / quit Voice VLAN, and the VLAN voice traffic transmission. Create VLAN2 for the Voice VLAN, Voice VLAN to work in security mode and only allows voice
Data. IP phone sends untag voice traffic, the access port is a Trunk port ge1 / 1. Users need to set up a user-defined OUI address 0812-f231-05e1, the mask is ffff-ff00-0000.

Configure automatic mode Voice VLAN diagram.

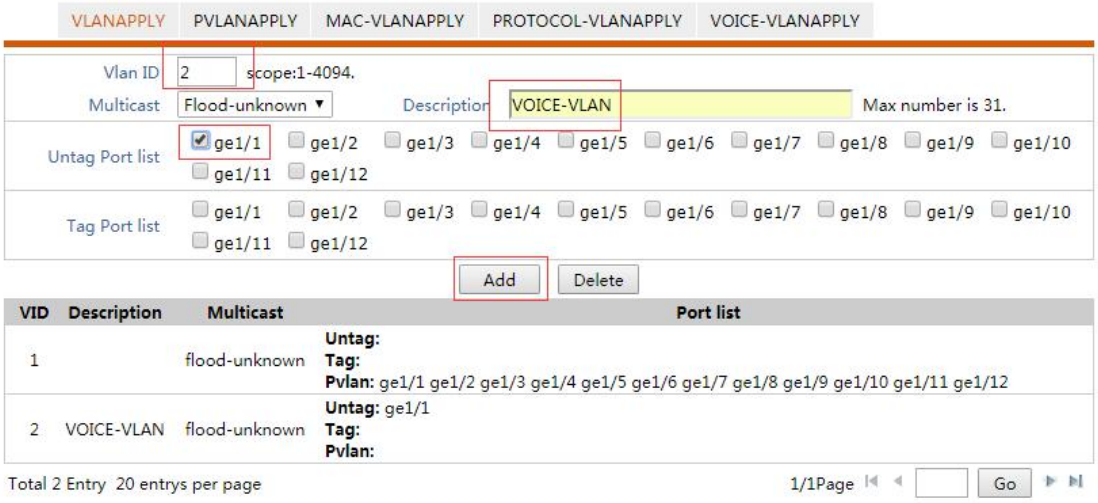


Steps:

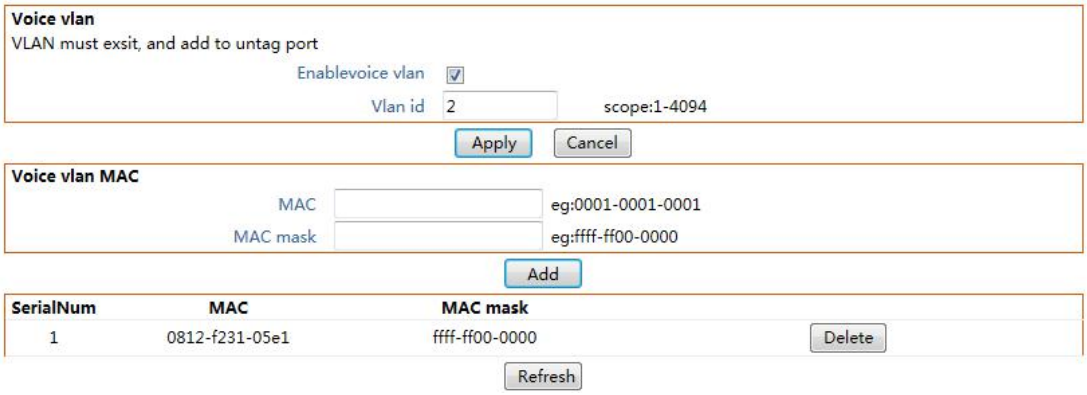
1. Create VLAN,assure the Vlan each service belongs to,Click the navigation tree "Layer Configuration> VLAN Configuration> VLAN Configuration" menu, enter the "VLAN Configuration" screen, create vlan2, select Flood-unknown, click "Add" to complete the configuration, shown as below.



2. Configure Switch Ethernet interface ge1 / 1 to untag way to join need to link the port joins VLAN. Click the navigation tree "Layer Configuration> VLAN Configuration> VLAN Configuration" menu, enter "VLAN Configuration" screen, enter Vlan ID "2", in the "Untag port list" Select Port ge1 / 1, click the "Add" complete the configuration, shown as below.



3. Click the navigation tree "Layer Configuration> Voice vlan" menu, enter "Voice vlan" interface, Tick the Enable voice vlan, enter Vlan id 2, click the "Settings", enter the MAC address language,0812-f231-05e1， MAC mask， ffff-ff00-0000,Click”add” to complete the configuration,show as below.



5.5 MAC Configuration

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:

- Destinate MAC address
- VLAN ID the ports belongs to
- 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.

5.5.1 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 not 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 "Layer Configuration> MAC Configuration> MAC Configuration" menu, enter "MAC Configuration"interface.

Interface information meaning as followings

Confi item	Description
MAC aging time	Enter the MAC aging time

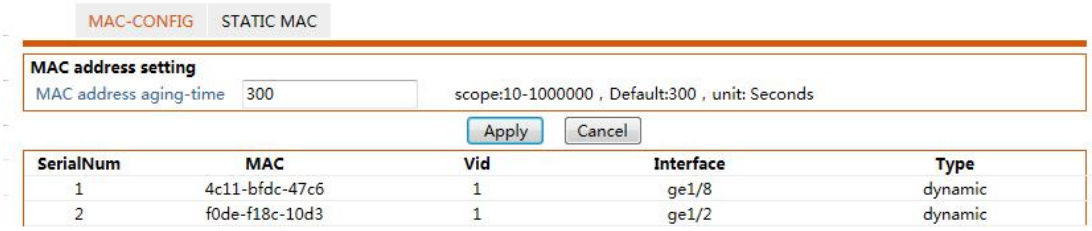
2. Fill in the appropriate configuration items.

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 "Layer Configuration> MAC Configuration> MAC Configuration" menu, enter "MAC Configuration" interface, shown as below.



Interface information meaning as followings

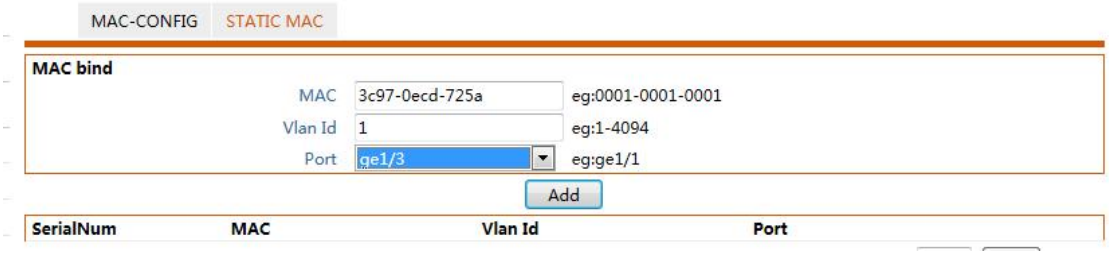
Item	Description
Serial Num	Sort No.
MAC	Destination MAC address
Vid	VLAN ID port belongs to
Iinterface	Forwarding egress port number
Type	Dynamic MAC addresses that can be configured by the user according to the aging time and aging out MAC address table, the switch can add dynamic MAC address entry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

5.5.2 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 "Layer Configuration> MAC Configuration> 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.

5.6 MSTP Configuration

Ethernet switching network to link backup and enhance network reliability, often redundant

links. However, the use of redundant links are 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).Development 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

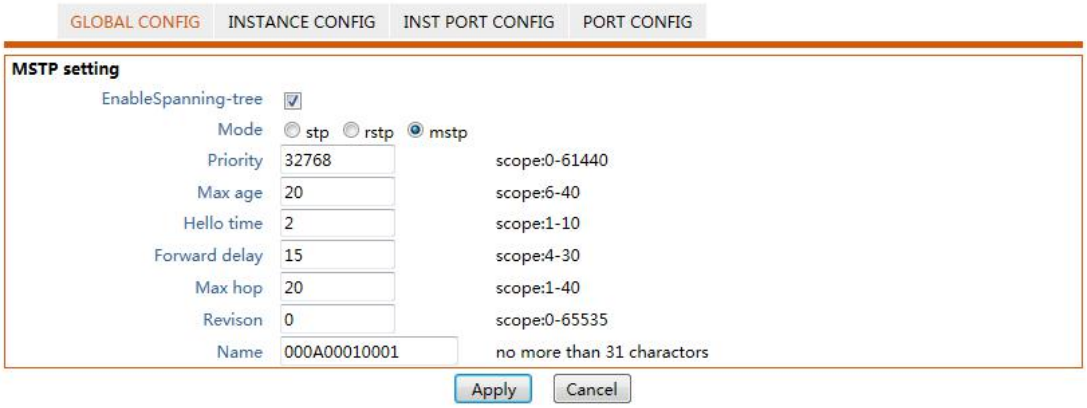
- Link Backup: when the currently active path fails, the activation link redundancy, restore the network connectivity.

5.6.1 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 "Layer Configuration> Spanning TreeConfig> Global Configuration" menu, enter the "Global Configuration" screen, shownas below.



Interface information meaning as below

Configuration Item	Description
Start Using Spanning-tree	Ticked by default, assure that the switchstart 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.
Revison	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.

5.6.2 Instance Configuration

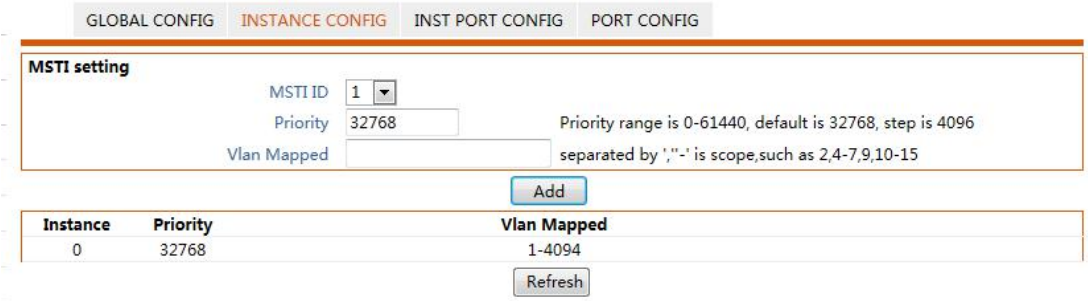
By MSTP divides a switched network into multiple regions, each of which has multiple trees spanning independent of one another. Each spanning tree is called an MSTI MSTI (Multiple Spanning Tree Instance), each region is called an MST region (MST Region: Multiple Spanning Tree Region).

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 "Layer2 Configuration> MSTP Configuration> Instance Configuration" menu, enter "instance configuration" interface,shown as below.

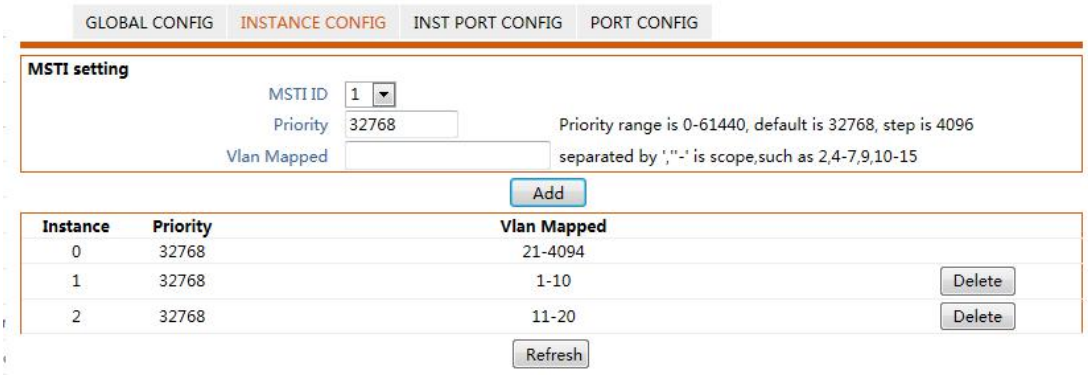


Interface information meaning as followings.

2.Fill in the appropriate configuration items.

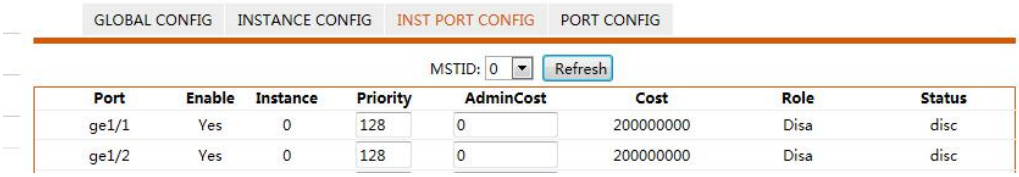
Configurate Item	Description
MSTI ID	Enter any instance number during 1-63.
Priority	Setting specifies the priority of the instance, it must be a multiple of 4096. Its range is 0 to 65535. The default value is 32768.
Vlan Mapped	Enter the desired VLAN mapping

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



5.6.3 Examples port configuration

1.Click the navigation tree "Layer2 Configuration> MSTP Configuration> instance Port Configuration" menu, enter "instance Port Configuration" screen, shown as below.



Interface information meaning as followings:

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

Configurate 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’select,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	Inculding 2 status,discarding and forwarding

5.6.4 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 "Layer Configuration> MSTP Configuration> Port Configuration" menu, enter the "Port Configuration" screen, shown as below.

Interface information meaning as followings.

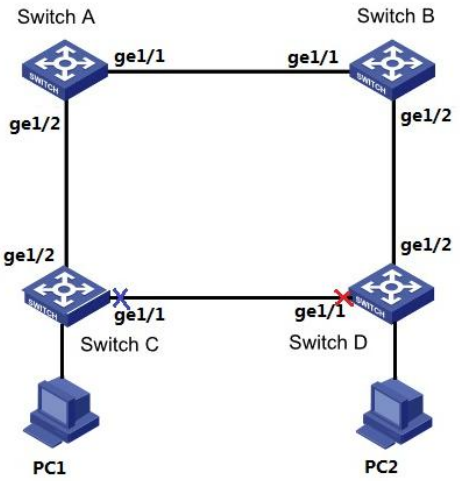
Configurate Item	Description
Port	Not selectable. Port list
Enable	Radio. Choose whether to open the port configuration or not. Ticked and unticked. The default is unticked.
BPDU Guard	Radio. Choose whether to open the BPDU protection function. Ticked and unticked two cases. The default is unticked. 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.

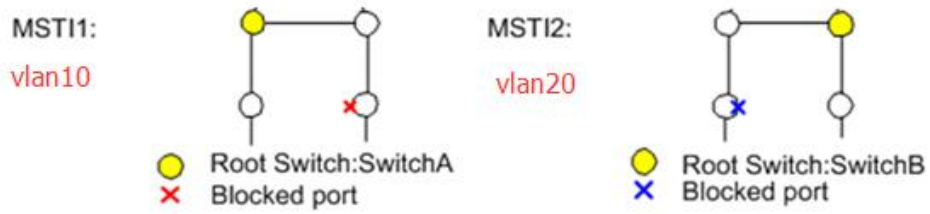
2.Fill in the appropriate configuration items.

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

Example for Configuring MSTP

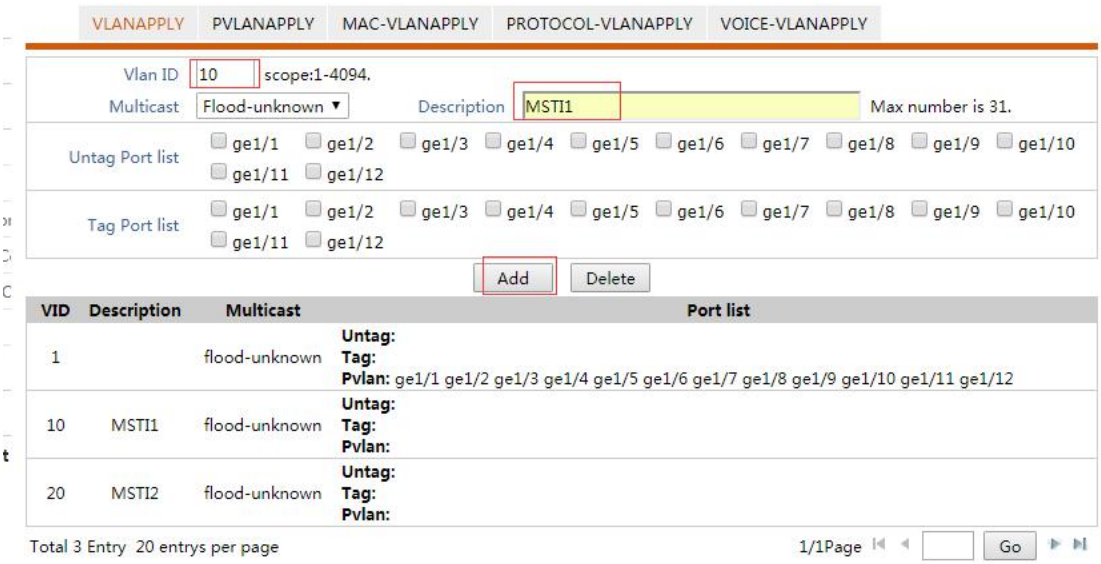
SwitchA, SwitchB, SwitchC and SwitchD run MSTP. To achieve VLAN10 VLAN20 and traffic load balancing, MSTP introduces multi-instance. MSTP VLAN mapping table can be set to VLAN and MSTI associated Instance 1 Map VLAN10, Example 2 mapping VLAN20.





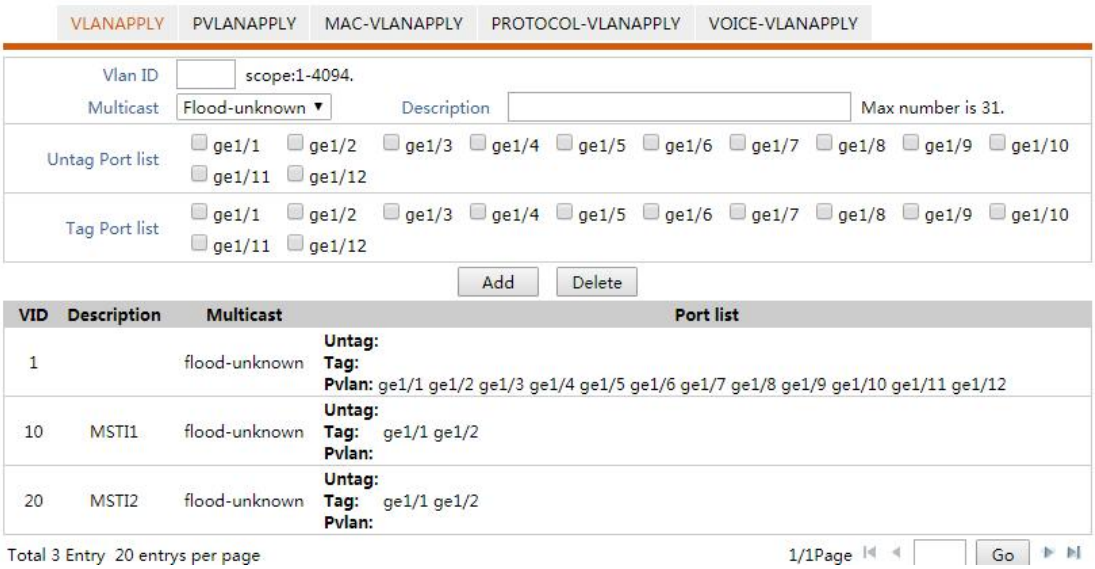
Steps

1.Configuring the device in the ring network Layer 2 forwarding function, create VLAN10, vlan20 on the switching device SwitchA, SwitchB, SwitchC and SwitchD. Click the navigation tree "Layer Configuration> VLAN Configuration> VLAN Configuration" menu, enter the "VLAN Configuration" screen, fill in the appropriate configuration, select Flood-unknown, click "Add" to complete the configuration, shown as below.

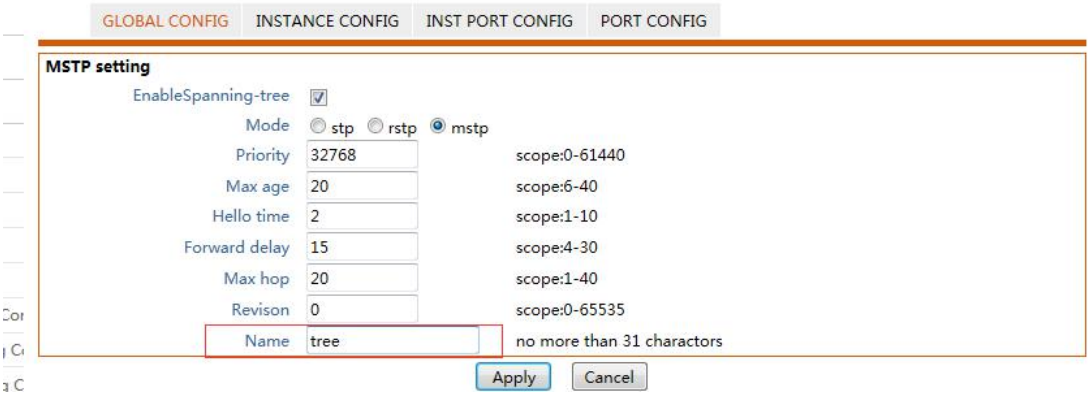


1.The switch device add VLAN on the access loop port. Click the navigation tree "Layer Configuration> VLAN Configuration> VLAN Configuration" menu, enter "VLAN Configuration" screen, enter the permit VLAN10, VLAN20 through Trunk port, Tag port list,

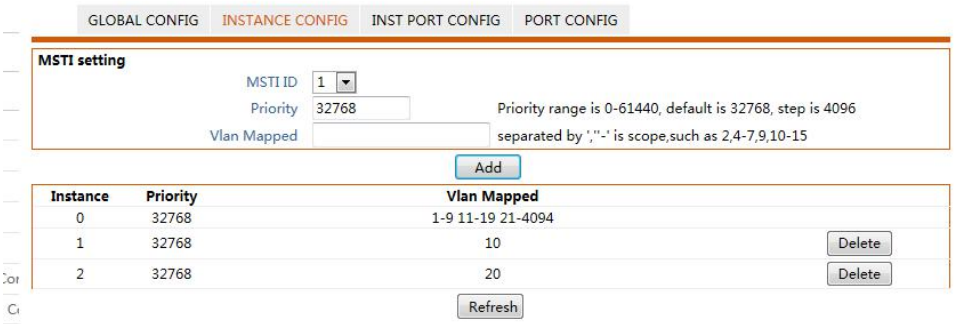
Tick"ge1 / 1, ge1 / 2 ",click" Add "to complete the configuration



2.Configure SwitchA, SwitchB, SwitchC and SwitchD to the domain name of the domain tree. Click the navigation tree "Layer Configuration> MSTP Configuration> Global Configuration" menu, enter the "Global Configuration" and fill in the appropriate configuration interface ,shown as below.

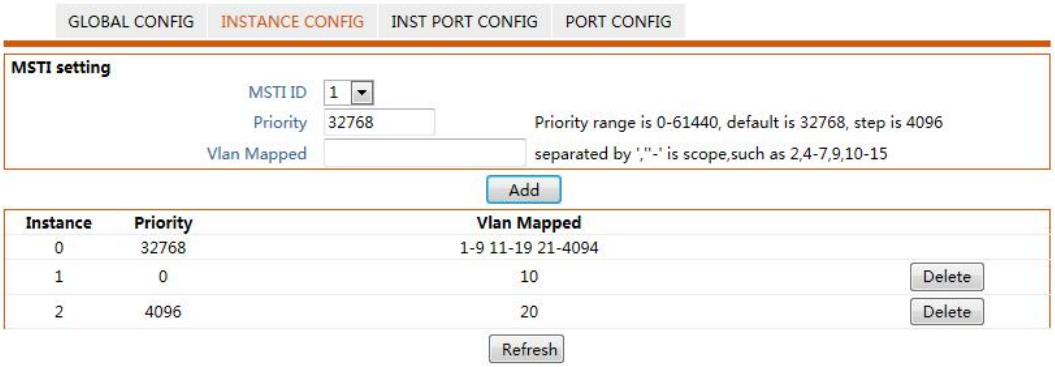


4.Create an instance and instance MSTI1 MSTI2. Click the navigation tree "Layer Configuration> MSTP Configuration> Instance Configuration" menu, go to "instance configuration", fill in the appropriate parameters, click "add" interface is shown below.



5.In the domain, and configure MSTI1 MSTI2 root bridge and root bridge is configured

as the root bridge SwitchA MSTI1, configuration SwitchA MSTI2 the root bridge. Click the navigation tree "Layer Configuration> MSTP Configuration> Instance Configuration" menu, go to "instance configuration", fill in the appropriate parameters, click "add" interface is shown below.



Attention:

When configuring SwitchA Change MSTI1 priority to 0, MSTI2 priority to 4096.

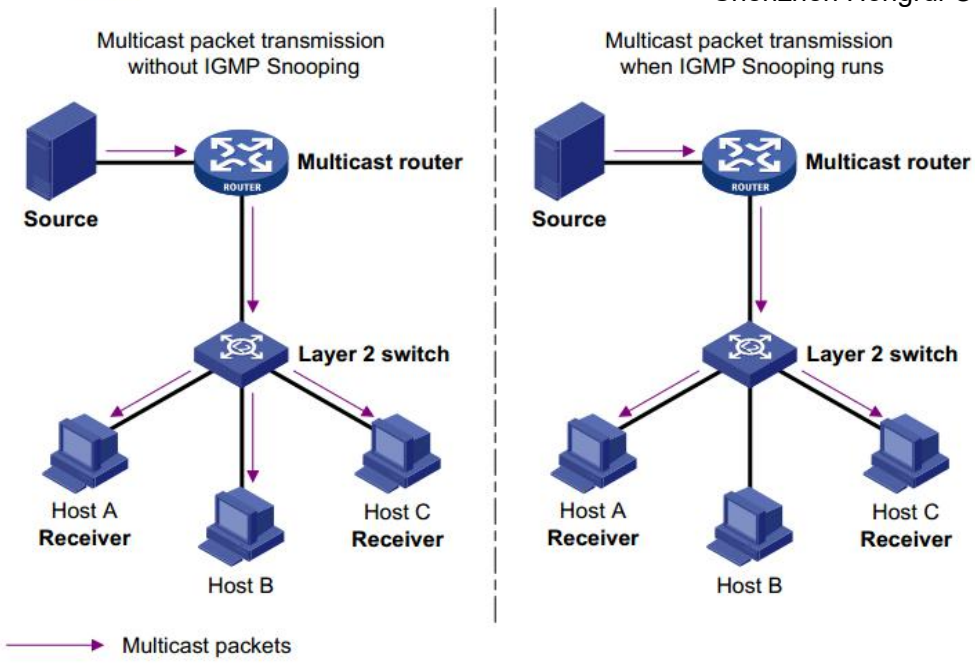
When configuring SwitchB change MSTI1 priority to 4096, MSTI2 priority to 0. Configuration consistent with SwitchA, not repeat them.

Priority must be a multiple of 4096

6.In the domain, and configure MSTI1 MSTI2 root bridge and root bridge, configure SwitchB as the root bridge MSTI2, configuration SwitchB MSTI1 the root bridge. The procedure is the same as 5, not repeat them.
7. After the above configuration, network pruned into a tree, the purpose of eliminating loops.

5.7 IGMP-snooping Configuration

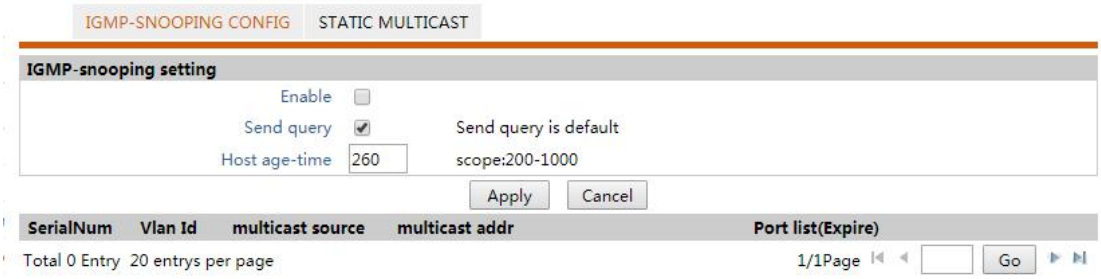
IGMP Snooping (Internet Group Management Protocol Snooping) is a multicast control mechanism running on Layer 2 devices to manage and control multicast groups.
Layer 2 device IGMP Snooping By analyzing received IGMP messages, analyze, ports and multicast MAC addresses to establish a mapping relationship, 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.



5.7.1 IGMP-snooping Configuration

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 "Layer2 Configuration> IGMP-snooping Configuration> IGMP-snooping Configuration" menu, enter "IGMP-snooping Configuration" screen as shown below.



Interface information meaning as followings.

Config Item	Description
Enable IGMP-snoopingConfi	To globally enable IGMP Snooping situation is not configured IGMP Snooping in the VLAN. Radio, and go into enable 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.

5.7.2 Static 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

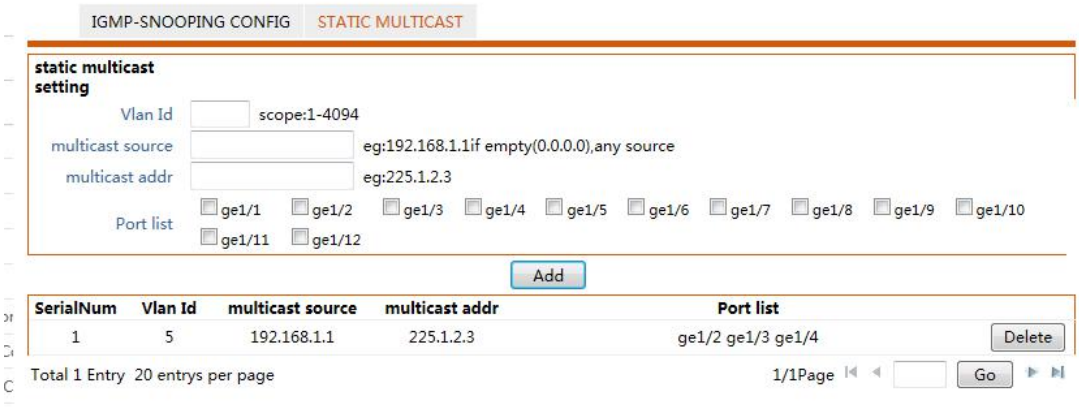
1.Click the navigation tree "Layer Configuration> IGMP-snooping configuration> Static Multicas settingt" menu, enter "static multicas settingt" interface as shown below.

Interface information meaning as followings.

Config 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 addr	Enter the multicast address
Port list	Joins the multicast members, you can multi-select

2.Fill in the appropriate configuration items.

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



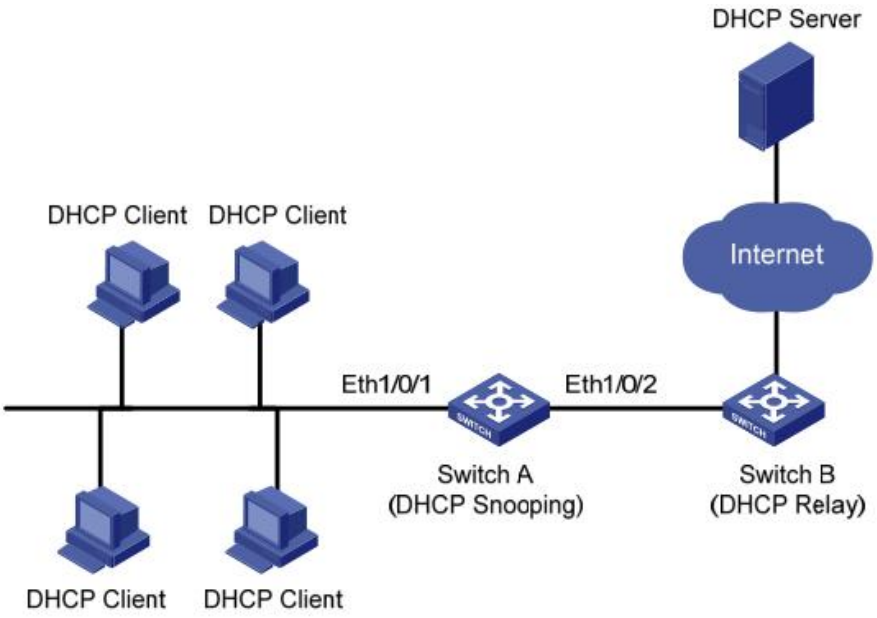
5.8 DHCP-snooping Configuration

Because of security , the network administrator may need to record IP addresses used by Internet users to confirm the correspondence between the user obtained from the DHCP server IP address and the user host MAC address.

The switch can record the user's IP address information at the network layer security features of DHCP relay by running. Switches can be run at the data link layer monitor function DHCP Snooping DHCP packet, records the user's IP address information. Further, in the network if there is an unauthorized DHCP server may obtain invalid IP addresses. In order to enable users to obtain authorized DHCP server IP address, DHCP Snooping security mechanism allows the port to a trusted port or an untrusted port.

An untrusted port is authorized DHCP server directly or indirectly connected. Port Trust received DHCP packets forwarded, to guarantee that DHCP clients can obtain valid IP addresses.

Mistrust port is connected to an authorized DHCP server connections. If you received from the port to the DHCP server responds DHCP-ACK and DHCP-OFFER packets are discarded, preventing DHCP clients from receiving invalid IP addresses.



DHCP Snooping Typical Networking

DHCP Snooping through the following two methods to obtain the IP address and the MAC address of the user to obtain information from the DHCP server:

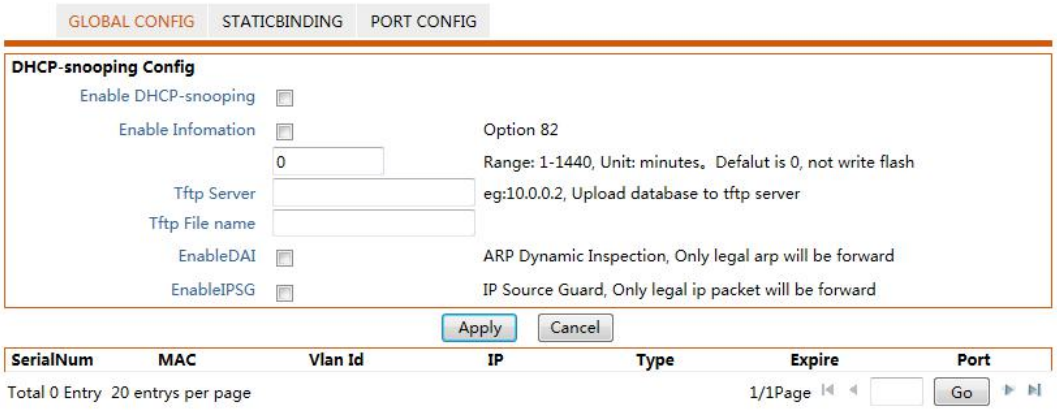
- Monitoring DHCP-REQUEST packet
- Monitoring DHCP-ACK packet

5.8.1 DHCP-snooping Global Configuration

Enable DHCP-snooping

Steps

1.Click the navigation tree "Layer2 Configuration> DHCP-snooping Configuration> Global Configuration" menu, enter the "Global Configuration" screen as shown below.



Interface information meaning as followings.

2.Fill

Config item	Description
Enable DHCP-snooping	Opening and closingDHCP-snooping
Enale Infomation	Open DHCP Snooping to support Option 82
Write delay	Range from 1-1440, in minutes. Default 0 means no written
TFTP server	Upload database to ftp server
TFtp file name	Save ftp server file name
Enable DAI	Dynamic ARP inspection, only forwards legitimate host sends ARP
Enable IPSG	IP source address check, forwards only legitimate host to send IP packets

in the appropriate configuration items.

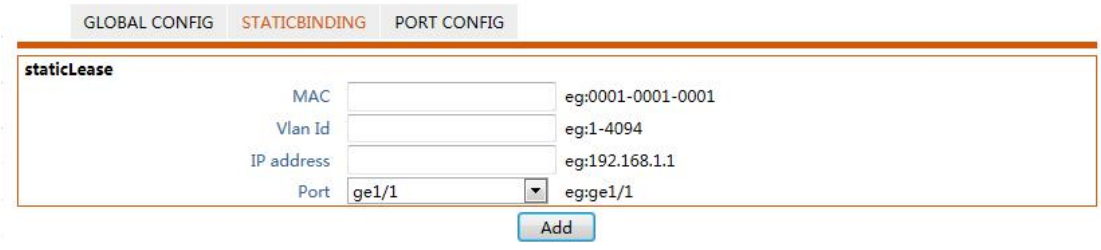
3.Click “Apply” , to complete the configuration.

5.8.2 Static BINDING

In DHCP network, users get a static (non-DHCP user) may be multiple attacks on the network IP address, such as fake DHCP Server, configured false DHCP Request packets. This will legitimate DHCP users use the network normally brings some security risks.
In order to effectively prevent non-DHCP user attack, it can open the static MAC address entry function device generates an interface based on DHCP Snooping binding table. Thereafter, the device will generate a static MAC entries based on these user interface corresponding to the user all DHCP DHCP Snooping binding table entries automatically execute the command, and at the same time close the dynamic MAC entries learned by an interface capabilities. At this time, only the source MAC static MAC packets whose entries match through the interface, otherwise, the packets are discarded. Therefore, for non-DHCP users on the interface, only the administrator to manually configure static MAC entries such users whose packets can pass through, otherwise the packet is discarded.

Steps

1. Click the navigation tree "Layer2 Configuration> DHCP-snooping configuration> Static BINDING" menu, enter the "Global Configuration" screen as shown in the following figure.



Interfaceinformation meaning as followings.

Config item	Description
MAC	Bound User MAC address

Vlan Id	VLAN number the user belongs to
IP addr	Static IP address of the user
Port	Switch Port Mapping

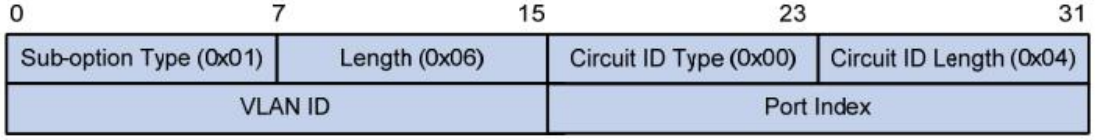
2.Fill in the appropriate configuration items.
3.Click "Add" to complete the configuration, as shown below.

5.8.3 DHCP-snooping port configuration

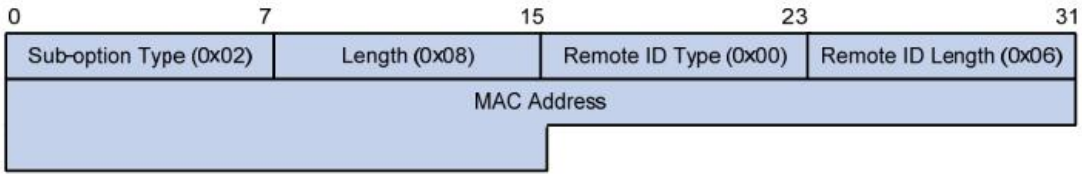
In the network if there is an unauthorized DHCP server may obtain invalid IP addresses. In order to enable users to obtain authorized DHCP server IP address, DHCP Snooping security PS7024 Ethernet switches, allows the port to a trusted port or an untrusted port.

- An untrusted port is authorized DHCP server directly or indirectly connected. Port Trust received DHCP packets forwarded, to guarantee that DHCP clients can obtain valid IP addresses.
- Mistrust port is connected to an authorized DHCP server connections. If you received from the port to the DHCP server responds DHCP-ACK and DHCP-OFFER packets are discarded, preventing DHCP clients from receiving invalid IP addresses.

Option 82 is a DHCP packets in the relay agent option (Relay Agent Information option), which records the location information of the DHCP client. After the DHCP relay (or DHCP Snooping device) receives a DHCP client sends a request to the DHCP server packets, you can add Option 82 to the packet so that the administrator locate the DHCP client, the client's security and counter fees control. Support Option 82, the server can also assign policies to develop IP address and other parameters based on the information this option provides a more flexible address allocation.
Option 82, can contain up to 255 sub-options. If the definition of Option 82, at least to define a sub-option. Currently the device supports two sub-options: Circuit ID sub-option and Remote ID sub-option.
Since there is no unified definition in RFC 3046 Option 82 content vary with vendors need to be filled. Ethernet switch as the DHCP relay device that supports extended padding format of Option 82 sub-option, the default padding contents in case of the following figure. The contents of sub-option 1 belongs to the port that received the DHCP client request packets VLAN ID and port index (port index value of the physical port number by 1).



The contents of sub-option 2 that received the DHCP relay DHCP client request packets the bridge MAC address.



DHCP Relay Option 82 support mechanism

DHCP client obtains an IP address from the DHCP server through the DHCP relay process and directly from the DHCP server IP address is basically the same, go through discovery, offer, select and confirm the four stages, described here only DHCP relay support Option mechanism 82, as follows:

(1) DHCP relay device receives the DHCP request packets, checks whether the packet contains Option 82, and make the appropriate treatment.

- If the request packet contains Option 82, DHCP relay device in accordance with the policy configuration of the packet processing (discard, relay device itself with the Option 82 packets substitute any original Option 82, or keep the newspaper option 82, the text of the original), and then forwards the request packet to the DHCP server.
- If the request packet does not Option82 option, the DHCP relay device adds Option 82 to the DHCP server to add to the forwarding messages later.

(2) After the DHCP relay device receives the DHCP server returns the packet, the release packets Option 82 information with the DHCP configuration information packets forwarded to the DHCP client.

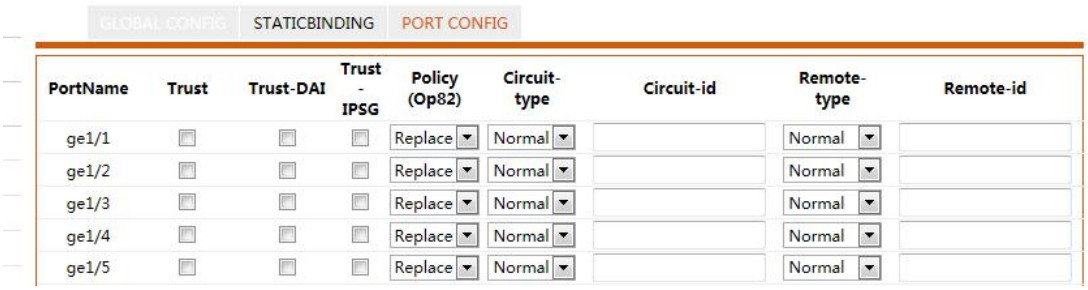
✍illustrate:

DHCP request packet sent by the client, there are two, namely DHCP-DISCOVER packets and DHCP-REQUEST packet. Due to different manufacturers DHCP server device on request processing packets in different ways, some devices handle DHCP-DISCOVER packets in the Option 82 information, while others deal with DHCP-REQUEST packets in the Option 82 information, DHCP relay device the all adds option 82 in two packets.

After the switch is configured with DHCP Snooping, and Option 82 support, when DHCP DHCP client sends the received request packet contains Option 82, depending on the configuration of processing strategies and sub-option, DHCP Snooping for packets different mechanism.

Steps:

1. Click the navigation tree "Layer2 Configuration> DHCP-snooping Configuration> Port Configuration" menu, enter the "Port Configuration" screen as shown below.



Interface information meaning as followings.

Config item	description
Port name	Not selectable
Trust	You can tcik a trusted port, unticked means the untrusted port.
Trust-DAI	Dynamic ARP inspection, only forwards legitimate host sends ARP
Trust-IPSG	IP source address check, forwards only legitimate host to send IP packets
Policy(Op82)	Open DHCP Snooping support Option 82 function
Circuit-type	Filling Option type Circuit ID field of 82 (Normal and string)
Circuit-id	Filling contents Circuit ID field in Option 82 (such as user-defined content abcd)
Remote-type	Fill in the Remote-id Option Type field of 82 (Normal, sysname and string)
Remote-id	Content (such as custom content abcd) in the Remote-id field is filled Option 82

After the device is configured with DHCP Snooping and DHCP Snooping to support Option 82 When the DHCP client receives a DHCP request sent packets containing Option 82, the process according to the configuration of different strategies and sub-option, DHCP Snooping packets different mechanisms, the table below

Processing Policy	Sub-option	DHCP Snooping device for packet processing instructions
Drop		Discarded packets
Keep		Holding packets of the Option 82 unchanged and forwards
Replace	No configuration sub-option content	Option 82 is filled with the default content field, replacing the original Option 82 with options and forwards
	Configured the Circuit ID sub-option	The Option82 option Circuit ID populated user-defined content (storage format ASCII), replace the original Option 82 options and forwards
	Configured the Remote ID sub-option	Remote ID option will Option82 filled with user-defined content storage format ASCII), replace the original Option 82 options and forwards

If received request messeage from DHCP client sent don't have "option82",forwarding

packets after filled option fields according to configured sub-option

Sub-option	DHCP Snooping device for packet processing
No configuration sub-option content	Default content filling packets Option 82 field and forwards
Configured the Circuit ID sub-option	The Option82 option Circuit ID populated user-defined content (storage format ASCII) and forwards
Configured the Remote ID sub-option	Remote ID option will Option82 filled with user-defined content (storage format ASCII) and forwards

---

✍illustrate:

Option 82 field for the content of sub-option Circuit ID or Remote ID sub-option configured independently and can be individually configured to be configured at the same time, in no particular order and configuration order.

DHCP Option82 must be configured in the user side of the device. Otherwise, DHCP packets sent from the device to the DHCP Server option does not carry Option82 content.

When the DHCP server receives a DHCP response packet, if the packet contains Option 82, is deleted Option 82 field forwards; if the packet does not contain Option 82, is forwarded directly.

2.Fill in the appropriate configuration items.

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

DHCP Snooping Configuration Examples

a. DHCP Snooping support Option 82

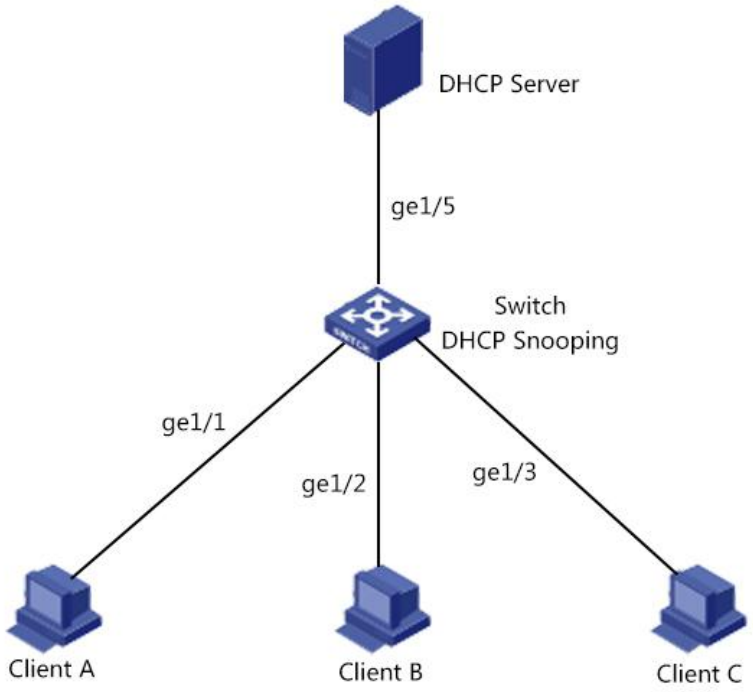
As shown in the following figure, Switch Port ge1 / 5 is connected to the DHCP server, port ge1 / 1, ge1 / 2, ge1 / 3 respectively DHCP Client A, DHCP Client B, DHCP Client C is connected.

Open the DHCP Snooping on the Switch.

Settings SwitchA port “ge1 / 5” as DHCP Snooping trusted port.

Open DHCP Snooping Option 82 support on the Switch. Elapsed port ge1 / 3 message, press the Option 82 padded switch Circuit ID and Remote-id default configuration.

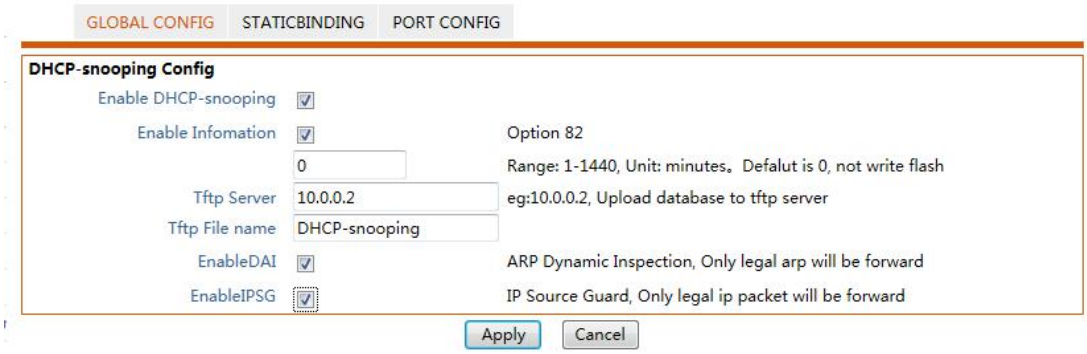
Network diagram



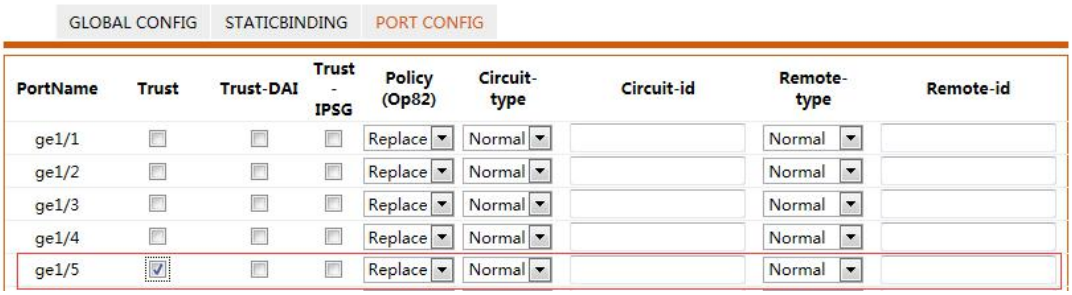
Configurate DHCP Snooping Support optiona 82 function Diagram

Steps:

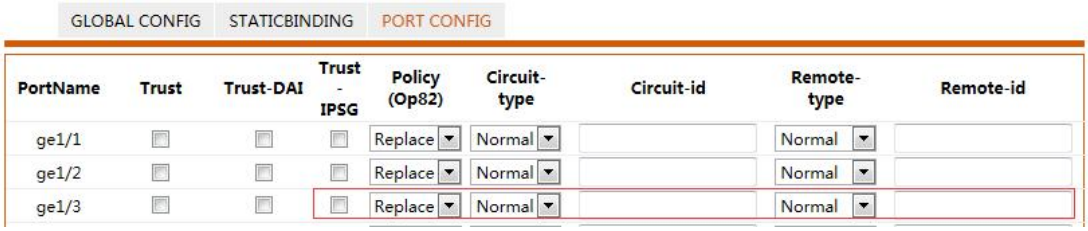
1. Turn the switch DHCP Snooping function. Click the navigation tree "Layer2 Configuration> DHCP-snooping Configuration> Global Configuration" menu, enter the "Global Configuration" screen as shown below.



1. Set the port ge1 / 5 as DHCP Snooping trusted port. Click the navigation tree "Layer Configuration> DHCP-snooping Configuration> Port Configuration" menu, enter the "Port", fill in the appropriate configuration, click "Apply." Interface is shown below.



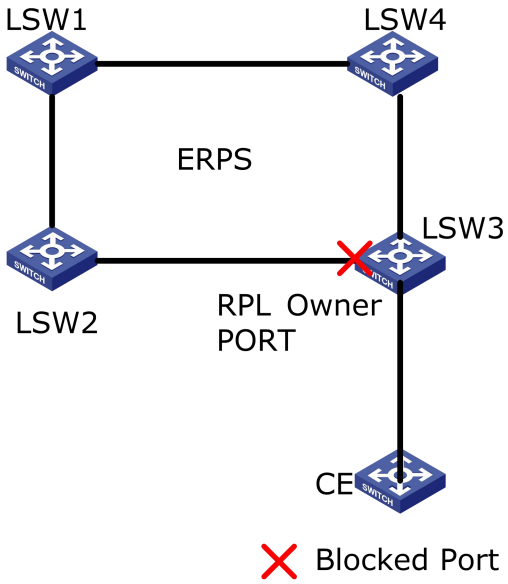
2. Ethernet port ge1 / 3 configurations for DHCP packets with Option Circuit ID in Remote-id 82. Click the navigation tree "Layer Configuration> DHCP-snooping Configuration> Port Configuration" menu, enter the "Port", blank and click "Apply." Interface is shown below.



5.9 ERPS-Ring Configuration

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.



5.9.1 ERPS-Ring Golable Configuration

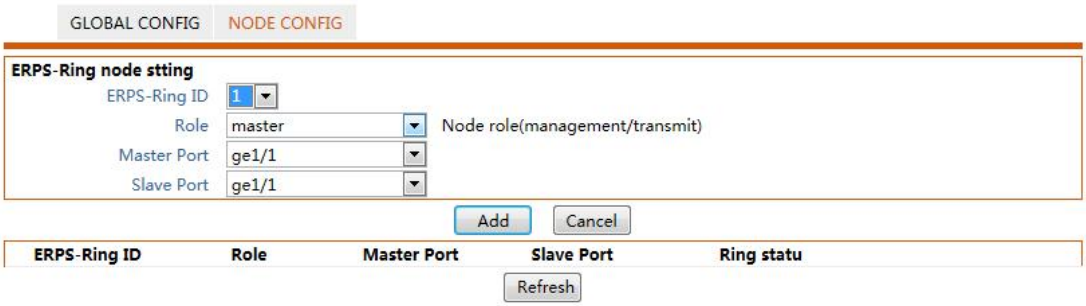
Enable ERPS-Ring

1.Click the navigation tree "Layer Configuration> ERPS-Ring Configuration> Global Configuration" menu, enter the "Global Configuration", after ticked, click the "Apply" . interface as shown below.

5.9.2 Node Configuration

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 "Layer Configuration> ERPS-Ring Configuration > Node Configuration" menu, enter the "Node Configuration" screen as shown below.



Interface information meaning as followings.

Config item	Description
ERPS-Ring ID	ERPS-Ring(0-15 instances Optional)
role	The node (managed node / transit node)
Master port	Port can forward user traffic and receive / transmit ERPS protocol packets.
Slave port	ERPS port only sends and receives packets.

2.Fill in the appropriate configuration items.

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

5.10 GMRP Configuration

GARP Multicast Registration Protocol (GMRP) is a generic Layer 2 protocol standard, high efficiency and can support it on behalf of any multicast protocol, not just IP multicast. GMRP is described by 802.1d bridge protocol standards. A wish to receive a multicast group sent to the system's network traffic using GMRP to register with the adjacent switch. GMRP enable hosts, switches, routers, and network monitoring equipment they take the initiative to request the desired network traffic. After GMRP embodiment, the switch will no longer registered to the receiver port on the sending multicast frames. GMRP working process, a system using GMRP to register their desire to receive the multicast traffic. The system can request to receive the following frame:

In a particular multicast MAC address as the destination address of the multicast frames;

All multicast frames (as long as no manual filter table entry to prevent some of the traffic is forwarded). This service is called "All Groups" service and is likely to be registered by a router or network monitoring equipment.

No other filter table entry specifies all multicast frames whether they should be forwarded. This is called "all unregistered group" Generic Attribute Registration Protocol (GARP, General Attribute Registration Protocol) is provided to enable a workstation capable of

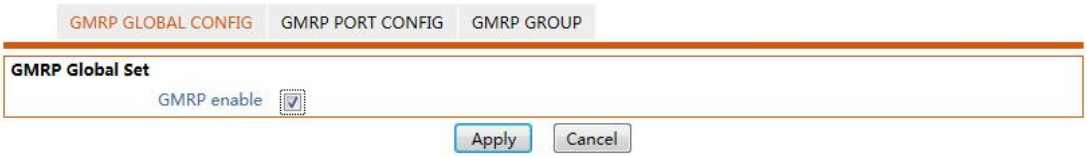
disseminating information through local area network LAN system registration information for some mechanism. GMRP is an application in the form of GARP. Another form GVRP, (GARP VLAN Registration Protocol), which is a workstation can dynamically join or quit a VLAN. GMRP is a Layer 2 protocol that can be implemented in the NIC driver. When a system joins a multicast group by IGMP protocol when the network card driver can send a message to the adjacent GMRP registration switch automatically, you do not need to snoop.

GARP works points:

System is directly connected to the switch by issuing 2 Join messages to register a group; the system must refresh its membership by periodically sending a new join message; workstation by sending a leave message to exit a group; if you exit the message is lost, the switch still we hope that the workstation is still retained within the group. After a long period of time, leave all switch sends a message stating that if it does not soon receive new join message will terminate the registration of all ports. Since GMRP and GARP fully operational in the second layer, so it is easier than IGMP snooping is more accurate and more efficient.

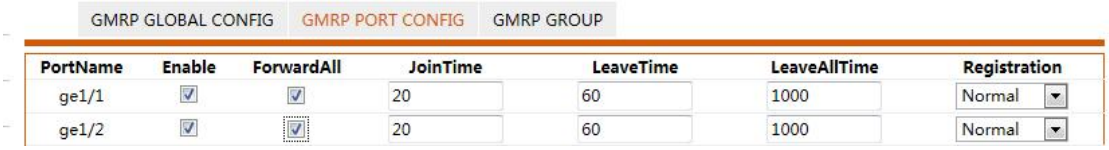
5.10.1 GMRP Globle Configuration

Enable GMRP Procedure
1.Click the navigation tree "Layer2 Configuration> GVRP Configuration> GMRP Global Configuration" menu, enter "GMRP global configuration," tick "Enable GMRP", click "Apply" to complete the configuration. Interface is shown below.



5.10.2 GMRP Port Configuration

Steps
1. Click the navigation tree "Layer Configuration> GMRP Configuration> GMRP Port Settings" menu, enter "GMRP Port Settings", Tick "Enable",tick "ForwardAll", default Join Time, Leave Time, LeaveAll time, select "Registration" Normal, click "Apply" to complete the configuration. Interface is shown below.



Interface informtion meaning as followings.

Config item	Description
Port Name	You can select multiple ports
Enable	tick or untick
ForwardAll	ForwardAll
Join time	By periodically sending a new message to join refresh its membership, periodic time range is 1-400000000, the default is 20
Leave time	Workstation by sending a leave message to exit a group, if you exit the message is lost, the switch still considers the workstation still want to keep in a group. Exit message retention time range is 1-400000000, the default is 60
Leave all time	After a long period of time, leave all switch sends a message stating that if it did not join soon receive a new message, it will terminate the registration of all ports. The range is 1-400000000, the default is 60

6 Network security

6.1 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 "Layer Configuration> Network Security> Access Control" menu, enter "Access Control" interface as shown below.

Interface information meaning as following.

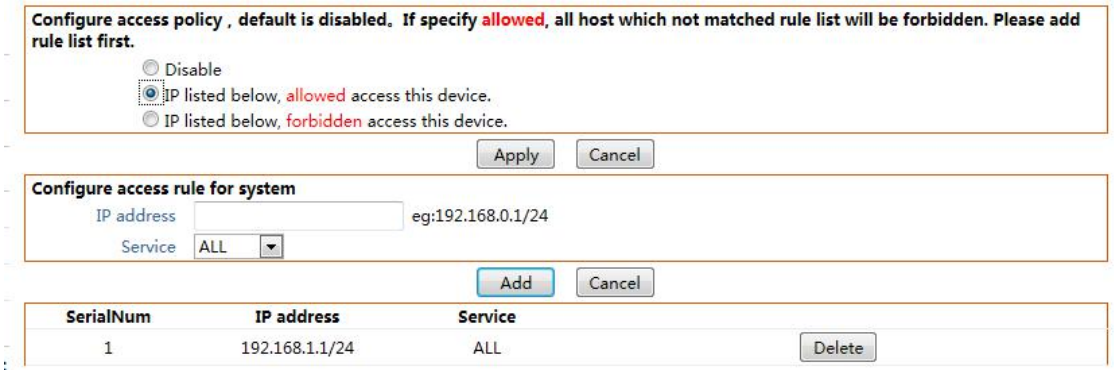
Config item	Sub-Option	Description
Configure access policy	Disable	Disable by default
	Host who meet the following rules to allow access to the corresponding service equipment	
	Host who meet the following rules to prohibit access to the corresponding service equipment	
Configue access rule for system	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 can not access the web.

2. First set up the device access rules, click the navigation tree "Layer Configuration> Network Security> Access Control> Set the device access rules" menu, enter the IP address 192.168.1.1/24, service options all, click "Add" As shown below:

3. then setting filter rules, click the navigation tree "Layer Configuration> Network Security> Access Control> Set filtering rules" 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:



6.2 Attack prevention settings

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

Steps

1. Choose the "Layer Configuration> Network Security> Anti-Attack Settings" menu, go to "attack prevention settings", respectively, to enable "ignore ping packet", "prevent SYN

DOS attacks," set "CPU receives data packets threshold ", click" Apply "to complete the configuration interface as shown below.

Inerface information meaning as followings.

Config item	description
Ignoreping	Ignore ping attacks
SYN DOS attack	TCP SYN attack prevention
CPU receive threshold	Range: 0-100000 (the default is 0, indicating limited speed), the threshold is exceeded, the packet is not received

6.3 ACL Configuration

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 particular 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:基本 IP ACL (Basic IP ACL): Rules are based on source IP address of the packet. ACL ID range: 100 to 999.

Advanced IP ACL (Advanced IP ACL): rules based on source IP address, destination IP address, protocol type over IP, and protocol-specific features such as three, four information. ACL ID range: 100 to 999.

Layer ACL (L2 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

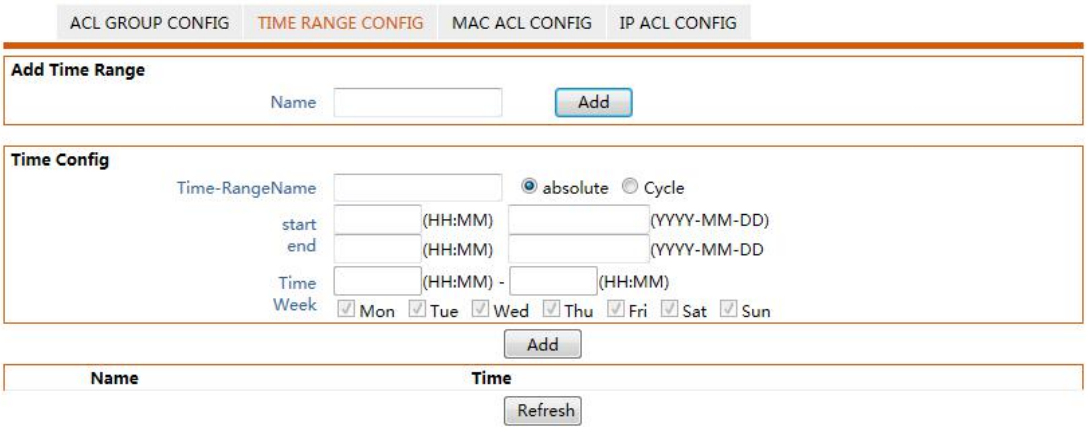
99.

6.3.1 TIME RANGE Configuration

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

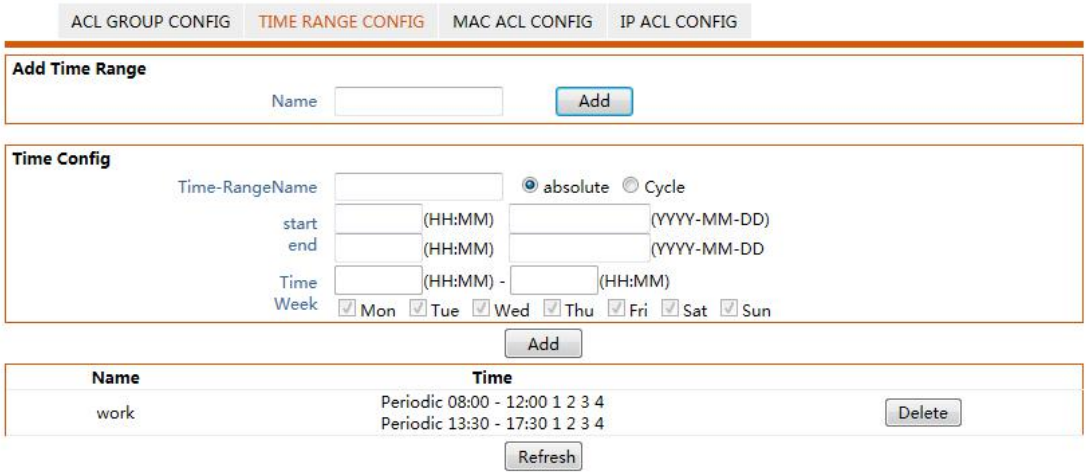
Click in the navigation tree "Network Security> ACL Configuration> TIME RANGE Configuration" menu, enter "TIME RANGE Configuration" screen, as shown below.



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.

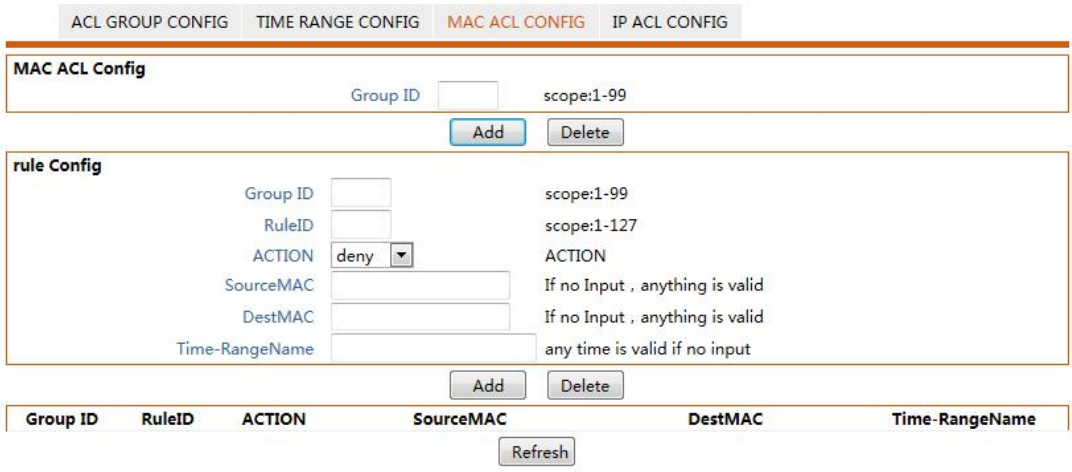


6.3.2 MAC ALC Configuration

Layer2 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 Configuration> MAC ALC Configuration" menu, enter "MAC ALC Configuration" screen as shown in the following figure.



Interface information meaning as followings.

Config item	description
Group ID	Layer2 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

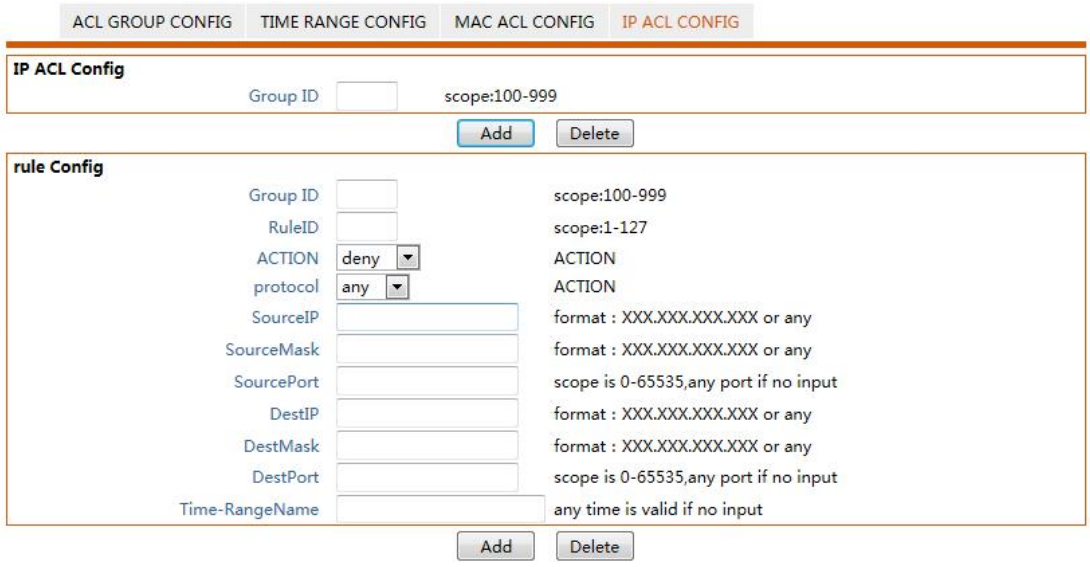
	"deny" (reject) rules.
SourceMAC	ACL rule source MAC address. Format for the H-H.
Dest MAC	ACL rule destination MAC address. Format for the H-H.
Time-Range name	Enter the configured time range name.

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

6.3.3 IP ALC Configuration

Basic IP ACL (Basic IP ACL): Rules are based on source IP address of the packet. ACL ID range: 100 to 999.
Advanced IP ACL (Advanced IP ACL): rules based on source IP address, destination IP address, protocol type over IP, and protocol-specific features such as three, four information. ACL ID range: 100 to 999

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



Interface information meaning as followings.

Config item	description
Group ID	Layer2 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
DestIP	Enter Destination IP of ACL rule
Dest mask	Enter the dest mask of ACL rule
Dest port	Enter the destination port ACL rule
Time-Rangename	Enter the configured time range name.

2.Fill in the appropriate configuration items.

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

Group ID	RuleID	ACTION	protocol	SourceIP	SourceMask	SourcePort	DestIP	DestMask	DestPort	TimeRange
100										
	1	permit	tcp	any	any	0	any	any	25	work
	2	permit	tcp	any	any	0	any	any	110	work
	3	permit	udp	any	any	0	any	any	53	work
	4	deny	ip	any	any	0	any	any	0	work

Refresh

6.3.4 ACL GROUP Configuration

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 Configuration> ACL GROUP Configuration" menu, enter "ACL GROUP Configuration" screen as shown below.

ACL GROUP CONFIG | TIME RANGE CONFIG | MAC ACL CONFIG | IP ACL CONFIG

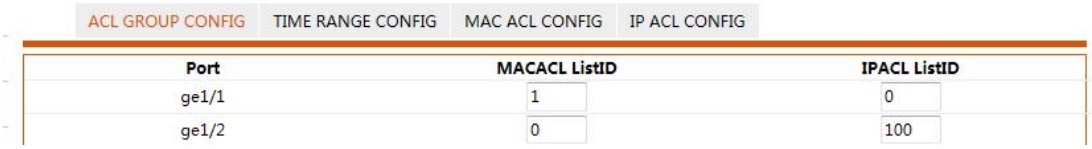
Port	MACACL ListID	IPACL ListID
ge1/1	0	0
ge1/2	0	0

Interface information meaning as followings.

Config item	Description

MACACLlistID	Already created MAC access list applied to the port ID
IPACL listID	Already created IP access list applied to the port ID

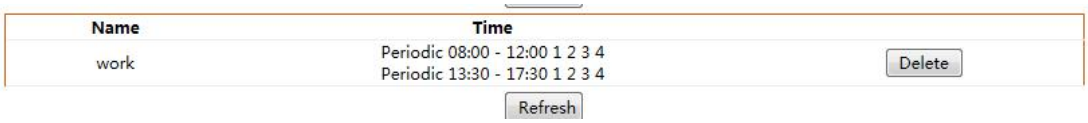
2.Fill in the appropriate configuration items to create good acl 1 and acl 100 as an example, are applied to the ge1 / 1 and ge1 /
3.Click "Apply" to complete the configuration, as shown in FIG.



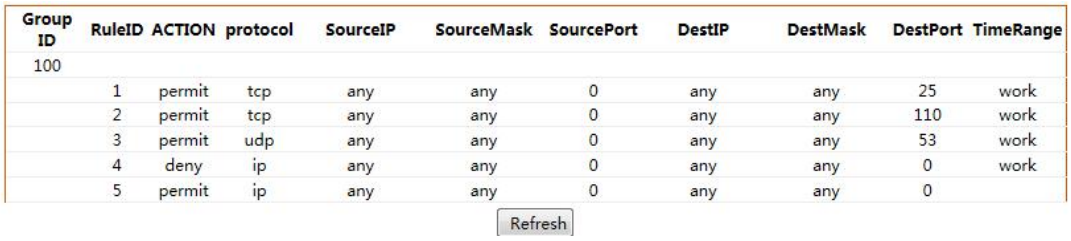
Here is an example to illustrate the definition of the method of time-based ACL. If you want to use a unit-based ACL on the switch in time to achieve: Monday to Friday (working days) from 8:00 am to 12:00 pm from 13:30 to 17:30 only allow users to receive and send mail, non-working time allowed all access.

Steps:

1. Define the time range. Click in the navigation tree "Network Security> ACL Configuration> TIME RANGE Configuration" menu, enter "TIME RANGE Configuration" 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 Configuration> IP ALC Configuration" menu, enter "IP ALC Configuration" 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 Configuration> ACL GROUP Configuration" menu, enter "ACL GROUP Configuration" screen, as shown below.

7 Advanced Configuration

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.

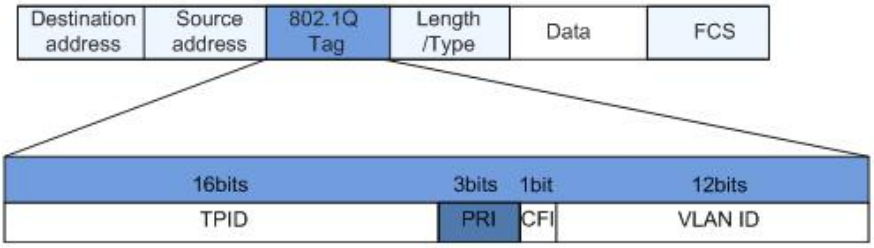
Different packets using different QoS priorities, such as VLAN packets using 802.1p, or called CoS (Class of Service) field, IP packets DSCP. When the packets pass through different networks, in order to maintain the priority of the packets, you need to configure the mapping between these priorities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

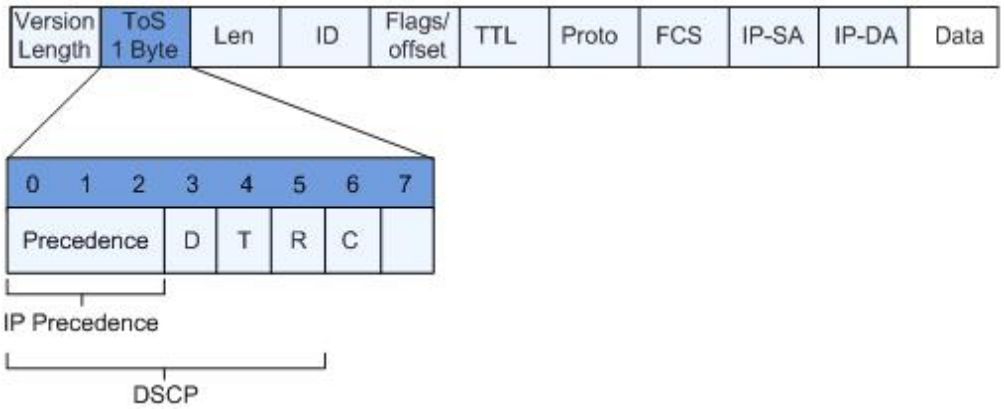


PRI field contains 3 bits long in the 802.1Q header. PRI field defines eight business priorities CoS, in priority order from highest to lowest value of 7,6, ..., 1 and 0.

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.

7.1 QOS Configuration

7.1.1 QOS Global configuration

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), WFQ (Weighted Fair Queue, weighted fair queuing) and WRR (Weighted Round Robin, WRR queue), DRR scheduling (DRR (Deficit Round Robin) scheduling RR is also extended).

Steps:

1. Choose the "Advanced Configuration> QOS> Global Configuration" menu, go to "scheduling" 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.
WFQ	Users can queue scheduling algorithm is 0-7 WFQ queue for each queue specified bandwidth, and then decide which flow into the queue according to which the CoS value of each stream and the mapping between queues, which also determines the share of flow how much bandwidth.
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.

COS Queue Mapping Procedure

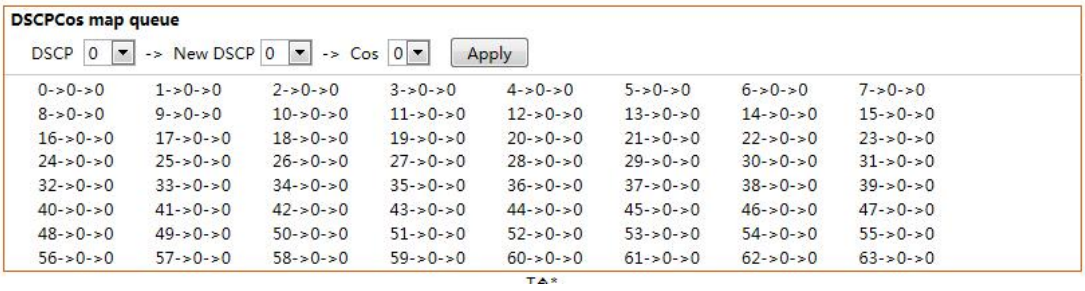
1. Choose the "Advanced Configuration> QOS> Global Configuration" menu, enter "COS map Queue" screen, as shown below.

Interface information meaning as followings.

Config item	description
Cos	Range 0-7
Queue	Range 0-7

DSCP Queue Mapping Procedure

1.Click the navigation tree "Advanced Configuration> QOS> Global Configuration" menu, enter "COS Queue Mapping" screen, as shown below.



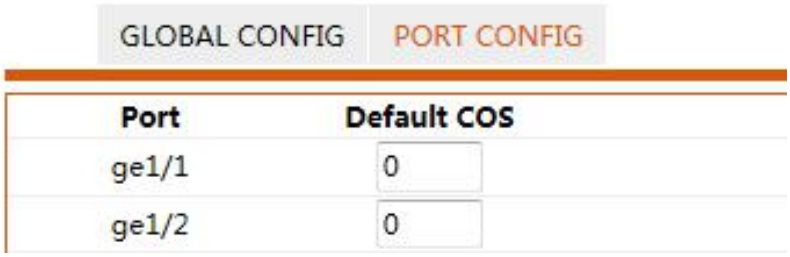
Interface information meaning as following.

Config item	Description
DSCP	Range 0-63
New DSCP	Range 0-63
Cos	Range 0-7

7.1.2 QOS port configuration

QOS port configuration Procedure

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



Interface information meaning as followings

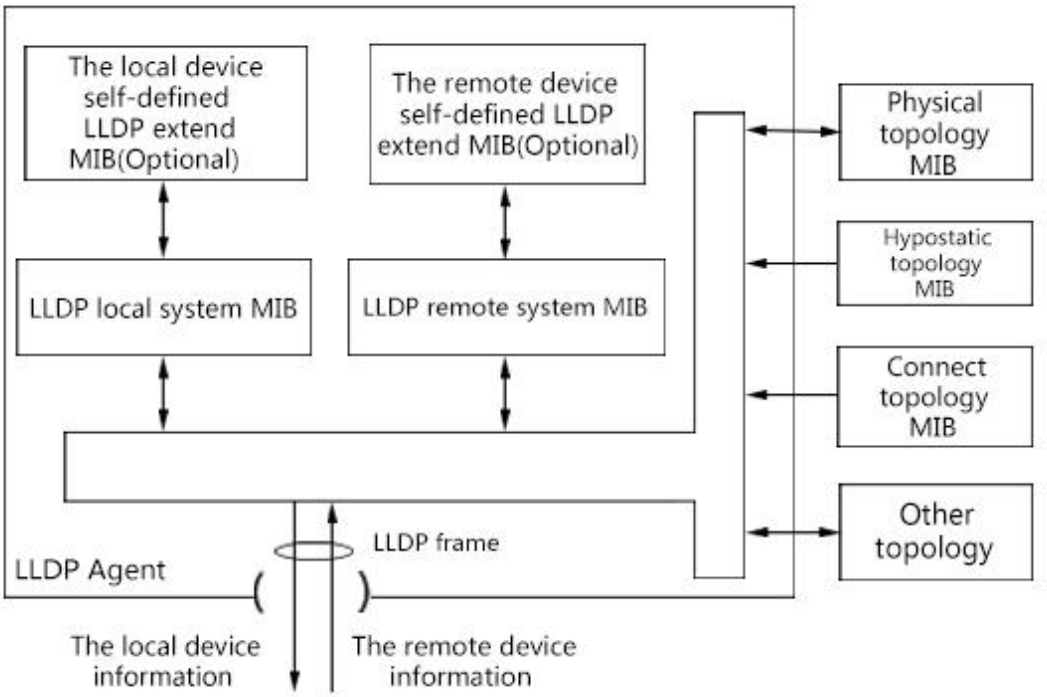
Config item	Description
Port	You can choose multiple ports
Default cos	Range from0-7

7.2 LLDP Configuration

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 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



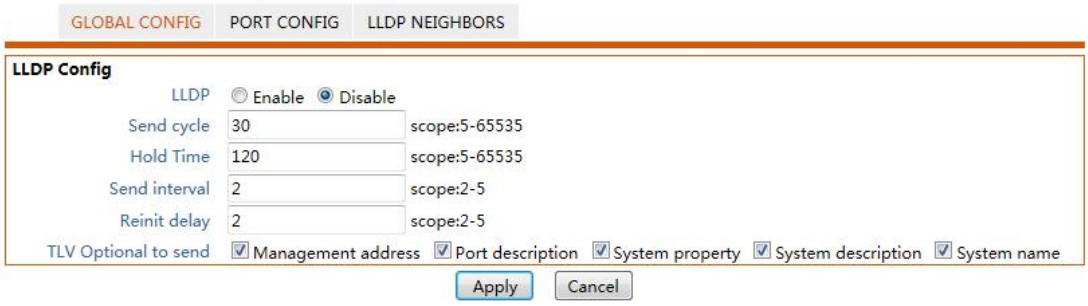
LLDP basic principle is:

- LLDP module LLDP agent on the physical topology and device interfaces MIB MIB 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.

7.2.1 LLDP Global Configuration

Steps:

1.Click the navigation tree "Advanced Configuration> LLDP Configuration> Global Configuration" menu, enter the "Global Configuration" screen, as shown below.



Interface information meaning as followings.

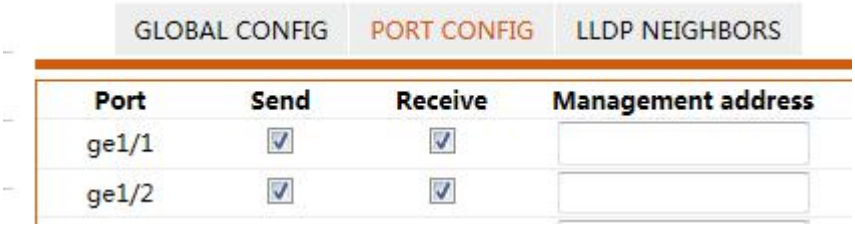
Config item	Description
LLDP	Radio. Enable or disable the UDP protocol
Hold time	120 seconds by Default ,Scope: 5-65535s
Send interval	2 seconds by Default ,Scope: 2-5s
Reinit delay	2 seconds by Default ,Scope: 2-5s
TLV optional to send	Management address, port description, system properties, system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

7.2.2 port configuration

Steps

1. Choose the "Advanced Configuration> LLDP Configuration> Port Configuration" menu, enter the "Port Configuration" screen, as shown below.



Interface information meaning as followings

Config item	Description
port	Support for configuring multiple ports
Send	Send LLDP
Receive	ReceivedLLDP
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 "Advanced Configuration> LLDP Configuration> Port Configuration" menu, enter the "Port" interface, ge1 / 1 tickthe "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.

7.2.3 LLDP Neighbors

LLDP neighbor displayed Procedure

Click the navigation tree "Advanced Configuration> LLDP Configuration> LLDP Neighbor" menu, enter "LLDP Neighbor" screen, as shown below.

7.3 SNMPConfiguration

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:

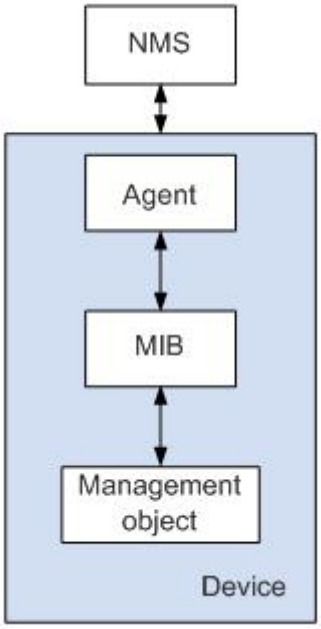
Simple: SNMP adopts the polling mechanism and provides the basic feature set, suitable for small, fast, low-cost environment, and SNMP UDP packets to carry, which is supported by the vast majority of devices.

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 "Advanced Configuration> SNMP Configuration> System Information" menu, enter "SNMP System Configuration" screen, as shown below.

Interface information meaning as followings

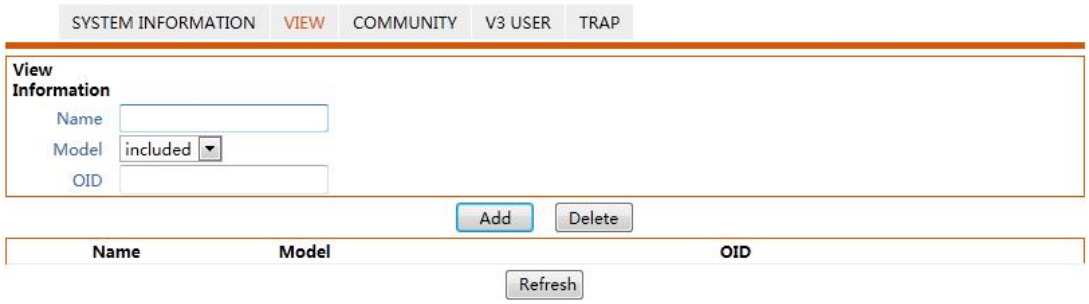
Config Item	Sub-Config	Description
SNMP System Configuration	Model	Optional, enable or disable
	Version	Not Optional,The device Support 3 kind of version by default,SNMPv1、SNMPv2c 和 SNMPv3
	Name	You can enter the system name of the switch
	Description	You can enter the system description of the switch
	Location	Enter the installed location of the switch
	Contact	Enter the switch maintainer’s contacts
	Engine no.	The system automatically generates
Trap Config	Coldstart&Warm start	It can grab system abnormal start alarminformaion if ticked.
	Link Change	It can grab the warning of switch’s ports status change if ticked .

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

b.User Settings switch write view, the definition of read-write mib.

Steps:

1.Click the navigation tree "Advanced Configuration> SNMP Configuration> View" menu, enter " view" interface, as shown below.



Interface information meaning as followings.

Config item	Sub-Config	Description
SNMP View Information	Name	You can enter the name of the View.
	Model	2 models for optional. Included,excluded
	Node OID	Enter Node OID

C. For SNMPv1, SNMPv2c need to configure groups

Steps:

Click the navigation tree "Advanced Configuration> SNMP Configuration> group" menu, enter "SNMP Community " screen, as shown below.

Interface information meaning as followings.

Config item	Sub-Config	Desrcription

SNMP Community Information	name	You can enter a community name
	Read view	Select Configured View
	Write view	Select Configured View

D. For SNMPV3 you need to configure the user name and password.

Steps

1.Click the navigation tree "Advanced Configuration> SNMP Configuration> V3 Users" menu, enter "V3 User" screen, as shown below.

Interface information meaning as followings.

Config item	Sub-Config	Description
V3 User	Name	You can enter V3user's name
	Authentication	Security level to authentication and encryption, authentication protocol to MD5 and SHA
	Privacy	Specifies the privacy protocol as AES and DES
	Read View	Select Configured View
	Write View	Select Configured View

D. When switch startis abnormal, or the port state transition, the user needs to set the target host to receive traps.

Steps:

1.Click the navigation tree "Advanced Configuration> SNMP Configuration> Alarm" menu, enter the "trap configuration" interface, as shown below.

Interface information meaning as followings.

Config item	Sub-Config	Description
Trap Config	Address	Required, set alarm destination host address information received
	Version	Select only can be SNMPv1,SNMPv2c

7.4 RMON Configuration

RMON (Remote Monitoring, Remote Network Monitoring) is the IETF (Internet Engineering Task Force, Internet Engineering Task Force) of the defined MIB (Management Information Base, MIB), MIB II standard is an important enhancement. RMON is mainly used for a whole segment of data network traffic monitoring, and is currently a commonly used network management standard. RMON includes NMS (Network Management Station, a network management station) and run on various network devices Agent in two parts. RMON Agent running on the network monitors or network probes, track various traffic information on the segment connected to its port (such as the total number of packets on a segment on a certain period of time, or sent to a host of The total number of correct messages, etc.) text. RMON is fully based on SNMP architecture that is compatible with the existing SNMP framework. RMON enables SNMP to more effectively and proactively monitor remote network devices for operation monitoring subnets provides an efficient means. RMON decreases the traffic between NMS and the agent (SNMP Agent) room, which can easily and efficiently manage large interconnected networks. RMON allows multiple monitors to collect data which can be used two ways: Using the dedicated RMON probe (detector) to collect data, NMS can obtain management information from RMON probe and controls network resources. This way you can obtain all RMON MIB information; the RMON Agent directly into network equipment (routers, switches, HUB, etc.), making them the network facilities with RMON probe function. RMON NMS using SNMP basic commands and SNMP Agent by exchanging information, to gather network management information, but this approach due to system resources limitation, may not cover all the RMON MIB. Most only four groups of information, which is four groups alarm group, group events, history, and statistics group. Ethernet switch to the second method to achieve RMON. Ethernet

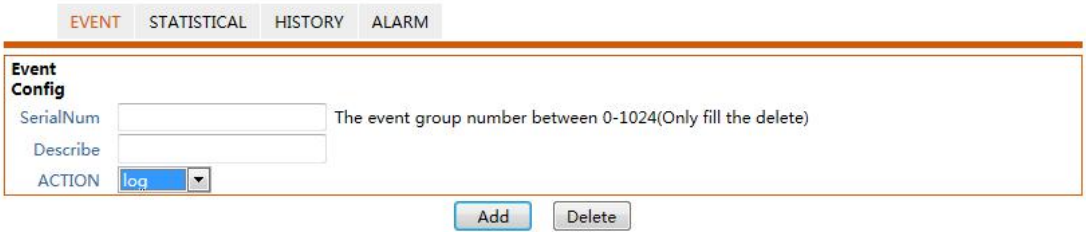
switch can implant RMON Agent, become network facilities with RMON probe function. RMON support by running on the Ethernet Switch SNMP Agent, overall traffic network NMS can obtain the Ethernet switch connected to the port on the error statistics and performance statistics and other information, to achieve the management of the network.

7.4.1 Event Group

Event group is used to define events and the handling of the event. Event group defined mainly used in the alarm group and extended alarm group in the alarm triggering event generated. Events following ways: record events in the log table; send Trap message to the NMS; events recorded in the log table to send Trap message NMS; without any treatment.

Steps

1.Click the navigation tree "Advanced Configuration> Events Groups" menu and enter the "Event Group" screen, as shown below.

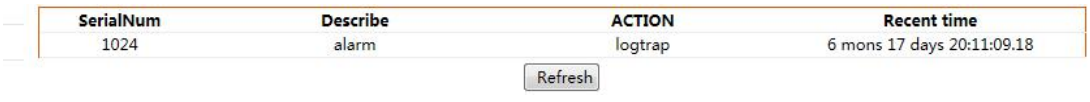


Interface information meaning as followings

Config item	description
SerialNum	The ebent group number between0-1024(only fill the delete
Describe	Describe event group
Action	None:Without any treatment. Log:The event recorded in the log table Trap:Send Trap message to the NMS Log'Trap:The event recorded in the log table to send Trap message NMS

2.Fill in the appropriate configuration items.

3.Click "Add" to complete the configuration.



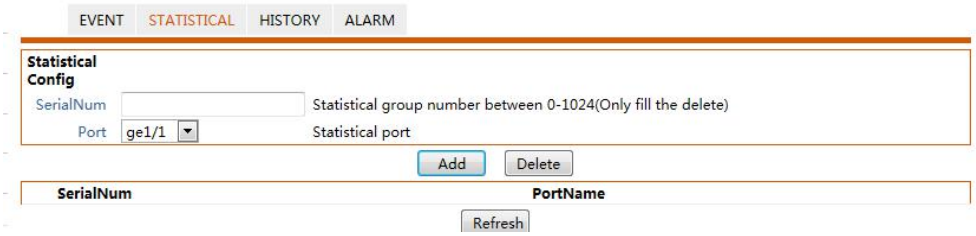
7.4.2 Statistics Section

Statistics of each monitored port on Statistics group reflect the switch. Statistics

group information is accumulated from the time the statistics group to create a beginning. Statistics about network collisions, CRC checksum error packets, is too small (or large) data packets, broadcasts, and the number of bytes received multicast packets, and so the number of packets received message. With the RMON statistics management function, you can monitor the use of the port, an error occurred in the port statistics.

Steps

1.Click the navigation tree "Advanced> Statistics group" menu, enter the "Group Statistics" screen, as shown below.



Interface information meaning as followings

Config item	Description
Serialnum	Statistical group number between 0~1024_only fill the delete)
port	Enter the statistical port

2.Fill in the appropriate configuration items.

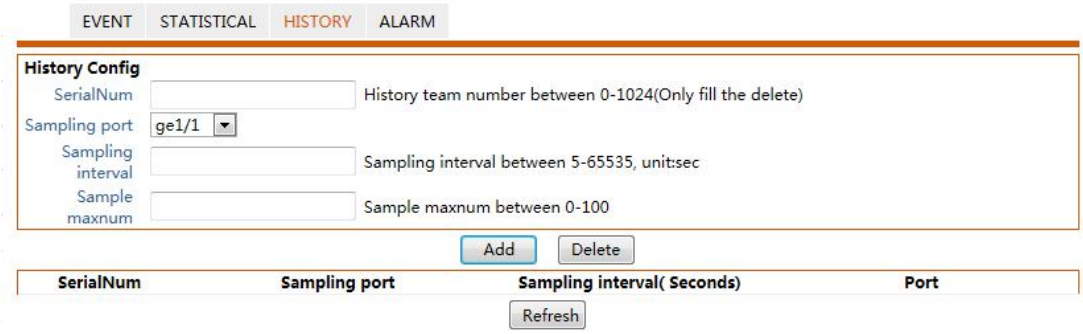
3.Click "Add" to complete the configuration, as shown below.

7.4.3 History team

After configuring RMON history group, the Ethernet switch will periodically collect network statistics, in order to facilitate the process, these statistics are temporarily stored, and provides information about network traffic, error packets, broadcast packets, bandwidth utilization and other statistics historical data. Using historical data management function, you can set up the device. Task settings include: collecting historical data, sample and store data for the specified port.

Steps

1.Click in the navigation tree "Advanced> History " menu and enter "History" screen, as shown below.

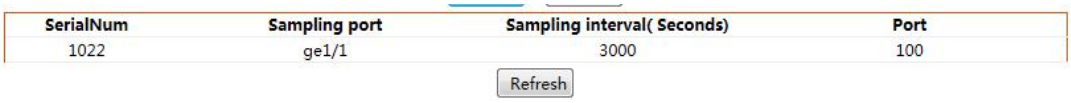


Interface information meaning as followings

Config item	Description
Serialnum	History team number between0~1024(onli fill the delete)
Sampling port	Enter the sampling port
Sampling interval	Sampling interval between 5~65535,unit:sec.
Sampling maxnum	Sample maxnum between 0~100

2.Fill in the appropriate configuration items.

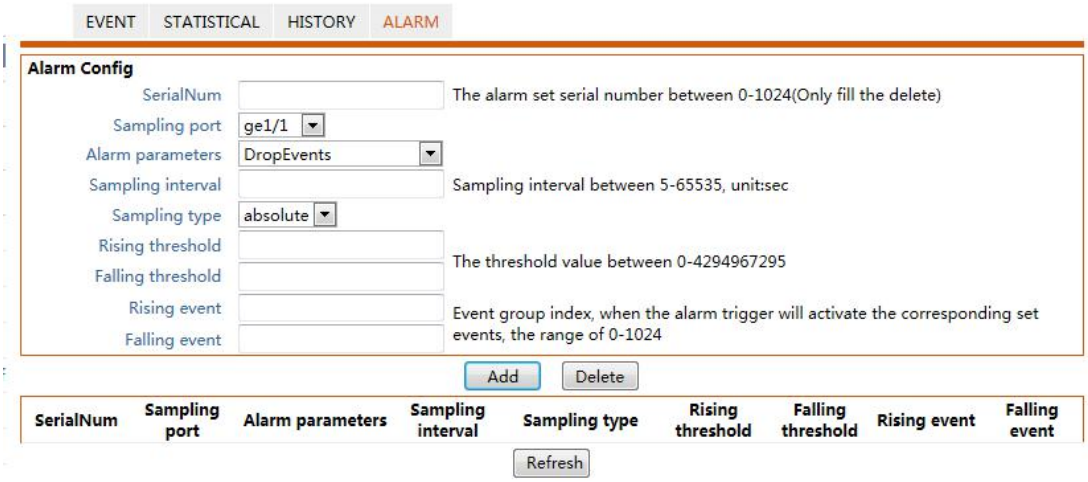
3.Click "Add" to complete the configuration, as shown below.



7.4.4 Alarm group

RMON alarm management can be specified alarm variable (such as statistical data ports) to monitor, when the value of the monitored data exceeds the defined threshold value in the corresponding direction will generate an alarm event, and then follow the events defined handled accordingly deal with. Events are defined in the event group. After you define an alarm entry, the system alarm entry process is as follows: alarm variables defined alarm-variable according to the defined time interval sampling-time sampling; sampled value and the set threshold value, more than once the threshold, triggering the corresponding event.

Click the navigation tree "Advanced Configuration> Alarm Groups" menu and enter "alarm group" screen, as shown below.



Interface information meaning as followings

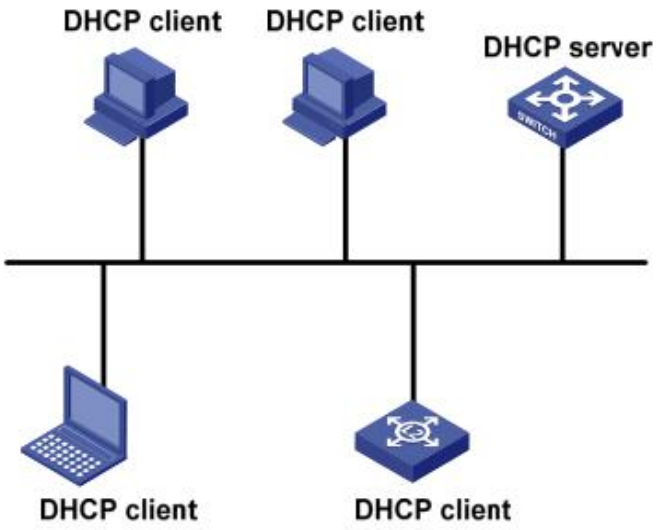
Config item	Description
Serial num	The alarm set serial number between 0~1024(only fill the delete)
Sampling port	Enter the sampling port
Alarm parameters	
Sampling interval	Sampling interval between 5~65535,unit:sec
Sampling type	Absolutea nd delte
Rising threshold	The thresholdd value between 0-4294967295
Falling threshold	The thresholdd value between 0-4294967295
Rising event	Event group index, when the alarm tigger will activate the corresponding event group, range 0-1024
Falling event	Event group index, when the alarm tigger will activate the corresponding event group, range 0-1024

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

7.5 DHCP Server Configuration

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

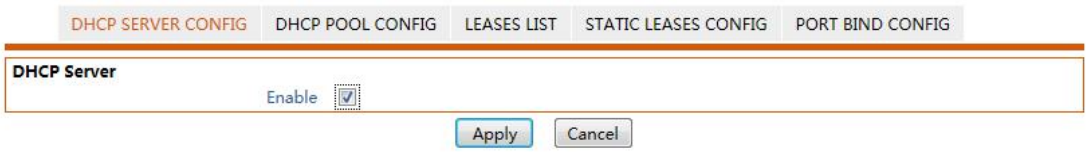
address lease. When DHCP client's IP address lease duration half-time, DHCP client to the DHCP server a DHCP-REQUEST unicast packets, to update IP lease. If the IP address is valid, the DHCP server to respond to unicast DHCP-ACK packet to notify the DHCP client of the new IP lease; If the IP address can not be assigned to the client, the DHCP server responds DHCP-NAK packets notify the DHCP client can not 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.

7.5.1 DHCP Server Configuration

Enable DHCP server

Steps:

1.Click the navigation tree "Advanced Configuration> DHCP Server Configuration> DHCP Server Configuration" menu, enter "DHCP Server Configuration" screen, select Enabled, click "Apply", as shown below.

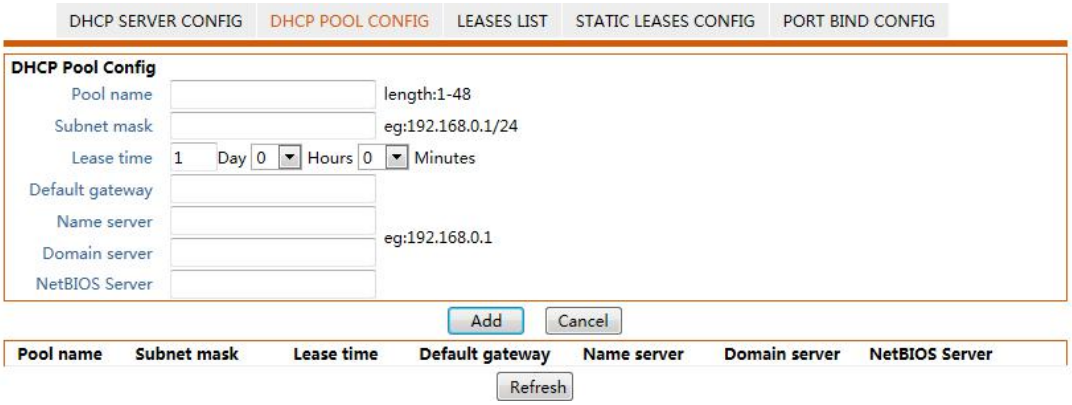


7.5.2 Address pool configuration

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 "Advanced Configuration> DHCP Server Configuration> Address Pool Configuration" menu, go to "address pool configuration" interface, as shown below.



Interface information meaning as followings.

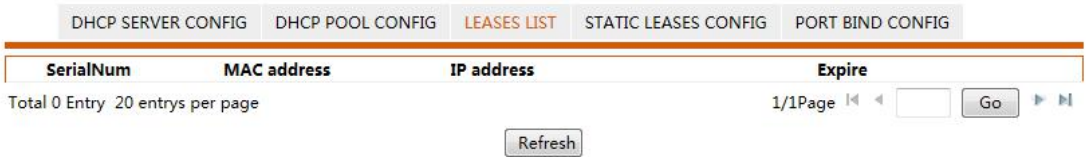
Config item	Description
Pool name	Enter the poor name
Subnet mask	Enter the IP address pool address and subnet mask.
Lease time	The lease of dynamic IP addresses. The default is 1 day. The range: Day: an integer ranging from 0 to 999. Hours: integer ranging from 0 to 23. Score: integer ranging from 0 to 59.
Default gateway	Enter the gateway IP add
DNSserver	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.

7.5.3 Leases list

View leases IP Address List Procedure

1. Choose the "Advanced Configuration> DHCP Server Configuration> LEASES List" menu, go to "Client List" screen, as shown below.

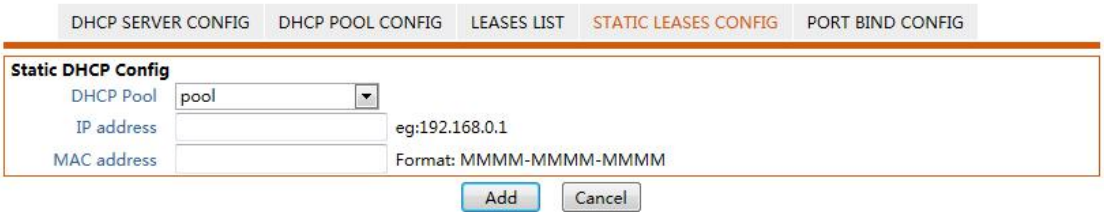


7.5.4 Static Leases configuration

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 "Advanced Configuration> DHCP Server Configuration> Static Client Configuration" 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	Enter the IP address to be bound.
MAC address	Enter the MAC address to be bound

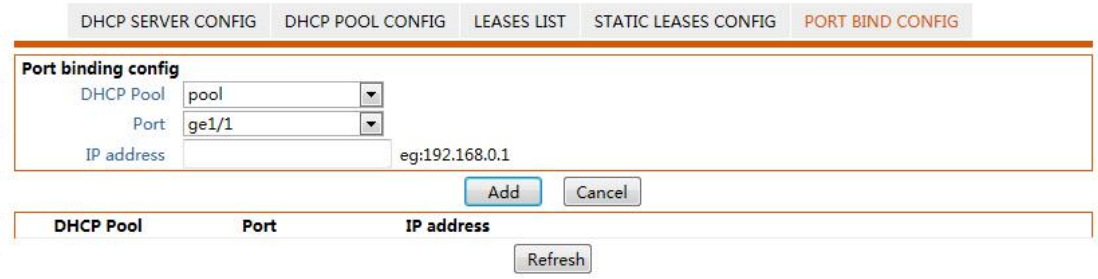
2. Fill in the appropriate configuration items.
3. Click "Add" to complete the configuration, as shown below.

7.5.5 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 "Advanced Configuration> DHCP Server Configuration> Port Binding" menu, go to "port binding" 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.

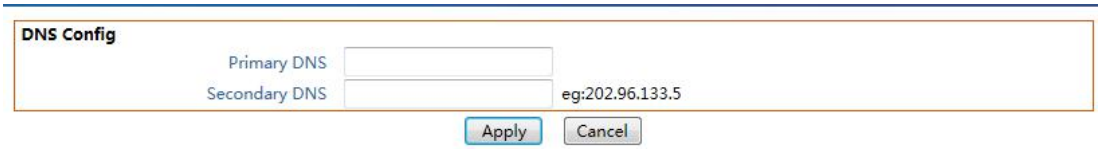
2. Fill in the appropriate configuration items.

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

7.6 DNS Configuration

Steps:

1.Click in the navigation tree "Advanced Configuration> DNS Configu" menu, enter the "DNS Config" interface as shown in the following figure.



Interface information meaning as followings

Config item	Description
Primary DNS	Enter the Primary DNS IP address.
Secondary DNS	Enter a secondary DNS IP address.

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

7.7 NTP Configuration

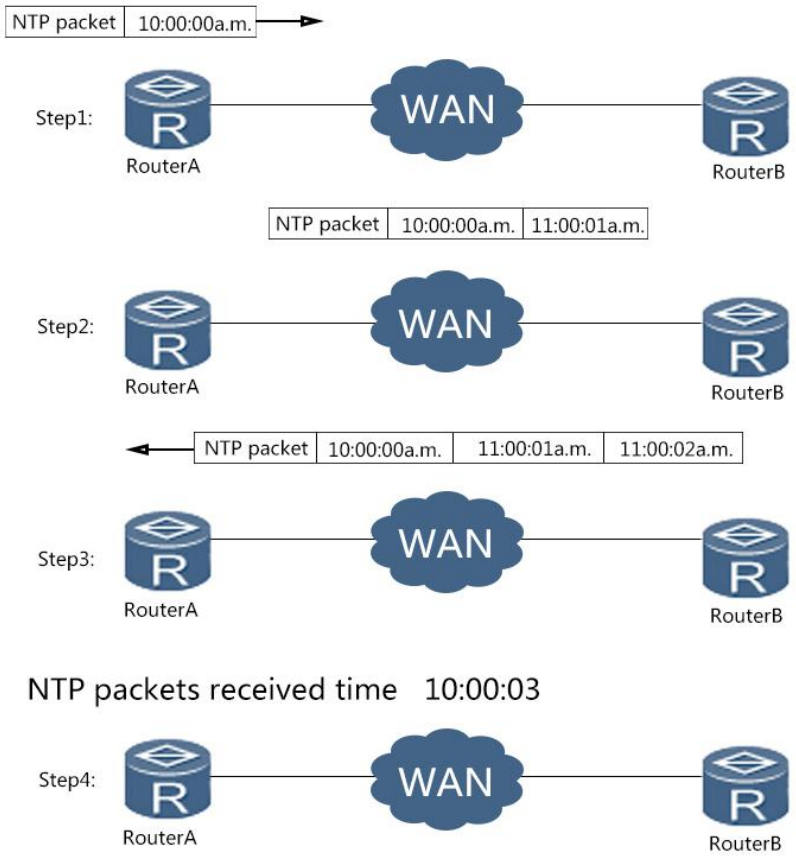
Network Time Protocol NTP (Network Time Protocol) is a TCP / IP protocol suite, which is an application layer protocol. NTP is used across a range of distributed time server and client to synchronize clocks. NTP implementation based on IP and UDP. NTP packets transmitted over UDP port number is 123. 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 can not 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 a 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).

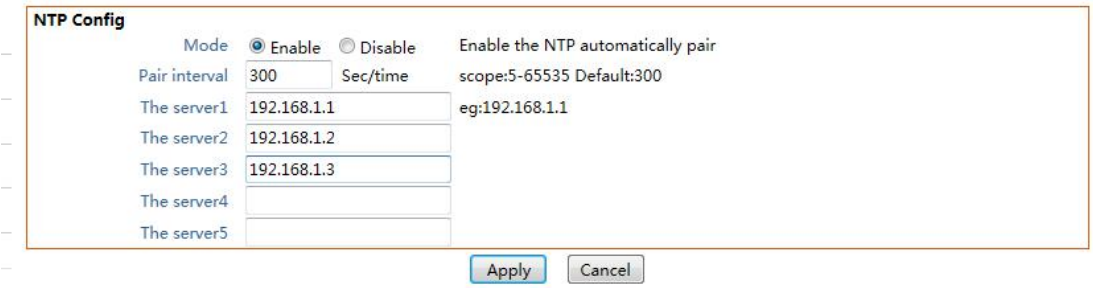
When Router A receives the response packet, it adds a new timestamp 10:00:03 a.m. (T4).
So far, RouterA get enough information to calculate the following two important parameters:
NTP back and forth a period of latency:Delay= (T4 - T1) - (T3 – T2)。
RouterA RouterB relative time difference:Offset= ((T2- T1) + (T3 – T4)) / 2。
RouterOS 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 "Advanced Configuration> NTP Settings" menu, enter "NTP Server Configuration" screen, as shown below.



Interface information meaning as followings

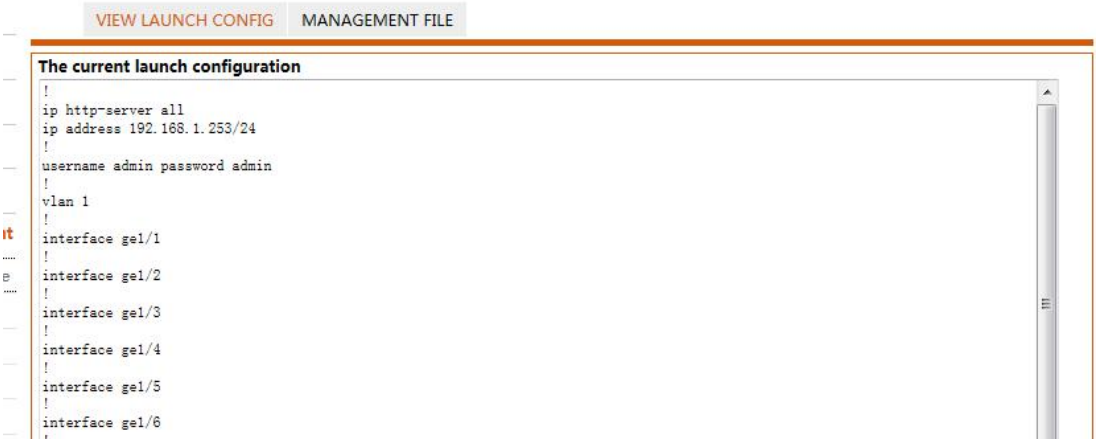
Config item	Description
Mode	Enable or disable NTP automatically
Pair interval	Scope:5-65535 Default:300
The reserver1	Maximum support 5 server IP address

8 System maintenance

8.1 Configuration File Management

a.See the startup configuration steps

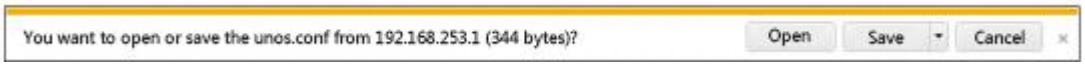
1.Click theNavigation tree "System Maintenance> Configuration File Management" menu, go to "Profile Management" screen, click "View startup configuration", as shown below.



Download the configuration file Procedure

Navigation tree "System Maintenance> Configuration File Management> Configuration File Management" menu, go to "management file" screen, as shown below.

Click on "download", as shown below.



b. Upload profile Procedure

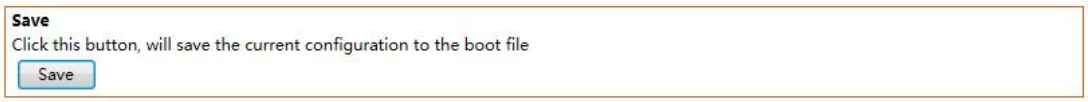
1.Click Navigation tree "System Maintenance> Configuration File Management> Configuration File Management" menu, go to "Management file" screen, click "File path", choose the configuration that has been created, as shown below.

2.Click "Upload" to complete the configuration.

8.2 Save Configuration

Steps:

1. Choose the "System Maintenance> Save Configuration" menu, go to "Save Configuration" screen, click "Save ", as shown below.



8.3 Reboot the device

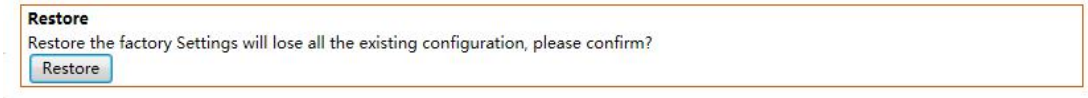
Steps:

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

8.4 Restore

Steps:

1.Click "System Maintenance> Restore factory settings" menu, go to "restore factory settings" interface, click "Restore", as shown below.



Attention:

Click "restore factory settings", need to click the "Reboot", the device will return to the factory settings.

8.5 Online upgrade

Steps:

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


Management Upgrade File
Upgrade file path
Browsed

Upload