Switch Configuration Guide

Release time: 2023.2.1

1.1. System management

1.2. CLI command line mode

The device CLI management interface is divided into several modes. The current command mode determines the commands that can be used. Type the question mark (?) key at the command prompt. You can list the supported commands for each command pattern. When a user logs on to the device, they are first in user mode。

Schema name	Prompt	Switching mode	Pattern description
User mode	(Routing)>	Configure enable to switch to the privileged mode	Supports device information display and debugging command lines
Privileged mode	(Routing)#	configure to switch to global mode； Configure exit to switch to user mode	Support network testing; Support function module information view; You can save and clear configurations
Global mode	(Routing)(config)#	Configure exit to switch to the privileged mode； The interface was set to the interface mode	Global configuration commands are supported
Interface mode	(Routing)(config-if)#	Configure exit to switch to the global mode.； Configure end to switch to privileged mode	Commands can be configured in interface mode. Interfaces include physical interfaces, aggregation interfaces, and SVI interfaces

1.2.1. Configure the management IP address

1.2.2. 1.2.2. Configure commands

- Configures the Ipv4 management IP address of the device

command	(Routing)#network parms ipaddr netmask [gateway]
Description	Configure an Ipv4 management IP address for the device

- Configure the management vlan

command	(Routing)#network mgmt_vlan [vlan_id}

	(Routing)#no network mgmt_vlan [vlan_id}
Description	The device management vlan was configured or deleted

- Configure the device Ipv4 management IP address dynamically obtained by DHC

command	(Routing)#network protocol dhcp client-id
Description	Configure an Ipv4 management IP address

- Configure an Ipv6 management IP address for the device

command	(Routing)#network ipv6 address ipv6 ipv6-address/prefix-length [eui64] (Routing)#network ipv6 gateway ipv6-address (Routing)#no network ipv6 address ipv6 ipv6-address/prefix-length (Routing)#no network ipv6 gateway
Description	The Ipv6 management IP address of the device was configured or deleted

- Configure the Ipv6 management IP address dynamically obtained by DHCP 取

command	(Routing)#network ipv6 address autoconfig

	(Routing)**#no network ipv6 address autoconfig**
Description	The Ipv6 management IP address of the device was configured or deleted

- View the device management IP address configuration

command	(Routing)#show running-config
Description	Viewing ip Configuration

1.3. Configure the save/clear operations

- Configuration save command

Command	(Routing)#write memory
Description	Save configuration

- Restore the default configuration command

Command	((Routing)) #clear config Are you sure you want to clear the configuration? (y/n) y
Description	The default system Settings are restored and take effect after the device is restarted

1.3. THE HOT RESTART OPERATION OF THE DEVICE

- Configure the hot restart command

Command	(Routing)#**reload**
Description	Device hot restart

1.4. USER LOGIN MANAGEMENT

- Adding or deleting a user and changing a user password

Command	(Routing)(config)# **username** NAME **password** LINE (Routing)(config)# **no username** NAME
Description	If the user NAME does not exist, the user is added. If the user name does exist, the user password is changed. By default, the device has user admin and password admin. You can change or delete the password; The device supports a maximum of eight users. The user and password length is <8-64> bytes. The password is encrypted; Password characters are case sensitive;

- WEB management function was enabled

Command	(Routing)# `ip http server` (Routing)# `ip http secure-server` (Routing)# **no** `ip http server`

	(Routing)#no ip http secure-server
Description	WEB management function was enabled Default enable state Support Ipv6

- Telnet management was enabled

Command	(Routing)# ip telnet server enable (Routing)# no ip telnet server enable
Description	telnet management was enabled Default disable state Support Ipv6

- SSH management was enabled. Procedure

Command	(Routing)# **ip ssh server enable** (Routing)# **no ip ssh server enable**
Description	SSH management was enabled. Procedure Default disable state Support Ipv6

Display command:

```
(Routing) #show users

                                  User
User Name                     Access Mode
-------------------------     -----------
admin                         Privilege-15
```

1.5. CONFIGURE SYSTEM NAME

- Configure system name

Command	(Routing)(config)# **hostname** WORD
Description	Set the system name, which must consist of printable characters and cannot exceed 64 bytes. The configuration takes effect immediately

1.6. SETTING SYSTEM TIME

- Configure the system time manually

Command	(Routing)(config)# clock set hh:mm:ss (Routing)(config)# clock set mm/dd/yyyy
Description	Setting the system time For example, configure 15:30 seconds on October 1, 2017: clock set 15:30:00 clock set 10/1/ 2017

- Configuring the ntp Server

Command	(Routing)(config)# sntp server {ipaddress | ipv6address | hostname} [priority [version]

	(Routing)(config)#s**ntp server** A.B.C.D
Description	Configure the IP address of the NTP server (domain name is not supported). After the configuration, if the device is connected to the server, the device automatically synchronizes time from the server. The first time synchronization takes about 4 to 8 minutes。

- Configuring the System Time Zone

Command	(Routing)(config)# clock timezone {hours} [minutes minutes] [zone acronym] (Routing)(config)# `no clock timezone`
Description	Configure the system time zone. The default time zone is UTC. Standard time zone configurations are supported, such as Shanghai and Hong_Kong.

- Checking the system time

Command	(Routing)# **show clock**
Description	Checking the system time

1.7. CONFIGURATION INTERFACE

1.8. OVERVIEW OF INTERFACE TYPES

According to the business level, the interface of switching equipment can be divided into the following two categories: the second-layer interface and the third-layer interface.

The second floor interface(L2 interface)，Common physical port ((Routing) Port) and aggregate port (Port Channel are included here)。(Routing) Port consists of a single physical port on the device with only second 2 switching. The port can be a Access Port, a Hybrid Port, or a Trunk Port, and you can

configure a port as a Access Port, Hybrid Port, or Trunk Port through the (Routing) Port interface configuration command.

Port Channel PO, for short, is composed of multiple physical member ports aggregation. We can bundle multiple physical links together to form a simple logical link, which we call a aggregation port. For layer 2 switching, the aggregate port is like a high-bandwidth (Routing) port, which can stack the bandwidth of multiple ports and expand the link bandwidth.

Three-layer interface (L3 interface), here mainly refers to the SVI ((Routing) virtual interface) port.

SVI is an exchange virtual interface, a logic 9 interface for three layers of exchange. SVI can be used as a local management interface, managing the administrator. You can create SVI through the interface vlan interface configuration command and then assign IP address to SVI to establish the routing between VLAN.

1.9. CONFIGURATION COMMAND

- Configure the port range

Command	(Routing)(config)# **interface** <intf-range> (Routing)(config)# **interface** 0/1-0/4 (Routing)(config)# **interface** 0/1 (Routing)(config)# show interface ethernet all
Description	<intf-range> Format such as 0/1-0/4,

- Configure the port descriptor

Command	(Routing)(config-if)# **description** <description>
Description	Configure the interface descriptors, up to 80 characters

- Configure port enabling

Command	(Routing)(config-if)# **shutdown** (Routing)(config-if)# **no shutdown**
Description	Close or enable ports, default; Only the physical port configuration is supported

- Configure port rate

Command	(Routing)(config-if)# **speed** [10G | 1000 | 100 | 10] {half-duplex | `full-duplex}}` (Routing)(config-if)# speed auto-detect (Routing)(config-if)# **speed** auto-neg [10G | 1000 | 100 | 10] {half-duplex | `full-duplex}}`
Description	Configure the port rate, when configured as auto, the port rate enters into self-negotiation mode; Default port rate is negotiated from; Configuration on the aggregate member ports is not supported; Configuration on the SVI ports is not supported

Instruction

✦When both rate and duplex exit the self-negotiation mode, the port self-negotiation closes

- Configure port flow control

When the local switch and the opposite switch are turned on the flow control function, if the local switch congestion:

The local switch will send a message to the opposite switch to temporarily stop sending messages or slow down the message transmission speed.

After receiving the message, the opposite switch will suspend the message or slow down the speed, so as to avoid the occurrence of message loss and ensure the normal operation of network services.command	(Routing)(config-if)# **flowcontrol** { **asymmetric** | **symmetric** }
	(Routing)(config-if)# no **flowcontrol**
	((Routing)) (Interface 0/1)#show flowcontrol 0/1
	Admin Flow Control: Inactive
	Flow Control Flow Control RxPause TxPause
	Intf Oper Mode
	------- ------------ ------------ -------- --------
	0/1 Inactive Symmetric 0 0
	((Routing)) (Interface 0/1)#

Description	Configure port flow control, default port flow control from negotiation; Configuration on aggregate member ports is not supported; Configuration on the SVI ports is not supported

- Configure the port MTU

When the port performs a large-throughput data exchange, you may encounter frames greater than the Ethernet standard frame length, which are called jumbo frames. The user can control the maximum frame length the port allows to receive by setting the MTU of the port. An MTU is the length of a valid data segment in a frame, excluding the overhead of an Ethernet encapsulation. Frames received or forwarded by the port are discarded if they exceeds the set MTU.

Due to chip limitations, the MTU value only supports even numbers. If the user is odd, the device will be automatically aligned. If the MTU is 127, and the actual 128 length message is supported.

Command	(Routing)(config-if)# **mtu** LENGTH (Routing)(config-if)# **no mtu**
Description	Configure the port MTU, allow to set a range of <1500 to 12270>, bytes, with a default of 1518 bytes Configuration on the aggregate member ports is not supported; Configuration on the SVI ports is not supported

- Configure port isolation

In some application environments, it is required that some ports of the device can not communicate with each other, which can be achieved by setting these ports as isolation ports. When the port is set as the isolation port, the isolation port cannot communicate with each other, the isolation port and the nonisolation port can communicate normally, and the non-isolation port and the nonisolation port can communicate normally.

Command	(Routing)(config-if)#(Routing)port protected <0-2> (Routing)(config-if)# **no** (Routing)port protected <0-2>
Description	The default port is a non-quarantine port; Currently, configured isolation on aggregate, vlan ports is not supported

- Display the port light / copper cable module information

This command is used to display information about the optical / copper cable module inserted on the optical port.

Command	(Routing)#show fiber-ports optics {all | unit/slot/port} (Routing)#show fiber-ports optics all (Routing)#show fiber-ports optics 0/1
Description	Not specified unit / slot / port displays module information for all ports The info displays the DDM information and the complete module information (basic information, alarm information, vendor information)

2. CONFIGURING STORM CONTROL

2.1. OVERVIEW OF STORM CONTROL

When there is excessive broadcast, multicast or unknown unicast data flow in LAN, it will lead to network performance decline, even network paralysis, called broadcast storm. Storm control provides speed limit for broadcast, multicast and unknown unicast data flow. When the rate of broadcast, unknown multicast or unknown unicast data flow received by the switch port exceeds the set bandwidth, the device will only allow the data flow through the set bandwidth, and the data flow beyond the bandwidth will be discarded, so as to avoid excessive flood data flow into the LAN.

2.2. CONFIGURING COMMANDS

- Configure the interface storm control policy

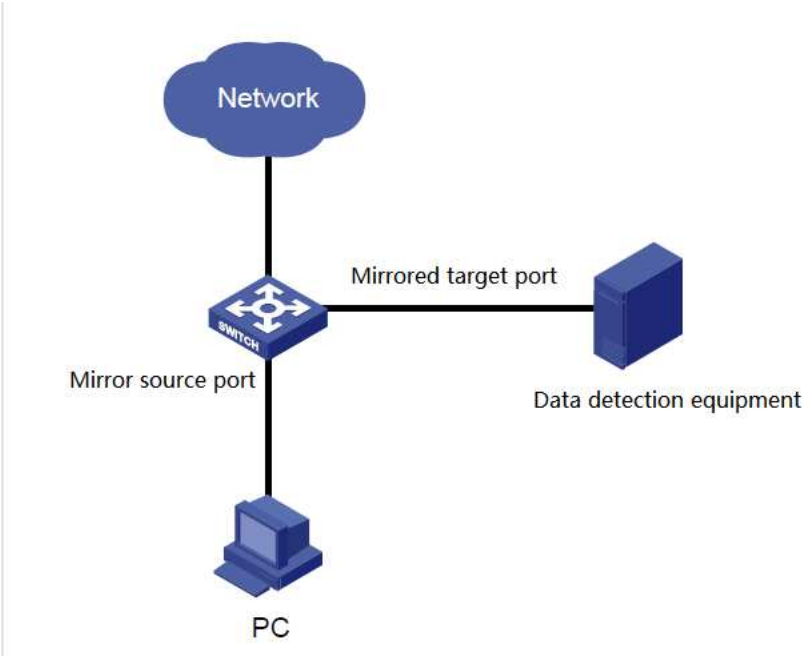
Command	(Routing)(config-if)#storm-control {**broadcast** | **multicast** | **unicast** | **}** (Routing)(config-if)#no storm-control {**broadcast** | **multicast** | **unicast** | **}** (Routing)(config-if)#storm-control {**broadcast** | **multicast** | **unicast** | **}**level threshold (Routing)(config-if)#no storm-control {**broadcast** | **multicast** | **unicast** | **}** level (Routing)(config-if)#storm-control {**broadcast** | **multicast** | **unicast** | **}** rate threshold (Routing)(config-if)#no storm-control {**broadcast** | **multicast** | **unicast** | **}** rate ((Routing)) #show storm-control all
Description	Configure / delete the port storm control policies;

	Support broadcast/multicast/unicast/all/unicast-broadcast/ multicast-broadcastSelect configuration in, select configuration cannot coexist; Among them, multicast said no well-known broadcast, unicast said unknown list broadcast; The level value is the port bandwidth percentage, and the rate is the port rate change

3. CONFIGURE SPAN

3.1. SPAN SUMMARY

SPAN (Local (Routing) ed Port Analyzer) is a local mirror function. The SPAN function copies the message of the specified port to the destination port. Generally, the SPAN destination port will access the data detection setting. Users can analyze the message received by the destination port with these devices for network monitoring and troubleshooting.



The SPAN does not affect the message exchange of the source port and the destination port, but only copies all the incoming and output packets of the source port to the destination port. When the mirror traffic of the source port exceeds the bandwidth of the destination port, such as the 100Mbps destination port that monitors the traffic of the 1000Mbps source port, it may cause the packets to be discarded。

The SPAN is based on session management and configures the source and destination port of the SPAN. In one session, there can only be one destination port, but multiple source ports can be configured simultaneously。

3.2. CONFIGURING COMMANDS

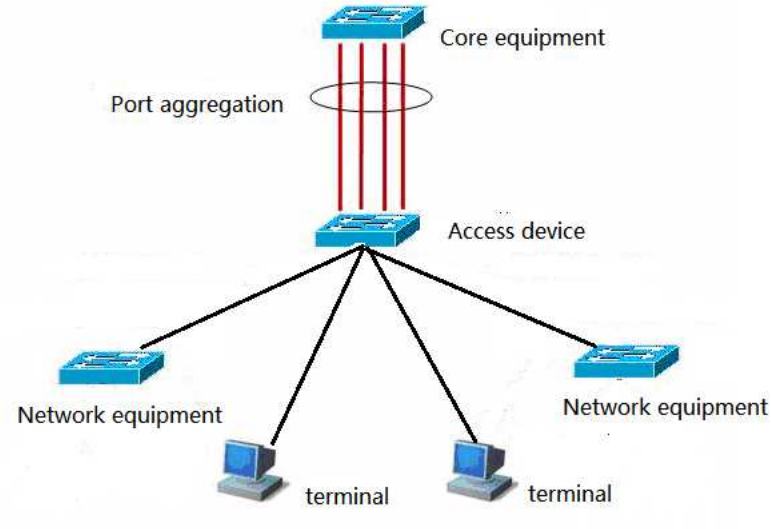
- Create a session

Command	(Routing)(config)#monitor session session-id {source {interface unit/slot/port | cpu || vlan vlan-id | remote vlan vlan-id }[{rx | tx}] | destination {interface unit/slot/port |remote vlan vlan-id reflector-port unit/slot/port}| mode | (Routing)(config)#**no monitor session** SESSION-ID ((Routing)) #show monitor session all
Description	Create / delete / display session, create session into session mode; 4 supported sessions

4. CONFIGURE PORT AGGREGATION

4.1. SUMMARY OF POLYMERIZATION MOUTH

Bunind multiple physical links together to build a logical link, which we call aggregation port (port-channel, the latter PO port), this function is called port aggregation function. The aggregate port function meets the IEEE802.3ad standard, which can be used to expand the link bandwidth and provide higher connection reliability. It is often used for port overconnection, as shown in the figure below.



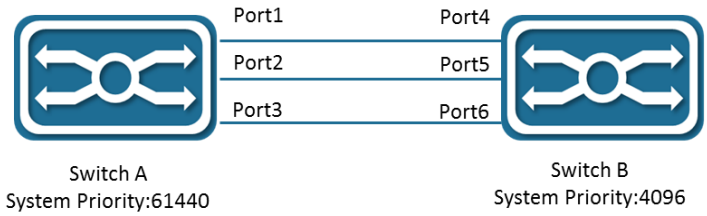
The aggregate port has the following characteristics: high bandwidth, the total bandwidth of the aggregate port is the sum of the physical member port bandwidth; supports the traffic balancing policy, which can allocate the traffic to each member link according to the strategy; support link backup. When a member link in the aggregate port is disconnected, the system will automatically allocate the traffic of the member link to other effective member links in the aggregate port.

4.2. LACP SUMMARY

LACP (Link Aggregation Control Protocol, link convergence control protocol) based on IEEE802.3ad standard is a protocol to realize dynamic link convergence. If the port enables the LACP protocol, the port sends a LACPDU to notify its own system priority, system MAC, port priority, port number, operation key, etc. After receiving the opposite-terminal LACP message from the connected device, compare the system priority at both ends according to the system ID in the message. At the end of the system ID with a high port ID priority, the port in the aggregation group will be set in the aggregation state, and issue the updated LACP message. After the opposite device receives the message, the port

will set the corresponding port to the aggregation state, so that the port exit or join the aggregation group. The physical link can forward the data messages only after the ports of both sides complete the dynamic aggregation binding operation.

After the LACP member port link is bound, the periodic LACP message interaction will be conducted. When the LACP message is not received for a period of time, the packet receipt is considered to time out, the member port link is unbound, and the port is in a non-forwarding state again. There are two modes of timeout time here: long timeout mode and short timeout mode. In the long timeout mode, the port sends a message at 30 seconds interval, if the opposite packet is not received for 90 seconds, the packet timeout; in the short timeout mode, the port sends a message at 1 second interval, if the paired packet is not received for 3 seconds, the packet timeout.



As shown in the figure above, the switches A and the switch B are connected together through 3 ports. The system priority for switch A is set to 61440 and the system priority for switch B to 4096. Open LACP link aggregation on 3 direct connection ports of switch A and B, set the aggregation mode of 3 ports to active mode, and set the port priority of 3 ports to the default priority 32768.

After receiving the LACP message from the opposite end, the switch B found that its system ID priority is higher (the system priority of switch B is higher than the switch A), so the ports 4,5, and 6 are aggregated in the order of the order of port number). After switch A received the updated LACP message from switch B, it found that the system ID of the opposite end had a high priority, and set the port to the aggregation state, and also set ports 1,2 and 3 to the aggregation state。

4.3. CONFIGURING COMMANDS

- Port join / exit aggregate port

Command	Add the static polymerization port: (Routing)(config-if)#addport lag <lag-group-id>

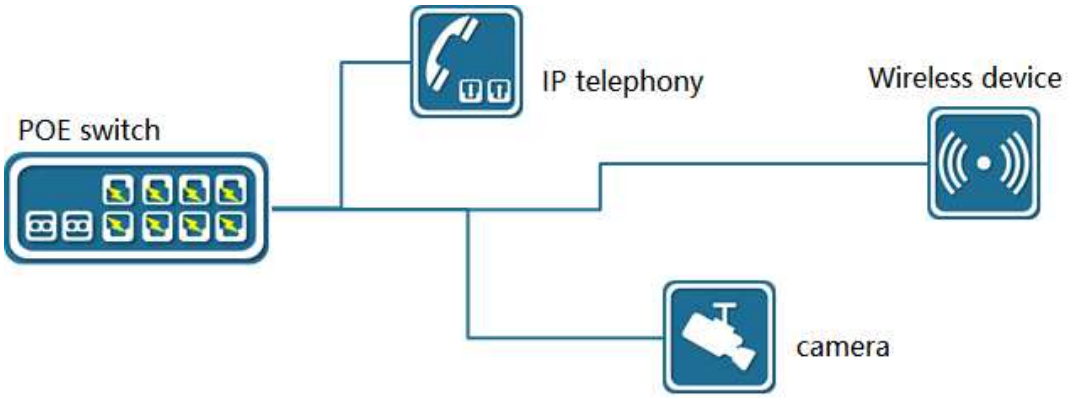
	(Routing)(config-if)#addport lag 1 Add dynamic aggregation(LACP): (Routing)(config)#interface 1/1 (Routing)(Interface 1/1)#no port-channel static View port convergence ((Routing)) #show interface lag 1
Description	Support for 8 aggregate ports <1-8>; A converged port is either static or dynamic, as determined by the first member of the mouth。 Active Aggregation mode indicates that the port actively initiates LACP aggregation, and Passive aggregation mode indicates that the port does not actively initiate LACP aggregation, but passively participates in LACP calculation after receiving a neighbor LACP message。

5. CONFIGURE POE

5.1. POE SUMMARY

Power over Ethernet, PoE for short, is a technology that can provide DC power supply through data interaction with terminals in the Ethernet network. Often used to the network telephone, WIFI AP, network camera, hub, computer and other equipment for power supply.

According to the standard, the longest distance of the power supply is 100m。



PSE (Power Sourcing Equipment, power supply equipment) as in the picture above. PSE looks for and detects PD on the line of POE port, grades PD and supplies power to it. When the PD withdrawal is detected, the PSE stops the power supply. PD is a device that receives PSE power supply, such as IP phone, wireless device and camera in the picture above。

The PoE development has gone through two sets of standards：

IEEE 802.3af(15.4W) is the first PoE power supply standard, which stipulates the Ethernet power supply standard, and is now the mainstream implementation standard of PoE application. It clearly defines the power detection and control matters in the remote system, and specifies the way that routers, switches, and hubs supply power to IP phones, security systems, and wireless LAN access points through ethernet cables. IEEE802.3at(25.5W) According to the demand of high-power terminals, on the basis of the 802.3af compatibility, to provide greater power supply demand, to meet the new demand. According to the IEEE 802.3af specification, the PoE power consumption on the receiving device (PD) is limited to 12.95W. IEEE 802.3at, It defines devices with higher power requirements than 12.95W as Class 4 (this

level is described in IEEE 802.3af but reserved for future use) and extends the power level to 25W or higher。

5.2. CONFIGURING COMMANDS

- Configure the external power supply power

Command	(Routing)(config)#poe power limit {class-based | none | user-defined maximum-power} (Routing)(config)#no poe power limit [user-defined]
Description	Configure the external power supply power Default power power calculation method: the product of PoE power ports and single port 15.4W If the configured power is less than the current device consumption, the port priority of the low priority port is the higher priority with the low port ID。

- Configure the port power supply enabled

Command	(Routing) (config-if)#**poe** (Routing) (config-if)#**no poe**
Description	Configure the port to enable the power supply Default port power supply is enabled

- Configuration enables a compatible mode

Command	(Routing) (config-if)#`poe high-power {legacy | pre-dot3at | dot3at | upoe}`

	(Routing) (config)#`no poe high-power`
Description	Configuration enables a compatible mode Using this command on a port that is not connected to the PD device may cause the opposite device to be burned by the wrong power on, so make sure that the port uses the command when connected to the PD device For PoE devices that do not meet the standard, the Class classification is uniformly displayed as 0

6. CONFIGURE VLAN

6.1. OVERVIEW OF THE VLAN FUNCTIONS

A VLAN is short for a virtual local area network (Virtual Local Area Network), which is a logical network divided on a physical network. This network corresponds to the second layer network of the ISO model. The VLAN division is not limited by the actual physical location of the network port. A VLAN has the same properties as a normal physical network, except for no physical location restrictions, etc. The second layer of unicast, broadcast, and multicast frames are forwarded and spread within one VLAN without being directly entered into any other VLAN.

Port-based VLAN is the simplest method to divide the VLAN. The user can divide the ports on the device into different VLAN, and then the message received from a port can only be transmitted within the corresponding VLAN, thus realizing the isolation of the broadcast domain and the virtual working group.Port link types can be divided into three types: Access, Trunk, and Hybrid. These three ports are processed differently when adding VLAN and forwarding messages。

Access Type: Port can only belong to 1 VLAN; generally used for connection between switch and end user;

Trunk Type: Port can belong to multiple VLAN, and can receive and send multiple VLAN messages, but only native VLAN can be carried without the VLAN tag; generally used for connection between switches;

Hybrid Type: The port can belong to multiple VLAN, can receive and send the packets of multiple VLAN, and can configure the relevant VLAN with VLAN tags according to the user's needs; it can be used to connect between switches or to connect the user's computer。

6.2. CONFIGURING COMMANDS

- Create a delete VLAN

Command	(Routing)#vlan database

	(Routing)(vlan)# **vlan** VLAN_RANGE (Routing)(vlan)# **no vlan** VLAN_RANGE
Description	Create / delete a VLAN

- Configure a VLAN based on the Access port

Command	(Routing)(config)#**interface** 0/1 (Routing)(config-if)#**(Routing)port mode access**
Description	Enter the Ethernet port mode。 Configure port type Access port (Access type by default)。

Command	(Routing)(config-if)#**(Routing)port access vlan** VLANID (Routing)(config-if)#**no (Routing)port access vlan**
Description	Add the current port to the specified VLAN (by default, all Access ports belong to and only to VLAN 1) and the no command returns to the default。 The command as above can be used only when the interface has been configured as a Access port, and the specified VLAN must have been created。 When configured as non-VLAN 1, the corresponding VLAN deletion will automatically restore to VLAN 1.

- Configure a VLAN based on the Trunk ports

Command	(Routing)(config)#**interface** 0/1 (Routing)(config-if)#**(Routing)port mode trunk**
Description	Enter the Ethernet port mode。 Configure the port type Trunk port。

Command	(Routing)(config-if)#**(Routing)port trunk allowed vlan** { **all** | VLAN_LIST | **none**} (Routing)(config-if)#**no (Routing)port trunk allowed vlan** VLAN_LIST
Description	Maintain the Allowed VLAN list of the Trunk port。 The above command is used only when the interface has been configured as a Trunk port。 All represents automatic mode that automatically joins all VLAN created (even for subsequent creation)； None blanks the Allowed VLAN list where the port does not belong to any VLAN (including native vlan)； VLAN _ LIST means that the Allowed VLAN list is set manually. If it is previously an ALL (automatic mode), the Allowed VLAN list will be emptied before adding the VLAN list. VLAN _ LIST supports standard multi-vlan representations ("-" and "," and a combination of both); The previous added no keyword indicates the deletion of the VLAN represented by the VLAN _ LIST from the Allowed VLAN list。

	When setting all, change the maintenance of Allowed VLAN list to automatic mode, and other commands are modified to manual mode.(By default, in automatic mode when switched from other port mode to Trunk port)。 Only the VLAN already created can be added to the Allowed VLAN list; when the VLAN is deleted, the corresponding VLAN is automatically deleted in the Allowed VLAN list.

Command	(Routing)(config-if)#**(Routing)port trunk native vlan** VLANID (Routing)(config-if)#**no (Routing)port trunk native vlan**
Description	Set up the native vlan for the Trunk port.(By default, the native VLAN of the Trunk port is VLAN 1), and the no command returns to the default。 The above command is used only when the interface has been configured as a Trunk port。 The setting of Native VLAN is not related to whether Allowed VLAN contains this VLAN or even whether VLAN is created, that is, native VLAN can be set to a VLAN not created。

Instructions

✦The default VLAN ID of the local device Trunk port and the Trunk port of the connected device must be consistent, otherwise the default VLAN message will not be transmitted correctly。

- Configure a VLAN based on the general port

Command	(Routing)(config)#**interface** 0/1 (Routing)(config-if)#**(Routing)port mode general**
Description	Enter the Ethernet port mode。 Configure the port type general port。

Command	(Routing)(config-if)#(Routing)port trunk allowed vlan 2 (Routing)(config-if)#vlan participation include 2,3001 (Routing)(config-if)#vlan tagging 2 (Routing)(config-if)#**no** vlan participation include 2,3001 (Routing)(config-if)#no vlan tagging 2
Description	include :inclusive vlan Tagging： Export when it hits the tag

Instructions

✦The default VLAN ID must be the default VLAN ID of the general port of the connected device, otherwise the default VLAN message will not be transmitted correctly。

6.3. DISPLAY COMMAND； DISPLAY ORDER

In privilege mode, you can view the VLAN information. The information displayed includes VLAN VID, VLAN status, VLAN member port, and VLAN, configuration information。

- show VLAN

(Routing) #show vlan

VLAN ID VLAN Name VLAN Type

------- -------------------------------- -------------------

1 default Default

2 VLAN0002 Static

3001 VLAN3001 Static

(Routing) #

7. CONFIGURE QINQ

7.1. QINQ SUMMARIZE

QinQ technology is also called Stacked VLAN or Double VLAN. The standard comes from IEEE 802.1ad, which refers to the public network VLAN Tag of a service provider network before the user message enters the service provider network, and takes the private network user VLAN Tag in the user message as data, so that the message carries two layers of VLAN Tag through the service provider network.

A large number of VLAN is required to isolate users in man, and only 4094 VLAN supported by IEEE 802.1Q protocol is far from meeting the requirements. Through the two-layer Tag package of QinQ technology, the service provider network only spreads according to the unique outer VLAN Tag allocated on the public network, so that different private network users VLAN can be reused, expanding the number of VLAN Tag available to users, and at the same time providing a simple second-layer VPN function, so in fact QINQ technology is a kind of VLAN VPN technology。

In addition to QINQ, VLAN Mapping is another common VLAN VPN technology. The difference between the two is only that QINQ stacks vlans and VLAN Mapping maps vlans.。

- VLAN Stacking: From the user network to the provider network, single-layer Tag to double-layer Tag, C-Tag remains in the message as the inner Tag; reverse, from double-layer Tag to single-layer Tag。

7.2. CONFIGURATION INSTRUCTIONS

QINQ to be divided three classes：

- Class A: basic QINQ, the interface is opened and closed. When the interface of the basic QINQ receives the message, it is treated as untag message. On the basis of the original message, add a layer of VLAN Tag of the port default VLAN。
- Class B: Flexible QINQ based on C-tag, based on C-VLAN Tag on the user-side, and add a layer of S-VLAN Tag to the original message. There are two optional ways to configure this type of QINQ, and only one one can be chosen. One to configure the mapping of C-VLAN and S-VLAN directly on the interface; one to configure VLAN VPN globally (which includes the mapping between C-VLAN and S-VLAN) and then associate the VPN on the interface. If the same mapping

strategy is adopted for multiple interfaces, the latter configuration mode is generally selected. For such QINQ, if the message received by the interface is untag, C-tag is the default VLAN Tag of the interface。

- Class C: Flexible QINQ based on ACL, adding the outer Tag according to the configured flow strategy. The configuration of this QINQ is put into the "QOS" module in the "Configuring QOS" section, Policy-map and Class-map: "nest vlan <1-4094>" is used to configure the flexible QINQ based on ACL。

For example, the above three types of QINQ can be opened on the same port at the same time, and its priority relationship is: Class C> Class B> Class A。

7.3. CONFIGURING COMMANDS

- Create / Removed vlan-tunnel ethertype

Command	(Routing)(config)#dvlan-tunnel ethertype {802.1Q | vman | custom value} (Routing)(config)#no dvlan-tunnel ethertype (Routing)(config)#dvlan-tunnel ethertype {802.1Q | vman | custom value} [primary-tpid] (Routing)(config)#no dvlan-tunnel ethertype {802.1Q | vman | custom 1–65535} [primary-tpid]
Description	Create / Remove dvlan-tunnel ethertype

- Create / Remove mode dvlan-tunnel

Command	(Routing)(Interface 0/1)#mode dvlan-tunnel (Routing)(config-vlan-vpn)#**no mode dvlan-tunnel**
Description	Create / Remove dvlan-tunnel

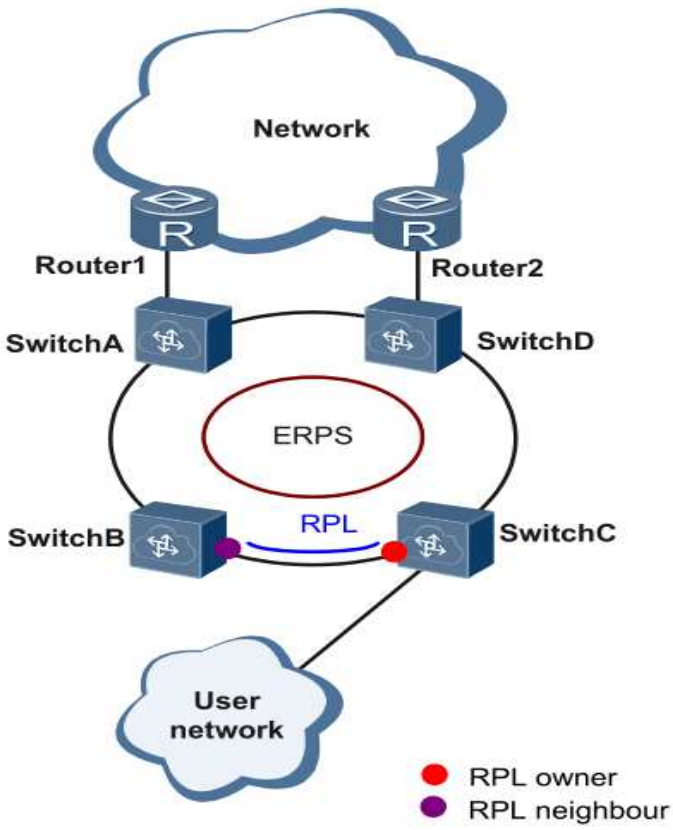
8. CONFIGURE ERPS

8.1. OVERVIEW OF THE ERPS FUNCTIONS

ERPS (Ethernet Ring Protection (Routing) ing, Ethernet net protection switching protocol) is a ring net protection protocol developed for ITU, also known as G.8032. It is a link layer protocol specifically applied to Ethernet ring networks. It can prevent the broadcast storms caused by the data loop when the ethernet net is complete, and can quickly restore the communication between the various nodes when an ethernet link is disconnected。

At present, the technology to solve the problem of the second layer network loop is STP. STP application is relatively mature, but its convergence time is longer (second level). ERPS is a link layer protocol specially applied to the Ethernet ring network. The convergence performance of the second layer is up to 50ms, which has a faster convergence rate than STP。

ERPS typical networking：



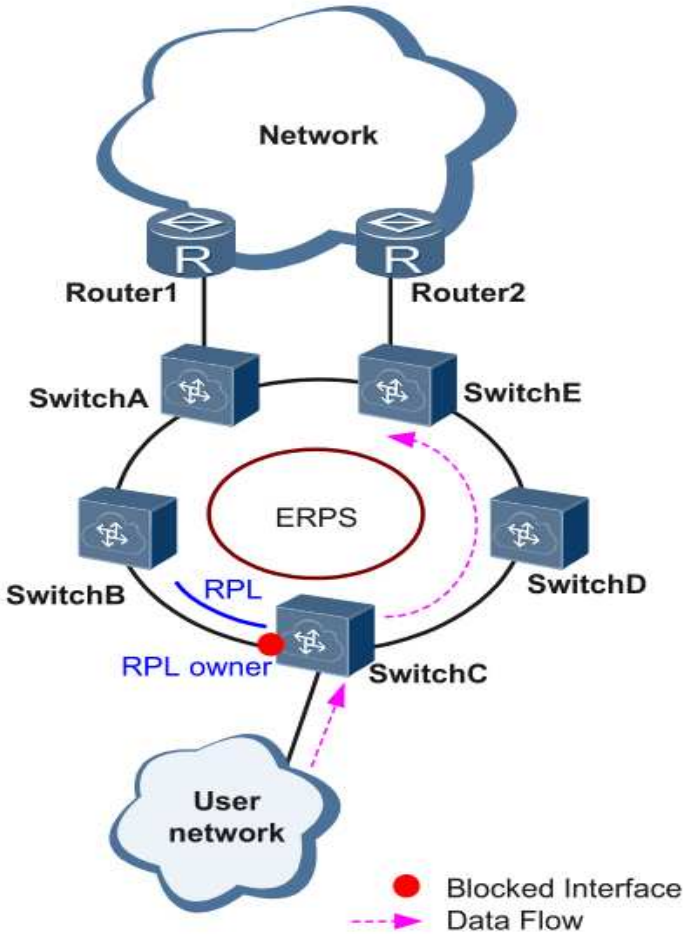
8.2. ERPS, INTRODUCTION OF THE PRINCIPLE

ERPS is a standard ring network protocol dedicated to the Ethernet link layer, with the ERPS ring as the basic unit. Only two ports can join the same ERPS ring. In the ERPS loop, to prevent the appearance of the loop, the breaking loop mechanism can be activated to block the RPL owner port and eliminate the loop. When the link failure occurs in the ring network, the device running the ERPS protocol can quickly open the blocking port, reverse the link protection, and restore the link communication between the nodes of the ring network. This section introduces the basic implementation principle of ERPS under single ring networking according to the process of link normal-> link fault-> link recovery process (including the protection reverse operation)。

The link is normal

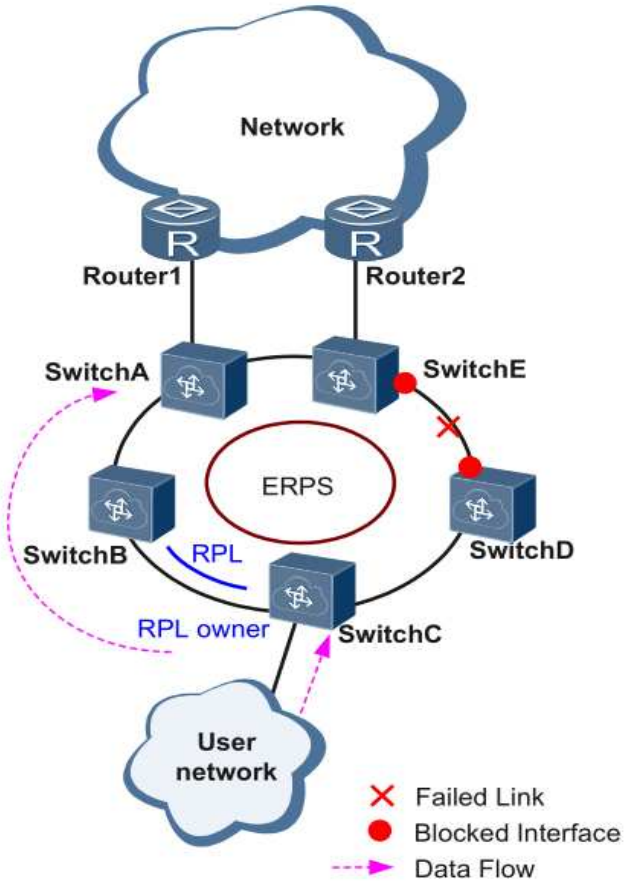
As shown in the figure below, the equipment on the loop composed of (Routing) A to (Routing) E communicate normally。

In order to prevent the loop generation, ERPS will first block the RPL owner port. If the RPL neighbour port is configured, the port will also be blocked, and other ports can forward the business traffic normally。



link failure

As shown in the figure, when the link between (Routing) D and (Routing) E fails, ERPS protocol starts the protection switching mechanism, blocks the ports at both ends of the fault link, and then opens the RPL owner port. The two ports restore the reception and transmission of user traffic, so as to ensure that the flow is not interrupted。



Link recovery

When the link is restored to normal, if the ERPS ring is configured in cut back mode, the device on the RPL owner port will reblock the traffic on the RPL link, and the fault link will be used again to complete the transmission of user traffic。

8.3. CONFIGURING COMMANDS

- Create a ring

Command	(Routing)(config)#**erps domain ring** <1-16> (Routing)(config)#**no erps domain ring** <1-16> (Routing) (Config-erps-domain-1)#role-mode none-interconnection

	(Routing) (Config-erps-domain-1)#ring <1-16>
Description	Create / delete the ERPS ring; The ERPS ring is composed of a set of second layer switching devices configured with the same control VLAN and interconnected. It is the basic unit of the ERPS protocol and needs to be configured。 The ring number is the unique identification of the ERPS ring。

- Associates the ERPS instance and the rings

Command	(Routing)(Config-erps-ring-1)#**erps ring** <1-16>
Description	Configure the correspondence of the ERPS instance and the ring;

- Configure the ERPS instance level

Command	(Routing)(Config-erps-ring-1)#**raps-mel** <0-7>
Description	Configure the ERPS instance level;

- Configure the RPL role in the ERPS instance

Command	(Routing)(Config-erps-ring-1)#**ring-port rpl** NAME (Routing)(Config-erps-ring-1)#**ring-port** rl
Description	Configure the ERPS instance RPL role; An ERPS ring has only one RPL owner port, which is determined by the user configuration to prevent the loop in the ERPS ring from forwarding user traffic by blocking the RPL owner port。

- Configure the management VLAN for instance protection

Command	(Routing)(Config-erps-ring-1))#**raps-vlan** <2-4094> (Routing)(Config-erps-ring-1)#**no raps-vlan**
Description	Configure / delete the management VLAN / data VLAN for the ERPS instance; Each ERPS loop must be configured with a control VLAN. Different ERPS loops cannot use the control VLAN with the same ID。

- Configure the ERPS runback mode

Command	(Routing)(config-erps-prof)#**revertive enable** | **non-revertive enable**
Description	Configure ERPS auto-back / no-back;

- Configure the ERPS timer parameters

Command	(Routing)(config-erps-prof)#wtr-time <1-12>
Description	Configure the ERPS timer reference 数; <1-12>: Unit minutes; the return time after fault recovery, the default is 5 minutes

8.4. DISPLAY COMMAND； DISPLAY ORDER

- The ERPS ring information is displayed

((Routing)) #show erps

D : Discarding

F : Forwarding

FS : Forced (Routing)

MS : Manual (Routing)

```
Domain Ring    Control    WTR Timer    Guard Timer      RL Port              RPL Port
ID     ID      VLAN       (min)        (msec)
-----  ----    ------     ---------    -----------    -------------    ---------------
    1      1      3001              1              500              0/9(B)             0/10(B)

Total number of rings configured = 1
Loacal ring node id: cc:52:91:0a:02:10
((Routing)) #show erps detail

-----------------------------------------------------
 Domain ID :                              1
 Ring ID :                                1
 Ring Topology mode :                     major-ring
 Node Type mode :                         rpl-owner-node
 RAPS Level     :                         0
 Control Vlan :                           3001
 Protected Instance :                     0
     Service Vlan : 0-4092
 WTR Timer Setting (min) :                1
 Guard Timer Setting (msec) :             500
 Holdoff Timer Setting (msec) :     0
 WTB Timer Setting (sec) :                5
 Ring State :                             protection
 Revertive Mode :                         revertive
 Time since last topology change : before 1175sec.
 Forced (Routing) Port :                  NULL
 Manual (Routing) Port :                  NULL
 RL Port :                                0/9(Block)
 RPL Port :                               0/10(Block)

((Routing)) #show erps statistics

-------------------------------------------------------------------------------
Ring   Port     RX/TX        SF           NR         NRRB           FS           MS       EVENT
---- ------ ------ ------- --------- --------- --------- --------- ---------
    1      0/9    RX              0            0            0            0            0            0
```

1	0/9	TX	0	0	0	0	0	0
1	0/10	RX	0	0	0	0	0	0
1	0/10	TX	0	0	0	0	0	0

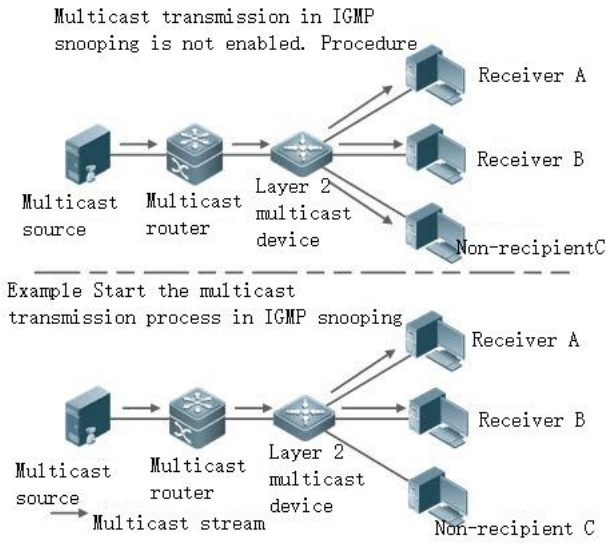
8.5. CONFIGURE IGMP SNOOPING

SUMMARIZE

IGMP Snooping Is short for Internet Group Management Protocol Snooping (Internet Group Management Protocol Pop), it is a mechanism of multicast constraints running on second layer devices, used to manage and control multicast groups。

The second 2 device running IGMP Snooping establishes the mapping relationship for the port and MAC multicast address by analyzing the received IGMP messages, and forwards the multicast data according to such mapping relationship. When the second floor device is not running IGMP Snooping, the multicast data is broadcast on the second floor; when the second floor device is running IGMP Snooping, the multicast data of the known multicast group is not broadcast on the second floor and is broadcast to the designated receiver on the second floor.

As shown in the figure below, when the device is not running IGMP Snooping, the IP message is broadcast in the VLAN; after running IGMP Snooping, the IP message is only sent to the receiver of the group members。



8.6. CONFIGURING COMMANDS

- Enable IGMP Snooping

Command	(Routing)(config)#**set igmp** (Routing)(config)#**no set igmp** (Routing)(config)#**set igmp** [*vlan-id*] (Routing)(config)#**no set igmp** [*vlan-id*]
Description	Enable or disable IGMP Snooping. Default off。 Global mode。

- Configure the IGMP Snooping port

Command	(Routing)(config)#set igmp interfacemode (Routing)(config#no set igmp interfacemode
Description	Open / close the IGMP Snooping port; optional configuration。

- Configure the IGMP Snooping query

Command	(Routing)(config)set igmp querier 1 (Routing)(config)set igmp querier election participate 1
Description	Configure / delete the IGMP Snooping querer

- Configure the IGMP Snooping to leave quickly

Command	(Routing)(config)#`set igmp fast-leave [`*vlan-id*`]` (Routing)(config)#**no** `set igmp fast-leave [`*vlan-id*`]`
Description	Configure / Remove the IGMP Snooping Quick Leave feature; optional configuration。 The SVI interface mode。

- Configure the IGMP Snooping aging time

Command	(Routing)(config)#`set igmp groupmembership-interval [`*vlan-id*`]` *second* (Routing)(config)#**no** `set igmp groupmembership-interval [`*vlan-id*`]` *second*
Description	Configure / delete the IGMP Snooping aging time; optional configuration

- Configure the IGMP Snooping maximum response time

Command	(Routing)(config)#`set igmp maxresponse [`*vlan-id*`]` *seconds* (Routing)(config)#**no** `set igmp maxresponse [`*vlan-id*`]` *seconds*
Description	Configure / delete the IGMP Snooping response time; optional configuration

- Configure IGMP Snooping mrouter

Command	(Routing)(config-0/1)#`set igmp mrouter` *vlan-id* (Routing)(config-0/1)#**no** `set igmp mrouter` *vlan-id* (Routing)(config-0/1)#`set igmp mrouter interface` (Routing)(config-0/1)#no `set igmp mrouter interface`
Description	Configure / delete the mrouter; Optional configuration

8.7. DISPLAY COMMAND

- View IGMP Snooping multicast groups

```
(Routing) #show igmpsnooping 1

VLAN ID..................................... 1
IGMP Snooping Admin Mode.................... Enabled
Fast Leave Mode............................. Enabled
Group Membership Interval (secs)............ 260
Max Response Time (secs).................... 10
Multicast Router Expiry Time (secs)......... 0
Report Suppression Mode..................... Disabled

(Routing) #
(Routing) #show igmpsnooping

Admin Mode.................................. Enable
Multicast Control Frame Count............... 15
IGMP header validation...................... Enabled
Interfaces Enabled for IGMP Snooping........... 0/1
                                               0/2
                                               0/3
                                               0/4
                                               0/5
                                               0/6
                                               0/7
                                               0/8
```

```
                                                0/9
                                                0/10
                                                0/11
                                                0/12
                                                1/1
                                                1/2
                                                1/3
                                                1/4
                                                1/5
                                                1/6
                                                1/7
                                                1/8
VLANs enabled for IGMP snooping.............. 1

(Routing) #show igmpsnooping mrouter

Command not found / Incomplete command. Use ? to list commands.

(Routing) #show igmpsnooping querier

Global IGMP Snooping querier status
-----------------------------------
IGMP Snooping Querier Mode.................... Enable
Querier Address............................... 0.0.0.0
IGMP Version.................................. 2
Querier Query Interval........................ 60
Querier Expiry Interval....................... 125
```

9. CONFIGURE THE STP SPANNING TREE PROTOCOL

9.1. SUMMARIZE

The spanning tree protocol is a second layer management protocol that eliminates the second layer loop by selectively blocking redundant links in the network, and also has the function of link backup。

Like the development process of many protocols, the spanning tree protocol is constantly updated with the development of the network, from the initial STP (Spanning Tree Protocol, spanning tree protocol) to RSTP (Rapid Spanning Tree Protocol, fast spanning tree protocol) to the latest MSTP (Multiple SpanningTree Protocol, multi-spanning tree protocol)。

For the second floor of Ethernet, there can only be one active path between the two LAN, otherwise there will be a broadcast storm. However, in order to strengthen the reliability of a LAN, it is necessary to establish redundant links, some of which must be in the backup state. If the network fails and the other link fails, the redundant link must be promoted to the active state. Manual controlling such a process is obviously a very hard work, and the STP protocol does it automatically. It enables a device in a LAN to function as follows:

Discover and initiate an optimal tree topology structure of the LAN。

The fault is found and recovered accordingly, and the network topology structure is automatically updated, so that the best possible tree structure is selected at any time。

9.2. CONFIGURING COMMANDS

- Configure the STP mode

Command	(Routing)(config)#**spanning-tree mode** {**stp** | **rstp** | **mst**}
Description	stp：Spanning tree protocol(IEEE 802.1d) rstp：Rapid spanning tree protocol(IEEE 802.1w)

	mst：Multiple spanning tree protocol(IEEE 802.1s) The default is mstp mode and the generator tree protocol is off by default and needs to be re-enabled。 Global mode。

- Enable the build tree protocol

Command	(Routing)(config)#**spanning-tree** (Routing)(config)#**no spanning-tree**
Description	Enable / turn off the STP function; the default is off。 Global mode。

- Configure the device priorities

Command	(Routing)(config)#**spanning-tree priority** <0-4094> <0-61440> (Routing)(config)#**no spanning-tree priority** <0-4094>
Description	Configure / remove the STP system priority; default 32768. Optional configuration。 Global mode。

- Configure Forward-Delay Time

Command	(Routing)(config)#**spanning-tree forward-time** <4-30> (Routing)(config)#**no spanning-tree forward-time**

Description	Configure / reset the STP port forwarding status delay time in seconds; the default is 15s. Optional configuration。 Global mode。

- configureMax-Age Time

Command	(Routing)(config)#**spanning-tree max-age** <6-40> (Routing)(config)#**no spanning-tree max-age**
Description	Configure / reset the lifetime of the BPDU message in seconds; the default is 20s. Optional configuration。 Hello Time、Forward-Delay Time、Max-Age Time Conditions need to be followed: 2*(Hello Time + 1.0 seconds) <= Max-Age Time <= 2*(Forward-Delay – 1.0seconds), Otherwise, it may lead to topological instability The longest path of STP / RSTP network is affected by this parameter. The default longest path is 20 sets. When exceeding 20 devices, modify the configuration (forward-delay 21s, max-age 40s), and the maximum longest path is 40 sets。 Global mode。

- Configure Max-Hops

Command	(Routing)(config)#**spanning-tree max-hops** <6-40> (Routing)(config)#**no spanning-tree max-hops**
Description	Configure / reset the maximum jumps of BPDU message; default is 20. Optional configuration。 The longest path of the MSTP network is affected by this parameter, requiring configuration modification when exceeding 20 devices, maximum 40。

	MSTP is compatible with the max-age function, which requires simultaneous adjustment of the max-age parameter, and refer to the corresponding command。 Global mode。

- configureTransmit-Holdcount

Command	(Routing)(config)#**spanning-tree transmit hold-count** <1-10> (Routing)(config)#**no spanning-tree transmit hold-count**
Description	Configure / reset the maximum number of BPDU sent per second; the default is 6. Optional configuration。 Global mode。

- Found instance

Command	(Routing)(config)#**spanning-tree mst instance** <1-4094> (Routing)(config)#**no spanning-tree mst instance** <1-4094>
Description	Create / delete the instance instance。 Global mode。

- Configure the correspondence of MST VLAN and instance

Command	(Routing)(config)# **spanning-tree mst vlan** <1-4094> <1-4094> (Routing)(config)# **no spanning-tree mst vlan** <1-4094> <1-4094>

Description	Configure / delete the association of the MST instance and the VLAN; optional configuration。 Global mode。

- Configure the MST area name

Command	(Routing)(config)#**spanning-tree configuration name** NAME (Routing)(config)#**no spanning-tree configuration name** NAME
Description	Configure / delete the MST area name; optional configuration。 Global mode。

- Configure the MST version number

Command	(Routing)(config)#**spanning-tree configuration revision** <0-65535>
Description	Configure / delete the MST version number, with the default to 0; optional configuration。 Global mode。

- Configure the port priority

Command	(Routing)(config-if)#**spanning-tree port-priority** <0-240> (Routing)(config-if)#**spanning-tree instance** <1-4094> **port-priority**<0-240>
Description	Configure port STP priority; default 128. Optional configuration。 Interface configuration mode。

- Configure the port path cost

Command	(Routing)(config-if)#**spanning-tree cost** <1-200000000> (Routing)(config-if)#**no spanning-tree cost**
Description	Configuring / reset port path cost; optional configuration。 Interface configuration mode。

- Configure the Protocol Migration processing

Command	(Routing)(config-if)#**clear spanning-tree detected protocols**
Description	Version checking is mandatory for all of the ports。 Privilege mode。

- Configure the Edge Port

Command	(Routing)(config-if)#**spanning-tree {edgeport | auto-edge}** (Routing)(config-if)#**no spanning-tree {edgeport | auto-edge}**
Description	Configuring / delete port Edge Port; configured with edgeport means that the port direct connection device is not a bridge device and can be fast forward; configured as autoedge indicates that the port automatically recognizes edge ports by the BPDU; closed by default; optional configuration. Interface configuration mode。

- configureRoot Guard

Command	(Routing)(config-if)# **spanning-tree guard root**

	(Routing)(config-if)**#no spanning-tree guard root**
Description	Configure / delete the port Root Guard; when the interface opens the Root Guard function, force its port role on all instances to be the specified port, and once the port receives higher priority configuration information, the Root Guard function places the interface to blocked status; off by default; optional configuration。 Interface configuration mode。

- configureBPDU Filter

Command	(Routing)(config)**#spanning-tree bpdufilter** (Routing)(config)**#no spanning-tree bpdufilter**
Description	Configure / delete BPDU Filter; after the port opens BPDU Filter, neither send BPDU nor receive BPDU message; optional configuration. Interface configure mode。

9.3. DISPLAY COMMAND

- View the STP status

```
(Routing)#show spanning-tree
```

- View the MSTP instance status

```
(Routing)#show spanning-tree mst detailed <0-4094>
```

10. MAC ADDRESS ADMINISTRATION

10.1. OVERVIEW OF THE MAC ADDRESSES

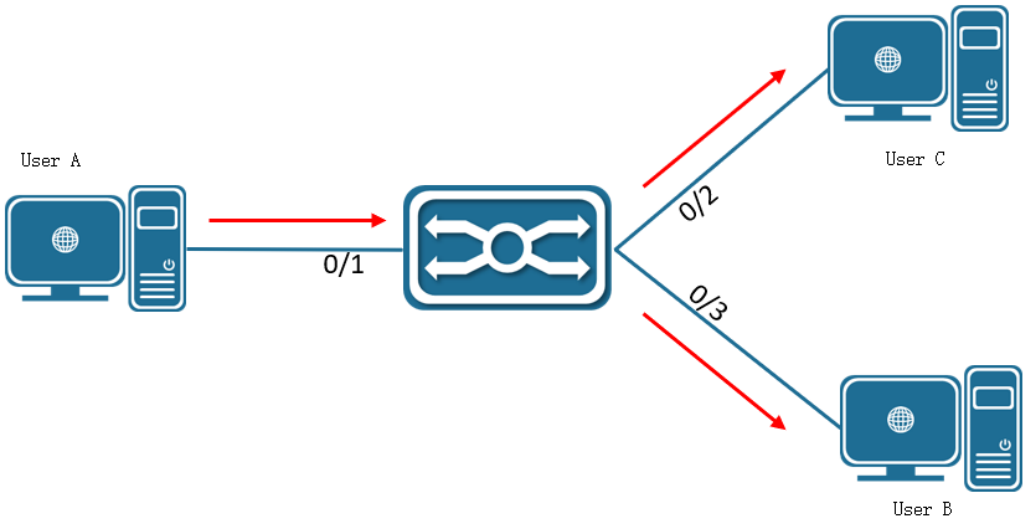
The Ethernet switch resolves the destination MAC address carried by the message, queries the MAC address table, and sends the message to the corresponding port. The MAC address table records the MAC address, the interface of the device connected to, and the VLAN ID information of the device. Ethernet switch decides to adopt the forwarding mode of known list broadcast or unknown broadcast according to the result of MAC address table search。

Know the list broadcast： The Ethernet switch finds the table item corresponding to the destination MAC address and VLAN ID of the message in the MAC address table, and the output port in the table item is unique, and the message is directly output from the port corresponding to the table item。

Unknown radio： The Ethernet switch does not find the table item corresponding to the target MAC address in the address table, and the message is sent to all other ports in the subordinate VLAN except the message input port。

The MAC address of the Ethernet switch can be obtained dynamically or by static configuration and generally obtained by dynamic acquisition. The following paper analyzes the interaction process between user A and user C, and gives the working principle of MAC address dynamic learning。

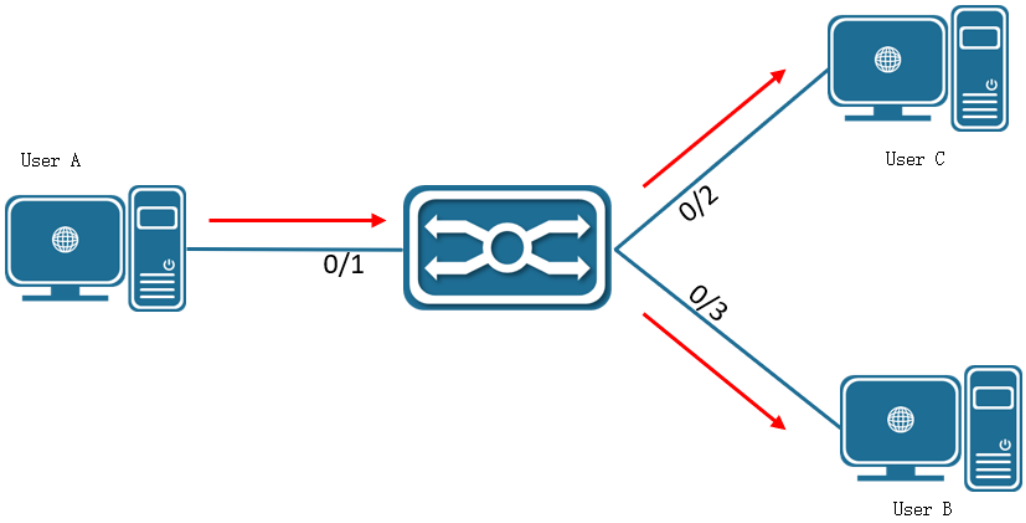
User A sends A message to the port gigabitEthernet0 / 1 of the switch, when the Ethernet switch learns the MAC address of user A into the MAC address table. Since there is no source MAC address for user C in the address table, the Ethernet Switch sends the message to all ports belonging to VLAN 1 except gigabitEthernet0 / 1 connecting user A, including the ports of user B and user C, where user B can receive the message not belonging by user A。



Current dynamic MAC address table information:

user	VLAN	MAC address	port
User A	1	000E.C6C1.C8AB	gigabitEthernet0/1

After receiving the message, user B will send the response message to user A through the port gigabitEthernet0 / 2 of the Ethernet switch, the MAC address exists in the MAC address table of the Ethernet switch, and the message is forwarded to the gigabitEthernet0 / 1 port by unicast, and the Ethernet switch will learn the MAC address of user C, what is different from the previous is that user B cannot receive the message sent by user C to user A at this time。



Current dynamic MAC address table information:

User	VLAN	MAC address	port
User A	1	000E.C6C1.C8AB	gigabitEthernet0/1
User C	1	000E.C6C1.C8AD	gigabitEthernet0/2

After an interaction between user A and user C, the device learns the source MAC address of user A and user C, and then the message interaction between user A and user C is forwarded by unicast, after which user B will not receive the interaction message between user A and user C.

10.2. CONFIGURING COMMANDS

- Configure the dynamic MAC address aging time

Command	(Routing)(config)#**bridge aging-time** <10-1000000> (Routing)(config)#**no bridge aging-time**
Description	Configure MAC address aging time, range 10-1000000 seconds; The default MAC address burn-in time is for 300 seconds;

- Configure the static MAC address

Command	(Routing)(config-0/1)#**port-security mac-address** MAC_ADDR VLANID (Routing)(config-0/1)#**no port-security mac-address** MAC_ADDR VLANID
Description	Configure the static MAC address; When the device receives a message addressing the MAC _ ADDR on the VLAN specified by the VLANID

- Clear the dynamic MAC address

Command	(Routing)#**clear mac-address-table all** (Routing)#**clear mac-address-table interface**

	(Routing)**#clear mac-address-table vlan**
Description	Dynamic MAC address clearing operation; Supports all, VLAN-based, port-based MAC address clearing operations

10.3. REVEALCOMMAND

- Show the MAC address

```
((Routing)) #show mac-addr-table all

VLAN ID  MAC Address         Interface             IfIndex  Status
-------  ------------------  --------------------  -------  ------------
1        00:E0:4C:1D:65:FE   0/3                   3        Learned
1        C8:39:0D:01:DC:99   0/1                   1        Static
1        C8:39:0D:01:DC:A0   3/1                   65       Management

((Routing)) #
```

- Displays the number of MAC addresses

```
((Routing)) #show mac-addr-table count

Dynamic Address count..................... 2
Static Address (User-defined) count..... 1
Total MAC Addresses in use..... 3
Total MAC Addresses available..... 32768
```

11. CONFIGURE LLDP

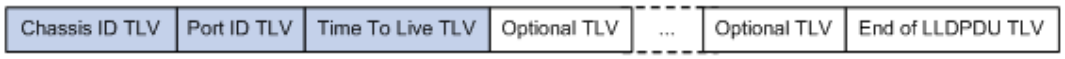
1.1. AGREEMENT OVERVIEW

LLDP (Link Layer Discovery Protocol, Link Layer Discovery Protocol) provides a standard link layer discovery method that enables devices of different vendors to discover and interact with their own system and configuration information in the network. LLDP will encapsulate the information of the equipment (including main capability, management address, equipment identification, interface identification, etc.) in LLDPDU (Link Layer Discovery Protocol Data Unit, link layer discovery protocol data unit) to the neighbors directly connected to save it in the form of standard MIB for the network management system to query and determine the communication status of the link。

LLDPDU

LLDPDU Is a data unit packaged in the data section of the LLDP message. Before forming the LLDPDU, the device first encapsulates the local information into TLV format, and then combines several TLVs into a LLDPDU packaged in the data part of the LLDP message for transmission。

Figure Figure 22 1 . Package format of the LLDPDU



As shown in Figure Figure 22 1, the blue Chassis ID TLV, Port ID TLV, and Time To Live TLV must be carried by each LLDPDU, while the remaining TLV is optional. Each LLDPDU can carry a maximum of 32 TLV species。

TLV

The TLV is the unit that constitutes the LLDPDU, and each TLV represents a message. TLVs that LLDP can package include basic TLV, 802.1 tissue definition TLV, 802.3 tissue definition TLV and LLDP-MED (Link Layer Discovery Protocol Media Endpoint Discovery, Link Layer Discovery Protocol Media Terminal Discovery) TLV。

basic TLV

Basic TLV is a group of TLVs based on network equipment management. 802.1 organizational definition TLV, 802.3 organizational definition TLV and LLDP-MED TLV are TLVs defined by standard organizations or other organizations to enhance the management of network equipment. They can choose whether to send in LLDPDU according to actual needs。

In basic TLV, several TLV are required for implementing LLDP functionality, that is, must be published in LLDPDU, as shown in Table Table 22 1。

Table Table 22 1 Basic TLV

TLV name	instruction	Is it necessary to publish
Chassis ID	The Bridge MAC address of the sending device	Yes
Port ID	Identifies the port of the LLDPDU sender. If LLDP-MED TLV is carried in LLDPDU, its content is the MAC address of the port; otherwise, its content is the name of the port	Yes
Time To Live	Survival time of this device information on the neighbor device	Yes
End of LLDPDU	The end identity of LLDPDU, is the last TLV of LLDPDU	No
Port Description	Description of the port	No
System Name	Name of the device	No
System Description	Description of the system	No
System Capabilities	Main functions of the system and the open function items	No
Management Address	Manage the address, and the corresponding answer slogan and OID (Object Identifier, object identifier)	No

802.1Organization defines a TLV

IEEE 802.1The contents of the tissue-defined TLV are shown in Table Table 22 2。

Currently, H3C devices do not support sending Protocol Identity TLV and VID Usage Digest TLV, but can receive both types of TLV.

Three-tier Ethernet interface is supported onlyLink Aggregation TLV。

Table Table 22 2　IEEE 802.1 tissue-defined TLV

TLV name	Instructions
Port VLAN ID(PVID)	Port VLAN ID
Port and protocol VLAN ID(PPVID)	Port protocol VLAN ID
VLAN Name	Name of the VLAN that the port belongs to
Protocol Identity	The type of protocol supported by the port
DCBX	Data center bridge capability exchange protocol (Data Center Bridging Exchange Protocol)

TLV name	Instructions
EVB module	(Not supported) Edge virtual Bridge (Edge Virtual Bridging) module, including EVB TLV and CDCP (S-Channel Discovery and Configurati on Protocol, S Channel Discovery and Config Protocol) TLV. For de tails of either TLV, see the EB Configuration Guide
Link Aggregation	Whether the port supports link aggregation and whether link aggreg ation is enabled
Management VID	manage VLAN
VID Usage Digest	Contains data for a summary of VLAN ID usage
ETS Configuration	Enhance transmission options (Enhanced Transmission Selection) co nfigure
ETS Recommendation	Enhanced transport selection recommendation
PFC	Priority-based flow control (Priority-based Flow Control)
APP	Application protocol (Application Protocol)
QCN	(Not yet supported) Quantified congestion notification (Quantized Co ngestion Notification)

802.3 Organization defines a TLV

IEEE 802.3 The contents of the tissue definition TLV are shown in Table Table 22 3。

Power Stateful Control TLV Is defined in IEEE P802.3at D1.0, and later versions no longer support this TLV. The H3C devices will send this type of TLV only after receiving the Power Stateful Control TLV。

Table 22 3 IEEE 802.3 TLV

TLV name	Instructions
MAC/PHY Configuration/Sta tus	Port support rate and duplex status, whether the port rate autom atic negotiation is supported, whether the automatic negotiation fu nction is enabled, and the current rate and duplex status
Link Aggregation	Whether the port supports link aggregation and whether link aggr egation is enabled
Power Via MDI	The power supply capacity of the port, including the types of Po E (Power over Ethernet, Ethernet supply) (including PSE (Power Sourcing Equipment, power supply equipment) and PD (Powered Device, receiving equipment)), remote power supply mode of PO SE port, whether PSE supply is supported, whether PSE supply mode is controlled, power supply type, power source, power prior ity, PD request power value, and PSE allocated power value

TLV name	Instructions
Maximum Frame Size	Maximum frame length supported by the ports
Power Stateful Control	Power status control of the port, including type of power used in PSE / PD, priority and power of PSE / PD
Energy-Efficient Ethernet	Energy-efficient Ethernet

Manage the address

Management address is the address for the network management system to identify and manage the network equipment. The management address can clearly identify a device, which is conducive to the drawing of network topology and facilitate network management. The management address is enclosed in the Management Address TLV of the LLDP message。

Working mode of LLDP

Under the LLDP agent of the specified type, LLDP has the following four working modes：

- TxRx：Both send and receive LLDP messages。
- Tx：Only send unreceived LLDP messages。
- Rx：Only receive and not send LLDP messages。
- Disable：Neither send nor receive LLDP messages。

When the LLDP operation mode of the port changes, the port initializes operations on the protocol status machine. In order to avoid frequent changes in the port working mode of the port, the port initialization delay time can be configured when the port working mode changes。

Protocol specification

The protocol specifications related to LLDP are：

- IEEE 802.1AB-2005：Station and Media Access Control Connectivity Discovery
- IEEE 802.1AB 2009：Station and Media Access Control Connectivity Discovery
- ANSI/TIA-1057：Link Layer Discovery Protocol for Media Endpoint Devices
- IEEE Std 802.1Qaz-2011：Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks-Amendment 18: Enhanced Transmission Selection for Bandwidth Sharing Between Traffic Classes

1.2. CONFIGURING COMMANDS

1.2.1. Switch and operating mode configuration

- Configure the switch working mode of the LLDP interface

Command	(Routing)(Interface 0/1)# **lldp** { receive | transmit }

	(Routing)(Interface 0/1)# **lldp disable**
Description	LLDP interface configuration mode。 Configure the working mode of the LLDP interface。 selectable。

1.2.2. **Optional basic parameter configuration**

- Configure system name

Command	(Routing)(Interface 0/1)#lldp transmit-tlv sys-name (Routing)(Interface 0/1)#lldp transmit-tlv sys-desc (Routing)(Interface 0/1)#lldp transmit-tlv sys-cap (Routing)(Interface 0/1)#lldp transmit-mgmt (Routing)(Interface 0/1)#lldp notification (Routing)(Interface 0/1)#lldp med
Description	Interface mode。 Configure / reset the system name。 selectable。

1.2.3. **Optional state machine parameter configuration**

- Configure the hold parameters for the LLDP interface

Command	((Routing)) (Config)#lldp timers

	<cr>	Press enter to execute the command.
	hold	The interval multiplier to set local LLDP data TTL.
	interval	The interval in seconds to transmit local LLDP data.
	reinit	The delay before re-initialization.
Description	Global modeLldp Send interval, etc selectable。	

- Configure the LLDP notification parameter

Command	(Routing)(lldp)# notification-interval <5 - 3600> (Routing)(lldp)#
Description	全 Bureau configuration mode。

1.3. DISPLAY COMMAND

- Displays the status of the LLDP interface

```
#show lldp interface 0/1

((Routing)) #show lldp interface 0/1

LLDP Interface Configuration

Interface  Link    Transmit  Receive   Notify    TLVs     Mgmt
---------  ------  --------  --------  --------  -------  ----
0/1        Down    Enabled   Enabled   Enabled   1,2,3    Y
```

```
TLV Codes: 0- Port Description,   1- System Name
           2- System Description, 3- System Capabilities
```

- Displays LLDP interface neighbors

```
#((Routing)) #show lldp remote-device int 0/1
```

12. CONFIGURING L3

12.1. L3 OVERVIEW

L3 functions include three layers of port management, ARP management, and routing management. Routing management does not include dynamic routing management。

- Three-layer mouth management：

The third layer port is for the second floor (exchange) port, generally divided into routing port (ordinary physical port or aggregation port switch to the third layer port) or SVI port ((Routing) Virtual Interface, corresponding to a VLAN). SVI port is a logical interface, architecture on the corresponding VLAN, all members port, after SVI three layers of forwarded message, in the input first through two (such as VLAN filtering, address learning) and then through three layers, in the output first through three layers and then through the second layer (such as VLAN output rules)。

The Internet Protocol (Internet Protocol, IP) uses a logically virtual address to send packets from the source party to the destination party, or the IP address. At the network layer, the routing device uses the IP address to complete packet forwarding。 （Protocol specification：RFC 1918：Address Allocation for Private Internets， RFC 1166：Internet Numbers）

Triple port management also includes triple port IP address maintenance. The IP address consists of 32-bit binary, which is generally expressed in decimal points for the convenience of writing and description. When expressed in decimal system, points are divided into four groups, ranging from 0 to 255, between groups with "." Number is separated, such as "192.168.1.1" is an IP address expressed in the decimal system. The IP address, as the name implies, is naturally the interconnect address of the IP layer protocol. The 32-bit IP address consists of two parts: 1) network address, indicating which network; 2) host address, indicating which host is in the network. The network address part of the IP address and the host address part are divided by the network mask. The network mask is also a 32-bit value, consisting of the previous bits "1" and the following bits "0". The IP address and the network mask are the corresponding network address part. Similarly, the network mask can be also directly represented by the mask length. For example, "192.168.1.1 255.255.255.0" and "192.168.1.1/24" represent the same IP address。

The three-level port does not support the configuration of second IP address, that is, a three-level port is configured with at most one IP address. When a three-layer port is configured with IP address, a network segment is determined. Different three-layer ports of the same device must belong to different network segments, and IP addresses configured with different three-layer ports must belong to different network segments. SVI represents the three-layer port, with the corresponding VLAN serving as the unique identification of the three-layer port。

After the different three layers of the device are divided into different network segments, the forwarding between these different network segments (such as VLAN 1 and VLAN 2) is called "three layers of forwarding" (across the network segments, or across different VLAN)。

- ARP manage：

In the LAN, each IP network device has two addresses: 1) local address, because it is included in the frame header of the data link layer, more accurately should be the data link layer address, but actually the local address is the MAC sublayer, so it is commonly called the MAC address, the MAC address represents the IP network device; 2) the network address, the network represents the IP network device on the Internet, and it also describes the network where the device belongs。

Two IP devices on the LAN require communication and must know their 48-bit MAC address. The process of knowing a MAC address based on an IP address is called address resolution. There are two types of address resolution methods: 1) address resolution protocol (ARP); 2) proxy address resolution protocol (Proxy ARP). For ARP and Proxy ARP, described in RFC 826, RFC 1027, respectively。

The ARP (Address Resolution Protocol, Address Resolution Protocol) is used to bind the MAC address and the IP address, with the IP address as the input, and the ARP can know its associated MAC address. Once the MAC address is known, the IP address corresponding to the MAC address is saved in the device's ARP cache. With the MAC address, the IP device can encapsulates the link layer frames and then send the data frames to the LAN. The package of IP and ARP on Ethernet is of the Ethernet II type。

ARP table items are divided into two categories: dynamic table items generated by ARP protocol, and static table items derived from static configuration. Dynamic ARP table items are triggered by IP message. The opening process is a process of ARP request / response. The ARP table items will

automatically age if they cannot be reached later. Static ARP table items do not need to be opened up, and will not age。

- Routing management：

Routing management is responsible for managing routing tables, integrating routes issued by various routing agreements, and optimizing. The routing tables are usually divided into the following three categories according to the different sources：

- Direct routing: routing discovered by the link layer protocol, also known as interface routing. Direct connection routing is automatically generated when the IP address is configured by the three layers, and the routing prefix is the direct connection network of the three layers。
- Static routing: manually configured by a network administrator。
- Dynamic routing: the routing discovered by dynamic routing protocols (such as RIP, OSPF)。

This device does not support a dynamic routing protocol and, therefore, does not support dynamic routing。

The routing table item consists of two parts：

- Prefix: represented by an IP address and network mask (or mask length), refers to the destination network or host determined by the routing table item (when the mask length is 32)。
- Direct connection or next jump: Direct connection indicates that the destination network or host belongs to the direct network, and direct routing belongs to this case. In the configuration of static routing, it instead of the IP address; to reach the destination network or host, it should be forwarded to the IP network device indicated by the IP address。

When the IP message is forwarded according to the routing table item, if the routing table item specifies the next jump, and the link layer package queries the ARP, use the next jump IP, that is, the destination MAC address of the link layer package is the destination MAC address of the next jump. If the routing table item is directly connected, the destination IP of the message is directly used for ARP query, that is, the MAC address of the destination of the link layer package is the MAC address of the ultimate purpose of the message. Either way, if the ARP query fails, the route will be triggered (generate dynamic ARP table items). If not, the IP message cannot be forwarded, it will be discarded。

There may be inclusion relationships between routing items (depending on the mask length), so the routing lookup process meets the LPM (Longest Prefix Match, longest prefix match). That is, when IP message forwarding for routing search, if multiple routing table items are hit at the same time, the prefix route table item with the longest mask length is selected。

12.2. CONFIGURING COMMANDS

12.2.1. **Configure / delete the rate mode**

Command	**Configuring Routing Mode：** (Routing)(config)#**interface** 0/1 (Routing)(config-0/1)#ip routing **Remove routing mode：** (Routing)(config-if)#no ip routing
Description	Turn on / delete the routing mode

12.2.2. **Configure / delete the SVI port IP address**

Command	**Configure the triple port IP address:** (Routing)(config)#vlan routing 10 1 (Routing)(config)#int vlan 10 (Routing)(config-if)#**ip address** IPADDR MASK

	Delete the Triport IP address： (Routing)(config)#int vlan10 (Routing)(config-if)#**no ip address** IPADDR MASK **View the IP address of the third port：** (Routing)#**show ip interface brief**
Description	Configuration is performed in the interface mode of the SVI。 When VLAN is created, SVI is automatically created, and when VLAN is deleted, SVI is automatically deleted.int vlanXX Is the interface mode entering the SVI, not the SVI port, so when the SVI does not exist (the corresponding VLAN does not exist), the interface mode entering the SVI will fail. Also, when the SVI is deleted, the IP address configured on it is automatically cleared。 The third layer port supports IP address configuration update, the same effect as deletion and reconfiguration. The IP addresses configured by different three-layer ports must belong to different network segments。 Configuration second ip is not supported for the triple port。 Note: After this command is configured, the system cleans up the management IP configuration (reference: Configuration Management IP) and instead uses the triple port IP address as the device management IP。

12.2.3. **Configure / delete the routing port IP address**

Command	**Configure the routing port IP address：**

	(Routing)(config)#**interface** 0/1 (Routing)(config-0/1)#ip address IP(A.B.C.D) MASK(A.B.C.D) **Delete the Triport IP address：** (Routing)(config-if)#no ip address IP(A.B.C.D) MASK(A.B.C.D)
Description	Configuration is performed in the interface mode。 Before you configure the routing port IP, since the default attribute of the interface is the second layer port attribute, switch the port from the second layer port attribute, and then configure the IP of the routing port with the ip address command, while the routing port will switch the second layer port attribute using the (Routing) port command。 The third layer port supports IP address configuration update, the same effect as deletion and reconfiguration. The IP addresses configured by different three-layer ports must belong to different network segments。 Configuration second ip is not supported for the triple port。

12.2.4. **Configure / delete the static ARP table items**

Command	(Routing)(config)#**arp** IPADDR MACADD (Routing)(config)#**no arp** IPADDR
Description	Configuration occurs in the global configuration mode。 The IP address of the static ARP configuration must belong to the direct connection segment, otherwise the configuration fails。

	Static ARP priority is higher than dynamic ARP, when the two conflict, to static ARP effective。 If the IP address of the three-tier port is deleted or the three-tier port is deleted, if the IP address of the static ARP belongs to the direct connection segment of the three-tier port, the static ARP fails (the table item is not present through show arp, but show run can see the configuration is still there); similarly, when the IP address of the three-tier port is configured, the ARP item of the IP address of the direct connection segment of the triple port will change from invalid state to valid state.(ARP table entries are visible through show arp)。

12.2.5. **Clear the ARP cache**

Command	(Routing)#**clear arp-cache**
Description	Clears the ARP cache in privilege mode。 This command only cleans up the dynamic ARP items, and the static ARP items will not be cleared。

12.2.6. **Configure / delete the static routes**

Command	(Routing)(config)#**ip route** { IPADDR MASK} {NH_IPADDR | <1-255> } (Routing)(config)#**no ip route** { IPADDR MASK} {NH_IPADDR | <1-255> }
Description	Configuration occurs in the global configuration mode。 Recursive routing is not supported (the next configured hop IP must belong to the direct connection segment); Routing prefix cannot belong to the direct connection network section (i. e., the direct connection route is automatically generated and cannot be configured statically)。

	When the third level port is configured with IP address, if the prefix of a static route table item belongs to the direct connection network segment of the third level port, the static route is automatically deleted and prompted by LOG; When the IP address of the third layer port is deleted or the third layer port is deleted, if the next jump IP of a static route table item belongs to the direct connected network segment of the third layer port, the static route is automatically deleted and prompted by LOG。

12.3. DISPLAY COMMAND

- ARP entries are displayed

```
(Routing)#show arp
Address                  HWaddress              Interface      Type
192.168.1.238          00:00:00:00:04:86       vlan2          Static
192.168.2.46            00:00:00:00:05:45       vlan3          Static
192.168.3.110          00:00:00:00:08:59       vlan4          Static
192.168.0.12            00:00:00:00:00:09       vlan1          Static
192.168.0.1              00:0e:c6:d8:c7:f7         vlan1          Dynamic
10.100.2.2               00:01:a0:00:10:11       GiE0/2         Dynamic
```

- Displays the routing table key

```
(Routing)#show ip route

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
       B - BGP Derived, IA - OSPF Inter Area
       E1 - OSPF External Type 1, E2 - OSPF External Type 2
       N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
       P - Net Prototype
```

13. CONFIGURE OSPFV2

13.1. OSPFV2 OVERVIEW

OSPF (Open Shortest Path First) is an internal gateway routing protocol based on link status developed by the IETF OSPF Working Group.

OSPF is a routing protocol developed for IP, running directly on the IP layer, protocol number 89, OSPF packet exchange with multicast address 224.0.0.5 (all OSPF devices) and 224.0.0.6 (specified devices). It is applied inside the AS (Autonomous System, autonomous system)。

A set of devices running the OSPF routing protocol constitutes an autonomous domain system of the OSPF routing domain。

An autonomous domain system refers to all the devices controlled and managed by an organization. Only one IGP routing protocol is run inside the autonomous domain system, and the routing information is usually exchanged by BGP routing protocol between the autonomous domain systems. Different autonomous domain systems can choose the same IGP routing protocol, and if you want to connect to the Internet, each autonomous domain system needs to apply to the relevant organization for the autonomous domain system number。

When the scale of the OSPF routing domain is large, the hierarchical structure is generally adopted, that is, the OSPF routing domain is divided into several regions (area). The regions are interconnected through a backbone region, and each non-backbone region needs to be directly connected to the backbone region。

In the OSPF routing domain, there are three device roles, depending on where the device is deployed：

- Area devices: All the interface networks of the device belong to one area；
- Regional boundary equipment: the ABR (Area Border Routers). The interface network of the device belongs to at least two regions, one of which must be a backbone region。
- Autonomous domain boundary device: ASBR (Autonomous System Boundary Routers), which is the only route exchange between the OSPF routing domain and the external routing domain。

The link state algorithm is a completely different algorithm from the Huffman vector algorithm (distance vector algorithm). The traditional routing protocol applying the Huffman vector algorithm is RIP, while the OSPF routing protocol is a typical implementation of the link state algorithm. Compared with RIP routing protocol, OSPF, besides different algorithms, also introduces new concepts such as routing update authentication, VLSMs (variable long subnet mask), and routing convergence. The RIP protocol has two fatal weaknesses: slow convergence and limited network size (maximum jumps below 16). OSPF overcomes the weakness of RIP and can be competent for medium to large and more complex network environments。

The OSPF routing protocol uses the link state algorithm to establish and calculate the shortest path to each target network. The algorithm itself is more complex, and the following briefly describes the overall process of the link state algorithm：

- In the initialization phase, the device generates a link status notification, which includes the entire link status of the device；
- All devices exchange link status information through multicast. When each device receives a link status update message, it will send a copy to the local database and then transmit it to other devices；

- When each device has a complete link status database, the device applies the Dijkstra algorithm to calculate the shortest path tree for all the target networks. The results include: the target network, the next hop address, and the cost, which is a key part of the IP routing table。

If there is no link cost, network addition and deletion change, OSPF will be very quiet. If there is any change in the network, OSPF will notify through the link state, but only the changing link state. The devices involved in the change will re-run the Dijkstra algorithm to generate a new shortest path tree。

13.2. CONFIGURING COMMANDS

13.2.1. **Create the OSPF process**

Command	(Routing)(config)**#router ospf** (Routing)(config-router)**#router-id** *router-id* (Routing)(config-router)# **network** *IP(A.B.C.D) MASK(A.B.C.D)* **area** *area-id*
Description	To run the OSPF routing protocol, you need to first create the OSPF routing process and associate the corresponding network with the OSFP routing process。 router router The command is creating the OSPF routing process, the process-id is the instance number of the OSPF routing process, and represents the process instance 1 when not configured。 The router-id command is the ID of the routing device, expressed as an IP address. Each OSPF process is distinguished using a different Router ID。 network The command represents the routing information of the associated network notified by the OSPF command, and also updates the protocol notification and routing information only on the interface corresponding to the associated network。 The IP and the MASK together constitute the address range。 The area-id is the OSPF area identity, which is always associated with an IP address range, and the subnet mask is usually used as the identification of the OSPF area for management convenience。

13.2.2. **Interface network type configuration**

Command	(Routing)(config-if)#**ip ospf network** {broadcast|point-to-point }
Description	broadcast Indicates the broadcast type, sends the OSPF message by group cast, can automatically find the neighbors, and elect DR (Designated Router) and BDR (Backup Designated Router)。 The point-to-point represents the point-to-point connection, which requires the interface 1 to 1 interconnection. The OSPF message is sent by multicast, which will automatically find the neighbors without DR / BDR election。

Command	(Routing)(config-if)#**ip ospf priority** *priority*
Description	priority Used to specify the priority of the interface, the larger the value, the higher the priority, the default is 1。

DR（Designated Router）：Specifies the router。

BDR（Designated Router）：Backup of the specified router。

In the OSPF network, only DR devices announce the link status of the network, and all other devices maintain neighbors, but all devices only neighbors to DR / BDR except DR, i. e., devices with DR / BDR only interact, DR is calculated and then notified to other devices, OSPF protocol uses this mechanism to ensure that the link status data of all devices in the network is consistent。

The DR is elected through the interface priority comparison. The equipment with the highest priority will be elected as the DR equipment, and the equipment with the priority set to 0 is the equipment that waives the election qualification. OSPF neighbors who did not receive DR for a certain period of time will think that DR is down to re-launch a new round of DR election, which is the only condition for DR election. Device dynamic modification priorities will not take effect immediately, only when a new round of elections is triggered。

13.2.3. **Protocol Control Configuration**

- Configure the hello message interval

Command	(Routing)(config-if)#**ip ospf hello-interval** *seconds*
Description	Hello-interval is used to set the sending interval of hello messages on the interface, and the values at both ends of the neighbors need to be the same。

- Configure the dead determination interval

Command	(Routing)(config-if)#**ip ospf dead-interval** *seconds*
Description	dead-interval seconds Use to set the time interval on the interface to determine the death of the neighbor, and the values of the two ends of the neighbor need to be the same

- Close mtu calibration

Command	(Routing)(config-if)#**ip ospf mtu-ignore**
Description	The mtu-ignore sets the MTU check to close the OSPF. The OSPF protocol will verify the MTU of the neighbor interface when receiving the database description message. If the MTU of the interface indicated in the receiving database description message is greater than the MTU of the receiving interface, the adjacency relationship cannot be established. At this time, in addition to modifying the mtu value, this configuration can also be used to turn off the mtu verification to solve the problem。

- LSA issuance is prohibited

Command	(Routing)(config-if)#**ip ospf database-filter all out**
Description	The mtu-ignore sets the MTU check to close the OSPF. The OSPF protocol will verify the MTU of the neighbor interface when receiving the database description message. If the MTU of the interface indicated in the receiving database description message is greater than the MTU of the receiving interface, the adjacency relationship cannot be

	established. At this time, in addition to modifying the mtu value, this configuration can also be used to turn off the mtu verification to solve the problem。

- Configure the lsu message sending delay

The Age field in the Lsu message containing the LSAs (link status description) is incremented before the LSU message is sent. When Age reaches 3600, the lsu message will be retransmitted or request retransmitted. If it is not refreshed in time, the timeout LSA will be deleted from the link status database. For low-speed lines, due to the large delay of the interface transmission and line propagation. At this time, the lsu message transmission delay should be increased, and the increasing step of the Age field should be added to trigger the retransmission。

Command	(Routing)(config-if)#**ip ospf tramsmit-delay** *seconds*
Description	transmit-Day is used to set the delay of lsu message on the interface in seconds。

- Configure the lsu message retransmission interval

After the device sends a lsu message, the lsu message may not be delivered or receive the confirmation reply from the other party due to various reasons. At this time, it is necessary to retransmit the lsu message and set the time of retransmission by setting the retransmission interval of the lsu message。

Command	(Routing)(config-if)#**ip ospf retransmit-interval** *seconds*
Description	retransmit-interval used to set the retransmission time interval of lsu packets on the interface in seconds. The time required is greater than the delay of round-trip packet transmission between neighbors。

- Configure the SPF refresh delay

Command	(Routing)(config-router)#**timers spf** *spf-holdtime*
Description	The spf-delay represents the time delay required from the network topology change to the SPF starting the calculation, which is used to set the sensitivity of the SPF calculation for sensing the network topology change。

	spf-holdtime Indicates the minimum time interval between the first triggered SPF calculation and the second triggered SPF calculation。

If the link oscillation is only occasional, the spf-delay value configuration is small to accelerate the OSPF convergence rate; the large value configuration can prevent the rapid link oscillation and the large consumption of CPU resources。

13.2.4. **Passive interface configuration**

The passive interface configuration can be used to prohibit the routing information of this device from being learned by other devices. It can be set based on the whole machine or the specified interface device. Passive interface / passive address cannot establish neighbors and interact with OSPF messages, but the routing information of passive address can be published through non-passive address and learned by the neighbors。

Command	(Routing)(config-router)#**passive-interface default** (Routing)(config-router)#**passive-interface** <slot/port> (Routing)(config-router)#**passive-interface** vlan
Description	Default indicates that all interfaces are set to a passive interface。 slot/port Indicates that all interfaces are set to a passive interface。 vlan means configuring the passive vlan。 The vlan means configuring the passive vlan。

13.2.5. **Default route release configuration**

Command	(Routing)(config-router)#**default-information originate** [always] [metric metric] [metric-type *type*]

Description	always It means that the OSPF will also unconditionally generate a default route regardless of whether there is a local default route。 metric Represents the metric value of the default route。 The metric-Type represents the type of the default route. There are two types of external routing of OSPF: external routes of type 1 have different measurements on different routing devices, and external routes of type 2 have the same measures on all routing devices。

When the default-information originate command is configured, the device automatically becomes an ASBR。

The ABR in the STUB area automatically releases the default route to the STUB area。

The ABR in the NSSA area automatically releases the default route to the NSSA area。

13.2.6. **Route rerelease configure**

Command	(Routing)(config-router)# **redistribute** {bgp | connected | rip | static} [metric *value*] [metric-type {1 | 2}] [route-map *map-name*] [subnets] [tag *value*]
Description	The ABR in the NSSA area automatically releases the default route to the NSSA area。

13.2.7. **Routing convergence configuration**

- Configure inter-regional routing convergence

Command	(Routing)(config-router)#**area area-id range** *ip-address/mask* [advertise|not-advertise]
Description	The area-id represents the routing of the converging OSPF domain id。 The ip-address and mark represent the network segment ip and mask of the converged route。

	advertise and not-advertise indicate whether the convergence route needs to be published。

This command is valid only on the ABR devices, and functions to merge multiple routes of the area into one route and then notify them to another area. Since convergence only occurs in ABR devices, the routing within the region sees specific routing information, but for other devices outside the region, only one route after the convergence. Multiple regional convergence routes can be defined simultaneously. Route convergence can streamline the routing of the entire routing field。

- Configure the external route convergence

Command	(Routing)(config-router)#**summary-address** *ip-address mask* [not-advertise|tag *tag-value*]
Description	The area-id represents the routing of the converging OSPF domain id。 The ip-address and mark represent the network segment ip and mask of the converged route。 The not-advertise indicates that the convergence route is not published and the parameter is not used to represent the release。 The tag-value represents the tag value of the route。

Other routing process issued to OSPF routing process routing notification to OSPF in the form of external link status, if the injected route is continuous address space, the AS domain convenient device routing device can notify continuous address space route into a route, which can reduce the routing scale of the routing device in the domain。

When summary-address is configured on the ABR of the NSSA domain, it converges only in the redistributed routing and LSA 7 to class 5 routing, and only in the ASBR。

The difference between summary-address and area range is that area range is a route within the OSPF domain, and summary-address is a route outside the OSPF domain。

13.2.8. **Shortest path configuration**

- Configure the orientation of the interface

There are three ways to configure the measurement of the interface out direction：

- There are three ways to configure the measurement of the interface out direction，假设接口带宽为100Mbps，We configure the reference bandwidth of 1000Mbps, and then the default cobest value of the interface is 1000 / 100=10。

Command	(Routing)(config-router)#**auto-cost reference-bandwidth** *ref-bw*
Description	ref-bw Indicates the reference bandwidth。

- The other is to configure measures directly on the interface according to elements such as link bandwidth and time delay。

Command	(Routing)(config-if)#**ip ospf cost** *cost-value*
Description	The cost-value represents the measure value。

- Configure the STUB / NSSA area default routing metric value

The default routing metric sent by the ABR device to the STUB / NSSA area is 1 default and can be specified by configuration。

Command	(Routing)(config-router)#**area** *area-id* **default-cost** *cost-value*
Description	The area-id indicates the OSPF domain id。 The cost-value represents the measure value。

- Configure the republish route default measure value

The metric value of BGP routes released by ASBR devices is 1 and the metric value is 20, which can be specified by configuration, but needs to be used with the redistribute command。

Command	(Routing)(config-router)#**default-metric** *metric-value*

Description	The cost-value represents the measure value。

- Configure the route-managed distance values

Routing management distance is the credibility of the routing source, which is a value between 0 and 255. The larger the data, the lower the credibility. OSPF will selects the route with small management distance, or high credibility when selecting routes. The OSPF management distance is 110。

Command	(Routing)(config-router)#**distance** {*distance* | ospf {intra-area distance|inter-area distance|external *distance*}}
Description	intra-area represents intra-regional routing。 inter-area representation indicates inter-regional routing。 external Represents an external routing。 external Represents an external routing。

13.3. REVEAL COMMAND

- Displays routing information

```
(Routing) #show ip route

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
        B - BGP Derived, IA - OSPF Inter Area
        E1 - OSPF External Type 1, E2 - OSPF External Type 2
        N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type
2
        P - Net Prototype
```

- Only the OSPF routing information is displayed

```
(Routing) #show ip route ospf

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
        B - BGP Derived, IA - OSPF Inter Area
        E1 - OSPF External Type 1, E2 - OSPF External Type 2
        N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
        P - Net Prototype
```

(Routing) #

- Other OSPF information

Command	function
show ip ospf	Displays the OSPF profile information
show ip ospf asbr	Displays the boundary and the boundary router information for the OSPF
show ip ospf database	Displays the boundary and the boundary router information for the OSPF
show ip ospf interface	Displays the interface-related information for the OSPF
show ip ospf neighbor	Display the neighbor information for the OSPF

14. CONFIGURE BGP

14.1. BGP SUMMARY

BGP (Border Gateway Protocol) is an external gateway protocol (Exterior Gateway Protocol, EGP) for communication between routing devices of different autonomous systems. Its main function is to exchange network accessible information between different autonomous systems (Autonomous Systems, AS) and eliminate the routing loop through the protocol itself mechanism。

BGP uses TCP protocol as the transmission protocol and guarantees the transmission reliability of BGP through the reliable transmission mechanism of TCP protocol。

Run BGP, the Router of the protocol is called BGP Speaker, established the BGP Speakers of the BGP session connection (BGP Session), between which is called the peer (BGP Peers)。

BGP Speaker There are two modes of equivalence between them: IBGP (Internal BGP) and EBGP (External BGP). IBGP refers to BGP junctions established within the same AS, and EBGP refers to BGP connections established between different AS. The role of both is in short: EBGP is to complete the exchange of routing information between different AS, and IBGP is to complete the transition of routing information within this AS。

14.2. CONFIGURING COMMANDS

14.2.1. **Create the BGP process**

Command	(Routing)(config)#**router bgp** *as-number* (Routing)(config-router)# **bgp router-id** *router-id*
Description	Create the process, and configure the unique identity。

14.2.2. **BGP address family configuration**

Command	(Routing)(config-router)#address-family ipv4 [unicast | multicast]

Description	The routing pattern of the BGP is located in the IPv4 unicast address family. For commands configured for subaddress families, configured in BGP routing mode, operates on the IPv4 unicast address family。

14.2.3. **BGP neighbor configuration**

BGP neighbors need to be configured manually, and the opposite end of the BGP speaker should be configured at the same time, so BGP neighbors are also called BGP counterparts。

- Configure the peer

Command	(Routing)(config-router)# [**no**] **neighbor** *address* **remote-as** *as-number*
Description	address Represents the address of the BGP counterpart。 The as-number indicates the as number, range 14294967295。

14.2.4. **Reflector configuration**

Full connections need to be established between all BGP Speaker in an AS, so as the number of BGP Speaker in AS increases, the connections that need to be maintained between Speaker increase accordingly, aggravating the resource consumption of Speaker. To reduce this consumption, the network can be designed using the BGP routing reflector mode。

In routing reflector use, BGP Speaker devices can be divided into client and non-client based on type. Between a routing reflector and its client (more than one). For the client of the routing reflector only connects with the reflector, no connection between the client and the client, and no connection between the client and the Speaker outside the group. Based on the above principle, the BGP routing reflector can reduce the number of connections of IBGP counterparts in AS。

Configuring a router as a reflector is by assigning it which neighbors act as the client。

The routing reflector has the following rules for routing learning：

- The route learned by the client is synchronized to other clients and other non-clients；

- Routing learned through IBGP non-clients will be synchronized to other clients。
- Routing learned through EBGP Speaker is synchronized to other clients and other non-clients;

If there are multiple routing reflectors within a group, you need to configure a group ID for the group, and if only one of this goes without configuration, the group uses the Router-id of the reflector。

- Configure the device as a routing reflector, and specify the client side

Command	(Routing)(config-router)# [**no**] **neighbor** {**address** } **route-reflector-client**
Description	address Represents the peer-like IP address。 Group-name indicates the peer group address。

- Configure the routing reflector cluster ID

Command	(Routing)(config-router)#**bgp cluster-id** *cluster-id*
Description	cluster-id represents the group ID of the routing reflector。

- Configure unroute reflection between clients

Command	(Routing)(config-router)#**no bgp client-to-client reflection**
Description	Cancel the route reflection between the clients。

14.2.5. **Routing convergence configuration**

Command	(Routing)(config-router)#**aggregate-address** *address mask* [as-set] [summary-only]
Description	The address and mask parameters represent the configured aggregate address。 The as-set parameter indicates that the AS path information for the path within the aggregate address range is retained if the parameter is configured。

	The summary-only parameter indicates that if it is configured, only the aggregated path will be notified. The default is to notify all the path information before and after the aggregation。

14.2.6. **Manage distance configuration**

Management distance is a attribute used to evaluate the credibility of routing sources. The smaller the management distance, the more preferred the routing。

Command	(Routing)(config-router)#**distance bgp** *external-distance internal-distance local-distance*
Description	The external-distance parameter represents the administrative distance of the routing learned from the EBGP counterpart。 The external-distance parameter represents the administrative distance of the routing learned from the EBGP counterpart。 The local-distance parameters represent those learned from peers but are considered to exist curated distances that can be learned from IGP to more optimal routes, and these routes are often represented by the network backdoor command。

If a route is configured as a secondary route, if both IGP and EBGP learn this route, IGP route is used preferred, but IGP learns the route will not be notified。

Command	(Routing)(config-router)#**network** *address mask* **backdoor**
Description	The address and mask parameters indicate the network segment address。 backdoor The parameter indicates that this route is the back route。

14.2.7. **Multi-path load balancing configuration**

If there are multiple paths to the unified network segment, data can be balanced forward through these multiple paths is called multi-path load balancing, which can be enabled or turned off by enabling / closing multi-path load balancing configuration. In BGP, the routing of EBGP can form multi-path load balancing with the routing of EBGP, but can not form multi-path load balancing with IBGP routing. Similarly, IBPG cannot form multi-path load balancing with EBGP routing。

- IBGP Multi-diameter load equilibrium

Command	(Routing)(config-router)#**maximum-paths ibgp** *number*
Description	number Represents the number of supported and equivalent jumps, ranging from 1 to 32。

- Loose comparison of AS-path

By default, the two routes that want to combine to form a multi-path load equilibrium needs to meet the condition that all properties of AS-path are completely equal. If you want to reduce the above harsh conditions to form a multi-path load equilibrium, it can be achieved by enabling the AS-path loose comparison. AS-path loose comparison only needs to meet the condition of the AS-path length and the alliance AS-path length under the premise of the same route multi-path。

Command	(Routing)(config-router)#**bgp bestpath as-path ignore**
Description	The command indicates that the BGP AS-path loose comparison mode is enabled

14.2.8. **Routing the redistribution configuration**

- Routing injection

Command	(Routing)(config-router)# **redistribute** { connected | isis [area-tag] | ospf process-id | rip | static} [metric value] [metric-type {1 | 2}] [route-map map-name] [subnets] [tag value]

Description	This command is used to inject external routing into the BGP process (including static routing / other routing protocols)。

- The default route is injected

Command	(Routing)(config-router)#**default-informnation originate**
Description	Use this command to inject the default route into the BGP, distributed by protocol。

14.2.9. **Protocol parameter configuration**

- Configure the neighbor-preserving timer

Command	(Routing)(config-router)#**timer bgp** *holdtime*
Description	The keepalive parameter refers to the period in which the peer remains effectively connected in seconds, ranging from 0 to 65535 with a default value of 60. The protocol sends keepalive messages to maintain the connection during the keepalive cycle。 holdtime The parameter is the period to determine whether the counterpart is valid in seconds and range from 0 to 65535 with a default value of 180. The peer connection is considered invalid if the device does not receive a keepalive message from the peer within the holdtime time。

When a BGP connection is established between the BGP Speakers, the holdtime will be negotiated, and the small holdtime will be selected as the effective configuration. The effective value of keepalive will be holdtime after the negotiation, the holdtime value based on the negotiation, and compared with the configured keepalive value, and the smaller value of both will be used as the effective configuration of keepalive。

You can also configure the keepalive and holdtime values based on the BGP counterpart (group)。

Command	(Routing)(config-router)#**neighbor** {address | group-name} times

Description	adress Represents the address of the counterpart。 The group-name indicates the name of the peer group。

- Configure the neighbor reconnection timer

When the connection to the peer fails, the reconnection period can be specified by configa reconnection timer。

Command	(Routing)(config-router)#**neighbor** {address | group-name} **timer connect** *connect-retry*
Description	adress Represents the address of the counterpart。 The group-name indicates the name of the peer group。 connect-Retry represents reconnection cycles in seconds, range 1-65535, with a default value of 15 seconds。

- Configure the routing notification timer

When the device generates routing changes locally, the updated routing notification is given to the peer body (group), and the frequency of the notification can be set by the configuration of the routing notification timer。

Command	(Routing)(config-router)#**neighbor** {address | group-name} **advertisemet-interval** *interval-time*
Description	adress Represents the address of the counterpart。 The group-name indicates the name of the peer group。

	The interval-time represents the minimum interval of sending routing updates in seconds, range 1-600 with a default of 5s for IBGP counterparts and 30s for EBGP counterparts.

14.3. REVEALCOMMAND

```
(Routing) #show ip route

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
        B - BGP Derived, IA - OSPF Inter Area
        E1 - OSPF External Type 1, E2 - OSPF External Type 2
        N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
        P - Net Prototype
```

- Only the BGP routing information is displayed

```
(Routing) #show ip route bgp

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
        B - BGP Derived, IA - OSPF Inter Area
        E1 - OSPF External Type 1, E2 - OSPF External Type 2
        N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
```

- Other BGP information

Command	作用
show ip bgp	Display the profile information for the BGP
show ip bgp summary	Displays the connection summary information for the BGP
show ip bgp neighbors	Show the neighbor details of the BGP

15. CONFIGURE RIP

15.1. RIP SUMMARY

The RIP (Routing Information Protocol) routing protocol is a routing protocol that uses the distance vector algorithm and is mainly used in small networks. RIPv 1 and RIPv 2, respectively (RIPv 1 is defined in RFC 1058 and RIPv 2 in the RFC 2453 document)。

The RIP protocol message is a UDP protocol-based message with a UDP port number of 520. RIPv 1 messages generally adopt the form of broadcast messages; RIPv 2 messages have an address of 224.0.0.9;

The RIP protocol sends the update message every 30 seconds. If the paired-end route update message is not received for 180 seconds, all the routes from the opposite device will be marked as inaccessible. After this state, the routes notified by the paired-end device will be deleted from the routing table after 120 seconds。

The routing measure of RIP refers to the number of jumps used to measure the distance to the destination. The number of jumps on the direct network is marked as 0, and the number of network jumps on each device is 1; the number of jumps on the inaccessible network is 16。

The RIP routing process will only send update packets to the network interface associated with the process。

15.2. CONFIGURING COMMANDS

15.2.1. **Create the RIP process**

Command	(Routing)(config)#router rip
Description	To run the RIP routing protocol, you need to first create the RIP routing process and associate the corresponding network with the RIP routing process。 The router rip command is for creating a RIP routing process。

	network The command represents the routing information of the associated network notified by the ride command, and also updates the protocol notification and the routing information only on the corresponding interface of the associated network。 The IP and the MASK together constitute the address range。

15.2.2. **Configure the RIP version**

Product supports versions 1 and 2 of RIP. Version 2 supports authentication, routing and aggregation, and key management。

By default the product can receive RIP packets for versions 1 and 2, but only for version 1。

The product supports packets based on the RIP version received and sent by the machine or port designation。

The product supports packets based on the RIP version received and sent by the machine or port designation：

Command	(Routing)(config-if)# ip rip send version {1|2} {1|2}
Description	The product supports packets based on the RIP version received and sent by the machine or port designation。

Specifies the received RIP version based on the port：

Command	(Routing)(config-if)# ip rip receive version {1|2} {1|2}
Description	Specifies the received RIP version based on the port。

15.2.3. **Route the republish configuration**

Command	(Routing)(config-router)# redistribute {bgp | connected [area-tag] | ospf process-id | rip | static} [metric value] [metric-type {1 | 2}] [route-map map-name] [subnets] [tag value]
Description	This command is used to configure an external routing to the OSPF process (including other processes / static routing / other routing protocols)。

15.2.4. **Configure routing convergence**

When the subnetwork routing passes through the network boundary of the like routing, the subnetwork routing can be converged into the like network routing, which can improve the scalability and effectiveness of the network, that is, the subrouting included in the converged route can not be seen in the routing table, so that the routing table can greatly reduce the scale of the routing table. Version 2 of RIP automatically routes aggregation by default and is not supported in version 1。

Command	(Routing)(config)#router rip (Routing)(config-router)#[no] auto-summary
Description	The auto-summary indicates that the open route is automatically converged。 The no keyword indicates that the closed route is automatically converged。

15.2.5. **Configure horizontal segmentation**

Distance vector routing protocols due to their own mechanism cause frequent routing loops when multiple devices are connected to an IP broadcast type network. The horizontal segmentation mechanism is used to avoid the formation of a routing loop。

The horizontal segmentation mechanism optimizes the routing information exchange between multiple devices by preventing some routing information from learning the interface to the routing information. However, this mechanism cannot learn complete routing information for non-broadcast multi-access network (frame-relay network, X.25) because the notification is blocked, so it is not suitable for horizontal segmentation.

Toxicity reversal is an improved mechanism of horizontal segmentation technology, open the horizontal division of toxicity reversal, the device learned the interface for routing information will still notify the routing information, but will set the measurement properties in the routing information to inaccessible, so that the opposite after receiving such routing information, will immediately abandon the route, without waiting for the aging time, accelerate the convergence of the route。

The horizontal segmentation is configured in the global mode。

Command	(Routing)(config)#[no] ip rip split-horizon {poisoned-reverse}
Description	The split-horizon keyword represents the horizontal segmentation of the open rip。 The poisoned-reverse keyword represents a reversal of the toxicity profile。

15.2.6. **Configure the default route notifications**

You can produce a default route in the route update message based on the interface. You can also specify routes that only pass this default route without notifying others。

Command	(Routing)(config-if)#ip rip default-information {originate | only} [metric metric-value] (Routing)(config)#default-information originate
Description	originate Keyword indicates that in addition to the default route。 originate Keyword indicates that in addition to the default route。

Note: Between the default-information configured in the RIP process and the ip rip default-information configured under the interface, the interface configuration is more priority than the RIP process configuration, i. e. the default route configured under the interface is notified if both exist。

15.3. REVEALCOMMAND

- Displays routing information

```
(Routing) #show ip route

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
```

```
        B - BGP Derived, IA - OSPF Inter Area
        E1 - OSPF External Type 1, E2 - OSPF External Type 2
        N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
        P - Net Prototype
```

- Only the RIP routing information is displayed

```
(Routing) #show ip route rip

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
        B - BGP Derived, IA - OSPF Inter Area
        E1 - OSPF External Type 1, E2 - OSPF External Type 2
        N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
        P - Net Prototype
```

- Other RIP information

Command	作用
show ip rip	Display of the RIP database
show ip rip interface	Display the relevant interface information for the RIP

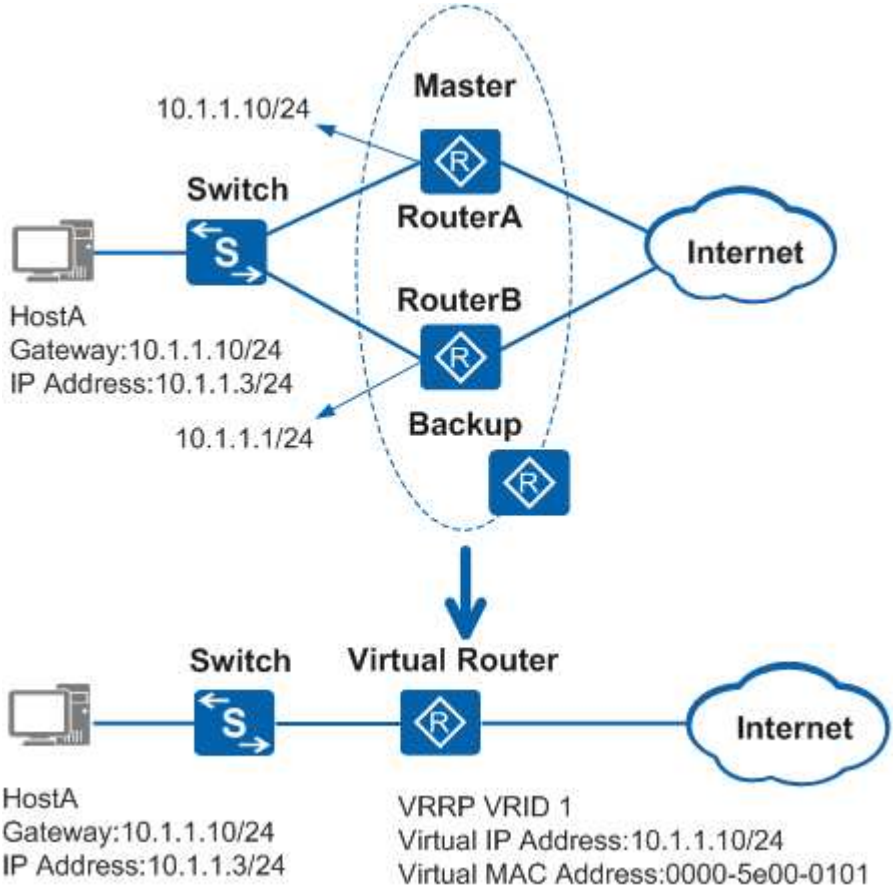
16. CONFIGURE VRRP

16.1. AGREEMENT OVERVIEW

Virtual routing redundancy protocol VRRP (Virtual Router Redundancy Protocol) combines several routing devices to form a virtual routing device, and implements the IP address of the virtual routing device as the user's default gateway. When the gateway equipment fails, the VRRP mechanism can elect the new gateway equipment to undertake the data traffic, thus ensuring the reliable communication of the network。

This device only supports the VRRPv2 function。

Networking topology



Terms defined

- VRRP Router (VRRP Router): A device running the VRRP protocol that may belong to one or more virtual routers, such as RouterA and RouterB。
- Virtual router (Virtual Router): Also known as the VRRP backup group, it consists of one Master device and multiple Backup devices, and is used as a default gateway for the host within the shared LAN. Such as RouterA and RouterB together form a virtual router。
- Master Router (Virtual Router Master): VRRP devices responsible for forwarding messages, such as RouterA。
- Backup Router (Virtual Router Backup): A group of VRRP devices that do not undertake the forwarding task, when the Master device fails, they will become the new Master devices, such as RouterB。
- VRID: Identification of the virtual router. A virtual router such as RouterA and RouterB has a VRID of 1。
- Virtual IP Address (Virtual IP Address): The IP address of a virtual router, a virtual router can have one or more IP addresses, configured by the user. The virtual IP address of a virtual router such as RouterA and RouterB is 10.1.1.10/24。
- IP Address Owner (IP Address Owner): If a VRRP device takes the virtual router IP address as the real interface address, the device is called the IP address owner. If the IP address owner is available, usually it will become the Master. For example, RouterA, the IP address of its interface is the same as the IP address of the virtual router, both are 10.1.1.10/24, so it is the IP address owner of this VRRP backup group.
- Virtual MAC Address (Virtual MAC Address): The MAC address generated by the virtual router according to the virtual router ID. A virtual router has a virtual MAC address in the format: 00-00-5E-00-01- {VRID} (VRRP for IPv4); 00-00-5E-00-02- {VRID} (VRRP for IPv6). When the virtual router responds to an ARP request, use the virtual MAC address instead of the real MAC address of the interface. A virtual router such as RouterA and RouterB has a VRID of 1, so the MAC address of this VRRP backup group is 00-00-5E-00-01-01。

16.2. CONFIGURING COMMANDS

- Create / delete a VRRP group

Command	(Routing)(config)# **ip vrrp** (Routing)(config)#**no ip vrrp**

Description	Global configuration mode。 Create / delete a VRRP group。

- Associated VRRP interface

Command	(Routing)(inteface0/1)#ip vrrp 1 (Routing)(inteface0/1)#ip vrrp 1 accept-mod
Description	The VRRP group configuration mode。 Configure / delete the triple port associated with the VRRP group. Support SVI ports, such as vlan 1; no level II ports, such as gigabitEthernet0 / 1 not configured as level III ports。

- Configure / delete the VRRP virtual address

Command	(Routing)(Interface 0/1)#ip vrrp 1 ip A.B.C.D
Description	The VRRP group configuration mode。 Virtual address is the virtual router gateway address。 Configas the master role must ensure that the virtual IP is a group-associated interface IP。

- Configure / delete the VRRP priorities

Command	(Routing)(Interface 0/1)#**ip vrrp 1 priority <1-254>** (Routing)(Interface 0/1)#no **ip vrrp 1 priority <1-254>**

Description	Configure / delete the VRRP priorities。 Priority 0 is reserved by the system for a special use; the priority value 255 is reserved for the IP address owner。 By default, the value of the backup router priority is 100. A larger value indicates a higher priority。

- Configure / reset the VRRP group notification interval

Command	(Routing)(Interface 0/1)#**ip vrrp 1 timers advertise <1-255>** (Routing)(config-vrrp)#**no ip vrrp 1 timers advertise**
Description	The VRRP group configuration mode。 Optional configuration in seconds, with the default to 1。

- Configure / delete the preemption mode

Command	(Routing)(config-vrrp)#ip vrrp 1 preempt (Routing)(config-vrrp)#no ip vrrp 1 preempt
Description	The VRRP group configuration mode。 Optional configuration, with preemption enabled by default。

- Configuring authentication functions

Command	(Routing) (Interface 0/1)#ip vrrp 1 authentication simple

Description	The VRRP group configuration mode。 Optional configuration, with the default authentication-free mode。 VRRPv1 Supports authentication free mode, simple key authentication mode and md 5 authentication mode, but does not improve security; VRRPv2 compatible v1 compatible authentication mode; VRRPv3 cancels the security field。 Devices is not recommended to configure authentication functions。

16.3. REVEALCOMMAND

- Displays the vrrp group information

```
#show vrrp
  ---------------- VRRP 1 ----------------
  ID:                    1
  State:                 Master (Enabled)
  Virtual IP:            2.2.1.1/24 (Not IP owner)
  Last Master:           2.2.1.3 (63510s ago)
  Interface:             vlan100
  Priority:              100 (conf.-1)
  Advertisement interval: 1 sec
  Preempt mode:          TRUE
  Authentication:        none
  ---------------- VRRP 2 ----------------
  ID:                    2
  State:                 Backup (Enabled)
  Virtual IP:            2.2.2.1/24 (Not IP owner)
  Last Master:           2.2.2.3 (0s ago)
  Interface:             vlan200
  Priority:              90 (conf.90)
  Advertisement interval: 1 sec
  Preempt mode:          TRUE
  Authentication:        none
```

17. CONFIGURE ACL

17.1. ACL SUMMARY

ACL (Access Control List, Access Control List) implements the function of packet filtering by configmatching rules and processing operations for packets. It can effectively prevent illegal users to access the network, but also can control the traffic, save network resources。

Packet matching rules defined by the ACL can also be referenced by other functions that need to distinguish traffic, such as the definition of flow classification rules in QoS。

ACL classifies packets by a series of matching conditions, which can be SMAC, DAC, MAC, SIP, DIP, etc. According to the matching conditions, the ACL can be divided into the following categories：

Standard ACL based on IP：Rule is only based on the source IP address of the packet。

Extension of the ACL based on IP：Rule based on packet source IP address, destination IP address, ETYPE, protocol.

The MAC-based ACL：Rule based on the source MAC address and the destination MAC address of the packet。

Named ACL：The rules are the same as IP based standard ACL and extended ACL。

17.2. CONFIGURING COMMANDS

- Configure an IP-based standard ACL

Command	(Routing)(config)#**ip-access-list** {<1-99>} {**permit** | **deny**} {every | **any**} (Routing)(config)#**no ip-access-list** {<1-99>} {**permit** | **deny**} {every | **any**}
Description	Create / remove standard IP-based ACLs

- Configure the IP-based extension ACL

Command	(Routing)(config)# **ip-access-list** {<100-199> |} {**permit** | **deny**} {TYPE} {SIPADDR SIPADDRMASK | **any**} {DIPADDR DIPADDRMASK | **any**} (Routing)(config)#**no ip-access-list** {<100-199> } {**permit** | **deny**} TYPE {SIPADDR SIPADDRMASK | **any**} {DIPADDR DIPADDRMASK | **any**} (Routing)(config)# **no ip-access-list** {<100-199> }
Description	Create / delete an IP-based extended ACL TYPE tabulation: <0-255>: Specifies the ID of the protocol any: Any protocol message gre: GRE message IGMP: IGMP message IP: IPv4 message ipcomp: IPComp message ospf: OSPF message pim: PIM message rsvp: RSVP message tcp: TCP message

	udp：UDP　message vrrp：VRRP　message

- Configure a MAC-based ACL

Command	(Routing)(config)#mac access-list extended h (Routing)(config)#permit any any (Routing)(config)#**no** mac access-list extended h
Description	Create / delete MAC-based ALs

- Configure the ACL to apply on the port

Command	(Routing)(config-if)#mac access-group h in 1 (Routing)(config-if)#**no** mac access-group h in 1
Description	Configure / remove the ACL application on the port

---

Instructions

✦ If ACL is already applied on the port, you need to add the deletion rule to remove it from the port;

17.3. REVEALCOMMAND

- show ACL

```
Routing) #show access-lists interface 0/1 in

ACL Type              ACL ID               Sequence Number
--------  ------------------------------  ---------------


(Routing) #
```

18. CONFIGURE QOS

18.1. QOS SUMMARY

QoS (Quality of Service, quality of Service) means that a network can utilize a variety of basic technologies to provide better service capabilities for the designated network communication。

The traditional network adopts the forwarding mechanism of "doing your best". When the network bandwidth is abundant, all the data streams are well processed, and when the network congestion occurs, all the data streams may be discarded. In order to meet the requirements of different service quality for different applications, the network needs to allocate and schedule resources according to the requirements of users, and provide different service quality for different data streams。

Support QoS function of equipment, can provide transport quality service, for a certain category of data flow, can give it a certain level of transport priority, to identify its relative importance, and use the equipment provided by various priority forwarding strategy, congestion avoidance mechanism to provide special transport services for these data flow。

The network environment configured with QoS increases the predictability of network performance, and can effectively allocate network bandwidth and use network resources more reasonably。

18.2. CONFIGURE COMMAND

- Turn the QOS on / off globally

Command	(Routing)(config)#`classofservice dot1p-mapping` *userpriority trafficclass* (Routing)(config)#`no classofservice ip-dscp-mapping` (Routing)(config)#`no classofservice ip-dscp-mapping` (Routing)(config)#`classofservice trust {dot1p | ip-dscp | untrusted}`

(Routing)(config)#no classofservice trust

(Routing)(config)#cos-queue min-bandwidth *bw-0 bw-1 … bw-n*

(Routing)(config)#no cos-queue min-bandwidth

(Routing)(config)#cos-queue random-detect *queue-id-1* [*queue-id-2 … queue-id-n*]

(Routing)(config)#no cos-queue random-detect *queue-id-1* [*queue-id-2 … queue-id-n*]

(Routing)(config)#cos-queue strict *queue-id-1* [*queue-id-2 … queue-id-n*]

(Routing)(config)#no cos-queue strict *queue-id-1* [*queue-id-2 … queue-id-n*]

Description	Turn the QOS functions on and off globally Default closed

Command	(Routing)(config-pmap-c)#**police cir** <32-1000000> **cbs** <4-31250> **exceed-action drop** (Routing)(config-pmap-c)#**no police**
Description	Configure the policy / delete policy Cir is the speed-limiting waterline in a unit of kbps Cbs are burst abilities, in Kbyte

---

Instructions

✦ The cir value is certain, like if the speed limit is 1M, then the cir value is 1024, but the cbs value is taken from the empirical value. When the cbs value is large, the flow spike is higher and the rate limit is stable, but the average rate may be higher than the rate limit value; when the cbs value is small, the flow spike is lower and the rate limit fluctuation is large, the average rate may be smaller than the rate limit value. It is suggested that the cbs configuration takes the 4 times value of cir with a small value of 31250。

- Configure the policy-map to apply on the interface

Command	(Routing)(config-if)#**service-policy input** PNAME (Routing)(config-if)#**no service-policy input**
Description	Configuring / removing the application of the policies on the interface Only one policy-map can be applied on one interface

- Configure the port inlet speed limit

Command	(Routing)(config-if)#**rate-limit input** <64-1000000> <32-16384> (Routing)(config-if)#**no rate-limit input**
Description	Configure / delete the port entry speed limit The first parameter is limit, in kbps The second parameter is the burst, in Kbyte

- Configure the port access speed limit

Command	(Routing)(config-if)#**rate-limit output** <64-1000000> <32-16384> (Routing)(config-if)#**no service-policy output**

Description	Configure / delete the port exit speed limit The first parameter is limit, in kbps The second parameter is the burst, in Kbyte

Instructions

✦ The limit value is definite, like if the speed limit is 1M, then the limit value is 1024, but the burst value is taken from the empirical value. When the burst value is large, the flow peak is higher and the rate limit is stable, but the average rate may be higher than the rate limit value; when the burst value is small, the flow peak is lower and the rate limit fluctuation is large, the average rate may be less than the rate limit value. The recommended burst configuration takes the 4 times value of limit with the small value of 16384。

18.3. REVEALCOMMAND

- Display the cos-map configuration information

```
show interfaces cos-queue [unit/slot/port]
```

- Displays the port configuration information

```
show classofservice ip-precedence-mapping [unit/slot/port]

show classofservice trust [unit/slot/port]
```

- Displays the class-map configuration information

```
show classofservice dot1p-mapping [unit/slot/port]
```

- Displays the policy-map configuration information

```
show classofservice ip-dscp-mapping
```

- Display the port speed limit configuration information

```
(Routing)#show rate-limit
-------------------------------------------------------
Interface     In limit  In burst  Out limit  Out burst
-------------------------------------------------------
GiE0/1        --        --        --         --
GiE0/2        --        --        --         --
GiE0/3        1024      4096      --         --
GiE0/4        --        --        --         --
GiE0/5        --        --        --         --
GiE0/6        --        --        --         --
GiE0/7        --        --        --         --
GiE0/8        --        --        --         --
GiE0/9        --        --        --         --
GiE0/10       --        --        1024       4096
```

19. CONFIGURE DHCP SNOOPING

19.1. DHCP SNOOPING SUMMARY

DHCP (Dynamic Host Configuration Protocol, Dynamic Host Configuration Protocol) is a LAN network protocol that is widely used to dynamically allocate reusable network resources. It is a means for users or internal network administrators to centralize all computers。

DHCP Snooping Is a DHCP security technology, through the detection and management of DHCP interactive messages, to realize the isolation function of illegal DHCP Server. DHCP Snooping The ports are divided into two types, the TRUST port and the UNTRUST port. The device only forwards the DHCP Offer messages received by the TRUST port, and discards all the DHCP Offer messages from the UNTRUST port, so as to realize the blocking of illegal DHCP Server。

19.2. CONFIGURING COMMANDS

- Global on / off of the DHCP Snooping

Command	(Routing)(config)**#ip dhcp snooping** (Routing)(config)**#no ip dhcp snooping**
Description	Turn the DHCP Snooping functions on and off globally

- configure 信任口

Command	OLT(config-if)**#ip dhcp snooping trust** OLT(config-if)**#no ip dhcp snooping trust**
Description	Set the port to the TRUST / UNTRUST port

19.3. REVEALCOMMAND

- Displays the DHCP Snooping configuration information

```
(Routing) #show ip dhcp snooping
```

```
DHCP snooping is Disabled
DHCP snooping source MAC verification is enabled
DHCP snooping is enabled on the following VLANs:


 Interface    Trusted     Log Invalid Pkts
-----------  ----------   ----------------


(Routing) #
```

20. CONFIGURE THE 802.1X AUTHENTICATION

20.1. AGREEMENT OVERVIEW

The IEEE802 LAN / WAN committee proposed the 802.1X protocol to solve the problem of wireless LAN network security. Later, 802.1X protocol was widely used as a common access control mechanism for LAN network port, mainly solving the problems of authentication and security in Ethernet。

The 802.1X protocol is a port-based network access control protocol (port based network access control protocol)."Port-based network access control" means that the access to the network resources is controlled by authentication at the level of the port of the LAN access device。

20.1.1. **The architecture of the 802.1X**

802.1X The system is a typical Client / Server structure, as shown in Figure 1 1, including three entities: client (Client), device end (Device), and authentication server (Server)。

Figure 1 1 . Architecture of the 802.1X authentication system

- A client is an entity located at one end of the LAN segment and is authenticated by the device end at the other end of the link. The client is generally a user terminal device, and the user can initiate 802.1X authentication by launching the client software. The client must support EAPOL (Extensible Authentication Protocol over LAN, a scalable authentication protocol on the LAN)。
- The device side is another entity located at one end of the LAN segment that authenticates the connected client. The device side is usually a network device that supports the 802.1X protocol, which provides the client with a port for access to the LAN, which can be either a physical port or a logical port.
- The authentication server is an entity that provides the authentication services on the device side. The authentication server is used to implement the authentication, authorization and billing of users, usually the RADIUS (Remote Authentication Dial-In User Service, remote authentication dial-up user service) server。

20.1.2. **802.1X Certification method**

802.1X The authentication system uses EAP (Extensible Authentication Protocol, extensible authentication protocol) to realize the exchange of authentication information between the client side, the device side and the authentication server。

- Between the client side and the device side, the EAP protocol message uses the EAPOL package format, directly hosted in the LAN environment。
- There are two ways to exchange information between the device side and the RADIUS server. One is that the EAP protocol message is relayed by the device side, Carted in the RADIUS protocol using the EAPOR (EAP over RADIUS) package format; The other is the EAP protocol message by the device end, With including PAP (Password Authentication Protocol, Password verification protocol) or CHAP (Challenge Handshake Authentication Protocal, Query handshake verification protocol) The message of the attribute interacts with the RADIUS server。

20.1.3. **The basic concept of the 802.1X**

20.1.3.1. Controlled / Uncontrolled ports

The device side provides ports for clients to access the LAN, which is divided into two logical ports: controlled and uncontrolled ports. Any frame that reaches that port is visible on both the controlled and non-controlled ports。

- Ununcontrolled ports are always bidirectional connected to deliver EAPOL protocol frames, ensure that the client is always able to issue or receive authentication messages。
- The controlled port is in two-way connectivity under authorized state to deliver business messages; receiving any messages from the client without unauthorized state。

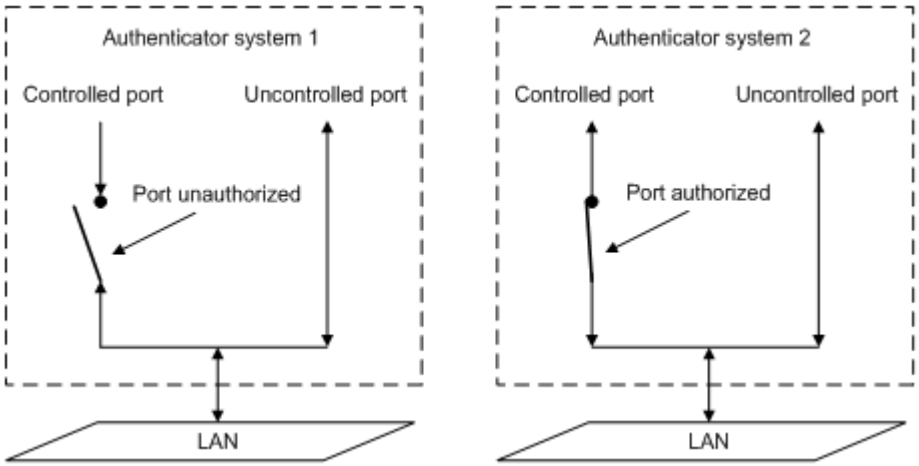
20.1.3.2. Authorized / unauthorized status

The device side uses the authentication server for the client needing to access the LAN, and controls the authorized / unauthorized status of the controlled port according to the authentication results (Accept or Reject)。

Figure 1 2 shows the effect of different authorization states on the controlled port on messages passing through that port. The port status of the two 802.1X authentication systems are compared in Fig. The

controlled port of system 1 is in unauthorized state (equivalent to port switch on) and the controlled port of system 2 is in authorized state (equivalent to port switch off)。

Figure 1 2 Effect of authorization status on the controlled port



The user can control the authorization status of the port through the mode of access control configured under the port. The port supports the following three access control modes：

- Compulsory authorization mode (authorized-force): The port is always in the authorization state, allowing users to access network resources without authentication authorization。
- Compulsory unauthorized mode (unauthorized-force): The port is always unauthorized and the user is not allowed to authenticate. The device side does not provide authentication services to the clients accessed through the port。
- Automatic identification mode (auto): the initial state of the port is unauthorized, which only allows EAPOL messages and does not allow the user to access the network resources; if the authentication passes, the port switches to the authorized state and allows the user to access the network resources. This is also the most common case。

20.1.3.3. Controlled direction

Without authorization, the controlled port can be set to be unidirectional and bidirectional controlled。

- Send and receive frames when prohibited controlled control bidirectional controlled；
- When controlled, do not receive frames from the client, but allow sending frames to the client。

20.1.4. **802.1X The certification process**

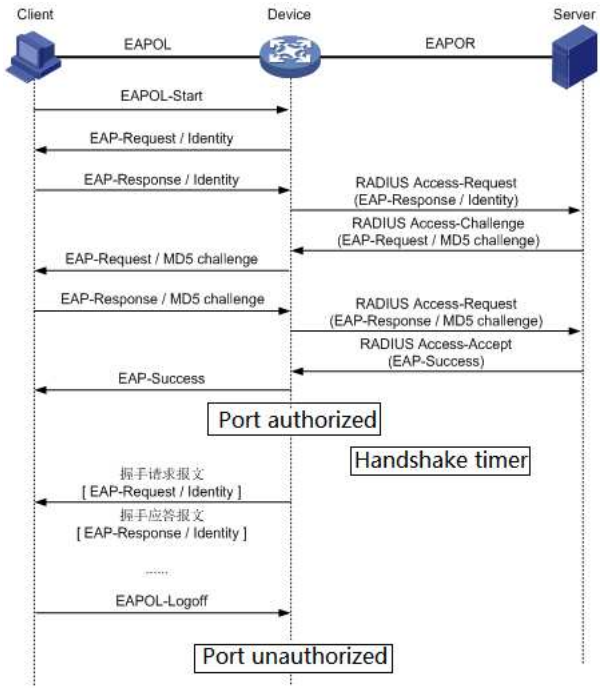
802.1X The system supports EAP relay mode and EAP end mode interaction with the remote RADIUS server to complete the authentication. The following process description of the two authentication methods takes the client-initiated authentication as an example。

20.1.4.1. The EAP relay mode

This approach is defined by the IEEE 802.1X standard for hosting the EAP (Extensible authentication Protocol) in other high-level protocols, such as the EAP over RADIUS, to extend the authentication protocol message across a complex network to the authentication server. Generally speaking, the EAP relay mode requires the RADIUS server to support EAP attributes: EAP-Message and Message-Authenticator, which are used to package EAP messages and protect RADIUS packets carrying EAP-Message respectively。

The EAP-MD5 method is used as an example to introduce the basic business process, as shown in Figure 1 3。

Figure 1 3 . EAP relay business process of IEEE 802.1X authentication system



The certification process is as follows：

1) Open the 802.1X client program when the user needs to access the network, enter the requested and registered user name and password, and initiate the connection request (EAPOL-Start message). At this point, the client program will send the message requesting authentication to the device to start the authentication process。
2) After receiving the data frame requesting authentication, a request frame (EAP-Request / Identity message) asks the user's client program to send the input user name。
3) In response to the device side request, the client program sends the user name information to the device side through the data frame (EAP-Response / Identity message). The device terminal sends the data frame sent by the client after packet processing (RADIUS Access-Request message) to the authentication server for processing。
4) RADIUS After receiving the forward the user name information of the device, compare the information with the user name table in the database, find the password information corresponding to the user name, with a randomly generated encrypted word to encrypt it, but also the encrypted word sent to the device through the RADIUS Access-Challenge message, forwarded to the client program by the device。
5) After the client program receives the encrypted word (EAP-Request / MD5 Challenge message) from the device side, then the encrypted word is used to encrypt the password part (the encryption algorithm is usually irreversible) to generate the EAP-Response / MD5 Challenge message and transmit it to the authentication server through the device side。
6) RADIUS The server will compare the encrypted password information received (RADIUS Access-Request message) with the local password information after encrypted operation. If the same, the user is considered a legitimate user and feedback the verified message (RADIUS Access-Accept message and EAP-Success message)。
7) Device receiving the authentication message changes the port to authorization status, allowing the user to access the network through the port. During this period, the device side will monitor the user's online situation by sending regular handshake messages to the client. In default, the two handshake request messages cannot be answered by the client, and the device side will let the user offline, to prevent the user from not perceiving the device due to abnormal reasons。
8) The client can also send EAPOL-Logoff message to the device and request to go offline. The device side changes the port status from authorized to unauthorized status and sends an EAP-Failure message to the client。

20.2. CONFIGURING COMMANDS

- Global 802.1X authentication on / off

Command	(Routing)(config)# **dot1x system-auth-control** (Routing)(config)#**no dot1x system-auth-control**
Description	Turn the 802.1X function on and off globally。

- Port on / off for 802.1X authentication

Command	(Routing)(config-if)# **dot1x port-control force-unauthorized** (Routing)(config-if)#**no dot1x port-control force-unauthorized** (Routing)(config-if)#**dot1x port-control force-authorized** (Routing)(config-if)#**no dot1x port-control force-authorized** (Routing)(config-if)#**dot1x port-control auto** (Routing)(config-if)#**no dot1x port-control auto**
Description	Port turn on and turn the 802.1X function off。

- Configure the RADIUS server

Command	(Routing)(config)# **radius-server host** A.B.C.D **auth-port** <0-65535> **acct-port** <0-65535> **key** WORD (Routing)(config)# aaa authentication dot1x default radius

	(Routing)(config)# radius server host auth "192.168.10.1" name "rad" (Routing)(config)# radius server key auth "192.168.10.1" encrypted e9dc904557361f19ac7716c3bd5429f1e2d061dea16e5d46c3cf45a54d523a470c792e7 a504198810a118cb67a633236be8ccd8fa8191f762791f53dc3ceeb45 (Routing)(config)# radius server primary "192.168.10.1" (Routing)(config)#**no radius-server** primary A.B.C.D
Description	Configure the authentication server information。 The default authentication port is 1812 and the billing port is 1813。 Ensure sure the RADIUS server and device management addresses communicate。

20.3. REVEALCOMMAND

- Displays the 802.1X port authentication information

```
(Routing) #show dot1x

Administrative Mode.............. Disabled
VLAN Assignment Mode............. Disabled
Dynamic VLAN Creation Mode........ Disabled
Monitor Mode..................... Disabled
EAPOL Flood Mode................. Disabled
```

21. CONFIGURE PORT SECURITY

21.1. PORT SECURITYFUNCTIONAL OVERVIEW

Port Security The function limits the number of legitimate MAC addresses to achieve the purpose of limiting illegal users' access to the port. Non-legal MAC messages will be discarded。

The legal MAC can be generated either static or dynamic. The static legitimate MAC is generated by the user command line configuration; the dynamic legitimate MAC is dynamically generated through the MAC address learning function。

When the number of security addresses on the port has reached the maximum configuration value of the number of security addresses, the new MAC access port will be identified as illegal MAC, generating violation events. Users can configure the response operation of violation events, restrict or shutdown port respectively。

Restrict: No illegal MAC data pass and generate alarm log message. The illegal MAC will prohibit access to the port during the MAC address aging time. It can be restored through the shutdown, no shutdown ports。

Shutdown: Force the port down drop, and can configure the port recovery time, time to the port to automatically recover; also through shutdown, no shutdown command recovery。

If you want to convert a dynamic security user to a static security user, you can open the sticky function on the port. When the port opens the sticky function, the dynamic users learned on the port will exist in the way of a static user. If the configuration is saved, the device will still exist after the restart。

Restriction instructions

- Only support L2 port configuration port security, such as normal physical port, AP port。
- Only support to configure port security in access mode。
- AP member port security is not supported。
- Target port configuration port security feature for SPAN is not supported。
- Port security feature with configured static MAC address ports is not supported。

21.2. CONFIGURING COMMANDS

- Global mode turns on port security

Command	(Routing)(config)#**port-security** (Routing)(config)#**no port-security**
Description	Enable / close the port security function on the interface

-

- Enabling port security feature

Command	(Routing)(config-if)#**port-security** (Routing)(config-if)#**no port-security**
Description	Enable / close the port security function on the interface

- Configure the maximum number of port security addresses

Command	(Routing)(config-if)#**port-security max-dynamic** VALUE (Routing)(config-if)#**no port-security max-dynamic**
Description	The default maximum number of secure addresses is 1 Range <1 1024>

- Configure the static security address

Command	(Routing)(config-if)#**port-security max-static** MAC_ADDR

	(Routing)(config-if)#**no port-security max-static** MAC_ADDR
Description	Security address format: XX: XX: XX: XX: XX: XX The Security address cannot be a broadcast or a multicast address

21.3. REVEALCOMMAND

In privileged mode, you can view port security configuration information, security address information and so on。

- Displays all port port security profiles

```
(Routing) #show port-security all

          Admin    Dynamic     Static    Violation  Violation  Sticky
 Intf     Mode       Limit      Limit     Trap Mode  Shutdown   Mode
-------  -------- ----------  ---------  ---------- ---------- --------
0/1      Disabled 600         20         Disabled   Disabled   Disabled
0/2      Disabled 600         20         Disabled   Disabled   Disabled
0/3      Enabled  600         20         Disabled   Disabled   Disabled
0/4      Disabled 600         20         Disabled   Disabled   Disabled
0/5      Disabled 600         20         Disabled   Disabled   Disabled
0/6      Disabled 600         20         Disabled   Disabled   Disabled
0/7      Disabled 600         20         Disabled   Disabled   Disabled
0/8      Disabled 600         20         Disabled   Disabled   Disabled
0/9      Disabled 600         20         Disabled   Disabled   Disabled
0/10     Disabled 600         20         Disabled   Disabled   Disabled
0/11     Disabled 600         20         Disabled   Disabled   Disabled
0/12     Disabled 600         20         Disabled   Disabled   Disabled
1/1      Disabled 600         20         Disabled   Disabled   Disabled
1/2      Disabled 600         20         Disabled   Disabled   Disabled
1/3      Disabled 600         20         Disabled   Disabled   Disabled
1/4      Disabled 600         20         Disabled   Disabled   Disabled
1/5      Disabled 600         20         Disabled   Disabled   Disabled
1/6      Disabled 600         20         Disabled   Disabled   Disabled
1/7      Disabled 600         20         Disabled   Disabled   Disabled
1/8      Disabled 600         20         Disabled   Disabled   Disabled
```

22. CONFIGURE IP SOURCE GUARD

22.1. IP SOURCE GUARDFUNCTIONAL OVERVIEW

Ip Source Guard Binding function allows IP messages conforming to IP + MAC binding to pass through the port, while non-conforming messages are directly discarded, so as to achieve the purpose of preventing IP / MAC deception attacks。

Ip Source Guard Binding entries have two main sources: user static configuration and dynamic acquisition in the ip dhcp snooping environment。

User Static configuration: the host users with IP address static configuration in the local area network。

Ip dhcp snooping Dynamic acquisition: the IP address in the local area network。

IP / MAC deception attack: illegal MAC users, send IP messages with legal source IP, to realize the legalization of access identity。

Restriction instructions

- The current software version only supports the static configuration。
- The AP member port configuration Ip Source Guard feature is not supported。

22.2. CONFIGURING COMMANDS

- Enable the Ip Source Guard function

Command	(Routing)(config-if)**#ip verify source** (Routing)(config-if)**#no ip verify source**

Description	Enable / close the Ip Source Guard function on the interface

- Configure the binding table key

Command	(Routing)(config)# **ip verify binding** xx:xx:xx:xx:xx:xx vlan 1 A.B.C.D **interface 0/1** (Routing)(config)**#no ip verify binding** xx:xx:xx:xx:xx:xx vlan 1 A.B.C.D **interface 0/1**
Description	Security address format: xx: xx: xx: xx: xx: xx Security address format: xx: xx: xx: xx: xx: xx Up to 128 table entries are configured for a single port

22.3. REVEALCOMMAND

In privilege mode, you can view the ip verify source effective rule and ip source binding binding items。

- In privilege mode, you can view the ip verify source effective rule and ip source binding binding items

```
(Routing) #show ip source binding dhcp-snooping

MAC Address           IP Address          Type                VLAN    Interface
----------------  --------------  -------------  -----  -------------
```

- Revealip source binding 表项

```
(Routing) #show ip source binding
interface   vlan   IP-address        Mac-address      Lease      Type
-----------------------------------------------------------------------------------------------
GiE0/1        1        1.1.1.1             0001.0001.0001 infinite      static
GiE0/2        1        1.1.2.1             0001.0002.0001 infinite      static
```

23. CONFIGURING SNMP NETWORK MANAGEMENT

23.1. SUMMARIZE

SNMP is the abbreviation for Simple Network Management Protocol (Simple Network Management Protocol), which became a network management standard RFC1157 in August 1988. So far, due to the support of many manufacturers to this agreement, SNMP has become a de facto network management standard, suitable for use in the interconnection environment of multi-manufacturer systems。

Using SNMP protocol, network administrators can make information query, network configuration, fault location and capacity planning for nodes on the network, and network monitoring and management are the basic functions of SNMP。

The following versions of the SNMP currently exist：

SNMPv1 ： The first formal version of the simple network management protocol, defined in RFC1157。

SNMPv2C： Community-based (Community-Based) SNMPv2, management architecture, defined in RFC1901。

SNMPv3 ： The following security features are provided by identifying and encryption the data：

1) Ensure that the data is not tampered with during the transmission process。
2) Ensure that the data is sent from a legitimate data source。
3) Encrypt the packets to ensure the confidentiality of the data。

23.2. CONFIGURECOMMAND

- Configure the communication community character

Command	(Routing)(config)#**snmp-server enable Global opening** (Routing)(config)#**snmp-server community** COMMUNITY **{ro** | **rw}**

	(Routing)(config)#**no snmp-server community** COMMUNITY
Description	Configure / delete the SNMP communication community word; **ro**: Read-only identity, configure group characters to group words with only read permission; default to group characters with both read and write permission; Support configure multiple community characters simultaneously

- Configure the SNMPv3 view

Command	(Routing)(config)# **snmp-server view** NAME OID **{include** | **exclude}** (Routing)(config)# **no snmp-server view** NAME
Description	Configure / delete the SNMPv3 view; It ports simultaneous configuration of multiple views, and a single view; The system has all and none views by default and is not modifiable

- Configure the SNMP group

Command	(Routing)(config)# **snmp-server group** NAME **{v3** | **} {noAuthNoPriv** | **authNoPriv** | **authPriv} read** RVIEW **write** WVIEW (Routing)(config)# **snmp-server group** NAME **{v1** | **v2c} read** RVIEW **write** WVIEW (Routing)(config)# **no snmp-server group** NAME
Description	Configure / delete the SNMP groups; Support for the simultaneous configuration of multiple groups;

	SNMPv1 SNMPv2c When configure community to be compatible with old configurations, group information is automatically created, usually without additional attention

- Configure the SNMPv3 user

Command	(Routing)(config)# **snmp-server user** NAME GROUPNAME **auth {md5** | **sha}** {AUTHPASS} **priv {aes** | **des}** PRIVPASS (Routing)(config)# **no snmp-server user** NAME
Description	Configure / delete the SNMP users; Supports configuring multiple users simultaneously;

- Configure the SNMP Host notification server

Command	(Routing)(config)# **snmp-server host** IPADDR **informs** community (Routing)(config)# **no snmp-server host** NAME
Description	Configure / delete the SNMP server; Supports the configuration of multiple servers simultaneously;

24. CONFIGURE RMON

24.1. SUMMARIZE

SNMP is the most widely used network management protocol in the Internet network, which realizes the collection and statistics of network communication information through the agent software embedded in the device. The management software sends out the query signal to the agent's MIB by polling mode to get this information, and realizes the management of the network through the obtained information. Although the MIB counter records the sum of statistics, it does a historical analysis of daily communication. In order to comprehensively view the flow of the day and the changes of the flow, the network management software needs to constantly poll, in order to analyze the situation of the network through the information obtained。

Using SNMP for polling has two obvious disadvantages：

- It occupies a large number of network resources. In a large network, a large number of network communication messages will be generated by means of polling, which will lead to network congestion or even cause network congestion. Therefore, SNMP is not suitable for managing large networks, and is not suitable for recovering a large amount of data, such as routing table information。
- It increases the burden of the manager. The task of collecting data in SNMP polling is completed by the network manager through the network management software. If the network manager monitors more than 3 network segments, the network manager may be unable to complete the task due to the heavy burden。

In order to improve the availability of management information, reduce the burden of management stations, and meet the needs of network administrators to monitor the performance of multiple network segments, IETF developed RMON to solve the limitations of SNMP in the expanding distributed interconnection, mainly realizing the monitoring function of monitoring the data flow of a network segment and even the whole network. Here are the characteristics of the RMON：

- SNMP is the basis of RMON implementation and RMON is an enhancement of SNMP functionality。

RMON is based on SNMP architecture and is compatible with existing SNMP framework. It is still composed of NMS and agent Agent running on each network equipment. Since RMON does not use another set of mechanisms, the network management workstation NMS and SNMP share, the network managers do not need to conduct additional learning, so the implementation is relatively simple。

- RMON enables SNMP to monitor remote network devices more effectively and actively, providing an efficient means for monitoring the operation of the network。

The RMON protocol stipulates that the managed device can automatically send Trap information when the alarm threshold is reached, so the management device does not need to obtain the value of MIB variables through multiple polling for comparison, so as to reduce the communication flow between the managed device and the managed device and achieve the simple and effective management of large interconnection network。

The RMON allows for multiple monitors, who can collect data in the following two methods：

- Through a dedicated RMON Probe (detector), NMS directly obtains management information from RMON Probe and controls network resources, which obtains all the information of RMON MIB。
- Embedding RMON Agent directly into network devices, making them network devices with RMON Probe capabilities. NMS uses SNMP to exchange data information with it and collect network management information. This method is limited by device resources, so it is generally impossible to obtain all the data of RMON MIB, and basically only collects information from four groups (alarm, events, history and statistics)。

Our device adopts the second method to implement the RMON Agent function on the device. Through this function, the management device can obtain the overall traffic, error statistics and performance statistics on the network segment connected to the managed network equipment interface, and then realize the monitoring of the network。

24.2. PRINCIPLE

Before configure RMON, you need to understand the basic concepts of the four groups of statistics, history, alarms, and events defined by the RMON specification。

RMON characteristic

RMON mainly realizes the statistics and alarm functions, which are used for the remote monitoring and management of the managed equipment in the network。

The statistical function of RMON can be realized through the RMON statistical group or the RMON history group, which is divided into the Ethernet statistical function and the historical statistical function。

- Ethernet statistics function (corresponding to statistics groups in RMON MIB): System statistics of the basic statistics of each network monitored. The system will continue to statistics a network segment of traffic and the distribution of various types of package, or various types of error frames, collisions, statistical objects including network conflict number, CRC check error message number, too small (or large) data messages, broadcast, multicast message number and receive bytes, receive messages, etc。
- Historical statistics function (corresponding to historical groups in RMON MIB): the system regularly samples and collects network status statistics and stores them for subsequent processing. The system will make statistics of various flow information according to the cycle, including bandwidth utilization, error packets and total packets, etc。

The RMON alarm function includes the event definition function and sets the alarm threshold function. The combination of these two sub-functions realizes the RMON alarm function。

- Event Definition function (corresponding to event groups in RMON MIB): Event groups control events and prompts from the device, providing all the events generated by the RMON Agent. When an event occurs, you can log or send Trap to the network station。
- Set the alarm threshold function (corresponding to the alarm group in RMON MIB): the system monitors the specified alarm variable (the OID corresponding to any alarm object). After the user defines a set of thresholds and sampling time for the specified alarm, the system will obtain the value of the specified alarm variable according to the defined time period. When the value of the alarm variable is greater than or equal to the upper threshold value, a lower limit alarm event is triggered. RMON Agent The above monitored status will be recorded as a log or Trap sent to the network management station。

Multiple RMON groups are defined in the RMON specification (RFC2819), and the device implements four groups of statistics, history, alarms, and events supported in the public MIB. The several groups are introduced separately below。

- Statistical group

The statistics group stipulates that the system will continuously count the various traffic information of the Ethernet interface and store the statistical results in the Ethernet Statistical table (etherStatsTable) for the management equipment to view at any time. Statistical information includes the number of network conflicts, number of CRC verification error messages, number of data packets too small (or too large), number of broadcasts and multicast packets, number of bytes received, number of messages received, etc。

After the statistical table item has been successfully created under the specified interface, the statistical group counts the number of packets in the current interface, and the statistical result is a continuous cumulative value。

- History group

The history group periodically collects network status statistics and stores them for subsequent processing。

The history group contains two tables：

  - Historical control table (historyControlTable): mainly used to set the sampling interval time and other control information。
  - Ethernet History Table (etherHistoryTable): It is mainly used to store history groups to regularly collect network status statistics, and provide network administrators with historical data about network segment traffic, error packets, broadcast packets, utilization, and collision number and other statistics。
- Event group

Event group-defined events are used in the alarm group configuration item and the extended alarm group configuration item, which are triggered when the monitoring object reaches the alarm condition. RMON Event Management adds events to the specified row of the event table and defines how the events are handled：

  - log：Send only logs
  - trap：Send Trap messages to NMS
  - log-trap：Send both logs and send Trap messages to the NMS
  - none：Do not do any processing
- The alarm group

An alarm group allows a set of thresholds for alarm variables (which can be any object of the local MIB). After the user defines the alarm table item (alarmTable), the system will obtain the value of the monitored alarm variable according to the defined time period. When the alarm variable is greater than or equal to the upper threshold, the alarm is triggered when the upper alarm variable is less than or equal to the lower threshold, the alarm is triggered by the alarm management according to the definition of the event。

24.3. CONFIGURING COMMANDS

- Configure the history group

Command	(Routing)(config)# **rmon hcalarm** <1-65535> **interface** IFNAME **buckets** <1-65535> **interval** <1-3600> **{owner** OWNERNAME **|}** (Routing)(config-if)#**no rmon history** <1-65535>
Description	Configure / delete the history group; <1-65535>: Group index IFNAME： The interface name <1-65535>： The size of the historical bucket <1-3600>： Record period; in seconds OWNERNAME： Owner's information

- Configure event groups

Command	(Routing)(config)# **rmon event** <1-65535> **{description** DESCRIPTION **|} {log** | **trap** COMMUNITY | **log-trap** COMMUNITY | **none} {owner** OWNERNAME **|}** (Routing)(config-if)#**no rmon event** <1-65535>

Description	Configure / delete event groups; <1-65535>: Group index DESCRIPTION: Event description COMMUNITY: Trap Communication group word OWNERNAME: Owner's information

- Configure the alarm group

Command	(Routing)(config)# **rmon alarm** <1-65535> **object** STRING <1-65535> **{absolute | delta} rising-threshold** <1-2147483645> <1-65535> **falling-threshold** <1-2147483645> <1-65535> **{owner** OWNERNAME **|}** (Routing)(config-if)#**no rmon alarm** <1-65535>
Description	Configure / delete the alarm group; <1-65535>: Group index STRING: OID for alarm monitoring; say 1.3.6.1.2.1.2.2.1.10.1 indicates the number of bytes received by the monitoring interface 1 <1-65535>: Monitoring period; in seconds <1-2147483645>: Rising threshold <1-65535>: Rising event index; the index in the corresponding event group <1-2147483645>: Depth threshold <1-65535>: Drop event index; the index in the corresponding event group

	OWNERNAME：Owner's information

24.4. REVEALCOMMAND

- Display the event group log

```
(Routing) #show rmon ?

alarm                    Show RMON alarm entries.
alarms                   Display the alarm table.
collection               Displays the configured requested group of
statistics.
events                   Displays the RMON event table.
hcalarm                  Show RMON high capacity alarm entries
hcalarms                 Displays the high capacity alarm table.
history                  Displays the RMON history ethernet statistics.
log                      Display the RMON logging table.
statistics               Display RMON ethernet statistics.
```

25. CONFIGURE THE DHCP SERVER

25.1. AGREEMENT OVERVIEW

DHCP (Dynamic Host Configuration Protocol, Dynamic Host Settings Protocol) is a LAN network protocol that works with the UDP protocol and is widely used to dynamically allocate reusable network resources, such as IP addresses。

DHCP is based on the Client / Server working mode, and the DHCP client obtains the IP address to the DHCP server by sending request messages, and other configuration information. When the DHCP client and the server are not on the same subnet, there must be a DHCP relay agent (DHCP Relay) to forward DHCP requests and reply messages。

25.1.1. **Protocol standard**

RFC2132 DHCP Options and BOOTP Vendor Extensions. S. Alexander, R. Droms. March 1997. (Format: TXT, HTML) (Obsoletes RFC1533) (Updated by RFC3442, RFC3942, RFC4361, RFC4833, RFC5494) (Status: DRAFT STANDARD) (DOI: 10.17487/RFC2132)

25.2. CONFIGURECOMMAND

25.2.1. **Global Configuration Command**

- Turn on / off the DHCP server globally

Command	(Routing)(config)# **service dhcp** (Routing)(config)#**no service dhcp**

Description	Global to open and close the DHCP server。

- Configure global parameters

Command	(Routing)(config)# **ip dhcp pool** NAME (Routing)(config)# lease infinite (Routing)(config)#network A.B.C.D mask (Routing)(config)#dns-server A.B.C.D (Routing)(config)#default-router A.B.C.D (Routing)(config)#ip dhcp excluded-address A.B.C.D A.B.C.D
Description	Global parameter configuration. When parameter values conflict, the global parameter is prioritized lower than the parameters of the subnetwork and address pool with more precise ranges。 Default lease time：43200s/12h Optional configuration。

25.3. ASSIGN THE COMMAND

- Displays the DHCP server status information

```
show ip dhcp server statistics
```

26. FAULT DIAGNOSIS

26.1. PING/TRACEROUT

- Perform the ping function

Command	(Routing)**#ping {ip** IPADDR | **ipv6** IPV6ADDR**}**
Description	Execute the ping command

- Perform the traceroute functions

Command	(Routing)# **traceroute {ip** IPADDR | **ipv6** IPV6ADDR **}**
Description	Execute the traceroute command