

SICOM3028GPT Series Industrial Ethernet Switches

CLI Operation Manual

Publication date: September 2016

Version This: V1.0

KYLAND

Disclaimer

Kyland Technology Co., Ltd. has made every effort to keep the information in this manual as accurate and up-to-date as possible. However, the company cannot guarantee that this manual is completely free of any technical errors or clerical errors, and reserves the right to modify it without notifying the user.

All permissions reserved

The copyright of this manual belongs to Kyland Technology Co., Ltd. Without the written permission of the copyright owner, no unit or individual may extract, reproduce, reproduce, translate or distribute for commercial purposes in any way.

Infringement must be investigated.

Copyright © 2016 Kyland Technology Co., Ltd.

Published by: Kyland Technology Co., Ltd.

<http://www.kyland.ru>

Customer Service Hotline: +7 (499) 969-81-21, +7 (495) 723-81-21

Email: support@kyland.ru

Content

Content.....	1
1 Product Description	1
1.1 Overview	1
1.2 Software Features	1
2 Access To The Switch	3
2.1 Introduction To Configuration Mode	3
2.2 Hot Key	4
2.3 Help Function	4
2.4 Support For Incomplete Matches	5
2.5 Console Port Access	5
2.6 Telnet Access.....	10
2.7 Web Access	11
3 Acl Configuration	13
3.1 Introduce	13
3.2 Acl Entries And Rules	13
3.3 Cli Configuration.....	14
3.3.1 Acl.....	14
3.3.2 Acl Acl_Id Apply.....	15
3.3.3 Apply	16
3.3.4 Description.....	17
3.3.5 Rule	17
3.3.6 Show Acl.....	18
3.3.7 Show This.....	19
3.4 Typical Configuration Example.....	20
4 Cable Diagnostics.....	21
4.1 Introduce	21
4.2 Accomplish.....	21

4.3 Cli Configuration.....21

 4.3.1 Cable-Test22

 4.3.2 Show Cable-Test22

5 Alert24

 5.1 Introduce24

 5.2 Cli Configuration.....24

 5.2.1 Alarm Address-Conflict-Detect.....24

6 Goose-Over-Ip-Tunnel.....25

 6.1 Introduce25

 6.2 Goose Tunnel.....25

 6.3 Work Process26

 6.4 Cli Configuration.....29

 6.4.1 Interface Tunnel.....30

 6.4.2 Mode.....30

 6.4.3 Destination.....31

 6.4.4 Source31

 6.4.5 Goose Default-Forward-Policy.....31

 6.4.6 Goose Forward-Policy32

 6.4.7 Goose Tunnel-Binding.....32

 6.4.8 Goose Vlan-Remark33

 6.4.9 Goose Static33

 6.4.10 Show Interface Tunnel.....34

 6.4.11 Show Goose Static34

 6.4.12 Show Goose Tunnel-Binding35

 6.4.13 Show Goose Vlan-Remark36

 6.5 Typical Configuration Example.....37

7 Basic Switch Configuration40

 7.1 Basic Configuration40

7.1.1 Clock Set	41
7.1.2 Config	41
7.1.3 Enable	41
7.1.4 Exec Timeout.....	42
7.1.5 Exit.....	42
7.1.6 Help	42
7.1.7 Ip Host	43
7.1.8 Hostname	43
7.1.9 Reboot.....	43
7.1.10 Set Default.....	44
7.1.11 Language.....	44
7.1.12 Save	44
7.2 Maintenance And Debugging Commands.....	45
7.2.1 Ping	47
7.2.2 Telnet.....	47
7.2.3 Traceroute	49
7.2.4 Show Clock.....	50
7.2.5 Show Debugging	50
7.2.6 Show Flash.....	50
7.2.7 Show History.....	51
7.2.8 Show Memory-Info.....	51
7.2.9 Show Running-Config.....	51
7.2.10 Show Startup-Config.....	52
7.2.11 Show Switchport Interface	52
7.2.12 Show Tcp.....	52
7.2.13 Show Udp	53
7.2.14 Show Version.....	53
7.3 Ip Address Configuration.....	53

7.3.1 Ip Address.....	54
7.3.2 Ip Bootp-Client Enable.....	54
7.3.3 Ip Dhcp-Client Enable.....	55
7.4 Snmp Configuration	55
7.4.1 Introduction To Snmp	55
7.4.2 Introduction To Mib	57
7.4.3 Introduction To Rmon	58
7.4.4 Cli Configuration	59
7.4.5 Typical Configuration Example	64
7.5 Switch Upgrade.....	65
7.5.1 Bootrom Mode	65
7.5.2 Ftp/Tftp Upgrade.....	69
7.6 Lldp Configuration	82
7.6.1 Introduce.....	82
7.6.2 Cli Configuration	82
7.6.3 Typical Configuration Example	84
8 Port Configuration.....	86
8.1 Introduce	86
8.2 Ethernet Port Cli Configuration.....	86
8.2.1 Bandwidth	87
8.2.2 Flow Control.....	88
8.2.3 Interface Ethernet	88
8.2.4 Loop-Detect	89
8.2.5 Mdi.....	89
8.2.6 Name	90
8.2.7 Rate-Suppression	90
8.2.8 Shutdown.....	91
8.2.9 Speed-Duplex	91

8.2.10 Clear Counters Ethernet	92
8.2.11 Show Interface Ethernet	92
8.3 Vlan Interface Cli Configuration.....	93
8.3.1 Interface Vlan.....	93
8.3.2 Ip Address.....	93
8.3.3 Shutdown.....	94
8.4 Port Mirroring Cli Configuration	94
8.4.1 Monitor Session Source Interface.....	95
8.4.2 Monitor Session Destination Interface	95
8.4.3 Show Monitor.....	96
8.5 Typical Configuration Example.....	96
9 Mac Address Table Configuration	98
9.1 Introduce	98
9.1.1 Obtaining The Mac Address Table	98
9.1.2 Forward Or Filter.....	100
9.2 Cli Configuration.....	101
9.2.1 Mac-Address-Table Aging-Time	102
9.2.2 Mac-Address-Table	102
9.3 Typical Configuration Example.....	103
10 Vlan Configuration	105
10.1 Introduce	105
10.2 Cli Configuration.....	106
10.2.1 Vlan	107
10.2.2 Name	107
10.2.3 Switchport Access Vlan	108
10.2.4 Switchport Interface	108
10.2.5 Switchport Mode.....	108
10.2.6 Switchport Trunk Allowed Vlan	109

10.2.7 Switchport Trunk Native Vlan.....	109
10.2.8 Vlan Ingress Disable.....	110
10.2.9 Vlan Aware	110
10.2.10 Vlan Unaware	110
10.2.11 Show Vlan.....	110
10.2.12 Show Vlan Brief	111
10.2.13 Show Vlan Summary	111
10.3 Typical Configuration Example.....	111
11 Igmp Snooping Configuration	114
11.1 Introduction To Igmp Snooping	114
11.2 Cli Configuration.....	114
11.2.1 Ip Igmp Snooping.....	116
11.2.2 Ip Igmp Snooping Vlan	116
11.2.3 Ip Igmp Snooping Vlan Mroute	116
11.2.4 Ip Igmp Snooping Vlan Static.....	117
11.2.5 Ip Igmp Snooping Vlan Query.....	117
11.2.6 Ip Igmp Snooping Vlan Query Robustness.....	118
11.2.7 Ip Igmp Snooping Vlan Query Interval	118
11.2.8 Ip Igmp Snooping Vlan Query Max-Response-Time.....	118
11.2.9 Ip Igmp Snooping Vlan Address	119
11.2.10 Show Ip Igmp Snooping.....	119
11.2.11 Show Mac-Address-Table Multicast	119
11.2.12 Debug Ip Igmp Snooping	120
11.3 Typical Configuration Example.....	120
12 Port Channel Configuration	124
12.1 Introduce	124
12.2 Cli Configuration.....	126
12.2.1 Port-Group.....	126

12.2.2 Port-Group Load-Balance	126
12.2.3 Interface Port-Channel.....	127
12.2.4 Show Port-Group	127
12.2.5 Debug Lacp	127
12.3 Typical Configuration Example.....	128
13 L3 Forwarding Configuration	132
13.1 Introduce	132
13.1.1 Layer 3 Interface Introduction	132
13.1.2 Introduction To Ip Forwarding	133
13.1.3 Introduction To Arp	133
13.2 Cli Configuration.....	133
13.2.1 Interface Vlan.....	134
13.2.2 Ip Fib Optimize.....	135
13.2.3 Show Ip Traffic.....	135
13.2.4 Debug Ip Packet	137
13.2.5 Arp	137
13.2.6 Ip Proxy-Arp.....	138
13.2.7 Clear Arp.....	138
13.2.8 Show Arp	138
13.2.9 Debug Arp.....	140
14 Layer 3 Routing Configuration	141
14.1 Routing Table.....	142
14.2 Static Routing.....	143
14.2.1 Introduction To Static Routing.....	143
14.2.2 Introduction To Default Routing	144
14.2.3 Cli Configuration	144
14.2.4 Typical Configuration Example	145
14.3 Rip.....	146

14.3.1 Introduction To Rip	146
14.3.2 Cli Configuration	149
14.3.3 Typical Configuration Example	161
14.4 Ospf	164
14.4.1 Introduction To Ospf	164
14.4.2 Cli Configuration	168
14.4.3 Typical Configuration Example	182
15 Ntp Configuration.....	193
15.1 Introduce	193
15.2 Cli Configuration.....	194
15.2.1 Sntp Enable	195
15.2.2 Sntp Server.....	195
15.2.3 Sntp Polltime.....	195
15.2.4 Sntp Timezone.....	196
15.2.5 Show Sntp	196
15.2.6 Debug Sntp.....	196
15.3 Typical Configuration Example.....	196
16 Dt-Ring Protocol Family Configuration.....	198
16.1 Dt-Ring	198
16.1.1 Introduce.....	198
16.1.2 CLI Configuration	200
16.2 Dt-Ring+	203
16.2.1 Introduce.....	203
16.2.2 CLI Configuration.....	204
16.3 Dt-Vlan	207
16.3.1 Introduce.....	207
16.3.2 CLI Configuration.....	209

Preamble

This series of products includes Layer 2 switches SICOM3028GPT-L2GT, SICOM3028GPT-L2FT, SICOM3028GPT-L2G, SICOM3028GPT-L2F and Layer 3 switches SICOM3028GPT-L3GT, SICOM3028GPT-L3FT, SICOM3028GPT-L3G, SICOM3028GPT-L3F.

This manual mainly introduces the access methods and software features of this series of industrial Ethernet switches, and introduces the configuration and use methods of this series of switches in detail through the CLI.

Content organization

This manual mainly introduces the following contents:

module	Feature Description
1. Product introduction	<ul style="list-style-type: none"> ➤ Overview ➤ Software features
2. Switch access mode	<ul style="list-style-type: none"> ➤ Introduction to Configuration Mode ➤ hot key ➤ Help function ➤ Support for incomplete matches ➤ Console port access ➤ Telnet access ➤ web access
3. ACL configuration	
4. Cable diagnosis	
5. Alarm	IP/MAC address conflict alarm
6. GOOSE-over-IP-Tunnel	
7. Basic configuration of the switch	<ul style="list-style-type: none"> ➤ basic configuration ➤ Maintenance and debugging commands ➤ IP address configuration ➤ SNMP configuration ➤ Switch upgrade ➤ LLDP configuration
8. Port configuration	<ul style="list-style-type: none"> ➤ Ethernet port configuration ➤ VLAN interface configuration ➤ Port mirroring configuration
9. MAC address table	

configuration	
10. VLAN configuration	
11. IGMP Snooping configuration	
12. Port Channel configuration	
13. L3 forwarding configuration	<ul style="list-style-type: none"> ➤ Layer 3 interface ➤ IP forwarding ➤ ARP
14. Layer 3 routing configuration	<ul style="list-style-type: none"> ➤ static routing ➤ RIP ➤ OSPF
15. NTP configuration	
16. DT-Ring	<ul style="list-style-type: none"> ➤ DT-Ring ➤ DT-Ring+ ➤ DT-VLAN

Conventions in this manual

1. Command line format convention




Format	illustrate
bold	Command keywords (the part of the command that remains unchanged and must be typed), in bold
<i>italic</i>	Command parameters (the part of the command that must be replaced by the actual value), in italics
[]	The content in "[]" indicates that the command configuration is optional
{x y ...}	Indicates to choose one of two or more options
[x y ...]	Indicates one or no choice from two or more options
<x y ...>	Indicates to choose one or more of two or more options
//	Behavior comment lines starting with "//"

2. Text format conventions

Format	illustrate
< >	The content in "< >" represents the button name, such as "Click the <Apply> button".
[]	The content in "[]" represents the window name and menu name, such as clicking the "[File]" menu item.

{ }	The content in "{ }" indicates a combination, for example, "{IP address, MAC address}" indicates that the IP address and the MAC address are a combination, which can be configured and displayed together.
→	Multi-level menus are separated by "→", for example, "Start→Programs→Accessories" means the [Accessories] menu item under the [Programs] submenu under the [Start] menu.
/	Choose one from two or more and separate them with "/", for example, "plus/minus" means adding or subtracting.
~	Indicates the range, such as "1~255" to indicate the range from 1 to 255.

3. Sign convention

logo		illustrate
	Notice	It reminds the matters that should be paid attention to in operation and configuration, and supplements the description of operation content.
	illustrate	Provide necessary explanations for the operation contents.
	warn	Special attention should be paid to the place where incorrect operation may result in data loss or equipment damage.

Product supporting information

The supporting materials of SICOM3028GPT series industrial Ethernet switches include the following:

Data name	Introduction
SICOM3028GPT Series Industrial Ethernet Switch Hardware Installation Manual	Learn more about SICOM3028GPT series product appearance structure, hardware specifications and installation and disassembly methods
SICOM3028GPT Series Industrial Ethernet Switches Web Operation Manual	Understand the switch software functions and master the Web page configuration method and configuration steps of each functional module
SICOM3028GPT Series Industrial Ethernet Switch CLI Operation Manual	Understand the switch software functions and master the CLI configuration method and configuration steps of each functional module

How to get data

Users can obtain product-related manuals in time from the following two ways:

- Obtained through random CD-ROM and random printed manual;
- Obtained through the website of Kyland Company;

1 Product description

1.1 Overview

This series of switches is mainly used in the smart grid industry. Based on the all-gigabit switching platform, it is the first time in the world to use IEC61850 MMS modeling management technology for industrial Ethernet switch products, which realizes the unified management of IEC61850 modeling; at the same time, it adopts advanced clock frequency Synthesis technology, supports IEEE1588-2008 precise clock synchronization protocol, supports IEC62439-6 ring network redundancy protocol, all adopt modular design, expandable B code module, GPS module, serial port module, HSR module and other configurations are flexible. Compliant with IEC61850-3, IEEE1613 standard power industry standards, superior performance can meet the application of smart grid industry.

1.2 Software features

This series of switches has rich software features to meet the different needs of customers.

- Redundancy protocols: STP/RSTP, MSTP, DT-Ring, VRRP and IEC62439-6;
- Routing protocol: OSPFv2, static routing protocol;
- Multicast protocols: IGMP Snooping, GMRP and static multicast;
- Switching attributes: VLAN, PVLAN, QoS, ARP;
- Bandwidth management: port aggregation, port speed limit, broadcast storm suppression;
- Synchronization protocols: GPS, IRIG-B, PTP (IEEE1588-2008), ITU-TG8261/G.8262, SNTP and NTP;
- Security management: IEEE802.1x, TACACS+, RADIUS, SSH, SSL, MAC address binding, port isolation, user management;
- Device management: FTP/TFTP software upgrade, FTP/TFTP file

transfer, log record and upload;

- Device diagnosis: port mirroring, LLDP, link status detection;
- Alarm function: port alarm, power alarm, ring alarm, high temperature alarm and low temperature alarm and abnormal port traffic alarm;
- Network management: support CLI, Telnet, Web, Kyvision network management software management, DHCP and SNMPv1/v2/v3, IEC61850 network monitoring;
- ...

2 access to the switch

The following methods are supported to access the switch:

- Console port access;
- Telnet/SSH access;
- Web browser access;
- Kyvision management software access;

Kyvision is a network management software developed by Kyland Company, please refer to the relevant user manual for usage.

2.1 Introduction to Configuration Mode

When logging in to the CLI (Command Line Interface) through the Console port and Telnet, you can enter different views or switch between different views through different commands, such as shown on Table 1;

Table 1 Various view types

view display	view type	View function	view switch
SWITCH>	General User Configuration Mode	Configure the CLI interface locale; View system date and time; View software version information; View interface information	"enable" to enter privileged user configuration mode
SWITCH#	Privileged User Configuration Mode	Configure the system clock and date; Transfer files/upgrade software; Delete files in the switch; View switch configuration and system information; restore default configuration; save the current configuration; reboot the switch	"config" enters global configuration mode from privileged user configuration mode; "exit" returns to normal user configuration mode
SWITCH(config)#	Global configuration mode	Configure the function modules of the switch	"exit" returns to privileged user configuration mode



Notice:

In the privileged user configuration mode (SWITCH#), you can enter the global configuration mode (SWITCH(config)#) to configure and modify the switch. Therefore, when entering the privileged user configuration mode (SWITCH#), a privileged user password is set to prevent the illegal use of non-privileged users and malicious modification of the switch configuration, resulting in unnecessary losses.

2.2 hot key

For the convenience of user configuration, this series of switches provides multiple shortcut key operations, as shown.

Table 2 Shortcut operation

button	Features
Delete key "Backspace"	Delete the previous character at the cursor position, move the cursor forward
up cursor key "↑"	Display the last input command
down cursor key "↓"	Display the next input command
left cursor key "←"	Move the cursor one position to the left
Right cursor key "→"	Move the cursor one position to the right
Ctrl+z	Fall back directly to privileged user configuration mode from other configuration modes (except SWITCH>)
Tab key	When the input string can represent a command or keyword without conflict, you can use the Tab key to supplement it into a complete command or keyword

2.3 Help function

When configuring the switch using the CLI, users can obtain help information in the following two ways:

Table 3 Help function

input the command	How to use and function
Help	In any command mode, enter the "help" command to get information about all the commands in that command mode and their brief descriptions
?	In any command mode, enter the "?" command to get all the commands in that command

	mode and their brief descriptions
	Enter a space-separated "?" after a command keyword or parameter. If the position is a parameter, the description of the parameter type, range, etc. will be output; if the position is a keyword, the set of keywords and their brief descriptions will be listed. ;If the output is "<cr>", it means that the command has been input completely, you can directly type Enter
	Type "?" immediately after a string to list all commands that begin with that string

2.4 Support for incomplete matches

This series of switches supports search commands and keywords that do not match exactly, and input commands or keywords without conflict can be correctly parsed. For example: for the configuration command "show interface ethernet 1/1" in privileged user mode, just enter "sh in e 1/1".

2.5 Console port access

You can use the HyperTerminal of Windows system or other software that supports serial connection, such as HTT3.3, to access the switch through the Console port. The following uses HyperTerminal as an example to introduce how to access the switch through the console port.



Notice:

The console port of this series of devices has two types of connectors: RJ45 connector and Mini USB connector. Users can choose one of them according to their needs. If two kinds of connectors are connected at the same time, the Console port of the Mini USB connector will work, and the Console port of the RJ45 connector will stop working.

Choose RJ45 connector

1. Use the DB9-RJ45 cable to connect the 9-pin serial port of the PC and the Console port of the switch;

Choose Mini-USB connector

1. Install the Mini USB serial driver Mini USB driver.exe, see the [Software Download] folder on the CD, and use the Mini USB cable to connect the USB port of the PC and the Console port of the switch;

2. Open HyperTerminal from the Windows desktop, [Start]→[All Programs]→[Accessories]→[Communications]→[HyperTerminal], for example as shown on Picture 1;



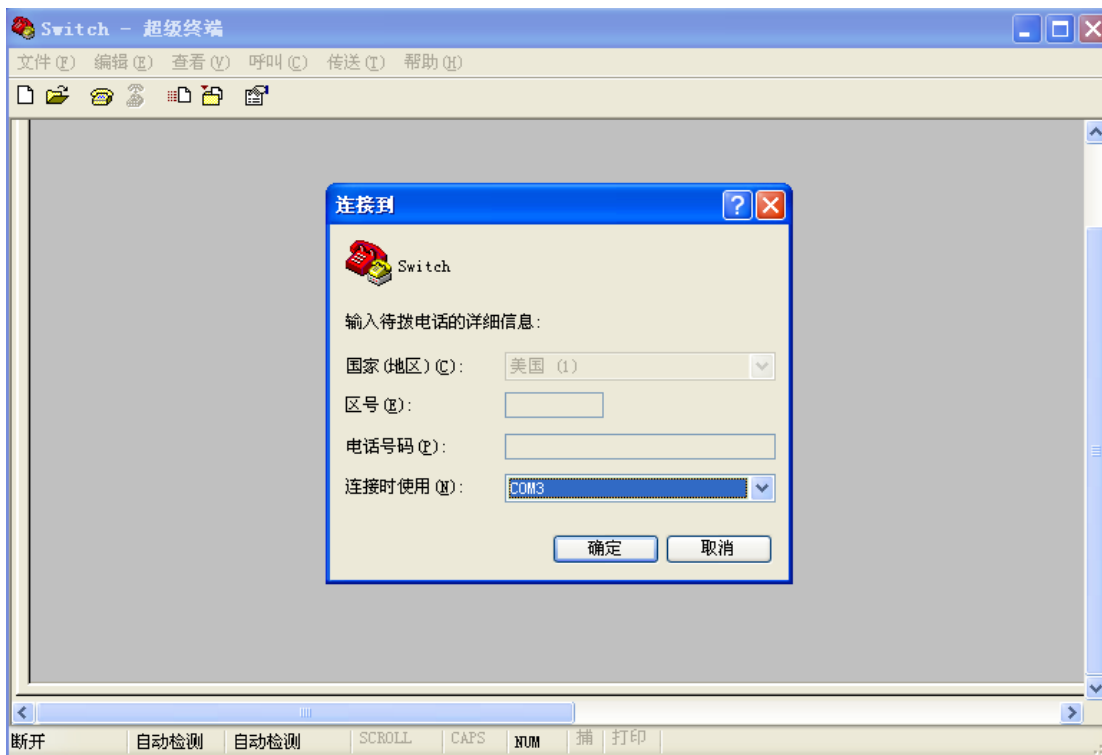
Picture 1 HyperTerminal

3. Establish a new connection "Switch", such as shown on Picture 2;



Picture 2 New connection

4. Select the correct communication port to connect, such as shown on Picture 3;



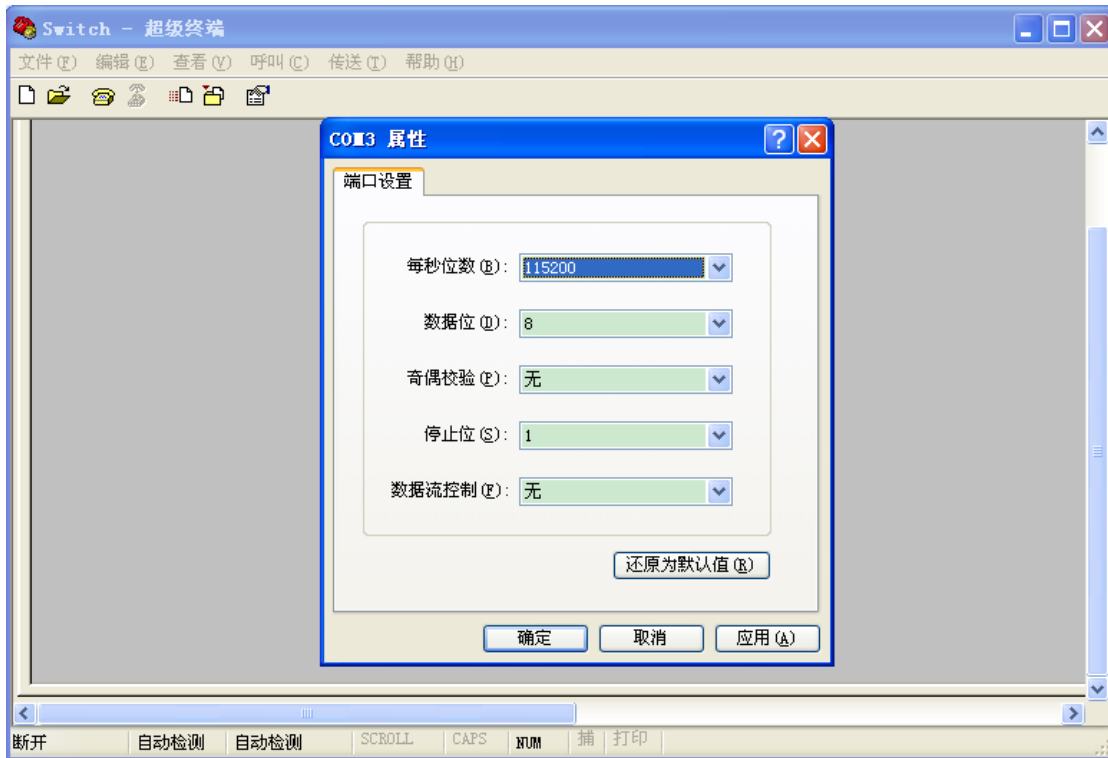
Picture 3 Communication port selection



illustrate:

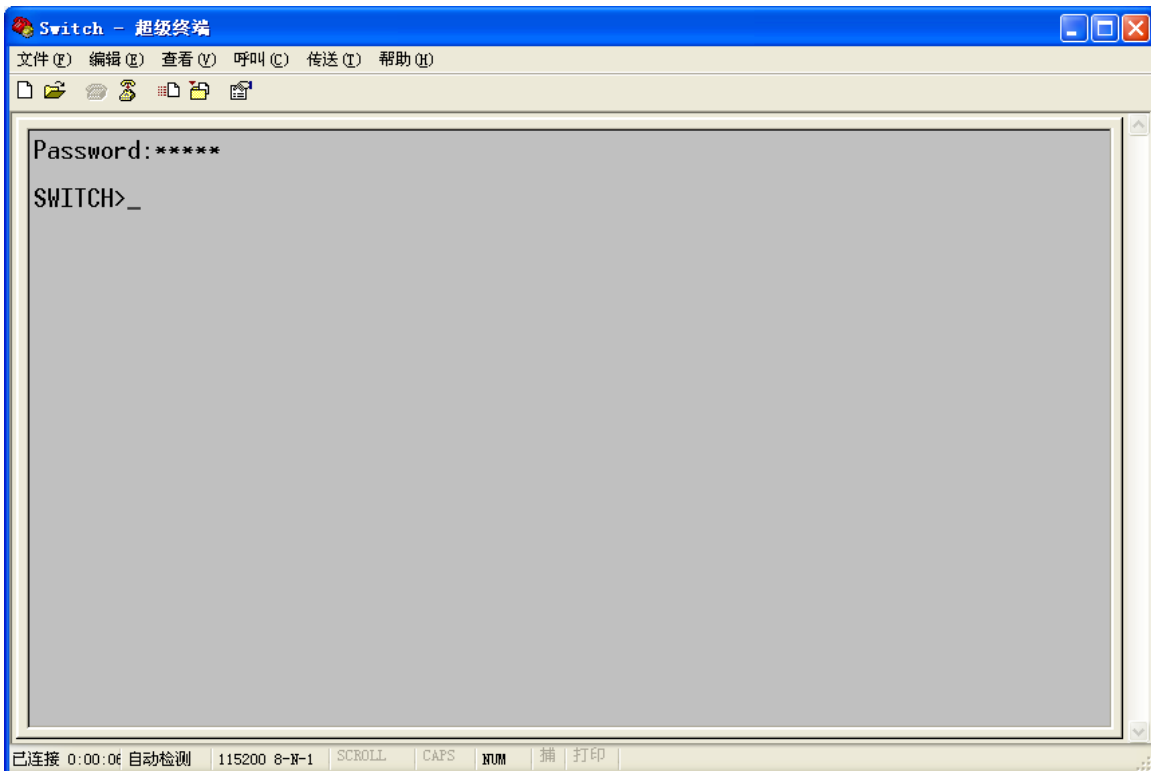
If you do not know the communication port of the current device, you can right-click [My Computer]→[Properties]→[Hardware]→[Device Manager]→[Port] to check the communication port used by the USB port.

5. Serial port parameter configuration such as shown on Picture 4, bits per second (baud rate): 115200; data bits: 8; parity: none; stop bits: 1; data flow control: none;



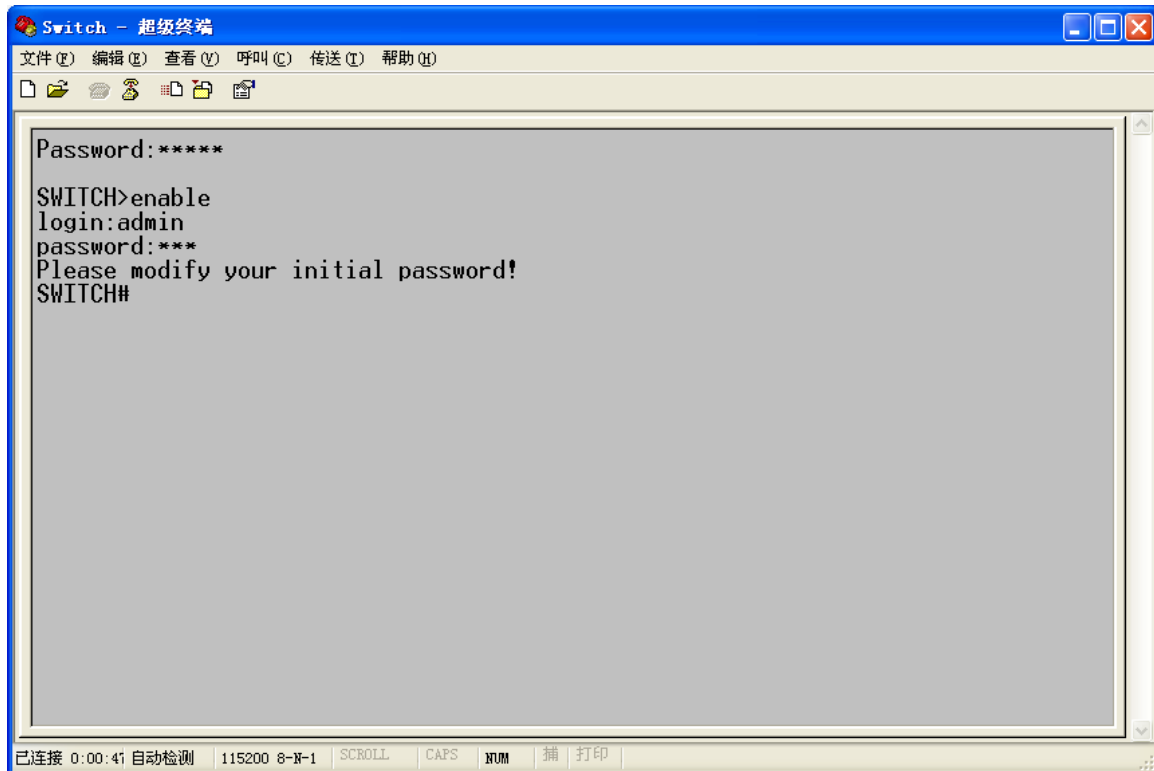
Picture 4 Property configuration

6. Click the <OK> button to successfully enter the command line interface of the switch, enter the password "admin", and press the <Enter> key to enter the general user configuration mode, such as shown on Picture 5;



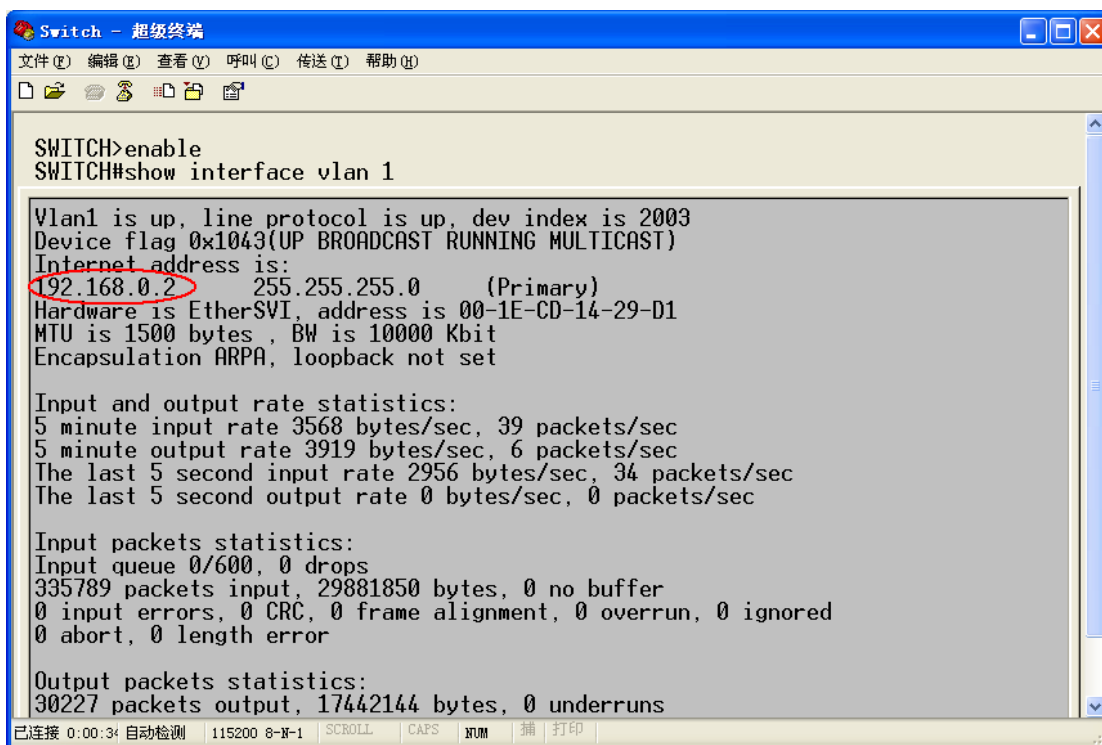
Picture 5 CLI interface

7. Enter the command "enable", the default user name "admin" and password "123"; you can also enter other created user names and passwords to enter the privileged user configuration mode, such as limage 6 shown;



Picture 6 Privileged User Configuration Mode

8. Enter the command "show interface vlan 1" to view the switch IP address, such as Shown on Picture 7 in the red area;

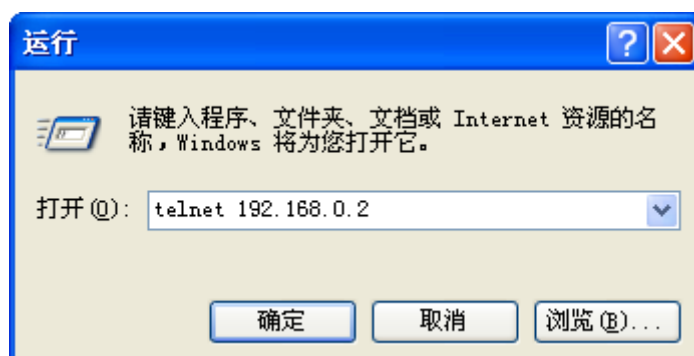


Picture 7 View IP address

2.6 Telnet access

Telnet login requires that the PC and the switch can communicate normally.

1. Enter "telnet IP address" in the run dialog box, the default IP address of Kyland's switch is "192.168.0.2", such as shown on Picture 8;



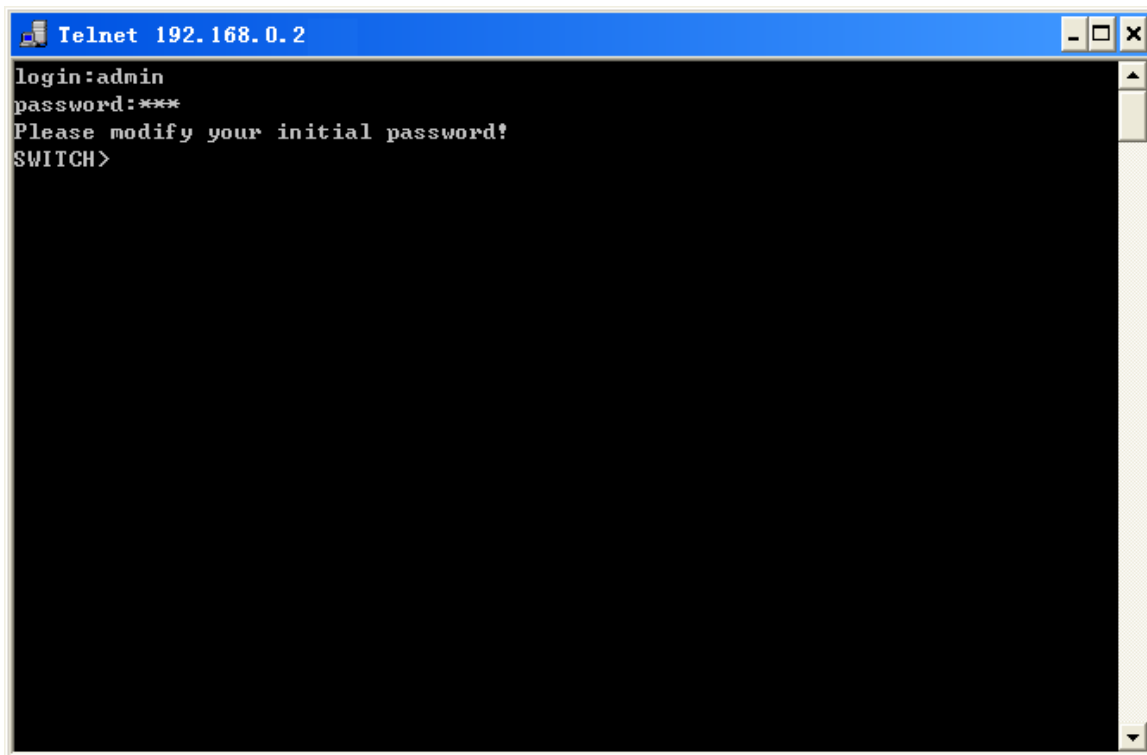
Picture 8 Telnet access



illustrate:

If you do not know the current switch IP address, please refer to Picture 7 Get the IP address.

2. Enter the default user name "admin" and password "123" in the Telnet interface; you can also enter other created user names and passwords to enter the switch command line interface, such as shown on Picture 9;



Picture 9 Telnet interface

2.7 web access

Web login requires that the PC and the switch can communicate normally.



illustrate:

It is recommended to use IE8.0 or above browser to make the web management interface more friendly.

1. Enter "IP address" in the browser address bar and a login dialog box will appear, such as shown on Picture 10, enter the default user name "admin" and password "123" and the verification code displayed below, or enter other created user names and passwords, and click the <Login> button;



Picture 10 Web login

Language selection English can switch to the English login interface, the factory default is the English login interface, select Chinese to switch to the Chinese login interface.



illustrate:

If you do not know the current switch IP address, please refer to Picture 7 Get the IP address.

2. When a prompt to change the password appears, click the <OK> button;
3. Successfully log in to the switch web management page, the left is the configuration navigation tree, such as shown on Picture 11;



Picture 11 Web interface

For the Web operation of the switch, please refer to "SICOM3028GPT Series Industrial Ethernet Switches Web Operation Manual".

3 ACL configuration

3.1 introduce

ACL (Access Control List, Access Control List) can filter packets by configuring matching rules and processing operations for packets in the inbound direction of switch ports, effectively preventing illegal users from accessing the network, and can also control traffic and save the network resource.

3.2 ACL entries and rules

An ACL entry can contain multiple rules, and each rule specifies different packet matching options and packet processing actions. Before configuring rules, you need to create ACL entries. Among multiple rules in the same ACL entry, the smaller the rule number has higher priority, and the action on the packet is matched from the first rule until a rule is matched, and subsequent rules will not be matched.

ACL entries can be applied to ports, VLANs, and the whole world. When multiple entries conflict, the port application priority is the highest, and the global application priority is the lowest. For example, configure ACL1 entry (to discard packets with destination IP 192.168.0.3) to apply globally; configure ACL2 entry (to receive packets with destination IP 192.168.0.3) to apply to VLAN1; configure ACL3 entry (to mirror destination IP address 192.168.0.3) is applied to port 2/1, which belongs to VLAN1. For port 2/1, since the port application priority is higher than the VLAN application priority, port 2/1 mirrors the packets whose destination IP address is 192.168.0.3. For VLAN 1, since the VLAN application is higher than the global application, VLAN 1 receives packets with the destination IP address 192.168.0.3. In other cases, the packets whose destination IP address is 192.168.0.3 are discarded.

Since an ACL entry is a collection of one or more rules, after an ACL entry is applied to a port/VLAN/global, all the rules belonging to the ACL will be applied to the port/VLAN/global.

By default, the priority of ACLs applied to the same port/VLAN/global is delivered first, and users can adjust the priority of ACL entries as needed.

3.3 CLI configuration

Table 4 configuration command

Order	configuration mode	Features
acl no acl	Global configuration mode SWITCH(Config)#	Create an ACL entry (enter ACL configuration mode); Delete ACL entries.
acl acl_id apply no acl acl_id apply	port configuration mode SWITCH(Config-Ethernet1/1)#	Apply ACL entries in port mode; Cancel the application of ACL entries in port mode.
	VLAN configuration mode SWITCH(Config-Vlan1)#	Apply ACL entries in VLAN mode; Cancel the application of ACL entries in VLAN mode.
	Global configuration mode SWITCH(Config)#	Apply ACL entries in global mode; Cancel the application of ACL entries in global mode.
description no description	ACL configuration mode SWITCH(Config-acl1)#	Add description information to ACL entries; Delete the description information of the ACL entry.
apply no apply	ACL configuration mode SWITCH(Config-acl1)#	Configure the application scope of ACL entries; Delete the application scope of the ACL entry.
rule no rule	ACL configuration mode SWITCH(Config-acl1)#	Add rules to ACL entries; Delete ACL entry rules.
show this	ACL configuration mode SWITCH(Config-acl1)#	Display current ACL entry information.
show acl	Privileged User Configuration Mode SWITCH#	Displays information about ACL entries configured by the user.

3.3.1 acl

Features	Create an ACL entry (enter ACL configuration mode); Delete ACL entries.
command format	acl <i>acl_id</i> no acl {all <i>acl_id</i> }
parameter	<i>acl_id</i> : ACL entry ID, the configuration range is 1~1024;

	all: All created ACL entries.
illustrate	The product supports up to 512 ACL entries. If the entry is applied to multiple ports, the application under each port is an ACL entry; similarly, if the entry is applied to multiple VLANs, each VLAN The application below is an ACL entry.
configuration mode	Global configuration mode SWITCH(Config)#



Notice:

Because there are some system ACL entries on the device, the actual ACL entries that can be configured by users are less than 512.

【Example】

Create ACL entry 1.

```
SWITCH(Config)#acl 1
```

```
SWITCH(Config-acl1)#
```

3.3.2 acl acl_id apply

Features	Apply ACL entries in port/VLAN/global mode; Cancel the application of ACL entries in port/VLAN/global mode.
command format	acl acl_id apply ingress no acl acl_id apply [ingress]
parameter	<i>acl_id</i> : ACL entry ID.
configuration mode	port configuration mode SWITCH(Config-Ethernet1/1)# VLAN configuration mode SWITCH(Config-Vlan1)# Global configuration mode SWITCH(Config)#

【Example】

Apply ACL entry 1 to ports 2/1-2/4, VLAN1, and VLAN2.

```
SWITCH(Config)#interface ethernet 2/1
```

```
SWITCH(Config-Ethernet2/1)#acl 1 apply ingress
```

```
SWITCH(Config-Ethernet2/1)#exit
```

```
SWITCH(Config)#interface ethernet 2/2
```

```
SWITCH(Config-Ethernet2/2)#acl 1 apply ingress
```

```
SWITCH(Config-Ethernet2/2)#exit
```

```

SWITCH(Config)#interface ethernet 2/3
SWITCH(Config-Ethernet2/3)#acl 1 apply ingress
SWITCH(Config-Ethernet2/3)#exit
SWITCH(Config)#interface ethernet 2/4
SWITCH(Config-Ethernet2/4)#acl 1 apply ingress
SWITCH(Config-Ethernet2/4)#exit
SWITCH(Config)#vlan 1
SWITCH(Config-Vlan1)#acl 1 apply ingress
SWITCH(Config-Vlan1)#exit
SWITCH(Config)#vlan 2
SWITCH(Config-Vlan2)#acl 1 apply ingress
    
```

3.3.3 apply

Features	Configure the application scope of ACL entries; Delete the application scope of the ACL entry.
command format	apply {global interface ethernet interface_list vlan vlan_id} ingress no apply {all global ingress interface ethernet interface_list ingress vlan vlan_id ingress}
parameter	global : global application; <i>interface_list</i> : one or more ports; <i>vlan_id</i> : one or more VLANs; When including multiple ports, you can use ";" and "-" special characters to connect. ";" connects discontinuous port numbers, and "-" connects continuous port numbers.
configuration mode	ACL configuration mode SWITCH(Config-acl1)#

【Example】

Apply ACL entry 1 to ports 2/1-2/4, VLAN1, and VLAN2.

```

SWITCH(Config-acl1)#apply interface ethernet 2/1-4 ingress
SWITCH(Config-acl1)#apply vlan 1 ingress
SWITCH(Config-acl1)#apply vlan 2 ingress
    
```

3.3.4 description

Features	Add description information to ACL entries; Delete the description information of the ACL entry.
command format	description <i>ACL_description</i> no description
parameter	<i>ACL_description</i> : ACL description information, the configuration range is 1~127 characters.
configuration mode	ACL configuration mode SWITCH(Config-acl1)#

【Example】

Add description information a for ACL entry 1.

SWITCH(Config-acl1)#description a

3.3.5 rule

Features	Add rules to ACL entries; Delete ACL entry rules.
command format	rule <i>rule_id</i> [<ethtype ethernet_type_value ip-dst ip_dst_address ip_address_mask ip-protocol ip_protocol_id ip-src ip_src_address ip_address_mask mac-dst mac_dst_address mac_address_mask mac-src mac_src_address mac_address_mask port-dst port_id port-src port_id vid vlan_id>] action [deny mirror {cpu interface ethernet port_id} permit redirect {cpu interface ethernet port_id}] no rule {all rule_id}
describe	If all parameters in the command are selected, ethtype , ip-dst, ip-protocol, ip-src, mac-dst, mac-src, port-dst, port-src, vid can be arranged in any order. If multiple parameters are selected, there is an "and" relationship between them.
parameter	<i>rule_id</i> : ACL entry rule number, the configuration range is 1~1024. A maximum of 512 rules can be added to each ACL entry, and the total number of rules added to all ACL entries does not exceed 512. <i>ethernet_type_value</i> : Protocol type, the configuration range is 0~65535; <i>ip_protocol_id</i> : IP protocol number, the configuration range is 0~255; <i>ip_dst_address</i> : destination IP address; <i>ip_src_address</i> : source IP address; <i>ip_address_mask</i> : IP address mask, 1 in the IP address mask represents the concerned IP address bit, and 0 represents the ignored IP address bit;

	<p><i>mac_dst_address</i>: destination MAC address;</p> <p><i>mac_src_address</i>: source MAC address;</p> <p><i>mac_address_mask</i>: MAC address mask, 1 in the MAC address mask represents the concerned MAC address bit, and 0 represents the ignored MAC address bit;</p> <p><i>port_id</i>: source/destination port number, the configuration range is 0~65535;</p> <p><i>vlan_id</i>: VLAN ID, the configuration range is 1~4093;</p> <p>deny: discard successfully matched packets;</p> <p>mirror: Receive successfully matched packets and mirror them to the CPU or specified port;</p> <p>permit: Receive successfully matched packets;</p> <p>redirect: redirect successfully matched packets to the CPU or specified port;</p> <p>By default, packets that match successfully are received.</p>
configuration mode	ACL configuration mode SWITCH(Config-acl1)#

【Example】

Add rule 1 to ACL entry 1, destination MAC address 00-00-00-00-00-01, destination MAC mask 00-ff-ff-ff-ff-ff; source MAC address 00-00-00-00-11-01, source MAC mask 00-ff-ff-ff-ff-00;

Protocol type 2048; IP protocol number 60; source IP address 192.168.1.5, source IP mask 255.255.255.0; destination IP address 192.168.0.5, destination IP mask 255.255.255.0; the matching action is discarded.

```
SWITCH(Config-acl1)#rule 1 mac-dst 00-00-00-00-00-01 00-ff-ff-ff-ff-ff mac-src 00-00-00-00-11-01 00-ff-ff-ff-ff-00 ethtype 2048 ip-protocol 60 ip-src 192.168.1.5 255.255.255.0 ip-dst 192.168.0.5 255.255.255.0 action deny
```

3.3.6 show acl

Features	Displays information about ACL entries configured by the specified user.
command format	show acl {all ACL_id}
parameter	<p><i>acl_id</i>: ACL entry ID, the configuration range is 1~1024;</p> <p>all: All created ACL entries.</p>
configuration	Privileged User Configuration Mode SWITCH#

mode	
------	--

【Example】

Displays all ACL entries configured by the user.

SWITCH#show acl all

```
SWITCH#show acl all
=====
ACL ID : 1
Description : a
State : A
Instances : 6
Rules : 1
Instance list : interface Ethernet2/1 ingress
                interface Ethernet2/2 ingress
                interface Ethernet2/3 ingress
                interface Ethernet2/4 ingress
                vlan 1 ingress
                vlan 2 ingress

ID  Stat Action          Rule Content
-----
1   A    Deny                  L2 EthType 0x800
                                L2 MAC src 00-00-00-00-11-01 00-ff-ff-ff-ff-00
                                L2 MAC dst 00-00-00-00-00-01 00-ff-ff-ff-ff-ff
                                L3 IP protocol 60
                                L3 IP src 192.168.1.5 255.255.255.0
                                L3 IP dst 192.168.0.5 255.255.255.0
=====

ACL ID : 2
Description : Undefined
State : A
Instances : 2
Rules : 0
Instance list : vlan 1 ingress
                vlan 2 ingress
=====
```

3.3.7 show this

Features	Display current ACL entry information.
command	show this
format	
configuration mode	ACL configuration mode SWITCH(Config-acl1)#

【Example】

Displays current ACL entry information in ACL 1 configuration mode.

SWITCH(Config-acl1)#show this

```
SWITCH(Config-acl1)#show this
=====
ACL ID : 1
Description : a
State : A
Instances : 6
Rules : 1
Instance list : interface Ethernet2/1 ingress
                interface Ethernet2/2 ingress
                interface Ethernet2/3 ingress
                interface Ethernet2/4 ingress
                vlan 1 ingress
                vlan 2 ingress

ID  Stat Action          Rule Content
-----
1   A    Deny                  L2 EthType 0x800
                                L2 MAC src 00-00-00-00-11-01 00-ff-ff-ff-ff-00
                                L2 MAC dst 00-00-00-00-00-01 00-ff-ff-ff-ff-ff
                                L3 IP protocol 60
                                L3 IP src 192.168.1.5 255.255.255.0
                                L3 IP dst 192.168.0.5 255.255.255.0
=====
```

3.4 Typical configuration example

Port 2/1 discards the host on the 192.168.1.0 network segment and sends the TCP packet with the source port number 80 to the host on the 192.168.0.0 network segment.

The configuration is as follows:

```
SWITCH(Config)#acl 1 //Create ACL entry 1
SWITCH(Config-acl1)#apply interface ethernet 2/1 ingress //Apply entry 1 to port 2/1
SWITCH(Config-acl1)#rule 1 ip-src 192.168.1.5 255.255.255.0 ip-dst 192.168.0.5
255.255.255.0 ip-protocol 6 port-src 80 action deny //Configure ACL rule
```

4 Cable Diagnostics

4.1 introduce

Cable Diagnostics utilizes TDR (Time Domain Reflectometry) to detect twisted pair status. Cable faults are detected by sending a pulse signal to the wire and detecting the reflection of this pulse signal. When the cable line is faulty, when the transmitted pulse signal reaches the end of the cable or the fault point of the cable, part or all of the pulse energy is reflected back to the original transmission source. This diagnostic technology measures the transmission of the pulse signal in the wire, reaching the fault point and sending back source time and convert the time to a distance value.

4.2 accomplish

Cable diagnosis can detect the link medium of the cable connected to the Ethernet electrical port and return the detection result. The cable diagnosis can be used to detect the following cable pair states:

Short: Indicates that a pair is shorted.

Open: Indicates an open circuit, indicating that there is a disconnection in the line pair.

Normal: Indicates that the line pair status is normal.

Mismatch: indicates that the impedance does not match. For example, the impedance of a Category 5 cable is 100 ohms. To prevent waveform reflection and data errors, the impedance of the terminators at both ends of the cable must also be 100 ohms.



illustrate:

RJ45 plug wiring according to standard 568B (1-orange-white, 2-orange, 3-green-white, 4-blue, 5-blue-white, 6-green, 7-brown-white, 8-brown), among which (1, 2) , (3, 6), (4, 5), (7, 8) are 4 line pairs.

4.3 CLI configuration

Table 5 Configuration command

Order	configuration mode	Features
cable-test	Privileged User Configuration Mode	Check the port pair status.

	SWITCH#	
show cable-test	Privileged User Configuration Mode SWITCH#	Displays the status of the specified pair.

4.3.1 cable-test

Features	Check the port pair status.
command format	cable-test start [all down interface ethernet port_id up]
describe	If no parameter is specified, the pair status of the faulty port is detected.
parameter	all : Detect the line pair status of all electrical ports on the switch; down : Detect the line pair status of all Link Down ports on the switch; <i>port_id</i> : The port number; up : Detects the line pair status of all Link Up ports on the switch.
illustrate	This function only detects electrical ports; The 100M electrical port only detects (1,2) and (3,6) two pairs; the Gigabit electrical port needs to detect (1,2), (3,6), (4,5) and (7,8)) four pairs.
configuration mode	Privileged User Configuration Mode SWITCH#



Notice:

The detection port is in the Link down state during the detection process.

【Example】

Check the line pair status of all electrical ports in the current device.

SWITCH#cable-test start all

4.3.2 show cable-test

Features	Displays the pair status of the detected port.
command format	show cable-test [all down interface ethernet port_id up]
describe	If no parameter is specified, the pair status of the detected faulty port is displayed.
parameter	all : Display the line pair status of all electrical ports detected; down : Display the line pair status of all detected Link Down electrical ports;

	<i>port_id</i> :The port number; up : Display the line pair status of all the detected Link Up status electrical ports.
configuration mode	Privileged User Configuration Mode SWITCH#

【Example】

Displays the wire pair status of all electrical ports detected.

SWITCH#show cable-test all

```
SWITCH#show cable- all
  port      type      pair      cable-status      cable-length(m)
-----
 Ethernet1/1  GE      (1,2)     Open              0
              (3,6)     Open              0
              (4,5)     Open              0
              (7,8)     Open              0
 Ethernet1/2  GE      (1,2)     Open              0
              (3,6)     Open              0
              (4,5)     Open              0
              (7,8)     Open              0
 Ethernet2/1  FE      (1,2)     Normal            unknown
              (3,6)     Normal            unknown
 Ethernet2/2  FE      (1,2)     Open              0
              (3,6)     Open              0
 Ethernet2/3  FE      (1,2)     Open              0
              (3,6)     Open              0
 Ethernet2/4  FE      (1,2)     Open              0
              (3,6)     Open              0
 Ethernet6/1  FE      (1,2)     Open              0
              (3,6)     Open              0
 Ethernet6/2  FE      (1,2)     Open              0
              (3,6)     Open              0
 Ethernet6/3  FE      (1,2)     Open              0
              (3,6)     Open              0
 Ethernet6/4  FE      (1,2)     Open              0
              (3,6)     Open              0
```

Display content	describe
pair	pair
cable-status	Wire pair status, there are four statuses of open circuit, short circuit, normal and mismatch
cable-length	Shows the length from the cable port connection to the point of failure, this measurement technique has a small amount of error. Line pairs in the normal state do not display lengths.

5 alert

5.1 introduce

IP/MAC address conflict alarm: When enabled, an alarm is generated when IP/MAC addresses conflict. The time interval for detecting address conflict is 5s.

5.2 CLI configuration

Table 6 Configuration command

Order	configuration mode	Features
alarm address-conflict-detect enable	Global configuration mode SWITCH(Config)#	Enable IP/MAC address conflict alarm; IP/MAC address conflict alarm is disabled.
alarm address-conflict-detect disable		

5.2.1 alarm address-conflict-detect

Features	Enable IP/MAC address conflict alarm Disable IP/MAC address conflict alarms
command format	alarm address-conflict-detect enable alarm address-conflict-detect disable
Default configuration	Disable
configuration mode	Global configuration mode SWITCH(Config)#

After the IP/MAC address conflict alarm is enabled, if an IP/MAC address conflict occurs, the following log information is displayed.

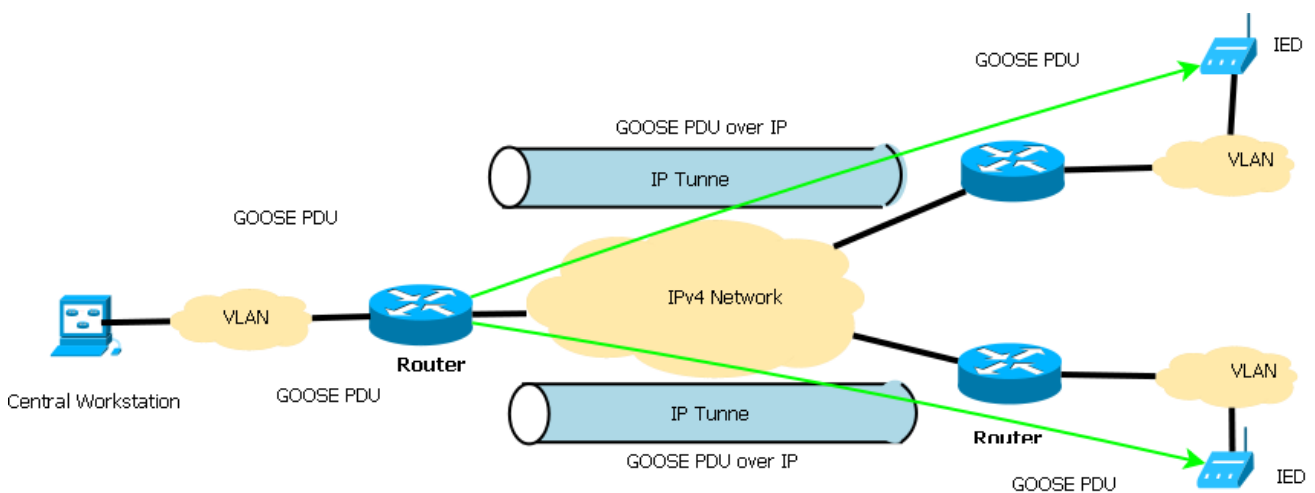
```
SWITCH#%Apr 13 17:40:29 2016 WARNING:IP_CONFLICT IP address 192.168.0.26 ,remote MAC address 00-1E-CD-11-01-B1!
SWITCH#
```

6 GOOSE-over-IP-Tunnel

6.1 introduce

GOOSE is a general object-oriented substation event defined in IEC61850, such as alarm, tripping action command, etc. As the definition of the application layer, in the substation communication model mapping, the GOOSE frame uses the Layer 2 multicast technology without going through the network layer. The maximum transmittable domain of the message is the broadcast domain where the GOOSE source is located.

In substation applications, the usual networking situation is that the central control station and the remote substation are not in the same network, that is, the communication between each other needs to be forwarded through three-layer routing, such as shown on Picture 12. In practical applications, the characteristic that GOOSE frames can only be propagated in the Layer 2 network becomes the limitation of its use. Therefore, in order to use GOOSE in practical applications, there needs to be a way to make GOOSE messages propagate in the three-layer network.



Picture 12 GOOSE Tunnel app

6.2 GOOSE Tunnel

The IP tunneling technology encapsulates a protocol packet in an IP packet to form a routable format, performs routing and forwarding in the IP network, and converts the GOOSE PDU (Protocol Data Unit) into a routable format. Combined with IP tunnel technology, it can

break through the limitation that GOOSE PDU itself can only be propagated in LAN/VLAN, and propagate the specified GOOSE PDU to another LAN/VLAN that cannot be directly propagated through IP network.

GRE (Generic Routing Encapsulation, Generic Routing Encapsulation) defines a general encapsulation format for routable tunnels. It defines a complete tunnel encapsulation into three levels: transport protocol, encapsulation protocol and passenger protocol. The relationship between them is: the passenger protocol is encapsulated in the format of the encapsulation protocol, and the data of the transmission protocol is formed into a message in the form of a transmission protocol, and the routable tunnel transmission is carried out in the tunnel. Encapsulate and then release the passenger protocol.

The GOOSE packet is used as the tunnel-encapsulated passenger protocol packet, the GRE encapsulation is used as the encapsulation protocol, and the IP protocol is used as the transmission protocol, thus forming a GRE-IP tunnel for transmitting GOOSE packets in the IP network, which is called GOOSE Tunnel.

GOOSE Tunnel technology is mainly a process of encapsulation and decapsulation. Simply put, GOOSE packets are encapsulated in IPv4 at the start end of the tunnel, and the corresponding IPv4 packets are decapsulated at the end of the tunnel to restore the GOOSE packets. This process mainly applies the GRE encapsulation protocol.

6.3 work process

1. Tunnel start binding search

At the beginning of the GOOSE Tunnel, in order to determine the GOOSE flow that needs to be tunneled, and then determine the tunnel interface that the selected GOOSE flow will pass through, it is necessary to configure the binding relationship between the specified GOOSE flow and the Tunnel interface to form a GOOSE packet with The mapping table of tunnel interfaces (GOOSE-Tunnel-Binding-List), which can be configured. The binding of GOOSE stream and tunnel interface is divided into Tunnel-Only mode and Normal mode.

After the GOOSE message arrives at the originating device, it searches the GOOSE-

Tunnel-Binding-List for the binding between the GOOSE stream and the Tunnel interface. If a binding is found, the following processing is performed according to the mode setting in the binding table entry:

Tunnel-Only mode: Eligible GOOSE traffic is forwarded only to the bound Tunnel interface.

Normal mode: Eligible GOOSE traffic is forwarded to the bound Tunnel interface and forwarded normally in the source VLAN according to the FDB entry.

If no binding is found, normal forwarding is performed in the VLAN without special processing.

When looking for the binding between the GOOSE stream and the Tunnel interface, different matching is performed according to the binding range:

Global-based binding: When searching the GOOSE-Tunnel-Binding-List, only the destination MAC address information (excluding VLAN information) of the GOOSE packet is used to match the entries in the binding table that also do not contain VLAN information.

VLAN-based binding: When searching the GOOSE-Tunnel-Binding-List, use the destination MAC address of the GOOSE packet + VLAN information for exact matching; if the matching fails, perform global binding matching.

2. Package

The GOOSE packet enters the tunnel, and the starting interface forms the outer IP header according to the configured destination IP address (IP unicast address or IP multicast address) and source interface IP address; after the GOOSE PDU is encapsulated in the GRE header, the outer IP header is encapsulated. Layer IP header.

**Notice:**

In the encapsulated GOOSE PDU, when the IEEE802.1Q field is reserved and the VID is 0, the VID value can be replaced with the source VLAN ID of the GOOSE PDU overlaid on the Tunnel Initiating Device.

3. Transmission

The IP packet formed after encapsulation is routed through the IP protocol stack of the device to obtain the actual outgoing interface, and sent to the next-hop router for routing and forwarding in the IP network.

4. Decapsulation

The encapsulated packet reaches the tunnel termination device through the tunnel. After determining that the destination of the encapsulated packet is the local device, the device decapsulates the packet and releases the GOOSE PDU of the passenger protocol packet.

5. VLAN remapping

After the GOOSE message arrives at the GOOSE-Tunnel terminal, decapsulates and releases it, the secondary VLAN remapping is performed, and the remapping is configurable.

After the tunnel is terminated and the GOOSE PDU is released, the VID field in the IEEE802.1Q domain will be extracted, the source VLAN will be obtained, and then the GOOSE PDU VLAN remapping table configured on the device will be searched to obtain the VLAN that is actually released by the GOOSE PDU.

If remapping is configured, the GOOSE PDU is released in the new VLAN; if the new VLAN is not created, the GOOSE PDU is discarded.

If no remapping is configured, the GOOSE PDU is released in the source VLAN; if the VLAN is not created, the GOOSE PDU is discarded.

6. Propagation in the target VLAN

On the GOOSE-Tunnel termination device, you can configure the static binding relationship (Static-GOOSE-Entry-List) of the GOOSE PDU with the outgoing interface in the outgoing VLAN.

After the GOOSE PDU released by the tunnel termination and decapsulation has been determined, the actual outgoing interface needs to be further determined in the destination VLAN after the target VLAN is determined. First, look up the static GOOSE entry, if found, forward it according to the configured outbound interface; if not found, take further action according to the release mode of the final GOOSE PDU:

When the release mode is strict, the packet is discarded.

When the release mode is normal, forwarding is performed according to the FDB table. If there is no entry in the FDB table, it is broadcast in the target VLAN.

6.4 CLI configuration

Table 7 Configuration command

Order	configuration mode	Features
interface tunnel no interface tunnel	Global configuration mode SWITCH(Config)#	Create a tunnel interface (enter Tunnel interface configuration mode); Delete the tunnel interface.
mode	Tunnel interface configuration mode SWITCH(Config-Tunnel1)#	Configure the encapsulation mode of GOOSE Tunnel.
destination no destination	Tunnel interface configuration mode SWITCH(Config-Tunnel1)#	Configure the IP address of the tunnel termination end; Delete the IP address of the tunnel termination end.
source no source	Tunnel interface configuration mode SWITCH(Config-Tunnel1)#	Configure the tunnel source interface; Delete the tunnel source interface.
goose default-forward-policy no goose default-forward-policy	Global configuration mode SWITCH(Config)#	Configure the default binding mode between GOOSE packets and the tunnel start interface as Tunnel-Only mode; Restore the default binding mode between GOOSE packets and the tunnel's initial interface to Normal mode.
goose forward-policy	Global configuration mode SWITCH(Config)#	Configure the binding mode of the GOOSE message and the tunnel starting interface; Configure the release mode for terminating GOOSE PDUs.
goose vlan-remark no goose vlan-remark	Global configuration mode SWITCH(Config)#	Configure VLAN remapping for GOOSE packets; Delete VLAN remapping of GOOSE packets.
goose tunnel-binding no goose tunnel-binding	Global configuration mode SWITCH(Config)#	Configure the binding table entry between the GOOSE message and the initial interface of the Tunnel; Delete the binding entry between the GOOSE

		packet and the initial interface of the tunnel
goose static no goose static	Global configuration mode SWITCH(Config)#	Configure static GOOSE entries; Delete static GOOSE entries.
show interface tunnel	Privileged User Configuration Mode SWITCH#	Displays information about the tunnel interface.
show goose static	Privileged User Configuration Mode SWITCH#	Displays release mode and static for terminating GOOSE PDUs. GOOSE entry
show goose tunnel-binding	Privileged User Configuration Mode SWITCH#	Displays the default binding mode and binding entry between GOOSE packets and the tunnel starting interface.
show goose vlan-remark	Privileged User Configuration Mode SWITCH#	Show VLAN remapping.

6.4.1 interface tunnel

Features	Create a tunnel interface (enter Tunnel interface configuration mode); Delete the tunnel interface.
command format	interface tunnel <i>tunnel_index</i> no interface tunnel <i>tunnel_index</i>
parameter	<i>tunnel_index</i> : Tunnel interface index, the configuration range is 1~64.
illustrate	The product supports up to 64 Tunnel interfaces.
configuration mode	Global configuration mode SWITCH(Config)#

6.4.2 mode

Features	Configure the encapsulation mode of GOOSE Tunnel.
command format	mode gre-ip
parameter	gre-ip : GRE encapsulation mode.
illustrate	Currently, the encapsulation mode of GOOSE Tunnel only supports GRE-IP.
configuration mode	Tunnel interface configuration mode SWITCH(Config-Tunnel1)#

6.4.3 destination

Features	Configure the IP address of the tunnel termination end; Delete the IP address of the tunnel termination end.
command format	destination ip address <i>ip_address</i> no destination ip address
parameter	<i>ip_address</i> : The IP address of the tunnel termination terminal.
illustrate	The IP address of the tunnel termination end can be configured as a unicast IP address or as a multicast IP address.
configuration mode	Tunnel interface configuration mode SWITCH(Config-Tunnel1)#

6.4.4 source

Features	Configure the tunnel source interface; Delete the tunnel source interface.
command format	source interface <i>vlan_interface</i> no source interface
parameter	<i>vlan_interface</i> : The created VLAN interface.
configuration mode	Tunnel interface configuration mode SWITCH(Config-Tunnel1)#

6.4.5 goose default-forward-policy

Features	Configure the default binding mode between GOOSE packets and the tunnel start interface as Tunnel-Only mode; Restore the default binding mode between GOOSE packets and the tunnel's initial interface to Normal mode.
command format	goose default-forward-policy tunnel-start tunnel-only no goose default-forward-policy tunnel-start tunnel-only
parameter	tunnel-only : In this binding mode, the qualified GOOSE traffic is only forwarded to the bound tunnel interface; otherwise, the qualified GOOSE traffic is forwarded to the bound tunnel interface and forwarded normally in the source VLAN according to the FDB entry.
Default configuration	Normal mode
configuration mode	Global configuration mode SWITCH(Config)#

6.4.6 goose forward-policy

Features	Configure the binding mode of the GOOSE message and the tunnel starting interface; Configure the release mode for terminating GOOSE PDUs.
command format	goose forward-policy tunnel-start {default normal tunnel-only} mac-address mac_address [vlan vlan_id] goose forward-policy tunnel-end {normal strict}
parameter	default : The binding mode of the GOOSE packet and the initial interface of the tunnel adopts the mode configured by the command "goose default-forward-policy"; normal /tunnel-only: The binding mode of the GOOSE packet and the tunnel start interface adopts the normal/tunnel-only mode; <i>mac_address</i> / <i>vlan_id</i> : The destination MAC address and VLAN ID of the GOOSE packet. The configuration range of MAC address: 01-0C-CD-01-00-00 ~ 01-0C-CD-01-01-FF. Specify GOOSE packets by MAC address or VLAN ID. normal : When a GOOSE packet is released, it is forwarded according to the static GOOSE entry. If there is no matching entry, the packet is discarded. strict : When releasing a GOOSE message, first look for a static GOOSE entry to forward it. If there is no matching entry, forward it according to the FDB table. If there is no entry in the FDB table, broadcast it in the target VLAN.
Default configuration	The default binding mode between GOOSE packets and the tunnel starting interface is default; The release mode for terminating GOOSE PDUs is strict by default.
illustrate	The binding mode of the GOOSE packet specifying the MAC address and VLAN ID has a higher priority than the binding mode of the GOOSE packet specifying only the MAC address.
configuration mode	Global configuration mode SWITCH(Config)#

6.4.7 goose tunnel-binding

Features	Configure the binding table entry between the GOOSE message and the initial interface of the Tunnel; Delete the binding entry between the GOOSE message and the tunnel's initial interface.
command format	goose tunnel-binding mac-address <i>mac_address</i> [vlan vlan_id] interface tunnel tunnel_index no goose tunnel-binding mac-address <i>mac_address</i> [vlan vlan_id] interface tunnel tunnel_index

parameter	<i>mac_address/vlan_id</i> : The MAC address and VLAN ID in the binding table entry. The configuration range of MAC address: 01-0C-CD-01-00-00 ~ 01-0C-CD-01-01-FF. <i>tunnel_index</i> : Tunnel interface.
illustrate	ShouldThe product can be configured with 512 binding entries.
configuration mode	Global configuration mode SWITCH(Config)#

6.4.8 goose vlan-remark

Features	Configure VLAN remapping for GOOSE packets; Delete VLAN remapping of GOOSE packets.
command format	goose vlan-remark [mac-address <i>mac_address</i>] vlan <i>vlan_id</i> target-vlan <i>target_vlan_id</i> no goose vlan-remark [mac-address <i>mac_address</i>] vlan <i>vlan_id</i> target-vlan <i>target_vlan_id</i>
parameter	<i>mac_address/vlan_id</i> : Destination MAC address and source VLAN ID of the GOOSE packet. The configuration range of MAC address: 01-0C-CD-01-00-00 ~ 01-0C-CD-01-01-FF. <i>target_vlan_id</i> : The mapped VLAN ID.
illustrate	The VLAN remapping priority of the GOOSE packet with the specified MAC address and the source VLAN ID is higher than the VLAN remapping of the GOOSE packet with only the specified VLAN ID.
configuration mode	Global configuration mode SWITCH(Config)#

6.4.9 goose static

Features	Configure static GOOSE entries; Delete static GOOSE entries.
command format	goose static mac-address <i>mac_address</i> vlan <i>vlan_id</i> interface ethernet port <i>port_id</i> no goose static mac-address <i>mac_address</i> vlan <i>vlan_id</i> interface ethernet port <i>port_id</i>
parameter	<i>mac_address/vlan_id</i> : The destination MAC address and VLAN ID of the GOOSE packet. The configuration range of MAC address: 01-0C-CD-01-00-00 ~ 01-0C-CD-01-01-FF. <i>port_id</i> : Outgoing interface for GOOSE packets.
configuration mode	Global configuration mode SWITCH(Config)#

6.4.10 show interface tunnel

Features	Displays information about the tunnel interface.
command format	show interface tunnel <i>tunnel_index</i>
parameter	<i>tunnel_index</i> : Tunnel interface.
configuration mode	Privileged User Configuration Mode SWITCH#

[Example] Display the interface information of Tunnel 1.

SWITCH#show interface tunnel 1

```
SWITCH#show in t 1
tunnell is UP, tunnel index is 1
mode is GRE OVER IP.
destination ip is:
192.168.3.1
0 packets output, 0 bytes
the tunnel interface is binding with Vlan2
```

6.4.11 show goose static

Features	Displays the release mode and static GOOSE entry of the terminating GOOSE PDU.
command format	show goose static
configuration mode	Privileged User Configuration Mode SWITCH#

[Example] Display static GOOSE entries.

SWITCH#show goose static


```
SWITCH#show goose static

GOOSE end forwarding-policy:strict

index:1
mac:01-0C-CD-01-00-01
vlan:2
interface name:Ethernet1/1

index:2
mac:01-0C-CD-01-00-01
vlan:3
interface name:Ethernet1/1

index:3
mac:01-0C-CD-01-00-01
vlan:1
interface name:Ethernet2/1 Ethernet1/1
```

6.4.12 show goose tunnel-binding

Features	Displays the default binding mode and binding entry between GOOSE packets and the tunnel starting interface.
command format	show goose tunnel-binding
configuration mode	Privileged User Configuration Mode SWITCH#

[Example] Display the binding entry between the GOOSE packet and the initial interface of the tunnel.

```
SWITCH#show goose tunnel-binding
```

```
SWITCH#show goo t
GOOSE start default-forward-policy:Noraml
index:1
mac:01-0C-CD-01-00-01
vlan:2
tunnel-only:Default
interface name:Tunnell

index:2
mac:01-0C-CD-01-00-01
tunnel-only:Default
interface name:Tunnell

index:3
mac:01-0C-CD-01-00-01
vlan:1
tunnel-only:Default
interface name:Tunnell Tunnel2
```

tunnel-only is default: the default binding mode is used for GOOSE packets and the tunnel starting interface;

tunnel-only is true: the binding mode of the GOOSE packet and the initial interface of the tunnel adopts the tunnel-only mode;

tunnel-only is false: The binding mode of GOOSE packets and the tunnel starting interface adopts the normal mode.

6.4.13 show goose vlan-remark

Features	Show VLAN remapping.
command format	show goose vlan-remark
configuration mode	Privileged User Configuration Mode SWITCH#

[Example] Display the VLAN remapping of GOOSE packets.

```
SWITCH#show goose vlan-remark
```

```

SWITCH#show goo v

index:1
mac:01-0C-CD-01-00-01
packet vlan:2
target vlan:1

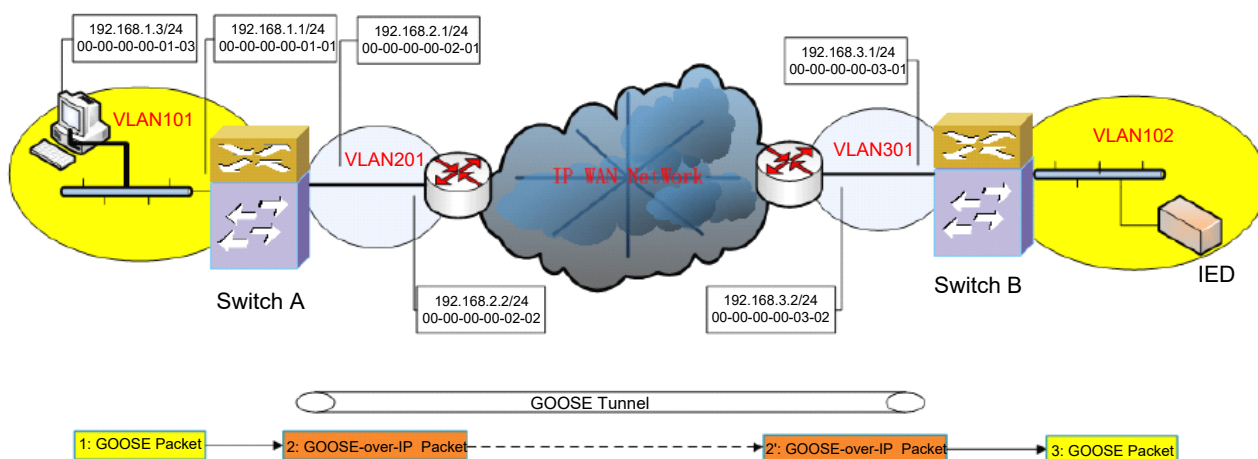
index:2
packet vlan:1
target vlan:3    2

index:3
mac:01-0C-CD-01-00-02
packet vlan:3
target vlan:1

index:4
mac:01-0C-CD-01-00-01
packet vlan:1
target vlan:2    3

index:5
mac:01-0C-CD-01-00-02
packet vlan:2
target vlan:1
    
```

6.5 Typical configuration example



Picture 13 GOOSE-Tunnel application example

As shown on Picture 13, the central control station is located on the left and is connected to the public IP network through Layer 3 switch A that supports GOOSE-Tunnel; the substation is located on the right, and is connected to the public IP network through Layer 3

switch B that supports GOOSE-Tunnel. The IP address of the station controller is 192.168.1.3/24; the IP address of the VLAN101 interface of switch A is 192.168.1.1/24, the IP address of the VLAN201 interface of switch A is 192.168.2.1/24; the IP address of the VLAN301 interface of switch B The address is 192.168.3.1/24. It is required that the GOOSE PDU (01-0C-CD-01-00-01) issued by the central control station controller in VLAN101 can be transmitted to VLAN102 on the other side of the IP network.

Switch A configuration:

```
SWITCH(Config)#interface tunnel 1
    //Create GOOSE Tunnel 1 interface and enter Tunnel 1 interface configuration mode
SWITCH(Config-Tunnel1)#mode gre-ip //Configure the encapsulation mode of GOOSE
Tunnel to GRE-IP
SWITCH(Config-Tunnel1)#destination ip address 192.168.3.1
    //Configure the destination IP address of Tunnel 1 interface
SWITCH(Config-Tunnel1)#source interface vlan 101 //Configure the source interface of
Tunnel 1
SWITCH(Config-Tunnel1)#exit //Enter global configuration mode
SWITCH(Config)#goose forward-policy tunnel-start tunnel-only mac-address 01-0c-cd-
01-00-01 vlan 101
    //Configure the tunnel-only binding mode for GOOSE packets and Tunnel 1 interface
SWITCH(Config)#goose tunnel-binding mac-address 01-0c-cd-01-00-01 vlan 101
interface tunnel 1 //Configure the binding entry between GOOSE packets and Tunnel 1
interface
```

Switch B configuration:

```
SWITCH(Config)#interface tunnel 1
    //Create GOOSE Tunnel 1 interface and enter Tunnel 1 interface configuration mode
SWITCH(Config-Tunnel1)#mode gre-ip //Configure the encapsulation mode of GOOSE
Tunnel to GRE-IP
SWITCH(Config-Tunnel1)#source interface vlan 301 //Configure the source interface of
```

Tunnel 1

```
SWITCH(Config-Tunnel1)#exit //Enter global configuration mode
```

```
SWITCH(Config)#goose vlan-remark mac-address 01-0c-cd-01-00-01 vlan 101 target-  
vlan 102 //Configure VLAN remapping for GOOSE packets
```

```
SWITCH(Config)#goose forward-policy tunnel-end normal
```

```
//Configure the release mode of terminating GOOSE PDU to normal mode
```

```
SWITCH(Config)#goose static mac 01-0c-cd-01-00-01 vlan 102 interface ethernet 2/3
```

```
//Configure static GOOSE entry
```

7 Basic switch configuration

7.1 basic configuration

Table 8 Configuration command

Order	configuration mode	Features
clock set	Privileged User Configuration Mode SWITCH#	Set the system date and clock.
config	Privileged User Configuration Mode SWITCH#	Enter global configuration mode from privileged user configuration mode.
enable	General User Configuration Mode SWITCH>	Enters privileged user configuration mode from normal user configuration mode.
exec timeout	Global configuration mode SWITCH(Config)#	Sets the timeout for exiting privileged user configuration mode.
exit	Various configuration modes	Exit from the current mode and enter the previous mode. For example, use this command in the global configuration mode to return to the privileged user configuration mode, and use this command to return to the general user configuration mode in the privileged user configuration mode.
help	Various configuration modes	Print a brief description of the command interpreter help system.
ip host no ip host	Global configuration mode SWITCH(Config)#	Set the host and IP address mapping relationship; Delete this mapping relationship.
hostname	Global configuration mode SWITCH(Config)#	Sets the prompt for the switch command line interface.
reboot	Privileged User Configuration Mode SWITCH#	Warm-start the switch.
set default	Privileged User Configuration Mode SWITCH#	Restore the factory settings of the switch.

language	General User Configuration Mode SWITCH>	Sets the language type of the displayed help information.
save	Privileged User Configuration Mode SWITCH#	Save the current runtime configuration parameters to Flash Memory.

7.1.1 clock set

Features	Set the system date and clock.
command format	clock set HH:MM:SS YYYY.MM.DD
parameter	HH:MM:SS: The current clock, the value range of HH is 0~23, and the value range of MM and SS is 0~59; YYYY.MM.DD: The current year, month, and day. YYYY ranges from 1970 to 2100, MM ranges from 1 to 12, and DD ranges from 1 to 31.
Default configuration	The default is January 1, 2001 0:0:0 when the system starts.
illustrate	The switch cannot continue to time after a power failure, so in an application environment that requires exact time, the current date and time of the switch must be set first.
command mode	Privileged User Configuration Mode SWITCH#

7.1.2 config

Features	Enter global configuration mode from privileged user configuration mode.
command format	config [terminal]
parameter	terminal : Perform terminal configuration.
configuration mode	Privileged User Configuration Mode SWITCH#

7.1.3 enable

Features	Enters privileged user configuration mode from normal user configuration mode.
command format	enable
configuration	General User Configuration Mode SWITCH>

mode	
------	--

7.1.4 exec timeout

Features	Sets the timeout for exiting privileged user configuration mode.
command format	exec timeout minutes
parameter	<i>minutes</i> : Time value, the unit is minutes, the value range is 0~44640; 0 means no timeout.
Default configuration	The system defaults to 5 minutes.
illustrate	In order to ensure the security of the switch and prevent the malicious operation of illegal users, when the privileged user finishes the last configuration and starts timing, when the set time value is reached, the system automatically exits the privileged user configuration mode. If the user wants to enter the privileged user configuration mode again, he needs to enter the privileged user password and password again. If the value of the configuration exec timeout is 0, it means that the privileged user configuration mode will not be exited.
configuration mode	Global configuration mode SWITCH(Config)#

7.1.5 exit

Features	Exit from the current mode and enter the previous mode. For example, use this command in the global configuration mode to return to the privileged user configuration mode, and use this command to return to the general user configuration mode in the privileged user configuration mode.
command format	exit
configuration mode	Various configuration modes

7.1.6 help

Features	Print a brief description of the command interpreter help system.
command format	help
illustrate	The switch provides online help anytime and anywhere, and the help command displays information about the entire help system, including full help and partial help,

	users can type ? Get online help.
configuration mode	Various configuration modes

7.1.7 ip host

Features	Set the host and IP address mapping relationship; Delete this mapping relationship.
command format	ip host hostname ip_addr no ip host {hostname all }
parameter	<i>hostname</i> : host name, up to 15 characters long; <i>ip_addr</i> : The corresponding IP address of the host name, in dotted decimal format; all : All mappings.
illustrate	set a certain host and The correspondence between IP addresses, which can be used for example "ping <host>" and other commands.
configuration mode	Global configuration mode SWITCH(Config)#

7.1.8 hostname

Features	Sets the prompt for the switch command line interface.
command format	hostname hostname
parameter	<i>hostname</i> : A string of prompts, up to 30 characters long.
Default configuration	The system default prompt is " KYLAND".
configuration mode	Global configuration mode SWITCH(Config)#

7.1.9 reboot

Features	Warm-start the switch.
command format	reboot
illustrate	The user can use this command to restart the switch without turning off the power.
configuration mode	Privileged User Configuration Mode SWITCH#

7.1.10 set default

Features	Restore the factory settings of the switch.
command format	set default
illustrate	Restore the factory settings of the switch, that is, all the configurations made by the user on the switch disappear. After the user restarts the switch, the prompt that appears is the same as when the switch is powered on for the first time. Note: After configuring this command, you must execute the write command. After the configuration is preserved, restart the switch to restore the switch to the factory settings.
configuration mode	Privileged User Configuration Mode SWITCH#

7.1.11 language

Features	Sets the language type of the displayed help information.
command format	language {chinese english}
parameter	chinese : Chinese display; english : Display in English.
Default configuration	The system defaults to English display.
illustrate	SICOM3028GPT provides help information in two languages, and users can choose the language type according to their own preferences. If the system is restarted, the help display information will return to English display.
configuration mode	Privileged User Configuration Mode SWITCH#

7.1.12 save

Features	Save the current runtime configuration parameters to Flash Memory.
command format	save
illustrate	When a set of configurations is completed and the predetermined function has been achieved, the current configuration should be saved in the Flash, so that the system can automatically restore to the previously saved configuration when the system is accidentally shut down or powered off. Equivalent to the copy running-config startup-config command.
configuration mode	Privileged User Configuration Mode SWITCH#

mode	
------	--

7.2 Maintenance and debugging commands

When the user configures the switch, it is necessary to check whether the configuration is correct and whether the switch meets the expectations and works normally; or when the network fails, the user needs to diagnose the fault. SICOM3028GPT provides various debugging such as ping, telnet, show, and debug for this purpose. command to help users check the system configuration, running status, and find the cause of the failure.

Table 9 Configuration command

Order	configuration mode	Features
ping	Privileged User Configuration Mode SWITCH#	The switch sends an ICMP request packet to the remote device to check whether the switch and the remote device are reachable.
monitor no monitor	Privileged User Configuration Mode SWITCH#	Enable the display of debugging information on the Telnet client, and disable the function of displaying debugging information on the Console side; Disable the function of displaying debugging information on the Telnet client, and restore the function of displaying debugging information on the console side.
telnet	General User Configuration Mode SWITCH>	Log in to the remote host by Telnet.
telnet-server enable no telnet-server enable	Global configuration mode SWITCH(Config)#	Open the Telnet server function of the switch; Disable the Telnet server function of the switch.
telnet-server securityip no telnet-server securityip	global mode	Configure the switch as the Telnet server to allow the secure IP address of the Telnet client to log in; Deletes the secure IP address of the specified Telnet client.
tracert	General User Configuration Mode SWITCH>	This command is used to test the gateway that data packets pass through from the sending device to the destination device, check whether

		the network is reachable, and locate the network fault.
show clock	Privileged User Configuration Mode SWITCH#	Displays the current clock of the system.
show debugging	Privileged User Configuration Mode SWITCH#	Displays the status of debug switches.
show flash	Privileged User Configuration Mode SWITCH#	Displays files and sizes saved in flash.
show history	Privileged User Configuration Mode SWITCH#	Displays the history commands entered recently by the user.
show memory-info	Privileged User Configuration Mode SWITCH#	Displays the contents of the specified memory area.
show running-config	Privileged User Configuration Mode SWITCH#	Displays the switch parameter configuration that takes effect in the current running state.
show startup-config	Privileged User Configuration Mode SWITCH#	Displays the switch parameter configuration written in the Flash Memory in the current running state, which is usually the configuration file used when the switch is powered on next time.
show switchport interface	Privileged User Configuration Mode SWITCH#	Displays the VLAN port mode and VLAN number of the switch port and the trunk port information of the switch.
show tcp	Privileged User Configuration Mode SWITCH#	Displays the current TCP connections established with the switch.
show udp	Privileged User Configuration Mode SWITCH#	Displays the current UDP connections established with the switch.
show version	Privileged User Configuration Mode SWITCH#	Display switch version information.

7.2.1 ping

Features	The switch sends an ICMP request packet to the remote device to check whether the switch and the remote device are reachable.
command format	ping [ip_addr]
parameter	<i>ip_addr</i> : The IP address of the destination host to be pinged, in dotted decimal format.
Default configuration	Send 5 ICMP request packets; the packet size is 56 bytes; the timeout period is 2 seconds.
illustrate	When the user enters the ping command and press Enter, the system provides an interactive configuration mode for the user, and the user can define the parameter values of ping by himself.
configuration mode	Privileged User Configuration Mode SWITCH#

7.2.2 telnet

7.2.2.1 introduce

Telnet is a simple remote terminal protocol. Users can use Telnet to register (ie log in) to another remote host (using an IP address or host name) at their location through a TCP connection. Telnet can transmit the user's keystrokes to the remote host, and can also return the output of the remote host to the user's screen through a TCP connection. This service is transparent because the user feels that the keyboard and monitor are directly connected to the remote host.

Telnet uses the client-server mode, the local system is the Telnet client, and the remote host is the Telnet server. SICOM3028GPT can be used as both Telnet server and Telnet client.

When SICOM3028GPT is used as a Telnet server, users can log in to SICOM3028GPT through Telnet through the Telnet client software that comes with Windows or other operating systems, as described in the previous chapter on in-band management. When SICOM3028GPT acts as a Telnet server, it can establish TCP connections with up to 5 Telnet clients at the same time.

When used as a Telnet client, use the telnet command in the privileged user configuration mode of the switch to log in to other remote hosts. When SICOM3028GPT acts as a Telnet

client, it can only establish a TCP connection with one remote host. If you want to establish a connection with another remote host, you must first disconnect the TCP connection with the last remote host.

7.2.2.2 CLI configuration

7.2.2.2.1 monitor

Features	Enable the display of debugging information on the Telnet client, and disable the function of displaying debugging information on the Console side; Disable the function of displaying debugging information on the Telnet client, and restore the function of displaying debugging information on the console side.
command format	monitor no monitor
illustrate	Usually, when a Telnet client accesses the switch, if the debugging information is enabled, the debugging information will not be displayed on the Telnet interface, but on the hyperterminal connected to the Console port. Use this command to display the debugging information on the specified Telnet terminal. interface rather than Console or other Telnet terminal interfaces.
configuration mode	Privileged User Configuration Mode SWITCH#

7.2.2.2.2 telnet

Features	Log in to the remote host in Telnet mode.
command format	telnet [ip_addr] [port]
parameter	<i>ip_addr</i> : IP address of the remote host, in dotted decimal format; <i>port</i> : Port number, the value ranges from 0 to 65535.
illustrate	This command is used when the switch acts as a Telnet client. Users can log in to the remote host through this command for configuration. When the switch acts as a Telnet client, it can only establish a TCP connection with one remote host. If you want to establish a connection with another remote host, you must first disconnect the TCP connection with the last remote host. To disconnect from the remote host, you can use the shortcut "CTRL+ ". Enter the keyword Telnet directly without adding any parameters, and the user will enter the Telnet configuration mode.
configuration	General User Configuration Mode SWITCH>

mode	
------	--

7.2.2.2.3 telnet-server enable

Features	Open the Telet server function of the switch; Disable the Telnet server function of the switch.
command format	telnet-server enable no telnet-server enable
Default configuration	By default, the Telnet server function is enabled.
illustrate	This command can only be used under the Console. Administrators can use this command to allow or deny Telnet clients to log in to the switch.
configuration mode	Global configuration mode SWITCH(Config)#

7.2.2.2.4 telnet-server securityip

Features	Configure the switch as the Telnet server to allow the secure IP address of the Telnet client to log in; Deletes the secure IP address of the specified Telnet client.
command format	telnet-server securityip ip_addr no telnet-server securityip ip_addr
parameter	<i>ip_addr</i> : The secure IP address of the switch that can be accessed, in dotted decimal format.
Default configuration	The system does not configure any secure IP address by default.
illustrate	Before a secure IP address is configured, the IP address of the Telnet client logging in to the switch is not restricted; after the secure IP address is configured, only the host with the secure IP address can Telnet to the switch for configuration. The switch allows configuration of multiple secure IP addresses.
configuration mode	Global configuration mode SWITCH(Config)#

7.2.3 traceroute

Features	This command is used to test the gateway that data packets pass through from the sending device to the destination device, check whether the network is reachable, and locate the network fault.
command	traceroute {ip_addr host hostname} [hops hops] [timeout timeout]

format	
parameter	<i>ip_addr</i> : IP address of the destination host, in dotted decimal format; <i>hostname</i> : the hostname of the remote host; <i>hops</i> : The maximum number of gateways that Traceroute passes through; <i>timeout</i> : Packet timeout, in milliseconds, ranging from 100 to 10000.
Default configuration	The default number of gateways that the data packet can pass through is 16, and the timeout period is 2000 milliseconds.
illustrate	Traceroute is generally used to locate the fault when the destination network is unreachable.
configuration mode	General User Configuration Mode SWITCH>

7.2.4 show clock

Features	Displays the current clock of the system.
command format	show clock
illustrate	By checking the system date and clock, users can find that if the system time is wrong, they can adjust it in time.
configuration mode	Privileged User Configuration Mode SWITCH#

7.2.5 show debugging

Features	Displays the status of debug switches.
command format	show debugging
illustrate	If the user needs to check which debugging switches are currently turned on, run the show debugging command.
configuration mode	Privileged User Configuration Mode SWITCH#

7.2.6 show flash

Features	Displays files and sizes saved in flash.
command format	show flash
configuration mode	Privileged User Configuration Mode SWITCH#

7.2.7 show history

Features	Displays the history commands entered recently by the user.
command format	show history
illustrate	The system saves up to 10 historical commands recently entered by the user. When entering a command, the user can use the up and down cursor keys or their equivalent keys (ctrl+p and ctrl+n) to access the historical commands.
configuration mode	Privileged User Configuration Mode SWITCH#

7.2.8 show memory-info

Features	Displays the contents of the specified memory area.
command format	show memory-info
illustrate	This command is used to debug the switch. The command interactively prompts the user to enter the first memory address of the information to be displayed and the number of output words. The displayed information is divided into three parts: address, hexadecimal display of information and character display.
configuration mode	Privileged User Configuration Mode SWITCH#

7.2.9 show running-config

Features	Displays the switch parameter configuration that takes effect in the current running state.
command format	show running-config
Default configuration	The configuration parameters that are in effect are not displayed if they are the same as the default working parameters.
illustrate	After the user completes a set of configurations, and needs to verify whether the configuration is correct, he can execute the show running-config command to view the currently effective parameters.
configuration mode	Privileged User Configuration Mode SWITCH#

7.2.10 show startup-config

Features	Displays the switch parameter configuration written in the Flash Memory in the current running state, which is usually the configuration file used when the switch is powered on next time.
command format	show startup-config
Default configuration	From If the configuration parameters read from the Flash are the same as the default working parameters, they will not be displayed.
illustrate	show running-config The difference from the show startup-config command is that after the user completes a set of configurations, the configuration can be seen through show running-config, but no configuration can be seen through show startup-config. But if the user passes write command to save the currently effective configuration to Flash Memory, the display result of show running-config is the same as that of show startup-config.
configuration mode	Privileged User Configuration Mode SWITCH#

7.2.11 show switchport interface

Features	Displays the VLAN port mode and VLAN number of the switch port and the trunk port information of the switch.
command format	show switchport interface [ethernet interface_list]
parameter	<i>interface_list</i> : Port number or port list, which can be any port information that exists in the switch.
configuration mode	Privileged User Configuration Mode SWITCH#

7.2.12 show tcp

Features	Displays the current TCP connections established with the switch.
command format	show tcp
configuration mode	Privileged User Configuration Mode SWITCH#

7.2.13 show udp

Features	Displays the current UDP connections established with the switch.
command format	show udp
configuration mode	Privileged User Configuration Mode SWITCH#

7.2.14 show version

Features	Display switch version information.
command format	show version
illustrate	Use this command to view the version information of the switch, including hardware version and software version information.
configuration mode	Privileged User Configuration Mode SWITCH#

7.3 IP address configuration

All Ethernet ports of SICOM3028GPT default to Layer 2 (DataLink Layer) ports for Layer 2 forwarding. A VLAN interface (Interface VLAN) represents the function of a Layer 3 interface of a VLAN, and an IP address can be configured, which is also the IP address of the switch. All configuration commands related to VLAN interface can be configured in VLAN interface mode. SICOM3028GPT provides users with three ways to configure the IP address:

- Manual configuration
- BootP method
- DHCP mode

Manually configure the IP address, that is, the user assigns an IP address to the switch. In BootP/DHCP mode, the switch acts as a BootP/DHCP client and sends a BootPRequest (request packet for obtaining an address) broadcast packet to the BootP/DHCP Server, and the BootP/DHCP Server assigns the address to the switch after receiving the request. In addition, SICOM3028GPT also has the function of DHCP Server, which can dynamically assign network parameters such as IP address, gateway address and DNS server address to DHCP Client. For specific DHCP Server configuration, see the following chapters.

Table 10 configuration command

Order	configuration mode	Features
ip address no ip address	VLAN interface configuration mode SWITCH(Config-If-Vlan100)#	Set the IP address and mask of the specified VLAN interface of the switch; Delete the IP address configuration.
ip bootp-client enable no ip bootp-client enable	VLAN interface configuration mode SWITCH(Config-If-Vlan100)#	Enable the switch as a BootP Client, and obtain the IP address and gateway address through BootP negotiation; Disable the BootP Client function, and release the address and gateway address obtained by BootP.
ip dhcp-client enable no ip dhcp-client enable	VLAN interface configuration mode SWITCH(Config-If-Vlan100)#	Enable the switch as a DHCP Client, and obtain the IP address and gateway address through DHCP negotiation; Disable the DHCP Client function, and release the address and gateway address obtained by DHCP.

7.3.1 ip address

Features	Set the IP address and mask of the specified VLAN interface of the switch; Delete the IP address configuration.
command format	ip address ip-address mask [secondary] no ip address [ip-address mask] [secondary]
parameter	<i>ip_address</i> : IP address, in dotted decimal format; <i>mask</i> : Subnet mask, in dotted decimal format; secondary : Indicates that the configured IP address is the slave IP address.
Default configuration	The switch does not have an IP address when it leaves the factory.
illustrate	To configure an IP address for the switch, users must first create a VLAN interface.
configuration mode	VLAN interface configuration mode SWITCH(Config-If-Vlan100)#

7.3.2 ip bootp-client enable

Features	Enable the switch as a BootP Client, and obtain the IP address and gateway address through BootP negotiation; Disable the BootP Client function, and release the address and gateway address
----------	---

	obtained by BootP.
command format	ip bootp-client enable no ip bootp-client enable
Default configuration	The BootP Client function is disabled by default.
illustrate	Obtaining an IP address through BootP is mutually exclusive with manual configuration and obtaining an IP address through DHCP.
configuration mode	VLAN interface configuration mode SWITCH(Config-If-Vlan100)#

7.3.3 ip dhcp-client enable

Features	Enable the switch as a DHCP Client, and obtain the IP address and gateway address through DHCP negotiation; Disable the DHCP Client function, and release the address and gateway address obtained by DHCP.
command format	ip dhcp-client enable no ip dhcp-client enable
Default configuration	The DHCP Client function is disabled by default.
illustrate	Obtaining an IP address through DHCP is mutually exclusive with manual configuration and obtaining an IP address through BootP, and it is not allowed to enable the two methods of obtaining an IP address at the same time.
configuration mode	VLAN interface configuration mode SWITCH(Config-If-Vlan100)#

7.4 SNMP configuration

7.4.1 Introduction to SNMP

SNMP (Simple Network Management Protocol) is a standard protocol for managing the Internet, called Simple Network Management Protocol, which is widely used in the management of computer networks. SNMP is an evolving protocol. SNMP v1 [RFC1157] is the first version of SNMP. The SNMPv1 protocol is simple and easy to implement, and is supported by many manufacturers. Later, after the enhancement of function and security, SNMP developed to the second version, SNMPv2. SNMPv2 is a natural progress of SNMPv1. It is still based on SNMPv1, so we will focus on SNMPv1. In the following, SNMP refers to

SNMPv1 unless otherwise specified.

The SNMP protocol provides a relatively straightforward method of exchanging management information between two points in the network. SNMP adopts the polling message query mechanism and the connectionless transport layer protocol UDP to transmit messages, so it can be well supported by the existing computer network.

The SNMP protocol adopts the management station/agent mode, so the SNMP structure consists of two parts: NMS (Network Management Station) network management station, which is a workstation running the network management software client program that supports the SNMP protocol, and plays a core role in the network management of SNMP. . Agent is the server-side software running on the managed network device and directly manages the managed objects. The NMS uses the means of communication to manage the managed objects through the Agent.

The client/server mode is adopted between the NMS and the Agent of SNMP to communicate through standard messages. The NMS sends a request and the Agent responds. There are 5 message types in SNMP:

- Get-Request
- Get-Response
- Get-Next-Request
- Set-Request
- Trap

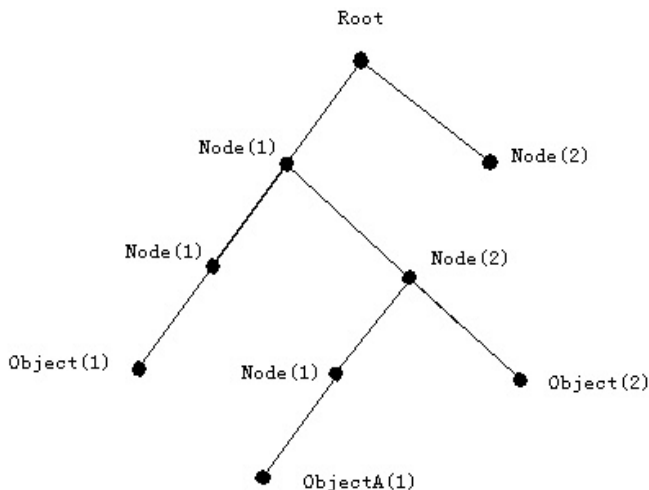
The NMS sends requests to the Agent to query and set management variables through the Get-Request, Get-Next-Request and Set-Request messages. After the Agent receives the request, it replies to the request with the Get-Response message. In some special cases, such as when the port of the network device is UP/DOWN or the network topology changes, the Agent will actively send a Trap message to the NMS to notify the NMS that an abnormal event has occurred. Of course, the NMS can also alert some abnormal situations by itself by setting the RMON function. When the set alarm event is triggered, the Agent will send Trap information or record it in the Log according to the settings.

The security mechanism of the SNMP protocol is not very sound, and the security protection method is relatively simple, mainly using the community string (Community String).

The community string is equivalent to the access password set on the Agent side. Read and write access permissions are set for each community string on the Agent side. The NMS must contain the community string in the packet sent to the Agent, so that the Agent can be accessed within the corresponding read and write permissions.

7.4.2 Introduction to MIB

The network management information that the NMS can access is precisely defined and organized in a management information database, namely MIB. The so-called MIB (Management Information Base) is a precise definition of information that can be accessed through network management protocols. It uses a hierarchical, structured form to define the management information that can be obtained from monitored network devices. ISO ASN.1 defines a tree structure for MIBs. Each MIB uses this tree structure to organize all available information. Each node of the tree contains an OID object identifier (Object Identifier) and an A short textual description of the node. OID is a set of integers separated by periods, which names a node and can be used to indicate the position of the node in the MIB tree structure, as shown in the following Picture:



Picture 14 ASN.1 tree instance

On this Picture, the OID of object A is 1.2.1.1. Through this unique OID, NMS can access this object without ambiguity, thereby obtaining the standard variables contained in this object. MIB defines a set of standard variables of monitored network devices according to this

structure.

If you need to browse the variable information in the MIB of the Agent, you need to run the MIB browser software on the NMS, such as the MIB browser in Kyvision, the network management software of KYLAND Company. The MIB on the Agent generally includes two parts: the public MIB and the private MIB. The public MIB defines the network management information that is public and accessible to all NMSs; the private MIB defines the attribute information specific to each device, and the NMS needs the device manufacturer. The support can only be browsed and controlled.

MIB-I [RFC1156] was the first version of the SNMP public MIB library, which was later expanded and superseded by MIB-II [RFC1213], which retained MIB-I's object identifiers in the original MIB tree. MIB-II contains many subtrees, which we call groups. The objects in these groups cover various functional domains of network management. NMS can obtain corresponding network management information by accessing the MIB library of SNMP Agent.

SICOM3028GPT can be used as SNMP Agent, supports SNMPv1/v2c, supports basic MIB-II, RMON public MIB, and also supports BRIDGE MIB and other related public MIBs.

7.4.3 Introduction to RMON

RMON is the most important extension to the basic system of the SNMP standard. RMON is a set of MIB definitions, and its role is to define standard network monitoring functions and interfaces, enabling communication between SNMP-based management terminals and remote monitors. RMON provides an effective and efficient way to monitor subnet-wide behavior.

The MIB is divided into 10 groups, SICOM3028GPT supports the most commonly used groups 1, 2, 3, 9, namely:

Statistics: Basic usage and error statistics for each subnet monitored by the maintenance agent.

History group: Records periodic statistical samples of information available from the

statistics group.

Alarm group (alarm): Allows management console personnel to set sampling intervals and alarm thresholds for any counts or integers logged by the RMON agent.

Event group (event):A table of all events generated by the RMON agent.

Among them, the alarm group depends on the implementation of the event group. Statistics group and historical group are to display some current or previous subnet statistics. Alarm groups and event groups provide a method to monitor any integer data changes on the network, and provide some warning actions (send Trap or record Log) when the data is abnormal.

7.4.4 CLI configuration

Table 11 configuration command

Order	configuration mode	Features
snmp-server enable no snmp-server enable	Global configuration mode SWITCH(Config)#	Enable SNMP function; Disable the SNMP function.
snmp-server community	Global configuration mode SWITCH(Config)#	Configure the community string.
snmp-server security-ip	Global configuration mode SWITCH(Config)#	Configure the NMS secure IP address.
snmp-server trap no snmp-server enable	Global configuration mode SWITCH(Config)#	Configure the device to send Trap messages; Sending Trap messages is prohibited.
snmp-server v3-access	Global configuration mode SWITCH(Config)#	Configure SNMPv3 user security mode access authorization.
snmp-server v3-context	Global configuration mode SWITCH(Config)#	Configure the SNMPv3 user security mode context.
snmp-server v3-group	Global configuration mode SWITCH(Config)#	Configure the SNMPv3 user security mode security group.
snmp-server v3-user	Global configuration mode SWITCH(Config)#	Configure SNMPv3 user security mode users.
snmp-server v3-view	Global configuration mode	Configure the SNMPv3 user

	SWITCH(Config)#	security mode MIB view.
rmon	Global configuration mode SWITCH(Config)#	Configure RMON function;
show snmp	Privileged User Configuration Mode SWITCH#	Display SNMP information.
debug snmp-server no debug snmp-server	Privileged User Configuration Mode SWITCH#	Turn on the SNMP debugging switch; Disable the SNMP debugging switch.

7.4.4.1 snmp-server enable

Features	Turn on the SNMP proxy server function; Disable the SNMP proxy server function.
command format	snmp-server enable no snmp-server enable
Default configuration	By default, the SNMP proxy server function is disabled.
illustrate	To configure and manage the switch through the network management software, you must first use the snmp-server enable command to enable the SNMP proxy server function of the switch.
configuration mode	Global configuration mode SWITCH(Config)#

7.4.4.2 snmp-server community

Features	Configure the community string for the switch.
command format	snmp-server community {ro rw delete} string
parameter	ro :Read-only access to MIB library; rw :Read and write access to MIB library; delete : delete the configured community string; <i>string</i> : Community string.
illustrate	The switch supports up to 4 community strings.
configuration mode	Global configuration mode SWITCH(Config)#

7.4.4.3 snmp-server port

Features	Configure the SNMP service port.
----------	----------------------------------

command format	snmp-server port {agent trap } port
parameter	agent : Configure the proxy port; trap : Configure the trap port; <i>port</i> : The port number.
configuration mode	Global configuration mode SWITCH(Config)#

7.4.4.4 snmp-server security-ip

Features	Configure the secure IP address of the NMS network management station that accesses the switch.
command format	snmp-server security-ip { <i>addip_address</i> <i>deleteip_address</i> enable disable }
parameter	add : Add a secure IP address; delete : delete the secure IP address; <i>ip_address</i> : The secure IP address of the NMS network management station, in dotted decimal format; enable : enable this function; disable : Disable this function.
illustrate	Only the IP address of the NMS management station is consistent with the security IP address set by this command, the SNMP packets sent by it will be processed by the switch.
configuration mode	Global configuration mode SWITCH(Config)#

7.4.4.5 snmp-server trap

Features	Configure the device to send Trap messages; Disable the device from sending Trap messages.
command format	snmp-server trap { <i>addip_address</i> { v1 v2c v3 } <i>deleteip_address</i> enable } no snmp-server trap enable
parameter	add : add a network management station; <i>ip_address</i> : IP address; v1 : SNMPv1; v2c : SNMPv2c; v3 : SNMPv3; delete : delete the network management station;

	enable: Enable sending trap messages.
Default configuration	By default, the system prohibits sending Trap messages.
illustrate	When the device is allowed to send Trap messages, if the port of the device is Down/Up or the system is Down/Up, the device will send the Trap message to the management station that receives the Trap message.
configuration mode	Global configuration mode SWITCH(Config)#

7.4.4.6 snmp-server v3-access

Features	Configure SNMPv3 user security mode access authorization;
command format	snmp-server v3-access
configuration mode	Global configuration mode SWITCH(Config)#

7.4.4.7 snmp-server v3-context

Features	Configure SNMPv3 user security model context;
command format	snmp-server v3-context
configuration mode	Global configuration mode SWITCH(Config)#

7.4.4.8 snmp-server v3-group

Features	Configure the SNMPv3 user security model security group;
command format	snmp-server v3-group
configuration mode	Global configuration mode SWITCH(Config)#

7.4.4.9 snmp-server v3-user

Features	Configure SNMPv3 users;
command format	snmp-server v3-user
configuration mode	Global configuration mode SWITCH(Config)#

7.4.4.10 snmp-server v3-view

Features	Configure SNMPv3 MIB view;
command format	snmp-server v3-view
configuration mode	Global configuration mode SWITCH(Config)#

7.4.4.11 rmon

Features	Configure the RMON function of the switch;
command format	rmon
Default configuration	By default, the system disables RMON.
configuration mode	Global configuration mode SWITCH(Config)#

7.4.4.12 show snmp

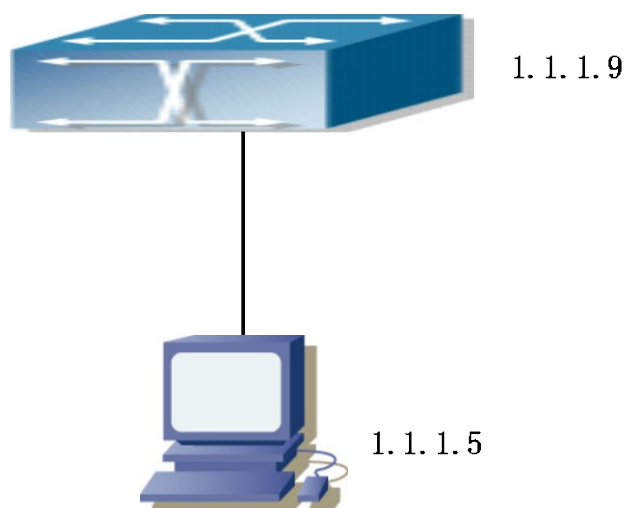
Features	Display SNMP information.
command format	show snmp {port statistics status trap v3-access v3-context v3-group v3-user v3-view}
parameter	<p>port: port information;</p> <p>statistics:Statistics;</p> <p>status:status information;</p> <p>trap: trap information;</p> <p>v3-access: SNMPv3 user security mode access authorization information;</p> <p>v3-context: SNMPv3 user security mode context information;</p> <p>v3-group: SNMPv3 user security mode user group information;</p> <p>v3-user: SNMPv3 user security mode user information;</p> <p>v3-view: SNMPv3 user security mode MIB view information.</p>
configuration mode	Privileged User Configuration Mode SWITCH#

7.4.4.13 debug snmp-server

Features	Turn on the SNMP debugging switch; Disable the SNMP debugging switch.
command	debug snmp-server

format	no debug snmp-server
illustrate	When a user encounters a problem when using SNMP, he or she can turn on the SNMP debugging switch to find the cause of the problem.
configuration mode	Privileged User Configuration Mode SWITCH#

7.4.5 Typical configuration example



Picture 15 SNMP configuration example

The IP address of the management station (NMS) is 1.1.1.5; the IP address of the switch (Agent) is 1.1.1.9.

Case 1: The network management software of the management station uses the SNMP protocol to obtain data from the switch.

The configuration on the switch side is as follows:

```
Switch(Config)#snmp-server enable
Switch(Config)#snmp-server community rw private
Switch(Config)#snmp-server community ro public
Switch(Config)#snmp-server securityip 1.1.1.5
```

In this way, the management station can use private as the community string to read and write access to the switch, and can also use public as the community string to access the switch for read-only.

Case 2: The management station needs to receive the Trap message from the switch (Note: the management station may have set the verification of the Trap community string, so this example assumes that the Trap verification community string of the management station is dcstrap).

The configuration on the switch side is as follows:

```
Switch(Config)#snmp-server host 1.1.1.5 dcstrap
```

```
Switch(Config)#snmp-server enable traps
```

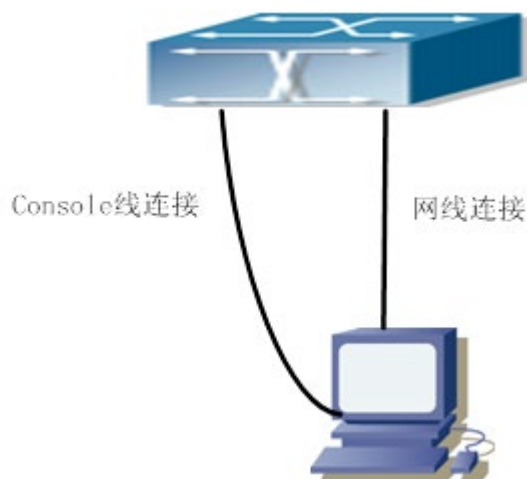
7.5 Switch upgrade

SICOM3028GPT provides users with switch upgrades in two modes:

1. BootROM mode;
2. TFTP upgrade and FTP upgrade in Shell mode.

7.5.1 BootROM mode

There are two upgrade methods for upgrading the switch in BootROM mode: TFTP and FTP. You can select the upgrade method through the command settings in BootROM.



Picture 16 Typical topology for switch upgrade in BootROM mode

The upgrade steps are as follows:

first step:

As shown on the Picture, a PC is used as the console of the switch, and the Ethernet port of the console is connected to the Ethernet port of the switch. The FTP/TFTP server software and the img file to be upgraded are installed on the PC.

Step 2:

During the switch startup process, press and hold the "ctrl+p" key until the switch enters the BootROM monitoring mode. The operation is displayed as follows:

KYLAND

Copyright (c) 2003 by KYLAND

All rights reserved.

Testing RAM...

67,108,864 RAM OK.

Loading BootROM...

Starting BootRom...

AT49BV160

CPU: PowerPC MPC8245MH266, Revision 12

Version: 1.1.4

Creation date: Jul 17 2003, 14:01:12

Attached TCP/IP interface to sc0.

[Boot]:

[Boot]:

[Boot]:

third step:

In BootROM mode, run the setconfig command to set the IP address, mask, server IP address, mask and upgrade mode of TFTP or FTP in BootROM mode. For example, set the local address to 192.168.1.2/24 and the PC address to 192.168.1.66/24, select the TFTP upgrade method, and configure as follows:

[Boot]: config net

Host IP Address: 10.1.1.1 192.168.1.2

Server IP Address: 10.1.1.2 192.168.1.66

FTP(1) or TFTP(2): 1 2

Network interface configure OK.

[Boot]:

the fourth step:

Open the FTP/TFTP server in the PC. If it is a TFTP server, run the TFTP Server program; if it is an FTP server, run the FTP Server program. When downloading the upgraded version to the switch, please check the connection status between the server and the upgraded switch first, and use the ping command on the server side. After the ping is successful, execute the load command in the BootROM mode of the switch; if the ping fails, check the reason. Here is the configuration for updating the system image file:

[Boot]: get nos.img

Loading...

entry = 0x10010

size = 0x1077f8

the fifth step:

In BootROM mode, execute the command write nos.img. The following is a save of the

updated system image file:

[Boot]: write nos.img

Programming...

Program OK.

[Boot]:

Step 6:

The switch is upgraded successfully. In BootROM mode, run the run command to return to the CLI configuration interface.

[Boot]:run (or reboot)

Other commands in BOOTROM mode

1. DIR command

Used to display existing files in FLASH.

[Boot]: dir

boot.rom 327,440 1900-01-01 00:00:00 --SH

boot.conf 83 1900-01-01 00:00:00 --SH

nos.img 2,431,631 1980-01-01 00:21:34 ----

startup-config 2,922 1980-01-01 00:09:14 ----

temp.img 2,431,631 1980-01-01 00:00:32 ----

2. CONFIG RUN command

It is used to set the IMG file to be executed when the system starts, and the configuration file to be executed when the configuration is restored.

[Boot]: config run

Boot File: [nos.img] nos1.img

Config File: [boot.conf]

7.5.2 FTP/TFTP upgrade

7.5.2.1 introduce

FTP (File Transfer Protocol)/TFTP (Trivial File Transfer Protocol) are file transfer protocols, which are at the fourth layer in the TCP/IP protocol suite, that is, an application layer protocol, mainly used between hosts and between hosts and switches. Transfer files. They all use client-server mode for file transfer. Here's how they differ.

FTP is carried on top of TCP and provides reliable connection-oriented data stream transmission services, but it does not provide file access authorization, and a simple authentication mechanism (authentication is achieved by transmitting user names and passwords in clear text). When FTP transfers files, two connections are established between the client and the server: a control connection and a data connection. First, the FTP client sends out a transfer request, establishes a control connection with port 21 of the server, and negotiates a data connection through the control connection.

There are two ways to connect data:

One is active connection. The client actively tells the server the address and port number used for data transmission, and the control connection will remain until the data transmission is completed. Then the server uses port 20 to establish a data connection with the address and port number provided by the client under the condition that port 20 is not used, and transmits data; if port 20 is in use, it can be reused by setting port 20, the server The data connection is established by the system automatically generating another port number.

Another way is passive connection. The client tells the server to establish a passive connection through the control connection, the server establishes its own data monitoring port, and tells the client of this port through the control connection, and the client actively establishes a data connection with the port of the specified address.

Since the data connection is through the specified address and port number, there is also a third party to provide data connection services.

TFTP is carried over UDP, It provides unreliable data stream transmission services, and also does not provide user authentication mechanism and file operation authorization based

on user permissions; it ensures the correct transmission of data by sending packets, replying, and retransmitting overtime. The advantage of TFTP over FTP is that it provides a simple, inexpensive file transfer service.

SICOM3028GPT realizes the functions of FTP/TFTP client and server. When SICOM3028GPT acts as an FTP/TFTP client, it can download configuration files or system files from a remote FTP/TFTP server (which can be a host and other switches) without affecting the normal operation of the switch (the FTP client can view the server The file list on the SICOM3028GPT can also upload the current configuration file or system file of the SICOM3028GPT to the remote FTP/TFTP server (which can be the host and other switches); when the SICOM3028GPT is used as the FTP/TFTP server, it can also provide Authorized FTP/TFTP clients provide services for uploading and downloading files (FTP server also provides the function of transferring file lists on the server).

The following introduces the terms often used in FTP/TFTP:

ROM: Abbreviation for EPROM, erasable read-only register. SICOM3028GPT uses FLASH memory stick instead of EPROM.

SDRAM: Switch memory, used for system software operation and storage of configuration sequences.

FLASH: Flash memory for saving system files and configuration files.

System Files: Include system image files and boot files.

System image file: Refers to the compressed file of the switch hardware driver and software support program, that is, the IMG upgrade file we usually say. SICOM3028GPT system image file is only allowed to be saved in FLASH. SICOM3028GPT stipulates that in the global configuration mode, the file name of the system image file uploaded through FTP is fixed as nos.img, and the upload of other system IMG files is rejected.

Boot file: Refers to the file that guides the switch initialization, that is, the ROM upgrade file we usually say (if the file is large, it can be compressed into an IMG file). KYLAND boot files are only allowed to be saved in ROM. SICOM3028GPT stipulates that the file name of the boot file is fixed as nos.rom.

Configuration file:Include startup profiles and run profiles. Distinguishing between startup configuration files and running configuration files facilitates backup and update of configurations.

Startup configuration file:Refers to the configuration sequence that the switch takes when it starts up. The SICOM3028GPT startup configuration file is only stored in FLASH, which corresponds to the so-called configuration reservation. In order to prohibit the upload of illegal files and facilitate configuration, SICOM3028GPT stipulates that the startup configuration file name is fixed as startup-config.

Run configuration file:Refers to the configuration sequence that the switch is currently running. The SICOM3028GPT operating configuration file is stored in memory. At present, by using the command write or the command copy running-config startup-config, the running configuration sequence running-config can be saved from the memory to the FLASH, that is, the transition from the running configuration sequence to the startup configuration file is realized, and the configuration retention is formed. In order to prohibit the upload of illegal files and facilitate configuration, SICOM3028GPT stipulates that the name of the running configuration file is fixed as running-config.

Factory configuration file:That is, the factory-config file is the configuration file of the SICOM3028GPT when it leaves the factory. Use the command set default and the command write to restore the configuration file to the factory configuration file after restarting.

7.5.2.2 CLI configuration

When SICOM3028GPT is used as FTP or TFTP client, the configuration is very similar, so this manual describes the configuration when FTP and TFTP are used as client together.

Table 12 configuration command

Order	configuration mode	Features
copy (FTP)	Privileged User Configuration Mode SWITCH#	Download files on the FTP client.
dir	Global configuration mode SWITCH(Config)#	View the list of files on the FTP server.
ftp-server enable	Global configuration mode	Start FTP Server;

no ftp-server enable	SWITCH(Config)#	Disable the FTP Server service and prohibit FTP users from logging in.
ftp-server timeout no ftp-server timeout	Global configuration mode SWITCH(Config)#	Set the data connection idle time limit; Restore default values.
ip ftp password	Global configuration mode SWITCH(Config)#	Configure the FTP login user password.
copy (TFTP)	Privileged User Configuration Mode SWITCH#	Download files on the TFTP client.
tftp-server enable no tftp-server enable	Global configuration mode SWITCH(Config)#	Start TFTP Server; Disable the TFTP Server service and prohibit TFTP users from logging in.
tftp-server retransmission-number	Global configuration mode SWITCH(Config)#	Sets the number of times the tftp server retransmits data.
tftp-server transmission-timeout	Global configuration mode SWITCH(Config)#	Set the tftp server transmission timeout.
show ftp	Privileged User Configuration Mode SWITCH#	Displays the settings of the FTP server parameters.
show tftp	Privileged User Configuration Mode SWITCH#	Displays the settings of TFTP server parameters.

7.5.2.2.1 copy (FTP)

Features	Download files on the FTP client.
command format	copy source_url destination_url [ascii binary]
parameter	<p><i>source_url</i>: The location of the copied source file or directory;</p> <p><i>destination_url</i>: The destination address to which the file or directory is to be copied;</p> <p><i>source_url</i> and <i>destination_url</i>: The specific form varies with the location of the file or directory;</p> <p>ascii: The file transfer uses the ASCII standard;</p> <p>binary: The file transfer uses the binary standard (the default transfer method). When the URL is an FTP address the format is: ftp://<username>:<password>@<ipaddress>/<filename>, where <username> is the FTP user name, <password> is the FTP user password, <ipaddress> is the IP address of the FTP server/client, <filename> is the name of the downloaded file on FTP.</p> <p>Special keywords for filename:</p>

	keywords	source or destination address
	running-config	run configuration file
	startup-config	startup configuration file
	nos.img	System Files
	nos.rom	system startup file
illustrate	<p>This command supports command line prompts, that is, if the user can enter the following command <code>copy <filename> ftp://</code> or <code>copy ftp:// <filename></code> and then press Enter, the system will display the following prompt:</p> <pre>ftp server ip address [xxxx] > ftp username> ftp password> ftp filename></pre> <p>You are required to enter the address, user name, password and file name of the FTP server.</p>	
configuration mode	Privileged User Configuration Mode SWITCH#	

7.5.2.2.2 dir

Features	View the list of files on the FTP server.
command format	dir ftp_server_url
parameter	<i>ftp_server_url</i> of The format is: ftp://<username>:<password>@<ipaddress>, where <username> is the FTP user name, password is the FTP user password, and ipaddress is the IP address of the FTP server.
configuration mode	Global configuration mode SWITCH(Config)#

7.5.2.2.3 ftp-server enable

Features	Start FTP Server; Disable the FTP Server service and prohibit FTP users from logging in.
command format	ftp-server enable no ftp-server enable
Default configuration	By default, the FTP Server is not started.
illustrate	After the FTP server function is enabled, the switch still retains the FTP client function. By default, the system does not start the FTP Server.
configuration	Global configuration mode SWITCH(Config)#

mode	
------	--

7.5.2.2.4 ftp-server timeout

Features	Set the data connection idle time limit; Restore default values.
command format	ftp-server timeout seconds no ftp-server timeout
parameter	<i>seconds</i> : FTP connection idle time, in seconds, ranging from 5 to 4294967295.
Default configuration	The default idle time limit of the system is 600 seconds.
illustrate	When the FTP data connection is idle to achieve more than this value, cut off the FTP control connection
configuration mode	Global configuration mode SWITCH(Config)#

7.5.2.2.5 ip ftp password

Features	Configure the FTP login user password.
command format	ip ftp username password {encrypted plain number} password
parameter	<i>username</i> : The user name of the FTP connection, the value range cannot exceed 16 characters. encrypted : encrypted display password; plain : Display the password in plain text; <i>number</i> : can only be 0 or 7; represent plaintext display and encrypted display passwords respectively; <i>password</i> : The FTP connection uses a password, the value range cannot exceed 16 characters.
Default configuration	The default password used by the system is <i>username@Switchname.domain</i> , where the variable <i>username</i> is the current user name, <i>Switchname</i> is the switch name, and <i>domain</i> is the domain name of the Switch.
configuration mode	Global configuration mode SWITCH(Config)#

7.5.2.2.6 copy (TFTP)

Features	Download files on the TFTP client.
command	copy source_url destination_url [ascii binary]

format											
parameter	<p><i>source_url</i>: The location of the copied source file or directory;</p> <p><i>destination_url</i>: The destination address to which the file or directory is to be copied;</p> <p><i>source_url</i>/<i>destination_url</i>: The exact form of <i>source_url</i> and <i>destination_url</i> varies with the location of the file or directory.</p> <p>ascii: The file transfer uses the ASCII standard;</p> <p>binary: The file transfer uses the binary standard (the default transfer method). When the URL is a TFTP address, the format is: <code>tftp://<ipaddress>/<filename></code>, where <i>ipaddress</i> is the IP address of the TFTP server/client, and <i>filename</i> is the name of the downloaded file on TFTP.</p> <p>Special keywords for filename:</p> <table border="1"> <thead> <tr> <th>keywords</th> <th>source or destination address</th> </tr> </thead> <tbody> <tr> <td>running-config</td> <td>run configuration file</td> </tr> <tr> <td>startup-config</td> <td>startup configuration file</td> </tr> <tr> <td>nos.img</td> <td>System Files</td> </tr> <tr> <td>nos.rom</td> <td>system startup file</td> </tr> </tbody> </table>	keywords	source or destination address	running-config	run configuration file	startup-config	startup configuration file	nos.img	System Files	nos.rom	system startup file
keywords	source or destination address										
running-config	run configuration file										
startup-config	startup configuration file										
nos.img	System Files										
nos.rom	system startup file										
illustrate	<p>This command supports command line prompts, that is, if the user can enter the following command <code>copy <filename> tftp://</code> or <code>copy tftp:// <filename></code> and then press Enter, the system will display the following prompt:</p> <p>tftp server ip address></p> <p>tftp filename></p> <p>You are asked to enter the address and filename of the TFTP server.</p>										
configuration mode	Privileged User Configuration Mode SWITCH#										

7.5.2.2.7 tftp-server enable

Features	<p>Start TFTP Server;</p> <p>Disable the TFTP Server service and prohibit TFTP users from logging in.</p>
command format	<p>tftp-server enable</p> <p>no tftp-server enable</p>
Default configuration	TFTP Server is not started by default.
illustrate	After the TFTP server function is enabled, the switch still retains the TFTP client function. By default, the TFTP Server is not started.
configuration mode	Global configuration mode SWITCH(Config)#

7.5.2.2.8 tftp-server retransmission-number

Features	Sets the number of times the tftp server retransmits data.
command format	tftp-server retransmission-number number
parameter	<i>number</i> : Number of retransmissions, ranging from 1 to 20.
Default configuration	By default, the system retransmits 5 times.
configuration mode	Global configuration mode SWITCH(Config)#

7.5.2.2.9 tftp-server transmission-timeout

Features	Set the tftp server transmission timeout.
command format	tftp-server transmission-timeout seconds
parameter	<i>seconds</i> : Timeout time, the value range is 5~3600s.
Default configuration	The default timeout period of the system is 600s.
configuration mode	Global configuration mode SWITCH(Config)#

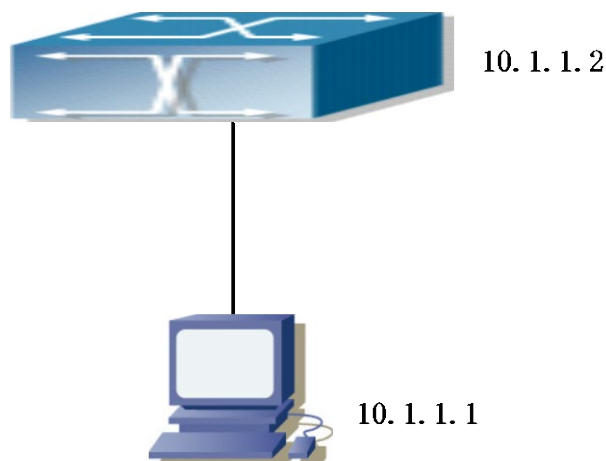
7.5.2.2.10 show ftp

Features	Displays the settings of the FTP server parameters.
command format	show ftp
configuration mode	Privileged User Configuration Mode SWITCH#

7.5.2.2.11 show tftp

Features	Displays the settings of TFTP server parameters.
command format	show tftp
command mode	Privileged User Configuration Mode SWITCH#

7.5.2.3 Typical configuration example



Picture 17 Download the nos.img file as an FTP/TFTP client

Example 1: The switch is used as an FTP/TFTP client. The switch is connected to the computer through a certain port. The computer is an FTP/TFTP server with an IP address of 10.1.1.1. The switch acts as an FTP/TFTP client. The IP address of the management VLAN of the switch is 10.1.1.2. Download the switch's "nos.img" file from your computer.

- FTP configuration:

Computer side configuration:

Start the FTP Server software on the computer, and set the user name as "Switch" and the password as "KYLAND". Put the "12_30_nos.img" file in the corresponding FTP Server directory on the computer.

The configuration steps of the switch are as follows:

```
SWITCH(Config)#inter vlan 1
SWITCH(Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0
SWITCH(Config-If-Vlan1)#no shut
SWITCH(Config-If-Vlan1)#exit
SWITCH(Config)#exit
SWITCH#copy ftp://Switch: KYLAND@10.1.1.1 /12_30_nos.img nos.img
SWITCH#reload
```

After executing the above command, the switch can download the "nos.img" file on the

computer to the FLASH.

- TFTP configuration:

Computer side configuration:

Start the TFTP Server software on the computer, and put the "nos.img" file in the corresponding TFTP Server directory on the computer.

The configuration steps of the switch are as follows:

```
SWITCH(Config)#inter vlan 1
SWITCH(Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0
SWITCH(Config-If-Vlan1)#no shut
SWITCH(Config-If-Vlan1)#exit
SWITCH(Config)#exit
SWITCH#copy tftp://10.1.1.1/12_30_nos.img nos.img
SWITCH#reload
```

Example 2: The switch is used as an FTP server. The switch is connected to the computer through a certain port. The switch acts as an FTP server and the computer acts as an FTP client. The "nos.img" file on the switch is transferred to the computer and saved as 12_25_nos.img.

The configuration steps of the switch are as follows:

```
SWITCH(Config)#inter vlan 1
SWITCH(Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0
SWITCH(Config-If-Vlan1)#no shut
SWITCH(Config-If-Vlan1)#exit
SWITCH(Config)#ftp-server enable
SWITCH(Config)#ip ftp username Switch
SWITCH(Config)#ip ftp password 0 KYLAND
```

Computer side configuration:

Log in to the switch through the FTP client software, the user name is "Switch", the password

is "KYLAND", and the "nos.img" file on the switch is downloaded to the computer through the "get nos.img 12_30_nos.img" command.

Example 3: The switch is used as a TFTP server. The switch is connected to the computer through a certain port, the switch acts as a TFTP server, and the computer acts as a TFTP client, and transfers the "nos.img" file on the switch to the computer.

The configuration steps of the switch are as follows:

```
SWITCH(Config)#inter vlan 1
```

```
SWITCH(Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0
```

```
SWITCH(Config-If-Vlan1)#no shut
```

```
SWITCH(Config-If-Vlan1)#exit
```

```
SWITCH(Config)#tftp-server enable
```

Computer side configuration:

Log in to the switch through the TFTP client software, and download the "nos.img" file on the switch to the computer through the "tftp" command.

Example 4: The switch is used as an FTP/TFTP client. The switch is connected to the computer through a certain port. The computer is an FTP/TFTP server with an IP address of 10.1.1.1. It records multiple user context configuration files of the switch. The switch acts as an FTP/TFTP client, and the IP address of the management VLAN of the switch is 10.1.1.2. Download the user context configuration file of the switch from the computer and save it to the FLASH of the switch.

- FTP configuration:

Computer side configuration:

Start the FTP Server software on the computer, and set the user name as "Switch" and the password as "KYLAND". Put the "Profile1", "Profile2", and "Profile3" files in the corresponding FTP Server directory on the computer.

The configuration steps of the switch are as follows:

```
SWITCH(Config)#inter vlan 1
SWITCH(Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0
SWITCH(Config-If-Vlan1)#no shut
SWITCH(Config-If-Vlan1)#exit
SWITCH(Config)#exit
SWITCH#copy ftp://Switch: KYLAND@10.1.1.1 /Profile1 Profile1
SWITCH#copy ftp://Switch: KYLAND@10.1.1.1 /Profile2 Profile2
SWITCH#copy ftp://Switch: KYLAND@10.1.1.1 /Profile3 Profile3
```

After executing the above command, the switch can download the user profile configuration file on the computer to the FLASH.

- TFTP configuration:

Computer side configuration:

Start the TFTP Server software on the computer, and put the "Profile1", "Profile2", and "Profile3" files in the corresponding TFTP Server directory on the computer.

The configuration steps of the switch are as follows:

```
SWITCH(Config)#inter vlan 1
SWITCH(Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0
SWITCH(Config-If-Vlan1)#no shut
SWITCH(Config-If-Vlan1)#exit
SWITCH(Config)#exit
SWITCH#copy tftp://10.1.1.1/ Profile1 Profile1
SWITCH#copy tftp://10.1.1.1/ Profile2 Profile2
SWITCH#copy tftp://10.1.1.1/ Profile3 Profile3
```

Case 5: SICOM3028GPT as an FTP client to view the file list on the FTP server

Synchronization: The switch is connected to the PC through the Ethernet port, the PC is the FTP server, the IP address is 10.1.1.1, the switch is the FTP client, and the IP address of the VLAN1 interface of the switch is 10.1.1.2.

- FTP configuration:

PC side:

Start the FTP Server software on the PC, and set the user Switch with the password KYLAND.

SICOM3028GPT:

```
SWITCH(Config)#inter vlan 1
```

```
SWITCH(Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0
```

```
SWITCH(Config-If-Vlan1)#no shut
```

```
SWITCH(Config-If-Vlan1)#exit
```

```
SWITCH(Config)#dir ftp://Switch: KYLAND@10.1.1.1
```

```
220 Serv-U FTP-Server v2.5 build 6 for WinSock ready...
```

```
331 User name okay, need password.
```

```
230 User logged in, proceed.
```

```
200 PORT Command successful.
```

```
150 Opening ASCII mode data connection for /bin/ls.
```

```
recv total = 480
```

```
nos.img
```

```
nos.rom
```

```
parsecommandline.cpp
```

```
position.doc
```

```
qmdict.zip
```

```
shell maintenance statistics.xls
```

```
...(Part of the display is omitted)
```

```
show.txt
```

```
snmp.TXT
```

```
226 Transfer complete.
```

```
SWITCH(Config)#
```

7.6 LLDP configuration

7.6.1 Introduce

Link Layer Discovery Protocol (LLDP) is a new protocol defined in 802.1ab, which enables neighboring devices to notify other devices of their status information, and all devices have stored on each port defining their own. If necessary, it can also send updated information to neighboring devices directly connected to them, and the neighboring devices will store the information in standard SNMP MIBs. The network management system can query the current Layer 2 connection status from the MIB. LLDP does not configure nor control network elements or traffic, it just reports layer 2 configuration.

The equipment of our company needs to specify the equipment identification (chassis ID) when configuring LLDP, so that the EMS system or other network management software can identify the equipment. At the same time, it supports the management address field of LLDP. This field is used to notify the MIB node of these IP addresses when the switch has multiple IP addresses, so that the relevant network management software can use them.

7.6.2 CLI configuration

Table 13 Configuration command

Order	configuration mode	Features
lldp no lldp	Global configuration mode SWITCH(Config)#	Turn on the LLDP function of the switch; Disable the LLDP function.
lldp chassis-id no lldp chassis-id	Global configuration mode SWITCH(Config)#	Set the chassis ID of LLDP; Delete the chassis ID of LLDP.
lldp tlv management-address no lldp tlv management-address	Global configuration mode SWITCH(Config)#	Enable the management address function of LLDP; Delete the management address function of LLDP.
show lldp	Privileged User Configuration Mode SWITCH#	Displays LLDP neighbor information.
debug lldp no debug lldp	Privileged User Configuration Mode	Turn on the debugging switch of LLDP; Disable the debug switch of LLDP.

	SWITCH#	
--	---------	--

7.6.2.1 lldp

Features	Turn on the LLDP function of the switch; Disable the LLDP function.
command format	lldp no lldp
Default configuration	The system disables LLDP by default.
configuration mode	Global configuration mode SWITCH(Config)#

7.6.2.2 lldp chassis-id

Features	Set the chassis ID of LLDP; Delete the chassis ID of LLDP.
command format	lldp chassis-id <i>ip_address</i> no lldp chassis-id
parameter	<i>ip_address</i> :The IP address of an interface that can be accessed by the device network management software.
command mode	Global configuration mode SWITCH(Config)#

7.6.2.3 lldp tlv management-address

Features	Enable the management address function of LLDP; Delete the management address function of LLDP.
command format	lldp tlv management-address no lldp tlv management-address
Default configuration	By default, the LLDP address management function is disabled.
configuration mode	Global configuration mode SWITCH(Config)#

7.6.2.4 show lldp

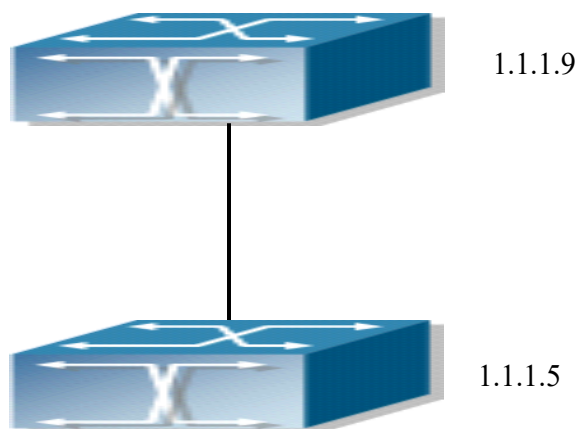
Features	Display lldp neighbor information.
command format	show lldp [mode]

configuration mode	Privileged User Configuration Mode SWITCH#
--------------------	--

7.6.2.5 debug lldp

Features	Turn on the debugging switch of LLDP; Disable the debug switch of LLDP.
command format	debug lldp {error tx rx all} no debug lldp {error tx rx all}
parameter	error : Error debugging switch; tx : message sending debugging switch; rx : message reception debugging switch; all : All debug switches.
illustrate	When users encounter problems when using LLDP, they can turn on the LLDP debugging switch to find the cause of the problem.
configuration mode	Privileged User Configuration Mode SWITCH#

7.6.3 Typical configuration example



Picture 18 LLDP Configuration Example

The two switches are directly connected, the interface IP address of the upper switch is 1.1.1.9, and the interface IP address of the lower switch is 1.1.1.5

step 1: Enable LLDP on the above switch.

The configuration on the switch side is as follows:

```
Switch(Config)#lldp
```

```
Switch(Config)#lldp chassis-id 1.1.1.9
```

Step 2:Enable LLDP on the switches below.

The configuration on the switch side is as follows:

```
Switch(Config)#lldp
```

```
Switch(Config)#lldp chassis-id 1.1.1.5
```

In this way, the switches at both ends will establish a neighbor relationship, that is, the link information of the peer device will be stored.

8 Port configuration

8.1 Introduce

The port number of each port is marked on the panel of each SICOM3028GPT board. In order to distinguish the ports on different boards, the port number (port number in the software sense) provided by the SICOM3028GPT operating system is ethernet X/Y.

If users want to configure some ports, they can use the command interface ethernet *interface_list* Enter the corresponding Ethernet interface configuration mode. The parameter *interface_list* is one or more ports. When the *interface_list* contains multiple ports, you can use special characters such as ";" and "-" to connect, and ";" to connect discontinuous port numbers, "-" to connect consecutive port numbers. In the Ethernet interface configuration mode, you can configure the port rate, duplex mode, flow control, etc., and the performance of the corresponding physical port changes accordingly.

8.2 Ethernet Port CLI Configuration

Table 14 configuration command

Order	configuration mode	Features
interface ethernet	Global configuration mode SWITCH(Config)#	Enter the Ethernet interface configuration mode.
shutdown no shutdown	Ethernet interface configuration mode SWITCH(Config-Ethernet1/1)#	Close the specified port; Open the specified port.
name no name	Ethernet interface configuration mode SWITCH(Config-Ethernet1/1)#	Set the name of the specified port; Cancel the name of the specified port.
mdi no mdi	Ethernet interface configuration mode SWITCH(Config-Ethernet1/1)#	Set the connection type of the specified port; Restore the default configuration.
speed-duplex	Ethernet interface configuration mode SWITCH(Config-Ethernet1/1)#	Set the speed and duplex mode of the specified port.

bandwidth no bandwidth	Ethernet interface configuration mode SWITCH(Config-Ethernet1/1)#	Set the bandwidth occupied by the specified port to receive and send data; Cancel the bandwidth occupied by the specified port for receiving and sending data.
flow control no flow control	Ethernet interface configuration mode SWITCH(Config-Ethernet1/1)#	Turn on the flow control function of the specified port; Disable the flow control function of the specified port.
loop-detect no loop-detect	Ethernet interface configuration mode SWITCH(Config-Ethernet1/1)#	Turn on the loopback test function of the specified port; Disable the loopback test function of the specified port.
rate-suppression no rate-suppression	Ethernet interface configuration mode SWITCH(Config-Ethernet1/1)#	Turn on the function of broadcast storm suppression (or multicast, unicast of unknown destination, the same below); Cancel the broadcast storm suppression function.
clear counters ethernet	Privileged User Configuration Mode SWITCH#	Clear the statistics of the Ethernet port.
show interface ethernet	Privileged User Configuration Mode SWITCH#	Displays information about the specified port.

8.2.1 Bandwidth

Features	Turn on the bandwidth limit function of the port; Disable the bandwidth limit function of the port.
command format	bandwidth control <i>bandwidth</i> [both receive transmit] no bandwidth control
parameter	<i>bandwidth</i> : Limit bandwidth, the unit is Mbps, the value range is 1-10000M; both : Bandwidth control is performed when the port is receiving and sending; receive : Bandwidth control is performed only when the port receives data from outside the switch; transmit : Bandwidth control is performed only when the port sends data outside the switch.
Default configuration	By default, the bandwidth limitation function is disabled on the port.
illustrate	When the port is set with the bandwidth limit function and the size of the limited bandwidth

	is specified, the maximum bandwidth of the port is determined instead of 10/100/1000M as the maximum bandwidth. If the [both receive transmit] keyword is not specified, the default is both.
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

8.2.2 flow control

Features	Enable port flow control function; Disable the port flow control function.
command format	flow control no flow control
Default configuration	The flow control function of the port is disabled by default.
illustrate	After the flow control function of the port is enabled, when the traffic received by the port is larger than the size that the port buffer can accommodate, the port will notify the device sending traffic to it through an algorithm or protocol to slow down the sending speed to prevent packet loss. The port of the switch supports 802.3X flow control based on back pressure; the port works in half-duplex mode and supports back pressure flow control. When the back pressure control reaches the possible severe head blocking (HOL), the switch will automatically perform head blocking control (drop some packets in the COS queue that may cause head blocking) to avoid a significant drop in network performance. Unless the user needs a network with slow speed and low performance but less packet loss, it is not recommended for users to enable the port flow control function. The flow control between different boards of SICOM3028GPT does not work. When enabling the flow control function of the port, make sure that the speed and duplex mode of both ends are the same.
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

8.2.3 interface ethernet

Features	Enters Ethernet interface configuration mode from global configuration mode.
command format	interface ethernet interface_list
parameter	<i>interface_list</i> : Port number. For the format and value range of the port number, see the description in the Port Introduction section of this chapter.
Default	The flow control function of the port is disabled by default.

configuration	
illustrate	Use the command exit to return from the Ethernet interface configuration mode to the global configuration.
configuration mode	Global configuration mode SWITCH(Config)#

8.2.4 loop-detect

Features	Set the Ethernet port loopback test function; Cancel the loopback test function of the Ethernet port.
command format	loop-detect no loop-detect
Default configuration	Ethernet ports are not tested for loopback.
illustrate	Use the loopback test to verify that the Ethernet port is functioning properly. After the loopback is set, the port will assume that a connection has been established with itself, and all traffic sent from the port will be received from the port again.
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

8.2.5 mdi

Features	Set the connection type supported by the Ethernet port; Restore the default configuration.
command format	mdi {auto across normal} no mdi
parameter	auto : indicates automatic identification of the connection type; across : Indicates that the port only supports crossover cables; normal : Indicates that the port only supports direct connection.
Default configuration	By default, the port connection type is automatic identification.
illustrate	Users are advised to use automatic line type recognition. Generally speaking, the switch and the PC are connected with a straight cable, and the switches are connected with a crossover cable.
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

8.2.6 name

Features	Set the port name; Cancel the port name.
command format	name string no name
parameter	<i>string</i> : A string of port names, up to 64 characters long.
Default configuration	Ports do not have names by default.
illustrate	This command is helpful for users to manage the switch. For example, the user can set the name according to the usage of the ports. For example, ports 1/1-2 are used by the financial department, and they are defined as financial, and ports 2/9 are used by the engineering department. For engineering, port 3/12 connects to the server, then define Servers. In this way, the usage of the ports can be seen at a glance.
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

8.2.7 rate-suppression

Features	Set the broadcast, multicast or unicast traffic of unknown addresses that is allowed to pass through all ports of the switch; the no operation of this command is to disable the port's function of suppressing broadcast, multicast or unicast traffic of unknown addresses, that is, to allow wire-speed through broadcast, Multicast or unicast traffic to unknown addresses.
command format	rate-suppression {bandwidth {bps number kbps number percent number} dlf broadcast multicast} no rate-suppression {bandwidth dlf broadcast multicast}
parameter	bandwidth : limit bandwidth; bps : bits per second; <i>number</i> : number; kbps : kilobits per second; percent : percentage; dlf : Restrict unknown address unicast traffic; multicast : limit multicast traffic; broadcast : limit broadcast traffic;
Default configuration	The default is unlimited.

illustrate	Without any VLAN settings, all ports of the switch are in the same broadcast domain. For the above three types of traffic, the switch will send it to all ports in the broadcast domain, which may form a broadcast storm. Broadcast storm greatly affects the performance of the switch. Turning on the broadcast storm suppression function of the switch can protect the switch from being affected by the broadcast storm as little as possible. Note that this command has different meanings for 10G ports and other ports. When the broadcast traffic allowed by the 10 Gigabit port is set to 3, it means that when the number of broadcast packets received by the port per second is greater than 3120, the part more than 3120 will be discarded; for common ports, the same setting means that when the port receives more than 3120 broadcast packets per second When the number of broadcast packets received by the clock is greater than 3, the part greater than 3 will be discarded.
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

8.2.8 shutdown

Features	close the ethernet port; Open the Ethernet port.
command format	shutdown no shutdown
Default configuration	The Ethernet port is open by default.
illustrate	When the Ethernet port is shut down, the Ethernet port will not send data frames, and the port state is displayed as down when the user enters the show interface command.
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

8.2.9 speed-duplex

Features	Set the speed and duplex mode of the specified port.
command format	speed-duplex {auto force10-full force10-half force100-full force100-half force1g-full force1g-half}
parameter	auto : Auto-negotiation; force10-full : Force 10Mbit/s rate; full duplex; force10-half : Force 10Mbit/s rate; half duplex; force100-full : Force 100Mbit/s rate; full duplex; force100-half : Force 100Mbit/s rate; half duplex;

	<p>force1g-full: Force 1000Mbit/s rate; full duplex;</p> <p>force1g-half: Force 1000Mbit/s rate; half duplex.</p>
Default configuration	The port defaults to auto-negotiation.
illustrate	<p>According to the IEEE 802.3 protocol, the auto-negotiation of port speed and duplex is unified. When the port rate is set to auto-negotiation, the duplex mode of the port will be automatically set to auto-negotiation, When the port's rate mode changes from auto-negotiation to forced, the port's duplex mode also changes to forced full-duplex mode. Note that the speed of the optical interface on various boards of SICOM3028GPT cannot be set by the user, and can only be automatically negotiated. If the port is forced to 1000M speed, the duplex will automatically become forced full-duplex.</p> <p>It is strongly recommended that users set the speed and duplex mode of each port to auto-negotiation, so as to avoid connection problems caused by the protocol as much as possible. If the user needs to set the port to forced rate/duplex, please make sure that the rate/duplex settings of both sides of the connection are the same, and both sides are forced rate/duplex.</p>
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

8.2.10 clear counters ethernet

Features	Set the speed of the specified port.
command format	clear counters [ethernet interface_list]
parameter	<i>interface_list</i> : The port number.
Default configuration	By default, statistics on Ethernet ports are not deleted.
configuration mode	Privileged User Configuration Mode SWITCH#

8.2.11 show interface ethernet

Features	Displays information about the specified port.
command format	show interface ethernet interface_list
parameter	<i>interface_list</i> : The port number.
configuration mode	Privileged User Configuration Mode SWITCH#

8.3 VLAN interface CLI configuration

Table 15 configuration command

Order	configuration mode	Features
interface vlan no interface vlan	Global configuration mode SWITCH(Config)#	Enter VLAN interface configuration mode; Delete VLAN interface.
ip address no ip address	VLAN interface configuration mode SWITCH (Config-If-Vlan1)#	Set IP address and mask; Delete the IP address configuration.
shutdown no shutdown	VLAN interface configuration mode SWITCH (Config-If-Vlan1)#	Close the VLAN interface; Open the VLAN interface.

8.3.1 interface vlan

Features	Enter VLAN interface configuration mode; Delete an existing VLAN interface.
command format	interface vlan <i>vlan_id</i> no interface vlan <i>vlan_id</i>
parameter	<i>vlan_id</i> : is the VLAN ID of the established VLAN, the value range: 1~4094.
illustrate	Before configuring a VLAN interface, make sure that the VLAN exists. Use the command exit to return from VLAN interface configuration mode to global configuration mode.
configuration mode	Global configuration mode SWITCH(Config)#

8.3.2 ip address

Features	Set the IP of the switch; Delete IP configuration.
command format	ip address <i>ip_address mask</i> [secondary] no ip address [<i>ip_address mask</i>] [secondary]
parameter	<i>ip_address</i> : IP address, in dotted decimal format; <i>mask</i> : Subnet mask, in dotted decimal format; secondary : Indicates that the configured IP address is the slave IP address.
illustrate	This command manually configures an IP address on a VLAN interface. If the optional parameter secondary is not configured, it means the primary IP address of the VLAN interface. If the optional parameter secondary is configured, it means that the IP address is the secondary IP address of the VLAN interface. A VLAN interface can only have one

	primary IP address and can have multiple secondary IP addresses. Both master IP and slave IP can be used for SNMP/Web/Telnet management. In addition, SICOM3028GPT also provides BOOTP/DHCP method to obtain IP address.
configuration mode	VLAN interface configuration mode SWITCH (Config-If-Vlan1)#

8.3.3 shutdown

Features	Close the specified VLAN interface of the switch; Open the VLAN interface.
command format	shutdown no shutdown
default properties	The VLAN interface is disabled by default.
illustrate	When shutting down the VLAN interface of the switch, the VLAN interface will not send data frames. If the VLAN interface of the switch needs to obtain an IP address through the BOOTP/DHCP protocol, the VLAN interface must be enabled.
configuration mode	VLAN interface configuration mode SWITCH (Config-If-Vlan1)#

8.4 Port mirroring CLI configuration

The port mirroring function means that the switch copies the data frames received or sent by one port to another port in the same way; the copied port is called the mirror source port, and the copied port is called the mirror destination port. Usually a protocol analyzer (such as Sniffer) or RMON monitor is connected to the mirror destination port, which can monitor and manage the network and diagnose network failures.

SICOM3028GPT only supports one mirroring destination port, and the mirroring source port has no restrictions on its use. It can be one or more. Multiple source ports can be in the same VLAN or in different VLANs. The destination port and source port can be in different VLANs.

Table 16 Configuration command

Order	configuration mode	Features
monitor session source interface no monitor session source interface	Global configuration mode SWITCH(Config)#	Specify the mirroring source port; Delete the mirror source

		port.
monitor session destination interface no monitor session destination interface	Global configuration mode SWITCH(Config)#	Specify the mirroring destination port; Delete the mirror destination port.
show monitor	Privileged User Configuration Mode SWITCH#	Displays information about mirroring source and destination ports.

8.4.1 monitor session source interface

Features	Specify the mirroring source port; Delete the mirror source port.
command format	monitor session session source interface interface_list {rx tx both} no monitor session session source interface interface_list
parameter	<i>session</i> : mirror session value, currently only 1 is supported; <i>interface_list</i> : mirror source port list, support "-" ";" and other special characters; rx : Mirror the traffic received by the source port; tx : mirror the traffic sent from the source port; both : Mirror the incoming and outgoing traffic of the source port.
illustrate	This command sets the source port of mirroring. SICOM3028GPT has no restrictions on the source port of mirroring. It can be one port or multiple ports. It can not only mirror the outgoing and receiving bidirectional traffic of the source port, but also mirror the outgoing traffic of the source port independently. and receive traffic. If the [rx tx both] keyword is not specified, the default is both. When mirroring multiple ports, the directions of multiple source ports can be inconsistent, but the configuration should be done several times.
configuration mode	Global configuration mode SWITCH(Config)#

8.4.2 monitor session destination interface

Features	Specify the mirroring destination port; Delete the mirror destination port.
command format	monitor session session destination interface interface_number [tag{all preserve}] no monitor session session destination interface interface_number
parameter	<i>session</i> : mirror session value, currently only 1 is supported;

	<p><i>interface_number</i>: mirror destination port;</p> <p>tag: Set the vlan tag of the mirroring package sent from the mirroring destination port;</p> <p>all: Indicates that all image packages have vlan tag;</p> <p>preserve: Indicates that if the mirrored packet has a vlan tag when it enters the switch, the mirrored packet also has a vlan tag; if the mirrored packet does not have a vlan tag when it enters the switch, the mirrored packet also does not have a vlan tag.</p>
Default configuration	If the tag mode is not specified, the default tag mode is preserve.
illustrate	SICOM3028GPT supports only one mirror target port. It should be noted that the mirroring target port cannot be a member of a port aggregation group, and the port throughput is preferably greater than or equal to the sum of the throughputs of all source ports it mirrors.
configuration mode	Global configuration mode SWITCH(Config)#

8.4.3 show monitor

Features	Displays information about mirroring source and destination ports.
command format	show monitor
illustrate	This command can display the currently set mirroring source port and destination port.
configuration mode	Privileged User Configuration Mode SWITCH#

8.5 Typical configuration example

No VLAN is configured on the switch, so the default VLAN1 is used.

switch	port	Attributes
SW1	2/7	Ingress bandwidth limit, 150M
SW2	1/8	Port mirroring source port
	3/9	100M/full, port mirroring source port
	4/12	1000M/full, port mirroring destination port
SW3	3/10	100M/full

The configuration is as follows:

SW1:

```
Switch1(Config)#interface ethernet 2/7
```

```
Switch1(Config-Ethernet2/7)#bandwidth control 150 both
```

SW2:

```
Switch2(Config)#interface ethernet 3/9
```

```
Switch2(Config-Port-Range)#speed force100
```

```
Switch2(Config-Port-Range)#duplex full
```

```
Switch2(Config-Port-Range)#exit
```

```
Switch2(Config)#interface ethernet 4/12
```

```
Switch2(Config-Ethernet1/2)#speed force1000
```

```
Switch2(Config-Ethernet1/2)#duplex full
```

```
Switch2(Config-Ethernet1/2)#exit
```

```
Switch2(Config)#monitor session 1 source interface ethernet 1/8;3/9
```

```
Switch2(Config)#monitor session 1 destination interface ethernet 4/12
```

SW3:

```
Switch3(Config)#interface ethernet 3/10
```

```
Switch3(Config-Ethernet3/10)#speed force100
```

```
Switch3(Config-Ethernet3/10)#duplex full
```

9 MAC address table configuration

9.1 introduce

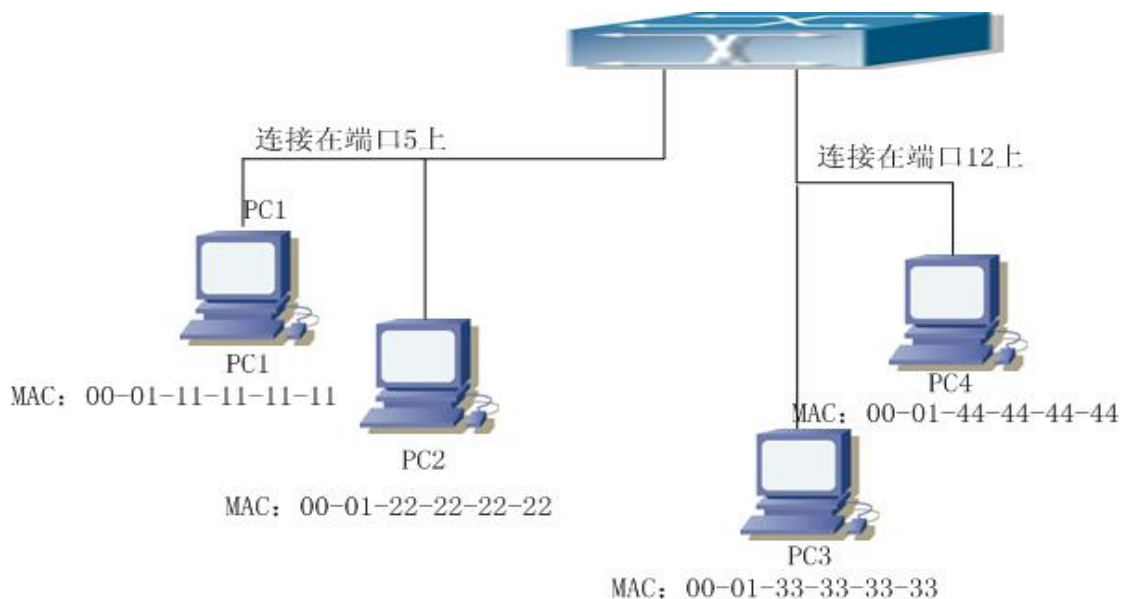
The MAC address table is a table that identifies the mapping relationship between destination MAC addresses and switch ports. The MAC addresses are classified into static MAC addresses and dynamic MAC addresses. The static MAC address is configured by the user, has the highest priority (cannot be overwritten by the dynamic MAC address) and takes effect permanently; the dynamic MAC address is learned by the switch during the process of forwarding data frames and takes effect within a limited time. When the switch receives the data frame that needs to be forwarded, it first learns the source MAC address of the data frame and establishes a mapping relationship with the receiving port; then it queries the MAC address table according to the target MAC address. If the relevant entry is hit, the switch sends the data frame from the corresponding port. Forward; otherwise, the switch broadcasts the data frame in the broadcast domain to which it belongs. If the dynamic MAC address is not learned from the forwarding data frame for a long time, the switch will delete it from the MAC address table.

The operation of the MAC address table can be divided into two steps:

1. Obtaining the MAC address;
2. Forward or filter based on MAC address table.

9.1.1 Obtaining the MAC address table

The acquisition of the MAC address table can be divided into static configuration and dynamic learning. Static configuration means that the user manually establishes the mapping relationship between MAC addresses and ports; dynamic learning means that the switch dynamically discovers the mapping between MAC addresses and ports, and regularly updates the MAC address table. Below we will focus on the dynamic learning process of the MAC address table.



Picture 19 MAC address table dynamic learning

The topological environment in the above Picture is: 4 hosts are connected On SICOM3028GPT, hosts 1 and 2 are in the same physical segment (that is, the same collision domain), and the physical segment is connected to port 1/5 of SICOM3028GPT; hosts 3 and 4 are in the same physical segment, and the physical segment is in the same physical segment. The segment is connected to port 1/12 of the SICOM3028GPT.

In the initial state, there is no learned address mapping table entry in the MAC address table. Taking the communication between host 1 and host 3 as an example, the learning process of the MAC address table is as follows:

1. When host 1 transmits information to host 3, the switch receives the source MAC address 00-01-11-11-11-11 of the information at port 1/5, and the switch's MAC address table adds MAC address 00- 01-11-11-11-11 and port 1/5 mapping table entry;
2. At the same time, the switch will check the destination MAC address 00-01-33-33-33-33 of the information. At this time, the switch only has the mapping table entry for the MAC address 00-01-11-11-11-11 and port 1/5. , there is no port mapping corresponding to 00-01-33-33-33-33, so the switch can only broadcast the information to each port of the switch(Assuming that all ports of the switch belong to the default VLAN);
3. Hosts 3 and 4 on port 1/12 both receive the information sent by host 1, but host 4 will

not respond to host 1 because the destination MAC address is 00-01-33-33-33-33, and only host 3 will respond. Respond to host 1. At this time, port 1/12 of the switch receives the information sent by host 3, and the MAC address table of the switch adds MAC address 00-01-33-33-33-33 and port 1/12 mapping table entry;

4. Currently, the contents of the MAC address table are that MAC address 00-01-11-11-11-11 dynamically corresponds to port 1/5, and MAC address 00-01-33-33-33-33 dynamically corresponds to port 1/12.
5. After a period of communication between host 1 and host 3, the switch never receives the information sent from host 1 and host 3. After 300 seconds, the MAC address table of the switch will delete the MAC address mapping table entry saved above. 300 seconds here is SICOM3028GPT default MAC address aging time, SICOM3028GPT provides modification of aging time.

9.1.2 forward or filter

The switch will forward or filter the received data frame according to the MAC address table. Take the above Picture as an example, assuming that the current SICOM3028GPT MAC address table dynamically learned the MAC addresses of host 1 and host 3, and the user manually configured the mapping relationship between host 2 and host 4 and ports. The MAC address table of SICOM3028GPT is:

MAC address	The port number	method of obtaining
00-01-11-11-11-11	1/5	dynamic
00-01-22-22-22-22	1/5	static
00-01-33-33-33-33	1/12	dynamic
00-01-44-44-44-44	1/12	static

1. Forwarding according to the MAC address table

If host 1 sends information to host 3, the switch will send data received from port 1/5 from port 1/12 according to the MAC address table.

2. Filter by MAC address table

If host 1 sends information to host 2, the switch checks that host 2 and host 1 are in the same physical segment according to the MAC address table, and the switch filters the information, that is,

does not send frame information.

In addition the switch can forward three types of frames:

- ✧ broadcast frame;
- ✧ multicast frame;
- ✧ Unicast frame.

The following is a brief introduction to the processing of the three frames by the switch:

1. Broadcast frame: The switch can block the collision domain, but cannot block the broadcast domain. All devices connected to the switch are in the same broadcast domain without setting VLAN. When the switch receives a broadcast frame, it will send it to all port forwards the broadcast frame. When VLAN is set on the switch, the MAC address table will also be adjusted accordingly, and the information of VLAN will be added. At this time, after the switch receives the broadcast frame, it will not forward the broadcast frame to all ports in the switch, but change it to only Forward to all ports belonging to the same VLAN.
2. Multicast frame: When the switch does not have the IGMP Snooping function, the switch handles multicast the same way as the broadcast; when the switch has the IGMP Snooping function, the switch will only forward the multicast frame to the ports that belong to the multicast group.
3. Unicast frame: If no VLAN is set, when the destination MAC address of the unicast frame received by the switch exists in the MAC table, the switch will directly forward the unicast frame to the corresponding port; when the unicast frame is received When the destination MAC address does not exist in the MAC address table, the switch will broadcast the unicast frame. When a VLAN is set on the switch, the switch can only forward unicast frames within the same VLAN; when the destination MAC address of the forwarded unicast frame exists in the MAC address table, but does not belong to the same VLAN, the switch can only forward the unicast frame Broadcast within the VLAN to which it belongs.

9.2 CLI configuration

Table 17 Configuration command

Order	configuration mode	Features
mac-address-table	Privileged User	Set the aging time of the dynamically learned

aging-time no mac-address-table aging-time	Configuration Mode SWITCH#	address mapping table entries in the MAC address table; Restore the default aging time of the system to 300 seconds.
mac-address-table no mac-address-table	Global configuration mode SWITCH(Config)#	Add or modify static address entries, filter address entries; Delete static address entries and filter address entries.

9.2.1 mac-address-table aging-time

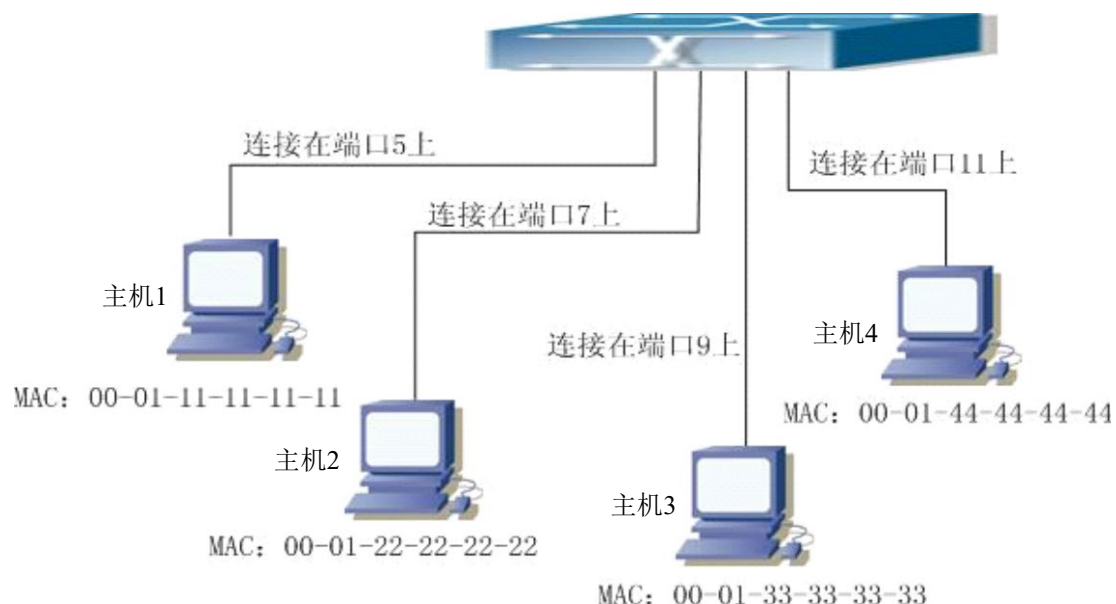
Features	Set the aging time of the dynamically learned address mapping table entries in the MAC address table; Restore the default aging time of the system to 300 seconds.
command format	mac-address-table aging-time {age 0} no mac-address-table aging-time
parameter	<i>age</i> : aging time, the unit is second, the value range is 10~100000; 0 : Not aging.
Default configuration	The default aging time of the system is 300 seconds.
illustrate	If the aging time is set too small, many unnecessary broadcasts will be added to the switch and affect the performance; if the aging time is set too large, some long-term unused entries will exist in the MAC address table for a long time. Therefore, the user should set the aging time reasonably according to the actual situation. When the aging time is set to 0 seconds, the address dynamically learned by the switch will not age with time, and the dynamically learned address will always be stored in the MAC address table.
configuration mode	Privileged User Configuration Mode SWITCH#

9.2.2 mac-address-table

Features	Add or modify static address entries, filter address entries; Delete static address entries and filter address entries.
command format	mac-address-table {static blackhole} address mac_addr vlan vlan_id no mac-address-table [static blackhole dynamic] [address mac_addr] [vlan vlan_id]
parameter	static : static entry;

	<p>blackhole: Filter entry, the purpose of configuring the filter entry is to discard the frame with the specified MAC address, which is used to filter the traffic that does not want to pass through, and the source address and destination address can be filtered;</p> <p>dynamic: dynamic address table entry;</p> <p><i>mac_addr:</i> MAC address to add or delete;</p> <p><i>vlan_id:</i> VLAN ID.</p>
Default configuration	When a VLAN interface is configured and the VLAN interface is Up, the system will generate a static address mapping entry corresponding to the unique MAC address of the system and the VLAN number.
illustrate	<p>In some special purposes or the switch cannot learn the MAC address dynamically, the user can use this command to manually establish the mapping relationship between the MAC address and the port and VLAN.</p> <p>The command <code>no mac-address-table</code> deletes all dynamic, static and filtering MAC address entries in the MAC address table of the switch, except for the mapping entries reserved by the system by default.</p>
configuration mode	Global configuration mode SWITCH(Config)#

9.3 Typical configuration example



Picture 20 Typical configuration example of MAC address table

Case: As shown on the Picture above, the four hosts are respectively connected to ports 1/5,

1/7, 1/9, and 1/11 of the SICOM3028GPT switch. These four hosts belong to the default VLAN1. According to the needs of the actual network, the dynamic learning function is enabled; host 1 stores confidential information, and any host that is not in a physical segment with it cannot access it; host 2 and host 3 establish static mapping relationships with ports 7 and 9, respectively.

The configuration steps are as follows:

1. Set the MAC address 00-01-11-11-11-11 of host 1 as the filter address;

```
SWITCH(Config)#mac-address-table blackhole address 00-01-11-11-11-11 vlan 1 interface ethernet 1/1
```

2. Host 2 and host 3 establish static mapping relationships with ports 7 and 9, respectively.

```
SWITCH(Config)#mac-address-table static address 00-01-22-22-22-22 vlan 1 interface ethernet 1/7
```

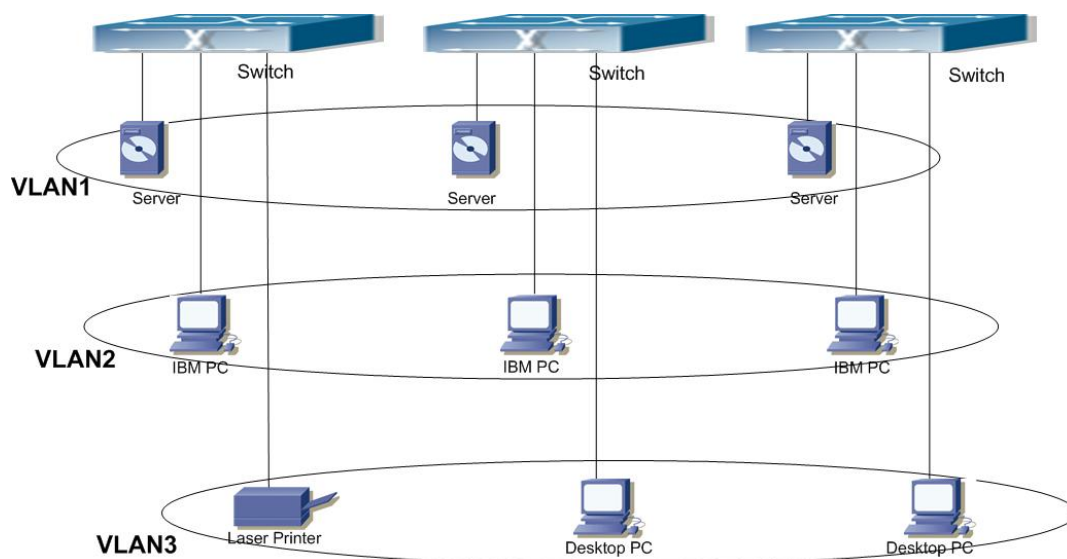
```
SWITCH(Config)#mac-address-table static address 00-01-33-33-33-33 vlan 1 interface ethernet 1/9
```

10 VLAN configuration

10.1 introduce

VLAN (Virtual Local Area Network) is a virtual local area network. This technology can logically divide the devices inside the local area network into network segments according to the needs of functions, applications or management, so as to form virtual work groups, and do not need to consider the actual physical location of the device. IEEE promulgated the IEEE802.1Q protocol to specify the implementation scheme of standardized VLAN, and the VLAN function of SICOM3028GPT is implemented according to the 802.1Q standard.

The characteristic of VLAN technology is that a large local area network can be dynamically divided into many different broadcast domains according to the needs:



Picture 21 Logically defined VLAN network

Each broadcast domain is a VLAN. A VLAN has the same attributes as a physical LAN. The only difference is that VLANs are divided logically rather than physically. Therefore, the division of VLANs does not have to be based on the actual physical location. All broadcast, multicast, and unicast traffic are isolated from other VLANs.

Based on the above characteristics of VLAN, VLAN technology brings us the following conveniences:

- Improve network performance
- Save network resources

- Simplify network management
- Reduce network costs
- Improve network security

10.2 CLI configuration

Table 18 Configuration command

Order	configuration mode	Features
vlan no vlan	Global configuration mode SWITCH(Config)#	Create VLAN and enter VLAN configuration mode; Delete the specified VLAN.
name no name	VLAN configuration mode SWITCH(Config-Vlan100)#	Specify a name for the VLAN; Delete the VLAN name.
state no state	VLAN configuration mode SWITCH(Config-Vlan100)#	
switchport access vlan no switchport access vlan	interface configuration mode SWITCH(Config-Ethernet1/1)#	Add the current access port to the specified VLAN; Remove the current port from the VLAN.
switchport interface no switchport interface	interface configuration mode SWITCH(Config-Ethernet1/1)#	Allocate Ethernet ports to VLANs; Deletes a port or a group of ports within the specified VLAN.
switchport mode	interface configuration mode SWITCH(Config-Ethernet1/1)#	Set the port mode of the switch.
switchport trunk allowed vlan no switchport trunk allowed vlan	interface configuration mode SWITCH(Config-Ethernet1/1)#	Set the trunk port to allow through VLAN; Restore the default configuration.
switchport trunk native vlan no switchport trunk native vlan	interface configuration mode SWITCH(Config-Ethernet1/1)#	Set the PVID of the trunk port; Restore default values.
vlan ingress disable no vlan ingress disable	interface configuration mode SWITCH(Config-Ethernet1/1)#	Close the VLAN entry rule of the port; Open the VLAN ingress rule for the port.
vlan aware	Global configuration mode SWITCH(Config)#	

vlan unaware	Global configuration mode SWITCH(Config)#	
show vlan	Privileged User Configuration Mode SWITCH#	Display VLAN details.
show vlan brief	Privileged User Configuration Mode SWITCH#	Display VLAN summary information.
show vlan summary	Privileged User Configuration Mode SWITCH#	Displays summary information for all VLANs.

10.2.1 vlan

Features	Create VLAN and enter VLAN configuration mode; Delete the specified VLAN.
command format	Vlan <i>vlan_id</i> no vlan <i>vlan_id</i>
parameter	<i>vlan_id</i> : The ID of the VLAN to be created/deleted, ranging from 1 to 4094.
Default configuration	The switch has only VLAN 1 by default.
illustrate	VLAN1 is the default VLAN of the switch, and users cannot configure or delete VLAN1. The total number of VLANs allowed to be configured is 4094. Another reminder is that you cannot use this command to delete the dynamic VLAN learned through GVRP.
configuration mode	Global configuration mode SWITCH(Config)#

10.2.2 name

Features	Specify a name for the VLAN; Delete the VLAN name.
command format	name <i>vlan_name</i> no name
parameter	<i>vlan_name</i> : VLAN name string.
Default configuration	The default VLAN name is vlanXXX, where XXX is the VID.
configuration mode	VLAN configuration mode SWITCH(Config-Vlan100)#

10.2.3 switchport access vlan

Features	Add the current access port to the specified VLAN; Remove the current port from the VLAN.
command format	switchport access vlan <i>vlan_id</i> no switchport access vlan
parameter	<i>vlan_id</i> : ID of the VLAN to which the current port is to be added, ranging from 1 to 4094.
Default configuration	All ports belong to VLAN 1 by default.
illustrate	Only ports in access mode can be added to the specified VLAN, and access ports can only be added to one VLAN at the same time.
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

10.2.4 switchport interface

Features	Allocate Ethernet ports to VLANs; Deletes a port or a group of ports within the specified VLAN.
command format	switchport interface <i>interface_list</i> no switchport interface <i>interface_list</i>
parameter	<i>interface_list</i> : The list of ports to be added or removed, ";" "-" is supported, such as: ethernet 1/1;2;5 or ethernet 1/1-6;8.
Default configuration	The newly established VLAN does not contain any ports by default.
illustrate	The access port is a common port and can be added to a VLAN, but only one VLAN is allowed to be added at the same time.
configuration mode	VLAN configuration mode SWITCH(Config-Vlan100)#

10.2.5 switchport mode

Features	Set the port mode of the switch.
command format	switchport mode {trunk access}
parameter	trunk : The port allows traffic through multiple VLANs. access : The port can only belong to one VLAN.
Default configuration	The port defaults to access mode.

illustrate	The port working in trunk mode is called trunk port. The trunk port can pass the traffic of multiple VLANs. Through the interconnection between trunk ports, the same VLAN on different switches can be communicated. The port working in access mode is called Access ports, access ports can be assigned to one VLAN, and can only be assigned to one VLAN at the same time.
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

10.2.6 switchport trunk allowed vlan

Features	Set the VLANs that the trunk port is allowed to pass through; Restore the default configuration.
command format	switchport trunk allowed vlan {vlan_list all} no switchport trunk allowed vlan
parameter	<i>vlan_list</i> : List of VLANs allowed to pass on the trunk port; all : Allow the trunk port to pass all VLAN traffic.
Default configuration	The trunk port is allowed to pass through all VLANs by default.
illustrate	Users can use this command to set which VLAN traffic passes through the trunk port, and the VLAN traffic that is not included is prohibited.
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

10.2.7 switchport trunk native vlan

Features	Set the PVID of the trunk port; Restore default values.
command format	switchport trunk native vlan vlan_id no switchport trunk native vlan
parameter	<i>vlan_id</i> : PVID of the trunk port.
Default configuration	The default PVID of a trunk port is 1.
illustrate	The concept of PVID is defined in 802.1Q. The function of the PVID of the trunk port is that when an untagged frame enters the trunk port, the port will tag the untagged frame with the native PVID set by this command for VLAN forwarding.
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

10.2.8 vlan ingress disable

Features	Close the VLAN entry rule of the port; Open the VLAN ingress rule for the port.
command format	vlan ingress disable no vlan ingress disable
Default configuration	By default, the VLAN entry rule of the port is opened.
illustrate	When the VLAN entry rule of the port is opened, the system will check whether the source port is a member port of the VLAN when receiving data. If so, it will accept the data and forward it to the destination port, otherwise it will discard the data.
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

10.2.9 vlan aware

Features	Data frames need to add VLAN information
command format	vlan aware
illustrate	When the switch is configured as aware, VLAN tags need to be added to the sending and receiving of all data frames
configuration mode	Global configuration mode SWITCH(Config)#

10.2.10 vlan unaware

Features	Ignore the VLAN information of the data frame
command format	vlan unaware
illustrate	When the switch is configured as unaware, all data frames are sent and received without VLAN tags
configuration mode	Global configuration mode SWITCH(Config)#

10.2.11 show vlan

Features	Display VLAN details.
command format	show vlan [id vlan_id] [name vlan_name]

parameter	<i>vlan_id</i> : The ID of the VLAN whose information is to be displayed; <i>vlan_name</i> : The name of the VLAN for which information is to be displayed.
illustrate	If no <i>vlan_id</i> or <i>vlan_name</i> is specified, the status information of all VLANs on the switch will be displayed.
configuration mode	Privileged User Configuration Mode SWITCH#

10.2.12 show vlan brief

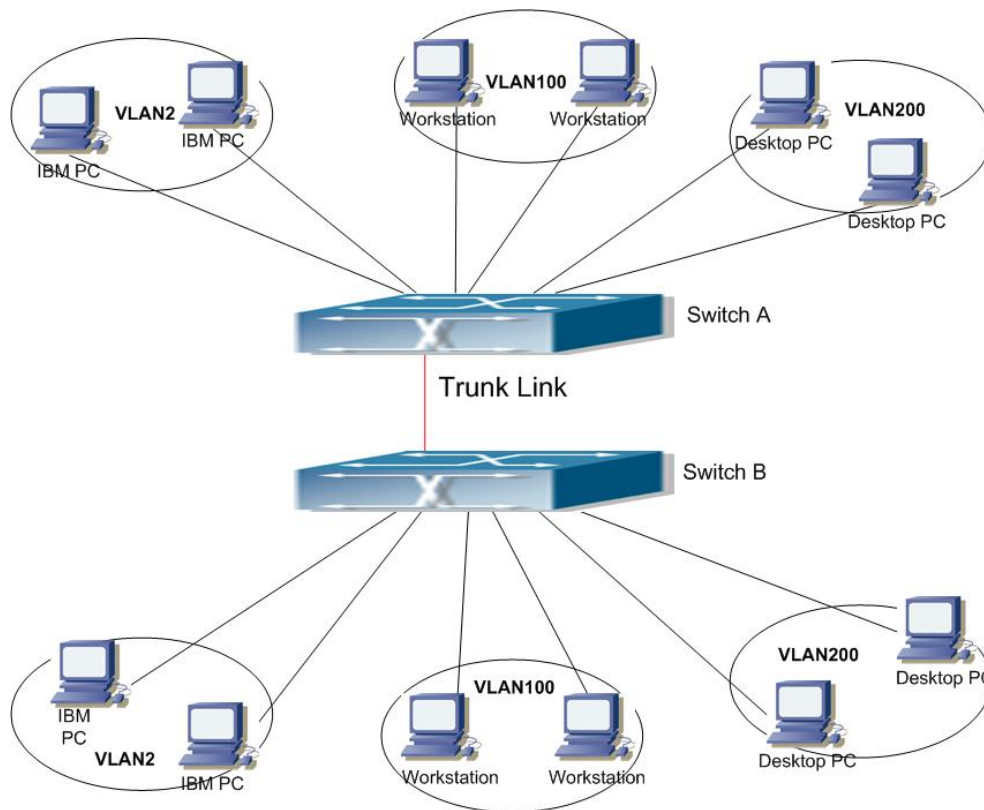
Features	Display VLAN summary information.
command format	show vlan brief [id <i>vlan_id</i>] [name <i>vlan_name</i>]
parameter	<i>vlan_id</i> : The ID of the VLAN whose information is to be displayed; <i>vlan_name</i> : The name of the VLAN for which information is to be displayed.
illustrate	If no <i>vlan_id</i> or <i>vlan_name</i> is specified, the status information of all VLANs on the switch will be displayed.
configuration mode	Privileged User Configuration Mode SWITCH#

10.2.13 show vlan summary

Features	Displays summary information for all VLANs.
command format	show vlan summary
configuration mode	Privileged User Configuration Mode SWITCH#

10.3 Typical configuration example

case



Picture 21 Typical application topology of VLAN

Due to the needs of local area network security and applications, the entire existing local area network needs to be divided into 3 VLANs: VLAN 2, VLAN 100 and VLAN 200, and these three VLANs are required to span two regions A and B. Now a switch is placed in each of the two locations. Therefore, as long as VLAN traffic can be transmitted between switches, it can meet the requirements of cross-region.

configuration item	Configuration instructions
VLAN2	A ground, B ground switch 2 to 4 ports
VLAN100	A ground, B ground switch 5~7 ports
VLAN200	Ports 8 to 10 of switches at A and B
trunk port	11 ports of A ground and B ground switches

The trunk ports of the two switches are connected to form a trunk link, which is used to carry vlan traffic across the switches; various network devices are connected to the ports of each VLAN of the switch, and they belong to the corresponding VLAN.

In this example, ports 1 and 12 are free and can be used as management ports or for other purposes.

The configuration steps are as follows:

A switch:

```
SWITCH (Config)#vlan 2
SWITCH (Config-Vlan2)#switchport interface ethernet 1/2-4
SWITCH (Config-Vlan2)#exit
SWITCH (Config)#vlan 100
SWITCH (Config-Vlan100)#switchport interface ethernet 1/5-7
SWITCH (Config-Vlan100)#exit
SWITCH (Config)#vlan 200
SWITCH (Config-Vlan200)#switchport interface ethernet 1/8-10
SWITCH (Config-Vlan200)#exit
SWITCH (Config)#interface ethernet 1/11
SWITCH (Config-Ethernet1/11)#switchport mode trunk
SWITCH (Config-Ethernet1/11)#exit
SWITCH (Config)#
```

B switch:

```
SWITCH (Config)#vlan 2
SWITCH (Config-Vlan2)#switchport interface ethernet 1/2-4
SWITCH (Config-Vlan2)#exit
SWITCH (Config)#vlan 100
SWITCH (Config-Vlan100)#switchport interface ethernet 1/5-7
SWITCH (Config-Vlan100)#exit
SWITCH (Config)#vlan 200
SWITCH (Config-Vlan200)#switchport interface ethernet 1/8-10
SWITCH (Config-Vlan200)#exit
SWITCH (Config)#interface ethernet 1/11
SWITCH (Config-Ethernet1/11)#switchport mode trunk
SWITCH (Config-Ethernet1/11)#exit
```

11 IGMP Snooping Configuration

11.1 Introduction to IGMP Snooping

IGMP (Internet Group Management Protocol) Internet Group Management Protocol, used to implement IP multicast. Network devices (such as routers) that support multicast use the IGMP protocol to query host qualifications; hosts that want to join a multicast group notify the router through the IGMP protocol that they want to receive packets from a certain multicast address. The router first sends an IGMP Host Membership Query message using a group address that is addressable to all hosts (ie 224.0.0.1). If a host wishes to join a multicast group, it responds with an IGMP Host Membership Report message using the group address of the multicast group.

IGMP Snooping, or IGMP snooping, is a multicast constraint mechanism running on Layer 2 devices to manage and control multicast groups. IGMP Snooping relies on IGMP packets and mechanisms to manage and control multicast group data forwarding. Switches use IGMP Snooping to limit the flooding of multicast traffic and only forward multicast traffic to the ports that request the corresponding multicast group information. The switch listens to the IGMP messages between the multicast router and the host, and maintains the multicast forwarding table according to the listening result, and the switch decides the forwarding of multicast packets according to the multicast forwarding table.

SICOM3028GPT implements the IGMP Snooping function, and also provides the switch to send the Query function. In this way, users can implement IGMP Snooping to implement Layer 2 multicast management and multicast group control.

11.2 CLI configuration

Table 19 Configuration command

Order	configuration mode	Features
ip igmp snooping	Global configuration mode	Enable the IGMP Snooping function of the switch;
no ip igmp snooping	mode	To turn off IGMP Snooping.

	SWITCH(Config)#	
ip igmp snooping vlan no ip igmp snooping vlan	Global configuration mode SWITCH(Config)#	Enable the IGMP Snooping function of the specified VLAN; Disable the IGMP Snooping function of the specified VLAN.
ip igmp snooping vlan mrouter no ip igmp snooping vlan mrouter	Global configuration mode SWITCH(Config)#	Configure static multicast routing ports in the specified VLAN; Delete the multicast routing port.
ip igmp snooping vlan static no ip igmp snooping vlan static	Global configuration mode SWITCH(Config)#	Set IGMP snooping static multicast group membership function; Cancel this function.
ip igmp snooping vlan query no ip igmp snooping vlan query	Global configuration mode SWITCH(Config)#	Enable the IGMP Query function of the specified VLAN; Turn off the Query function.
ip igmp vlan query robustness no ip igmp snooping vlan query robustness	Global configuration mode SWITCH(Config)#	Set the vitality parameter of the IGMP Query function in the specified VLAN; Restore Defaults.
ip igmp snooping vlan query interval no ip igmp snooping vlan query interval	Global configuration mode SWITCH(Config)#	Set the time interval for sending IGMP Query within the specified VLAN; Restore Defaults.
ip igmp snooping vlan query max-response-time no ip igmp snooping vlan query max-response-time	Global configuration mode SWITCH(Config)#	Set the maximum response time of IGMP Query in the specified VLAN; Restore Defaults.
ip igmp snooping vlanaddress no ip igmp snooping vlanaddress	Global configuration mode SWITCH(Config)#	Set the IP address used by IGMP Snooping to specify the VLAN; Restore Defaults.
show ip igmp snooping	Privileged User Configuration Mode SWITCH#	Displays IGMP Snooping information.
show mac-address-table multicast	Privileged User Configuration	Display multicast MAC address table information.

	Mode SWITCH#	
debug ip igmp snooping	Privileged User	Turn on the debugging switch of IGMP
no debug ip igmp snooping	Configuration	Snooping of the switch;
	Mode SWITCH#	Turn off this debug switch.

11.2.1 ip igmp snooping

Features	Enable the IGMP Snooping function of the switch; Turn off IGMP Snooping.
command format	ip igmp snooping no ip igmp snooping
Default configuration	The switch does not enable IGMP Snooping by default.
illustrate	Enable the IGMP Snooping function of the switch to enable the switch to monitor the multicast traffic on the network.
configuration mode	Global configuration mode SWITCH(Config)#

11.2.2 ip igmp snooping vlan

Features	Enable the IGMP Snooping function of the specified VLAN; Disable the IGMP Snooping function of the specified VLAN.
command format	ip igmp snooping vlan <i>vlan_id</i> no ip igmp snooping vlan <i>vlan_id</i>
parameter	<i>vlan_id</i> : VLAN ID.
Default configuration	By default, IGMP Snooping is not enabled for VLANs.
illustrate	The IGMP snooping function of the switch must be enabled before the IGMP snooping function of the specified VLAN can be enabled. This command is mutually exclusive with the command ip igmp snooping vlan <i>vlan_id</i> query, that is, only one function of snooping or query can be performed in the same VLAN.
configuration mode	Global configuration mode SWITCH(Config)#

11.2.3 ip igmp snooping vlan mroute

Features	Configure static multicast routing ports in the specified VLAN; Delete the multicast routing port.
command	ip igmp snooping vlan <i>vlan_id</i> mrouter interface <i>interface_name</i>

format	no ip igmp snooping vlan <i>vlan_id</i> mrouter
parameter	<i>vlan_id</i> : Specified VLAN number; <i>interface_name</i> : Specifies the multicast routing port number.
Default configuration	There is no M-Router port in the default VLAN.
illustrate	At present, the switch does not support the configuration function of static multicast routing ports, but supports the learning function of dynamic multicast routing ports..
configuration mode	Global configuration mode SWITCH(Config)#

11.2.4 ip igmp snooping vlan static

Features	Set IGMP snooping static multicast group membership function; Cancel this function.
command format	ip igmp snooping vlan <i>vlan_id</i> static <i>multicast_addr</i> interface <i>interface_name</i> no ip igmp snooping vlan <i>vlan_id</i> static <i>multicast_addr</i>
parameter	<i>vlan_id</i> : Specify the VLAN number; <i>multicast_addr</i> : multicast group address; <i>interface_name</i> : Multicast group member port.
Default configuration	By default, there is no static multicast group.
illustrate	When the configured static multicast address is the same as the existing dynamic multicast address, the static multicast address will overwrite the dynamic multicast address.
configuration mode	Global configuration mode SWITCH(Config)#

11.2.5 ip igmp snooping vlan query

Features	Enable the IGMP Query function of the specified VLAN; Turn off the Query function.
command format	ip igmp snooping vlan <i>vlan_id</i> query no ip igmp snooping vlan <i>vlan_id</i> query
parameter	<i>vlan_id</i> : The specified VALN number.
Default configuration	By default, the IGMP Query function is not enabled.
illustrate	The premise of enabling the IGMP Query function in a specified VLAN is that the corresponding VLAN is configured on the switch and IGMP Snooping is enabled on the switch. It should be noted that this command and the command ip igmp snooping vlan

	vlan_id are mutually exclusive, that is, only one function of Snooping or Query can be performed in the same VLAN at the same time.
configuration mode	Global configuration mode SWITCH(Config)#

11.2.6 ip igmp snooping vlan query robustness

Features	Set the robustness parameters of the IGMP Query function in the specified VLAN; Restore Defaults.
command format	ip igmp snooping vlan <i>vlan_id</i> query robustness <i>robustness_variable</i> no ip igmp snooping vlan <i>vlan_id</i> query robustness
parameter	<i>vlan_id</i> : Specified VLAN number; <i>robustness_variable</i> : Robustness parameter, the value range is 2~10.
Default configuration	robustnessThe default value of the parameter is 2.
illustrate	The robustness parameter allows adjustment according to the expected packet loss on the link. If the expected packet loss is severe, the robustness parameter can be increased. That is, when the network environment is good, the robustness parameter can be set to a small value, and when the network environment is poor, the robustness parameter should be appropriately increased.
configuration mode	Global configuration mode SWITCH(Config)#

11.2.7 ip igmp snooping vlan query interval

Features	Set the time interval for sending IGMP Query within the specified VLAN; Restore Defaults.
command format	ip igmp snooping vlan <i>vlan_id</i> query interval <i>interval_value</i> no ip igmp snooping vlan <i>vlan_id</i> query interval
parameter	<i>vlan_id</i> : Specified VLAN number; <i>interval_value</i> Indicates the time interval for sending Query, ranging from 1 to 65535.
Default configuration	The default interval for sending Query is 125 seconds.
configuration mode	Global configuration mode SWITCH(Config)#

11.2.8 ip igmp snooping vlan query max-response-time

Features	Set the maximum response time of IGMP Query in the specified VLAN;
----------	--

	Restore Defaults.
command format	ip igmp snooping vlan <i>vlan_id</i> query max-response-time <i>time_value</i> no ip igmp snooping vlan <i>vlan_id</i> query max-response-time
parameter	<i>vlan_id</i> : Specified VLAN number; <i>time_value</i> : Specifies the maximum query response time, ranging from 10 to 25.
Default configuration	The default value of the maximum query response time is 10 seconds.
configuration mode	Global configuration mode SWITCH(Config)#

11.2.9 ip igmp snooping vlan address

Features	Set the IP address used by the specified VLAN for IGMP Snooping. If the query function is enabled, the address will participate in the querier election; Restore Defaults.
command format	ip igmp snooping vlan <i>vlan_id</i> address <i>ip_address</i> no ip igmp snooping vlan <i>vlan_id</i> address
parameter	<i>vlan_id</i> : Specified VLAN number; <i>ip_address</i> : The specified IP address.
Default configuration	The default IP address is 192.168.0.2.
configuration mode	Global configuration mode SWITCH(Config)#

11.2.10 show ip igmp snooping

Features	Displays IGMP Snooping information.
command format	show ip igmp snooping [<i>vlan <i>vlan_id</i></i>]
parameter	<i>vlan_id</i> : Specify the vlan number to display IGMP Snooping information.
illustrate	If no VLAN ID is specified, the IGMP Snooping and Query summary information of all VLANs will be displayed. If a VLAN number is specified, the IGMP Snooping and Query details of the VLAN are displayed.
configuration mode	Privileged User Configuration Mode SWITCH#

11.2.11 show mac-address-table multicast

Features	Display multicast MAC address table information.
----------	--

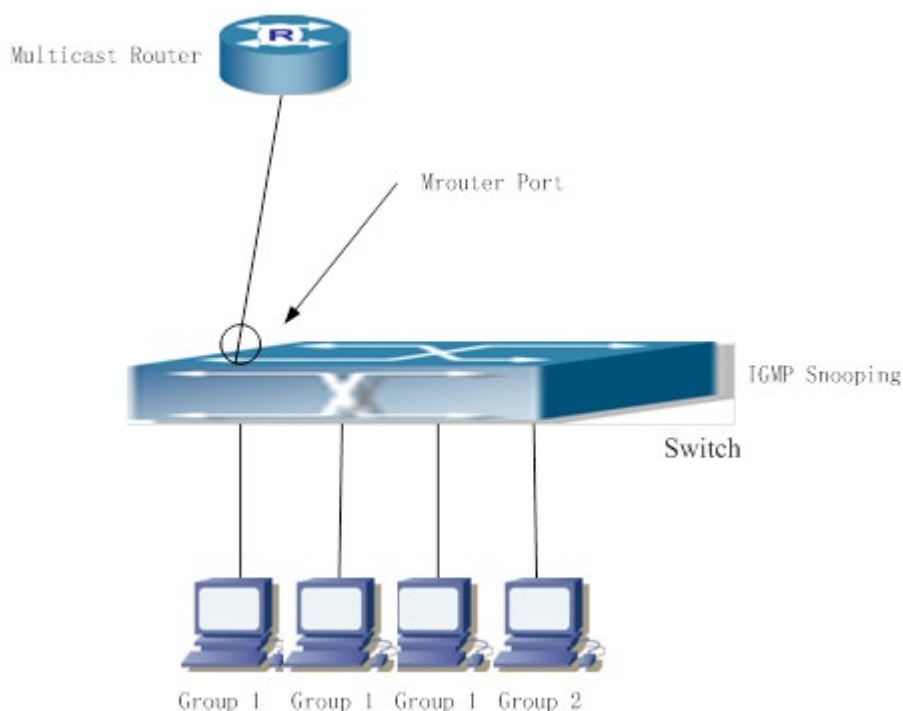
command format	show mac-address-table multicast [vlan <i>vlan_id</i>]
parameter	<i>vlan_id</i> : The VLAN ID contained in the entry to be displayed.
Default configuration	By default, the system does not display the mapping between multicast MAC addresses and ports.
illustrate	This command displays the multicast MAC address table information of the current switch.
configuration mode	Privileged User Configuration Mode SWITCH#

11.2.12 debug ip igmp snooping

Features	Turn on the debugging switch of IGMP Snooping of the switch; Turn off this debug switch.
command format	debug ip igmp snooping no debug ip igmp snooping
Default configuration	By default, the IGMP Snooping debugging switch of the switch is disabled.
illustrate	It is used to enable the IGMP Snooping debugging switch of the switch, and it can display the information about the IGMP data packet processed by the switch.
configuration mode	Privileged User Configuration Mode SWITCH#

11.3 Typical configuration example

Case 1: IGMP Snooping function.



Picture 23 Open the switch IGMP Snooping function diagram

As shown on the Picture, vlan 100 configured on the Switch includes ports 1, 2, 6, 10, and 12. The four hosts are connected to ports 2, 6, 10, and 12 respectively, and the multicast router is connected to port 1. Suppose we need to do igmp snooping on vlan 100. By default, the global igmp snooping function of the switch and the igmp snooping function of each VLAN are disabled. Therefore, it is necessary to turn on the igmp snooping function under the global, and at the same time turn on igmp snooping on vlan 100.

The configuration steps are as follows:

```
SWITCH#config
SWITCH (config)#ip igmp snooping
SWITCH (config)#ip igmp snooping vlan 100
```

Multicast configuration:

Suppose the multicast server provides two programs, using the group addresses Group1 and Group2 respectively, the multicast application software is running on the four hosts at the same time, and the three hosts connected to ports 2, 6, and 10 play program 1, which is

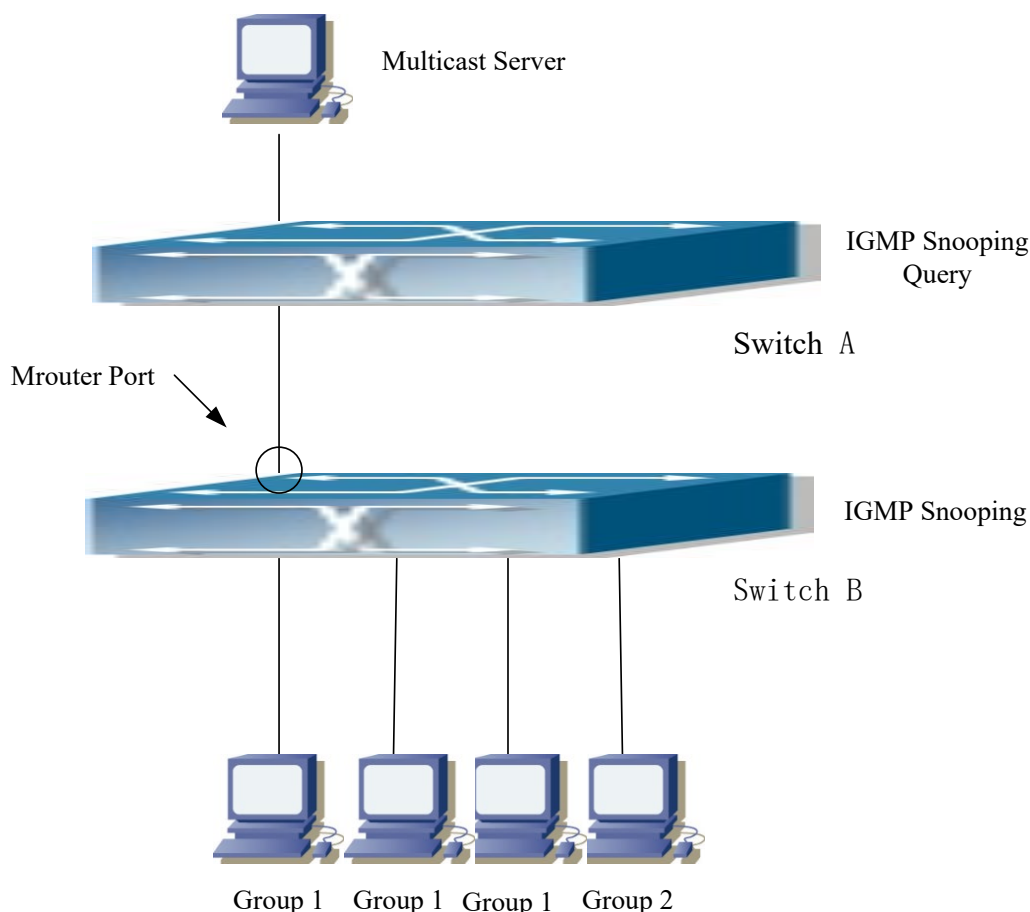
connected to port 12. host to play program 2.

IGMP snooping result:

The multicast table established by igmp snooping on vlan 100 shows that ports 1, 2, 6, and 10 are in Group1, and ports 1 and 12 are in Group2.

The four hosts can normally receive the programs they are interested in. Ports 2, 6, and 10 will not receive the traffic of program 2, and port 12 will not receive the traffic of program 1.

Case 2: IGMP Query



Picture 24 Switch as IGMP Querier Functional Diagram

VLAN 100 is configured on Switch B to include ports 1, 2, 6, 10, and 12. The four hosts are connected to ports 2, 6, 10, and 12 respectively, and port 1 is connected to Switch A. The switch Switch A functions as a multicast router. Configure vlan 100 to include ports 1 and 2.

Port 1 is connected to the multicast server, and port 2 is connected to Switch B. To periodically send queries, Switch A needs to enable igmp snooping globally and enable igmp snooping query on vlan 100. On Switch B, you need to enable igmp snooping globally and enable igmp snooping on vlan 100.

The configuration steps are as follows:

```
SwitchA#config
```

```
SwitchA(config)#ip igmp snooping
```

```
SwitchA(config)#ip igmp snooping vlan 100 query
```

```
SwitchB#config
```

```
SwitchB(config)#ip igmp snooping
```

```
SwitchB(config)#ip igmp snooping vlan 100
```

Multicast configuration:

It is assumed that the Multicast Server provides two programs, using the group addresses Group1 and Group2 respectively. The multicast application software runs on the four hosts at the same time. The three hosts connected to ports 2, 6, and 10 of SwitchB play program 1, and the host connected to port 12 of SwitchB plays program 2.

IGMP snooping snooping result:

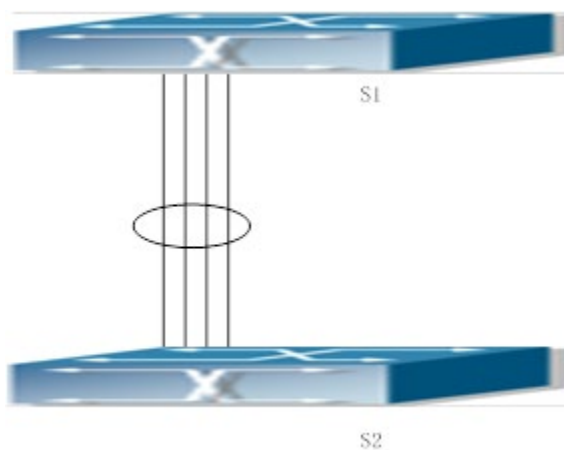
The multicast table established by igmp snooping on vlan 100 of SwitchB shows that ports 1, 2, 6, and 10 are in Group1, and ports 1 and 12 are in Group2.

The four hosts can normally receive the programs they are interested in. Ports 2, 6, and 10 of SwitchB will not receive the traffic of program 2, and port 12 will not receive the traffic of program 1.

12 Port Channel configuration

12.1 introduce

Before introducing Port Channel, let's first introduce the concept of Port Group: Port Group is a physical port group at the configuration level. Only physical ports configured in Port Group can participate in link aggregation and become a member of Port Channel. port. Logically, a Port Group is not a port, but a sequence of ports. When the physical ports added to the Port Group meet certain conditions, port aggregation is performed to form a Port Channel. This Port Channel has the attributes of a logical port, and it truly becomes an independent logical port. Port aggregation is a logical abstraction process that abstracts a group of port sequences with the same attributes into a logical port. A Port Channel is a collection of physical ports and is logically regarded as a physical port. For users, this Port Channel can be used as a port, so it can not only increase the bandwidth of the network, but also provide the backup function of the link. Port trunking is usually used when a switch is connected to a router, host or other switch.



Picture 22 Port Aggregation Diagram

As shown on the Picture above, ports 1-4 of switch S1 are aggregated into a port channel, and the bandwidth of the port channel is the sum of the bandwidth of the four ports. If there is traffic on S1 to be transmitted to S2 through the Port Channel, the Port Channel of S1 will perform the traffic distribution calculation according to the lowest digit of the source MAC address and destination MAC address of the traffic, and according to the calculation

result, a member port in the Port Channel will be responsible for the calculation. the flow. When a port in the Port Channel fails to connect, the traffic originally borne by the port will be distributed to other ports with normal connections again through the traffic distribution algorithm. The traffic distribution algorithm is determined by the hardware of the switch.

SICOM3028GPT provides two methods for configuring port aggregation: manually generating Port Channel, and LACP (Link Aggregation Control Protocol) dynamically generating Port Channel. Only ports whose duplex mode is full-duplex mode can perform port aggregation.

In order for the Port Channel to work normally, the member ports of the Port Channel of this switch must have the same attributes as follows:

- ☞ All ports are in full duplex mode;
- ☞ The port rate is the same;
- ☞ The ports are both Access ports and belong to the same VLAN or are both Trunk ports;
- ☞ If the port is a trunk port, its Allowed VLAN and Native VLAN attributes should also be the same.

When the SICOM3028GPT manually configures the Port Channel or dynamically generates the Port Channel by LACP, the system will automatically select the port with the smallest port number in the Port Channel as the Master Port of the Port Channel. If the switch enables the Spanning-tree function, Spanning-tree regards the Port Channel as a logical port, and the master port sends BPDU frames.

In addition, the realization of the port aggregation function is closely related to the hardware used by the switch. The SICOM3028GPT series switches support the aggregation of any two physical ports of the switch. The maximum number of groups is 8, and the maximum number of ports in a group is 8.

Once the aggregation port is successfully converged, it can be used as an ordinary port. In the SICOM3028GPT, the aggregation interface configuration mode is also established. Like the vlan and physical interface configuration modes, the user can perform related

aggregation ports in the aggregation interface configuration mode. configuration.

12.2 CLI configuration

Table 20 Configuration command

Order	configuration mode	Features
port-group no port-group	Global configuration mode SWITCH(Config)#	Create a new port group; Delete a port group.
port-group load-balance no port-group load-balance	Global configuration mode SWITCH(Config)#	Set the traffic sharing method; Restore the default configuration.
interface port-channel	Global configuration mode SWITCH(Config)#	Enter the aggregation interface configuration mode.
show port-group	Privileged User Configuration Mode SWITCH#	Displays the port group.
debug lacp no debug lacp	Privileged User Configuration Mode SWITCH#	Turn on the debug switch of the switch's lacp; Turn off this debug switch.

12.2.1 port-group

Features	Create a new port group; Delete a port group.
command format	port-group <i>port_group_number</i> no port-group <i>port_group_number</i>
parameter	<i>port_group_number</i> :The group number of the Port Channel, ranging from 1 to 8, if the group number already exists, an error will be reported;
configuration mode	Global configuration mode SWITCH(Config)#

12.2.2 port-group load-balance

Features	Set the traffic sharing method; Restore the default configuration.
command format	port-group load-balance { ip-l4 ip-only mac-ip mac-ip-l4 mac-only} no port-group load-balance
parameter	ip-l4 :Traffic sharing based on IP and port; ip-only :Traffic sharing based on IP addresses; mac-ip :Traffic sharing based on MAC and IP; mac-ip-l4 :Traffic sharing based on MAC, IP and port;

	mac-only :Traffic balancing is performed based on MAC addresses.
Default configuration	By default mac-only .
configuration mode	Global configuration mode SWITCH(Config)#

12.2.3 interface port-channel

Features	Enter the aggregation interface configuration mode
command format	interface port-channel <i>port_group_number</i>
parameter	<i>port_group_number</i> :The group number of the Port Channel, ranging from 1 to 8;
illustrate	Use the command exit to return from the Ethernet interface configuration mode to the global configuration configuration. This interface is automatically created when a port is added to an aggregation group, and is deleted when there is no port in the aggregation group.
configuration mode	Global configuration mode SWITCH(Config)#

12.2.4 show port-group

Features	Displays the port group.
command format	show port-group [<i>port_group_number</i>] { brief detail load-balance port port-channel }
parameter	<i>port_group_number</i> :The group number of the Port Channel to be displayed, ranging from 1 to 8; brief :display summary information; detail :show details; load-balance :Display traffic sharing information; port :Display member port information; port-channel :Displays aggregate port information.
illustrate	If no port-group-number is specified, information about all port-groups will be displayed.
configuration mode	Privileged User Configuration Mode SWITCH#

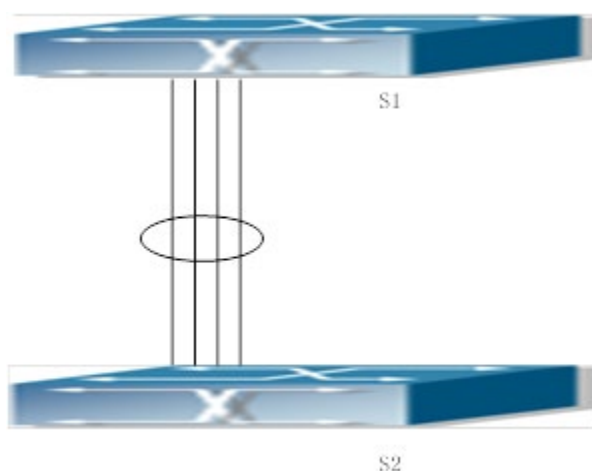
12.2.5 debug lacp

Features	Turn on the debug switch of the switch's lacp; Turn off this debug switch.
command	debug lacp

format	no debug lacp
default configuration	By default, the debug switch of lacp of the switch is disabled.
illustrate	It is used to open the switch lacp debugging switch, which can display the information of the switch processing lacp data packets.
configuration mode	Privileged User Configuration Mode SWITCH#

12.3 Typical configuration example

Case 1: Configure Port Channel in LACP mode.



Picture 23 Configuring Port Channels in LACP Mode

In the following description, Switch is used to represent SICOM3028GPT.

As shown on the Picture, ports 1, 2, and 3 on Switch1 are all access ports and belong to vlan 1. These three ports are added to group 1 in active mode, and ports 6, 8, and 9 on Switch2 are trunk ports. And it is allow all, add these three ports to group 2 in passive mode, and connect the above corresponding ports with network cables respectively. (4 wires on the picture)

The configuration steps are as follows:

```
Switch1#config
Switch1 (Config)#interface eth 1/1-3
Switch1 (Config-Port-Range)#port-group 1 mode active
Switch1 (Config-Port-Range)#exit
Switch1 (Config)#interface port-channel 1
```

```
Switch1 (Config-If-Port-Channel1)#
```

```
Switch2#config
```

```
Switch2 (Config)#port-group 2
```

```
Switch2 (Config)#interface eth 1/6
```

```
Switch2 (Config-Ethernet1/6)#port-group 2 mode passive
```

```
Switch2 (Config-Ethernet1/6)#exit
```

```
Switch2 (Config)# interface eth 1/8-9
```

```
Switch2 (Config-Port-Range)#port-group 2 mode passive
```

```
Switch2 (Config-Port-Range)#exit
```

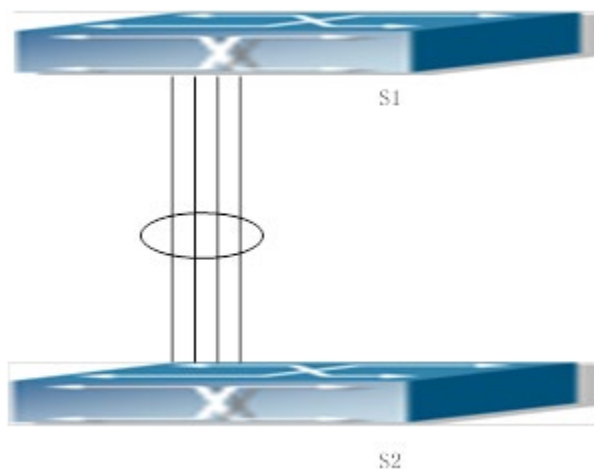
```
Switch2 (Config)#interface port-channel 2
```

```
Switch2 (Config-If-Port-Channel2)#
```

Configuration result:

After a period of time, the shell prompts that the port aggregation is successful. At this time, the ports 1, 2, and 3 of Switch1 are aggregated into an aggregation port. The aggregation port is named Port-Channel1. The port name is Port-Channel2, and both can be configured by entering the aggregation interface configuration mode.

Case 2:Configure Port Channel in ON mode.



Picture 24 Configure Port Channel in ON mode

As shown in the Picture , ports 1, 2, and 3 on Switch1 are all access ports and belong to vlan 1.

These three ports are added to group 1 in the on mode, and ports 6, 8, and 9 on Switch2 are trunk ports, and allow all, add these three ports to group 2 in on mode.

The configuration steps are as follows:

```
Switch1#config
Switch1 (Config)#interface eth 1/1
Switch1 (Config-Ethernet1/1)# port-group 1 mode on
Switch1 (Config-Ethernet1/1)#exit
Switch1 (Config)#interface eth 1/2
Switch1 (Config-Ethernet1/2)# port-group 1 mode on
Switch1 (Config-Ethernet1/2)#exit
Switch1 (Config)#interface eth 1/3
Switch1 (Config-Ethernet1/3)# port-group 1 mode on
Switch1 (Config-Ethernet1/3)#exit
```

```
Switch2#config
Switch2 (Config)#port-group 2
Switch2 (Config)#interface eth 1/6
Switch2 (Config-Ethernet1/6)#port-group 2 mode on
Switch2 (Config-Ethernet1/6)#exit
Switch2 (Config)# interface eth 1/8-9
Switch2 (Config-Port-Range)#port-group 2 mode on
Switch2 (Config-Port-Range)#exit
```

Configuration result:

After adding ports 1, 2, and 3 on the switch Switch1 to port-group1 in turn, we can see that it is completely mandatory to join a group in the on mode, and the switches at both ends will not complete the aggregation by exchanging LACP PDUs. Aggregation is also triggered. When the command to add

port 2 to port-group1 is entered, 1 and 2 are aggregated together to form port-channel1. When port 3 is added to port-group1, The three ports 1, 2, and 3 are re-aggregated into port-channel1. As a result, the three ports on Switch1 and Switch2 are all aggregated in ON mode, and each forms an aggregated port.

13 L3 forwarding configuration

SICOM3028GPT switch supports Layer 3 forwarding function. Layer 3 forwarding is to forward Layer 3 protocol packets (IP packets) across VLANs. This forwarding is addressed by IP addresses. When an interface of the switch receives an IP packet, it will perform the forwarding according to its own routing table. Search, and then decide the operation of the data packet according to the result. If the destination address of the IP packet is another subnet reachable by the switch, then the packet will be sent from the corresponding interface of the switch. SICOM3028GPT switch can use hardware to forward IP packets. The forwarding chip of SICOM3028GPT has host routing table and default routing table. Among them, the host routing table is used to store the host routes directly connected to the switch, and the default routing table stores the network segment routes (calculated by the aggregation algorithm).

When the route (host route or network segment route) required for unicast traffic forwarding exists in the forwarding chip, the traffic forwarding is completely responsible for the hardware, rather than the CPU responsible for the router, so the forwarding efficiency is greatly improved, which can achieve Wire-speed forwarding.

13.1 introduce

13.1.1 Layer 3 Interface Introduction

Layer 3 interfaces can be created on the SICOM3028GPT switch. The Layer 3 interface is not an actual physical interface, it is a virtual interface. Layer 3 interfaces are created on the basis of VLANs. A Layer 3 interface can contain one or more Layer 2 interfaces (they belong to the same VLAN), but it can also not contain any Layer 2 interface. Among the Layer 2 interfaces included in the Layer 3 interface, at least one of them must be in the UP state. The Layer 3 interface is in the UP state, otherwise it is in the DOWN state. By default, all Layer 3 interfaces in the switch use the same MAC address, which is selected from the MAC addresses reserved by the switch when the Layer 3 interface is created. The Layer 3 interface is the basis of the Layer 3 protocol. An IP address can be configured on the Layer 3 interface. The switch can transmit the IP protocol with other devices through the IP address configured

on the Layer 3 interface. The switch can also forward IP protocol packets between different Layer 3 interfaces.

13.1.2 Introduction to IP Forwarding

The gateway device can forward IP protocol packets from one subnet to another, and this forwarding is routed through routing. The IP forwarding of the SICOM3028GPT switch is assisted by hardware, which can achieve wire-speed forwarding of the port; at the same time, it can also provide various flexible controls to adjust and monitor the forwarding behavior. The SICOM3028GPT switch can support the aggregation algorithm that prohibits or allows optimization to adjust the generation of network segment routing entries in the switch chip, check the statistics of IP forwarding, monitor the sending and receiving status of IP packets, and check the status of the hardware forwarding chip.

13.1.3 Introduction to ARP

ARP (Address Resolution Protocol) address resolution protocol, mainly used for IP address to Ethernet MAC address resolution. In addition to supporting dynamic ARP, SICOM3028GPT also supports static configuration. In addition, in some applications, SICOM3028GPT also supports the configuration of proxy ARP. For example, when the interface of the switch receives an ARP request, the requested IP address and the interface address are in the same IP network segment, but not in the same physical network. If the interface has the proxy ARP function enabled, the interface will send its own ARP request. The MAC address is used as a response to the ARP, and then the actual data packets received are forwarded. Enabling the proxy ARP function can make machines that are separated from the physical network but belong to the same IP network segment ignore the fact that the physical network is separated, and forward through the proxy ARP interface as if they are in a physical network.

13.2 CLI configuration

Table 21 Configuration command

Order	configuration mode	Features
interface vlan no interface vlan	Global configuration mode SWITCH(Config)#	Create a VLAN interface, i.e. Create a Layer 3 interface of a switch; Delete the Layer 3 interface specified by the switch.
ip fib optimize no ip fib optimize	Global configuration mode SWITCH(Config)#	Configure the switch to use the optimized IP route aggregation algorithm; The optimized IP route aggregation algorithm is not used.
show ip traffic	Privileged User Configuration Mode SWITCH#	Display IP packet statistics.
debug ip packet no debug ip packet	Privileged User Configuration Mode SWITCH#	Turn on the IP packet debugging switch; Turn off this debug switch.
arp no arp	VLAN interface configuration mode SWITCH(Config-If-Vlan100)#	Configure static ARP entries; Delete static ARP entries.
ip proxy-arp no ip proxy-arp	VLAN interface configuration mode SWITCH(Config-If-Vlan100)#	Enable the proxy ARP function of the VLAN interface; Disable the function of proxy ARP.
clear arp	Privileged User Configuration Mode SWITCH#	Clear all dynamic ARP entries.
show arp	Privileged User Configuration Mode SWITCH#	Display the ARP mapping table.
debug arp no debug arp	Privileged User Configuration Mode SWITCH#	Turn on the ARP debugging switch; Turn off this debugging feature.

13.2.1 interface vlan

Features	Create a VLAN interface, i.e. Create a Layer 3 interface of a switch; Delete the Layer 3 interface specified by the switch.
command format	interface vlan <i>vlan_id</i> no interface vlan <i>vlan_id</i>
parameter	<i>vlan_id</i> : ID of the established VLAN.
Default configuration	There are no Layer 3 interfaces.
illustrate	Before creating a VLAN interface (Layer 3 interface), you need to configure a VLAN. For details, see the chapter on VLAN. Use this command to enter the VLAN interface (Layer 3 interface) configuration mode while creating a VLAN interface (Layer 3

	interface). After the VLAN interface (Layer 3 interface) is created, you can still use the interface vlan command to enter the Layer 3 interface mode.
configuration mode	Global configuration mode SWITCH(Config)#

13.2.2 ip fib optimize

Features	Configure the switch to use the optimized IP route aggregation algorithm; The optimized IP route aggregation algorithm is not used.
command format	ip fib optimize no ip fib optimize
Default configuration	The optimized IP route aggregation algorithm is not applicable.
illustrate	This command is used to optimize the aggregation algorithm. The optimization method is: if the routing table does not have a default route, construct a virtual default route based on the next hop that is most quoted to simplify the aggregation result. The advantage of using this method is that it simplifies the result of aggregation more effectively; the disadvantage is that although the CPU load of the switch is reduced (by adding the virtual default route to the routing table entry of the chip network segment), it may introduce unnecessary changes to the next-hop switch. Necessary data flow (actually transferring part of the CPU load of this switch to the next-hop switch).
configuration mode	Global configuration mode SWITCH(Config)#

13.2.3 show ip traffic

Features	Display IP packet statistics.
command format	show ip traffic
illustrate	Displays statistical information such as IP and ICMP packet reception and transmission.
configuration mode	Privileged User Configuration Mode SWITCH#

Example:

Switch #show ip traffic

IP statistics:

Rcvd: 290 total, 44 local destinations
 0 header errors, 0 address errors
 0 unknown protocol, 0 discards
 Frags: 0 reassembled, 0 timeouts
 0 fragment rcvd, 0 fragment dropped
 0 fragmented, 0 couldn't fragment, 0 fragment sent
 Sent: 0 generated, 0 forwarded
 0 dropped, 0 no route

ICMP statistics:

Rcvd: 0 total 0 errors 0 time exceeded
 0 redirects, 0 unreachable, 0 echo, 0 echo replies
 0 mask requests, 0 mask replies, 0 quench
 0 parameter, 0 timestamp, 0 timestamp replies
 Sent: 0 total 0 errors 0 time exceeded
 0 redirects, 0 unreachable, 0 echo, 0 echo replies
 0 mask requests, 0 mask replies, 0 quench
 0 parameter, 0 timestamp, 0 timestamp replies

Display information	explain
IP statistics:	Statistics of IP packets:
Rcvd: 290 total, 44 local destinations 0 header errors, 0 address errors 0 unknown protocol, 0 discards	Statistics of the total amount received and how many arrived locally, how many packets have errors in the header, how many addresses have errors, how many packets with unknown protocols, how many packets are lost, etc.
Frag: 0 reassembled, 0 timeouts 0 fragment rcvd, 0 fragment dropped 0 fragmented, 0 couldn't fragment, 0 fragment sent	Fragmentation statistics: How many packets are reassembled, how many are overtime, the number of received fragments, the number of lost fragments, how many cannot be fragmented, how many fragments are sent, etc.
Sent: 0 generated, 0 forwarded 0 dropped, 0 no route	Statistics of the total amount of sending and how many are generated locally, how many are

	forwarded, how many are lost, how many are not routed, etc.
ICMP statistics:	Statistics for ICMP packets:
Rcvd: 0 total 0 errors 0 time exceeded 0 redirects, 0 unreachable, 0 echo, 0 echo replies 0 mask requests, 0 mask replies, 0 quench 0 parameter, 0 timestamp, 0 timestamp replies	Receive the statistics of the total amount of ICMP data packets and classify these ICMP data packets, and the statistical data after classification.
Sent: 0 total 0 errors 0 time exceeded 0 redirects, 0 unreachable, 0 echo, 0 echo replies 0 mask requests, 0 mask replies, 0 quench 0 parameter, 0 timestamp, 0 timestamp replies	Send the statistics of the total amount of ICMP data packets and classify these ICMP data packets, and the statistical data after classification.

13.2.4 debug ip packet

Features	Turn on the IP packet debugging switch; Turn off this debug switch.
command format	debug ip packet no debug ip packet
Default configuration	The debug switch is disabled by default.
illustrate	Display the content of received or sent IP data packets, including: source address, destination address, number of bytes, etc.
configuration mode	Privileged User Configuration Mode SWITCH#

13.2.5 arp

Features	Configure static ARP entries; Delete static ARP entries.
command format	arp ip_address mac_address [ethernet] port_name no arp ip_address
parameter	<i>ip_address</i> : IP address; <i>mac_address</i> : MAC address; <i>port_name</i> : Layer 2 port name.
Default configuration	By default, there is no static ARP entry.
configuration	VLAN interface configuration mode SWITCH(Config-If-Vlan100)#

mode	
------	--

13.2.6 ip proxy-arp

Features	Enable the proxy ARP function of the VLAN interface; Disable the function of proxy ARP.
command format	ip proxy-arp no ip proxy-arp
Default configuration	The default proxy ARP function is disabled.
illustrate	When the Layer 3 interface of the switch receives an ARP request, the requested IP address and the address of the Layer 3 interface are in the same IP network segment, but not in the same physical network. If the Layer 3 interface has the function of proxy ARP enabled, The Layer 3 interface will use its own MAC address as the ARP response, and then forward the actual data packets it receives. Enabling this function can make the machines that belong to the same IP network segment ignore the fact that the physical network is separated because the physical network is separated, and the forwarding through the proxy ARP interface seems to be in a physical network. Before the proxy ARP responds to the ARP request, it needs to look up the routing table to determine whether the destination network is reachable. Only the ARP request that the destination network is reachable will respond to the ARP request. Note: ARP requests matching the default route are not proxied.
configuration mode	VLAN interface configuration mode SWITCH(Config-If-Vlan100)#

13.2.7 clear arp

Features	Clear all dynamic ARP entries.
command format	clear arp
configuration mode	Privileged User Configuration Mode SWITCH#

13.2.8 show arp

Features	Display the ARP mapping table.
command format	show arp [[ip_addr] [vlan_id] [hw_addr] [type {static dynamic}] [count]]
parameter	<i>ip_addr</i> : Display the entry of the specified IP address;

	<i>vlan_id</i> : Display the entry with the specified vlan identifier; <i>hw_addr</i> : Display the entry for the specified Mac address; static : Display static ARP entries; dynamic : Display dynamic ARP entries; count : Display the number of ARP entries.
configuration mode	Privileged User Configuration Mode SWITCH#

Example:

Switch#sh arp

Total arp items: 3, the matched: 3, InCompleted: 0

Address Hardware Addr Interface Port Flag

50.1.1.6 00-0a-eb-51-51-38 Vlan50 Ethernet3/11 Dynamic

50.1.1.9 00-00-00-00-00-09 Vlan50 Ethernet1/1 Static

150.1.1.2 00-00-58-fc-48-9f Vlan150 Ethernet3/4 Dynamic

Display information	explain
Total arp items	The total number of Arp entries;
the matched	The number of Arp entries that meet the filtering rules;
InCompleted	The Arp request was sent, but the number of Arp entries in the Arp reply was not received;
Addrss	Arp entry IP address;
Hardware Address	Arp entry hardware address;
Interface	The Layer 3 interface corresponding to the Arp entry;
Port	The physical (Layer 2) interface corresponding to the Arp entry;
Flag	Specifies whether the Arp entry is dynamic or static.

13.2.9 debug arp

Features	Turn on the ARP debugging switch; Turn off this debugging feature.
command format	debug arp no debug arp
Default configuration	The default ARP debugging function is disabled.
illustrate	Displays the content of received or sent ARP packets, including: type, source address, and destination address.
configuration mode	Privileged User Configuration Mode SWITCH#

14 Layer 3 routing configuration

In the Internet network, in order to access another remote host, a host must select an appropriate path through a series of routers or Layer 3 switches.

A router or a Layer 3 switch calculates the path through the CPU. The difference is that the Layer 3 switch adds the calculated path to the switching chip, and the chip performs wire-speed forwarding; while the router always saves the calculated path in the routing table. And in the routing buffer area, the CPU is responsible for data forwarding. It can be seen that both routers and Layer 3 switches can select paths, and Layer 3 switches have relatively strong advantages in data forwarding. SICOM3028GPT Layer 3 switch is a Layer 3 switch launched by KYLAND. The following briefly describes the basic principles and methods of path selection for Layer 3 switches.

In the process of path selection, each Layer 3 switch is only responsible for selecting a suitable intermediate path according to the destination address of the received data packet, and then transmits the data packet to the next Layer 3 switch until the last Layer 3 switch on the path. The switch forwards the packet to the destination host. The path chosen by each Layer 3 switch to transmit the packet to the next Layer 3 switch is called routing. Routing can be divided into direct routing, static routing and dynamic routing.

The direct route refers to the path to the network directly connected to the Layer 3 switch, and the Layer 3 switch can obtain it without calculation.

A static route refers to an artificially designated path to a network or a specific host, and static routing cannot be changed arbitrarily. The advantages of static routing are that it is simple and easy to configure, stable, and restricts illegal route changes, facilitates load sharing, and facilitates route backup. However, because it is an artificial setting, the routing that needs to be set for a large network is too large and complicated, so it is not suitable for medium and large networks.

Dynamic routing means that the Layer 3 switch dynamically calculates the path to a network or a specific host according to the activated routing protocol. If the next hop Layer 3 switch in the path is unreachable, the Layer 3 switch can automatically discard the path passing through the Layer 3 switch and select the path passing through other Layer 3 switches.

Dynamic routing protocols are generally divided into two categories: Interior Gateway Routing

Protocol (IGP) and Exterior Gateway Routing Protocol (EGP). The Interior Gateway Routing Protocol (IGP) is a protocol used to compute routes to destinations within an autonomous system. The internal gateway dynamic routing protocols supported by the SICOM3028GPTGC Layer 3 switch include RIP and OSPF routing protocols, and RIP and OSPF routing protocols can be configured as required. SICOM3028GPT Layer 3 switch supports running multiple internal gateway dynamic routing protocols at the same time, and can also re-introduce other dynamic routing protocols and static routes in a dynamic routing protocol to connect multiple routing protocols.

14.1 routing table

As mentioned above, the Layer 3 switch is mainly used to establish a route for the current Layer 3 switch to reach a certain network or a specific host, and forward data packets according to the route. Each Layer 3 switch has a routing table that records all routes used by the Layer 3 switch. Each routing entry in the routing table indicates which vlan interface of a Layer 3 switch a packet to a certain subnet or host should send through, so that it can reach the destination host or the next Layer 3 switch in the path to the destination host.

The routing table contains the following main contents:

1. Destination address: used to identify the destination address or destination network of the IP data packet.
2. Netmask: Together with the destination address, it identifies the network segment address of the network segment where the destination host or Layer 3 switch is located. The netmask consists of several consecutive "1"s, usually identified by dotted decimal (usually an address consisting of 1 to 4 255s). After "ANDing" the destination address and the network mask, the network address of the destination host or the network segment where the Layer 3 switch is located can be obtained. For example, if the destination address is 200.1.1.1, the network address of the host or layer 3 switch with the mask of 255.255.255.0 is 200.1.1.0.
3. Output interface: Indicate which interface of the Layer 3 switch the IP data packet will be forwarded from.
4. Next Layer 3 Switch (Next Hop) IP Address: Indicates the next Layer 3 switch through which IP packets will pass.
5. Route item priority: For the same destination, there may be several routes with different next hops. These routes may be discovered by different dynamic routing protocols, or may be manually configured static routes. The one with higher priority (smaller value) will become the current optimal route. Users can configure multiple

routes to the same destination with different priorities, and the Layer 3 switch will select a unique route for IP packet forwarding in priority order.

In order not to make the routing table too large, a default route can be set. Once the routing table lookup fails, the default route is selected to forward the packet.

The various routing protocols supported by the SICOM3028GPT Layer 3 switch and the default priorities of the discovered routes are shown in the following table:

Routing protocol or routing type	priority default
Direct routing	0
OSPF	110
Static routing (static)	1
RIP	120
OSPF ASE	150
unknown route	255

14.2 static routing

14.2.1 Introduction to Static Routing

As mentioned earlier, a static route is an artificially assigned path to a network or a specific host. The advantages of static routing are that it is simple and easy to configure, stable, and can prohibit illegal route changes, and is convenient for load sharing and route backup. However, it also has many disadvantages. Static routes are static. Once the network fails, the route cannot be automatically modified, and must be manually configured. It is not suitable for medium and large networks.

Static routing is mainly used in two cases: 1) For a stable network, in order to reduce the load of routing and routing data flow, static routing can be used. For example, routing to the STUB network can be static routing. 2) In order to realize route backup, you can use static route (configure static route on the backup line, the priority of the route is lower than that of the main line).

Static routes and dynamic routes can exist at the same time. Layer 3 switches select the route with the highest priority according to different routing protocol priorities. At the same

time, in dynamic routing, static routes can be added to dynamic routes by redistributing static routes, and the priority of importing static routes can be changed as required.

14.2.2 Introduction to Default Routing

The default route is also a static route, which is used when no matching route is found. In the routing table, the default route is represented as a route with a destination address of 0.0.0.0 and a netmask of 0.0.0.0. If there is no destination for the data packet in the routing table, and there is no default route, the data packet is discarded, and an ICMP datagram is returned to the source address indicating that the destination address or the network is unreachable.

14.2.3 CLI configuration

Table 22 Configuration command

Order	configuration mode	Features
ip route no ip route	Global configuration mode SWITCH(Config)#	configure static routes; Delete static routes.
show ip route	Privileged User Configuration Mode SWITCH#	Display the routing table.

14.2.3.1 ip route

Features	configure static routes; Delete static routes.
command format	ip route <i>ip_address</i> mask gateway [preference] no ip route <i>ip_address</i> mask gateway [preference]
parameter	<i>ip_address</i> : destination IP address; <i>mask</i> : Subnet mask, in dotted decimal format; <i>gateway</i> : IP address of the next hop, in dotted decimal format; <i>preference</i> : Route priority, the value ranges from 1 to 255. The smaller the value of preference, the higher the priority.
Default configuration	The default priority of static routes is 1.
illustrate	When configuring the next hop of a static route, you can use the specified route to send the next hop IP address.

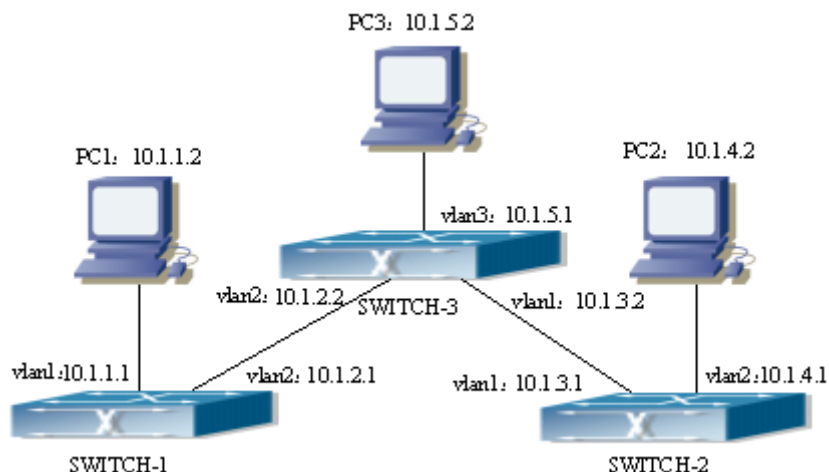
configuration mode	Global configuration mode SWITCH(Config)#
--------------------	---

14.2.3.2 show ip route

Features	Display the routing table.
command format	show ip route [destdestination] [maskdestMask] [nextHopnextHopValue] [protocol {connected static rip ospf ospf_ase bgp dvmrp}] [vlan_id] [preferencepref] [count]
parameter	<i>destination</i> : target network address; <i>destMask</i> : The mask of the target network; <i>nextHopValue</i> : next hop IP address; connected : Direct route; static : static route; rip : RIP route; ospf : OSPF route; ospf_ase : Route imported by OSPF; bgp : BGP route; dvmrp : DVMRP route; <i>vlan_id</i> : Vlan identifier; <i>pref</i> :Route priority, the value ranges from 0 to 255; count : Displays the number of IP routing entries.
configuration mode	Privileged User Configuration Mode SWITCH#

14.2.4 Typical configuration example

The Picture below is a simple network composed of three SICOM3028GPT Layer 3 switches. The netmask of each Layer 3 switch and the IP address of the PC is 255.255.255.0. Between SWITCH-1 and SWITCH-3, static routes are configured to enable communication between PC1 and PC3. The communication between PC3 and PC2 is realized by configuring a static route to SWITCH-2 on SWITCH-3. PC2 to The communication between PC3 is realized by configuring the default route on SWITCH-2.



Picture 25 Static routing diagram

Configuration steps:

Configuration of Layer 3 Switch SWITCH-1

```
Switch#config
```

```
Switch(config)#ip route 10.1.5.0 255.255.255.0 10.1.2.2
```

Configuration of Layer 3 Switch SWITCH-3

```
Switch#config
```

! The next hop uses the peer IP address

```
Switch(config)#ip route 10.1.1.0 255.255.255.0 10.1.2.1
```

! The next hop uses the peer IP address

```
Switch(config)#ip route 10.1.4.0 255.255.255.0 10.1.3.1
```

Configuration of Layer 3 Switch SWITCH-2

```
Switch#config
```

```
Switch(config)#ip route 0.0.0.0 0.0.0.0 10.1.3.2
```

In this way, PC1 and PC3, PC2 and PC3 can all be pinged.

14.3 RIP

14.3.1 Introduction to RIP

The RIP protocol was first used in the ARPANET network and was specially used in small

and simple networks. RIP protocol is a distance vector routing protocol based on Bellman-Ford algorithm. Network devices running distance vector protocols periodically send two types of information to neighboring devices:

- The number of hops taken to reach the destination network, that is, the metric used, or the number of passes through the network.
- What is the next hop, or the direction (vector) to be used by the network to reach the destination.

Distance vector Layer 3 switches periodically send their entire routing tables to neighboring Layer 3 switches. The Layer 3 switch builds its own routing information table on the basis of the information received from the adjacent Layer 3 switch. Then, pass the information to its adjacent Layer 3 switch. The result is that the routing table is built on the basis of second-hand information, and routes with a distance cost of more than 15 hops will be considered unreachable.

RIP protocol is an optional routing protocol, it is a UDP-based protocol, each host using RIP sends and receives datagrams on port 520 of UDP. All Layer 3 switches running the RIP protocol send routing table update information to all neighboring Layer 3 switches every 30 seconds. If no information is received from the peer within 180 seconds, the device is considered crashed or the connected network is unreachable. But the route to the Layer 3 switch will remain in the routing table for 120 seconds before being deleted.

Since the Layer 3 switches running the RIP protocol use second-hand information to build routing tables, they will encounter at least one problem - the infinite counting problem. For a network running the RIP routing protocol, when a RIP route becomes unreachable, the RIP Layer 3 switch usually does not send a routing update packet immediately, but waits until the periodic update interval (every 30 seconds) is reached. An update datagram for this routing information. If the neighbor sends a datagram containing the routing table information of the neighbor's Layer 3 switch to the Layer 3 switch before receiving the update packet, it will cause an "infinite count" phenomenon, that is, the unreachable Layer 3 switch will appear. The phenomenon that the routing metric is fixedly incremented. This greatly affects route

selection and route aggregation time.

In order to avoid the phenomenon of "infinite counting", the RIP protocol provides mechanisms such as "split horizon" and "triggered update" to solve the routing loop problem. The principle of "split horizon" is to avoid sending the route learned from the gateway to the gateway, which includes "simple split horizon" - deleting the routes learned from the neighbor gateway that will be sent to the neighbor gateway, and "reverse toxicity level" Split" - not only delete the above routes in the update packet, but also set the cost of these routes to infinity. The "triggered update" mechanism defines that whenever the gateway changes the routing metric, the update datagram will be broadcast immediately, regardless of the status of the 30-second update timer.

The RIP protocol includes version 1 and version 2: the RIP-I protocol is introduced in RFC1058; the RIP-II protocol is introduced in RFC2453, and is compatible with RFC1723 and RFC1388. RIP-I sends routing update datagrams by sending broadcast datagrams. It does not support subnet masks and authentication. There are some fields in the datagram of RIP-I that are not used and are required to be guaranteed to be all "0". Therefore, if RIP-I is used, all "0" fields should be checked. If these fields are not "0", this RIP- I datagram. RIP-II version is more perfect than RIP-I version. It sends routing update datagram by sending multicast datagram (multicast address is 224.0.0.9). It adds subnet mask field and RIP verification field (support simple plaintext password and MD5 password authentication), supports variable-length subnet mask. RIP-II uses some of the all-zero fields in RIP-I, so there is no need for an all-zero field check. KYLAND series Layer 3 switches send RIP-II datagrams and receive RIP-I and RIP-II datagrams by default.

Each Layer 3 switch running the RIP protocol has a routing database, which contains all the routing items of the reachable destinations of the Layer 3 switch, and establishes a routing table based on this. When the RIP Layer 3 switch sends a routing update datagram to its adjacent device, the routing update datagram contains the entire routing table established by the Layer 3 switch according to the routing database. Therefore, for a larger network system, each Layer 3 switch needs to transmit and process a large amount of routing data and has a

heavy burden, which greatly affects the network performance.

At the same time, the RIP protocol supports importing routing information discovered by other routing protocols into the routing table.

The operation process of the RIP protocol is described as follows:

1. Start RIP and send request datagrams to its adjacent Layer 3 switches in the form of broadcast. After receiving the request datagram, the adjacent device responds to the request and returns a response datagram containing local routing information.
2. After the Layer 3 switch receives the response datagram, it modifies the local routing table, and at the same time sends a trigger update datagram to adjacent devices to broadcast the routing update information. After receiving the trigger update datagram, the adjacent Layer 3 switch sends the trigger update datagram to its adjacent Layer 3 switch. After a series of broadcasts that trigger the update report, each Layer 3 switch obtains and maintains the latest routing information.

At the same time, the RIP Layer 3 switch broadcasts the local routing table to its neighboring devices every 30 seconds. After receiving the datagram, the adjacent devices maintain the local route, select the best route and broadcast the update information to their respective devices, so that the updated route is finally globally effective. In addition, RIP uses a timeout mechanism to process outdated routes, that is, if the Layer 3 switch does not receive a periodic update datagram from a neighbor within a certain time interval (invalid timer interval), it will consider the route from the Layer 3 switch. It is an invalid route, and then the route is kept in the routing table for a certain time interval (holddown timer interval), and finally the route is deleted.

14.3.2 CLI configuration

Table 23 Configuration command

Order	configuration mode	Features
auto-summary no auto-summary	RIP protocol configuration mode SWITCH(Config-Router-Rip)#	Configure the route aggregation function; Cancel the route aggregation function.
default-metric no default-metric	RIP protocol configuration mode SWITCH(Config-Router-Rip)#	Set the default route metric of imported routes; Restore default values.

ip rip authentication key-chain no ip rip authentication key-chain	interface configuration mode SWITCH(Config-Ethernet1/1)#	Set the key used for RIP authentication; Cancel RIP verification.
ip rip authentication mode	interface configuration mode SWITCH(Config-Ethernet1/1)#	Set the type of authentication used; Restore the default authentication type, which is text authentication.
ip rip metricin no ip rip metricin	interface configuration mode SWITCH(Config-Ethernet1/1)#	Set the additional routing metric added to receive RIP packets on the interface; Restore default values.
ip rip metricout no ip rip metricout	interface configuration mode SWITCH(Config-Ethernet1/1)#	Set the additional routing metric added to send RIP packets from the interface; Restore default values.
ip rip input no ip rip input	interface configuration mode SWITCH(Config-Ethernet1/1)#	Set the interface to be able to receive RIP packets; The interface cannot receive RIP packets.
ip rip output no ip rip output	interface configuration mode SWITCH(Config-Ethernet1/1)#	Set the interface to be able to send out RIP packets; The interface cannot send out RIP packets.
ip rip receive version no ip rip receive version	interface configuration mode SWITCH(Config-Ethernet1/1)#	Set the version information of RIP packets received by the interface; Restore default values.
ip rip send version no ip rip send version	interface configuration mode SWITCH(Config-Ethernet1/1)#	Set the version of RIP packets sent by the interface; Restore default values.
ip rip work no ip rip work	interface configuration mode SWITCH(Config-Ethernet1/1)#	Set the interface to run the RIP protocol; This interface does not send and receive RIP packets.
ip split-horizon no ip split-horizon	interface configuration mode SWITCH(Config-Ethernet1/1)#	Set to allow horizontal split; Horizontal splitting is prohibited.
redistribute no redistribute	RIP protocol configuration mode SWITCH(Config-	Import routes of other routing protocols into RIP routing

	Router-Rip)#	Cancel import.
rip broadcast no rip broadcast	RIP protocol configuration mode SWITCH(Config-Router-Rip)#	Configure all interfaces of the Layer 3 switch to send RIP broadcast packets or multicast packets; All ports are prohibited from sending broadcast packets or multicast packets, and only RIP packets can be sent between Layer 3 switches configured with neighbors.
rip checkzero no rip checkzero	RIP protocol configuration mode SWITCH(Config-Router-Rip)#	Use this command to check the zero field of RIPv1 packets; Cancel the zero search operation for the zero field.
rip preference no rip preference	RIP protocol configuration mode SWITCH(Config-Router-Rip)#	Specifies the routing priority of the RIP protocol; Restore default values.
router rip no router rip	Global configuration mode SWITCH(Config)#	Start the RIP routing process and enter the RIP configuration mode; Disable the RIP routing protocol.
timer basic no timer basic	RIP protocol configuration mode SWITCH(Config-Router-Rip)#	Adjust the time of RIP timer update, expiration and suppression; Restore the default values of various parameters.
version no version	RIP protocol configuration mode SWITCH(Config-Router-Rip)#	Set the version of RIP packets sent/received by all router interfaces; Restore default settings.
show ip protocols	Privileged User Configuration Mode SWITCH#	Displays information about the routing protocols currently running on the Layer 3 switch.
show ip rip	Privileged User Configuration Mode SWITCH#	Displays the current running status and configuration information of RIP.
debug ip rip no debug ip rip	Privileged User Configuration Mode SWITCH#	Turn on the RIP related debugging switch; Disable the RIP-related debugging switch.

14.3.2.1 auto-summary

Features	Configure the route aggregation function; Cancel the route aggregation function.
command format	auto-summary no auto-summary
Default configuration	Do not Use the automatic route aggregation feature.
illustrate	Route aggregation reduces the amount of routing information in the routing table and also reduces the amount of information exchanged. RIP-1 does not support subnet masks, which may cause ambiguity if subnet routes are forwarded. Therefore, RIP-1 always enables the route aggregation function. If you use RIP-2, you can disable the route aggregation function with the no auto-summary command. When you need to broadcast subnet routes, you can disable the route aggregation function.
configuration mode	RIP protocol configuration mode SWITCH(Config-Router-Rip)#

14.3.2.2 default-metric

Features	Set the default route metric of imported routes; Restore default values.
command format	default-metric <i>value</i> no default-metric
parameter	<i>value</i> : The routing weight to be set, ranging from 1 to 16.
Default configuration	The default routing metric is 1.
illustrate	default-metric The command is used to set the default route metric used when importing routes of other routing protocols into RIP routes. When using the redistribute command to import routes of other protocols, if no specific route metric is specified, the default route metric specified by default-metric is used.
configuration mode	RIP protocol configuration mode SWITCH(Config-Router-Rip)#

14.3.2.3 ip rip authentication key-chain

Features	Set the key used for RIP authentication; Cancel RIP verification.
command format	ip rip authentication key-chain <i>name_of_chain</i> no ip rip authentication key-chain

parameter	<i>name_of_chain</i> : Chain name.
Default configuration	By default, no RIP authentication is performed.
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

14.3.2.4 ip rip authentication mode

Features	Set the type of authentication used; Restore the default authentication type, which is text authentication.
command format	ip rip authentication mode {text md5 type {cisco usual}} no ip rip authentication mode
parameter	text : text validation; md5 : Indicates MD5 verification, and MD5 verification is divided into two verification methods: Cisco MD5 and conventional MD5.
Default configuration	Text authentication is used by default.
illustrate	RIP-I does not support authentication, RIP-II supports two kinds of authentication: text authentication (ie Simple authentication) and datagram authentication (ie MD5 authentication). There are two datagram formats for MD5 authentication: one follows the RFC1723 (RIP Version 2 Carrying Additional Information) regulations, and the other follows the RFC2082 (RIP-II MD5 Authentication) regulations.
configuration mode	interface configuration mode SWITCH(Config-Ethernet2/1)#

14.3.2.5 ip rip metricin

Features	Set the additional routing metric added to receive RIP packets on the interface; Restore default values.
command format	ip rip metricinvalue no ip rip metricin
parameter	<i>value</i> : Additional routing weight, ranging from 1 to 15.
Default configuration	When RIP receives packets, the default additional routing metric is 1.
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

14.3.2.6 ip rip metricout

Features	Set the additional routing metric added to send RIP packets from the interface;
----------	---

	Restore default values.
command format	ip rip metricout value no ip rip metricout
parameter	<i>value</i> : Additional routing weight, ranging from 0 to 15.
Default configuration	When RIP sends packets, the default additional routing metric is 0.
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

14.3.2.7 ip rip input

Features	Set the interface to be able to receive RIP packets; The interface cannot receive RIP packets.
command format	ip rip input no ip rip input
Default configuration	The interface receives RIP packets by default.
illustrate	This command is used in cooperation with the other two commands ip rip output and ip rip work. ip rip work is functionally equivalent to ip rip input & ip rip output. The latter two commands respectively control the reception of RIP packets on the interface. And send, the former command is equal to the sum of the effect of the latter two commands.
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

14.3.2.8 ip rip output

Features	Set the interface to be able to send out RIP packets; The interface cannot send out RIP packets.
command format	ip rip output no ip rip output
Default configuration	The interface sends RIP packets by default.
illustrate	This command is used in cooperation with the other two commands ip rip output and ip rip work. ip rip work is functionally equivalent to ip rip input & ip rip output. The latter two commands respectively control the reception of RIP packets on the interface. And send, the former command is equal to the sum of the effect of the latter two commands.
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

mode	
------	--

14.3.2.9 ip rip receive version

Features	Set the version information of RIP packets received by the interface; Restore default values.
command format	ip rip receive version {v1 v2 v12} no ip rip receive version
parameter	v1 : RIP version 1; v2 : RIP version 2; v12 : RIP version 1, 2.
Default configuration	The default is v12, that is, all RIP versions 1 and 2 are received.
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

14.3.2.10 ip rip send version

Features	Set the version of RIP packets sent by the interface; Restore default values.
command format	ip rip send version {v1 v2 [bc mc]} no ip rip send version
parameter	v1 : RIP version 1; v2 : RIP version 2; bc : broadcast mode; mc : Multicast mode.
Default configuration	By default, the interface sends RIP version 2 packets.
illustrate	When an interface is configured to send RIP version 2 packets, the default sending mode is multicast. Only after the bc mode is set, broadcast packets can be sent on this interface.
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

14.3.2.11 ip rip work

Features	Set the interface to run the RIP protocol; This interface does not send and receive RIP packets.
command format	ip rip work no ip rip work

Default configuration	After the RIP routing switch is enabled, the interface runs the RIP protocol by default.
illustrate	This command is functionally equivalent to ip rip input & ip rip output. The latter two commands control the receiving and sending of RIP packets on the interface respectively. The former command is equal to the sum of the functions of the latter two commands.
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

14.3.2.12 ip split-horizon

Features	Set to allow horizontal split; Horizontal splitting is prohibited.
command format	ip split-horizon no ip split-horizon
Default configuration	Horizontal splits are allowed.
illustrate	Split horizon is used to prevent Routing Loops, that is, to prevent a Layer 3 switch from broadcasting a route learned from an interface from this interface.
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

14.3.2.13 redistribute

Features	Import routes of other routing protocols into RIP routing; Cancel import.
command format	redistribute { static ospf bgp } [metric value] no redistribute { static ospf bgp }
parameter	static : Specifies to import static routes; ospf : Specify imported OSPF routes; bgp : Specify imported BGP routes; <i>value</i> : Specifies the route weight with which the route is imported. The value ranges from 1 to 16.
Default configuration	RIP does not import other routes by default. If another routing protocol is imported without specifying its metric value, the default routing metric value default-metric is imported.
illustrate	Using this command, you can import other routes as RIP's own routes to improve the performance of RIP.
configuration	RIP protocol configuration mode SWITCH(Config-Router-Rip)#

mode	
------	--

14.3.2.14 rip broadcast

Features	Configure all interfaces of the Layer 3 switch to send RIP broadcast packets or multicast packets; All ports are prohibited from sending broadcast packets or multicast packets, and only RIP packets can be sent between Layer 3 switches configured with neighbors.
command format	rip broadcast no rip broadcast
Default configuration	By default, RIP broadcast packets are sent.
configuration mode	RIP protocol configuration mode SWITCH(Config-Router-Rip)#

14.3.2.15 rip checkzero

Features	Check the zero field of the RIPv1 message; Cancel the check operation on the zero field.
command format	rip checkzero no rip checkzero
Default configuration	Checked by default.
illustrate	Since there is no zero field in RIPv2 packets, this command has no effect on RIPv2.
configuration mode	RIP protocol configuration mode SWITCH(Config-Router-Rip)#

14.3.2.16 rip preference

Features	Specifies the routing priority of the RIP protocol; Restore default values.
command format	rip preference <i>value</i> no rip preference
parameter	<i>value</i> : Specifies the value of the priority, ranging from 0 to 255.
Default configuration	The default priority of the specified RIP is 120.
illustrate	Each routing protocol has its own priority, and its default value is determined by the specific routing policy. The priority level will determine which route in the core routing table is the best route obtained by the routing algorithm. You can use this command to manually adjust the RIP priority. After the priority is adjusted, it will take effect for

	new routes. Determined by the nature of the RIP protocol, the priority of RIP should not be too high.
configuration mode	RIP protocol configuration mode SWITCH(Config-Router-Rip)#

14.3.2.17 router rip

Features	Start the RIP routing process and enter the RIP configuration mode; Disable the RIP routing protocol.
command format	router rip no router rip
Default configuration	The RIP routing process is not enabled.
configuration mode	Global configuration mode SWITCH(Config)#

14.3.2.18 timer basic

Features	Adjust the time of RIP timer update, expiration and suppression; Restore the default values of various parameters.
command format	timer basic <i>update invalid holddown</i> no timer basic
parameter	<i>update</i> :The interval for sending update packets, in seconds, ranging from 1 to 2147483647; <i>invalid</i> :The time period for declaring the RIP route invalid, in seconds, ranging from 1 to 2147483647; <i>holddown</i> :Indicates the time period that a route can still exist in the routing table after it is declared invalid, in seconds, ranging from 1 to 2147483647.
Default configuration	<i>update</i> The default value is 30; the default value of <i>invalid</i> is 180; the default value of <i>holddown</i> is 120.
illustrate	By default, the system broadcasts RIP update packets every 30 seconds; when the update packet of a route cannot be received after 180 seconds, the route is considered invalid; however, the route can still exist in the routing table for 120 seconds. After 120 seconds, delete the route in the routing table. When adjusting the time of each RIP timer, it should be noted that the time of declaring the RIP route invalid should be at least greater than the time of RIP update, and the time period of holddown (that is, the time to delete the route in the routing table after the RIP route is declared invalid) should also be at least Should be greater than the RIP update time and must be an integer multiple.

configuration mode	RIP protocol configuration mode SWITCH(Config-Router-Rip)#
--------------------	--

14.3.2.19 version

Features	Set the version of RIP packets sent/received by all router interfaces; Restore default settings.
command format	version {1 2} no version
parameter	1: RIP version 1; 2: RIP version 2.
Default configuration	Send version 2, receive version 1 and 2 datagrams.
configuration mode	RIP protocol configuration mode SWITCH(Config-Router-Rip)#

14.3.2.20 show ip protocols

Features	Displays information about the routing protocols currently running on the Layer 3 switch.
command format	show ip protocols
configuration mode	Privileged User Configuration Mode SWITCH#

Example:

Switch#sh ip protocols

RIP information

rip is turning on

default metric 16

neighbour is:NULL

preference is 100

rip version information is:

interface send version receive version

vlan2 V2BC V12

vlan3 V2BC V12

vlan4 V2BC V12 (not bold)

Display information	explain
RIP is turning on	The running routing protocol is RIP protocol;
default metric	RIP protocol default metric value;
neighbour is:	The IP address of the neighboring Layer 3 switch connected to this RIP Layer 3 switch
Preference	Priority of RIP routing;
rip version information	Display version information of running RIP protocol, including sending RIP version (V1 means RIPI, V2 means RIPII), RIP sending mode (BC means broadcast, MC means multicast), receiving RIP version (V1 means RIPI, V2 means RIPII, V12 means receive both RIPI and RIPII).

14.3.2.21 show ip rip

Features	Displays the current running status and configuration information of RIP.
command format	show ip rip
configuration mode	Privileged User Configuration Mode SWITCH#

Example:

Switch#sh ip rip

RIP information

rip is turning on

default metric 16

neighbour is

preference is 100

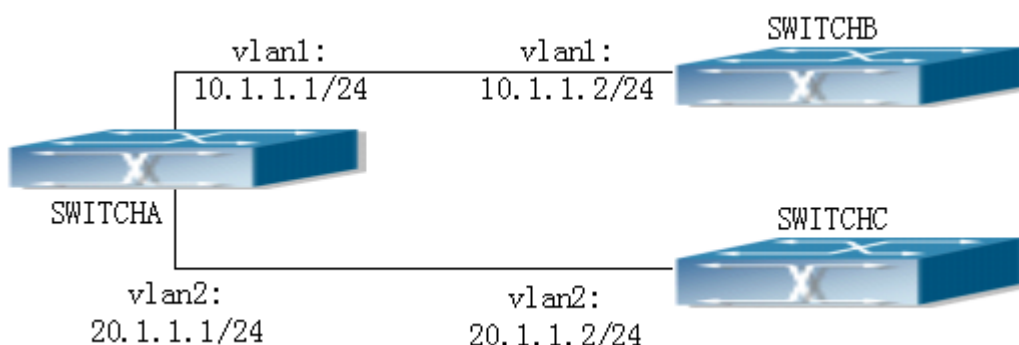
Display information	explain
rip is turning on	RIP routing process is open;

default metric 16	The default weight of imported routes is 16;
neighbour is	The destination address of the fixed-point sending;
preference is 100	The priority of the RIP route is 100.

14.3.2.22 debug ip rip

Features	Turn on the RIP related debugging switch; Disable the RIP-related debugging switch.
command format	debug ip rip [packet recv send] no debug ip rip [packet recv send]
parameter	packet : message sending and receiving information; recv : message reception information; send : message sending information.
Default configuration	The debug switch is not turned on.
configuration mode	Privileged User Configuration Mode SWITCH#

14.3.3 Typical configuration example



Picture 26 RIP case

Picture 29 It is a network composed of three Layer 3 switches. The Layer 3 switch SWITCHA is connected to the Layer 3 switch SWITCHB and the Layer 3 switch SWITCHC through the interface vlan1 and the interface vlan2 respectively. The three Layer 3 switches all run the RIP routing protocol. Set the three-layer switch SWITCHA vlan1: 10.1.1.1, vlan2: 20.1.1.1

only exchanges the update information of the Layer 3 switch with the Layer 3 switch SWITCHB vlan1: 10.1.1.2, but does not exchange the update information of the Layer 3 switch with the Layer 3 switch SWITCHC vlan2: 20.1.1.2.

The configurations of Layer 3 switches SWITCHA, SWITCHB, and SWITCHC are as follows:

a) Layer 3 switch SWITCHA:

!Configure the IP address of interface vlan1.

```
SWITCHA#config
```

```
SWITCHA(config)# interface vlan 1
```

```
SWITCHA(Config-If-Vlan1)# ip address 10.1.1.1 255.255.255.0
```

```
SWITCHA (config-If-vlan1)#exit
```

!Configure the IP address of interface vlan2

```
SWITCHA(config)# interface vlan 2
```

```
SWITCHA(config-If-vlan2)# ip address 20.1.1.1 255.255.255.0
```

! Start the RIP protocol

```
SWITCHA(config)#router rip
```

```
SWITCHA(config-router-rip)#exit
```

! Enable interface vlan1 to send/receive RIP datagrams

```
SWITCHA(config)#interface vlan 1
```

```
SWITCHA(config-If-vlan1)#ip rip work
```

```
SWITCHA(config-If-vlan1)#exit
```

! Enable interface vlan2 to send/receive RIP datagrams

```
SWITCHA (config-If-vlan2)# ip rip work
```

```
SWITCHA (config-If-vlan2)#exit
```

```
SWITCHA(config)#exit
```

```
SWITCHA#
```

b) Layer 3 switch SWITCHB:

!Configure the IP address of interface vlan1.

```
SWITCHB#config
```

```
SWITCHB(config)# interface vlan 1
```



```
SWITCHB(config-if-vlan1)# ip address 10.1.1.2 255.255.255.0
```

```
SWITCHB (config-if-vlan1)#exit
```

! Enable the RIP protocol and configure the IP address of the neighbor Layer 3 switch

```
SWITCHB(config)#router rip
```

```
SWITCHB(config-router-rip)#exit
```

! Enable interface vlan1 to send/receive RIP datagrams

```
SWITCHB(config)#interface vlan 1
```

```
SWITCHB (config-if-vlan1)#ip rip work
```

```
SWITCHB (config-if-vlan1)#exit
```

```
SWITCHB(config)#exit
```

```
SWITCHB#
```

c) Layer 3 switch SWITCHC:

! Configure the IP address of interface vlan2.

```
SWITCHC#config
```

```
SWITCHC(config)# interface vlan 2
```

```
SWITCHC(config-if-vlan2)# ip address 20.1.1.2 255.255.255.0
```

```
SWITCHC (c config-if-vlan2)#exit
```

! Start the RIP protocol

```
SWITCHC(config)#router rip
```

```
SWITCHC(config-router-rip)#exit
```

! Enable interface vlan2 to send/receive RIP datagrams

```
SWITCHC(config)#interface vlan 2
```

```
SWITCHC (config-if-vlan2)#ip rip work
```

```
SWITCHC (config-if-vlan2)#exit
```

```
SWITCHC(config)#exit
```

```
SWITCHC#
```

14.4 OSPF

14.4.1 Introduction to OSPF

OSPF (Open Shortest Path First) protocol is "Open Shortest Path First Protocol". It is a dynamic routing protocol within the autonomous system based on link state. It forms a link state database by exchanging link state information between Layer 3 switches, and then generates a routing table with the shortest path first algorithm based on this database.

An Autonomous System (AS) is a self-managing interconnected network. In a large network, such as the Internet, a very large interconnected network is decomposed into autonomous systems. A large corporate network connected to the Internet is an independent autonomous system because it does not manage other hosts on the Internet, and it does not share internal routing information with Internet Layer 3 switches.

Each link-state Layer 3 switch can provide information about the topology of its neighbor Layer 3 switches:

1. The network segment (link) connected to the Layer 3 switch
2. link status

Link state information is flooded on the network so that all Layer 3 switches can receive first-hand information. Link-state Layer 3 switches do not broadcast all the information contained in their routing tables, instead link-state Layer 3 switches will send information about the link state that has changed. Link-state Layer 3 switches will send call information to their neighbors to establish adjacencies, and then send Link State Advertisements (LSAs) between adjacent Layer 3 switches. Adjacent Layer 3 switches copy the LSA into their routing tables and pass this information on to the rest of the network. This process is called flooding. In this way, it is possible to send first-hand information to the network and establish an accurate mapping of the updated route for the network. Link-state routing protocols use a method called cost (instead of using hops) to select paths. The cost is assigned automatically or manually. According to the algorithm of the link state protocol, the cost can be calculated by the number of hops that the data packet must traverse, the link bandwidth, the current load on the link, and even the weight added by the administrator.

- 1) When a link-state Layer 3 switch enters a link-state interconnect network, it sends a call packet (HELLO) to learn about its neighbors and establish adjacencies.
- 2) Neighbors reply with information about the link they are connected to and the associated cost degree.
- 3) The originating Layer 3 switch uses this information to build its routing table.
- 4) Then, as part of regular updates. A Layer 3 switch sends link-state packets to its adjacent Layer 3 switches. This LSA includes the link of that Layer 3 switch and the associated cost.
- 5) Each adjacent Layer 3 switch replicates the LSA packet and passes the LSA to the next neighbor (ie, floods).
- 6) Because the Layer 3 switch does not recompute the routing database before flooding the LSA forward, the convergence time is greatly reduced.

A major advantage of link-state routing protocols is the fact that an infinite number of routes cannot be formed due to the way link-state protocols independently build their own routing information tables. The second advantage is that convergence is very fast in a link-state interconnection network because updates flood the interconnection network rapidly once the routing topology changes. These advantages, in turn, free up Layer 3 switch resources because less processing power and bandwidth consumption are spent on bad routing information.

Features of OSPF protocol: OSPF protocol supports networks of various scales, and can support up to hundreds of Layer 3 switches; OSPF can immediately send link state update packets after the routing topology changes, and the convergence is fast; OSPF The state adopts the shortest path algorithm to calculate the route, which ensures no self-loop routing; OSPF divides the autonomous system into multiple domains, which reduces the size of the database, reduces the occupied network bandwidth, and reduces the computational burden (according to the three-layer switch in the autonomous system) The location can be divided into intra-domain Layer 3 switches, domain boundary Layer 3 switches, autonomous system boundary Layer 3 switches, and backbone Layer 3 switches); OSPF supports load balancing and supports multiple equal-cost routes to the same destination address; OSPF supports 4-level routing mechanism (intra-domain routing, inter-domain routing, first-type external routing and second-type external routing hierarchically process routing); OSPF protocol

supports IP subnets, supports the import of routes with other routing protocols, and supports interface-based packet authentication; OSPF supports multicast sending of packets.

Each OSPF Layer 3 switch maintains a database describing the entire autonomous system topology. Each Layer 3 switch collects local state information, such as available interface information, reachable neighbor information, and then uses link state advertisements (that is, sending link state information to the outside world), and this Layer 3 switch communicates with other OSPF Layer 3 switches. The switches exchange link state information, thereby forming a link state database that describes the entire autonomous system. According to the link state database, each Layer 3 switch builds a shortest path tree with itself as the root, and this tree gives the routes to the nodes in the autonomous system. If there are two or more Layer 3 switches (that is, a multi-access network), the designated Layer 3 switch and the Backup Designated Layer 3 switch should be selected on the network, and the designated Layer 3 switch should be responsible for linking the network. The introduction of this concept helps reduce the data traffic between the Layer 3 switches on a multi-access network.

The OSPF protocol requires that the network of the autonomous system be divided into areas for management, that is, the autonomous system is divided into 0 domains (backbone domains) and non-0 domains, and the routing information transmitted between the areas is further abstracted and summarized, thereby reducing the practical bandwidth of the entire network. OSPF uses four different types of routes, which are intra-area routes, inter-area routes, type-1 external routes, and type-2 external routes in order of preference. Intra-area and inter-area routing describe the network structure inside the autonomous system, while external routing describes how to select destinations outside the autonomous system. The first type of external route corresponds to the information imported by OSPF from other internal routing protocols, and the cost of these routes is comparable to the cost of OSPF's own routing; the second type of external route corresponds to the information imported by OSPF from external routing protocols. The cost of OSPF is much greater than that of OSPF itself, so the routing cost of OSPF itself is not considered when calculating the routing cost.

The OSPF area takes the Backbone (backbone area) as the core, which is identified as the 0 domain. All other areas must be logically connected to the 0 domain, and the 0 domain must be continuous. For this reason, the concept of virtual connection is specially introduced in the backbone area to ensure that the area is still logically connected even if it is physically divided. The configurations of all Layer 3 switches in the same area must be consistent.

As mentioned above, LSAs can only be transferred between adjacent Layer 3 switches. The OSPF protocol includes five types of LSAs: router LSAs, network LSAs, summary LSAs to the networks where other domains are located, summary LSAs to the border layer 3 switches of the autonomous system, and LSA outside the autonomous system. They may also be called Type 1 LSA, Type 2 LSA, Type 3 LSA, Type 4 LSA, and Type 5 LSA, respectively. The router LSA is generated by each Layer 3 switch in the OSPF domain and sent to all other adjacent Layer 3 switches in the domain; the network LSA is generated by the designated Layer 3 switch in the OSPF domain where the multi-access network is located (to reduce For the data traffic between the three-layer switches, in the multi-access network, it is necessary to select "designated layer-3 switch" and "backup designated layer-3 switch", and the designated layer-3 switch is responsible for broadcasting the link status of the network), and sent to all other adjacent Layer 3 switches in the domain; summary LSAs are generated by OSPF domain boundary Layer 3 switches and transmitted between domain boundary Layer 3 switches; autonomous system external LSAs are generated by autonomous system external boundary Layer 3 switches, and are distributed throughout the Delivery within the autonomous system.

For the autonomous system mainly based on external link state advertisement, in order to reduce the size of the topology database, OSPF allows some domains to be configured as STUB domains. Two types of LSAs, such as type 4 LSA (ASBR summary LSA) and type 5 LSA (AS external LSA), are not allowed to flood into/through the STUB domain. The default route must be used in the STUB domain. The Layer 3 switches at the domain boundary of the STUB domain advertise default routes to the STUB domain by summarizing type 3 LSAs; these default routes are only flooded within the STUB domain, not outside the STUB domain.

Each STUB domain corresponds to a default route, and the route from the STUB domain to the external destination of the AS only depends on the default route of the domain.

The simple calculation process of OSPF protocol routing is as follows:

- 1) Each Layer 3 switch that supports OSPF maintains a link state database (ie, LS database) that describes the topology of the entire autonomous system. Each Layer 3 switch generates a link state advertisement (that is, router LSA) according to the network topology around it, and sends its LSA to other Layer 3 switches in the network by sending link state update packets (LSUs) to each other. . In this way, each Layer 3 switch has received the LSAs of other Layer 3 switches, and all LSAs together form a link state database.
- 2) Since an LSA is a description of the topology of the network around the Layer 3 switch, the LS database is a description of the topology of the entire network. Layer 3 switches can easily build a weighted directed graph based on the LS database. Obviously, all Layer 3 switches in the autonomous system will get the same network topology graph.
- 3) Each Layer 3 switch uses the shortest path SPF algorithm to calculate a shortest path tree with itself as the root. The tree gives the routes to each node in the autonomous system. The external routing information is the leaf node, and the external routing can be broadcast according to the broadcast. Its Layer 3 switches are tagged to record additional information about the autonomous system. It can be seen that the routing tables obtained by each Layer 3 switch are different.

The OSPF protocol was developed by the IETF organization, and the OSPFv2 version that is widely used at present is implemented with reference to the content described in RFC2328.

14.4.2 CLI configuration

Table 23 Configuration command

Order	configuration mode	Features
default redistribute cost no default redistribute cost	OSPF protocol configuration mode SWITCH(Config-Router-Ospf)#	Configure the default cost value when OSPF imports external routes; Restore default values.
default redistribute internal no default redistribute internal	Privileged User Configuration Mode SWITCH#	Configure the interval for importing external routes by OSPF; Restore default values.
default redistribute limit no default redistribute limit	OSPF protocol configuration mode SWITCH(Config-Router-	Configure the maximum value of external routes that OSPF can import

	Ospf)#	at one time; Restore default values.
default redistribute tag no default redistribute tag	OSPF protocol configuration mode SWITCH(Config-Router-Ospf)#	Configure the default tag value when importing external routes; Restore default values.
default redistribute type no default redistribute type	OSPF protocol configuration mode SWITCH(Config-Router-Ospf)#	Configure the interval for importing external routes by OSPF; Restore default values.
ip ospf authentication no ip ospf authentication	interface configuration mode SWITCH(Config-Ethernet1/1)#	Specifies the authentication method required to receive OSPF packets on the interface; Cancel verification.
ip ospf cost no ip ospf cost	interface configuration mode SWITCH(Config-Ethernet1/1)#	Specifies the cost required for the interface to run the OSPF protocol; Restore default values.
ip ospf dead-internal no ip ospf dead-internal	interface configuration mode SWITCH(Config-Ethernet1/1)#	Specifies the length of time for the route failure of adjacent Layer 3 switches; Restore default values.
ospf enable area no ospf enable area	interface configuration mode SWITCH(Config-Ethernet1/1)#	Configure the interface to belong to an OSPF area; Cancel this configuration.
ip ospf passive-interface no ip ospf passive-interface	interface configuration mode SWITCH(Config-Ethernet1/1)#	Set the interface to only receive and not send OSPF packets; Cancel this configuration.
ip ospf priority no ip ospf priority	interface configuration mode SWITCH(Config-Ethernet1/1)#	Configure the priority of the interface when electing the "Designated Layer 3 Switch" (DR); Restore default values.
ip ospf retransmit-internal no ip ospf retransmit-internal	interface configuration mode SWITCH(Config-Ethernet1/1)#	Configure the interval for importing external routes by OSPF; Restore default values.
ip ospf transmit-delay no ip ospf transmit-delay	interface configuration mode SWITCH(Config-Ethernet1/1)#	Specifies the retransmission interval when transmitting Link State Announcements (LSA) between the interface and the adjacent Layer 3 switch; Restore default values.

network no network	OSPF protocol configuration mode SWITCH(Config-Router- Ospf)#	Define the area to which each network of the Layer 3 switch belongs; Delete this configuration.
preference no preference	OSPF protocol configuration mode SWITCH(Config-Router- Ospf)#	Configure the priority of the OSPF protocol among routing protocols, and the priority of the imported routes outside the autonomous system; Restore default values.
redistribute ospfase no redistribute ospfase	OSPF protocol configuration mode SWITCH(Config-Router- Ospf)#	Import bgp routes, directly connected routes, static routes and RIP routes as external routing information; Cancel the imported external routing information.
router id no router id	OSPF protocol configuration mode SWITCH(Config-Router- Ospf)#	Configure a Layer 3 switch that runs the OSPF protocol ID number; Cancel the Layer 3 switch ID number.
router ospf no router ospf	Global configuration mode SWITCH(Config)#	If the OSPF protocol is enabled, it will enter the OSPF mode after it is enabled; Disable the OSPF protocol.
stub cost no stub cost	OSPF protocol configuration mode SWITCH(Config-Router- Ospf)#	Define an area as a STUB area; Cancel the definition.
virtuallink neighbored	OSPF protocol configuration mode SWITCH(Config-Router- Ospf)#	Create and configure virtual connections; Delete a virtual connection.
show ip protocols	Privileged User Configuration Mode SWITCH#	Displays information about the routing protocols currently running on the Layer 3 switch.
show ip ospf	Privileged User Configuration Mode SWITCH#	Displays the current running status and configuration information of OSPF.
debug ip ospf no debug ip ospf	Privileged User Configuration Mode SWITCH#	Turn on the OSPF related debugging switch; Disable OSPF-related debugging switches.

14.4.2.1 default redistribute cost

Features	Configure the default cost value when OSPF imports external routes; Restore default values.
command format	default redistribute cost <i>cost</i> no default redistribute cost
parameter	<i>cost</i> : Cost value, ranging from 1 to 65535.
Default configuration	The default introduced cost value is 1.
illustrate	When OSPF routing protocol imports routes discovered by other routing protocols, it regards these routing information as routing information outside its own autonomous system. Importing external routing information requires some additional parameters, such as the default cost of the route and the default label. This command provides users to set a reasonable default cost when importing external routes according to the actual situation.
configuration mode	OSPF protocol configuration mode SWITCH(Config-Router-Ospf)#

14.4.2.2 default redistribute interval

Features	Configure the interval for importing external routes by OSPF; Restore default values.
command format	default redistribute internal <i>time</i> no default redistribute internal
parameter	<i>time</i> : Interval for importing external routes, in seconds, ranging from 1 to 65535.
Default configuration	The default interval for importing external routes by OSPF is 1 second.
illustrate	OSPF will periodically import external routing information and spread the routing information to the entire AS. This command is used to modify the time interval for importing external routing information.
configuration mode	OSPF protocol configuration mode SWITCH(Config-Router-Ospf)#

14.4.2.3 default redistribute limit

Features	Configure the maximum value of external routes that OSPF can import at one time; Restore default values.
command format	default redistribute limit <i>routes</i> no default redistribute limit

parameter	<i>routes</i> : The maximum number of imported routes, ranging from 1 to 65535.
Default configuration	The maximum number of external routes imported by OSPF is 100 by default.
illustrate	OSPF periodically imports external routing information and spreads it to the entire autonomous system. This command specifies the maximum number of external routing information that can be imported at one time.
configuration mode	OSPF protocol configuration mode SWITCH(Config-Router-Ospf)#

14.4.2.4 default redistribute tag

Features	Configure the default tag value when importing external routes; Restore default values.
command format	default redistribute tag <i>tag</i> no default redistribute tag
parameter	<i>tag</i> : Flag value, the value range is 0 to 4294967295.
Default configuration	Default is 0.
illustrate	When OSPF routing protocol imports routes discovered by other routing protocols, it regards these routing information as routing information outside its own autonomous system. Importing external routing information requires some additional parameters, such as the default cost of the route and the default label. This command provides the user with information related to the routing tag identification protocol.
configuration mode	OSPF protocol configuration mode SWITCH(Config-Router-Ospf)#

14.4.2.5 default redistribute type

Features	Configure the interval for importing external routes by OSPF; Restore default values.
command format	default redistribute type {1 2} no default redistribute type
parameter	1 : The first type of external routing; 2 : The second type of external routing.
Default configuration	By default, the system considers the imported external routes to be the second type of external routes.
illustrate	OSPF specifies two types of cost selection methods for external routing information in the protocol: the first type of external routing and the second type of external routing. The cost of the first type of external route = the advertisement cost of the external

	route + the cost from a certain Layer 3 switch to the advertisement Layer 3 switch (the AS external Layer 3 switch). The cost of the second type of external route = the advertisement cost of the external route. When the first type of external route and the second type of external route exist at the same time, the first type of external route cost has a higher priority.
configuration mode	OSPF protocol configuration mode SWITCH(Config-Router-Ospf)#

14.4.2.6 ip ospf authentication

Features	Specifies the authentication method required to receive OSPF packets on the interface; Cancel verification.
command format	ip ospf authentication {simpleauth_key md5auth_key key_id} no ip ospf authentication
parameter	simple : Simple verification method; md5 : MD5 encryption authentication method; <i>auth_key</i> :The verification key is a continuous string with a maximum length of 8 bytes in simple verification mode and 16 bytes in MD5 verification mode; <i>key_id</i> :Authentication word in MD5 authentication mode, the value ranges from 1 to 255.
Default configuration	By default, no authentication is required for receiving OSPF packets on an interface.
illustrate	The value of the key will be written into the OSPF packet. To ensure the normal sending and receiving of OSPF packets between the Layer 3 switch and the adjacent Layer 3 switch, the same key parameters must be set on the opposite end.
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

14.4.2.7 ip ospf cost

Features	Specifies the cost required for the interface to run the OSPF protocol; Restore default values.
command format	ip ospf costcost no ip ospf cost
parameter	<i>cost</i> :The value required by the OSPF protocol, ranging from 1 to 65535.
Default configuration	The default OSPF protocol cost of an interface is 1.
configuration	interface configuration mode SWITCH(Config-Ethernet1/1)#

mode	
------	--

14.4.2.8 ip ospf dead-interval

Features	Specifies the length of time for the route failure of adjacent Layer 3 switches; Restore default values.
command format	ip ospf dead-interval no ip ospf dead-interval
parameter	<i>time</i> :The length of time for the failure of adjacent Layer 3 switches, in seconds, in the range of 1 to 65535.
Default configuration	The default OSPF protocol cost of an interface is 1.
illustrate	When a Layer 3 switch does not receive a HELLO packet from a neighboring Layer 3 switch within the dead-interval interval, the Layer 3 switch is considered unreachable and invalid. This command can modify the value of the route failure time of adjacent Layer 3 switches according to the actual conditions of the link. The set dead-interval value will be written into the Hello packet and sent with the Hello packet. For the OSPF protocol to run normally, the dead-interval parameter between the Layer 3 switches adjacent to the interface must be the same and at least 4 times the hello-interval value.
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

14.4.2.9 ospf enable area

Features	Configure the interface to belong to an OSPF area; Cancel this configuration.
command format	ip ospf enable area <i>area_id</i> no ip ospf enable area
parameter	<i>area_id</i> :The area number of the area to which the interface belongs, ranging from 0 to 4294967295.
Default configuration	Interfaces are not configured to belong to a zone by default.
illustrate	To run OSPF on an interface, you must first specify that the interface belongs to an area. .
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

14.4.2.10 ip ospf hello-interval

Features	Specifies the time interval for sending HELLO packets on the interface; Restore default values.
command format	ip ospf hello-interval <i>time</i> no ip ospf hello-interval
parameter	<i>time</i> :The interval for sending HELLO packets, in seconds, ranging from 1 to 255.
Default configuration	The default interval for sending HELLO packets on an interface is 10 seconds.
illustrate	The HELLO packet is one of the most common types of packets. It is periodically sent to adjacent Layer 3 switches to discover and maintain adjacency, and to elect DR and BDR. The hello-interval value set by the user will be written into the HELLO message and sent with the HELLO message. The smaller the value of hello-interval, the faster the network topology changes will be discovered, and the routing overhead will also increase. To make the OSPF protocol run normally, the hello-interval parameter must be consistent with the Layer 3 switches adjacent to the interface.
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

14.4.2.11 ip ospf passive-interface

Features	Set the interface to only receive and not send OSPF packets; Cancel this configuration.
command format	ip ospf passive-interface no ip ospf passive-interface
Default configuration	The default state of an interface is to send and receive OSPF packets.
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

14.4.2.12 ip ospf priority

Features	Configure the priority of the interface when electing the "Designated Layer 3 Switch" (DR); Restore default values.
command format	ip ospf priority <i>priority</i> no ip ospf priority
parameter	<i>priority</i> :Priority, the legal value range is 0 to 255.
Default	When an interface elects a designated Layer 3 switch, the default priority is 1.

configuration	
illustrate	When two Layer 3 switches connected to the same network segment want to be "Designated Layer 3 Switches", who is the "Designated Layer 3 Switch" is determined according to the value of the priority, usually the one with higher priority is selected as the "Designated Layer 3 Switch". Switch"; if the priority values are equal, choose the router-id with a larger number. When the priority value of a Layer 3 switch is 0, this Layer 3 switch will not be elected as the "Designated Layer 3 Switch" or "Backup Designated Layer 3 Switch".
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

14.4.2.13 ip ospf retransmit-interval

Features	Specifies the retransmission interval when transmitting Link State Announcements (LSA) between the interface and the adjacent Layer 3 switch; Restore default values.
command format	ip ospf retransmit-interval <i>time</i> no ip ospf retransmit-interval
parameter	<i>time</i> :The retransmission interval when transmitting the link state announcement with the adjacent Layer 3 switch, in seconds, in the range of 1 to 65535.
Default configuration	The default retransmission interval is 5 seconds.
illustrate	When a Layer 3 switch transmits a link state announcement to its neighbors, it will keep the link state announcement until it receives an acknowledgment from the other party. If the acknowledgment packet is not received within the time interval, the Layer 3 switch will retransmit the link state announcement. Link state announcement. The value of the retransmission interval must be greater than one round-trip time for two Layer 3 switches to transmit packets.
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

14.4.2.14 ip ospf transmit-delay

Features	Sets the delay value for transmitting Link State Announcements (LSA) on the interface; Restore default values.
command format	ip ospf transmit-delay <i>time</i> no ip ospf transmit-delay
parameter	<i>time</i> :The delay value for transmitting link state announcements on the interface, in

	seconds, in the range of 1 to 65535.
Default configuration	The default delay for transmitting link state announcements on an interface is 1 second.
illustrate	The link state announcement will age over time in the Layer 3 switch, but not during network transmission. Therefore, increase the transmit-delay delay before sending the link state announcement, so that the link can be deactivated before aging. Status announcements are sent.
configuration mode	interface configuration mode SWITCH(Config-Ethernet1/1)#

14.4.2.15 network

Features	Define the area to which each network of the Layer 3 switch belongs; Delete this configuration.
command format	network <i>network mask area area_id</i> [advertise notadvertise] no network <i>network mask area area_id</i>
parameter	<i>network</i> : network IP address; <i>mask</i> :Address wildcard bit, dotted decimal format; <i>area_id</i> :is the area number, ranging from 0 to 4294967295; advertise :Broadcast summary information for routes to this network range. notadvertise :Broadcasting summary information for routes to this network range is prohibited.
Default configuration	The system does not configure the area to which the network belongs by default; if it is configured, it is assumed to be broadcast summary information by default.
illustrate	Once the scope of a network is added to an area, all the internal routes of the network are no longer independently broadcast to other areas, but only the summary information of the entire network-wide route. The introduction of the network scope and the limitation of the scope can reduce the exchange of routing information between areas.
configuration mode	OSPF protocol configuration mode SWITCH(Config-Router-Ospf)#

14.4.2.16 preference

Features	Configure the priority of the OSPF protocol among routing protocols, and the priority of the imported routes outside the autonomous system; Restore default values.
command format	preference [ase] <i>preference</i> no preference [ase]

parameter	ase : Specifies the priority for importing external routes from the AS; <i>preference</i> : Priority value, ranging from 1 to 255.
Default configuration	The default priority of OSPF protocol is 10; The default priority of imported external routing protocols is 150.
illustrate	Since multiple dynamic routing protocols may run simultaneously on the Layer 3 switch, there is a problem of routing information sharing and selection among the routing protocols. Therefore, a default priority is specified for each routing protocol. When different protocols find the same route, the protocol with the higher priority will play a decisive role. The priority change takes effect on newly constructed routes. Determined by the nature of OSPF, the priority of OSPF should not be too low.
configuration mode	OSPF protocol configuration mode SWITCH(Config-Router-Ospf)#

14.4.2.17 redistribute ospfase

Features	Import bgp routes, directly connected routes, static routes and RIP routes as external routing information; Cancel the imported external routing information.
command format	redistribute ospfase{ bgp connected static rip} [type { 1 2 }] [tagtag] [metriccost_value] no redistribute ospfase { bgp connected static rip}
parameter	bgp : Import BGP routes as external routing information; connected :Indicates that a directly connected route is imported as external routing information; static :Indicates that static routes are imported as external routing information; rip :Indicates that the route discovered by the RIP protocol is imported as the external routing information; 1 :The first type of external routing; 2 : The second type of external route; <i>tag</i> :The tag value of the route, ranging from 0 to 4294967295; <i>cost_value</i> :The weight of the route, which ranges from 1 to 16777215.
Default configuration	OSPF does not import external routes by default.
illustrate	Dynamic routing protocols on Layer 3 switches can share routing information with each other. Due to the characteristics of OSPF, routes discovered by other routing protocols are always treated as routing information outside the AS.
configuration mode	OSPF protocol configuration mode SWITCH(Config-Router-Ospf)#

14.4.2.18 router id

Features	Configure a Layer 3 switch that runs the OSPF protocol ID number; Cancel the Layer 3 switch ID number.
command format	router id <i>router_id</i> no router id
parameter	<i>router_id</i> : Layer 3 switch ID, in dotted decimal format.
Default configuration	By default, the ID number of the Layer 3 switch is not configured. When the protocol is running, one of the IP addresses of each interface is selected as the ID number of the Layer 3 switch.
illustrate	When the OSPF protocol is running, the ID number of the Layer 3 switch is used as the unique identifier of the Layer 3 switch in the autonomous system. Usually, the IP address of an interface running the OSPF protocol in the Layer 3 switch is selected as the ID number. The SICOM3028GPT Layer 3 switch uses the router id as the IP address of the first Layer 3 interface of the switch by default. If no IP addresses are configured on all interfaces of the Layer 3 switch, you must use this command to specify the ID number of the Layer 3 switch, otherwise the OSPF protocol cannot run. The change of the ID number of the Layer 3 switch takes effect only after OSPF is restarted.
configuration mode	Global configuration mode SWITCH(Config)#

14.4.2.19 router ospf

Features	If the OSPF protocol is enabled, it will enter the OSPF mode after it is enabled; Disable the OSPF protocol.
command format	router ospf no router ospf
Default configuration	The system does not run the OSPF protocol by default.
illustrate	Use this command to run or terminate the OSPF protocol. The configuration of OSPF takes effect only after the system runs OSPF.
configuration mode	Global configuration mode SWITCH(Config)#

14.4.2.20 stub cost

Features	Define an area as a STUB area; Cancel the definition.
----------	--

command format	stub cost costareaarea_id no stub areaarea_id
parameter	<i>cost</i> : The cost of the default route in the stub area, ranging from 1 to 65535; <i>area_id</i> : The area number of the stub area, ranging from 1 to 4294967295.
Default configuration	By default, the STUB area is not configured in the system.
illustrate	When an area has only one exit point (connected to only one Layer 3 switch), or when it is not necessary to select an exit point for each external destination, it can be configured as a STUB domain. In the STUB area, two types of LSAs, such as type 4 LSA (ASBR summary LSA) and type 5 LSA (AS external LSA), are not allowed to enter/pass through flooding, which can save the resources spent by each Layer 3 switch in the area to process external routing information.
configuration mode	OSPF protocol configuration mode SWITCH(Config-Router-Ospf)#

14.4.2.21 virtuallink neighbored

Features	Create and configure virtual connections; Delete a virtual connection.
command format	virtuallink neighboridrouter_idtransitareaarea_id[hellointervaltime] [deadintervaltime] [retransmittime] [transitdelaytime] no virtuallink neighborid router_idtransitareaarea_id
parameter	<i>router_id</i> : ID of the virtual connection neighbor, in dotted decimal format; <i>area_id</i> : The area number of the conversion area, the value ranges from 0 to 4294967295; the other four optional time interval configuration parameters are the same as the commands in OSPF interface configuration mode; <i>time</i> : Time value, same as the previous command.
Default configuration	By default, no virtual connection is configured in the system.
illustrate	The concept of virtual connection is introduced to realize or enhance the connectivity of the backbone area (area 0). Since the backbone area must be logically connected, if there is no intra-area route between two nodes in the backbone area, a transition area (Transit Area) should be passed between the two nodes. Create a virtual connection. The virtual connection is identified by the ID number of the peer Layer 3 switch. The area that provides a non-backbone area internal route for both ends of the virtual link is called the conversion area, and its area number must also be specified during configuration. The virtual connection is activated after the route passing through the conversion area is calculated, which is equivalent to forming a point-to-point connection between

	the two endpoints. Therefore, on this connection, the parameters of the interface can be configured just like the physical interface. Such as HELLO interval and so on.
configuration mode	OSPF protocol configuration mode SWITCH(Config-Router-Ospf)#

14.4.2.22 show ip protocols

Features	Displays information about the routing protocols currently running on the Layer 3 switch.
command format	show ip protocols
configuration mode	Privileged User Configuration Mode SWITCH#

14.4.2.23 show ip ospf

Features	Displays the current running status and configuration information of OSPF.
command format	show ip ospf [ase cumulative database [asbr-summary external network router summary] interface [[vlan]name] neighbor routing virtual-links]
parameter	<p>ase: Information about external routes of the autonomous system.</p> <p>cumulative:Statistics;</p> <p>database: Link state database information;</p> <p>asbr-summary: Inter-domain summary link state announcement information;</p> <p>external: aggregated link state announcement information outside the autonomous system;</p> <p>network: Network link status announcement information;</p> <p>router: router link state announcement information;</p> <p>summary: Network summary link state announcement information;</p> <p>interface: Protocol related interface information;</p> <p><i>name</i>: interface name;</p> <p>neighbor: neighbor information;</p> <p>routing: routing table information;</p> <p>virtual-links: Virtual link information.</p>
configuration mode	Privileged User Configuration Mode SWITCH#

14.4.2.24 debug ip ospf

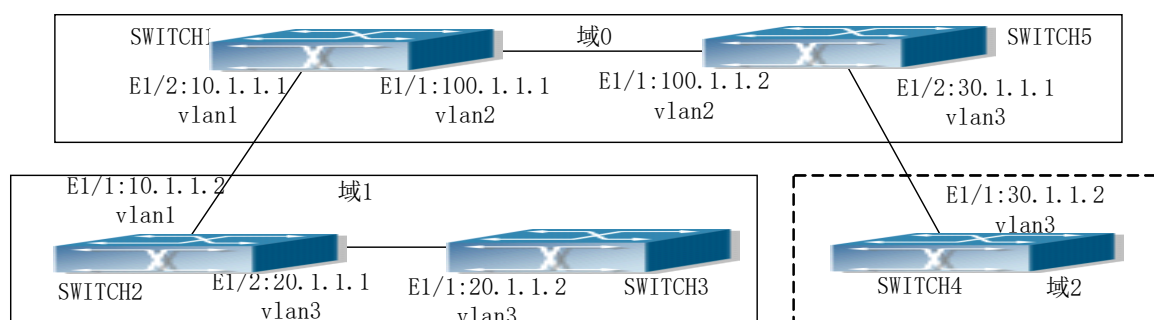
Features	Turn on the OSPF related debugging switch; Disable OSPF-related debugging switches.
----------	--

command format	debug ip ospf [event lsa packet spf] nodebug ip ospf [event lsa packet spf]
parameter	event :event information; lsa :Link state announcement information; packet :datagram information; spf :spf information.
Default configuration	The debug switch is not turned on.
configuration mode	Privileged User Configuration Mode SWITCH#

14.4.3 Typical configuration example

Case 1: OSPF Autonomous System

Take five SICOM3028GPT Layer 3 switches as an example to form an OSPF autonomous system. Layer 3 switches SWITCH1 and SWITCH5 form an OSPF domain 0, and Layer 3 switches SWITCH2 and SWITCH3 form an OSPF domain 1 (the vlan 1 interface of the Layer 3 switch SWITCH1 belongs to domain 0).), the Layer 3 switch SWITCH4 forms an OSPF 2 domain (it is assumed that the vlan 2 interface of the Layer 3 switch SWITCH5 belongs to domain 0). SWITCH1 and SWITCH5 are backbone Layer 3 switches, SWITCH2 and SWITCH4 are domain boundary Layer 3 switches, and SWITCH3 is an intra-domain Layer 3 switch.



Picture 27 OSPF autonomous system network topology diagram

The configurations of Layer 3 switches SWITCH1- SWITCH5 are as follows:

Layer 3 switch SWITCH1:

!Configure the IP address of interface vlan1.

```
SWITCH1#config
```

```
SWITCH1(config)# interface vlan 1
```

```
SWITCH1(config-if-vlan1)# ip address 10.1.1.1 255.255.255.0
```

```
SWITCH1(config-if-vlan1)#no shut-down
```

```
SWITCH1(config-if-vlan1)#exit
```

! Configure the IP address of the interface vlan2

```
SWITCH1(config)# interface vlan 2
```

```
SWITCH1(config-if-vlan2)# ip address 100.1.1.1 255.255.255.0
```

```
SWITCH1 (config-if-vlan2)#exit
```

! Start the OSPF protocol and configure the domain numbers to which the interfaces vlan1 and vlan2 belong.

```
SWITCH1(config)#router ospf
```

```
SWITCH1(config-router-ospf)#exit
```

```
SWITCH1(config)#interface vlan 1
```

```
SWITCH1 (config-if-vlan1)#ip ospf enable area 0
```

```
SWITCH1 (config-if-vlan1)#exit
```

```
SWITCH1(config)#interface vlan2
```

```
SWITCH1 (config-if-vlan2)#ip ospf enable area 0
```

```
SWITCH1 (config-if-vlan2)#exit
```

```
SWITCH1(config)#exit
```

```
SWITCH1#
```

Layer 3 switch SWITCH2:

! Configure the IP addresses of interfaces vlan1 and vlan2.

```
SWITCH2#config
```

```
SWITCH2(config)# interface vlan 1
```

```
SWITCH2(config-if-vlan1)# ip address 10.1.1.2 255.255.255.0
```

```
SWITCH2(config-if-vlan1)#no shut-down
```

```
SWITCH2(config-if-vlan1)#exit
SWITCH2(config)# interface vlan 3
SWITCH2(config-if-vlan3)# ip address 20.1.1.1 255.255.255.0
SWITCH2(config-if-vlan3)#no shut-down
SWITCH2(config-if-vlan3)#exit
! Enable OSPF and configure the OSPF area to which interfaces vlan1 and vlan3 belong
SWITCH2(config)#router ospf
SWITCH2(config-router-ospf)#exit
SWITCH2(config)#interface vlan 1
SWITCH2(config-if-vlan1)#ip ospf enable area 0
SWITCH2(config-if-vlan1)#exit
SWITCH2(config)#interface vlan 3
SWITCH2(config-if-vlan3)#ip ospf enable area 1
SWITCH2(config-if-vlan3)#exit
SWITCH2(config)#exit
SWITCH2#
Layer 3 switch SWITCH3:
! Configure the IP address of interface vlan3.
SWITCH3#config
SWITCH3(config)# interface vlan 3
SWITCH3(config-if-vlan1)# ip address 20.1.1.2 255.255.255.0
SWITCH3(config-if-vlan3)#no shut-down
SWITCH3(config-if-vlan3)#exit
! Enable OSPF and configure the OSPF area to which interface vlan3 belongs
SWITCH3(config)#router ospf
SWITCH3(config-router-ospf)#exit
SWITCH3(config)#interface vlan 3
SWITCH3(config-if-vlan3)#ip ospf enable area 1
```

```
SWITCH3(config-if-vlan3)#exit
SWITCH3(config)#exit
SWITCH3#
Layer 3 switch SWITCH4:
! Configure the IP address of interface vlan3.
SWITCH4#config
SWITCH4(config)# interface vlan 3
SWITCH4(config-if-vlan3)# ip address 30.1.1.2 255.255.255.0
SWITCH4(config-if-vlan3)#no shut-down
SWITCH4(config-if-vlan3)#exit
! Enable OSPF and configure the OSPF area to which interface vlan3 belongs
SWITCH4(config)#router ospf
SWITCH4(config-router-ospf)#exit
SWITCH4(config)#interface vlan 3
SWITCH4(config-if-vlan3)#ip ospf enable area 0
SWITCH4(config-if-vlan3)#exit
SWITCH4(config)#exit
SWITCH4#
Layer 3 switch SWITCH5:
! Configure the IP address of interface vlan2.
SWITCH5#config
SWITCH5(config)# interface vlan 2
SWITCH5(config-if-vlan2)# ip address 30.1.1.1 255.255.255.0
SWITCH5(config-if-vlan2)#no shut-down
SWITCH5(config-if-vlan2)#exit
! Configure the IP address of the interface vlan3
SWITCH5(config)# interface vlan 3
SWITCH5(config-if-vlan3)# ip address 100.1.1.2 255.255.255.0
```

```
SWITCH5(config-if-vlan3)#no shut-down
```

```
SWITCH5(config-if-vlan3)#exit
```

! Start the OSPF protocol and configure the domain numbers to which the interfaces vlan2 and vlan3 belong.

```
SWITCH5(config)#router ospf
```

```
SWITCH5(config-router-ospf)#exit
```

```
SWITCH5(config)#interface vlan 2
```

```
SWITCH5(config-if-vlan2)#ip ospf enable area 0
```

```
SWITCH5(config-if-vlan2)#exit
```

```
SWITCH5(config)#interface vlan 3
```

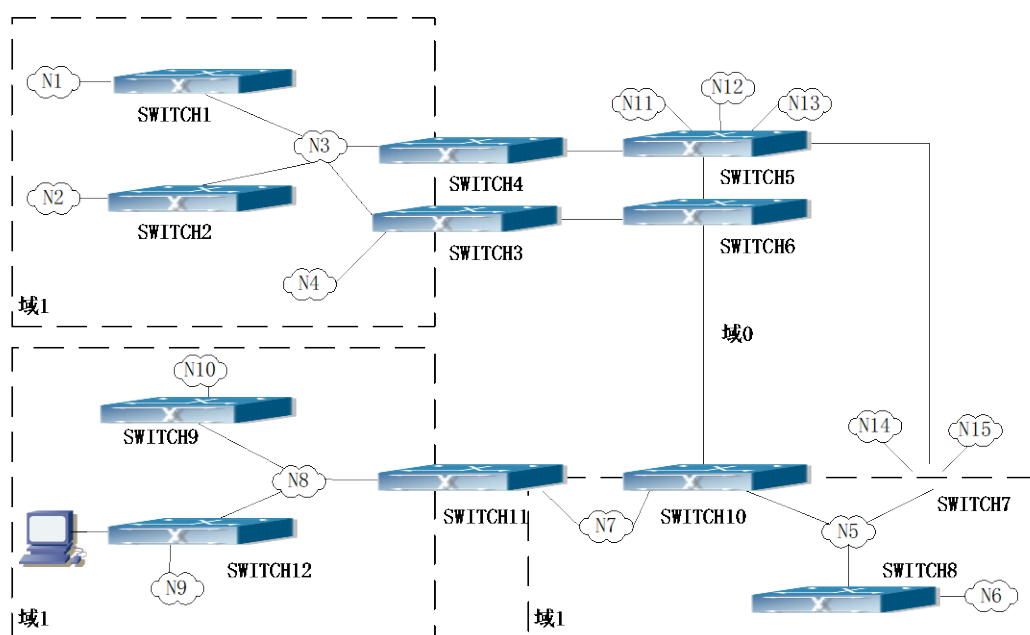
```
SWITCH5(config-if-vlan3)#ip ospf enable area 0
```

```
SWITCH5(config-if-vlan3)#exit
```

```
SWITCH5(config)#exit
```

```
SWITCH5#
```

Case 2: Typical complex topology of OSPF protocol



Picture 28 Complex Typical OSPF Autonomous System

On Picture 31 it is a typical complex OSPF autonomous system network topology. Domain 1 includes networks N1-N4 and Layer 3 switches SWITCH1-SWITCH4, Domain 2 includes networks N5-N7 and Layer 3 switches SWITCH7, SWITCH8, SWITCH10 and SWITCH11, Domain 3 includes N8-N10, host H1 and Layer 3 switches SWITCH9, SWITCH11 and SWITCH12, and the network N8-N10 and the host H1 are configured to use a summary route (that is, define domain 3 as the STUB domain). Layer 3 switches SWITCH1, SWITCH2, SWITCH5, SWITCH6, SWITCH8, SWITCH9, and SWITCH12 are Layer 3 switches in the domain. Layer 3 switches SWITCH3, SWITCH4, SWITCH7, SWITCH10, and SWITCH11 are Layer 3 switches at the domain boundary. Layer 3 switches SWITCH5 and SWITCH7 are autonomous systems. Border Layer 3 switch.

As far as domain 1 is concerned, the Layer 3 switches SWITCH1 and SWITCH2 are Layer 3 switches in the domain, and the Layer 3 switches SWITCH3 and SWITCH4 at the boundary of the domain are responsible for advertising all the distance costs to the destination outside the domain to domain 1. At the same time, SWITCH3 and SWITCH4 must also report to domain 1. The positions of the Layer 3 switches SWITCH5 and SWITCH7 at the border of the autonomous system are advertised, and the external link state advertisements of the autonomous system from SWITCH5 and SWITCH7 are flooded in the entire autonomous system. These LSAs are included in the Domain 1 database, resulting in routes to networks N11-N15, when the autonomous system external link state advertisements are flooded in Domain 1.

In addition, the Layer 3 switches SWITCH3 and SWITCH4 must also summarize the topology of domain 1 to the backbone domain (ie, domain 0, all non-zero domains must be connected through domain 0, and they are not allowed to be directly connected), and advertise the network included in domain 1 (ie. N1-N4) and the cost from SWITCH3 and SWITCH4 to these networks. Since the backbone domain must be connected, a virtual link must be established between the backbone Layer 3 switches SWITCH10 and SWITCH11. The Layer 3 switches at the boundary of the domain exchange summary information through

the Layer 3 backbone switches, and each Layer 3 switch at the boundary of the domain monitors the summary information from the Layer 3 switches at the boundary of other domains.

The virtual link is not only used to ensure the connectivity of the backbone area, but also used to strengthen the backbone area. For example, if the link between the backbone Layer 3 switches SWITCH6 and SWITCH10 is cut off, the backbone domain will be discontinuous. By establishing a virtual link between the backbone Layer 3 switches SWITCH7 and SWITCH10, the backbone domain will become more robust. At the same time, the virtual link between SWITCH7 and SWITCH10 provides a shorter path to Domain 3 and Layer 3 switch SWITCH7.

Taking domain 1 as an example, assume that the IP address of the interface vlan2 of the Layer 3 switch SWITCH1 is 10.1.1.1; the IP address of the interface VLAN 2 of the Layer 3 switch SWITCH2 is 10.1.1.2; the IP address of the interface VLAN 2 of the Layer 3 switch SWITCH3 is 10.1. 1.3; The IP address of the interface VLAN2 of the Layer 3 switch SWITCH4 is 10.1.1.4. SWITCH1 uses the Ethernet port VLAN1 to connect to the network N1, and the IP address is 20.1.1.1; SWITCH2 uses the Ethernet port VLAN1 to connect to the network N2, and the IP address is 20.1.2.1; SWITCH3 uses the Ethernet port VLAN3 to connect to the network N4, and the IP address is 20.1.3.1 ; both belong to domain 1. SWITCH3 uses the Ethernet port VLAN1 to connect to the Layer 3 switch SWITCH6 with the IP address 10.1.5.1; SWITCH4 uses the Ethernet port VLAN1 to connect to the Layer 3 switch SWITCH5 with the IP address 10.1.6.1; both belong to domain 0. Simple key authentication is used between the Layer 3 switches in Domain 1, and MD5 key authentication is used between the Layer 3 switches at the border of Domain 1 and the backbone Layer 3 switches in Domain 0.

Only the configurations of Layer 3 switches in Domain 1 are given below, and the configurations of Layer 3 switches in other domains are omitted. The configurations of SWITCH1, SWITCH2, SWITCH3 and SWITCH4 are as follows:

1) SWITCH1:

!Configure the IP address of interface vlan2

```
SWITCH1#config
```

```
SWITCH1(config)# interface vlan 2
```

```
SWITCH1(config-If-Vlan2)# ip address 10.1.1.1 255.255.255.0
```

```
SWITCH1(config-If-Vlan2)#exit
```

! Enable OSPF and configure the domain number to which interface vlan2 belongs

```
SWITCH1(config)#router ospf
```

```
SWITCH1(config-router-ospf)#exit
```

```
SWITCH1(config)#interface vlan 2
```

```
SWITCH1(config-If-Vlan2)#ip ospf enable area 1
```

!Configure Simple Key Authentication

```
SWITCH1(config-If-Vlan2)#ip ospf authentication simple DCS
```

```
SWITCH1(config-If-Vlan2)exit
```

!Configure the IP address of the interface vlan1, and configure the domain number to which it belongs

```
SWITCH1(config)# interface vlan 1
```

```
SWITCH1(config-If-Vlan1)#ip address 20.1.1.1 255.255.255.0
```

```
SWITCH1(config-If-Vlan1)#ip ospf enable area 1
```

```
SWITCH1(config-If-Vlan1)#exit
```

2) SWITCH2:

!Configure the IP address of interface vlan2

```
SWITCH2#config
```

```
SWITCH2(config)# interface vlan 2
```

```
SWITCH2(config-If-Vlan2)# ip address 10.1.1.2 255.255.255.0
```

```
SWITCH2(config-If-Vlan2)#exit
```

! Enable OSPF and configure the domain number to which interface vlan2 belongs

```
SWITCH2(config)#router ospf
```

```
SWITCH2(config-router-ospf)#exit
```

```
SWITCH2(config)#interface vlan 2
```

```
SWITCH2(config-If-Vlan2)#ip ospf enable area 1
```

```
!Configure Simple Key Authentication
```

```
SWITCH2(config-If-Vlan2)#ip ospf authentication simple DCS
```

```
SWITCH2(config-If-Vlan2)#exit
```

!Configure the IP address of the interface vlan1, and configure the domain number to which it belongs

```
SWITCH2(config)# interface vlan 1
```

```
SWITCH2(config-If-Vlan1)#ip address 20.1.2.1 255.255.255.0
```

```
SWITCH2(config-If-Vlan1)#ip ospf enable area 1
```

```
SWITCH2(config-If-Vlan1)#exit
```

```
SWITCH2(config)#exit
```

```
SWITCH2#
```

3) SWITCH3:

```
!Configure the IP address of interface vlan2
```

```
SWITCH3#config
```

```
SWITCH3(config)# interface vlan 2
```

```
SWITCH3(config-If-Vlan2)# ip address 10.1.1.3 255.255.255.0
```

```
SWITCH3(config-If-Vlan2)#exit
```

```
! Enable OSPF and configure the domain number to which interface vlan2 belongs
```

```
SWITCH3(config)#router ospf
```

```
SWITCH3(config-router-ospf)#exit
```

```
SWITCH3(config)#interface vlan 2
```

```
SWITCH3(config-If-Vlan2)#ip ospf enable area 1
```

```
!Configure Simple Key Authentication
```

```
SWITCH3(config-If-Vlan2)#ip ospf authentication simple DCS
```

```
SWITCH3(config-If-Vlan2)#exit
```

```
!Configure the IP address of the interface vlan3, and configure the domain number to
```

which it belongs

```
SWITCH3(config)# interface vlan 3
SWITCH3(config-If-Vlan3)#ip address 20.1.3.1 255.255.255.0
SWITCH3(config-If-Vlan3)#ip ospf enable area 1
SWITCH3(config-If-Vlan3)#exit
```

!Configure the IP address of interface vlan1, and configure the domain number to which the interface belongs

```
SWITCH3(config)# interface vlan 1
SWITCH3(config-If-Vlan1)#ip address 10.1.5.1 255.255.255.0
SWITCH3(config-If-Vlan1)#ip ospf enable area 0
!Configure MD5 key authentication
SWITCH3 (config-If-Vlan1)#ip ospf authentication md5 DCS
SWITCH3 (config-If-Vlan1)#exit
SWITCH3(config)#exit
```

SWITCH3#

4) SWITCH4:

!Configure the IP address of interface vlan2

```
SWITCH4#config
SWITCH4(config)# interface vlan 2
SWITCH4(config-If-Vlan2)# ip address 10.1.1.4 255.255.255.0
SWITCH4(config-If-Vlan2)#exit
```

! Enable OSPF and configure the domain number to which interface vlan2 belongs

```
SWITCH4(config)#router ospf
SWITCH4(config-router-ospf)#exit
SWITCH4(config)#interface vlan 2
SWITCH4(config-If-Vlan2)#ip ospf enable area 1
!Configure Simple Key Authentication
SWITCH4(config-If-Vlan2)#ip ospf authentication simple DCS
```

```
SWITCH4(config-If-Vlan2)#exit
```

!Configure the IP address of interface vlan1, and configure the domain number to which the interface belongs

```
SWITCH4(config)# interface vlan 1
```

```
SWITCH4(config-If-Vlan1)# ip address 10.1.6.1 255.255.255.0
```

```
SWITCH4(config-If-Vlan1)#ip ospf enable area 0
```

!Configure MD5 key authentication

```
SWITCH4(config-If-Vlan1)#ip ospf authentication md5 DCS
```

```
SWITCH4(config-If-Vlan1)exit
```

```
SWITCH4(config)#exit
```

```
SWITCH4#
```

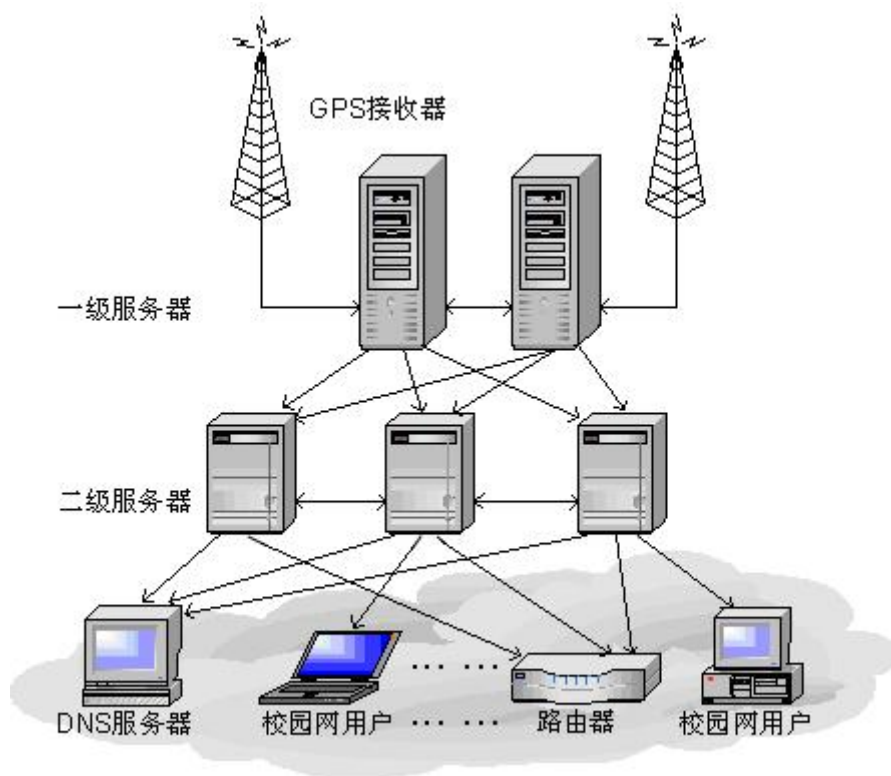
15 NTP configuration

15.1 introduce

The NTP (Network Time Protocol) protocol is widely used to maintain the clock synchronization of computers in the global Internet. In addition to estimating the round-trip delay of packets on the network, the NTP protocol can also independently estimate the computer clock deviation, thereby realizing high-precision computer time calibration on the network. In most places, NTP provides an accuracy of 1~50ms, depending on the characteristics of the synchronization source and the network path.

SNTP (Simple Network Time Protocol) is a simplified version of the NTP protocol, which removes the complex algorithm of NTP. SNTP is used for hosts that do not need the complexity of a full NTP implementation, and is a subset of NTP. Usually, several hosts on the local area network are synchronized with other NTP hosts through the Internet, and then the time synchronization service is provided to other clients in the local area network.

The following Picture depicts an NTP/SNTP application network structure, in which SNTP mainly works between secondary servers and various terminals, mainly because the time accuracy requirements of these scenarios are not high, and the time accuracy that SNTP itself can provide (1- 50ms) can generally meet the application of these services.



Picture 29 NTP/SNTP working scenarios

15.2 CLI configuration

Table 24 Configuration command

Order	configuration mode	Features
sntp enable no sntp enable	Global configuration mode SWITCH(Config)#	Turn on the SNTP function; Disable the SNTP function.
sntp server no sntp server	Global configuration mode SWITCH(Config)#	set up SNTP/NTP Serve; Cancel SNTP/NTP Serve.
sntp polltime no sntp polltime	Global configuration mode SWITCH(Config)#	Set the request interval; Cancel the set interval.
sntp timezone no sntp timezone	Global configuration mode SWITCH(Config)#	Set the client's time zone and time difference from UTC; Cancel the time difference setting.
show sntp	Privileged User Configuration Mode SWITCH#	Displays the current configuration of the SNTP client and server status.

debug sntp no debug sntp	Privileged User Configuration Mode SWITCH#	Turn on the SNTP debugging switch; Disable the SNTP debugging switch.
-----------------------------	---	--

15.2.1 sntp enable

Features	Turn on the SNTP function; Disable the SNTP function.
command format	sntp enable no sntp enable
Default configuration	The SNTP function is disabled by default.
configuration mode	Global configuration mode SWITCH(Config)#

15.2.2 sntp server

Features	set upSNTP/NTP The server address starts with; Unset SNTP/NTP server address.
command format	sntp serverserver_address [version version_no] no sntp serverserver_address
parameter	<i>server_address</i> : SNTP/NTP server's IP unicast address; <i>version_no</i> : current client's SNTP version number, the value is <1-4>. The version defaults to 1.
Default configuration	There is no such configuration by default when leaving the factory.
configuration mode	Global configuration mode SWITCH(Config)#

15.2.3 sntp polltime

Features	set up SNTP client to The interval at which the NTP/SNTP server sends requests; unset polltime, restore default value 64s.
command format	sntp polltimeinterval no sntp polltime
parameter	<i>interval</i> : interval to set, ranging from 16~16284.
Default configuration	Default is 64s.
configuration mode	Global configuration mode SWITCH(Config)#

15.2.4 sntp timezone

Features	set up The time zone where the SNTP client is located is the same as time difference from UTC; Cancel the set time zone and restore the default value.
command format	sntp timezone name {add subtract} time_difference no sntp timezone
parameter	name : The name of the set time zone, not exceeding 16 characters; add : Indicates that the set time zone is UTC time plus time_difference; subtract : Indicates that the set time zone is UTCtime minus time_difference; time_difference : Time difference to set, ranging from 1~12.
Default configuration	The default time difference is set to add 8.
configuration mode	Global configuration mode SWITCH(Config)#

15.2.5 show sntp

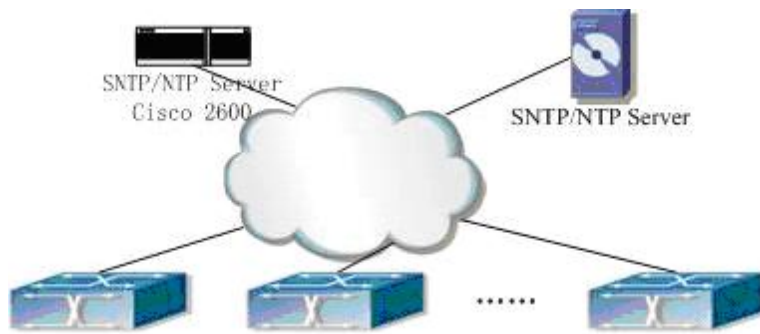
Features	show The current configuration of the SNTP client and server status.
command format	show sntp
configuration mode	Privileged User Configuration Mode SWITCH#

15.2.6 debug sntp

Features	Turn on the SNTP debugging switch; closure SNTP debug switch.
command format	debug sntp {adjust packet select} no debug sntp {adjust packet select}
parameter	adjust : SNTP clock adjustment information; packet : SNTP message; select : SNTP clock selection.
configuration mode	Privileged User Configuration Mode SWITCH#

15.3 Typical configuration example

Typical application cases of SNTP are as follows:



Picture 30 Typical SNTP configuration

All switches in the AS domain need to perform time synchronization. Time synchronization is achieved through two redundant SNTP/NTP servers. To achieve time synchronization, the current network must be properly configured to ensure that there is a reachable route between any switch and two SNTP/NTP servers. Assuming that the IP addresses of the two SNTP/NTP servers are configured as 10.1.1.1 and 20.1.1.1 respectively, and the SNTP/NTP server function has been enabled, the configuration of any switch is as follows:

```
Switch#config
```

```
Switch(config)#sntp server 10.1.1.1
```

```
Switch(config)#sntp server 20.1.1.1
```

After that, SNTP will synchronize time with the server according to the default settings (polltime 64s, version 1).

16 DT-Ring protocol family configuration

Industrial Ethernet switches are gradually being used in power distribution networks, digital substations, wind power generation, rail transit, high-speed railways, industrial control and other fields.

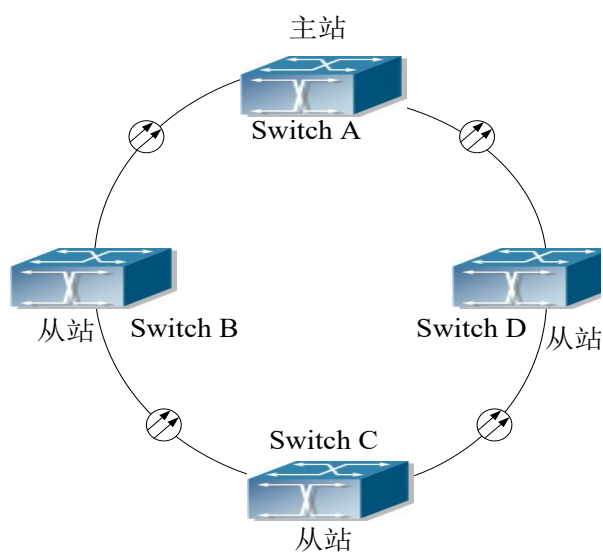
Industrial field communication requires stable and reliable communication and fast fault recovery. In some fields, it also requires business shunting and isolation to ensure load balancing; STP/RSTP/MSTP protocols in the communication field cannot well guarantee the above requirements. The DT-Ring protocol family is a proprietary communication protocol of Kyland Company, and it is a proprietary protocol tailored for the field of industrial communication. It includes DT-Ring, DT-Ring+ and DT-VLAN protocols.

16.1 DT-Ring

16.1.1 introduce

DT-Ring protocol is our proprietary communication protocol. This protocol determines the status of the ring and port by quickly detecting the LINK status of the ring port and passing fewer protocol packets, so as to ensure that the redundant network does not form a ring; Maintenance is convenient, so that it can better meet the needs of the industrial communication field.

The following Picture shows its network topology. One of the switch ports is configured as the master station, and the rest are configured as slave stations.



Picture 31 DT-Ring networking mode

Configuration instructions:

- On the same switch, multiple domains can be configured; this can meet the networking mode of tangent ring;
- In the same ring, each switch needs to be configured with the same domain ID. For the convenience of maintenance, it is better to configure the same domain name as well;
- In the same ring, there can only be one master station, and the rest should be configured as slave stations;

The number of devices forming a ring network must be considered from the following aspects:

1. Network traffic; when the number of ring networks is large, the business traffic of the ring ports will increase, and it is necessary to calculate that the network traffic of the ring network is less than the business traffic of the ring ports;
2. Switching delay; DT-Ring can realize protection switching of the network, but the

switching has a short delay. The calculation formula is as follows:

$$\text{Maximum switching delay} = (\text{number of devices} \times 2.5 + 10) \text{ milliseconds};$$

The maximum switching delay is related to the number of devices. The greater the number, the greater the switching delay.

3. Protection effectiveness; DT-Ring can achieve 1:n protection, that is, use one device to protect the rest of the devices forming the ring network. If there are more devices in the ring, its protection capability is weaker;

4. Convenience of maintenance; too many devices that make up the ring network equipment will bring inconvenience in maintenance;

16.1.2 CLI configuration

Table 25 configuration command

Order	configuration mode	Features
dt-ring	Global configuration mode SWITCH(Config)#	Enter the DT-Ring configuration mode.
dt-ring new domain	Global configuration mode SWITCH(Config)#	Create a DT-Ring domain.
dt-ring del domain	Global configuration mode SWITCH(Config)#	Delete the DT-Ring field.
ringport add	DT-Ring configuration mode SWITCH(Config-DT-Ring-1)#	Add ring ports.
ringport delete	DT-Ring configuration mode SWITCH(Config-DT-Ring-1)#	Delete ring ports.
protocol enable	DT-Ring configuration mode SWITCH(Config-DT-Ring-1)#	Enable the DT-Ring domain protocol.
protocol disable	DT-Ring configuration mode SWITCH(Config-DT-Ring-1)#	DT-Ring domain protocol is prohibited.
show dt-ring	Privileged User Configuration Mode SWITCH#	Displays DT-Ring status.
debug dt-ring no debug dt-ring	Privileged User Configuration Mode SWITCH#	Turn on the DT-Ring debugging switch; Turn off the DT-Ring debugging switch.

16.1.2.1 dt-ring

Features	Enter the DT-Ring configuration mode.
command format	dt-ring <i>1-31</i>
parameter	<i>1-32</i> : domain ID;
configuration mode	Global configuration mode SWITCH(Config)#

16.1.2.2 dt-ring new domain

Features	Create a DT-Ring domain.
command format	dt-ring new <i>1-31</i> domain <i>1-32</i> { master slave }
parameter	<i>1-31</i> : domain name; <i>1-32</i> : domain ID; master : Configure the DT-Ring domain as the master station; slave : Configure the DT-Ring domain as a slave.
Default configuration	There is no such configuration by default when leaving the factory.
configuration mode	Global configuration mode SWITCH(Config)#

16.1.2.3 dt-ring del domain

Features	Delete the DT-Ring field.
command format	dt-ring del domain <i>1-32</i>
parameter	<i>1-32</i> : domain ID;
Default configuration	There is no such configuration by default when leaving the factory.
configuration mode	Global configuration mode SWITCH(Config)#

16.1.2.4 ringport add

Features	Create ring ports.
command format	ringport add <i>interface_id</i>
parameter	<i>interface_id</i> : Switch port ID.

Default configuration	There is no such configuration by default when leaving the factory.
illustrate	In a DT-Ring ring, you need to configure ring ports according to actual needs to form a redundant protection ring network. There are only two ring ports; if only one ring port is configured, the entire ring will not work properly.
configuration mode	DT-Ring configuration mode SWITCH(Config-DT-Ring-1)#

16.1.2.5 ringport delete

Features	Delete ring ports.
command format	ringport delete <i>interface_id</i>
parameter	<i>interface_id</i> : Switch port ID.
Default configuration	There is no such configuration by default when leaving the factory.
configuration mode	DT-Ring configuration mode SWITCH(Config-DT-Ring-1)#

16.1.2.6 protocol enable

Features	Enable the DT-Ring domain protocol.
command format	protocol enable
Default configuration	This function is not enabled by default.
configuration mode	DT-Ring configuration mode SWITCH(Config-DT-Ring-1)#

16.1.2.7 protocol disable

Features	Do not enable the DT-Ring domain protocol.
command format	protocol disable
configuration mode	DT-Ring configuration mode SWITCH(Config-DT-Ring-1)#

16.1.2.8 show dt-ring

Features	Displays the DT-Ring domain status.
----------	-------------------------------------

command format	show dt-ring [1-32 config]
parameter	1-32: indicates the domain ID; config : Configuration information.
illustrate	Commands to display DT-Ring status, including basic configuration information and protocol status information.
configuration mode	Privileged User Configuration Mode SWITCH#

16.1.2.9 debug dt-ring

Features	Turn on the DT-Ring debugging switch; Turn off the DT-Ring debugging switch.
command format	debug dt-ring {all config error port event fsm intf rx test tx} no debug dt-ring { all config error port event fsm intf rx test tx }
parameter	all : all information; config : configuration information; error : error message; prot : port information; event : event information; fsm : state machine information; intf : interface information; rx : received message information; test : test information; tx : sent message information.
configuration mode	Privileged User Configuration Mode SWITCH#

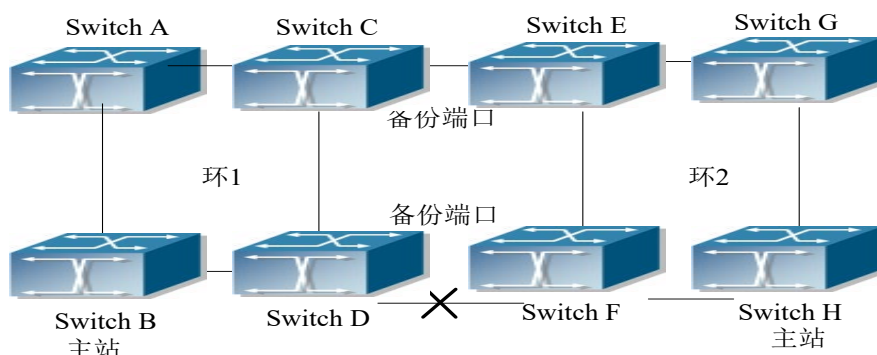
16.2 DT-Ring+

16.2.1 introduce

The DT-Ring+ protocol is a proprietary communication protocol of Kyland Company. This protocol realizes the backup between two rings on the basis of DT-Ring, and determines the state of the ring and the port according to the ID of the backup device, so as to ensure that the redundant network does not form a ring. It can realize fast and stable Ethernet redundant

ring, so as to better meet the needs of the industrial communication field.

The following Picture shows its networking method;



Picture 32 DT-Ring+ networking mode

Configuration instructions:

- On the same switch, there can only be one backup port for the configured DT-Ring;
- In the same ring, the number of backup ports on all devices cannot exceed 2.
- In the same ring, a backup port can be configured on the master station.

16.2.2 CLI configuration

Table 26 Configuration command

Order	configuration mode	illustrate
DT-plus enable	DT-Ring configuration mode SWITCH(Config-DT-Ring-1)#	Create DT-Ring+.
DT-plus disable	DT-Ring configuration mode SWITCH(Config-DT-Ring-1)#	Remove DT-Ring+.
backport add	DT-Ring configuration mode SWITCH(Config-DT-Ring-1)#	Add backup port.
backport delete	DT-Ring configuration mode SWITCH(Config-DT-Ring-1)#	Delete the backup port.
show dt	Privileged User Configuration Mode SWITCH#	Displays DT-Ring+ status.

show dt-plus	Privileged User Configuration Mode SWITCH#	Displays DT-Ring+ status.
debug DT-plus no debug DT-plus	Privileged User Configuration Mode SWITCH#	Turn on the DT-Ring+ debug switch; Turn off the DT-Ring+ debug switch.

16.2.2.1 DT-plus enable

Features	Turn on the DT-Ring+ function.
command format	DT-plus enable
Default configuration	This feature is not turned on.
illustrate	To configure DT-Ring+, first create a DT-Ring domain.
configuration mode	DT-Ring configuration mode SWITCH(Config-DT-Ring-1)#

16.2.2.2 DT-plus disable

Features	Deactivate the DT-Ring+ function.
command format	DT-plus disable
configuration mode	DT-Ring configuration mode SWITCH(Config-DT-Ring-1)#

16.2.2.3 backport add

Features	Add backup port.
command format	backport add <i>interface_id</i>
parameter	<i>interface_id</i> : Indicates the port ID.
Default configuration	There is no such configuration by default when leaving the factory.
illustrate	In a DT-Ring ring, you need to configure backup ports according to actual needs to form backups between redundant protection ring networks.
configuration mode	DT-Ring configuration mode SWITCH(Config-DT-Ring-1)#

16.2.2.4 backport delete

Features	Delete the backup port.
command format	backport delete <i>interface_id</i>
parameter	<i>interface_id</i> : Indicates the port ID.
Default configuration	There is no such configuration by default when leaving the factory.
configuration mode	DT-Ring configuration mode SWITCH(Config-DT-Ring-1)#

16.2.2.5 show dt

Features	Displays DT-Ring+ status.
command format	show dt [master]
parameter	master : Indicates the master station.
Default configuration	There is no such configuration by default when leaving the factory.
configuration mode	Privileged User Configuration Mode SWITCH#

16.2.2.6 show dt-plus

Features	Displays DT-Ring+ status.
command format	show dt-plus [master]
parameter	master : Indicates the master station.
Default configuration	There is no such configuration by default when leaving the factory.
configuration mode	Privileged User Configuration Mode SWITCH#

16.2.2.7 debug DT-plus

Features	Turn on the DT-Ring+ debug switch; Turn off the DT-Ring+ debug switch.
command format	debug DT-plus {all config error port event fsm intf rx test tx} no debug DT-plus { all config error port event fsm intf rx test tx }
parameter	all : all information;

	<p>config: configuration information;</p> <p>error: error message;</p> <p>prot: port information;</p> <p>event: event information;</p> <p>fsm: state machine information;</p> <p>intf: interface information;</p> <p>rx: received message information;</p> <p>test: test information;</p> <p>tx: sent message information.</p>
configuration mode	Privileged User Configuration Mode SWITCH#

16.3 DT-VLAN

16.3.1 introduce

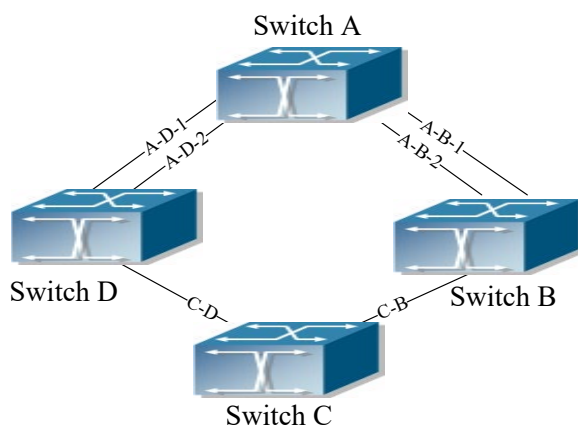
The DT-VLAN protocol is an extension of the DT-Ring protocol; the DT-Ring protocol is based on port-based redundant ring protection, and only one redundant ring can be configured in a redundant link; the DT-VLAN protocol is based on the same chain. Different VLAN groups on the road are used for link redundancy protection, which is on a redundant ring physical link. Multiple redundant rings can be configured according to the VLAN group to control the forwarding status of the VLAN groups on the ring ports respectively, and can complete the fast switch.

If the redundant backup of the same link is configured into multiple rings, since the master station can be set on different switches, data can be distributed and key services can be guaranteed; Do load balancing.

The typical network topology of DT-VLAN is shown in the Picture below; taking the network on the left as an example, configure SWICH A (link AD-1), SWITCH D (link AD-1), SWITCH B (LINK A (link AB-1) as a redundant ring, SWICH A (link AD-2), SWITCH D (link AD-2), SWITCH B (LINK A (LINK AB-2) as a redundant ring, the two rings belong to different VLAN groups.

Configuration instructions:

- On the same switch, multiple domains can be configured; this can meet the networking mode of tangent ring;
- In the same ring, each switch needs to be configured with the same domain ID. For the convenience of maintenance, it is better to configure the same domain name as well;
- In the same ring, there can only be one master station, and the rest should be configured as slave stations;
- A VLAN can only belong to one DT-Ring domain;
- When a switch is configured with DT-VLAN, port-based DT-Ring cannot be configured;
- Please refer to the introduction to the DT-Ring protocol for the number of devices that make up the ring network.



Picture 33 Typical Topology of DT-VLAN

16.3.2 CLI configuration

Table 27 Configuration command

Order	configuration mode	Features
dt-ring mode	Global configuration mode SWITCH(Config)#	Set the redundant environment mode.
vlan add	Global configuration mode SWITCH(Config)#	Add VLANs.
vlan delete	Global configuration mode SWITCH(Config)#	Delete VLAN.

16.3.2.1 dt-ring mode

Features	Set the redundant environment mode.
command format	dt-ring mode {vlan-based port-based}
parameter	vlan-based : based on VLAN; port-based : port based;
Default configuration	There is no such configuration by default when leaving the factory.
illustrate	To create a VLAN-based ring, you must first set the redundant environment mode to VLAN mode; RSTP and DT-Ring are both port-based, so to enable a VLAN-based redundant ring, neither RSTP nor DT-Ring can be configured.
configuration mode	Global configuration mode SWITCH(Config)#

16.3.2.2 vlan add

Features	Add VLANs.
command format	vlan add <i>vlan_id</i>
Default configuration	<i>vlan_id</i> : Indicates the VLAN ID.
illustrate	Configure the effective VLAN for DT-Ring. A VLAN can only be added to one DT-Ring, and cannot be added repeatedly.
configuration mode	DT-Ring configuration mode SWITCH(Config-DT-Ring-1)#

16.3.2.3 vlan delete

Features	Delete VLAN.
command format	vlan delete <i>vlan_id</i>
Default configuration	<i>vlan_id</i> : Indicates the VLAN ID.
illustrate	Configure the effective VLAN for DT-Ring. A VLAN can only be added to one DT-Ring, and cannot be added repeatedly.
configuration mode	DT-Ring configuration mode SWITCH(Config-DT-Ring-1)#