L3 Manage Switch

CLI Configuration Manual

(Applicable to DH-PFS6428-24T)

Contents

1. System Status Commands

1.1 Mode Description

Command Description

How to enter and exit each mode (the privilege mode, global mode, and interface mode)

Parameter

None

Default

None

Command Mode

Privileged mode

Example

username: admin

password: admin（Hidden）

switch#

switch# exit

press ENTER to get started

username:

// This command is used to enter the privileged mode, and the exit command is used to exit the privileged mode.

switch# configure terminal

switch(config)# exit

switch#

// This command is used to enter the global mode, and the exit command is used to exit the global mode and return to the privileged mode.

switch# configure terminal

switch(config)# interface G1

switch(config-G1)# exit

switch(config)#

// This command is used to enter the G1 interface mode from the global mode, and the exit command is used to exit the interface mode.

switch(config)# interface vlan1

switch(config-vlanif1)# exit

switch(config)#

// This command is used to enter the vlan1 interface mode from the global mode, and the exit command is used to exit the vlan1 interface mode.

1.2 System information

Function Brief

This module is used to display the device name, software version, hardware version, MAC address, compile time, run time, and current system time.

1.2.1 show version

Command Description

This command is used to display the version information, including the device name, software version, hardware version, MAC address, compile time, system run time, current version information, and backup version information.

Parameter

None

Default

None

Command Mode

Privileged mode(To enter the privileged mode, connect a serial port, and enter the user name and password. To exit the privileged mode, run the exit command.)

Example

username: admin

password: admin（The password is hidden.）

switch# show version

```
switch# show version
Switch OS V2.0.5-R1
Compiled Wed, 16 Mar 2016 19:08:50 +0800

Product Type :DH-PFS6428-24T
Serial Number:A1111111111111111155
Mac Address  :00-00-66-11-11-33
CPU use: 18.7%
Mem Usage rates:52%, Total:218508KB, Free:105936KB
```

1.2.2 show clock

Command Description

This command is used to display the current system time.

Parameter

None

Default

None

Command Mode

Privileged mode

Example

switch# show clock

```
switch# show clock
Tue Mar  1 09:24:01 WAUST 2016
```

1.3 Log information

Function Brief

This module is used to display system logs when the system is running, so that maintenance staff can conveniently analyze relevant problems.

1.3.1 show logging

Command Description

This command is used to display the current log of the switch.

Parameter

None

Default

None

Command Mode

Privileged mode

Example

switch# show logging

1.4 Port statistics

Function Brief

The port statistics module is used to display the number of sent/received packets, sent/received bytes, and number of sent/received error packets on every port.

1.4.1 show interface

Command Description

This command is used to display the packet statistics of one or more ports.

Parameter

<cr>	It is used to display data statistics of all ports.
G<1-24>	It is used to display data statistics

Default

None

Command Mode

Privileged mode

Example

switch# show interface G1

```
switch# show interface G1
G1 is down
  Hardware address is 22-00-00-55-11-23
  Media type is MEDIUM_COPPER, loopback not set
  Autonegotiation enable, Flow control is on
  Speed: 1000, Duplex-auto, Max frame size: 1518
  Ifindex: 0x2010001
  Port link-type: access, PVID is 1
    Untag vid: 1
   0 packets input, 0 bytes
   0 broadcast, 0 multicast
   0 jabber, 0 pause
   0 input errors, 0 CRC, 0 drops
   0 packets output, 0 bytes
   0 broadcast, 0 multicast
   0 output errors, 0 drops
   0 late collision, 0 pause
```

1.5 LACP status

Function Brief

This function module is used to display the LACP port configurations.

1.5.1 lacp state

Command Description

This command is used to display the status of the LACP system.

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

switch(config)# lacp state

1.6 View route

Function Brief

The function module is used to display switch routing information.

1.6.1 show ip route

Command Description

This command is used to display the router information.

Parameter

bgp	View the BGP routing information
connected	View the connected routing information
ospf	View the ospf routing information
rip	View the rip routing information
static	View the static routing information
A.B.C.D	View contains specific IP routing information
A.B.C.D/M	View of a routing information
summary	View all routing summary information

Default

None

Command Mode

Privileged mode

Example

switch# show ip route connected

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

C>* 192.168.255.0/24 is directly connected, vlanif1
```

1.7 ERPS-RING status

Function Brief

The function module is used to display erps information.

1.7.1 show erps

Command Description

This command is used to display the erps information.

Parameter

None

Default

None

Command Mode

Privileged mode

Example

switch# show erps

1.8 Power status

Function Brief

The function module is used to display power supply information.

1.8.1 show power

Command Description

This command is used to display the power supply information.

Parameter

None

Default

None

Command Mode

Privileged mode

Example

switch# show power

2. System Setting Commands

2.1 IP config

IP address configuration commands include:

ip address

ip address dhcp

ip address old_ip A.B.C.D/M new_ip A.B.C.D/M

show ip interface

notice:A.B.C.D/M,Example:192.168.1.1/24

Function Brief

The IP configuration module is used to add, delete or display the interface IP information of a switch.

2.1.1 ip address

Command Description

Configure IP port for A.B.C.D/M

no ip address A.B.C.D/M

//Delete ports IP A.B.C.D/M

Parameter

None

Default

VLAN 1 interface

Command Mode

VLAN interface configuration mode

Example

switch(config)# interface vlanif1

switch(config-vlanif1)#ip address 192.168.100.1/24

switch(config-vlanif1)#no ip address 192.168.100.1/24

2.1.2 ip address dhcp

Command Description

Configure IP port for automatic access (network DHCP server will assign a dynamic IP) for the switch port.

no ip address dhcp

//Disables the IP of the interface to access automatically.

Parameter

None

Default

Open port

Command Mode

Interface configuration mode

Example

switch(config)# interface vlanif1

switch(config-vlanif1)#ip address dhcp

switch(config-vlanif1)#no ip address dhcp

2.1.3 ip address old_ip

Command Description

ip address old_ip A.B.C.D/M new_ip A.B.C.D/M

Change the IP configuration of the interface (amend the old_ip to new_ip)

Parameter

None

Default

None

Command Mode

Interface configuration mode

Example

switch(config)# interface vlanif1

switch(config-vlanif1)#ip address old_ip 192.168.255.1/24 new_ip 192.168.10.1/24

2.1.4 show interface

Command Description

This command is used to display the interface IP information.

Parameter

None

Default

Enabled port

Command Mode

Privileged mode and Global configuration mode

Example

switch(config)#show interface vlanif1

switch#show interface vlanif1

```
switch(config)# show interface vlan1
Interface vlanif1 is up, line protocol is up
  index 2 metric 1 mtu 1500
  flags: <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 22:00:00:55:11:22
  inet 192.168.255.2/24 broadcast 192.168.255.255
```

2.2 User config

User configuration commands include:

username name

show user

Note: **name** indicates the user name, which is a string of 1 to 32 characters. **password** indicates the password, which is a string of 1 - 32 characters.**level** indicates the user level, which ranges from 1 (lowest management rights) to 15 (highest management rights).

Function Brief

This function module is used to display, modify or add user information so as to protect the switch configurations.

2.2.1 username name

Command Description

username name password passwd privilege level

//This command is used to add a user, modify the password of an existing user, modify the management rights of an existing user, or modify the password and management rights of an existing user.

no username name

//This command is used to delete a known user.

Parameter

guest	permissions for all users of the guest is limited to check the system status information under the menu bar
admin	permissions for the admin user, you can add, modify, delete all configuration

Default

admin

Command Mode

Global configuration mode

Example

switch(config)#username test password test

//Add a user "test", it is the default password is testing and rights: the guest.

switch(config)#username test password test privilege admin

//Modify user: test, password: test, permissions: admin.

switch(config)#username test password test privilege guest

//Modify user: the test management authority for the guest.

switch(config)#no username test

//Delete user test.

2.2.2 show user

Command Description

This command is used to display all the current user configurations of the switch.

Parameter

None

Default

None

Command Mode

Privileged mode

Example

Switch#show user

2.3 Time setting

The configuration commands include:

sntp enable|disable

sntp unicast-server

sntp auto-sync timer

sntp connect

sntp timezone

local-time date

Function Brief

When enabled, this function can be used to automatically synchronize the switch time with the network time.

2.3.1 sntp enable|disable

Command Description

ntp:

//This command is used to enable the NTP function.

no ntp:

//This command is used to disable the NTP function.

Parameter

None

Default

Disable

Command Mode

Global configuration mode

Example

switch(config)#sntp enable

switch(config)#sntp disable

2.3.2 sntp unicast-server

Command Description

sntp unicast-server A.B.C.D

//This command is used to add the IP address of an NTP server.

no sntp unicast-server A.B.C.D

//This command is used to delete the ip address of an NTP server.

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

Switch(config)#sntp unicast-server 210.21.196.6

2.3.3 sntp auto-sync timer

Command Description

This command is used to set the SNTP synchronization time interval.

Parameter

sntp auto-sync timer time,time Values range 5-65535s, 300s default value.

Default

300s

Command Mode

Global configuration mode

Example

Switch(config)#sntp auto-sync timer 5

2.3.4 sntp connect

Command Description

sntp connect A.B.C.D

//This command is used to select the SNTP server to connect.

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

switch(config)#sntp connect 210.21.196.6

2.3.5 sntp timezone set

Command Description

switch(config)# sntp timezone set<0-39>

//This command is used to select the time zone.

Parameter

<0-39>	Each number represents a time zone, can use SNTP timezone show view the corresponding relationship

Default

0

Command Mode

Global configuration mode

Example

switch(config)#sntp timezone set 32

/ /Modify the time zone east eight area.

2.3.6 local-time date

Command Description

local-time date YYYY-MM-DD time HH:MM:SS

//Set the local time year - month - day hours: minutes: seconds

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

switch(config)# local-time date 2015-3-18 time 12:12:12

// Note: due to the chip is limited, can only be set after January 1,1970.

3. Port configuration commands

3.1 Port config

Port configuration commands include:

duplex
speed
flow-control
shutdown
description

Function Brief

This module is used to configure basic parameters related to ports of a switch. These basic parameters directly influence the port working mode.

3.1.1 duplex

Command Description

duplex {auto | full | half }

no duplex

//These commands are used to set the port rate mode.

Parameter

parameter	Parameters of the command mode
auto	Automatic negotiation.
full	Full duplex
half	Half duplex

Default

By default, the duplex modes of all ports are Auto. For an optical port, the duplex mode is always set to full.

Command Mode

Interface configuration mode

Note:

Light port duplex is fixed, is a full-duplex mode (full).

Example

// This command is used to modify the duplex mode of the G1 port.

switch(config)# interface G1

switch(config-G1)# duplex full

3.1.2 speed

Command Description

speed {10 | 100 | 1000|10000|auto }

no speed

//It is used to set the port rate.

Parameter

parameter	Parameters of the command mode
10,100,1000,10000	The port rate is set to 10M, 100M and 1000M.
auto	The port rate is set to Auto.

Default

By default, the speed mode is set to **auto** for an electric port,

- 10000M for a f-port fiber port

Command Mode

Interface configuration mode

Note:

Port speed of light is coerced into 1000M and 10000M.

Electricity mouth can only set auto, 10M and 100M

Example

// The port rate of G1 is set to 100M.

switch(config)# interface G1

switch(config-G1)# speed 100

3.1.3 flow-control

Command Description

flowctrl

no flowctrl

//This command is used to enable or disable the flow control function of a port.

Parameter

None

Default

The flow control function is enable by default

Command Mode

Interface configuration mode

Example

//enable the function.

switch(config-G1)# flowctrl

3.1.4 shutdown

Command Description

shutdown

no shutdown

//This command is port switch.

Parameter

None

Default

The port is enabled by default.

Command Mode

Interface configuration mode

Example

//This command is used to disable a port.

switch(config)#interface G1

switch(config-G1)# shutdown

3.1.5 description

Command Description

This command is to configure the port description information, convenient for management (composed of letters, Numbers and underscore).

Parameter

None

Default

None

Command Mode

Interface configuration mode

Example

switch(config)#interface G1

switch(config-G1)# description A1_1

3.2 Rate limit

Function Brief

It is used to configure the speed limiting policy of a port to limit the ingress and egress rates of all packets of the port.

3.2.1 rate-limit

Command Description

rate-limit {1-10000000 } egress/ingress

no rate-limit egress/ingress

//Configure port egress / ingress speed limit function, use the no form, port restore default settings .

Parameter

1-10000000	Port speed range is 1-10000000kbps

Default

0

Command Mode

Interface configuration mode

Example

//The speed limit exports 10000 Kbps

switch(config)#interface G1

switch(config-G1)# rate-limit 10000 egress

3.3 Port mirroring

Function Brief

Port mirroring is also called port monitoring. Port monitoring is a data packet acquisition technology. It can be configured on a switch to copy data packets from one or more ports (mirror source ports) to a specified port (mirror destination port). The destination port is connected to a host installed with the packet analysis software. The software analyzes the collected packets to implement network monitoring and eliminating network faults.

3.3.1 monitor

Command Description

monitor session <1-4> ingress destination <IFNAME> source <IFNAME>

no monitor session <1-4>

//Configure port mirroring function, use the no form of the command, delete the image settings.

Parameter

Parameter	Parameters of the command mode

1-4	Port mirror number
IFNAME	port number,Example G1,T1

Default

None

Command Mode

Global configuration mode

Example

//This command is to configure the session 1 source port for G1,G2, destination port for G3.

switch(config)# monitor session 1 both destination G3 source G1 G2

3.4 Link aggregation

Static aggregation configuration commands include:

Trunk

Dynamic aggregation configuration commands include:

lacp enable | disable

lacp active | passive

lacp key

lacp port-priority

Function Brief

Link aggregation is used to form a logical port using multiple physical ports of a switch. Multiple links within the same aggregation group are deemed as a larger bandwidth logical link.

By link aggregation, the communication traffic is shared among member ports of the aggregation group, and thus the bandwidth is increased. Besides, member ports of the same aggregation share dynamic backups with each other, and thus the link reliability is improved.

Member ports of the same aggregation group shall have the same configurations. The configurations mainly include STP, QoS, VLAN, port attribute, MAC address learning, ERPS configuration, loop protection configuration, mirror, 802.1x, IP filtering, MAC filtering, port isolation, etc.

3.4.1 trunk

Command Description

interface trunk [trunk ID]

Configuration trunk

trunk [trunk ID]

Default

None

Command Mode

Global configuration mode

Example

switch(config)# interface trunk 1

switch(config)# interface G1

switch(config-G1)# trunk 1

3.4.2 load-balance

Command Description

load-balance

//This command is to set up static aggregation of load balance mode.

Parameter

both-mac	Based on the source mesh MAC load balancing
dst-mac	Based on the destination MAC load balancing
src-mac	Based on the source MAC load balancing

Default

Disable

Command Mode

Interface configuration mode

Example

//This command is to set up load balancing model based on source and destination MAC.

switch(config)# load-balance both-mac

3.4.3 lacp enable | disable

Command Description

lacp enable

//This command is used to enable dynamic aggregation of ports.

lacp disable

//This command is used to disable dynamic aggregation of ports.

Parameter

None

Default

Disable

Command Mode

Interface configuration mode

Example

switch(config)#interface G1

switch(config-G1)# lacp disable

3.4.4 lacp active | passive

Command Description

lacp active

lacp passive

//This command is used to configure the role of an LACP port.

//It specifies the role of a port, which is active or passive.

Parameter

None

Default

active

Command Mode

Interface configuration mode

Example

switch(config)#interface G1

switch(config-G1)# lacp active

3.4.5 lacp key

Command Description

LACP key refers to the management key value of a dynamic aggregation port and determines whether the port can be added into an aggregation port. LACP protocol generates an operation key based on the port configuration (that is, the rate, duplex, basic configuration and management key). Members of a dynamic aggregation group can only be aggregated when they have the same operation key.

Parameter

<1-65535>: The key value is manually specified. The value ranges from **1** to 65535.

auto: The key value is automatically negotiated.

Default

auto

Command Mode

Interface configuration mode

Example

switch(config)# interface G1

switch(config-G1)# lacp key 100

3.4.6 lacp port-priority

Command Description

lacp port-priority *<1-32768>*

//This command is used to configure the priority of an LACP port.

Parameter

<1-32768>: It specifies the priority range. A smaller value indicates a higher priority.

Default

0

Command Mode

Interface configuration mode

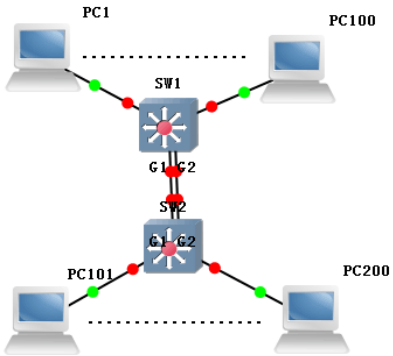
Example

switch(config)# interface G1

switch(config-G1)# lacp port-priority 100

3.4.7 example

The link aggregation is used to increase the bandwidth of device-level serial ports and share loads based on the source/destination MAC address.



SW1/SW2:

switch# configure terminal

```
switch(config)# load-balance both-mac
switch(config)# interface trunk 1
switch(config)# interface G1
switch(config-G1)# trunk 1
switch(config)# interface trunk 1
switch(config)# interface G2
switch(config-G1)# trunk 1
```

phenomenon:

After aggregation, two links form one logical link and thus the bandwidth is doubled. Besides, the load is shared based on the source or destination MAC address. When one link in the aggregation group is disconnected, the packet is sent through another link, and thus the communication is not interrupted.

4. Advanced configuration commands

4.1 VLAN config

VLAN configuration commands include:

switchport mode

switchport pvid

switchport trunk|hybrid| access

show vlan

Function Brief

Ethernet is a shared communication media based on the Carrier Sense Multiple Access/Collision Detect (CSMA/CD) technology. A LAN built using the Ethernet technology is not only a collision domain, but also a broadcast domain. When the number of hosts on the network is large, the collision becomes serious, broadcast flooding occurs, and the performance is significantly degraded. Even worse, the network is unavailable. Deployment of bridges or L2 switches on the Ethernet can resolve the problem of serous collision, but still cannot isolate broadcast packets. To address this issue, the Virtual Local Area Network (VLAN) technology emerges. This technology can divide a physical LAN into multiple logical LANs, that is, VLANs. Hosts located in the same VLAN can directly communicate with each other, but hosts located in different VLANs cannot communicate with each other. In this way, broadcast packets are confined in the same VLAN. That is, each VLAN is a broadcast domain.

Advantages of VLAN are as follows:

1) Improve network performance. Broadcast packets are confined in the VLAN, which effectively controls broadcast storms of the network, saves the network bandwidth, and improves the network processing capability.

2) Enhance network security. Devices in different VLANs cannot access each other, and hosts in different VLANs cannot directly communicate with each other. Packets must be forwarded at L3 through network layer devices, such as routers or L3 switches.

3) Simplify network management. Hosts in the same virtual work group are not limited to a certain physical range, which simplifies network management, and makes it convenient for people in different areas to set up work groups.

4.1.1 switchport mode

Command Description

switchport mode {access | trunk | hybrid }

//This command is to configure the port mode.

Parameter

Parameter	Parameters of the command mode
access	Access mode
trunk	Trunk mode
Hybrid	Hybrid mode

Default

Access mode

Command Mode

Interface configuration mode

A switch port supports the following modes:

- Access mode: The port belongs to only one VLAN, and only sends and receives untagged Ethernet frames.
- Trunk mode: The port is connected with other switches, and can receive and send tagged Ethernet frames.
- Hybrid mode: The port can be connected to a PC or a switch and router. (The hybrid mode is the combination of the access mode and the trunk mode.)

Example

//The port is configured to VLAN trunk /hybrid/access.

Switch(config)# interface T1

Switch(config-T1)#switchport mode trunk /hybrid/access

4.1.2 switchport pvid

Command Description

switchport pvid { vlan-id}

Parameter

Parameter	Parameters of the command mode
Vlan-id	Vlan id.Value range:1-4094.

Default

Vlan1

Command Mode

Interface configuration mode

Example

//The default vlan Settings for the port for vlan2.

Switch(config)# interface T1

Switch(config-T1)# switchport pvid 2

4.1.3 switchport trunk|hybrid| access

Command Description

switchport trunk tag {vlan-id}

switchport hybrid tag|untag|unpvid {vlan-id}

switchport access {vlan-id}

Parameter

Parameter	Parameters of the command mode.
Vlan-id	Vlan id,Value range:1-4094.

Default

All ports are members of vlan1, do not belong to other vlan

Command Mode

Interface configuration mode

Example

//This command is the trunk mode port to join one vlan or multiple vlan.

switch(config)# interface T1

switch(config-T1)# switchport mode trunk

switch(config-T1)# switchport trunk tag 2

switch(config-T1)# switchport trunk tag 3-4

//This command is the hybrid mode port to join one vlan or multiple vlan.

switch(config-T1)# switchport mode hybrid

switch(config-T1)# switchport hybrid tag|untag 2

switch(config-T1)# switchport hybrid tag| untag 3-4

//This command is to access mode port to join vlan2

switch(config-T1)# switchport access 2

4.1.4 show vlan

Command Description

show vlan [vlan-id]

Parameter

Parameter	Parameters of the command mode
vlan-id	The display VLAN Value range:1－4094.

Default

None

Command Mode

Privileged mode

Example

//This command is to display all VLAN information.

Switch#show vlan

Vid Status Name Ports

---

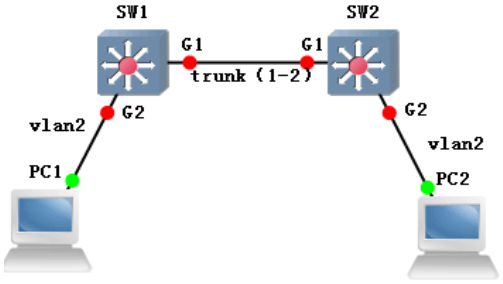
1 static vlan1 G1 G2 G3 G4 T1 T2 T3 T4 T5 T6 T7 T8 T9 T10 T11 T12 T13 T14 T15 T16 T17 T18 T19 T20 T21 T22 T23 T24

2 static vlan2

3 static vlan3

4.1.5 example

Enable VLAN communication across different switches. (PC1 and PC2 can communicate with each other normally.)

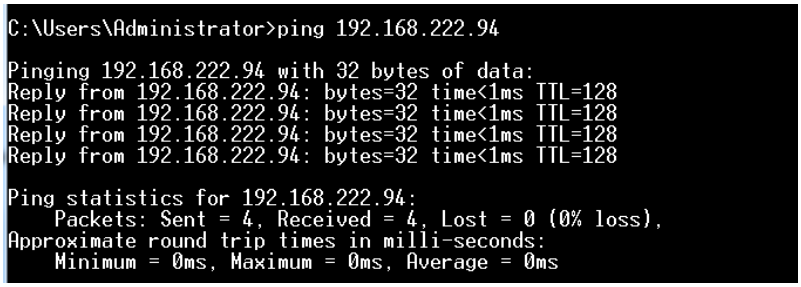


SW1/SW2:

```
switch# configure terminal
switch(config)# interface G1
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk tag 2
switch(config-if)# exit
switch(config)# interface G2
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 2
```

phenomenon:

pc1（192.168.222.107）and pc2（192.168.222.94）are mutually pinged.



4.2 QinQ config

Qinq configuration commands include:

Qinq

Qinq otpid

Function Brief

QinQ technology through the stacked two 802.1Q in the Ethernet frame header, effectively expanded the number of VLAN, make the number of vlans up to 4094x4094.

4.2.1 qinq

Command Description

Enable qinq

//no qinq express disable qinq function.

Parameter

None

Default

None

Command Mode

Interface configuration mode

Example

switch(config)# interface G1

switch(config-G1)# qinq

4.2.2 qinq otpid

Command Description

Configuration tag QinQ layer protocol type.

Parameter

<0x0000-0x9999>	Tag QinQ layer protocol type

Default

0x8100

Command Mode

Interface configuration mode

Example

switch(config)# qinq otpid 0x88a8

4.3 MAC config

MAC configuration commands include:

mac-address aging-time

show mac-addres

Function Brief

The switch is able to send packets directly to the destination node instead of sending packets to all nodes as a hub,the key technology is that the switch can identify the network card MAC address of the node, then put them in a place called MAC address table. The MAC address table is stored in the switch's cache and remembers these addresses.In this way, when the data is sent to the destination address, the switch can locate the node position of the MAC address in the MAC address table, and then send the data directly to the node of the location. MAC address number refers to the number of MAC addresses that can be stored in the MAC address table of the switch, the more the number of MAC addresses is stored, the higher the speed and efficiency of data forwarding.

4.3.1 mac-address aging-time

Command Description

mac address-table aging-time time {10-1000000}:

//This command is used to set the aging time of the MAC address. If the aging time is set to 0, the MAC address is automatically aged.

no mac address-table aging time:

//This command is used to restore the default aging time.

Parameter

Parameter	Parameters of the command mode
time	The value range is <0, 10-1000000>.

Default

None

Command Mode

Global configuration mode

Example

//Set the MAC address aging time to 100s.

switch(config)# mac-address aging-time 100

//Set the MAC address aging time to 300s.

switch(config)# no mac-address aging-time

4.3.2 show mac-address

Command Description

show mac-addres{ aging-time}

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

//This command can display the MAC address and MAC address of the aging time.

switch# show mac-address

MAC Vlan Port Type

94-de-80-dc-cf-38 1 G4 dynamic

60-92-17-9d-30-c3 1 G4 dynamic

Switch# show mac-address aging-time

Mac address aging-time : 100

4.4 ARP config

ARP configuration commands include:

show arp

arp static

arp timeout

Function Brief

This function module, you can view the ARP entry information that the switch has learned, you can add ARP static entries to prevent unauthorized access to the

host and modify the aging time of ARP entries.

4.4.1 show arp

Command Description

show arp

//This command to display the ARP.

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

//This command to display the ARP.

switch(config)# show arp

4.4.2 arp static

Command Description

arp static ip_addr mac_addr

//This command is used to add a static entry.

no arp static ip_addr

//This command is used to delete a static entry.

Parameter

Parameter	Parameters of the command mode
ip_addr	Ip address,Value range:X.X.X.X.
mac_addr	Mac address,Value range:H.H.H.H

Default

None

Command Mode

Global configuration mode

Example

// Add a static entry.

switch(config)# arp static 192.168.111.1 00-00-a1-b2-c3-d4

4.4.3 arp timeout

Command Description

arp timeout seconds

//This command is used to set the aging time.

no arp timeout

//This command is used to cancel time Settings.

Parameter

Parameter	Parameters of the command mode
seconds	Unit :second, value range:60-86400.

Default

None

Command Mode

Interface configuration mode

Example

//This command is to set up the ARP aging time for 3000 seconds.

switch(config)# interface vlanif1

switch(config-vlanif1)# arp timeout 3000

4.5 MSTP config

MSTP configuration commands include:

spanning-tree

spanning-tree mode

spanning-tree max-age

spanning-tree hello-time

spanning-tree forward-delay

spanning-tree max-hop

spanning-tree instance

show spanning-tree

show spanning-tree interface brief

Function Brief

STP is developed based on IEEE 802.1D, and is a protocol used to eliminate physical loops at the data link layer in the LAN. STP-enabled devices exchange information to detect loops on the network, and selectively block some ports to change a loop topology into a loop-free tree topology. This prevents continuous growing and infinite loop of packets on the loop network, and prevents occurrence of problems such as degraded packet processing capability of devices caused by repeated receiving of the

same packets.

Protocol packets used by STP are Bridge Protocol Data Units (BPDUs), which are also called configuration messages. A BPDU contains sufficient information to ensure that a device can complete the spanning tree computation process. STP transfers BPDUs between devices to determine the network topology.

4.5.1 spanning-tree

Command Description

spanning-tree:

//This command is used to enable the STP function.

no spanning-tree:

//This command is used to disable the STP function.

Parameter

None

Default

Enable

Command Mode

Global configuration mode

Example

switch(config)# spanning-tree

switch(config)# no spanning-tree

4.5.2 spanning-tree mode

Command Description

spanning-tree mode {stp|rstp|mstp}

//This command is used to set the STP version.

Parameter

Stp	Enable STP
rstp	Enable RSTP
mstp	Enable MSTP

Default

stp

Command Mode

Global configuration mode

Example

switch(config)# spanning-tree mode rstp

//Set the STP version to RSTP.

4.5.3 spanning-tree max-age

Command Description

spanning-tree max-age {6-40}

Parameter

seconds	BPDU biggest survival time.Value range:6-40s.

Default

20s

Command Mode

Global configuration mode

Example

//This command configure the STP the largest survival time for 24 seconds.

switch(config)# spanning-tree max-age 24

4.5.4 spanning-tree hello-time

Command Description

spanning-tree hello-time｛1-10｝

Parameter

Time	Hello message sending interval,Value range:1-10s.

Default

2s

Command Mode

Global configuration mode

Example

Switch(config)# spanning-tree hello-time 10

//This command configure the STP hello message sending time interval to 10 seconds.

4.5.5 spanning-tree forward-delay

Command Description

spanning-tree forward-delay｛4-30｝

Parameter

time	Forwarding delay ,Value range:4-30s.

Default

15 seconds

Command Mode

Global configuration mode

Example

switch(config)# spanning-tree forward-delay 20

//This command configure the STP forwarding delay for 20 seconds.

4.5.6 spanning-tree max-hop

Command Description

spanning-tree max-hop { 1-40 }

Parameter

hop	BPDU max-hop, Value range:1-40.

Default

20

Command Mode

Global configuration mode

Example

switch(config)# spanning-tree max-hop 40

//This command configure bpdus protocol packet maximum hop count of 40 effective.

4.5.7 spanning-tree instance

Command Description

spanning-tree instance

//This command is to configure the vlan and examples of MSTP mapping relationship.

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

switch(config)# spanning-tree instance 44 vid 4

4.5.8 spanning-tree mstp name

Command Description

spanning-tree mstp name

//This command is to configure the MSTP domain name.

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

switch(config)# spanning-tree mstp name 2

4.5.9 spanning-tree mstp revision

Command Description

spanning-tree mstp revision

//This command is the configuration revision number of MSTP.

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

switch(config)# spanning-tree mstp revision 2

4.5.10 show spanning-tree

Command Description

show spanning-tree

Parameter

None

Default

None

Command Mode

Global configuration mode and Privileged mode

Example

//Display the STP configuration.

switch# show spanning-tree

Spanning-tree is disable:

max age 20 bridge forward delay 20

forward delay 15 max hops 20

hello time 2 orce protocol version mstp

4.5.11 show spanning-tree interface brief

Command Description

show spanning-tree interface brief

Parameter

None

Default

None

Command Mode

Global configuration mode and Privileged mode

Example

switch(config)# show spanning-tree interface brief

```
switch(config)# show spanning-tree interface brief
MSTID Port        Role              State
----------------------------------------
0     G1          Disabled          discarding
0     G2          Disabled          discarding
0     G3          Disabled          discarding
0     G4          Disabled          discarding
0     G5          Disabled          discarding
0     G6          Disabled          discarding
0     G7          Designated        forwarding
0     G8          Disabled          discarding
```

4.6 IGMP-snooping

IGMP snooping configuration commands include:

igmp-snooping

igmp-snooping host-age-time

igmp-snooping fast-leave

igmp-snooping static-group

show igmp-snooping group

Function Brief

Internet Group Management Protocol Snooping, shorted as IGMP Snooping, is a multicast restriction mechanism running on a L2 device to manage and control multicast groups. The L2 device on which IGMP Snooping runs analyzes the received IGMP packets, create a mapping relationship between ports and MAC multicast addresses and forwards multicast data according to the mapping relationship

4.6.1 igmp-snooping

Command Description

ip igmp snooping:

//This command is used to enable the igmp-snooping function.

no ip igmp snooping:

//This command is used to disable the igmp-snooping function.

Parameter

None

Default

Disable

Command Mode

Global configuration mode

Example

//This command will configure open and closed igmp snooping:

switch(config)# igmp-snooping

switch(config)#no igmp-snooping

4.6.2 igmp-snooping host-age-time

Command Description

igmp-snooping host-age-time｛200-1000｝

Parameter

Parameter	Parameters of the command mode
time	Old Time,value range:200-1000s.

Default

260S

Command Mode

Global configuration mode

Example

//This command will configure a old time of 200s:

switch(config)# igmp-snooping host-age-time 200

4.6.3 igmp-snooping fast-leave

Command Description

ip igmp-snooping fast-leave:

//This command is used to enable the immediate leave function of a port.

no ip igmp-snooping fast-leave:

//This command is used to disable the immediate leave function of a port.

Parameter

None

Default

Disable

Command Mode

Interface configuration mode

Example

switch(config)# interface G1

switch(config-G1)# igmp-snooping fast-leave

4.6.4 igmp-snooping static-group

Command Description

igmp-snooping static-group

//This command is to add the static multicast group.

no igmp-snooping static-group

//This command is to delete the static multicast group.

Parameter

None

Default

Disable

Command Mode

Interface configuration mode

Example

switch(config)# interface G1

switch(config-G1)# igmp-snooping static-group 224.1.1.1 vlan 2

switch(config-G1)# no igmp-snooping static-group 224.1.1.1 vlan 2

4.6.5 show igmp-snooping group

Command Description

show igmp-snooping group

Parameter

None

Default

None

Command Mode

Privileged mode

Example

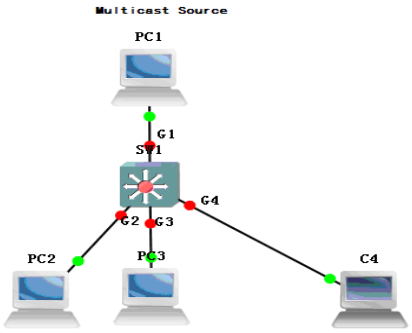
//This command is to display multicast group information:

switch# show igmp-snooping group

VID	SOURCE	GROUP	interFACE
1	0.0.0.0	233.45.18.88	G4
1	0.0.0.0	239.255.255.250	G4 G2
1	0.0.0.0	224.0.0.252	G2 G4

4.6.6 example

Member ports requesting to join the multicast group can receive multicast streams, but non-member ports not requesting to join the multicast group cannot receive multicast streams.



switch# configure terminal

switch(config)# igmp snooping

switch(config)# interface G1

switch(config-G1)# igmp-snooping static-group 233.2.2.2 vlan 1

switch(config)# interface G2

switch(config-G2)# igmp-snooping static-group 233.2.2.2 vlan 1

switch(config)# interface G3

switch(config-G3)# igmp-snooping static-group 233.2.2.2 vlan 1

phenomenon:

PC2/PC3 can receive video streams from the multicast source, but PC4 cannot.

4.7 DHCP server

DHCP server configuration commands include:

ip dhcpd
dhcp pool
network
default-router
dns-server
static
lease
domain-name
netbios-name-server

Function Brief

DHCP server refers to a computer that manages DHCP standards on a specific network. It allocates a unique IP address to each workstation that logs in to the server. DHCP server greatly simplifies network management which needs to be manually completed before.

4.7.1 ip dhcpd

Command Description

ip dhcpd enable:

//This command is used to enable the DHCP service.

ip dhcpd disable:

//This command is used to disable the DHCP service.

Parameter

None

Default

Disable

Command Mode

Global configuration mode

Example

//This command is used to globally enable the DHCP server.

switch(config)# ip dhcpd enable

4.7.2 dhcp pool

Command Description

dhcp pool <word>:

// This command is used to add a DHCP address pool.

No dhcp pool <word>:

// This command is used to delete a DHCP address pool with the specified name.

Parameter

Parameter	Parameters of the command mode
NAME	Pool name ,Example:dizhichi

Default

None

Command Mode

Global configuration mode

Example

//This command is to create a named dizhichi address pool.

switch(config)#dhcp pool dizhichi

4.7.3 network

Command Description

network A.B.C.D/M vlanif-id

//This command is used to add an IP address segment to the address pool.

Parameter

Parameter	Parameters of the command mode
A.B.C.D/M	Address pool,Example:192.168.1.0/24
vlanif-id	Interface Vlan id

Default

None

Command Mode

Address pool configuration mode

Example

switch(config-dhcp)#Network 192.168.1.0/24 vlanif1

//Set the DHCP from vlan1 distributed address segment is 192.168.1.0/24

4.7.4 default-router

Command Description

Default-router <A.B.C.D>:

//This command is used to configure the default gateway of the address pool.

Parameter

Parameter	Parameters of the command mode
A.B.C.D	Default-router

Default

None

Command Mode

Address pool configuration mode

Example

switch(config-dhcp)#Default-router 192.168.1.1

//This command is to set up DHCP issued a gateway.

4.7.5 dns-server

Command Description

Dns-server<A.B.C.D>:

// This command is used to configure the IP address of the DNS server.

Parameter

Parameter	Parameters of the command mode
A.B.C.D	dns address

Default

None

Command Mode

Address pool configuration mode

Example

switch(config-dhcp)#dns-server 192.168.1.1

//Set the DNS server address 192.168.1.1

4.7.6 static

Command Description

static A.B.C.D MAC

//This command is used to static binding IP and MAC.

no static A.B.C.D

//This command is used to delete static binding.

Parameter

Parameter	Parameters of the command mode
A.B.C.D	Static binding IP
MAC	Static binding MAC

Default

None

Command Mode

Address pool configuration mode

Example

switch(config-dhcp)#static 192.168.1.1 11-11-11-11-11-11

//This command is static binding 192.168.1.1 and 11-11-11-11-11-11

switch(config-dhcp)#no static 192.168.1.1

//This command is used to delete static binding.

4.7.7 lease

Command Description

lease <0-31536000>/infinite

//This command is used to configure the lease period of the IP address in the address pool.

Parameter

Parameter	Parameters of the command mode
<0-31536000>	Time range Unit: second
infinite	permanent

Default

Infinite

Command Mode

Address pool configuration mode

Example

// This command is used to configure the lease time of the address pool to 3600s.

switch(config)# dhcp pool 1

switch(config-dhcp)# lease 3600

4.7.8 domain-name

Command Description

domain-name domain

//This command is used to configure the DNS server domain name.

Parameter

Parameter	Parameters of the command mode
domain	Domain-name,Example:www.dahua.com

Default

None

Command Mode

Address pool configuration mode

Example

switch(config)# dhcp pool 1

switch(config-dhcp)# domain-name www.dahua.com

//This command is used to configure the DNS server domain name at www.dahua.com.

4.7.9 nbns-server

Command Description

nbns-server A.B.C.B

//This command is used to configure the secondary DNS server.

Parameter.

Parameter	Parameters of the command mode
A.B.C.D	DNS ip address

Default

None

Command Mode

Address pool configuration mode

Example

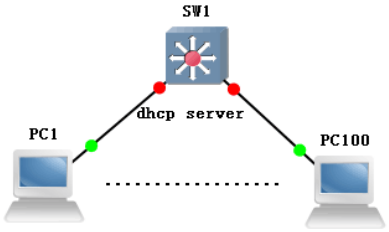
//Set the secondary DNS server address 114.114.114.114 .

switch(config)# dhcp pool 1

switch(config-dhcp)# nbns-server 114.114.114.114

4.7.10 example

This command is used to configure the switch to a DHCP server, so that IP addresses at the client are uniformly allocated by the server.



switch# configure terminal

switch(config)# ip dhcpd enable

switch(config)# dhcp pool a

switch(config-dhcp)# default-router 192.168.1.1

switch(config-dhcp)#dns-server 8.8.8.8

switch(config-dhcp)# lease 1000

switch(config-dhcp)# network 192.168.1.0/24 vlanif1

phenomenon:

Clients including PC1-PC100 can obtain correct IP addresses from the DHCP server (SW 1).

Note: An L3 interface of the same VLAN shall be configured for the DHCP server in the VLAN, so that the DHCP server can distribute IP addresses to clients in the VLAN.

4.8 DHCP relay

Function Brief

If the DHCP client and the DHCP server on the same physical network segment, the client can correctly obtain the IP address of dynamic allocation. If they are not in the same physical network, they need DHCP Relay Agent (relay agent). DHCP Relay agent can be removed to the necessary of DHCP server should be in each physical segment, It can deliver messages to the DHCP server that is not in the same physical subnet,it can also send a message back to the DHCP client that is not in the same physical subnet.

4.8.1 ip helper-address

Command Description

ip helper-address A.B.C.D

//This command is used to enable the DHCP relay.

no ip helper-address A.B.C.D

//This command is used to disable the DHCP relay.

Parameter

None

Default

Disable

Command Mode

Interface configuration mode

Example

//This command is used to open the DHCP relay in vlan 1

switch(config)#interface vlanif1

switch(config-vlanif1)# ip helper-address 192.168.1.1

4.9 DHCP snooping

DHCP snooping configuration commands include:

ip dhcp-snooping

ip dhcp-snooping trust

show ip dhcp-snooping lease

Function Brief

DHCP snooping is a security feature of DHCP, and provides the following functions: Ensure that a client obtains its IP address from an authorized server. If an unauthorized DHCP server that is built privately exists on the network, the DHCP clients may obtain incorrect IP addresses and network configuration parameters, and consequently cannot implement communication normally. To ensure that DHCP clients can obtain IP addresses from an authorized DHCP server, the DHCP snooping security mechanism supports configuration of ports as trusted or untrusted ports.

1、A trusted port can forward received DHCP packets normally.

2、On receiving the DHCP-ACK and DHCP-OFFER packets from the DHCP server, an untrusted port drops the packets.

4.9.1 ip dhcp-snooping

Command Description

ip dhcp-snooping:

//This command is used to enable the DHCP snooping configuration mode.

no ip dhcp-snooping:

//This command is used to disable the DHCP snooping configuration mode.

Parameter

None

Default

Disable

Command Mode

Global configuration mode

Example

None

4.9.2 ip dhcp-snooping trust

Command Description

ip dhcp-snooping trust:

//This command is used to configure the DHCP snooping trust mode.

no ip dhcp-snooping trust:

//This command is used to configure the DHCP snooping non-trust mode.

Parameter

None

Default

Non-Trust

Command Mode

Interface configuration mode

Example

//This command is to set port 1 model for trust.

switch(config)#interface G1

switch(config-G1)# ip dhcp-snooping trust

4.9.3 show ip dhcp-snooping lease

Command Description

show ip dhcp-snooping interface:

//This command is used to display the DHCP snooping trust mode of a port.

Parameter

None

Default

None

Command Mode

Privileged mode

Example

switch# show ip dhcp-snooping lease

```
switch# show ip dhcp-snooping lease
Mac-address          Vlan Ip              Type  Expire Interface
-----------------------------------------
fc-aa-14-d7-5e-5e 1    192.168.222.108 Dyn    6870   G16
```

4.10 QoS config

QoS configuration commands include:

remark

cos default

trust

cos map

dscp map

scheduler police

Function Brief

QoS(Quality of Service) refers to a network can use a variety of basic technology and provid better service capabilities for designated network communications. It is a technique that used to solve the problem of network delay and congestion.When the network overload or congestion, QoS can ensure that the important traffic is not delayed or discarded,while ensuring the efficient operation of the network.

4.10.1 remask

Command Description

Qos remask<all/cos/dscp>

Change the QoS trust mode weight.

Parameter

None

Default

Cos

Command Mode

Interface configuration mode

Example

//This command is to modify the G1 qos trust mode to DSCP port.

switch(config)# interface G1

switch(config-G1)# qos remask dscp

4.10.2 cos default

Command Description

cos default<0-7>

Parameter

None

Default

0

Command Mode

Interface configuration mode

Example

//This command is to modify the G1 qos trust mode to COS port.

switch(config)# interface G1

switch(config-G1)# cos default 6

4.10.3 trust

Command Description

qos trust

//This command is to set port trust packets take priority.

no qos trust

//This command is to set port trust default port priority.

Parameter

None

Default

Qos trust

Command Mode

Interface configuration mode

Example

//This command is to set port 1 trust port the default priority.

Switch(config)#interface G1

switch(config-G1)# no qos trust

4.10.4 cos map

Command Description

cos map

Set the mapping relationship between COS priority and queue.

Parameter

None

Default

Priority and queue one-to-one mapping

Command Mode

Global configuration mode

Example

//Map the cos priority 0 to the queue 3

switch(config)# cos map 0 3

4.10.5 dscp map

Command Description

dscp map

//Mapping relationship between DSCP priority and COS priority.

Parameter

None

Default

Dscp priority	Cos priority
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

Command Mode

Global configuration mode

Example

//Map the DSCP priority 45 to Cos priority 7

switch(config)# cos map 45 7

4.10.6 scheduler policy

Command Description

scheduler police

//Set Qos scheduling algorithm.

Parameter

sp	Strict priority mode: First in the queue with the highest priority service, until the priority is empty and service for the next high priority queue, and so on.
wrr	Weighted round robin scheduling algorithm: To support different bandwidth requirements, it can allocate different proportion of output bandwidth for different queues.

Default

sp

Command Mode

Global configuration mode

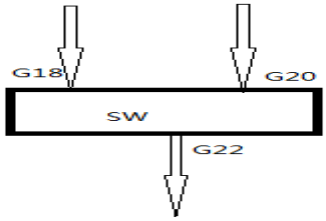
Example

switch(config)# scheduler policy wrr 1 2 3 4 5 6 7 8

4.10.7 example

Test topology map (test is based on the QoS of ports)

The 1-3 port of the Ixia tester corresponds to the G18-G22 of the switch.



（一）Configuration

// When the data packets in the port is not marked with any priority, the priority of the port is set to the corresponding queue.

a、Set the packets which enter the 18 port are marked with priority 7 and set the packets which enter the 20 port are marked with priority 6.

switch(config)#interface G18

switch(config-G18)cos default 7

switch(config-G18)no qos trust

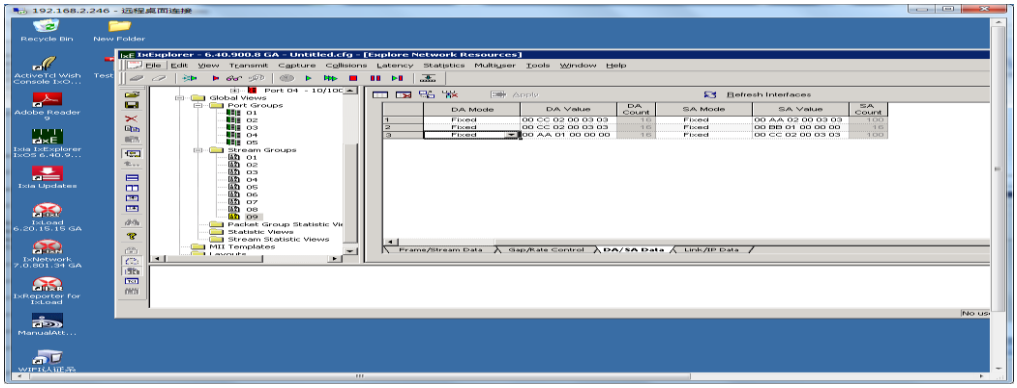
switch(config-G18)exit

switch(config)#interface G20

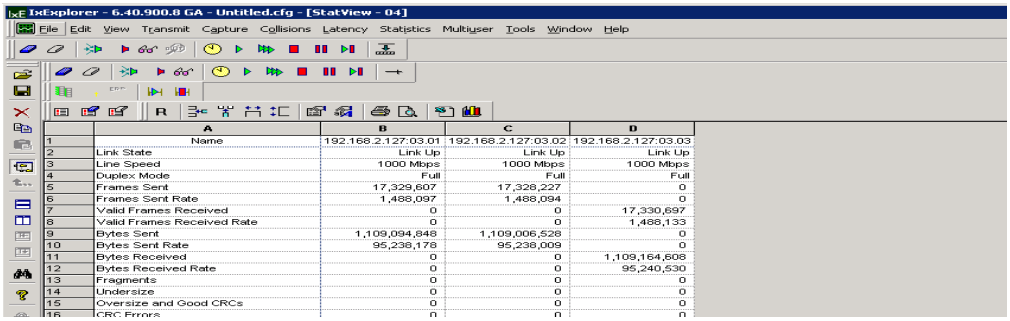
switch(config-G20)cos default 6

switch(config-G20)no qos trust

b、Set the destination address of the Ixia1-2 port to the source MAC address of the Ixia3 port.



c、1-2 ports start sending data packets after learning MAC addresss.



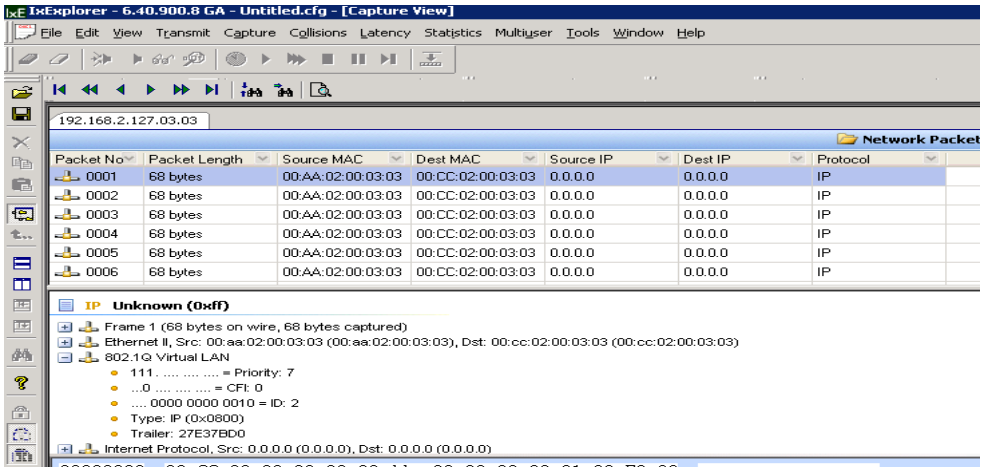
	A	B	C	D
1	Name	192.168.2.127:03.01	192.168.2.127:03.02	192.168.2.127:03.03
2	Link State	Link Up	Link Up	Link Up
3	Line Speed	1000 Mbps	1000 Mbps	1000 Mbps
4	Duplex Mode	Full	Full	Full
5	Frames Sent	17,329,607	17,328,227	0
6	Frames Sent Rate	1,488,097	1,488,094	0
7	Valid Frames Received	0	0	17,330,697
8	Valid Frames Received Rate	0	0	1,488,133
9	Bytes Sent	1,109,094,848	1,109,006,528	0
10	Bytes Sent Rate	95,238,178	95,238,009	0
11	Bytes Received	0	0	1,109,164,608
12	Bytes Received Rate	0	0	95,240,530
13	Fragments	0	0	0
14	Undersize	0	0	0
15	Oversize and Good CRCs	0	0	0
16	CRC Errors	0	0	0

（二）Test result

Conclusion:pass

Observe the source MAC address of the packets which capture in port 3 ,you can find that the received data packets from port 11.

the packets of high queue first pass



4.11 VRRP

configuration commands include:

vrrp advertisement

vrrp IP

vrrp preempt

vrrp preempt time

vrrp priority

Function Brief

Virtual Router Redundancy Protocol,or VRRPfor short, it is proposed by IETF to solve the routing protocol of single point of failure in the local area network configuration.It has introduced a standard RFC2338 protocol in 1998. VRRP is widely used in the edge network, It is design intent to support the IP data traffic failed to transfer in a given case will not cause confusion, allow the host to use a single router, make the connectivity between routers is still maintained timely in the case of the failure of the first hop router.

VRRP is a routing fault tolerance protocol, which can also be called backup routing protocol. A default route is set for all hosts in a local area network, when the destination address in the network from the host are not in the network segment, the message will be sent to the external router through the default route, so that the communication between the host and the external network is realized. The internal host will not be able to communicate with the external after the default router down off (port is closed), If the router set up VRRP, then the virtual router will enable the backup router at this time,so can achieve the whole network communication.

4.11.1 vrrp advertisement

Command Description

vrrp <group> advertisement <time>

Parameter

Parameter	Parameters of the command mode
Group	VRRP group,1-255
Time	Time interval between1-10s,default 1s

Default

None

Command Mode

Interface configuration mode

Example

//Modify notification time of group1 is 5 seconds.

switch(config)# interface vlanif1

switch(config-vlanif1)# vrrp 1 advertisement 5

4.11.2 vrrp ip

Command Description

vrrp<group> ip A.B.C.D

//This command is to set up virtual routing IP address.

Parameter

None

Default

None

Command Mode

Interface configuration mode

Example

//This command is to set up virtual IP as 192.168.1.254.

switch(config)#interface vlanif1

switch(config-vlanif1)# vrrp 1 ip 192.168.1.254

4.11.3 vrrp preempt

Command Description

vrrp<group> preempt

//This command is VRRP preemption mode.

no vrrp<group> preempt

//This command is disabled VRRP preemption mode.

Parameter

None

Default

Enable

Command Mode

Interface configuration mode

Example

//This command is disabled VRRP preemption mode.

switch(config)#interface vlanif1

switch(config-vlanif1)#no vrrp 1 preempt

4.11.4 vrrp preempt time

Command Description

vrrp<group> preempt time< 0-1000s>

//This command is to set the current VRRP group delay.

Parameter

Time: Time range 0-1000s,Default 0s

Default

0

Command Mode

Interface configuration mode

Example

//This command is to set up 3 seconds after the preemption.

switch(config)#interface vlanif1

switch(config-vlanif1)# vrrp 1 preempt 3

4.11.5 vrrp priority

Command Description

vrrp<group> priority <priority>

//This command is to set up the gateway priority.

Parameter

priority:Priority range1-254,Default 100,

the greater the number, the higher the priority.

Default

Enable

Command Mode

Interface configuration mode

Example

//This command is to set priorities for 111.

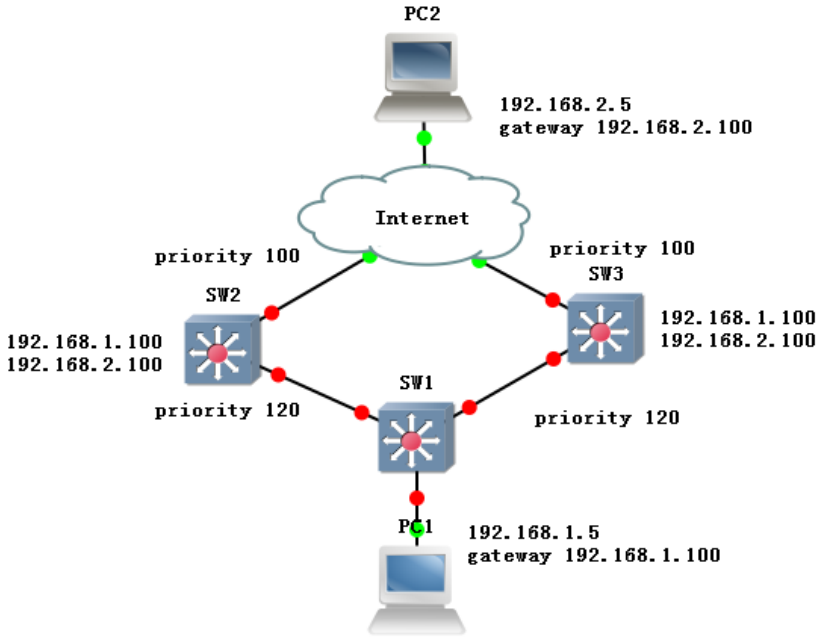
switch(config)#interface vlan1

switch(config-vlanif1)# vrrp 1 ip 192.168.2.1

switch(config-vlanif1)#vrrp 1 priority 111

4.11.6 example

a, Network diagram as shown in Figure:



Sw1:

switch(config)# interface vlan1

switch(config-vlanif2)# ip address 192.168.1.11/24

switch(config-vlanif2)#exit

switch(config)# interface vlan2

switch(config-vlanif2)# ip address 192.168.2.11/24

switch(config-vlanif2)#exit

switch(config)# interface g2

switch(config-G2)# switchport mode access

switch(config-G2)# switchport pvid 2

switch(config)# interface vlanif1

switch(config-vlanif1)# vrrp 1 ip 192.168.1.100

switch(config-vlanif1)#vrrp 1 priority 120

switch(config)# interface vlanif2

switch(config-vlanif2)# vrrp 2 ip 192.168.2.100

switch(config-vlanif1)#vrrp 2 priority 120

Sw2:

switch(config)# interface vlan1

switch(config-vlanif2)# ip address 192.168.1.22/24

switch(config-vlanif2)#exit

switch(config)# interface vlan2

switch(config-vlanif2)# ip address 192.168.2.22/24

switch(config-vlanif2)#exit

switch(config)# interface g2

switch(config-G2)# switchport mode access

switch(config-G2)# switchport pvid 2

switch(config)# interface vlanif1

switch(config-vlanif1)# vrrp 1 ip 192.168.1.100

switch(config)# interface vlanif2

switch(config-vlanif2)# vrrp 2 ip 192.168.2.100

Phenomena:

b, PC1 continued to ping PC2（you can capture data packets and find that the packets forwarded by SW2）

```
C:\Users\Administrator>ping 192.168.2.5

Pinging 192.168.2.5 with 32 bytes of data:
Reply from 192.168.2.5: bytes=32 time=1ms TTL=64
Reply from 192.168.2.5: bytes=32 time<1ms TTL=64
Reply from 192.168.2.5: bytes=32 time<1ms TTL=64
Reply from 192.168.2.5: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.2.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

c, Power down the SW2, observe the results of the Ping (switching time is about 3S)

```
Pinging 192.168.2.5 with 32 bytes of data:
Reply from 192.168.2.5: bytes=32 time<1ms TTL=64
Reply from 192.168.2.5: bytes=32 time<1ms TTL=64
Reply from 192.168.2.5: bytes=32 time<1ms TTL=64
Reply from 192.168.2.5: bytes=32 time<1ms TTL=64
Reply from 192.168.2.5: bytes=32 time<1ms TTL=64
Reply from 192.168.2.5: bytes=32 time<1ms TTL=64
Reply from 192.168.2.5: bytes=32 time<1ms TTL=64
Reply from 192.168.2.5: bytes=32 time<1ms TTL=64
Reply from 192.168.2.5: bytes=32 time<1ms TTL=64
Reply from 192.168.2.5: bytes=32 time<1ms TTL=64
Reply from 192.168.2.5: bytes=32 time<1ms TTL=64
Reply from 192.168.2.5: bytes=32 time<1ms TTL=64
Reply from 192.168.2.5: bytes=32 time<1ms TTL=64
Request timed out.
Reply from 192.168.2.5: bytes=32 time=1ms TTL=64
Reply from 192.168.2.5: bytes=32 time<1ms TTL=64
```

5. Routing configuration commands

5.1 Interface config

Interface configuration commands include:

interface

shutdown

ip address

show interface

Function Brief

Based on the switch L3 routing principle, the virtual interface is established for each Vlan to set up the L3 address information of each Vlan.

5.1.1 interface

Command Description

interface｛IFNAME｝

//This command is to enter interface configuration mode.

Parameter

Parameter	Parameters of the command mode
IFNAME	Interface vlan vlan range:vlan1-vlan4094

Default

None

Command Mode

Global configuration mode

Example

//This command is to vlan1 configuration mode.

switch(config)# interface vlan1

5.1.2 shutdown / no shutdown

Command Description

shutdown/no shutdown

//This command is turned on or off a vlan interface.

Parameter

None

Default

Open

Command Mode

Interface configuration mode

Example

switch(config-vlanif1)# shutdown

switch(config-vlanif1)# no shutdown

5.1.3 ip address

Command Description

ip address { A.B.C.D/M}

no ip address{ A.B.C.D/M}

Parameter

Parameter	Parameters of the command mode
A.B.C.D/M	Ipv4 address

Default

192.168.255.1

Command Mode

Interface configuration mode

Example

//This command is to add or delete an IP address.

switch(config)# interface vlan1

switch(config-vlanif1)# ip address 10.0.0.1/8

switch(config-vlanif1)# no ip address 10.0.0.1/8

5.1.4 show interface

Command Description

show interface{ IFNAME}

Parameter

Parameter	Parameters of the command mode
IFNAME	Vlan interface

Default

None

Command Mode

Privileged mode

Example

//This command is to look at the IP address of the vlan1.

switch# show interface vlan1

5.2 Static routing

Static routing configuration commands include:

ip route

show ip route

Function Brief

Static routing is a routing information that is manually configured by a user or network administrator. When the topology of the network or the state of the link changes, the network administrator needs to manually modify the routing table in the relevant static routing information.Static routing information is private by default and will not be passed to other routers.Of course, the network administrator can also be set to make the router to be shared.Static routing is generally applicable to a relatively simple network environment, in this environment, the network administrator can easily understand the topology of the network, easy to set up the correct routing information.

5.2.1 ip route

Command Description

ip route {A.B.C.D/M}{ gateway}{ 1-255}

ip route { A.B.C.D}{mask}gateway}{ 1-255}

//This command is to set up the static routing.

no ip route {A.B.C.D/M}{ gateway}{ 1-255}

no ip route { A.B.C.D}{mask}gateway}{ 1-255}

//This command is to delete the static routing.

Parameter

Parameter	Parameters of the command mode.
A.B.C.D	Ipv4 address.
A.B.C.D/M	Ipv4 address and mask.
Distance	administrative Distance range:1-255.

Default

None

Command Mode

Global configuration mode

Example

//This command is to add or delete the static routing.

switch(config)# ip route 0.0.0.0/8 0.0.0.0 1

switch(config)# no ip route 0.0.0.0/8 0.0.0.0 1

switch(config)# ip route 10.0.0.2 10.255.255.255.0 10.0.0.1 1

switch(config)# no ip route 10.0.0.2 10.255.255.255.0 10.0.0.1 1

5.2.2 show ip route

Command Description

show ip route:

//This command is used to display the static routes.

Parameter

None

Default

None

Command Mode

Privileged mode

Example

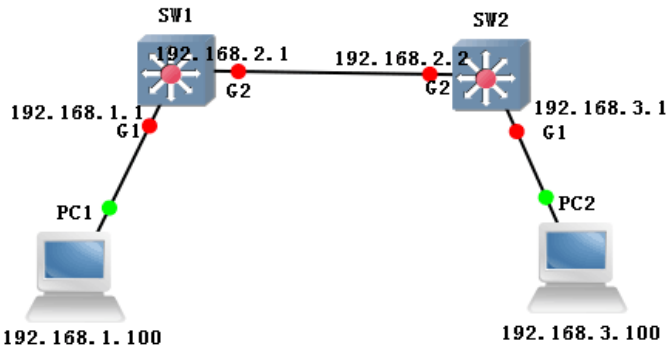
//Display the static routes.

switch# show ip route static

S>* 0.0.0.0/8 [1/0] via 192.168.255.1, vlanif1 S>* 0.0.0.0/8 [1/0] via 192.168.255.1, vlanif1

5.2.3 example

This command is used to realize trans-network segment communication between PC1 and PC2 through a static route.



sw1: switch# configure terminal

switch(config)# interface vlan1

switch(config-vlanif1)# ip address 192.168.1.1 /24

switch(config-vlanif1)# exit

switch(config)# interface vlan2

switch(config-vlanif2)# ip address 192.168.2.1/24

switch(config-vlanif2)# exit

switch(config)# interface G2

switch(config-G2)# switchport mode access

switch(config-G2)# switchport pvid 2

switch(config-G2)#exit

switch(config)# ip route 192.168.3.0/24 192.168.2.2 2

sw2: switch# configure terminal

switch(config)# interface vlan1

switch(config-vlanif1)# ip address 192.168.3.1/24

switch(config-vlanif1)# exit

switch(config)# interface vlan2

switch(config-vlanif2)# ip address 192.168.2.2/24

switch(config)# interface G2

switch(config-G2)# switchport mode access

switch(config-G2)# switchport pvid 2

switch(config-G2)#exit

switch(config)# ip route 192.168.1.0/24 192.168.2.1 2

pc1: ip 192.168.1.100 gateway 192.168.1.1

Pc2: ip 192.168.3.100 gateway 192.168.3.1

phenomenon:

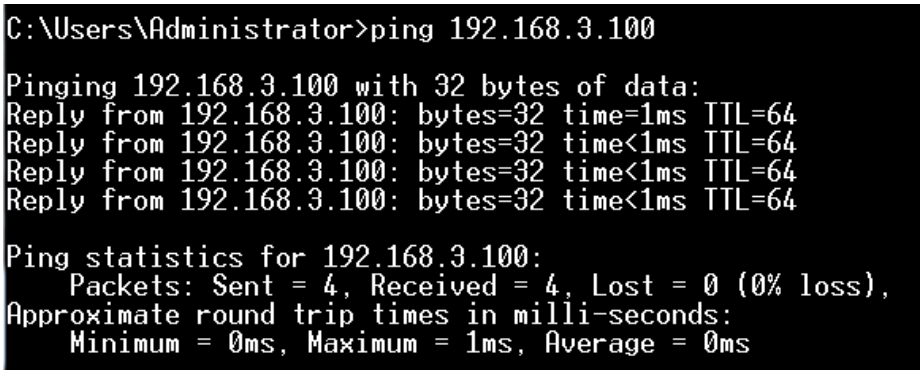
pc1 ping pc2

```
C:\Users\Administrator>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:
Reply from 192.168.1.100: bytes=32 time=1ms TTL=64
Reply from 192.168.1.100: bytes=32 time<1ms TTL=64
Reply from 192.168.1.100: bytes=32 time<1ms TTL=64
Reply from 192.168.1.100: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

pc2 ping pc1


C:\Users\Administrator>ping 192.168.3.100
Pinging 192.168.3.100 with 32 bytes of data:
Reply from 192.168.3.100: bytes=32 time=1ms TTL=64
Reply from 192.168.3.100: bytes=32 time<1ms TTL=64
Reply from 192.168.3.100: bytes=32 time<1ms TTL=64
Reply from 192.168.3.100: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.3.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms

5.3 OSPF config

OSPF configuration commands include:

router OSPF

network address wildmask area area-ID

router-id A.B.C.D

timers throttle spf

default-metric

passive-interface

redistribute rip|static|connected

default-information originate

ip ospf

Show ip ospf

Function Brief

OSPF is a link state routing protocol that uses bandwidth based metrics.OSPF uses the SPF algorithm to calculate the route,no routing loop is guaranteed from the algorithm,maintain route through neighbor relationship,Avoid periodic updates on bandwidth consumption.OSPF routing update rate is high, and the network convergence is fast,it is Suitable for large and medium sized networks.

5.3.1 router ospf

Command Description

router ospf

no router ospf

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

switch(config)#Router OSPF

//This command is enable the OSPF.

5.3.2 network

Command Description

network A.B.C.D/M area area-id

//Declaration of OSPF network and regional.

no network A.B.C.D/M area area-id

//Delete the declaration of OSPF network and regional.

Parameter

Parameter	Parameters of the command mode
A.B.C.D/M	Ip address and mask
area-id	area,range: <0-4294967295>

Default

None

Command Mode

Global configuration mode

Example

//Declaration of 192.168.1.0 network and divided in region 0

switch(config-ospf)#Network 192.168.1.0 0.0.0.255 area 0

5.3.3 router-id

Command Description

router-id A.B.C.D

//This command is to set up the router-id.

no router-id

//This command is set as the default router-id.

Parameter

Parameter	Parameters of the command mode
A.B.C.D	Router-id address

Default

0.0.0.0

Command Mode

Global configuration mode

Example

switch(config-ospf)#router-id 1.1.1.1

//This command is to modify the router-id for 1.1.1.1

5.3.4 timers throttle spf

Command Description

timers throttle spf TIME1 TIME2 TIME3

no timers throttle spf

//Configure the throttle SPF timer, use the no form of the command, the throttle SPF timer value is returned to the default value.

Parameter

Parameter	Parameters of the command mode
TIME1	Delay time,range:0-600000s
TIME2	Initialization time,range:0-600000s
TIME3	Max age, range:0-600000s

Default

Delay time 200s.

Initialization time 1000s.

Max age 10000s.

Command Mode

Global configuration mode

Example

//Set the delay, the initialization hold time, the maximum hold time is 111

switch(config-ospf)#timers throttle spf 111 111 111

5.3.5 default-metric

Command Description

default-metric metric

//This command is to configure OSPF default-metric.

no default-metric

//This command is to configure OSPF default-metric to default values.

Parameter

Parameter	Parameters of the command mode
Metric	Default-metric,range:0-16777214

Default

None

Command Mode

Global configuration mode

Example

switch(config-ospf)#default-metric 111

//This command is to configure OSPF default-metric for 111.

5.3.6 passive-interface default

Command Description

passive-interface default

//This command is to configure OSPF passive-interface default.

no passive-interface default

//This command is disable the OSPF passive-interface default.

passive-interface IFNAME

//This command is enable OSPF passive ports.

no passive-interface IFNAME

//This command is disable OSPF passive ports.

Parameter

Parameter	Parameters of the command mode
IFNAME	Port,Example G1,T1

Default

None

Command Mode

Global configuration mode

Example

switch(config-ospf)#passive-interface T1

//This command is the T1 for passive-interface.

5.3.7 redistribute

Command Description

redistribute RIP|static|connected

no redistribute RIP|static|connected

//The external routing is fully distributed into the OSPF network.

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

//This command is to set the OSPF redistribution RIP.

switch(config-ospf)#redistribute RIP

//This command is to set the OSPF redistribution static.

switch(config-ospf)#redistribute static

//This command is to set the OSPF redistribution connected.

switch(config-ospf)#redistribute connected

5.3.8 default-information originate

Command Description

default-information originate [always] [metric] [metric-type] [route-map]

no default-information originate [always] [metric] [metric-type] [route-map]

//default-information originate command is used to configure the local router to generate a default OSPF routing and related parameters, and to notify the neighbors.

//no default-information originate command is used to cancel the generation of the default route or to change the associated parameters.

Parameter

always	Always notify the default route.
always	Notice the cost of the default route.
metric-type	Notice the type of default route, the value of 1 or 2, the default is 2.
route-map	Notice the default route to call the route-map rule.

Default

None

Command Mode

OSPF configuration mode

Example

//Configure OSPF process 11 to generate a default route for metric 12:

switch(config-ospf-11)#default-information originate metric 12

5.3.9 ip ospf

Command Description

Ip ospf cost/network/priority/hello-interval/dead-interval/authentication/ authentication-key

//This command is set OSPF network attribute

Parameter

cost	Cost value,you can increase the measure value of this interface to go out.
network	Network type:point-to-point ,broadcast,non-broadcast
priority	Interface priority, broadcast multi access network to make it a DR
hello-interval	Valid time interval
dead-interval	Invalid time interval
authentication	Authentication Type:MD5、SIMPLE
authentication-key	Key authentication

Default

None

Command Mode

vlan configuration mode

Example

//This command is to modify the cost to 20.

switch(config)# interface vlanif2

switch(config-vlanif2)# ip ospf cost 20

//This command is to modify the network type of point-to-point.

switch(config)# interface vlanif2

switch(config-vlanif2)# ip ospf network point-to-point

//This command is to modify the interface priority for 254.

switch(config)# interface vlanif2

switch(config-vlanif2)# ip ospf priority 254

//Modify the effective interval of 30 seconds.

switch(config)# interface vlanif2

switch(config-vlanif2)# ip ospf hello-interval 30

//Modified failure interval time 300 seconds.

switch(config)# interface vlanif2

switch(config-vlanif2)# ip ospf dead-interval 300

//Modify the authentication type for MD5,The secret key for ABC certification .

switch(config)# interface vlanif2

switch(config-vlanif2)# ip ospf authentication message-digest
switch(config-vlanif2)# ip ospf authentication-key abc

5.3.10 show ip ospf

Command Description

//This command is used to display the OSPF

show ip ospf border-routers/database/interface/neighbor/route

Parameter

border-routers	Boundary router, which is used to display the border router.
database	Link state database, view OSPF link state database
interface	Display interface OSPF information
neighbor	Neighbor: view OSPF neighbor table
route	Route: view OSPF route

Default

None

Command Mode

Privileged mode

Example

//This command is to display the border-routers.

switch# show ip ospf border-routers

//This command is to display the database.

switch# show ip ospf database

//This command is to display OSPF interface information.

switch# show ip ospf interface vlanif1

//This command is to display the neighbor.

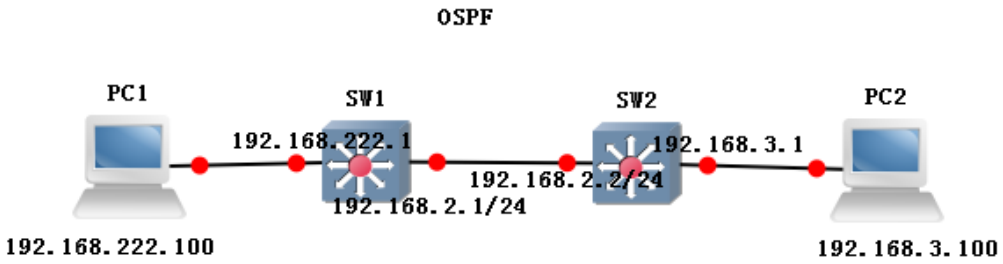
switch# show ip ospf neighbor

//This command is to display the OSPF route.

switch# show ip ospf route

5.3.11 example

Network diagram as shown in Figure:



sw1:

```
switch(config)#interface vlanif1
switch(config-vlanif1)# ip address 192.168.222.1/24
switch(config)#interface vlanif2
switch(config-vlanif2)# ip address 192.168.2.1/24
switch(config-vlanif2)#exit
switch(config)#interface G22
switch(config-G22)# switchport mode access
switch(config-G22)# switchport pvid 2
switch(config)# router ospf
switch(config-ospf)# ospf router-id 1.1.1.1
switch(config-ospf)# network 192.168.2.0/24 area 0
switch(config-ospf)# network 192.168.222.0/24 area 0
```

sw1:

```
switch(config)#interface vlanif3
switch(config-vlanif3)# ip address 192.168.3.1/24
switch(config-vlanif3)#exit
switch(config)#interface G23
switch(config-G23)# switchport mode access
switch(config-G23)# switchport pvid 3
switch(config)#interface vlanif2
switch(config-vlanif2)# ip address 192.168.2.2/24
switch(config-vlanif2)#exit
switch(config)#interface G22
switch(config-G22)# switchport mode access
switch(config-G22)# switchport pvid 2
switch(config)# router ospf
switch(config-ospf)# ospf router-id 2.2.2.2
switch(config-ospf)# network 192.168.2.0/24 area 0
switch(config-ospf)# network 192.168.3.0/24 area 0
```

phenomenon:

//Display OSPF route

SW1:

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

O   192.168.2.0/24 [110/10] is directly connected, vlanif2, 00:18:04
C>* 192.168.2.0/24 is directly connected, vlanif2
O>* 192.168.3.0/24 [110/20] via 192.168.2.2, vlanif2, 00:17:21
O   192.168.222.0/24 [110/10] is directly connected, vlanif1, 00:19:22
C>* 192.168.222.0/24 is directly connected, vlanif1
```

SW2:

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

O   192.168.2.0/24 [110/10] is directly connected, vlanif2, 00:18:54
C>* 192.168.2.0/24 is directly connected, vlanif2
O   192.168.3.0/24 [110/10] is directly connected, vlanif3, 00:18:10
C>* 192.168.3.0/24 is directly connected, vlanif3
O>* 192.168.222.0/24 [110/20] via 192.168.2.1, vlanif2, 00:18:04
```

PC1 ping PC2

```
C:\Users\Administrator>ping 192.168.3.100

Pinging 192.168.3.100 with 32 bytes of data:
Reply from 192.168.3.100: bytes=32 time=1ms TTL=64
Reply from 192.168.3.100: bytes=32 time<1ms TTL=64
Reply from 192.168.3.100: bytes=32 time<1ms TTL=64
Reply from 192.168.3.100: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.3.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

5.4 BGP config

BGP configuration commands include:

router bgp

timers bgp

redistribute

neighbor

Network

Function Brief

The border gateway protocol (BGP) is a routing protocol that runs on TCP,which is a kind of autonomous system. BGP is the only protocol that is used to

deal with the network size of the Internet, and is the only protocol that can properly handle the multi connection between the routing domain.BGP is built on the experience of EGP.The main function of the BGP system is to exchange network reachability information with other BGP systems.The network reachability information includes information of the autonomous system (AS) listed.These information effectively construct the topology of AS interconnection and thus clears the routing loop,At the same time, the AS level can be implemented in strategic decision-making.

5.4.1 router bgp

Command Description

router bgp

//This command is enable BGP.

Parameter

None

Default

None

Command Mode

Interface configuration mode

Example

//This command is enable BGP.

switch(config)# router bgp 1

5.4.2 timers bgp

Command Description

timers bgp

//This command is to set up BGP update-time and max age.

Parameter

None

Default

Update-time:60

Max age:180

Command Mode

Interface configuration mode

Example

//Setting the BGP update time is 50s, the aging time is 150s.

switch(config)# router bgp 1

switch(config-bgp)# timers bgp 50 150

5.4.3 redistribute

Command Description

redistribute

//This command is to set the BGP redistribution.

Parameter

None

Default

None

Command Mode

Interface configuration mode

Example

//This command is to set the BGP redistribution OSPF.

switch(config-bgp)# redistribute ospf

5.4.4 neighbor

Command Description

neighbor

//This command is to set up BGP neighbor information.

Parameter

None

Default

None

Command Mode

Interface configuration mode

Example

//This command is set the BGP neighbors to 192.168.222.222 belongs to AS1

switch(config)# router bgp 2

switch(config-bgp)# neighbor 192.168.222.22 remote-as1

5.4.5 network

Command Description

neighbor

//Set BGP neighbor information.

Parameter

None

Default

None

Command Mode

Interface configuration mode

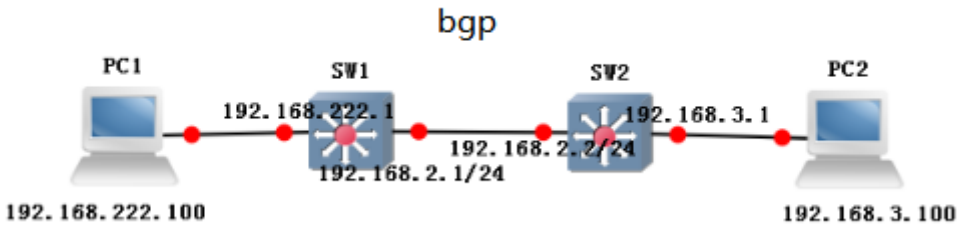
Example

//Declare the 192.168.3.0 network to BGP routing.

switch(config)# router bgp 1

switch(config-bgp)# network 192.168.3.0/24

5.4.6 example



sw1:

switch(config)# interface vlan1

switch(config-vlanif1)# ip address 192.168.222.1/24

switch(config)# interface vlan2

switch(config-vlanif2)# ip address 192.168.2.1/24

switch(config)# interface G2

switch(config-G2)# switchport pvid 2

switch(config)# router bgp 1

switch(config-bgp)# network 192.168.2.0

switch(config-bgp)# network 192.168.222.0

switch(config-bgp)# neighbor 192.168.2.2 remote-as 2

sw2:

switch(config)# interface vlan1

switch(config-vlanif1)# ip address 192.168.3.1/24

switch(config)# interface vlan2

switch(config-vlanif2)# ip address 192.168.2.2/24

switch(config)# interface G2

switch(config-G2)# switchport pvid 2

switch(config)# router bgp 2

switch(config-bgp)# network 192.168.2.0

switch(config-bgp)# network 192.168.3.0

switch(config-bgp)# neighbor 192.168.2.1 remote-as 1

phenomenon:

sw1:

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

C>* 192.168.2.0/24 is directly connected, vlanif2
B>* 192.168.3.0/24 [20/0] via 192.168.2.2, vlanif2, 00:01:14
C>* 192.168.222.0/24 is directly connected, vlanif3
switch#
```

Sw2:

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

B   192.168.2.0/24 [20/0] via 192.168.2.1 inactive, 00:02:04
C>* 192.168.2.0/24 is directly connected, vlanif2
C>* 192.168.3.0/24 is directly connected, vlanif1
B>* 192.168.222.0/24 [20/0] via 192.168.2.1, vlanif2, 00:02:04
switch#
```

PC1 ping PC2

```
C:\Users\Administrator>ping 192.168.3.100

Pinging 192.168.3.100 with 32 bytes of data:
Reply from 192.168.3.100: bytes=32 time=1ms TTL=64
Reply from 192.168.3.100: bytes=32 time<1ms TTL=64
Reply from 192.168.3.100: bytes=32 time<1ms TTL=64
Reply from 192.168.3.100: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.3.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

5.5 RIP config

RIP configuration commands include:

default-information

default-metric

distance

end

exit/quit

network

offset-list

passive-interface

redistribute

timers

version

Function Brief

RIP is Interior Gateway Protocol that more common used and used earlier.It is suitable for small and similar network,and it is a typical distance vector protocol.RIP exchange routing information through broadcast UDP messages,and it is send routing information update every 30 seconds.RIP provides count Hop (hop count) as a scale to measure routing distance.The hop count is the number of routers that a packet must pass to reach the target.If the same target has two different speed or bandwidth of the router, but the same hop count.Then RIP thinks that the two route is equal distance.RIP maximum support of the number of hops is 15,the number of hops 16 indicates that it is not reachable.

5.5.1 default-information originate

Command Description

//default-information originate

no default-information originate

Parameter

None

Default

None

Command Mode

Interface configuration mode

Example

Switch(config)#default-information originate

//Start rip to generate the default rip route function.

5.5.2 default-metric

Command Description

default-metric XX

no default-metric XX

Parameter

Parameter	Parameters of the command mode
XX	Default 1 ,range 1-16

Default

None

Command Mode

Interface configuration mode

Example

//This command is to set the default-metric to 5.

switch(config)# router rip

switch(config-rip)# default-metric 5

5.5.3 distance

Command Description

distance XX

Parameter

Parameter	Parameters of the command mode
XX	Range 1-255. Default 120

Default

120

Command Mode

Interface configuration mode

Example

//This command is to change administrative distance to 110.

switch(config)# router rip

switch(config-rip)# distance 110

5.5.4 end

Command Description

end

Parameter

None

Default

None

Command Mode

Interface configuration mode

Example

switch(config)# router rip

switch(config-rip)# end

5.5.5 exit/quit

Command Description

Exit/quit

Parameter

None

Default

None

Command Mode

Interface configuration mode

Example

switch(config)# router rip

switch(config-rip)# exit

5.5.6 network

Command Description

Network A.B.C.D/M

Network WORD

//Set the rip operating segments.

Parameter

Parameter	Parameters of the command mode
A.B.C.D/M	192.168.1.0/24
WORD	interface

Default

None

Command Mode

Interface configuration mode

Example

switch(config)# router rip

switch(config-rip)#network 192.168.1.0/24

5.5.7 offset-list

Command Description

offset-list <acl-name> {in | out} <metric> [<if-name>]

No offset-list <acl-name> {in | out} <metric> [<if-name>]

Parameter

Parameter	Parameters of the command mode
acl-name	Call access control list name
In| out	Call ACL application direction
Metric	Set offset by default 1, range 1-16
If-name	Application of the rules of the interface, the default all applications

Default

None

Command Mode

Interface configuration mode

Example

//The rule that calls the ACL1, the offset is set to 16 at G2 port import direction .

switch(config)# router rip

switch(config-rip)# offset-list 1 in 16 G2

5.5.8 passive-interface

Command Description

passive-interface <if-name>

//This command is to configure RIP passive-interface

No passive-interface <if-name>

//This command is disable RIP passive-interface

Parameter

None

Default

None

Command Mode

Interface configuration mode

Example

//this command is to configure vlan3 for passive-interface.

switch(config)# router rip

switch(config-rip)#passive-interface vlan3

5.5.9 redistribute

Command Description

redistribute <protocol> [metric <metric>] [route-map <route-map>]

no redistribute <protocol> [metric <metric>] [route-map <route-map>]

Parameter

Parameter	Parameters of the command mode
protocol	The routing protocols that need to be introduced into the RIP, such as IS-IS, OSPF, BGP, static, connect, etc., are introduced.
Metric	Specifies the metric value when the route is introduced
Route-map	Route-map name to be referenced when the route is introduced

Default

None

Command Mode

Interface configuration mode

Example

//The introduction of the direct route to RIP routing table, and through the route-map rule "list123" rule, the metric value of the specified route is 9.

switch(config)# router rip

switch(config-rip)#redistribute connected metric 9 route-map list123

5.5.10 timer

Command Description

timers basic <update-interval> <dead-interval> <garbage-interval>

no timers basic

//Change the time interval of the RIP periodic update packets, RIP route waiting time, RIP routing is set to not be used to completely remove the time interval from the routing table.

Parameter

Parameter	Parameters of the command mode

update-interval	RIP packet update interval , default 30S
dead-interval	RIP packet dead interval ,default 180S
garbage-interval	RIP packet garbage interval,default 120S.

Default

None

Command Mode

Interface configuration mode

Example

//The periodic update time of the configuration RIP protocol is 20 seconds, the death time is 100 seconds, garbage collection time is 60 seconds.

switch(config)# router rip

switch(config-rip)#timers basic 20 100 60

5.5.11 version

Command Description

Version

//This command is to modify the RIP version .

Parameter

None

Default

None

Command Mode

Interface configuration mode

Example

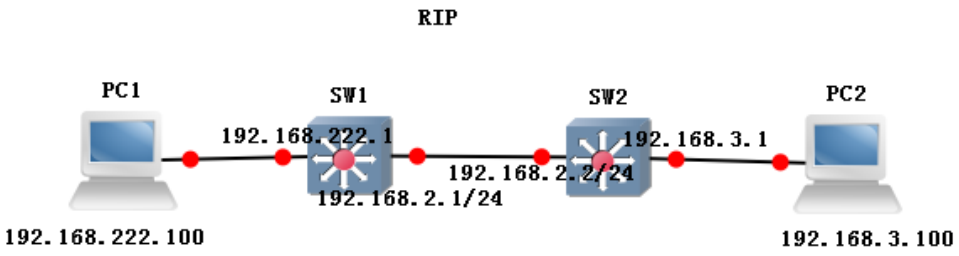
//This command is to modify the RIP version for V2

switch(config)# router rip

switch(config-rip)#version 2

5.5.12 example

Network diagram as shown in Figure:



sw1:

switch(config)#interface vlanif1

switch(config-vlanif1)# ip address 192.168.222.1/24

switch(config)#interface vlanif2

switch(config-vlanif2)# ip address 192.168.2.1/24

switch(config-vlanif2)#exit

switch(config)#interface G22

switch(config-G22)# switchport mode access

switch(config-G22)# switchport pvid 2

switch(config)# router rip

switch(config-rip)# network 192.168.2.0/24

switch(config-rip)# network 192.168.222.0/24

sw2:

switch(config)#interface vlanif3

switch(config-vlanif3)# ip address 192.168.3.1/24

switch(config-vlanif3)#exit

switch(config)#interface G23

switch(config-G23)# switchport mode access

switch(config-G23)# switchport pvid 3

switch(config)#interface vlanif2

switch(config-vlanif2)# ip address 192.168.2.2/24

switch(config-vlanif2)#exit

switch(config)#interface G22

switch(config-G22)# switchport mode access

switch(config-G22)# switchport pvid 2

switch(config)# router rip

switch(config-rip)# network 192.168.2.0/24

switch(config-rip)# network 192.168.3.0/24

phenomenon:

//Display RIP route

SW1:

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

C>* 192.168.2.0/24 is directly connected, vlanif2
R>* 192.168.3.0/24 [120/2] via 192.168.2.2, vlanif2, 00:00:55
C>* 192.168.222.0/24 is directly connected, vlanif1
```

SW2:

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

C>* 192.168.2.0/24 is directly connected, vlanif2
C>* 192.168.3.0/24 is directly connected, vlanif3
R>* 192.168.222.0/24 [120/2] via 192.168.2.1, vlanif2, 00:00:00
```

PC1 ping PC2

```
C:\Users\Administrator>ping 192.168.3.100

Pinging 192.168.3.100 with 32 bytes of data:
Reply from 192.168.3.100: bytes=32 time=1ms TTL=64
Reply from 192.168.3.100: bytes=32 time<1ms TTL=64
Reply from 192.168.3.100: bytes=32 time<1ms TTL=64
Reply from 192.168.3.100: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.3.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

6. Network security commands

6.1 Anti-attack

Anti-attack configuration commands include:

system ignore icmp-echo

system protection syn-ack

system rate-limit

Function Brief

Anti attack configuration is used to ignore the ICMP request for the purpose of this device, The defense equipment TCP SYN attack and control CPU data receiving threshold.

6.1.1 system ignore icmp-echo

Command Description

system ignore icmp-echo

no system ignore icmp-echo

//If you want to ignore the ICMP request for this device, it can be configured by this command. Use the no form of the command to cancel this configuration.

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

//Configur ignores purpose for the ICMP request of this device .

switch(config)# system ignore icmp-echo

6.1.2 system protection syn-ack

Command Description

If you want to defend against this device SYN TCP attack, you can configure this command. Use the no form of the command to cancel this

configuration.

system protection syn-ack

no system ignore icmp-echo

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

//Configur defense against this device SYN TCP attack.

switch(config)# system protection syn-ack

6.1.3 system rate-limit

Command Description

system rate-limit value

no system rate-limit

//If you want to control the CPU of the received data value, you can use this command to configure. Use the no form of the command to cancel this configuration.

Parameter

Parameter	Parameters of the command mode
value	<0-100000> pps , default 0 :disable limited.

Default

None

Command Mode

Global configuration mode

Example

//Configure the CPU data receiving threshold is 1000.

switch(config)# system rate-limit 1000

//Close the CPU data receiving threshold control function.

switch(config)# no system rate-limit

6.2 MAC binding

MAC binding configuration commands include:

mac-address static

6.2.1 mac-address static

Command Description

mac-address static mac-addr vlan vlan-id interface interface-id

//This command is used to add a static MAC address.

no mac-address static mac-addr vlan vlan-id

// This command is used to delete a static MAC address.

Parameter

Parameter	Parameters of the command mode
mac-addr	It specifies the MAC address.
vlan-id	It specifies the VLAN to which the MAC address belongs. The value ranges from **1** to **4094**.
interface-id	It specifies the physical port to which the MAC address belongs.

Default

None

Command Mode

Global configuration mode

Example

//Run the following command to bind the MAC address 00-00-00-00-00-01 to port 10 that belongs to VLAN2:

switch(config)# mac-address static 00-00-00-00-00-01 vlan 2 interface T10

6.3 ARP binding

ARP binding configuration commands include:

ip-mac bind

show ip-mac bind

Function Brief

In order to r manage the computer bette in the network, you can use the ARP binding function to control the network access (IP binding).

Note:

Because it is a private function, showing in ARP table is still dynamic item when static binding.

6.3.1 ip-mac bind

Command Description

//This command is used to enable the ip-mac banding.

ip-mac bind enable

//This command is used to disable the ip-mac banding.

ip-mac bind disable

//This command is used to enacble IP - MAC banding on the interface.

ip-mac bind enable port interface-id

//This command is used to disable IP - MAC banding on the interface.

ip-mac bind disable port interface-id

//This command is used to add a ip-mac binding.

ip-mac bind add interface-id ip-addr mac-addr

//This command is used to delete a ip-mac binding.

ip-mac bind del ip-addr

Parameter

Parameter	Parameters of the command mode
interface-id	The physical port of the MAC address.
ip-addr	Ip address
mac-addr	MAC address
enable	Global switch on
disable	Global switch off
enable port	Port opening
eisable port	Port shutdown
add	adjunction
del	delete

Default

None

Command Mode

Global configuration mode

Example

//This command is used to open the IP - MAC binding.

switch(config)# ip-mac bind enable

//This command is used to open IP - MAC binding in G2 .

switch(config)# ip-mac bind enable port G2

// Add a ip-mac binding.

switch(config)# ip-mac bind add G2 192.168.1.1 50-46-5D-E2-D5-50

6.3.2 show ip-mac bind

Command Description

//This command is used to display a IP ip-mac binding.

show ip-mac bind ip-addr

//This command is used to display the ip-mac configuration.

show ip-mac bind config

//This command is used to display the ip-mac bind.

show ip-mac bind statistics

//This command is used to display the ip-mac bind table.

show ip-mac bind table

Parameter

ip-addr	Ip address
config	Configuration
statistics	Static binding
table	list of bindin

Default

None

Command Mode

Privileged mode

Example

//This command is used to display the ip-mac bind table.

switch(config)# show ip-mac bind table

6.4 ACL config

ACL configuration commands include:

mac acl

ip acl

rule

ip/mac access-group

Function Brief

ACLs are used to filter packets based on the configured packet matching rules and processing operations. After an ACL is applied to a port, fields in each packet are analyzed. After matched packets are identified, these packets are processed according to the preset operations, such as permit, deny, rate limiting,

redirection, or port shutdown.

6.4.1 mac acl

Command Description

mac acl <1-99>

//This command is used to add an Mac-acl entry.

no mac acl <1-99>

//This command is used to delete an Mac-acl entry.

Parameter

Parameter	Parameters of the command mode
<1-99>	It specifies the ID of an MAC-ACL. The value ranges from **1** to **99**

Default

None

Command Mode

Global configuration mode

Example

switch(config)#mac acl 1

6.4.2 ip acl

Command Description

ip acl <100-999>

//This command is used to add an IP-ACL entry.

no ip acl <100-999>

//This command is used to delete an IP-ACL entry.

Parameter

Parameter	Parameters of the command mode
<100-999>	It specifies the ID of an IP-ACL. The value ranges from **100** to **999**

Default

None

Command Mode

Global configuration mode

Example

switch(config)#ip acl 100

6.4.3 rule

Command Description

rule <1-127> deny/permit <source mac> <destination mac> cos <0-7>/vlan <1-4094>/eth_type ETHTYPE

rule <1-127> deny/permit icmp/igmp/tcp/udp/ip <source ip> <destination ip> ip_pri<0-7> / tos_pri<0-15>/ dscp_pri<0-63>

//This command is used to add an ACL ACE entry.

no rulel <1-127>

//This command is used to delete an ACL ACE entry.

Parameter

Parameter	Parameters of the command mode
<1-127>	Rule number, range: 1-127
source mac	Source MAC address
destination mac	Destination MAC address,
1-4094	Vlan-id,range:1-4094
ETHTYPE	Ethernet type, range: 0x0000-0xFFFF; 0x0000 or do not fill in the representation does not match the Ethernet type field,
source ip	Source IP address
destination ip	Destination IP address,
<0-7>	Match the IP priority, range 0-7
<0-15>	Match the TOS, range 0-15
<0-63>	Match the DSCP, range 0-63

Default

None

Command Mode

Global configuration mode

Example

//This command is used to add a Mac - acl rules.

switch(config)#mac acl 1

switch(config-acl-mac)#rule 1 deny any any

6.4.4 ip/mac access-group

Command Description

ip access-group <100-999>

no ip access-group <100-999>

mac access-group <1-99>

no mac access-group <1-99>

//Using this command, you can bind the port to use the ACL rule.

Parameter

Parameter	Parameters of the command mode
<100-999>	ip acl group ID,range:100-999
<1-99>	mac acl group ID,range:1-99

Default

None

Command Mode

Interface configuration mode

Example

switch(config-G1)# ip access-group <100-999>

6.5 802.1X config

802.1X configuration commands include:

dot1x

dot1x auth-server

dot1x auth-server-type

dot1x acct-server

dot1x timer

dot1x auth-mode authorized-force/ auto/ unauthorized-force

dot1x controlled-mode based-on-mac/ based-on-port

dot1x auth

dot1x auth-user

Function Brief

802.1x was proposed by IEEE802 LAN/WAN Standards Committee to resolve the security issues of the WLAN. Later this protocol is used on the Ethernet as a common access control mechanism of LAN ports. 802.1x is mainly used to resolve the authentication and security issues on the Ethernet. It implements authentication and control on devices connected to ports of the LAN access devices.

6.5.1 dot1x

Command Description

Dot1x

//This command is used to globally enable the 802.1x .

no Dot1x

//This command is used to globally disable the 802.1x .

Parameter

None

Default

Disable

Command Mode

Global configuration mode

Example

switch(config)#dot1x

6.5.2 dot1x auth-server

Command Description

dot1x auth-server ip A.B.C.D secondary-ip A.B.C.D port<PORT> shared-secret< SECRET >

//The configuration of the authentication server IP address and IP address of the secret key and the standby server.

Parameter

Parameter	Parameters of the command mode.
A.B.C.D	Ipaddress
secondary-ip	The standby server ip address.

Default

Authentication server ip address:127.0.0.1

port number :1812

Key:radius

Command Mode

Global configuration mode

Example

switch(config)# dot1x auth-server ip 127.0.0.2 secondary-ip 127.0.0.3 port 1812 shared-secret 123

6.5.3 dot1x auth-server type

Command Description

dot1x auth-server type local/ remote

Parameter

None

Default

Remote

Command Mode

Global configuration mode

Example

switch(config)#dot1x auth-server-type local

switch(config)#dot1x auth-server-type remote

6.5.4 dot1x acct-sever

Command Description

dot1x acct-sever ip A.B.C.D secondary-ip A.B.C.D port<PORT>

shared-secret< SECRET >

//Configure the billing server IP address and the standby server IP address and secret key.

Parameter

Parameter	Parameters of the command mode.
A.B.C.D	IP address .
secondary-ip	The standby server ip address.

Default

Remote

Command Mode

Global configuration mode

Example

Switch(config)# dot1x acct-sever ip 127.0.0.2 secondary-ip 127.0.0.3 port 1812 shared-secret 123

6.5.5 dot1x timer

Command Description

dot1x timer reauth-period/quient-period value <1-65535>

//Configure authentication server update interval /hold authentication time.

Parameter

Parameter	Parameters of the command mode
value	Unit: second, range: 1-65535, aging update time
reauth-period	Authentication update interval time
quient-period	Quiet period update interval

Default

This command is to reauth-period is 3600s

Command Mode

Global configuration mode

Example

//This command is to reauth-period is 2400s.

switch(config)#Dot1x timer reauth-period 2400

switch(config)#Dot1x timer quient-period 20

6.5.6 dot1x auth-mode

Command Description

dot1x auth-mode authorized-force/ auto/ unauthorized-force

//Modify port Dot1x authentication after forced through / Auto / force no option.

Parameter

authorized-force	forced authenticating successfully
auto	automatic
unauthorized-force	forced authenticating unsuccessfully

Default

auto

Command Mode

Interface configuration mode

Example

//Configuration mandatory certification through of port1.

switch(config)#interface G1

switch(config-G1)# dot1x auth-mode authorized-force

6.5.7 dot1x controlled-mode

Command Description

dot1x controlled-mode based-on-mac/ based-on-port

//This command is used to configure based-on-mac/based-on-port 802.1x as the port authentication mode.

Parameter

based-on-mac	Authentication Based on MAC Address
based-on-port	Authentication Based on Port

Default

based-on-mac

Command Mode

Interface configuration mode

Example

//port 1 based on mac authentication .

switch(config)#interface G1

switch(config-G1)# dot1x controlled-mode based-on-mac

6.5.8 dot1x auth

Command Description

dot1x auth hold-time value<0-65535>

Parameter

value	Unit: second, range: 0-65535
hold-time	Certification aging time

Default

300S

Command Mode

Global configuration mode

Example

//The certification aging time changed to 50 seconds.

switch(config)# dot1x auth hold-time 50

6.5.9 dot1x auth-user

Command Description

dot1x auth-user *username* password *password*

//This command is to create a new user name and password.

Parameter

username	login username of switch
password	login password of switch

Default

None

Command Mode

Global configuration mode

Example

//This command to create a user called ABC password for 123 users.

switch(config)# dot1x auth-user abc password 123

6.6 Port isolation

Port isolation configuration commands include:

switchport protected

Function Brief

The port isolation function can be used to isolate ports in the same VLAN from each other. You only need to add ports to an isolation group to implement isolation of L2 data communication of different ports in the same isolation group. The port isolation function provides users with a more secure, flexible, and convenient networking solution.

6.6.1 switchport protected

Command Description

switchport protected

//This command is used to enable switchport protected.

no switchport protected

//This command is used to disable switchport protected.

Parameter

None

Default

Disable

Command Mode

Interface configuration mode

Example

//This command is used to add ports T1 to switchport protected.

switch(config)# interface T1

switch(config-T1)# switchport protected

6.7 Storm control

configuration commands include:

storm-control broadcast pps

storm-control multicast pps

storm-control unicast pps

Function Brief

Storm control means that users can limit the size of broadcast traffic that can be received on a port. When this type of traffic exceeds the preset threshold, the system drops the broadcast frames beyond the traffic limit to prevent occurrence of broadcast storms and ensure normal operation of the

network.

6.7.1 storm-control broadcast pps

Command Description

storm-control broadcast pps vlaue

//This command is used to enable the broadcast storm control function.

no storm-control broadcast

//This command is used to disable the broadcast storm control function.

Parameter

Parameter	Parameters of the command mode
Value	Range:0-1000000 unit:pps,Default: 0

Default

None

Command Mode

Interface configuration mode

Example

//This command is used to limit the rate of broadcast packet of Port 1 to 1000pps.

switch(config)# interface G1

switch(config-G1)# storm-control broadcast pps 1000

6.7.2 storm-control multicast pps

Command Description

storm-control multicast pps vlaue

//This command is used to enable the multicast storm control function.

no storm-control multicast

//This command is used to disable the multicast storm control function.

Parameter

Parameter	Parameters of the command mode
value	Range:0-1000000 unit:pps,Default: 0

Default

None

Command Mode

Interface configuration mode

Example

//This command is used to limit the rate of multicast packet of Port 1 to 1000pps.

switch(config)# interface G1

switch(config-G1)# storm-control multicast pps 1000

6.7.3 storm-control unicast pps

Command Description

storm-control unicast pps vlaue

//This command is used to enable the unicast storm control function.

no storm-control unicast

//This command is used to disable the unicast storm control function.

Parameter

Parameter	Parameters of the command mode
value	Range:0-1000000 unit:pps,Default: 0

Default

None

Command Mode

Interface configuration mode

Example

//This command is used to limit the rate of unicast packet of Port 1 to 1000pps.

switch(config)# interface G1

switch(config-G1)# storm-control unicast pps 1000

6.8 ERPS-RING config

configuration commands include:

loop-protection

loop-protection tx-time

loop-protection transmit

Function Brief

erps-ring is similar to STP, but it lacks an IEEE standard and is a private protocol. Loop protection is easy to configure and use. It is suitable for a simple ring topology and common network services, and has obvious advantages in line backup.

6.8.1 loop-protection

Command Description

loop-protection

//This command is used to enable the loop protection function.

no loop-protection

//This command is used to disable the loop protection function.

Parameter

None

Default

enable

Command Mode

Global configuration mode and interface configuration mode

Example

switch(config)# loop-protection

switch(config)# interface G1

switch(config-G1)# loop-protection

6.8.2 loop-protection tx-time

Command Description

loop-protection tx-time TIME

Parameter

Parameter	Parameters of the command mode
TIME	Unit: ms range:500-5000.

Default

500

Command Mode

Global configuration mode

Example

switch(config)# loop-protection tx-time 600

6.8.3 loop-protection transmit

Command Description

loop-protection transmit

//This command is used to enable the loop-protection transmit for a port.

no loop-protection transmit

//This command is used to disable the loop-protection transmit for a port.

Parameter

None

Default

Disable

Command Mode

Interface configuration mode

Example

switch(config)# interface G1

switch(config-G1)# loop-protection transmit

6.8.4 show loop-protection

Command Description

show loop-protection status

show loop-protection interface [NAME]

Parameter

None

Default

None

Command Mode

privilege mode

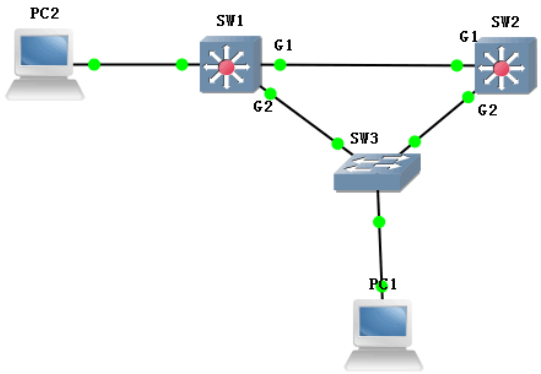
Example

switch# show loop-protection status

6.8.5 example

Three devices form a ring network (SW2 is a switch without the management function), and PC1 can communicate with PC2 normally.

When any of the other links except for the link in which the blocked port is located has a fault, the loop protection function can implement fast switching.



sw1: switch# configure terminal

switch(config)# loop-protection

switch(config)# loop-protection tx-time 600

//This command is used to globally enable the loop protection function and configure the interval.

switch(config)# interface G1

switch(config-G1)# loop-protection

switch(config-G1)# loop-protection transmit

switch(config-G1)#exit

//This command is used to enable the loop protection and loop-protect transmit for Port G1.

switch(config)# interface G2

switch(config-G2)# loop-protection

Switch(config-G2)# loop-protection transmit

//This command is used to enable the loop protection and loop-protect transmit for Port G2.

sw2: switch# configure terminal

switch(config)# loop-protection

switch(config)#loop-protection transmit-time 500

switch(config)# interface G1

switch(config-G1)# loop-protection

switch(config-G1)# loop-protection transmit

switch(config-G1)#exit

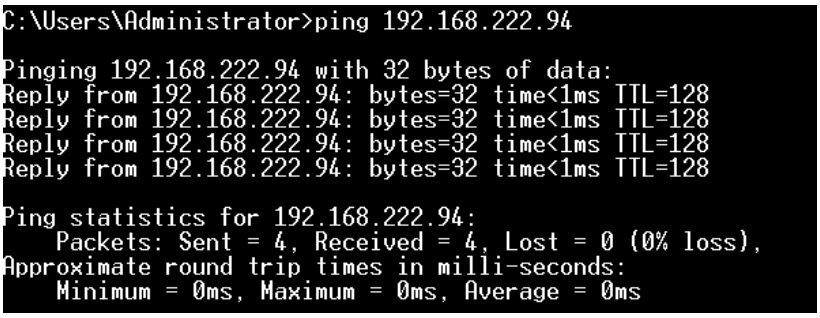
switch(config)# interface G2

switch(config-G2)# loop-protection

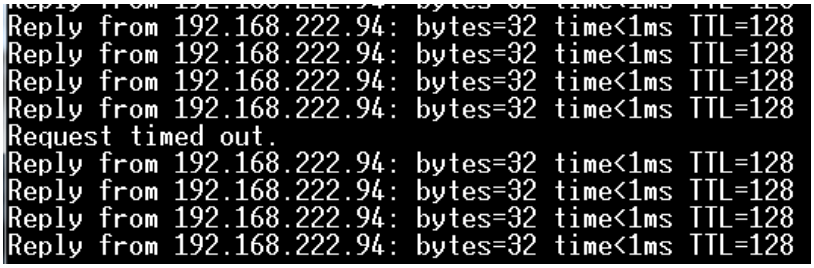
switch(config-G2)# loop-protection transmit

phenomenon:

pc1（192.168.222.107）ping pc2（192.168.222.94）



When links except for the link in which the blocked port is located are manually disconnected, the communication is interrupted in a short period of time but is restored in 5s.



Note: Among ports forming the ring network, the Tx mode of at least one port shall be enabled.

When the loop protection function is enabled to form a ring network, devices without the management function can be added into the ring network.

When a ring network is formed, blocked ports are located on the devices where loop protection is enabled.

6.9 ERPS-E config

Function Brief

Ethernet Ring Protection Switching (ERPS) is an Ethernet multi-ring protection technology defined in ITU-TG.8032. Aiming to improve network performance and security, ERPS is an Ethernet ring technology that becomes an important redundancy protection measure on the L2 network.

On the L2 network, STP is often used to ensure network reliability, and the loop protection protocol may also be used. STP is a standard ring protection protocol developed by IEEE, and has been widely used. In practice, application of STP is restricted by the network size, and the convergence time is affected by the network topology. The convergence time of STP is generally several seconds, or longer if the network diameter is large. The use of RSTP/MSTP can reduce the convergence time to several milliseconds, but still cannot meet the requirements of services (such as 3G and NGN voice services) that require a high Quality of Service (QoS). ERPS emerges to further reduce the convergence time and eliminate the impact caused by the network size.

ERPS is a link layer protocol dedicated for the Ethernet ring. It can prevent broadcast storms caused by data loops in an Ethernet ring. When a link on the Ethernet ring is disconnected, the backup link can be quickly enabled to recover communication between nodes on the ring network. Compared with STP, ERPS features a fast topology convergence speed (less than 20 ms) and the convergence time that is independent of the

number of nodes on the ring network.

6.9.1 erps

Command Description

erps

erps xx(1-24)

Parameter

None

Default

disable

Command Mode

Global configuration mode

Example

Switch(config)# erps

6.9.2 erps xx

Command Description

erps xx erps groupprimary PORT(A) slave PORT(B) role master vid VLAN wtr-time TIME guard-time GUARD-TIME

Parameter

Parameter	Parameters of the command mode
XX	1-24
PORT(A)	any port
PORT(B)	In addition to the above fill in the port
VLAN	1-4094, Default 3001
Wtr-TIME	1-12min ,When the RPL has a node that receives the first R-APS (NR) message, the WTR timer is started.
GUARD-TIME	100-2000ms,The default is 500ms, failure of adjacent nodes to detect the fault recovery time to start the warning time timer, so that the fault is connected to the port to continue to maintain the blocking state

Default

None

Command Mode

Global configuration mode

Example

//Configure the G1-G2 port to the ERPs group 3, and the use of vlan3001 communication protocol packet WTR time is 1min, the warning time is 500s

switch(config)# erps 3 primary G1 slave G2 role master vid 3001 wtr-time 1 guard-time 500

6.9.3 show erps

Command Description

show erps

show erps [erps ring id]

Parameter

erps ring id [rang 1-24]

Default

none

Command Mode

privilege mode

Example

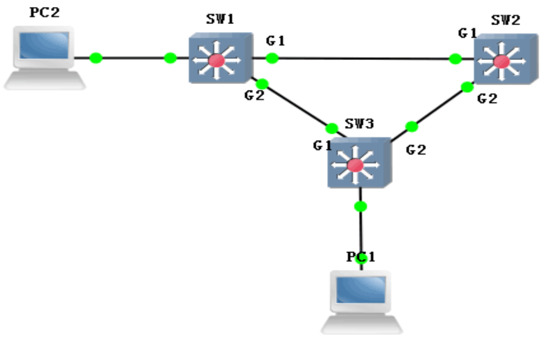
switch# show erps

6.9.4 example

Three devices group an ERPS ring. Port 0 on SW1 is configured to the owner port (it controls the forwarding state; that is, the port is blocked when there is a loop).

When there is a loop, PC1 and PC2 can communicate with each other normally.

When any of the other links except for the link in which the blocked port is located has a fault, ERPS can implement fast switching.



sw1:

switch(config)#erps 1 primary G1 slave G2 role master vid 3001 wtr-time 1 guard-time 500

sw2/sw3:

switch(config)#erps 1 primary G1 slave G2 role transit vid 3001 wtr-time 1 guard-time 500

phenomenon:

G1 of SW1 is blocked.

pc1（192.168.222.107） ping pc2（192.168.222.95）

```
Reply from 192.168.222.95: bytes=32 time<1ms TTL=64
Reply from 192.168.222.95: bytes=32 time<1ms TTL=64
Reply from 192.168.222.95: bytes=32 time<1ms TTL=64
Reply from 192.168.222.95: bytes=32 time<1ms TTL=64
Reply from 192.168.222.95: bytes=32 time<1ms TTL=64
Reply from 192.168.222.95: bytes=32 time<1ms TTL=64
Reply from 192.168.222.95: bytes=32 time<1ms TTL=64
Reply from 192.168.222.95: bytes=32 time<1ms TTL=64
Reply from 192.168.222.95: bytes=32 time<1ms TTL=64
```

When any of the other links except for the link in which the blocked port is located is disconnected manually, fast switching is implemented without interrupting the ping process.

```
Reply from 192.168.222.95: bytes=32 time<1ms TTL=64
Reply from 192.168.222.95: bytes=32 time<1ms TTL=64
Reply from 192.168.222.95: bytes=32 time<1ms TTL=64
Reply from 192.168.222.95: bytes=32 time<1ms TTL=64
Reply from 192.168.222.95: bytes=32 time<1ms TTL=64
Reply from 192.168.222.95: bytes=32 time<1ms TTL=64
Reply from 192.168.222.95: bytes=32 time<1ms TTL=64
Reply from 192.168.222.95: bytes=32 time<1ms TTL=64
Reply from 192.168.222.95: bytes=32 time<1ms TTL=64
Reply from 192.168.222.95: bytes=32 time<1ms TTL=64
Reply from 192.168.222.95: bytes=32 time<1ms TTL=64
Reply from 192.168.222.95: bytes=32 time<1ms TTL=64
Reply from 192.168.222.95: bytes=32 time<1ms TTL=64
Reply from 192.168.222.95: bytes=32 time<1ms TTL=64
Reply from 192.168.222.95: bytes=32 time<1ms TTL=64
Reply from 192.168.222.95: bytes=32 time<1ms TTL=64
Reply from 192.168.222.95: bytes=32 time<1ms TTL=64
Reply from 192.168.222.95: bytes=32 time<1ms TTL=64
```

6.10 IP source guard

IP source guard commands include:

ip source-guard

ip source-guard trust<0/1/2/3>

ip dhcp-snooping binding

Function Brief

The IP source guard function can be used to filter packets forwarded by a port, thus preventing invalid packets from passing through the port, restricting unauthorized use of network resources (for example, unauthorized hosts may access the network by forging IP addresses of authorized users), and improving the port security.

If IP source guard is enabled on a port of the switch, when packets reach this port, the switch checks the IP source guard entries. If the packet matches an entry, the switch forwards the packet or the packet enters the subsequent flow. If the packet does not match any entry, the switch drops the packet. The binding function is port-based. After a port is bound, only this port is affected by the binding relationship, and other ports are not affected.

6.10.1 ip source-guard

Command Description

ip source-guard

//This command is used to enable the IP source guard function.

no ip source-guard

//This command is used to disable the IP source guard function.

Parameter

None

Default

Disable

Command Mode

Global configuration mode

Example

switch(config)#Ip source-guard

6.10.2 ip source-guard trust

Command Description

ip source-guard trust<0/1/2/3>

no ip ip source-guard trust

Parameter

Parameter	Parameters of the command mode
0/1/2/3	It specifies the number of dynamic clients. The value ranges from **0** to **2**.

Default

Unlimited

Command Mode

Interface configuration mode

Example

switch(config)# interface G1

switch(config-G1)#ip source-guard trust 1

6.10.3 ip dhcp-snooping binding

Command Description

ip dhcp-snooping binding <MAC> vlan <VLANID> ip <A.B.C.D> mask <Msak> interface < IFNAME>

no ip dhcp-snooping binding <MAC> vlan <VLANID> ip <A.B.C.D> interface < IFNAME>

Parameter

Parameter	Parameters of the command mode
MAC	the MAC address of Static binding
VLANID	the VLAN ID of Static binding
A.B.C.D	the IP address of Static binding
Msak	the mask address of Static binding
IFNAME	port number

Default

Unlimited

Command Mode

Interface configuration mode

Example

switch(config)#ip dhcp-snooping binding 40-50-11-11-11-11 vlan 1

ip 192.168.1.1 mask 255.255.255.0 interface G1

6.10.4 show ip source-guard

Command Description

show ip source-guard leases

Parameter

none

Default

none

Command Mode

Privilege mode and global mode

Example

switch# show ip source-guard leases

7. Network management commands

7.1 HTTP config

HTTP configuration commands include:

ip http-server http

ip http-server https

Function Brief

Describe the HTTP configuration command. This command can configure the switch to accept the HTTP/HTTPS service request at the specified port, processing the request and return the results to the browser.

7.1.1 ip http-server http

Command Description

ip http-server http

//This command is used to enable the HTTP on the switch.

no ip http-server

//This command is used to disable the HTTP on the switch.After this command is executed, the switch cannot be managed in HTTP mode.

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

//Enable the HTTP service.

switch(config)# ip http-server http

7.1.2 ip http-server https

Command Description

ip http-server https

//This command is used to enable the HTTP service on the switch.

no ip http-server

//This command is used to disable the HTTP service on the switch. After this command is executed, the switch cannot be managed in HTTP mode.

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

//Enable the HTTP service.

switch(config)# ip http-server https

7.2 SNMP config

SNMP configuration commands include:

community
syscontact
syslocation
sysname
trap
trap2sink
trapsink
user

Function Brief

SNMP is a set of network management standards. It includes an application layer protocol, a database schema, and a set of data objects. It is widely used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. It is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF).

7.2.1 snmp

Command Description

snmp

// This command is used to enable the SNMP function.

no snmp

//This command is used to disable the SNMP function.

Parameter

None

Default

Enable

Command Mode

Global configuration mode

Example

//Enable the SNMP function of the switch.

switch(config)# snmp

7.2.2 snmp-server trap2sink

Command Description

snmp-server trap2sink ip

//This command is used to configure the SNMP version.

snmp-server trapsink ip

//This command is used to restore the default SNMP version.

Parameter

None

Default

snmp

Command Mode

Global configuration mode

Example

//Configure the SNMP version of the switch.

switch(config)# snmp-server trap2sink 192.168.1.1

7.2.3 snmp-server trap

Command Description

snmp-server trap

//This command is used to enable snmp trap.

no snmp-server trap

//This command is used to disable snmp trap.

Parameter

None

Default

Disable

Command Mode

Global configuration mode

Example

switch(config)# snmp-server trap

7.2.4 snmp-server community

Command Description

community

// The command is used to configure the authentication name and permission.

Parameter

ro: read only

rw: read and write

Default

public

Command Mode

Global configuration mode

Example

//This command is used to configure a switch.

switch(config)#snmp-server community ro 111

//The authentication name is 123 and the permission is read only.

7.2.5 snmp host

Command Description

snmp-server sysname

//This command is used to configure the host name.

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

switch(config)#snmp-server sysname 1111

// It indicates that the host name is 1111.

7.2.6 snmp-server user

Command Description

snmp-server

Parameter

None

Default

None

Command Mode

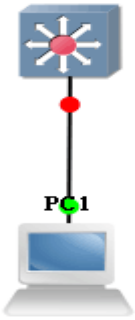
Global configuration mode

Example

switch(config)#snmp-server user ro 111

7.2.7 example

SNMP is enabled on the switch and PC1 is installed with MIB Browser to obtain the switch node information.



sw: switch(config)# snmp-server

switch(config)#snmp-server community ro 123

switch(config)#snmp-server community rw 123

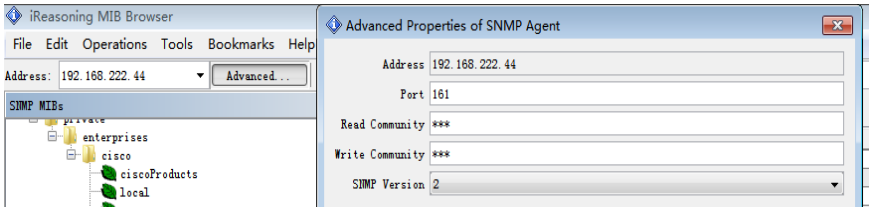
// This command is used to configure the SNMP version and read/write community.

switch(config)# snmp-server trap enable

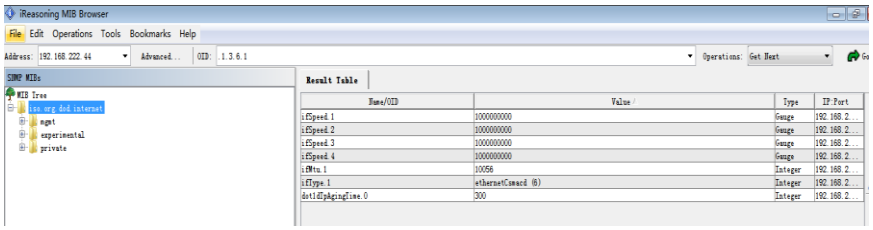
switch(config)# snmp-server trap2sink 192.168.222.107

// This command is used to configure SNMP trap information.

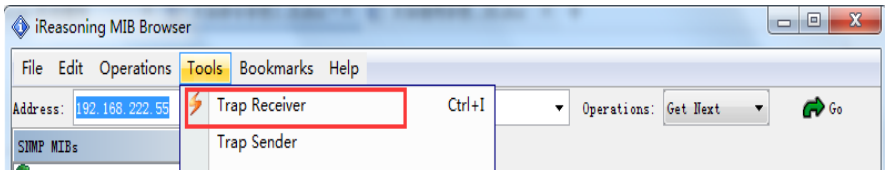
pc:Open MIB Browser on the PC and add the switch IP address and corresponding community name.



Right-click iso.org.dod.internet, and choose Work, as shown in the following figure. Related information is displayed.



Click Trap Receiver under Tools to display uploaded trap information.



8. System maintenance commands

8.1 Reboot

Function Brief

This chapter describes the device restart commands.Please pay attention to the configuration save operation Before using this command.

8.1.1 reboot

Command Description

reboot

// This command is used to restart the equipment.

Parameter

None

Default

None

Command Mode

Privileged mode

Example

switch# write

switch# reboot

//Run the following commands to save the configuration, and then restart the equipment.

8.2 Restore factory

The command for restoring factory settings is as follows:

default configure

default configure keep-ip

Function Brief

This chapter describes the recovery of the factory configuration command. This command can be used to restore the factory configuration, the configuration will be returned to the default value.

8.2.1 default configure

Command Description

default configure

//This command is used to restore factory settings of the switch. After this command is executed, the equipment automatically restarts and the factory settings are successfully restored.

Parameter

None

Default

None

Command Mode

Privileged mode

Example

//Restore factory settings, and the factory settings take effect after the equipment automatically restarts.

switch# default configure

8.3 Config management

Function Brief

This chapter describes the configuration file save command. This command can save the configuration.

Use commands of this chapter to configure the example, please read the final sample section of the document.

8.3.1 write

Command Description

write

//If you want to save the configuration of the switch, you can configure it through this command.

Parameter

None

Default

None

Command Mode

Privileged mode

Example

//Save the switch configuration.

switch# write

8.4 PING test

Function Brief

Like the ping command on a common PC, the PING diagnose function is used to test connectivity between two nodes on the network. The difference between the ping command and PING diagnose is as follows: The ping command executed between two common PCs is used to check whether the physical connection between the two PCs is normal. The PING diagnose function of the switch helps the network administrator test whether a network device is disconnected on a LAN and locate network faults based on the test result.

8.4.1 ping

Command Description

ping ip

//Test whether the switch and the host are reachable from each other.

Parameter

None

Default

None

Command Mode

Privileged mode

Example

//Test whether the switch and the host are reachable from each other.

switch# ping 192.168.1.100