L2+ Manage Switch

CLI Configuration Manual

(Applicable to DH-PFS5924-24X and DH-PFS5424-24T)

Document No.: 20150422-L2+ Manage switch_V 4.2.2

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 GigabitEthernet 1/1

switch(config-if)# exit

switch(config)#

// This command is used to enter the G1/1 interface mode from the global mode, and the **exit** command is used to exit the interface mode.

switch(config)# interface vlan 1

switch(config-if-vlan)# 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 Description

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

```
Username: admin
Password:
DH-PFS5424-24T# show ver

MEMORY           : Total=80594 KBytes, Free=55292 KBytes, Max=55289 KBytes
FLASH            : 0x40000000-0x40ffffff, 64 x 0x40000 blocks
MAC Address      : ac-31-9d-0c-d0-81
Previous Restart : Cool
Software Version : V1.0.0-R2
Hardware Version : V1.2

System Contact   :
System Name      : DH-PFS5424-24T
System Location  :
System Time      : 1970-01-01 00:06:00+00:00
System Uptime    : 00:06:00
```

1.2.2 show sys-time

Command Description

This command is used to display the current system time.

Parameter

None

Default

None

Command Mode

Privileged mode

Example

switch# show sys-time

```
DH-PFS5424-24T# show sys-time
2015-12-29 11:17:46
```

1.3 System Log

Function Description

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

<cr>	It is used to display all logs.
<logging_id: 1-4294967295>	It is used to display a log with a specified ID.
error	It is used to display logs of the error level.
info	It is used to display logs of the info level.
warning	It is used to display logs of the warning level.

Default

None

Command Mode

Privileged mode

Example

switch#show logging

1.4 Port Statistics

Function Description

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. If a port has too many error packets, the working status of the port is poor. You shall check whether the cable or peer device to which the port is connected has any problem.

1.4.1 show interface

Command Description

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

Parameter

*	statistics	It is used to display data statistics of all ports.
	status	It is used to display the status of all ports.
	veriphy	It is used to perform line diagnosis and display the results.
	switchport	It is used to display all port modes, including access, hybrid and trunk.
GigabitEthernet<port_type>	statistics | status | switchport	It is used to display data statistics, port status and port mode of a gigabit port.
XGigabitEthernet<port_type>	statistics | status | switchport	It is used to display data statistics, port status and port mode of a 10-gigabit port.
vlan<vlan_list>	It is used to display information about a specified VLAN.	

PORT_LIST: port list, which can be provided in such a format as "1/1-48", "1/1", or "1/1-2,3,5-8".

Default

None

Command Mode

Privileged mode

Example

switch# show interface * statistics

switch# show interface GigabitEthernet 1/1 statistics

switch# show interface GigabitEthernet 1/1-3,28-32 statistics

switch# show interface XGigabitEthernet 1/1-2 statistics

switch# show interface vlan 1

//Display the packet statistics of port 1 and port 2.

1.5 Detailed Statistics

Function Description

This function module is used to display the detailed information of each port, including the number of packets, broadcast packets and error packets (including dropped packets, CRC error packets, packets with small frames, packets with jumbo frames, and filtered packets). The information facilitates network maintenance of the network management personnel.

1.5.1 show interface

Command Description

This command is used to display detailed statistics of the port packets.

switch# show interface GigabitEthernet +port+ statistic +Parameter

Parameter

|	begin	<64、65-127、128-255、256-511 、 512-1023 、1024-1526、1527->	It is used to display statistics of packets of all bytes starting from the key character.
	exclude	<64、65-127、128-255、256-511 、 512-1023 、1024-1526、1527->	It is used to display statistics of packets of all bytes excluding the key character.
	include	<64、65-127、128-255、256-511 、 512-1023 、1024-1526、1527->	It is used to display statistics of packets containing the key character.
bytes			It is used to display statistics of port packets in bytes.
discards			It is used to display the number of packets dropped by the port.
down/up			It is used to display the port status (down or up).
errors/filtered			It is used to display the error frames and filtered

			frames of the port.
packages			It is used to display statistics of port packets.
priority			It is used to display the port priority.

Default

None

Command Mode

Privileged mode

Example

switch# show interface GigabitEthernet 1/1 statistics | begin 5

// This command is used to display statistics of packets of all bytes after the byte containing the key character 5.

```
DH-PFS5424-24T# show interface GigabitEthernet 1/1 statistics | begin 65
Rx 65-127:                              0    Tx 65-127:                              0
Rx 128-255:                             0    Tx 128-255:                             0
Rx 256-511:                             0    Tx 256-511:                             0
Rx 512-1023:                            0    Tx 512-1023:                            0
Rx 1024-1526:                           0    Tx 1024-1526:                           0
Rx 1527-    :                           0    Tx 1527-    :                           0

Rx Drops:                               0    Tx Drops:                               0
Rx CRC/Alignment:                       0    Tx Late/Exc. Coll.:                     0
Rx Undersize:                           0
Rx Oversize:                            0
Rx Filtered:                            0
```

switch# show interface GigabitEthernet 1/1 statistics | exclude 4

// This command is used to display statistics of packets of bytes excluding the byte containing the key character 4.

```
DH-PFS5424-24T# $how interface GigabitEthernet 1/1 statistics | exclude 4

GigabitEthernet 1/1 Statistics:
Rx Packets:                             0   Tx Packets:                             0
Rx Octets:                              0   Tx Octets:                              0
Rx Unicast:                             0   Tx Unicast:                             0
Rx Multicast:                           0   Tx Multicast:                           0
Rx Broadcast:                           0   Tx Broadcast:                           0
Rx Pause:                               0   Tx Pause:                               0

Rx 65-127:                              0   Tx 65-127:                              0
Rx 128-255:                             0   Tx 128-255:                             0
Rx 256-511:                             0   Tx 256-511:                             0
Rx 512-1023:                            0   Tx 512-1023:                            0
Rx 1527-    :                           0   Tx 1527-    :                           0

Rx Drops:                               0   Tx Drops:                               0
Rx CRC/Alignment:                       0   Tx Late/Exc. Coll.:                     0
Rx Undersize:                           0
Rx Oversize:                            0
Rx Filtered:                            0
```

switch# show interface GigabitEthernet 1/1 statistics | include 5

// This command is used to display statistics of packets of all bytes including the byte containing the key character 5.

```
DH-PFS5424-24T# $how interface GigabitEthernet 1/1 statistics | include 5
Rx 65-127:                              0   Tx 65-127:                              0
Rx 128-255:                             0   Tx 128-255:                             0
Rx 256-511:                             0   Tx 256-511:                             0
Rx 512-1023:                            0   Tx 512-1023:                            0
Rx 1024-1526:                           0   Tx 1024-1526:                           0
Rx 1527-    :                           0   Tx 1527-    :                           0
```

switch# show interface GigabitEthernet 1/1 statistics errors

// This command is used to display statistics of error frames on Port 1.

switch# show interface GigabitEthernet 1/1 statistics packets

// This command is used to display statistics of packets on Port 1.

1.6 ACL Statistics

Function Description

This function module is used to display statistics of function modules of the switch ACL.

1.6.1 show access-list ace-status

Command Description

This command is used to display the ACL rule.

Parameter

|<begin/exclude/include>	It is used to output results satisfying the filtering conditions.
arp-inspection	It is used to display configurations of

	the ARP inspection module.
conflicts	It is used to display hardware-caused rule conflicts.
dhcp	It is used to display configurations of the DHCP module.
ip-source-guard	It is used to display configurations of the source IP protection module.
ipmc	It is used to display configurations of the IPMC module.
loop-protect	It is used to display the loop protection configuration module.
mep	It is used to display ACE sentence related to information transmission methods.
static	It is used to display configurations manually added by a user.
upnp	It is used to display configurations of general and plug-in protocol modules.

Default

None

Command Mode

Privileged mode

Example

switch# show access-list ace-status

1.7 LACP Status

Function Description

This function module is used to display the LACP port configurations, LACP neighbor information, LACP statistics, LACP system priority.

1.7.1 show lacp neighbor

Command Description

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

Parameter

internal	It is used to display the LACP port configurations.
neighbour	It is used to display the LACP neighbor information.
statistics	It is used to display the LACP statistics.
system-id	It is used to display the LACP system priority.

Default

None

Command Mode

Privileged mode

Example

switch#show lacp neighbor

switch# show lacp internal

1.8 Showing STP Status

Function Description

This function module is used to display the STP bridge and port information, STP active ports, STP packet statistics, STP configurations, STP summary.

1.8.1 show spanning-tree

Command Description

This command is used to display the status of the spanning tree.

Parameter

<cr>	It is used to display the STP bridge and port information.
active	It is used to display STP active ports.
detailed	It is used to display STP packet statistics.
Interface	It is used to display the STP status of a port.
mst	It is used to display STP configurations.
summary	It is used to display the STP summary.

Default

None

Command Mode

Privileged mode

Example

switch#show spanning-tree

switch#show spanning-tree interface GigabitEthernet 1/45

1.9 LLDP Neighbors

Function Description

This module is used to display neighbor information, including the peer port, system name, port description, system performance, and management IP address, or to display the LLDP packet statistics.

1.9.1 show lldp

Command Description

This command is used to display LLDP information, including the neighbor information and packet statistics.

Parameter

neighbors	<cr>	It is used to display the LLDP neighbor information.
	interface	It is used to display the neighbor information learnt from a specific port.
statistics	<cr>	It is used to display the LLDP packet statistics.
	interface	It is used to display the LLDP packet statistics of a specific port.

Default

None

Command Mode

Privileged mode

Example

switch#show lldp neighbors

switch#show lldp statistics

1.10 L2 Forwarding Table

Function Description

This module is used to display all L2 MAC address forwarding tables, type, port, MAC address, and VLANs on a switch.

1.10.1 show mac address-table

Command Description

This command is used to display the L2 forwarding table.

Parameter

<cr>	It is used to display the L2 forwarding table.
address <mac_addr>	It is used to display the forwarding table of a specific mac address.
aging-time	It is used to display the aging time of a L2 forwarding table.
conf	It is used to display the static L2 forwarding table added by the user.
count	It is used to display the statistics of entries in the L2 forwarding table.
interface	It is used to display the entries in the L2 forwarding table under a specific port.
learning	It is used to display the L2 forwarding table learning status of each port. Aotu：It is used to automatically learning the MAC address into the L2 forwarding table. Disabled：It means MAC address learning is disabled. Secure：It means that adding static MAC address is allowed but dynamic learning is not allowed.
static	It is used to display the L2 forwarding table under a certain VLAN.

Default

None

Command Mode

Privileged mode

Example

switch#show mac address-table

switch#show mac address-table static

switch#show mac address-table count

switch#show mac address-table learning

switch#show mac address-table interface GigabitEthernet 1/45

switch#show mac address-table vlan 1

2 System Setting Commands

2.1 IP Address Configuration

IP address configuration commands include:

- show ip interface brief
- ip address

Function Description

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

2.1.1 show ip interface brief

Command Description

This command is used to display the IP configuration of a port. You can use the command to display the IP configuration of a network interface or a VLAN.

Parameter

None

Default

Enabled port

Command Mode

Privileged mode

Example

switch#show ip interface brief

switch#show interface vlan 1

2.1.2 Ip address

Command Description

ip address <address> <netmask>

This command is used to configure the management interface IP address of switch.

DHCP	It is used to automatically obtain the IP information.
<address>	It is used to display the IP address of the VLAN port.
<netmask>	It is used to display the subnet mask.

Default

VLAN 1 interface

Command Mode

VLAN interface configuration mode

Example

//This command is used to modify the switch management IP:

switch (config)# interface vlan 1

switch (config-if-vlan)# ip address 192.168.1.1 255.255.255.0

switch# copy running-config startup-config

// You shall save the configuration after modifying the IP.

2.2 Log Configuration

Log configuration commands include:

- logging on
- logging host
- logging level

Function Description

This function module is used to upload switch logs onto a remote log server.

2.2.1 logging on

Command Description

logging on: This command is used to enable the log server mode.

no logging on: This command is used to disable the log server mode.

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

switch(config)#logging on

switch(config)#no logging on

2.2.2 logging host

Command Description

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

Parameter

Hostname //Domain name or IP address of the log server

Default

None

Command Mode

Global configuration mode

Example

switch(config)#logging host 192.168.0.1

2.2.3 logging level

Command Description

This command is used to configure the levels of logs uploaded to the log server.

Parameter

Error | warning | info

Default

None

Command Mode

Global configuration mode

Example

switch(config)#logging level error

2.3 User Configuration

User configuration commands include:

username *name*

show user

Note: **name** indicates the user name, which is a string of 1 to 18 characters. **password** indicates the password, which is a string of 1 to 18 characters.

Function Description

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

2.3.1 username name

Command Description

username *name* privilege *level* password none|encrypted|unencrypted *password*: 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.

level indicates the user level, which ranges from 1 (lowest management rights) to 15 (highest management rights).

no username name: This command is used to delete an existing user.

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

switch(config)# username test privilege 15 password encrypted test

//Add a user "test", whose password is **test** and rights is the highest management. The password is encrypted.

switch(config)#no username test

2.3.2 show users

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 users

switch#show running-config //This command can also be used to display all the user accounts.

2.4 NTP Configuration

NTP configuration commands include:

- ntp

- ntp server

Function Description

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

2.4.1 ntp

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

None

Command Mode

Global configuration mode

Example

switch(config)# ntp

2.4.2 ntp server

Command Description

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

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

switch(config)# ntp server 1 ip-address 202.120.2.101 time-zone 8

// This command is used to set the IP address and time zone of the NTP server.

2.5 System time Setting

Function Description

You can manually set the current system time of the switch.

2.5.1 sys-time

Command Description

This command is used to set the system time of the switch.

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

switch(config)# sys-time 2015-01-02 11:11:11

3 Port Configuration Commands

3.1 Port Configuration

Port configuration commands include:

- duplex
- speed
- flowcontrol
- shutdown
- mtu

Note: You can configure multiple ports simultaneously. When finished, the configurations are simultaneously distributed to all ports in this list. Ports can be listed in such forms as 1/1-48 and 1/1-2, 3, 5-8.

Function Description

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. Unless otherwise specified, do not modify the port rate mode; otherwise, port communication fails if the configured port rate mode is different from the actual port rate mode.

Note: you can configure multiple ports simultaneously.

Parameter

auto	Auto 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

Example

switch (config)# interface GigabitEthernet 1/1-3

switch (config-if)# duplex full

switch (config-if)# no duplex full

// This command is used to modify the duplex mode of the G1-G3 ports.

switch (config)# interface GigabitEthernet 1/4

switch (config-if)# duplex full

switch (config-if)# no duplex full

// This command is used to modify the duplex mode of the G4 port.

3.1.2 speed

Command Description

Electrical port: speed {10 | 100 | 1000 | 1000 | auto }，It is used to set the port rate.

Optical port: speed {100 | 1000 | auto }，

Duplex port: speed {Auto: 1000-X-AMS Electrical port: 10 | 100 | 1000 | 1000 | auto Optical port: 1000-X }

10-gigabit optical port: speed { 10000 }

Parameter

Electrical port	10 | 100 | 1000 | 10000	The port rate is set to 10M, 100M and 1000M.
	Auto	The port rate is set to Auto.
Optical port	100 | 1000 | auto	The port rate is set to 100M (full) or 1000M (full).
	Auto	The port rate is set to Auto.
Duplex	1000-X-AMS	The port mode is set to electrical-optical Auto

port		(the optical port has a priority higher than the electrical port).
	10 | 100 | 1000 | 1000 | auto	The port mode is set to electrical port and the port rate is set to 10M, 100M, 1000M and Auto.
	1000-X	The port mode is set to optical mode and the port rate is set to 1000M.
10-gigabit optical port	10000	The port rate is set to 10000M.

Default

By default, the speed mode is set to **auto** for an electric port, **auto** for a gigabit optical port, and **10000M** for a 10-gigabit optical port.

Command Mode

Interface configuration mode

Example

switch (config)# interface GigabitEthernet 1/1

switch (config-if)# speed 100

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

switch (config)#interface GigabitEthernet 1/17-19

switch (config-if)# speed 1000-x

// This command is used to set the duplex ports G17-19 to optical ports.

3.1.3 flowcontrol

Command Description

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

Parameter

None

Default

The flow control function is disabled by default. A gigabit optical port does not support configuration of the flow control function.

Command Mode

Interface configuration mode

Example

switch # configure terminal

switch (config)# interface GigabitEthernet 1/1

switch (config-if)# flowcontrol on

switch (config-if)# flowcontrol off

3.1.4 mtu

Command Description

This command is used to configure the maximum frame length allowed by a port (the page displays the frame having the maximum length).

Parameter

<1518-10056>

Default

10056

Command Mode

Interface configuration mode

Example

switch (config)# interface GigabitEthernet 1/1

switch (config-if)# mtu 1518

3.1.5 shutdown

Command Description

shutdown: This command is used to disable a port.

no shutdown: This command is used to enable a port.

Parameter

None

Default

The port is enabled by default.

Command Mode

Interface configuration mode

Example

switch (config)# interface GigabitEthernet 1/1

switch (config-if)# no shutdown

3.2 Port Mirroring

Port Mirroring commands include:

- monitor destination
- monitor source

Function Description

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.

3.2.1 Monitor destination

Command Description

monitor destination: This command is used to enable the monitor destination port.

no monitor destination: This command is used to disable the monitor destination port.

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

switch(config)# monitor destination interface GigabitEthernet 1/1

switch(config)# no monitor destination

3.2.2 Monitor source

Command Description

monitor source: This command is used to configure the monitor source port.

no monitor source interface GigabitEthernet 1/2: This command is used to cancel the configuration of the monitor source port.

Parameter

monitor source {{interface (<port_type> [<v_port_type_list>])} | {{both | rx | tx}

port_type: It is set to **GigabitEthernet** or **XGigabitEthernet**.

Mirroring direction:

Both	It is used to mirror both outgoing and incoming packets of the source port to the destination port.
rx	It is used to mirror incoming packets of the source port to the destination port.
tx	It is used to mirror outgoing packets of the source port to the destination port.

Default

None

Command Mode

Global configuration mode

Example

switch(config)# monitor source interface GigabitEthernet 1/2 both

switch(config)# no monitor source interface GigabitEthernet 1/2

3.3 Port Speed limit

Function Description

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.

3.3.1 qos policer

Command Description

qos policer: It is used to configure port bandwidth limiting policy and set the rate limit value of each port.

Parameter

<Rate : 100-13200000> fbs

Default

None

Command Mode

Interface configuration mode

Example

switch (config) # interface GigabitEthernet 1/1

switch (config-if-ge1)# qos policer 1000

// The command is used to set the port rate limit value to 1000fps.

4 Advanced Configuration Commands

4.1 Link Aggregation

Static aggregation configuration commands include:

- aggregation mode
- aggregation group

Dynamic aggregation configuration commands include:

- lacp
- lacp key
- lacp port-priority
- lacp role
- lacp timeout

Function Description

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.

4.1.1 aggregation mode

Command Description

aggregation mode {ip | smac | dmac | smac dmac | port}: This command is used to configure the load balancing algorithm of an aggregation group.

no aggregation mode: This command is used to restore the default load balancing algorithm of an aggregation group.

Parameter

ip	Load balancing is based on the IP address.
smac	Load balancing is based on the source MAC address.
dmac	Load balancing is based on the destination MAC address.
smac dmac	Load balancing is based on the source and destination MAC addresses.
port	Load balancing is based on the TCP/UDP port number.

Default

By default, load balancing is based on the IP address.

Command Mode

Global configuration mode

Example

switch(config)# aggregation mode smac dmac

4.1.2 aggregation group

Command Description

aggregation group *group-id*: This command is used to add a port to an aggregation group.

no aggregation group: This command is used to delete the static aggregation configuration of a specified group.

Parameter

group-id specifies the ID of the aggregation group.

Default

None

Command Mode

Interface configuration mode

Example

switch(config)# interface GigabitEthernet 1/1-8

switch(config-if)# aggregation group 2

switch(config-if)# no aggregation group

4.1.3 lacp

Command Description

lacp: This command is used to enable dynamic aggregation of ports.

no lacp: This command is used to disable dynamic aggregation of ports.

Parameter

None

Default

None

Command Mode

Interface configuration mode

Example

switch(config)# interface GigabitEthernet 1/1-4

switch(config)# lacp

switch(config)# no lacp

4.1.4 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 GigabitEthernet 1/1

switch(config-if)# lacp key 100

4.1.5 lacp port-priority

Command Description

lacp port-priority ***<1-65535>****:* This command is used to configure the priority of an LACP port.

Parameter

<1-65535>: It specifies the priority range. A smaller value indicates a higher priority.

Default

None

Command Mode

Interface configuration mode

Example

switch(config)# interface GigabitEthernet 1/1

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

4.1.6 lacp role

Command Description

lacp role ***active*** **|** ***passive***: This command is used to configure the role of an LACP port.

Parameter

active | *passive*: It specifies the role of a port, which is **active** or **passive**.

Default

active

Command Mode

Interface configuration mode

Example

switch(config)# interface GigabitEthernet 1/1

switch(config-if)#lacp role active

switch(config-if)#lacp role passive

4.1.7 lacp timeout

Command Description

Lacp timeout fast | slow: This command is used to configure the timeout type of LACP.

Parameter

fast	The timeout type is fast. That is, one LACP packet is sent each second.
slow	The timeout type is slow. That is, one LACP packet is sent each 30 seconds.

Default

fast

Command Mode

Interface configuration mode

Example

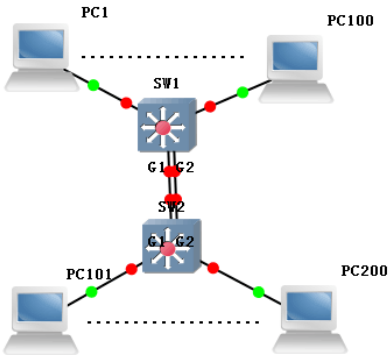
switch(config)# interface GigabitEthernet 1/5

switch(config-if)# lacp timeout fast

switch(config-if)# lacp timeout slow

Link Aggregation Configuration 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)# aggregation mode smac dmac

switch(config)# interface GigabitEthernet 1/1

switch(config-if)# aggregation group 1

switch(config-if)# exit

switch(config)# interface GigabitEthernet 1/2

switch(config-if)# aggregation group 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.

4.2 VLAN Management

VLAN configuration commands include:

- vlan
- name
- switchport mode

- switchport access vlan
- switchport forbidden vlan
- Switchport hybrid acceptable-frame-type
- Switchport hybrid native
- Switchport hybrid egress-tag
- show vlan

Function Description

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.

4.2.1 Vlan

Command Description

vlan {vlan_list}: This command is used to add a VLAN.

no vlan: This command is used to delete a vlan.

Parameter

<vlan_list>: It specifies the VLAN ID, which ranges from **1** to **4095**. The value **4095** is reserved.

Default

vlan 1 (By default, all the ports belong to vlan 1.)

Command Mode

Global configuration mode

Example

switch(config)#vlan 2-3,6,9 //Add four VLANs, including VLANs 2, 3, 6, and 9.

switch(config)#no vlan 6,9 //Delete VLANs 2 and 9.

4.2.2 Name

Command Description

Name <vword32>: This command is used to configure the name of a VLAN.

Parameter

<vword32>: It specifies the name of the VLAN.

Default

default

Command Mode

VLAN configuration mode

Example

switch(config)# vlan 2

switch(config-vlan)# name test123

4.2.3 switchport mode

Command Description

switchport mode {access | trunk | hybrid}

Parameter

access	Access mode
trunk	Trunk mode
Hybrid	Hybrid 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.)

Default

Hybrid mode

Command Mode

Interface configuration mode

Example

switch(config)# interface GigabitEthernet 1/2-4

switch(config-if)#switchport mode access

switch(config)# interface GigabitEthernet 1/1

switch(config-if)#switchport mode trunk

4.2.4 switchport access vlan

Command Description

switchport access vlan {vlan-id}

Parameter

Vlan-id: The VLAN ID ranges from **1** to **4094**.

Default

Vlan 1

Command Mode

Interface configuration mode

Example

switch(config)#vlan 2

switch(config)# interface GigabitEthernet 1/5-8

switch(config-if)#switchport mode access

switch(config-if)#switchport access vlan 2

4.2.5 Switchport hybrid acceptable-frame-type

Command Description

Switchport hybrid acceptable-frame-type <all | tagged | untagged>

Parameter

all | tagged | untagged: It specifies the type of frames that can be received by a hybrid port. **all** indicates all frame types, **tagged** indicates tagged frames, and **untagged** indicates untagged frames.

Default

all

Command Mode

Interface configuration mode

Example

switch(config)# interface GigabitEthernet 1/1

switch(config-if)# switchport hybrid acceptable-frame-type all

4.2.6 Switchport hybrid egress-tag

Command Description

Switchport hybrid egress-tag <all | none>: This command is used to configure the

tag attribute of the data egress port.

No switchport hybrid egress-tag

Parameter

<all | none>: It specifies the tag attribute of the data egress port, which is **tag** or **untag**.

Default

Untag Port vlan

Command Mode

Interface configuration mode

Example

switch(config)# interface GigabitEthernet 1/5

switch(config-if)# switchport hybrid egress-tag all

switch(config-if)# no switchport hybrid egress-tag

4.2.7 Switchport hybrid native

Command Description

Switchport hybrid native vlan <vlan-id>: This command is used to configure the local VLAN of a hybrid port.

Parameter

Vlan-id: The VLAN ID ranges from **1** to **4094**.

Default

all

Command Mode

Interface configuration mode

Example

switch(config)# interface GigabitEthernet 1/5

switch(config-if)# switchport hybrid native vlan 2

4.2.8 show vlan

Command Description

show vlan brief |id vlan-list| ip-subnet | mac |name | protocol | status

Parameter

The current VLAN configuration of the switch can be displayed by VLAN ID, VLAN name, or protocol.

brief	It is used to display the general VLAN configuration information.
id	The command vlan id is used to display relevant VLAN configuration.
ip-subnet	It is used to display VLAN entries of the IP subnet.
mac	It is used to display VLAN entries of the MAC address.
name	You can use VLAN name to display relevant VLAN status.
protocol	It is used to display the status of VLANs based on protocols.
status	It is used to display the VLAN configuration of each port.

Default

None

Command Mode

Privileged mode

Example

switch# show vlan brief

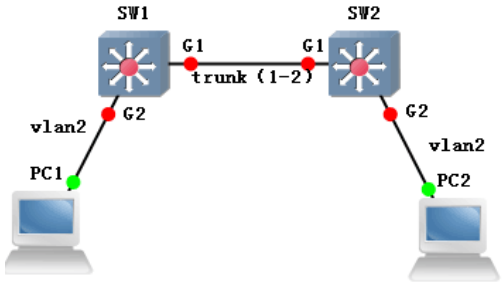
switch# show vlan status

switch# show vlan 2

switch# show vlan ip-subnet id 2

VLAN Management Example

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



SW1/SW2：

```
switch# configure terminal
switch(config)# interface GigabitEthernet 1/1
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1-2
switch(config-if)# exit
switch(config)# interface GigabitEthernet 1/2
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.

```
C:\Documents and Settings\ltn>ping 192.168.222.94

Pinging 192.168.222.94 with 32 bytes of data:

Reply from192.168.222.94: bytes=32 time<1ms TTL=128
Reply from192.168.222.94: bytes=32 time<1ms TTL=128
Reply from192.168.222.94: bytes=32 time<1ms TTL=128
Reply from192.168.222.94: bytes=32 time<1ms TTL=128
```

4.3 VCL Configuration

VCL configuration commands include:

- switchport vlan mac
- switchport vlan ip-subnet
- switchport vlan protocol

Note: 1. VCL needs to be used together with a port-based VLAN.

2. VLAN priority: MAC-based VLAN> Subnet-mask-based VLAN>Protocol-based VLAN.

Function Description

This module is used to configure VLANs based on MAC address, subnet mask and protocol. Different technologies are used based on different network demands.

4.3.1 switchport vlan mac

Command Description

switchport vlan mac: This command is used to configure a MAC-based VLAN.

no switchport vlan mac

Parameter

None

Default

None

Command Mode

Interface configuration mode

Example

switch(config)# interface GigabitEthernet 1/3

switch(config-if)# switchport mode access

switch(config-if)# switchport access vlan 2

// This command is used to configure the G1/3 port to VLAN 2.

switch(config)# interface GigabitEthernet 1/3

switch(config-if)# switchport vlan mac 00-00-00-00-00-01 vlan 2

// This command is used to add the label of VLAN 2 to the data frame of which the MAC address entering the G1/3 port is 00-00-00-00-00-01.

switch(config-if)# no switchport vlan mac 00-00-00-00-00-01 vlan 2

4.3.2 switchport vlan ip-subnet

Command Description

switchport vlan ip-subnet: This command is used to configure a subnet-based VLAN.

no switchport vlan ip-subnet: This command is used to delete a subnet-based VLAN.

Parameter

None

Default

None

Command Mode

Interface configuration mode

Example

switch(config)# interface GigabitEthernet 1/4

switch(config-if)# switchport mode access

switch(config-if)# switchport access vlan 2

// This command is used to configure the G1/4 port to VLAN 2.

switch(config)# interface GigabitEthernet 1/4

switch(config-if)# switchport vlan ip-subnet id 1 192.168.4.0/255.255.255.0 vlan 2

// This command is used to add the label of VLAN 2 to the IP of the 192.168.4.0/24 network segment entering the G1/3 port.

switch(config-if)# no switchport vlan ip-subnet id 1

4.3.3 switchport vlan protocol

Command Description

switchport vlan protocol: This command is used to configure the mapping between group names and VLANs.

no switchport vlan mac

Parameter

switchport vlan protocol group <group_name> vlan <vlan_id>

Default

None

Command Mode

Interface configuration mode

Example

switch(config)# interface GigabitEthernet 1/6

switch(config-if)# switchport mode access

switch(config-if)# switchport access vlan 2

// This command is used to configure the G1/6 port to VLAN 2.

switch(config)# interface GigabitEthernet 1/6

switch(config-if)# switchport vlan protocol group test vlan 2

// This command is used to add the label of VLAN 2 to the data frame from the protocol group under the G1/6 port.

switch(config-if)# no switchport vlan protocol group test vlan 2

4.3.4 vlan protocol

Command Description

vlan protocol eth2| llc | snap: This command is used to configure the mapping between protocols and groups.

no vlan protocol

Parameter

You can use **eth2** to configure the mapping between Ethernet protocols and VLANs.

Common Ethernet protocols include:

ARP	0x0806
IP	0x0800
LACP	0x8809
802.1X	0x888E
IPX	0x8137

Default

None

Command Mode

Global configuration mode

Example

switch(config)# vlan protocol snap 0xE02B 0x1 group test

// This command is used to add the data frame of the protocol snap 0xE02B 0x1 to the protocol group test.

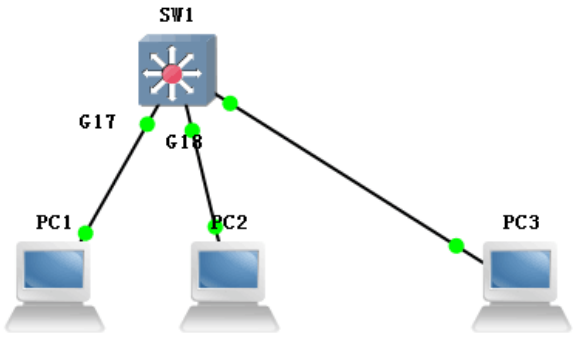
switch(config)# no vlan protocol snap 0xE02B 0x1 group test

VCL Configuration Example

1、Dividing VLANs based on MAC

You can configure the VLAN based on MAC address so that PC1 and PC2 can communicate with each other in VLAN 2, but cannot communicate with each other in other VLANs.

Add MAC addresses of PC1 and PC2 to VLAN 2, and add Ports 17 and 18 in the port-based VLAN to VLAN 2, as shown in the figure below:



switch(config)# interface GigabitEthernet 1/17

switch(config-if)# switchport mode access

switch(config-if)# switchport access vlan 2

switch(config-if)# switchport vlan mac 00-00-00-00-00-01 vlan 2

switch(config-if)# switchport vlan mac 00-00-00-00-00-02 vlan 2

switch(config-if)#exit

switch(config)# interface GigabitEthernet 1/18

switch(config-if)# switchport mode access

switch(config-if)# switchport access vlan 2

switch(config-if)# switchport vlan mac 00-00-00-00-00-01 vlan 2

switch(config-if)# switchport vlan mac 00-00-00-00-00-02 vlan 2

phenomenon:

If PC1 (192.168.1.1) pings PC2 (192.168.1.2), the communication is normal.

```
C:\Documents and Settings\ltn>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=64
Reply from 192.168.1.2: bytes=32 time<1ms TTL=64
Reply from 192.168.1.2: bytes=32 time<1ms TTL=64
Reply from 192.168.1.2: bytes=32 time<1ms TTL=64
```

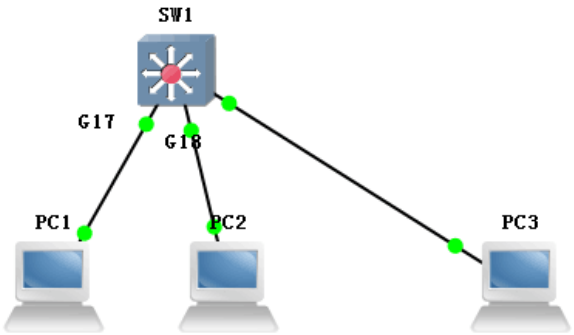
If PC1 (192.168.1.1) pings PC3 (192.168.1.3), the communication cannot be conducted.

```
C:\Documents and Settings\ltn>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

2、Dividing VLANs based on subnet mask

PC 1 is connected to the port G17 of the switch, PC 2 is connected to the port G18 of the switch, and PC 3 is connected to the port G19 of the switch. On the port-based VLAN configuration page, add all the three ports to VLAN 2. Configure the IP subnet-based VLAN so that PC 1 and PC 2 can ping with each other, but PC 3 cannot ping PC 1 and PC 2.

The IP address of PC 1 is 192.168.222.64, the IP address of PC 2 is 192.168.222.128, and the IP address of PC 3 is 192.168.222.2.



switch(config)# interface GigabitEthernet 1/17

switch(config-if)# switchport mode access

switch(config-if)# switchport access vlan 2

switch(config-if)#switchport vlan ip-subnet id 1 192.168.222.1/255.255.255.192 vlan 2

switch(config-if)#exit

switch(config)# interface GigabitEthernet 1/18

switch(config-if)# switchport mode access

switch(config-if)# switchport access vlan 2

switch(config-if)#switchport vlan ip-subnet id 1 192.168.222.1/255.255.255.192 vlan 2

phenomenon:

PC1 (192.168.222.64) can pings PC2 (192.168.222.128) successfully, and PC1 can communicate with PC2 normally.

```
C:\Documents and Settings>ping 192.168.222.128

Pinging 192.168.222.128 with 32 bytes of data:

Reply from 192.168.222.128: bytes=32 time<1ms TTL=128
Reply from 192.168.222.128: bytes=32 time<1ms TTL=128
Reply from 192.168.222.128: bytes=32 time<1ms TTL=128
Reply from 192.168.222.128: bytes=32 time<1ms TTL=128
```

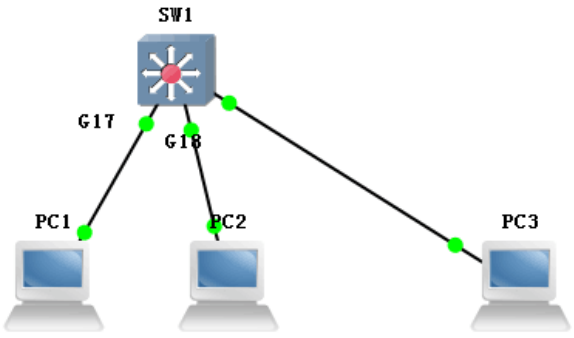
PC1 (192.168.222.64) cannot ping PC3 (192.168.222.2), and PC1 cannot communicate with PC3.

```
C:\Documents and Settings>ping 192.168.222.2

Pinging 192.168.222.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

3、Mapping a protocol to a group name and mapping a group name to VLAN

PC1 is connected to the port G17 under the switch. After the protocol-based VLAN is configured, the IP protocol cannot be transmitted in VLANs except for VLAN 2. The configuration steps are introduced below:

Step 1: Configure the port G17 to belong to VLAN 2 in the port-based VLAN group.
Step 2: Map the protocol to a group name
Step 3: Map the group name to VLAN



switch(config)# vlan protocol eth2 ip group ip

switch(config)interface GigabitEthernet 1/17

switch(config-if) switchport mode access

switch(config-if)switchport access vlan 2

switch(config-if) switchport vlan protocol group ip vlan 2

phenomenon:

After configuration, PC1 uses the interface IP of VLAN 2 to access the Web page of the switch. If the port G17 is configured to belong to VLAN 1 in the port-based VLAN group, PC1 cannot use the interface IP of VLAN 1 to access the Web page of the switch.

4.4 DHCP Snooping

DHCP snooping configuration commands include:

- ip dhcp snooping
- ip dhcp snooping trust
- show ip dhcp snooping table
- show ip dhcp snooping interface

Function Description

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.

4.4.1 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

switch(config)# ip dhcp snooping

switch(config)# no ip dhcp snooping

4.4.2 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

Trust

Command Mode

Interface configuration mode

Example

switch(config)# interface GigabitEthernet 1/1

switch(config-if)# ip dhcp snooping trust

switch(config-if)# no ip dhcp snooping trust

4.4.3 show ip dhcp snooping table

Command Description

show ip dhcp snooping table: This command is used to display the DHCP snooping table.

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

switch(config)# ip dhcp snooping

switch(config)# no ip dhcp snooping

4.4.4 show ip dhcp snooping interface

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

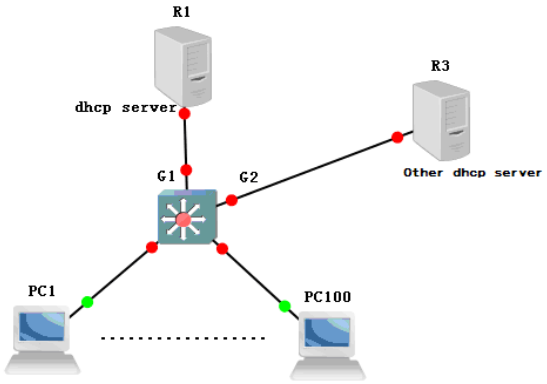
Privileged mode

Example

switch# show ip dhcp snooping interface GigabitEthernet 1/1

DHCP SNOOPING Configuration Example

Allow the client to obtain IP address information only from the DHCP server connected to Port G1, and not from other DHCP servers connected to Port G2.



switch#configure terminal
switch(config)# ip dhcp snooping
switch(config)# interface GigabitEthernet 1/1
switch(config-if)# ip dhcp snooping trust
switch(config)# interface GigabitEthernet 1/2
switch(config-if)#no ip dhcp snooping trust

phenomenon:

PCs 1 to 100 can obtain IP address information from the DHCP server connected to Port G1, but not from other DHCP servers connected to Port G2.

4.5 DHCP Server

DHCP server configuration commands include:

- ip dhcp server
- ip dhcp pool
- host/network
- lease time
- default-router
- dns
- show ip dhcp
- ip dhcp excluded-address

Function Description

In the following scenarios, the DHCP server is often used to allocate IP addresses:

1. The network is large in scale. The workload is huge if IP addresses are configured manually. It is difficult to perform centralized management on the entire network.

2. The number of hosts on the network is greater than the number of IP addresses supported by the network. It is impossible to allocate a fixed IP address to every host. For example, the Internet service provider (ISP) restricts the number of users who concurrently access the network, and users must dynamically obtain their own IP addresses.

3. Only a few hosts on the network need fixed IP addresses, and most hosts do not need fixed IP addressed.

4. The DHCP server configuration consists of three parts, including mode configuration, excluded IP address configuration, and address pool configuration.

4.5.1 ip dhcp server

Command Description

ip dhcp server: This command is used to enable the DHCP service.

no ip dhcp server: This command is used to disable the DHCP service.

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.

Parameter

None

Default

Disable

Command Mode

Global configuration mode or VLAN interface configuration mode

Example

switch(config)# ip dhcp server

switch(config)# no ip dhcp server

// This command is used to globally enable the DHCP server, so that all ports of the VLANs corresponding to the address pool can obtain IP addresses.

switch(config)# interface vlan 2

switch(config-if-vlan)# ip dhcp server //Configure the DHCP server to allow assignment of IP address in VLAN 2.

switch(config-if-vlan)# no ip dhcp server //Configure the DHCP server to prohibit assignment of IP address in VLAN 2.

4.5.2 ip dhcp pool

Command Description

ip dhcp pool <word>: This command is used to add a DHCP address pool.

ip dhcp pool <word>: This command is used to delete a DHCP address pool with the specified name.

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

switch(config)# ip dhcp pool vlan2_test1

switch(config)# no ip dhcp pool vlan2_test1

4.5.3 host/network

Command Description

Host <ip> <subnet_mask>: This command is used to add an IP address to the

address pool.

Network <ip> <subnet_mask>: This command is used to add an IP address segment to the address pool. (At most 1000 IP addresses can be assigned, and the capacity can be expanded to 4000 IP addresses.)

No host|network <ip> <subnet_mask>: This command is used to delete an IP address or IP address segment from the address pool.

Parameter

<ip>: It specifies the IP address

<subnet_mask>: It specifies the subnet mask.

Default

None

Command Mode

Address pool configuration mode

Example

switch(config)# ip dhcp pool test_pool

switch(config-dhcp-pool)# host 3.0.0.1 255.0.0.0

switch(config-dhcp-pool)# network 1.0.0.1 255.0.0.0

4.5.4 ip dhcp excluded-address

Command Description

ip dhcp excluded-address: This command is used to configure an excluded IP address or IP address segment in the address pool of the DHCP server.

noip dhcp excluded-address: This command is used to delete the excluded IP address or IP address segment from the address pool of the DHCP server.

An excluded IP address will not assigned to the client under the corresponding interface.

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

switch(config)# ip dhcp excluded-address 1.0.0.1 1.0.0.2

switch(config)#no ip dhcp excluded-address 1.0.0.1 1.0.0.2

4.5.5 lease time

Command Description

lease {<day> [<hour> [<min>]] | infinite}: This command is used to configure the lease period of the IP address in the address pool.

Parameter

{<day> [<hour> [<min>]] | infinite}: It specifies the lease period.

Default

Infinite

Command Mode

Address pool configuration mode

Example

switch(config)#ip dhcp pool 1

switch(config-dhcp-pool)# lease infinite

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

switch(config-dhcp-pool)# lease 1 0 0

// This command is used to configure the lease time of the address pool to 1d.

4.5.6 dns-server

Command Description

Dns <A.B.C.D>: This command is used to configure the IP address of the DNS

server.

Parameter

<A.B.C.D>: It specifies the IP address of the DNS server.

Default

None

Command Mode

Address pool configuration mode

Example

switch(config)#ip dhcp pool 1

switch(config-dhcp-pool)# dns 8.8.8.8

4.5.7 Default-router

Command Description

Default-router <A.B.C.D>: This command is used to configure the default gateway of the address pool.

Parameter

<A.B.C.D>: It specifies the IP address of the gateway.

Default

None

Command Mode

Address pool configuration mode

Example

switch(config-dhcp-pool)# default-router 1.0.0.100

4.5.8 Show ip dhcp

Command Description

Show ip dhcp pool|server: This command is used to display the configurations of the address pool and server.

Parameter

None

Default

None

Command Mode

Privileged mode

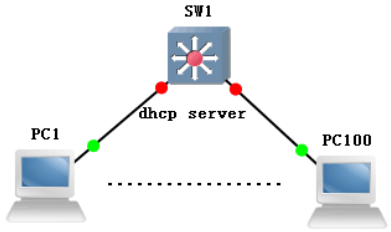
Example

switch# Show ip dhcp pool

switch# Show ip dhcp server

DHCP Server Configuration 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 dhcp server

switch(config)# interface vlan 1

switch(config-if-vlan)# ip dhcp server

switch(config-if-vlan)# exit

switch(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10

switch(config)# ip dhcp pool a

switch(config-dhcp-pool)# network 192.168.1.0 255.255.255.0

switch(config-dhcp-pool)#default-router 192.168.1.1

switch(config-dhcp-pool)#lease 1 0 0

switch(config-dhcp-pool)#dns-server 8.8.8.8

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.

4.6 IGMP Snooping Configuration

IGMP snooping configuration commands include:

- ip igmp snooping
- ip igmp snooping vlan
- ip igmp snooping immediate-leave
- show ip igmp-snooping

Function Description

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 ip 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.

Internet Group Management Protocol (IGMP) Snooping is a multicast restriction mechanism running on a L2 device to manage and control multicast groups.

Parameter

None

Default

Disable

Command Mode

Global configuration mode, VLAN configuration mode, or interface configuration mode

Example

switch (config)# ip igmp snooping //Enable the igmp-snooping function.

4.6.2 ip igmp snooping vlan

Command Description

ip igmp-snooping vlan <vlan_list>: This command is used to add an IGMP VLAN.

no ip igmp-snooping vlan <vlan_list>: This command is used to delete an IGMP VLAN.

Parameter

<vlan_list> **,** VLAN ID

Default

Disable

Command Mode

Global configuration mode

Example

switch (config)# ip igmp snooping vlan 1

// This command is used to globally add IGMP Snooping entries to VLAN 1.

switch(config)# interface vlan 1

switch(config-if-vlan1)# ip igmp snooping

// This command is used to enable IGMP Snooping under ports of VLAN 1.

4.6.3 ip igmp-snooping immediate-leave

Command Description

ip igmp-snooping immediate-leave: This command is used to enable the immediate leave function of a port.

no ip igmp-snooping immediate-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 GigabitEthernet 1/1

switch (config-if)# ip igmp snooping immediate-leave

4.6.4 show ip igmp snooping

Command Description

show ip igmp snooping |/detail/group-database/mrouter/vlan: This command is used to display the IGMP configuration.

Parameter

None

Default

None

Command Mode

Privileged mode

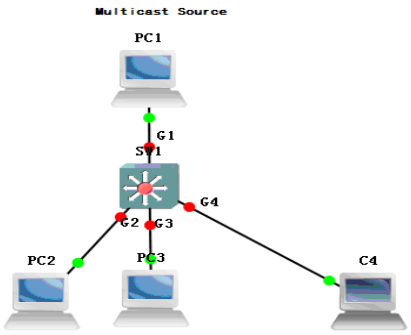
Example

switch #show ip igmp snooping //Display the IGMP configuration.

IGMP Snooping Configuration 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)# ip igmp snooping

switch(config)# no ip igmp unknown-flooding

switch(config)# interface GigabitEthernet 1/1

switch(config-if)# ip igmp snooping mrouter

PC 2/PC 3 requests to join the dynamic multicast group.

PC 4 does not request to join the dynamic multicast group.

phenomenon:

PC 2/PC 3 can receive video streams from the multicast source, but PC4 cannot.

4.7 MVR Configuration

MVR configuration commands include:

- mvr
- mvr vlan
- mvr name
- mvr immediate-leave
- show mvr
- type

Function Description

This function is used to solve the problem that IGMP Snooping does not work when receivers

in IGMP Snooping protocol are put in different VLANs. MVR can solve the flooding problem when receivers are put in different VLANs. It uses a specific manually configured VLAN (a VLAN for multicast) to forward multicast traffic on a L2 network. It can be used together with IGMP Snooping.

Just like IGMP Snooping protocol, MVR allows a L2 switch to monitor the IGMP control protocol. The two protocols work independently and can be configured on the switch simultaneously. If two features are enabled at the same time, MVR only monitor the john and report information statically configured to the group in which MVR is enabled. The john and report information of other groups are still managed by IGMP Snooping.

There are two types of MVR ports to be configured, namely, the source port and the receive port.

Source port: it refers to the port through which multicast streams in the multicast VLAN passes.

Receive port: it refers to the port connected to a monitoring multicast host. It can be put in any VLAN except the multicast VLAN or has no VLAN (in such a case, it is put in VLAN 1, and the traffic is untagged). It means, when executing the VLAN label replacement tasks, the switch on which MVR is enabled replaces the VLAN label of the multicast receive port to the VLAN label of the source port.

Multicast VLAN refers to the VLAN dedicated to MVR and manually configured in a specific network. It shall be configured to all source ports. It is usually used to transmit multicast streams in the network and avoid transmitting repeatedly one multicast stream to different VLANs. MVR VID must be in consistency with VLAN PVID in the multicast source.

4.7.1 mvr

Command Description

mvr: This command is used to globally enable the MVR mode.

no mvr: This command is used to globally disable the MVR mode.

Parameter

None

Default

Disable

Command Mode

Global configuration mode

Example

switch(config)# mvr

switch(config)# no mvr

4.7.2 Mvr vlan

Command Description

mvr vlan: This command is used to configure the MVR VLAN interface.

no mvr vlan: This command is used to delete the configuration of the MVR VLAN interface.

Parameter

mvr vlan <v_vlan_list> [name <mvr_name>]

Default

None

Command Mode

Global configuration mode

Example

switch(config)# mvr vlan 100 name 123

4.7.3 Mvr name/vlan

Command Description

mvr name <mvr_name> type

mvr vlan <mvr_vlan_list> type

This command is used to configure the port of the current MVR group to receive port

or source port.

Parameter

receive	This command is used to configure the port to receive port.
source	This command is used to configure the port to resource port.

Default

None

Command Mode

Interface configuration mode

Example

switch(config)#interface GigabitEthernet 1/10

switch(config-if)# mvr name 123 type source

// This command is used to configure Port G10 to multicast source port of MVR 123 group.

switch(config)#interface GigabitEthernet 1/10

switch(config-if-ge10)# mvr vlan 100 type source

// This command is used to configure Port G10 to multicast source port of MVR 100 group.

Note: The port role can be configured based on group name and VLAN. The two methods have the same effect and same priority. The last configuration prevails. For example, in the example above, the following command is entered first.

switch(config-if-ge10)# mvr vlan 100 type source

The port turns to a source port. Then the following command is entered：

switch(config-if)# mvr name 123 type receive

The port turns to a receive port. The last configuration prevails.

4.7.4 mvr immediate-leave

Command Description

mvr immediate-leave: This command is used to enable the MVR immediate leave function of a port.

no mvr immediate-leave: This command is used to disable the MVR immediate leave function of a port.

Parameter

None

Default

Disable

Command Mode

Interface configuration mode

Example

switch(config)#interface GigabitEthernet 1/10

switch(config-if)# mvr immediate-leave

switch(config-if)# no mvr immediate-leave

4.7.5 show mvr

Command Description

show mvr: This command is used to display the MVR configuration.

Parameter

None

Default

None

Command Mode

Privileged mode

Example

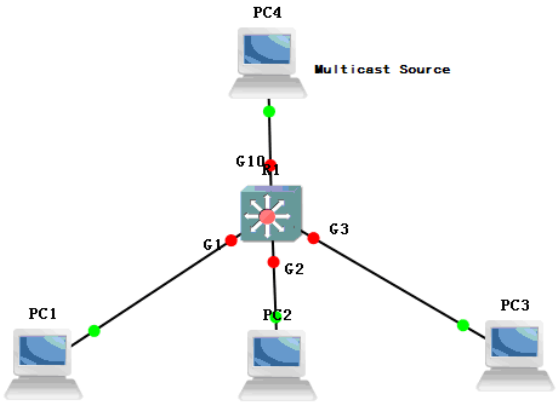
switch#show mvr

MVR Configuration Example

Ports 1, 2 and 10 are access ports. Set PVID to 10 and 11, and configure PVID of Port 10 to 100.

Enable MVR, and set MVR VID to 100 and MVR name to 123. Retain default settings of other parameters.

Set **Role** of Ports 1 and 2 to **R** and **Role** of Port 10 to **S**. Enable the fast leave function.



switch(config)# mvr

switch(config)#mvr vlan 100 name 123

// This command is used to configure VLAN 100 as the multicast source VLAN and name it.

switch(config)#interface GigabitEthernet 1/1

switch(config-if)#switchport mode access

switch(config-if)#switchport access vlan 10

switch(config-if)#mvr immediate-leave

switch(config-if)#mvr name 123 type receiver

// This command is used to configure G1 as an access port and set PVID to 10.

// This command is used to add G1 as the receive port and enable the fast leave function.

switch(config-if)#exit

switch(config)#interface GigabitEthernet 1/2

switch(config-if)#switchport mode access

switch(config-if)#switchport access vlan 11

switch(config-if)#mvr immediate-leave

switch(config-if)#mvr name 123 type receiver

// This command is used to configure G2 as an access port and set PVID to 11.

// This command is used to add G2 as the receive port and enable the fast leave function.

switch(config-if)#exit

switch(config)#interface GigabitEthernet 1/10

switch(config-if)#switchport mode access

switch(config-if)#switchport access vlan 100

switch(config-if)#mvr name 123 type source

// This command is used to configure G10 as an access port and set PVID to 100.

// This command is used to add G10 as the multicast source port.

phenomenon:

When the multicast source plays the video, PC 1 and PC 2 can receive multicast streams, but PC3 cannot receive multicast streams.

4.8 Route Configuration Commands

Route configuration commands include:

- ip routing
- ip dns proxy
- ip name-server
- interface vlan
- ip address
- ip route
- show ip interface brief
- show ip route

Function Description

Routing refers to the activity of transferring information from the source address to the destination address through an interconnected network.

4.8.1 ip routing

Command Description

ip routing: This command is used to enable the routing mode.

no ip routing: This command is used to disable the routing mode.

Host mode: The default route is not added to an L3 interface IP address.

Routing mode: The default route is added to an L3 interface IP address.

Parameter

None

Default

Route mode

Command Mode

Global configuration mode

Example

switch (config)#ip routing //Enable the routing mode.

4.8.2 ip dns proxy

Command Description

ip dns proxy

no ip dns proxy

Note: When the DNS proxy is enabled, you can use the **ip name-server** command to configure the DNS server address.

Parameter

None

Default

Disable

Command Mode

Global configuration mode

Example

switch (config)# ip dns proxy

// This command is used to enable the DNS proxy.

switch (config)# ip dns proxy

// This command is used to disable the DNS proxy.

4.8.3 ip name-server

Command Description

ip name-server This command is used to configure DNS server address.

no ip name-server This command is used to not configure DNS server address.

Parameter

<ip>		This command is used to specify the IP address of the DNS server.
dhcp	<cr>	This command is used to enable acquisition of the DNS server address from any DHCP server.
	Interface <port_id>	This command is used to enable acquisition of the DNS server address from a DHCP server connected to a specified interface.

Default

None

Command Mode

Global configuration mode

Example

switch(config)# ip name-server 1.2.3.4

// This command is used to specify the IP address of DNS server to 1.2.3.4.

4.8.4 interface vlan

Command Description

interface vlan<vlan_id>

Parameter

vlan_id: It specifies the ID of the VLAN interface. The value ranges from **vlan1** to **vlan4094**.

Default

None

Command Mode

Global configuration mode

Example

Run the following commands to enter the configuration mode of the VLAN1 interface:

switch(config)# interface vlan1

switch(config-if-vlan)#

4.8.5 ip address

Command Description

ip address <address> <netmask>: This command is used to add an IP address of an interface.

no ip address: This command is used to delete an IP address of an interface.

Parameter

Address	It specifies the IP address of a VLAN interface.
Netmask	It specifies the subnet mask.

Default

VLAN 1 interface

Command Mode

VLAN interface configuration mode

Example

Run the following commands to configure the IP address of the VLAN 2 interface:

switch(config)# interface vlan 2

switch(config-if-vlan)# ip address 192.168.1.1 255.255.255.0

4.8.6 ip route

Command Description

ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw> <v_nhop_vlanid>: This

command is used to add a static route.

no ip route: This command is used to delete a static route.

Parameter

v_ipv4_addr	It specifies the IP address.
v_ipv4_netmask	It specifies the subnet mask.
v_ipv4_gw	It specifies the gateway.
v_nhop_vlanid	It specifies the next-hop VLAN.

Default

None

Command Mode

Global configuration mode

Example

switch(config)# ip route 192.168.3.0 255.255.255.0 192.168.100.100 2 //Set a static route.

4.8.7 show ip interface brief

Command Description

show ip interface brief: This command is used to display IP addresses of interfaces.

Parameter

None

Default

None

Command Mode

Privileged mode

Example

switch#show ip interface brief //Display IP addresses of interfaces.

4.8.8 show ip route

Command Description

show ip route: This command is used to display the static routes.

Parameter

None

Default

None

Command Mode

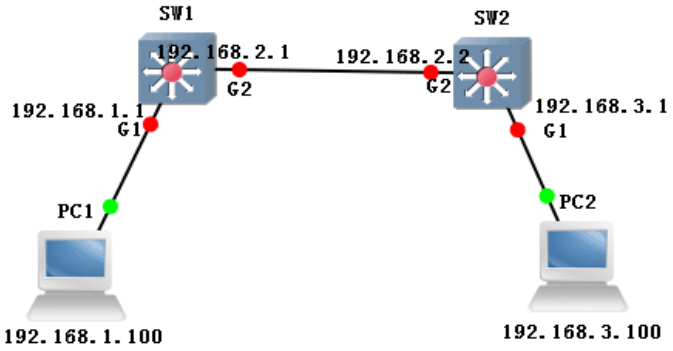
Privileged mode

Example

switch#show ip route //Display the static routes.

IP Routing Configuration 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 vlan 1

switch(config-if-vlan)# ip address 192.168.1.1 255.255.255.0

switch(config-if-vlan)# exit

switch(config)# interface vlan 2

switch(config-if-vlan)# ip address 192.168.2.1 255.255.255.0

switch(config)# interface GigabitEthernet 1/2

switch(config-if)# switchport mode access

switch(config-if)# switchport access vlan 2

switch(config-if)#exit

switch(config)# ip route 192.168.3.0 255.255.255.0 192.168.2.2 2

sw2： switch# configure terminal

switch(config)# interface vlan 1

switch(config-if-vlan)# ip address 192.168.3.1 255.255.255.0

switch(config-if-vlan)# exit

switch(config)# interface vlan 2

switch(config-if-vlan)# ip address 192.168.2.2 255.255.255.0

switch(config)# interface GigabitEthernet 1/2

switch(config-if)# switchport mode access

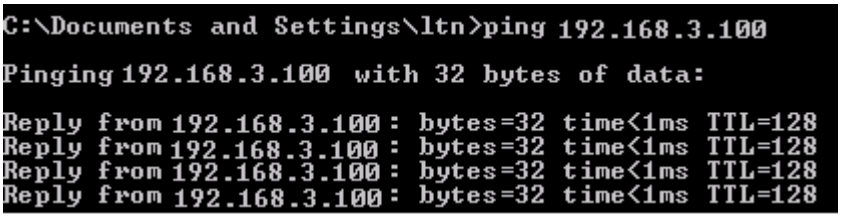
switch(config-if)# switchport access vlan 2

switch(config-if)#exit

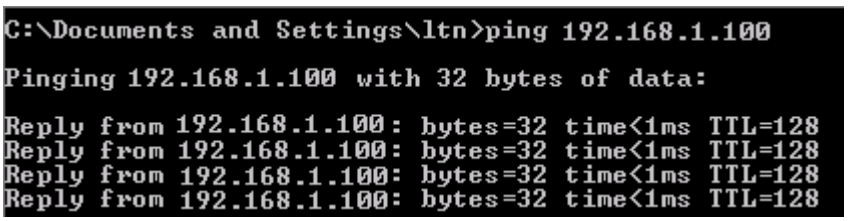
switch(config)# ip route 192.168.1.0 255.255.255.0 192.168.2.1 2

phenomenon:

pc1 ping pc2



pc2 ping pc1



5 Network Security Commands

5.1 MAC Address Table

Commands related to the MAC address table include:

- mac address-table learning
- mac address-table static
- mac address-table aging-time
- show mac address-table

Function Description

The Media Access Control (MAC) address table records the mapping between MAC addresses and ports, as well as VLANs to which the ports belong. When forwarding packets, the device queries the MAC address table based on the destination MAC address of each packet. If the MAC address table contains an entry that matches the MAC address of the packet, the device directly forwards the packet through the egress port in the entry. If the MAC address table does not contain any entry that matches the MAC address of the packet, the device broadcasts the packet through all ports in the corresponding VLAN except the receive port.

This module is used to configure the MAC learning mode and aging time, or add the static MAC entries.

5.1.1 mac address-table learning

Command Description

This command is used to select the learning mode of the MAC address table of a port.

Parameter

Auto	It is used to enable static binding and dynamic learning of the MAC address entries.
Off	It is used to disable learning of MAC address entries.
Safe	It is used to enable static binding and disable

	dynamic learning of the MAC address entries.

Default

None

Command Mode

Global configuration mode

Example

switch(config)# interface GigabitEthernet 1/1

switch(config-if)# mac address-table learning secure

5.1.2 mac address-table static

Command Description

mac address-table static mac-addr vlan vlan-id interface interface-id: This command is used to add a static MAC address.

no mac address-table static mac-addr vlan vlan-id interface interface-id: This command is used to delete a static MAC address.

Parameter

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-table static 00-00-00-00-00-01 vlan 2 interface 1/10

5.1.3 mac address-table aging-time

Command Description

mac address-table aging-time time: 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

Time: It specifies the aging time. The value range is <0, 10-1000000>.

Default

None

Command Mode

Global configuration mode

Example

switch(config)# mac address-table aging-time 200 //Set the MAC address aging time to 200s

5.1.4 show mac address-table

Command Description

show mac address-table {address | aging-time | conf | count | learning |[interface interface-id | vlan vlan-id] | static}: This command is used to display the MAC address table of the switch.

Parameter

Address	It specifies the MAC address.
aging-time	It specifies the aging time of the MAC address table.
Conf	It specifies the static MAC address added by the user.
Count	It specifies the total number of MAC addresses.
Learning	It specifies the MAC learning status.

interface-id	It specifies the interface ID.
vlan-id	It specifies the VLAN ID. The value ranges from **1** to **4094**.
Static	It specifies the static MAC address table.

Default

None

Command Mode

Privileged mode

Example

switch# show mac address-table //Display all the MAC address tables

5.2 Port Isolation

Function Description

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.

5.2.1 pvlan isolation

Command Description

When ports are added in an isolation group, ports in the isolation group cannot communicate with each other, but can communicate with ports that do not belong to the isolation group.

Parameter

None

Default

Disable

Command Mode

Interface configuration mode

Example

switch(config)# interface GigabitEthernet 1/1-5

switch(config-if)# pvlan isolation

// This command is used to add Ports G1-5 to an isolation group to prohibit communication between these ports.

5.3 Storm Control

Function Description

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.

5.3.1 qos storm

Command Description

qos storm broadcast /unicast /unknown: This command is used to enable the storm control function.

no qos storm broadcast /unicast /unknown: This command is used to disable the storm control function.

Parameter

Broadcast	Broadcast packet
Unicast	Unicast packet
Unknown	Unknown unicast packet

Default

Disable

Command Mode

Interface configuration mode

Example

This command is used to limit the rate of broadcast packet of Port 10 to 500kbps.

switch(config)# interface GigabitEthernet 1/10

switch (config-if)# qos storm broadcast 500

5.4 IP Source Guard

IP source guard commands include:

- ip verify source
- ip verify source translate
- ip verify source limit
- ip source binding interface
- show ip verify source

Function Description

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.

5.4.1 ip verify source

Command Description

ip verify source: This command is used to enable the IP source guard function.

no ip verify source: This command is used to disable the IP source guard function.

Parameter

None

Default

Disable

Command Mode

Global configuration mode

Example

switch (config)# ip verify source

This command is used to enable IP source guard for Port G1.

switch (config)# interface GigabitEthernet 1/1

switch (config-if-ge1)# ip verify source

5.4.2 ip verify source translate

Command Description

ip verify source translate: This command is used to translate a dynamic entry into a static entry.

no ip verify source translate: This command is used to cancel translation from a dynamic entry to a static entry.

Parameter

None

Default

Disable

Command Mode

Global configuration mode

Example

switch (config)# ip verify source translate

5.4.3 ip verify source limit

Command Description

ip verify source limit <0-2>: This command is used to set the maximum number of dynamic clients on the port.

no ip verify source limit: This command is used to restore the default maximum number of dynamic clients on the port.

Parameter

<0-2>	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 GigabitEthernet 1/1

switch (config-if)# ip verify source limit 2

5.4.4 ip source binding interface

Command Description

ip source binding interface <port_type> <in_port_type_id> <vlan_var> <ipv4_var> <mask_var>: This command is used to add a static entry.

no ip source binding interface<port_type> <in_port_type_id> <vlan_var> <ipv4_var> <mask_var>: This command is used to delete an entry.

Parameter

port_type	Port type
in_port_type_id	It specifies the port No.
vlan_var	It specifies the VLAN ID.
ipv4_var	It specifies the IP address.
mask_var	It specifies the subnet mask.

Default

None

Command Mode

Global configuration mode

Example

Run the following command to add a static entry, where the port No. is 1, VLAN ID is 1, IP address is 192.168.2.66, and subnet mask is 255.255.255.0:

switch(config)#ip source binding interface GigabitEthernet 1/1 1 192.168.2.66 255.255.255.0

5.4.5 show ip verify source

Command Description

show ip verify source: This command is used to display the configuration status of IP source guard.

Parameter

None

Default

Disable

Command Mode

Privileged mode

Example

switch# show ip verify source //Display the configuration status of IP source guard.

5.5 ARP Inspection Configuration

ARP inspection configuration commands include:

- ip arp inspection
- ip arp inspection trust
- ip arp inspection logging
- ip arp inspection entry interface

- ip arp inspection translate
- ip arp inspection vlan
- show ip arp inspection

Function Description

ARP is simple and easy to use, but attackers often take advantage of ARP to initiate attacks because ARP lacks of any security mechanism.

Attackers can send forged ARP packets in the place of other users and gateways to make ARP entries on the gateway or host incorrect, thus attacking the network. Attackers send a huge number of IP packets, the destination IP address of which cannot be translated, to a device. The device makes repeated attempts to translate the destination IP address, and consequently the CPU load is extremely high and the network traffic is extremely heavy. Attackers send a large number of ARP packets to the switch, increasing the CPU usage of the device. Currently, ARP attacks and APR virus have become a major threat to security of LANs. To avoid damages caused by various attacks, the switch provides the ARP inspection technology to prevent, detect, and eliminate the attacks.

After ARP inspection is enabled, related ports of the switch automatically checks whether APR packets come from correct ports and are not modified or spoofed by attackers. The switch can identify the correct ports based on the DHCP snooping binding table. If data received by the switch comes from incorrect ports, the switch automatically drops the packet, preventing attackers from attacking the network.

5.5.1 ip arp inspection

Command Description

ip arp inspection: This command is used to enable the ARP inspection function.

no ip arp inspection: This command is used to disable the ARP inspection function.

Parameter

None

Default

Disable

Command Mode

Global configuration mode

Example

switch(config)# ip arp inspection //Enable the ARP inspection function.

5.5.2 ip arp inspection trust

Command Description

ip arp inspection trust: This command is used to disable the ARP inspection function of a port.

no ip arp inspection trust: This command is used to enable the ARP inspection function of a port.

Parameter

None

Default

Disable

Command Mode

Interface configuration mode

Example

Enable the ARP inspection function of port 10.

switch(config)#interface GigabitEthernet 1/10

switch(config)#ip arp inspection trust

switch (config-if)# no ip arp inspection trust

5.5.3 ip arp inspection entry interface

Command Description

ip arp inspection entry interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>: This command is used to add a static entry.

no ip arp inspection entry interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>: This command is used to delete a static entry.

Parameter

port_type	Port type
port_type_id	It specifies the port No.
vlan_var	It specifies the VLAN ID
mac_var	It specifies the MAC address.
ipv4_var	It specifies the IP address.

Default

None

Command Mode

Global configuration mode

Example

switch(config)# ip arp inspection entry interface GigabitEthernet 1/1 1 00:00:00:00:00:08 192.168.2.3 // Add a static entry.

5.5.4 ip arp inspection translate

Command Description

ip arp inspection translate [interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>]: This command is used to translate a dynamic entry into a static entry.

no ip arp inspection translate [interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>]: This command is used to cancel translation from a dynamic entry to a static entry.

Parameter

port_type	It specifies the port type.
port_type_id	It specifies the port No.
vlan_var	It specifies the VLAN ID
mac_var	It specifies the MAC address.
ipv4_var	It specifies the IP address.

Default

None

Command Mode

Global configuration mode

Example

switch (config)# ip arp inspection translate //Translate all the dynamic entries into static entries.

5.5.5 show ip arp inspection

Command Description

show ip arp inspection entry/interface/vlan: This command is used to display the ARP inspection configuration.

Parameter

None

Default

None

Command Mode

Privileged mode

Example

switch (config)# show ip arp inspection //Display the ARP inspection configuration.

5.6 ACL Configuration Commands

ACL configuration commands include:

- access-list ace
- show access-list

Function Description

Access Control Lists (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.

The ACL configuration may be associated with port security (port ACL policy configuration) and bandwidth policies (port ACL bandwidth policies). Each ACE calls the ACL policy ID and bandwidth policy ID according to requirements.

5.6.1 access-list ace

Command Description

access-list ace: This command is used to add an ACL entry.

no access-list ace: This command is used to delete an ACL ACE entry.

Parameter

Ace id	It specifies the ID of an ACE. The value ranges from **1** to **512**
action	It specifies the access control behavior. The value is **permit** or **deny**
dmac-type	It specifies the type of the destination MAC
frame-type	It specifies the frame type
ingress interface	It specifies the ingress interface
logging	It specifies the log frame information
next	It specifies that a new ACE entry will be added under the current ACE entry
vid	It specifies the VID filter configuration

Default

Disable

Command Mode

Global configuration mode

Example

switch(config)# access-list ace 1 ingress interface GigabitEthernet 1/1 frame-type etype smac 00-00-00-00-00-01 action deny

5.6.2 Show access-list

Command Description

show access-list [interface [(<port_type> [<v_port_type_list>])]] [rate-limiter [<rate_limiter_list>]] [ace statistics [<ace_list>]]

show access-list ace-status [static] [link-oam] [loop-protect] [dhcp] [ptp] [upnp] [arp-inspection] [evc] [mep] [ipmc] [ip-source-guard] [ip-mgmt] [conflicts] [switch <switch_list>] //This command is used to display the ACE configuration

Parameter

None

Default

Disable

Command Mode

Privileged mode

Example

switch# show access-list ace statistics

switch# show access-list ace

5.7 STP Configuration

STP configuration commands include:

- spanning-tree
- spanning-tree mode
- spanning-tree mst 0 priority
- spanning-tree auto-edge
- spanning-tree bpdu-guard
- spanning-tree edge

- spanning-tree link-type
- spanning-tree mst
- spanning-tree restricted-role
- spanning-tree restricted-tcn
- show spanning-tree

Function Description

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.

5.7.1 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

Interface configuration mode

Example

switch(config)#interface GigabitEthernet 1/10

switch (config-if) #spanning-tree //Enable the STP function of port 10.

switch (config-stp-aggr)# spanning-tree //Enable the STP function of the aggregation port.

5.7.2 spanning-tree mode

Command Description

spanning-tree mode stp/mstp/rstp: This command is used to set the STP version.

no spanning-tree mode: This command is used to restore the default STP version.

Parameter

None

Default

stp

Command Mode

Global configuration mode

Example

switch (config) #spanning-tree mode rstp //Set the STP version to **RSTP**.

5.7.3 spanning-tree mst 0 priority

Command Description

spanning-tree mst 0 priority <0/4096/8192--61440>

This command is used to modify the STP and RSTP bridge priority.

Parameter

None

Default

32768

Command Mode

Global configuration mode

Example

switch (config) #spanning-tree mst 0 priority 4096

// This command is used to modify the current bridge priority of the device to 4096.

5.7.4 spanning-tree auto-edge

Command Description

spanning-tree auto-edge: This command is used to enable the auto edge function.

no spanning-tree auto-edge: This command is used to disable the auto edge function.

Parameter

None

Default

Enable

Command Mode

Interface configuration mode

Example

switch(config)#interface GigabitEthernet 1/10

switch (config-if) #spanning-tree auto-edge //Enable the auto edge function of port 10.

5.7.5 spanning-tree bpdu-guard

Command Description

spanning-tree bpdu-guard: This command is used to enable the BPDU guard function.

no spanning-tree bpdu-guard: This command is used to disable the BPDU guard function.

Parameter

None

Default

Disable

Command Mode

Interface configuration mode

Example

switch(config)#interface GigabitEthernet 1/10

switch (config-if) #spanning-tree bpdu-guard //Enable the BPDU guard function of port 10.

switch (config-stp-aggr)# spanning-tree bpdu-guard //Enable the BPDU guard function of the aggregation port.

5.7.6 spanning-tree edge

Command Description

spanning-tree edge: This command is used to enable the admin edge function.

no spanning-tree edge: This command is used to disable the admin edge function.

Parameter

None

Default

Non-Edge

Command Mode

Interface configuration mode

Example

switch(config)#interface GigabitEthernet 1/10

switch (config-if) #spanning-tree edge //Enable the admin edge function of port 10.

5.7.7 spanning-tree link-type

Command Description

spanning-tree link-type auto/ point-to-point/ shared: This command is used to configure the point-to-point type.

no spanning-tree link-type: This command is used to restore the default

point-to-point type.

Parameter

Auto	It corresponds to **auto** on the web page.
point-to-point	It corresponds to **forced true** on the web page.
shared	It corresponds to **forced false** on the web page.

Default

auto

Command Mode

Interface configuration mode

Example

switch(config)#interface GigabitEthernet 1/10

switch (config-if) spanning-tree link-type point-to-point //Set the point-to-point type of port 10 to **forced true**.

switch (config-stp-aggr)# spanning-tree link-type point-to-point //Set the point-to-point type of the aggregation port to forced true.

5.7.8 spanning-tree mst

Command Description

spanning-tree mst <instance> cost {<cost> | auto}: This command is used to set the path cost.

no spanning-tree mst <instance> cost {<cost> | auto}: This command is used to restore the default path cost.

spanning-tree mst <instance> port-priority <prio>: This command is used to set the priority.

no spanning-tree mst <instance> port-priority <prio>: This command is used to restore the default priority.

Parameter

instance	The value ranges from **0** to **7**.
Cost	The value ranges from **1** to **200000000**.
Prio	The value ranges from **0** to **240**.

Default

None

Command Mode

Interface configuration mode

Example

switch(config)#interface GigabitEthernet 1/10

switch (config-if) # spanning-tree mst 1 cost 144 //Set the path cost of port 10.

switch (config-stp-aggr)# spanning-tree mst 1 cost 144 //Set the path cost of the aggregation port.

5.7.9 spanning-tree restricted-role

Command Description

spanning-tree restricted-role: This command is used to enable the restricted role function.

no spanning-tree restricted-role: This command is used to disable the restricted role function.

Parameter

None

Default

Disable

Command Mode

Interface configuration mode

Example

switch(config)#interface GigabitEthernet 1/10

switch (config-if) # spanning-tree restricted-role //Enable the restricted role function of port 10.

switch (config-stp-aggr)# spanning-tree restricted-role //Enable the restricted role function of the aggregation port.

5.7.10 spanning-tree restricted-tcn

Command Description

spanning-tree restricted- tcn: This command is used to enable the restricted TCN function.

no spanning-tree restricted- tcn: This command is used to disable the restricted TCN function.

Parameter

None

Default

Disable

Command Mode

Interface configuration mode

Example

switch(config)#interface GigabitEthernet 1/10

switch (config-if) # spanning-tree restricted- tcn //Enable the restricted TCN function of port 10.

switch (config-stp-aggr)# spanning-tree restricted- tcn //Enable the restricted TCN function of the aggregation port.

5.7.11 show spanning-tree

Command Description

show spanning-tree |/active/ detailed/ interface / mst / summary: This command is used to display the STP configuration.

Parameter

None

Default

None

Command Mode

Privileged mode

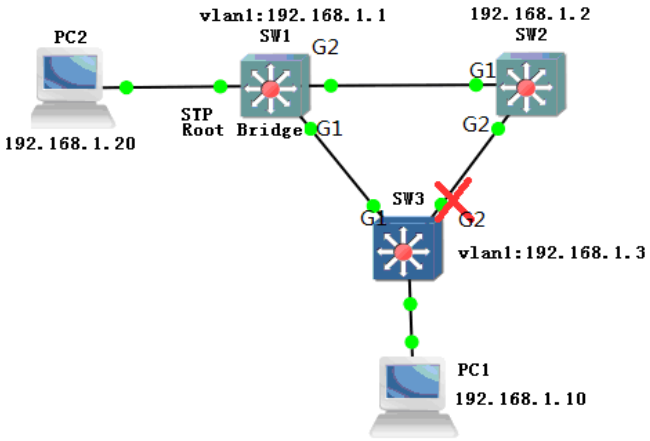
Example

switch # show spanning-tree //Display the STP configuration.

STP Configuration Example

Three devices form a STP loop, and SW1 is selected as the root bridge.

When any of the other links except for the link in which the blocked port is located has a fault, STP can realize a fast switch.



sw1: switch# configure terminal

switch(config)# spanning-tree mode stp
switch(config)# interface GigabitEthernet 1/1
switch(config-if)# spanning-tree

switch(config-if)#exit

switch(config)# interface GigabitEthernet 1/2
switch(config-if)# spanning-tree

switch(config-if)#exit

switch(config)# spanning-tree mst 0 priority 0

sw2: switch# configure terminal

switch(config)# spanning-tree mode stp
switch(config)# interface GigabitEthernet 1/1
switch(config-if)# spanning-tree

switch(config-if)#exit

switch(config)# interface GigabitEthernet 1/2
switch(config-if)# spanning-tree

switch(config-if)#exit

switch(config)# spanning-tree mst 0 priority 4096

sw3： switch# configure terminal

switch(config)# spanning-tree mode stp

switch(config)# interface GigabitEthernet 1/1

switch(config-if)# spanning-tree

switch(config-if)#exit

switch(config)# interface GigabitEthernet 1/2

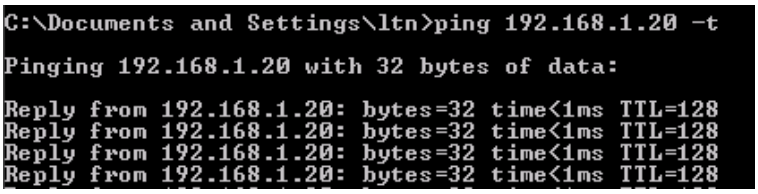
switch(config-if)# spanning-tree

switch(config-if)#exit

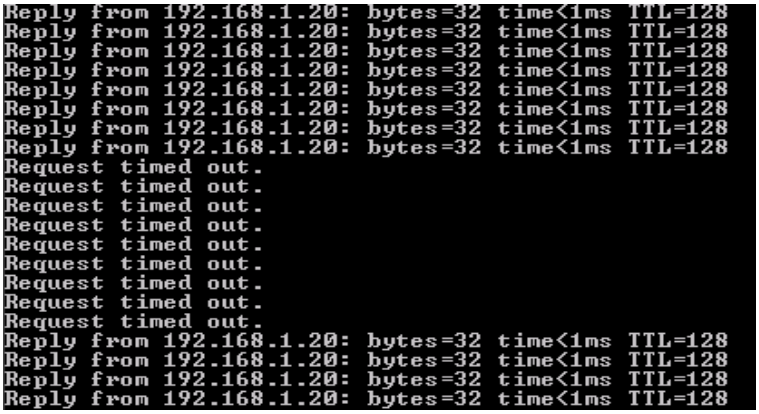
switch(config)# spanning-tree mst 0 priority 8192

phenomenon:

PC1 pings PC2 successfully, and two PCs can communicate normally.



The Port G1 on SW1 is manually disconnected. The communication is not allowed within a short period of time but is restored in 30-45s.



5.8 Loop Protection Configuration

Loop protection configuration commands include:

- loop-protect
- loop-protect tx-mode
- loop-protect transmit-time

- show loop-protect interface
- show loop-protect status

Function Description

Loop protection 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.

5.8.1 loop-protect

Command Description

loop-protect: This command is used to enable the loop protection function.

no loop-protect: This command is used to disable the loop protection function.

Parameter

None

Default

Disable

Command Mode

Global configuration mode or interface configuration mode

Example

switch# configure terminal

switch(config)# loop-protect

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

switch# configure terminal

switch(config)# interface GigabitEthernet 1/1

switch(config-if)#loop-protect

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

5.8.2 loop-protect tx-mode

Command Description

loop-protect tx-mode: This command is used to enable the Tx mode for a port.

no loop-protect tx-mode: This command is used to disable the Tx mode for a port.

Parameter

None

Default

Disable

Command Mode

Interface configuration mode

Example

switch(config)# interface GigabitEthernet 1/1

switch(config-if)#loop-protect tx-mode

// This command is used to enable the Tx mode for Port G1.

5.8.3 loop-protect transmit-time

Command Description

loop-protect transmit-time <100-1000>milliseconds

This command is used to configure the loop detection interval.

Parameter

None

Default

500 milliseconds

Command Mode

Global configuration mode

Example

switch(config)#loop-protect transmit-time 600

This command is used to set the loop detection interval to 600ms.

5.8.4 show loop-protect interface

Command Description

show loop-protect interface <port_type> <port_type_id>

This command is used to display the loop protection status of the port.

Parameter

None

Default

None

Command Mode

Privileged mode

Example

switch# show loop-protect interface XGigabitEthernet 1/1

// This command is used to display the loop protection status of the 10-gigabit Port T1.

5.8.5 show loop-protect status

Command Description

Display loop-protect status

Parameter

None

Default

None

Command Mode

Privileged mode

Example

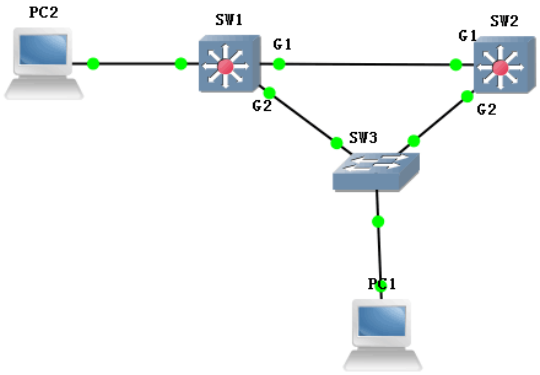
switch# show loop-protect status

// This command is used to display the global loop protection status.

LOOP-PROTECT Configuration 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-protect

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

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

switch(config)# interface GigabitEthernet 1/1

switch#(config-if)# loop-protect

switch(config-if)# loop-protect tx-mode

switch(config-if)#exit

// This command is used to enable the loop protection and Tx mode for Port G1.

switch(config)# interface GigabitEthernet 1/2

switch#(config-if)# loop-protect

switch(config-if)# loop-protect tx-mode

// This command is used to enable the loop protection and Tx mode for Port G2.

sw2： switch# configure terminal

switch#(config)# loop-protect

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

switch(config)# interface GigabitEthernet 1/1

switch#(config-if)# loop-protect

switch(config-if)# loop-protect tx-mode

switch(config-if)#exit

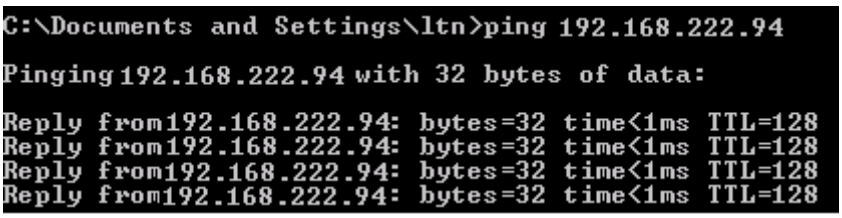
switch(config)# interface GigabitEthernet 1/2

switch#(config-if)# loop-protect

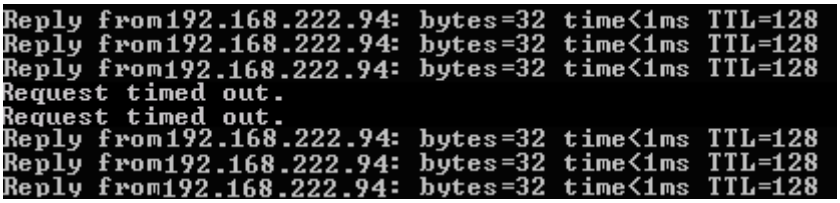
switch(config-if)# loop-protect tx-mode

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.

5.9 ERPS Configuration Commands

ERPS configuration commands include:

- erps <1-64> major
- erps <1-64> rpl
- erps <1-64> guard
- erps <1-64> holdoff
- erps <1-64> revertive
- erps <1-64> vlan

Note: ERPS configuration commands are relatively complicated. It is recommended that the easy-to-use web page be used for configuration.

Function Description

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.

5.9.1 erps <1-64> major

Command Description

erps <1-64> major

This command is used to add member ports to the current ERPS group.

Parameter

<1-64>	It indicates the ID of the ERPS group. At most 64 groups are supported.
Port 0	It indicates the Port 1 forming the loop in the current ERPS group.
Port 1	It indicates the Port 2 forming the loop in the current ERPS group.

Default

None

Command Mode

Global configuration mode

Example

switch(config)# erps 1 major port0 interface GigabitEthernet 1/1 port1 interface GigabitEthernet 1/2

// This command is used to add Ports 1 and 2 to ERPS group 1.

5.9.2 erps <1-64> rpl

Command Description

erps <1-64> rpl

This command is used to add an owner port or neighbor port to the current ERPS group.

Parameter

<1-64>	It indicates the ID of the ERPS group. At most

	64 groups are supported.
owner	It is used to configure the owner port of the current ERPS group.
neighbor	It is used to configure the neighbor port of the current ERPS group.

Default

None

Command Mode

Global configuration mode

Example

switch(config)# erps 1 rpl owner port0

// This command is used to configure Port 1 in the current ERPS group as an owner port.

5.9.3 erps <1-64> guard

Command Description

erps <1-64> guard <10-2000 ms>

This command is used to configure the guard time of the current ERPS group. The unit is millisecond.

Parameter

<1-64>	It indicates the ID of the ERPS group. At most 64 groups are supported.
<10-2000ms>	It is used to configure the guard time of the current ERPS group. When a link is recovered from a failure, the neighbor node detects a failure recovery, starts the guard timer, and periodically sends the R-APS (NR) message to indicate that there is no local fault request. But

	the port connected to the faulty link is still in blocked state.

Default

500ms

Command Mode

Global configuration mode

Example

switch(config)# erps 1 guard 600

// This command is used to set the guard time of the current ERPS group to 600ms.

5.9.4 erps <1-64> holdoff

Command Description

erps <1-64> holdoff<0-10000 ms>

This command is used to configure the holdoff time of the current ERPS group. The unit is millisecond.

<1-64>	It indicates the number of ERPS group. At most 64 groups are supported.
<0-10000ms>	It is used to configure the holdoff time of the current ERPS group. When a fault occurs, the fault is not immediately reported to ERPS. The fault is reported only if the fault persists when the hold off timer expires.

Default

0ms

Command Mode

Global configuration mode

Example

switch(config)# erps 1 holdoff 10

// This command is used to set the holdoff time of the current ERPS group to 10ms.

5.9.5 erps <1-64> revertive

Command Description

erps <1-64> revertive <1-12 min>

This command is used to configure the revertive time of the current ERPS group. The unit is minute.

Parameter

<1-64>	It indicates the number of ERPS group. At most 64 groups are supported.
<1-12min>	It is used to configure the holdoff time of the current ERPS group. When the ring protection link (RPL) node receives the first R-APS (NR) message, it starts the WTR timer. When the WTR timer expires, the RPL node re-blocks the RPL port, sends the R-APS (NR RB) message, and then updates the FDB table. The WTR timer prevents flapping of the blocking point that occurs because the RPL owner immediately blocks the RPL owner port after receiving the R-APS (NR) message.

Default

1min

Command Mode

Global configuration mode

Example

switch(config)# erps 1 revertive 5

// This command is used to configure the revertive time of the current ERPS group to 5 minutes (1min by default).

5.9.6 erps <1-64> vlan

Command Description

erps <1-64> vlan <vlan_list>

This command is used to configure the valid VLAN for the current ERPS group.

Parameter

<1-64>	It indicates the number of ERPS group. At most 64 groups are supported.
<vlan_list>	It is used to configure the valid VLAN for the current ERPS group. The valid VLAN is VLAN 1 by default.

Default

1min

Command Mode

Global configuration mode

Example

switch(config)# erps 1 vlan 2

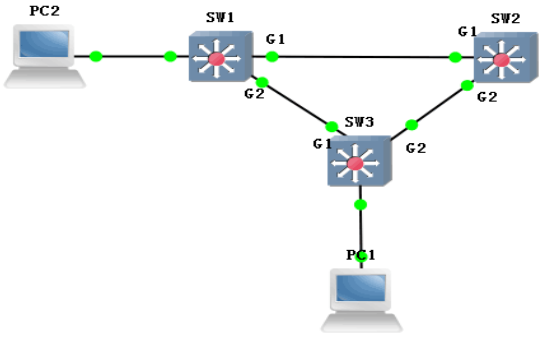
// It is used to configure VLAN 2 as the valid VLAN for the current ERPS group (the valid VLAN is VLAN 1 by default).

ERPS Configuration Example

Three devices form an ERPS loop. 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 major port0 interface GigabitEthernet 1/1 port1 interface

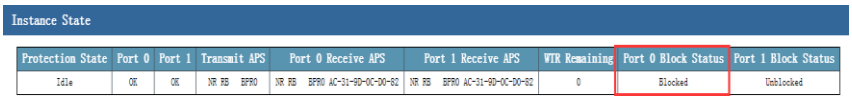
GigabitEthernet 1/2

switch(config)# erps 1 rpl owner port0

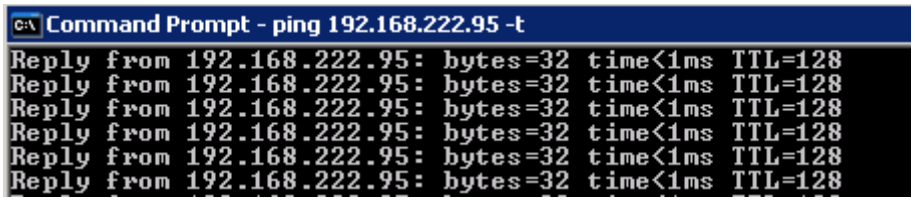
sw2/sw3：switch(config)#erps 1 major port0 interface GigabitEthernet 1/1 port1 interface GigabitEthernet 1/2

phenomenon:

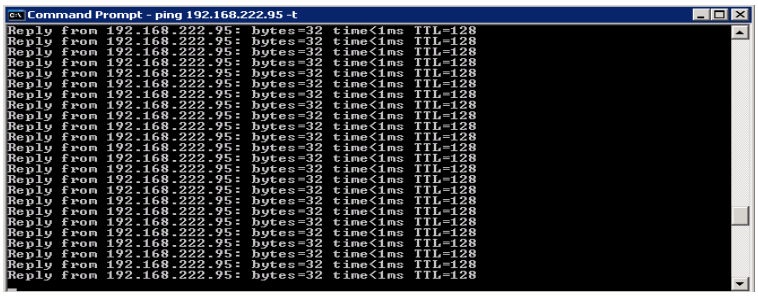
Port 0 of SW1 is blocked.



pc1（192.168.222.107） ping pc2（192.168.222.95）



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.



6 Network Management Commands

6.1 SSH Configuration

SSH configuration commands include:

- ip ssh
- no ip ssh

Function Description

Secure Shell (SSH) is a security protocol on the application layer and transmission layer developed by Network Working Group of IETF. SSH is a reliable protocol, which protects security of remote login sessions and other network services. The SSH protocol can be used to effectively prevent information leakage during remote management.

6.1.1 ip ssh

Command Description

ip ssh: This command is used to enable the SSH function.

no ip ssh: This command is used to disable the SSH function. After this command is executed, the switch cannot be managed in SSH mode.

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

switch(config)# ip ssh //Enable the SSH function.

6.2 HTTP Configuration

HTTP configuration commands include:

- ip http secure-server
- ip http-serve- redirect

Function Description

Hypertext Transfer Protocol (HTTP) defines how a browser (a WWW user process) requests a WWW text from a WWW server and how the server sends the text to the browser. HTTP is a transaction-oriented protocol used on the application layer. It ensures reliable exchange of documents (including texts, sound, images and other multimedia documents) on WWW.

Hyper Text Transfer Protocol over Secure Socket Layer (HTTPS) is a security-oriented HTTP channel. It is a secured HTTP. That is, SSL is added to HTTP and serves as a security base of HTTP. SSL is needed to encrypt detailed contents. HTTPS is a URI scheme, and is similar to http: scheme in terms of syntax. It is used for safe HTTP data transmission. https:URL means HTTP is used, but the HTTPS contains a default port other than HTTP and an encryption/identity verification layer (between HTTP and TCP). The system is preset in Netscape Navigator of the browser and provides identity verification and encrypted communication methods. Now, HTTPS is widely used for security sensitive communication on WWW.

6.2.1 ip http secure-server

Command Description

ip http secure-server: This command is used to enable the HTTP service on the switch.

no ip http secure-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

Disable

Command Mode

Global configuration mode

Example

switch(config)# ip http secure-server //Enable the HTTP service.

6.2.2 ip http secure-redirect

Command Description

ip http secure-redirect: This command is used to redirect the switch to the HTTPS service.

no ip http secure-redirect: This command is used to cancel the configuration of redirecting the switch to the HTTPS service. After this command is executed, the switch cannot be managed in HTTPS mode, but can be managed in HTTP mode.

Parameter

None

Default

Disable

Command Mode

Global configuration mode

Example

switch(config)# ip http secure-redirect //Enable the automatic HTTPS redirection service of the switch.

6.3 LLDP Configuration

LLDP configuration commands include:

- lldp
- lldp holdtime

- lldp transmission-delay
- lldp timer
- lldp reinit
- show lldp neighbors

Function Description

LLDP is a standard link layer discovery method. A device can organize the main capability, management address, device ID, and port ID of a local device into different Type/Length/Value (TLVs), encapsulate the TLVs in Link Layer Discovery Protocol Data Unit (LLDPDU), and send them to a neighbor directly connected to the local device. On receiving the LLDPDUs, the neighbor saves them in a standard Management Information Base (MIB), so that the network management system can query the information and determine the communication status of the link.

6.3.1 lldp

Command Description

lldp receive: This command is used to enable the LLDP frame receiving mode of a port.

lldp transmit: This command is used to enable the LLDP frame transmitting mode of a port.

The LLDP frame transmitting and receiving modes of a port are enabled at the same time.

no lldp receive|transmit: This command is used to disable the LLDP frame transmitting or receiving mode of a port at the same time.

Parameter

None

Default

Disable

Command Mode

Interface configuration mode

Example

switch(config)#interface GigabitEthernet 1/10

switch(config-if)# lldp receive

switch(config-if)# lldp transmit

switch(config-if)# no lldp transmit

6.3.2 lldp holdtime

Command Description

lldp holdtime: This command is used to configure the LLDP holdtime.

no lldp holdtime: This command is used to restore the default LLDP holdtime.

Parameter

<time>: The value ranges from **2** to **10**. The unit is second.

Default

4

Command Mode

Global configuration mode

Example

switch(config)# lldp holdtime 3

switch(config)# no lldp holdtime

6.3.3 lldp transmission-delay

Command Description

lldp transmission-delay <1-8192>: This command is used to configure the LLDP transmission delay.

Parameter

<1-8192>: It specifies the transmission delay. The value ranges from **1** to **8192**. The unit is second.

Default

2

Command Mode

Global configuration mode

Example

switch(config)# lldp transmission-delay 4

switch(config)# no lldp transmission-delay

6.3.4 lldp timer

Command Description

lldp timer <5-32768>: This command is used to configure the TTL of the LLDP transmitted packet.

no lldp timer <5-32768>: This command is used to restore the default TTL of the LLDP transmitted packet.

Parameter

<5-32768>: It specifies the TTL. The value ranges from **5** to **32768**. The unit is second.

Default

30

Command Mode

Global configuration mode

Example

switch(config)# lldp timer 20

6.3.5 lldp reinit

Command Description

lldp reinit <1-10>: This command is used to configure the delay of the LLDP continuous packet transmission.

no lldp reinit <1-10>: This command is used to restore the default delay of the LLDP continuous packet transmission.

Parameter

<1-10>: It specifies the transmission delay. The value ranges from **1** to **10**. The unit is second. .

Default

2

Command Mode

Global configuration mode

Example

switch(config)# lldp timer 2

6.3.6 show lldp neighbors

Command Description

show lldp neighbors: This command is used to display the brief information about neighbors.

Parameter

None

Default

None

Command Mode

Privileged mode

Example

switch# show lldp neighbors

6.4 802.1X Configuration Commands

802.1X configuration commands include:

- dot1x system-auth-control

- dot1x port-control auto
- dot1x port-control mac-based
- dot1x port-control single
- dot1x port-control force-unauthorized
- dot1x re-authentication
- show dot1x statistics
- dot1x authentication timer re-authenticate

Note: When using the 802.1x function, you must disable the STP function of the port.

Function Description

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.

The switch described in this manual can serve as an authentication system to perform authentication on PCs on the network. If user devices connected to ports of the switch can pass the authentication, they can access resources on the LAN. If they fail in authentication, their access to network resources will be denied.

6.4.1 dot1x system-auth-control

Command Description

dot1x system-auth-control: This command is used to globally enable the 802.1x NAS.

no dot1x system-auth-control: This command is used to globally disable the 802.1x NAS.

Parameter

None

Default

Disable

Command Mode

Global configuration mode

Example

switch(config)# dot1x system-auth-control

switch(config)# no dot1x system-auth-control

6.4.2 dot1x port-control auto

Command Description

dot1x port-control auto: This command is used to configure **Port_Based 802.1x** as the port authentication mode.

no dot1x port-control: This command is used to restore the default port authentication mode.

Parameter

None

Default

force-authorized

Command Mode

Interface configuration mode

Example

switch(config)#interface GigabitEthernet 1/10

switch(config-if)# dot1x port-control auto

6.4.3 dot1x port-control mac-based

Command Description

dot1x port-control mac-based: This command is used to configure **mac_Based 802.1x** as the port authentication mode.

no dot1x port-control: This command is used to restore the default port

authentication mode.

Parameter

None

Default

force-authorized

Command Mode

Interface configuration mode

Example

switch(config)#interface GigabitEthernet 1/10

switch(config-if)#dot1x port-control mac-based

6.4.4 dot1x port-control single

Command Description

dot1x port-control single: This command is used to configure **single 802.1x** as the port authentication mode.

no dot1x port-control: This command is used to restore the default port authentication mode.

Parameter

None

Default

force-authorized

Command Mode

Interface configuration mode

Example

switch(config)#interface GigabitEthernet 1/10

switch(config-if)# dot1x port-control single

6.4.5 dot1x port-control force-unauthorized

Command Description

dot1x port-control force-unauthorized: This command is used to configure **force-unauthorized** as the port authentication mode.

no dot1x port-control: This command is used to restore the default port authentication mode.

Parameter

None

Default

force-authorized

Command Mode

Interface configuration mode

Example

switch(config)#interface GigabitEthernet 1/10

switch(config-if)# dot1x port-control force-unauthorized

6.4.6 dot1x re-authentication

Command Description

dot1x re-authentication: This command is used to globally enable the port re-authentication function.

no dot1x re-authentication: This command is used to globally disable the port re-authentication function.

Parameter

None

Default

Disable

Command Mode

Global configuration mode

Example

switch(config)# dot1x re-authentication

switch(config)# no dot1x re-authentication

6.4.7 dot1x authentication timer re-authenticate

Command Description

dot1x authentication timer re-authenticate <1-3600>: This command is used to globally configure the port re-authentication cycle.

no dot1x authentication timer re-authenticate: This command is used to restore the default port re-authentication cycle.

Parameter

<1-3600>: It specifies the port re-authentication cycle. The value ranges from **1** to **3600**. The unit is second.

Default

3600

Command Mode

Global configuration mode

Example

switch(config)# dot1x authentication timer re-authenticate 1000

switch(config)# no dot1x authentication timer re-authenticate

6.4.8 show dot1x statistics

Command Description

show dot1x statistics: This command is used to display the port authentication statistics.

Parameter

all	This command is used to display all statistics.
eapol	This command is used to display request authentication

	statistics.
radius	This command is used to display server authentication statistics.

Default

None

Command Mode

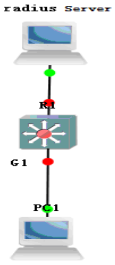
Privileged mode

Example

switch# show dot1x statistics all

802.1x Configuration Example

Device connected to Port G1 must pass the authentication before it can access the network.



switch(config)# dot1x system-auth-control

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

switch(config)#radius-server host 192.168.1.100 acct-port 0 key 123

switch(config)# interface GigabitEthernet 1/1

switch(config-if)# dot1x port-control auto

// This command is used to enable 802.1x automatic authentication for Port G1.

This command is used to configure the RADIUS server, add an authentication account for the authentication client. The NAS key must be in consistency with the switch key.

Note: STP must be disabled for the port before 802.1x authentication is enabled.

6.5 SNMP Configuration

SNMP configuration commands include:

- snmp
- snmp version
- snmp trap
- security-to-group
- view
- community
- host
- user

Function Description

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).

6.5.1 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

switch(config)# snmp //Enable the SNMP function of the switch.

6.5.2 snmp version

Command Description

snmp version: This command is used to configure the SNMP version.

no snmp version: This command is used to restore the default SNMP version.

Parameter

None

Default

snmp v2c

Command Mode

Global configuration mode

Example

switch(config)# snmp version v2c /Configure the SNMP version of the switch.

6.5.3 snmp trap

Command Description

snmp trap:This command is used to enable snmp trap.

no snmp trap: This command is used to disable snmp trap.

Parameter

None

Default

Disable

Command Mode

Global configuration mode

Example

switch(config)# snmp trap

6.5.4 snmp 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 community v2c 123 ro

// The version is v2c, the authentication name is 123 and the permission is read only.

6.5.5 snmp host

Command Description

snmp host host-name: This command is used to configure the host name.

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

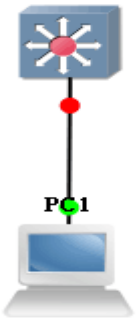
switch(config)#snmp host 1111 // It indicates that the host name is 1111.

switch(config-snmps-host)# host 192.168.111.111 // It indicates the host address.

switch(config-snmps-host)#traps switch stp //It indicates that the supported trap packet type is STP.

SNMP Configuration Example

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



switch(config)# snmp-server

switch(config)#snmp-server version v2c

switch(config)#snmp-server community v2c 123 RO

switch(config)#snmp-server community v2c 123 RW

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

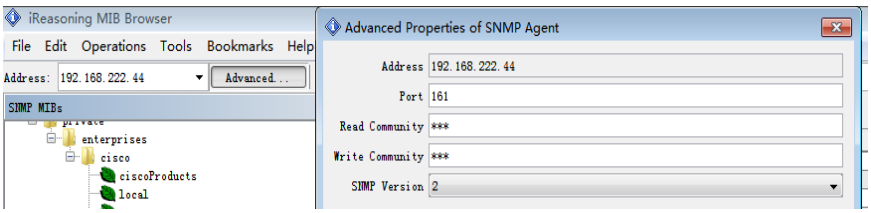
switch(config)# snmp-server host aa

switch(config-snmps-host)# no shutdown

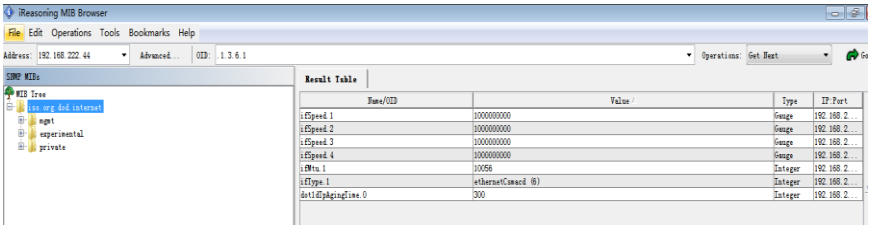
switch(config-snmps-host)# host 192.168.222.107

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

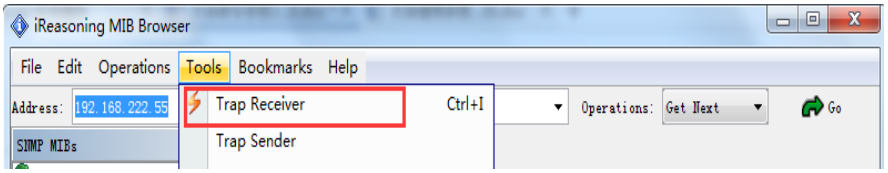
pc：Open MIB Browser on the PC and add the switch IP address and corresponding community name.



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.



6.6 RMON Configuration

RMON configuration commands include:

- rmon event
- rmon alarm
- rmon collection history <history entry ID>
- rmon collection stats <statistics entry ID>
- show rmon alarm/event/history/statistics

Function Description

Remote Monitor (RMON) is a standard monitoring specification that enables exchange of network monitoring data between various network monitors and consoles. RMON provides network administrators with more freedom in selecting consoles and network monitors that meet special network requirements. RMON implements unified remote management on a heterogeneous environment. It provides a solution for remotely monitoring a network segment through a port. Data traffic of a network segment or even the entire network can be monitored. Currently, RMON has become one of the successful network management standards.

RMON enables SNMP to monitor remote devices in a more effective and active manner. Network administrators can quickly trace faults that occur on a network, in a network segment, or on a device. With implementation of RMONMID, some network events, network performance data, and fault history can be recorded. The historical fault data can be accessed

at any time to facilitate fault diagnosis. This method reduces the traffic between the NMS and the agent, and makes it possible to manage a large-sized network in a simple and effective manner.

6.6.1 rmon event

Command Description

rmon event: This command is used to provide a table of all events generated by the RMON agent.

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

switch(config)# rmon event 111 description 111

// This command is used to set the event number to 111 and the description to 111.

switch(config)#rmon event 111 trap public

// This command is used to set the event type to **Trap** and the community name to **public**.

6.6.2 rmon collection history

Command Description

rmon collection history ｛History entry ID｝ [1-65535]

Parameter

None

Default

None

Command Mode

Interface configuration mode

Example

switch(config)# interface GigabitEthernet 1/1

switch(config-if)# rmon collection history 33 interval 200 // It indicates an entry whose number is 33 and the interval is 200s.

6.6.3 rmon alarm

Command Description

rmon alarm: This command is used to periodically monitor the specified alarm variable. An alarm is triggered when the count exceeds the threshold.

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

switch(config)#rmon alarm 12 .1.3.6.1.2.1.2.2.1.10.1 30 delta rising-threshold 10 10 falling-threshold 1 1 both

6.6.4 rmon collection stats

Command Description

rmon collection stats {Statistics entry ID} [1-65535]

Parameter

None

Default

None

Command Mode

Interface configuration mode

Example

switch(config)# interface GigabitEthernet 1/1

switch(config-if)# rmon collection stats 22 // This command is used to display statistics entries numbered 22 under Port 1.

6.6.5 show rmon alarm/ event/ history/statistics

Command Description

show rmon alarm/event/history/statistics: This command is used to display all events, historical data, and alarms generated by the RMON agent.

Parameter

None

Default

None

Command Mode

Global configuration mode

Example

switch# show rmon event 111

// This command is used to display the status of the event numbered 111.

switch# show rmon statistics

// This command is used to configure the status of all RMON events.

7 System Maintenance Commands

7.1 Restarting Equipment

The command for restarting the equipment is as follows:

- reload cold

7.1.1 reload cold

Command Description

reload cold: This command is used to restart the equipment.

Parameter

None

Default

None

Command Mode

Privileged mode

Example

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

switch# copy running-config startup-config

switch# reload cold

7.2 Restoring Factory Settings

The command for restoring factory settings is as follows:

- reload defaults

7.2.1 reload defaults

Command Description

reload defaults: 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

switch# reload defaults //Restore factory settings, and the factory settings take effect after the equipment automatically restarts.

7.3 Save Configuration

The command for save configuration is as follows:

- copy

7.3.1 copy

Command Description

copy running-config startup-config

Parameter

None

Default

None

Command Mode

Privileged mode

Example

switch#copy running-config startup-config

7.4 Ping Test

The ping test command is as follows:

- ping ip

7.4.1 ping ip

Command Description

ping ip ip_addr

Parameter

Ip_addr: It specifies the IP address, which is in the format of X.X.X.X.

Default

None

Command Mode

Privileged mode

Example

switch# ping ip 192.168.255.3 //Test whether the switch and the host are reachable from each other.