Xiamen Four-Faith Communication Technology Co.,Ltd

FNS200-Series Managed Switches CLI Manual

Contents

Chapter 1 System Status Commands

1.1 Command Mode

command description

How to enter and exit various mode states (privileged mode, global mode, interface mode, etc.)

Parameter

N/A

Default

N/A

Command mode

N/A

eg.

Switch Login: admin

password: admin（hide）

switch>

// enter user mode

switch>enable

switch#

// enter privileged mode

switch# configure terminal

switch(config)# exit

switch#

// Enter global mode, exit to exit global mode and return to privileged mode

switch# configure terminal

switch(config)# interface G1

switch(config-if)# exit

switch(config)#

// In global mode, enter G1 interface mode, exit to exit interface mode

1.2 System information

This module can query software version, compilation time, device name, device serial number, mac address, CPU utilization, memory utilization, current system time and other information.

1.2.1 show system

Command description

This command can query software version, compilation time, device name, device serial number, mac address, etc.

Parameter

N/A

Default

N/A

Command mode

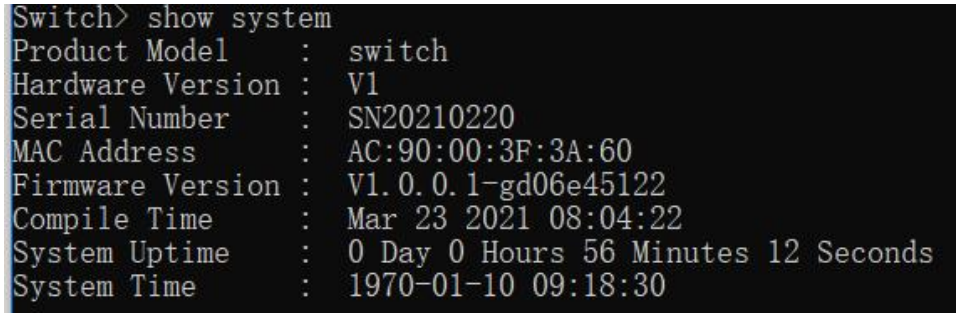
User mode (connect to the serial port, enter the device user name and password to enter the user mode, use exit to exit the current mode)

eg.

Switch Login: admin

password: admin（Password is hidden）

switch> show system



1.3 Log information

This module can view some system log information during the operation of the device, which is convenient for maintenance personnel to analyze problems.

1.3.1 show logging

Command description

View the current log information of the switch

Parameter

N/A

Default

N/A

Command mode

User mode

eg.

Switch> show logging

1.4 Port statistics

In the port statistics module, you can view the number of packets sent/received by the global port, the number of bytes, and the number of packets filtered by the port.

1.4.1 show interface

Command description

View switch port statistics

Parameter

<cr>	View statistics for all ports
G<1-24>	View statistics about 1 port

Default

N/A

Command mode

Privileged mode

eg.

switch# show interface G1

```
Switch# show interface G1
G1 is down
  Hardware address is AC-90-10-42-6A-D7
  Media type is MEDIUM_COPPER, loopback not set
  Autonegotiation enable, Flow control is off
  Speed: 1000, Duplex-half, Max frame size: 1518
  Ifindex: 0x2000001
  Port link-type: access, PVID is 1
Switch#
```

Chapter 2 System Setup Commands

2.1 IP config

IP configuration commands are：

ip address

ip address dhcp

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

show ip interface

Note: A.B.C.D/M, format example: 192.168.1.1/24

The ip configuration module can add, modify or view the interface ip information of the switch;

2.1.1 ip address

Command description

Configure the ip as A.B.C.D/M

Parameter

N/A

Default

Interface mode

Command mode

Configure this command in interface configuration mode.

eg.

switch(config)# interface eth0

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

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

2.1.2 ip address dhcp

Command description

Configure the port ip as the automatic acquisition method (the dhcp server in the network will assign a dynamic ip to the switch port)

no ip address dhcp， Indicates that the ip of the disabled interface is obtained automatically

Parameter

N/A

Default

N/A

Command mode

Configure this command in interface configuration mode.

eg.

switch(config)# interface eth0

switch(config-vif)#ip address dhcp

switch(config-vif)#no ip address dhcp

2.1.3 ip address old_ip

Command description

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

Modify the ip configuration of the interface (modify old_ip to new_ip)

Parameter

N/A

Default

N/A

Command mode

Interface mode

eg.

switch(config)# interface eth0

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

2.1.4 show interface

Command description

View the ip configuration of the interface

Parameter

N/A

Default

N/A

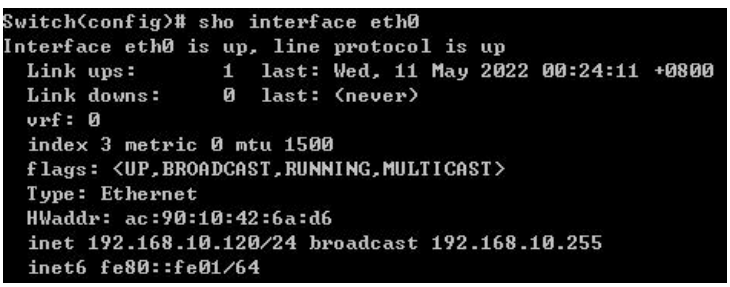
Command mode

Privileged Mode or Global Mode

eg.

switch(config)#show interface eth0

switch#show interface eth0



2.2 User config

User configuration commands are:

username

show user

Note: name means username, up to 32 characters; passwd means password, up to 32 characters;

2.2.1 username name

Command description

username name password passwd

Change a user's password

Parameter

N/A

Default

N/A

Command mode

Global mode

eg.

switch(config)#username admin password simple 123456

// Modify user: admin, password: 123456,

show user

Command description

View all current user configuration information of the switch;

Parameter

N/A

Default

N/A

Command mode

Privileged mode

eg.

Switch#show user

2.3 Time setting

The configuration commands are:

sntp enable|disable

sntp unicast-server

sntp auto-sync timer

sntp connect

sntp timezone

This feature enables the switch to automatically synchronize the network time

2.3.1 sntp enable|disable

Command description

sntp enable，enable ntp function;

sntp disable，disable ntp function;

Parameter

N/A

Default

Disable

Command mode

Global mode

eg.

switch(config)#sntp enable

switch(config)#sntp disable

2.3.2 sntp unicast-server

Command description

sntp unicast-server A.B.C.D

Configure sntp server address

no sntp unicast-server A.B.C.D,To delete an ntp server address

Parameter

N/A

Default

N/A

Command mode

Global mode

eg.

Switch(config)#sntp unicast-server 210.21.196.6

2.3.3 sntp auto-sync timer

Command description

Configure sntp synchronization interval

Parameter

sntp auto-sync timer time,The value range of time is 5-65535s, the default value is 300s;

Default

300s

Command mode

Global mode

eg.

Switch(config)#sntp auto-sync timer 5

2.3.4 sntp connect

Command description

sntp connect A.B.C.D

Use this command to select the current sntp server to connect to.

Parameter

N/A

Default

N/A

Command mode

Global mode

eg.

switch(config)#sntp connect 210.21.196.6

2.3.5 timezone

Command description

switch(config)# timezone

Use this command to select the time zone of the region where the current switch is located

Parameter

N/A

Default

0

Command mode

Global mode

eg.

switch(config)# timezone UTC-8

// Modify the time zone to UTC-8

Chapter 3 Port Configuration Commands

3.1 Port config

The port configuration commands are:

duplex

speed

flow-control

shutdown

Description

This module configures various basic parameters related to switch ports. The basic parameters of the port will directly affect the way the port works.

3.1.1 speed

Command description

speed {10-(auto/full) | 100-(auto/full/half) | 1000-(auto,full,half)|10000|auto }

Set the port speed and duplex mode

Parameter

Parameter	Directions
1000M-auto	Set the port rate to 1000M and the duplex mode to auto
1000M-full	Set the port rate to 1000M and the duplex mode to full duplex
100M-auto	Set the port rate to 100M and the duplex mode to auto
100M-full	Set the port rate to 100M and the duplex mode to full duplex
100M-half	Set the port rate to 100M and the duplex mode to half duplex
10M-auto	Set the port rate to 10M and the duplex mode to auto
10M-full	Set the port rate to 10M and the duplex mode to full duplex
10M-half	Set the port rate to 10M and the duplex mode to half duplex
auto	Set the port rate to auto-negotiation

Default

All interfaces are auto-negotiated (auto),

Command mode

Interface mode

eg.

Set the port rate of G1 to 100M full duplex.

Switch(config)# interface G1

switch(config-if)# speed 100M-full

3.1.2 flow-control

Command description

flowctrl

no flowctrl

Configure the flow control function of the port.

Parameter

N/A

Default

Disable

Command mode

Interface mode

eg.

Enable the flow control function of the port.

switch(config-if)# flowctrl

3.1.3 shutdown

Command description

shutdown

no shutdown

Configure the opening and closing of ports.

Default

Enabled

Command mode

Interface mode

eg.

Disable port

switch(config-if)# shutdown

3.1.4 description

Command description

Configure the description information of the port for easy management (composed of letters, numbers and underscores).

Default

N/A

Command mode

Interface mode

eg.

switch(config-if)# description A1

3.2 Rate limit

The rate limiting policy of the port can be configured to limit the rate of all data packets entering and leaving the port.

3.2.1 rate-limit

Command description

rate-limit {1-10000000 } {1-65535}{1-10000000 }{1-65535 }

no rate-limit

Configure the port egress/ingress rate limit function, use the no form, and the port returns to the Default setting.

Parameter

1-10000000	Port speed limit rate range 1-10000000kbps
1-65535	Port rate limit burst size range 1-65535kbits

Default

N/A

Command mode

Interface mode

eg.

The export speed limit is 10000kbps, the burst size is 1000kbits, and the entrance is not limited

switch(config-if)# rate-limit 10000 1000 0 0

3.3 Port mirroring

Port mirroring is also called port monitoring. Port monitoring is a data packet acquisition technology. By configuring the switch, the data packets of one or several ports (mirror source ports) can be copied to a specific port (mirror destination port). There is an installation on the mirror destination port. The host computer with data packet analysis software is used to analyze the collected data packets, so as to achieve the purpose of network

monitoring and troubleshooting.

3.3.1 monitor

Command description

mirror to <IFNAME>

mirror sources direction {both|egress|ingress}

no mirror

To configure the port mirroring function, use the no form of this command to delete the mirroring settings

Parameter

Parameter	Directions
IFNAME	Port number, such as G1, X1

Default

N/A

Command mode

Configuring Destination Ports in Global Configuration Mode

Configuring Source Ports in Interface Configuration Mode

eg.

Configure the destination port as G3 and the source ports as G1 and G2.

switch(config)# monitor to G3

switch(config)# interface G1

switch(config-if)# mirror source direction both

switch(config-if)#exit

switch(config)# interface G2

switch(config-if)# mirror source direction both

3.4 Link aggregation

The port static aggregation configuration commands are:

Trunk

The configuration commands for port dynamic aggregation are:

lacp enable | disable

lacp active | passive

lacp key

lacp port-priority

Link aggregation is to form multiple physical ports of a switch into a logical port, and multiple links belonging to the same aggregation group can be regarded as a larger bandwidth logical link.

Link aggregation can realize the sharing of communication traffic among the member ports in the aggregation group to increase the bandwidth. At the same time, each member port of the same aggregation group is backed up dynamically with each other, which improves the reliability of the link.

Member ports belonging to the same aggregation group must have the same configuration. These configurations mainly include STP, QoS, VLAN, port attributes, MAC address learning, ERPS configuration, loop Protect configuration, mirroring, 802.1x, IP filtering, Mac filtering, Port isolation, etc.

3.4.1 trunk

Command description

interface trunk [aggregation group ID]

Configure aggregation groups.

trunk [aggregation group ID]

Default

N/A

Command mode

Global mode

eg.

switch(config)# interface trunk 1

switch(config)# interface G1

switch(config-if)# trunk 1

3.4.2 load-balance

Command description

trunk load-balance (Set the load balancing mode for static aggregation)

Parameter

srcdst-mac	Load balancing based on source and destination mac
dst-mac	Load balancing based on destination mac
src-mac	Load balancing based on source mac

Default

Disable

Command mode

Interface mode

eg.

Set load balancing mode to source-destination mac

switch(config)# trunk load-balance both-mac

3.4.3 lacp enable | disable

Command description

lacp enable，Configuring Port Dynamic Aggregation Enable

lacp disable，Disable port Dynamic Aggregation

Parameter

N/A

Default

Disable

Command mode

Interface mode

eg.

switch(config-if)# lacp disable

3.4.4 lacp active | passive

Command description

lacp activity-mode active，*Set the port to active state*

lacp activity-mode passive，*Set the port to passive state*

Parameter

N/A

Default

Passive

Command mode

Interface mode

eg.

switch(config-if)# lacp activity-mode active

3.4.5 lacp port-key

Command description

Lacp key, which refers to the management key value of the dynamic aggregation port, is one of the identifiers that the port can add to an aggregation group. An operation key generated by the LACP protocol according to the port configuration (that is, rate, duplex, basic configuration, and management key). For a dynamic aggregation group, members of the same group must have the same operation key for successful aggregation.

Parameter

<1-65535>

Manually specify the range 1-65535;

Default

Command mode

Interface mode

eg.

switch(config)# interface G1

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

3.4.6 lacp port-priority

Command description

lacp port-priority *<1-32768>* ， Configure lacp port priority

Parameter

<1-32768> ， Priority range, the smaller the value, the higher the priority

Default

0

Command mode

Interface mode

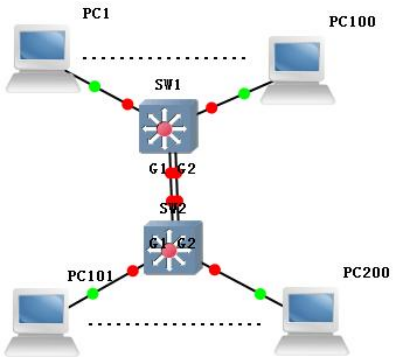
eg.

switch(config)# interface G1

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

3.4.7 example

Use link aggregation to increase device cascading port bandwidth and implement load balancing based on source and destination MAC addresses



SW1/SW2:

switch# configure terminal

switch(config)#trunk load-balance both-mac

switch(config)# interface G1

switch(config-if)# trunk 1

switch(config-if)# exit

switch(config)# interface G2

switch(config-if)# trunk 1

Phenomenon

After aggregation, the two links form a logical link, which doubles the bandwidth and performs load balancing according to the source or destination MAC address. Communication is interrupted.

Chapter 4 Advanced Configuration Commands

4.1 VLAN config

Vlan configuration commands are:

switchport mode

switchport pvid

switchport trunk|hybrid| access

show vlan

Ethernet is a shared communication medium based on CSMA/CD (Carrier Sense Multiple Access with Collision Detection) technology. A local area network built with Ethernet technology is both a collision domain and a broadcast domain. When there are a large number of hosts in the network, it will lead to serious conflicts, flooding of broadcasts, significant performance degradation, and even network unavailability. By deploying bridges or Layer 2 switches in the Ethernet, serious conflicts can be resolved, but broadcast

packets cannot be isolated. In this case, the VLAN (Virtual Local Area Network, virtual local area network) technology appears, which can divide a physical LAN into multiple logical LANs—VLANs. Hosts in the same VLAN can communicate with each other directly, but hosts in different VLANs cannot communicate with each other directly. In this way, broadcast packets are limited to the same VLAN, that is, each VLAN is a broadcast domain.

The advantages of VLAN are as follows:

1) Improve network performance. The broadcast packet is limited to the VLAN, so as to effectively control the broadcast storm of the network, save the network bandwidth, and thus improve the network processing capacity.

2) Enhance network security. Devices in different VLANs cannot access each other, and hosts in different VLANs cannot communicate directly. Packets need to be forwarded at Layer 3 through network layer devices such as routers or Layer 3 switches.

3) Simplify network management. The hosts of the same virtual workgroup are not limited to a certain physical range, which simplifies network management and facilitates the establishment of workgroups by people in different areas.

4.1.1 switchport mode

Command description

switchport mode {access | trunk | hybrid }

Configure Port Mode

Parameter

Parameter	Directions
access	access mode
trunk	trunk mode
Hybrid	hybrid mode

Default

Access mode

Command mode

Port configuration mode

The switch port supports the following modes: access mode, trunk mode, hybrid mode

Access mode means that the port belongs to only one VLAN and only sends and receives N/A tagged Ethernet frames

Trunk mode means that the port is connected to other switches and can send and receive tagged Ethernet frames

Hybrid mode means that the port can be connected to both a computer, a switch and a router (a collection of access mode and trunk mode)

eg.

Configure port in VLAN trunk mode/promiscuous mode/access mode

Switch(config)# interface G1

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

4.1.2 switchport pvid

Command description

switchport pvid { vlan-id}

Parameter

Parameter	Directions
Vlan-id	Vlan ID. Value range: 1-4094.

Default

Vlan1

Command mode

port configuration mode

This command can change the default vlan of the port

eg.

Set the default vlan of the port to vlan2

Switch(config)# interface G1

Switch(config-if)# switchport pvid 2

4.1.3 switchport trunk|hybrid| access

Command description

switchport trunk tag {vlan-id}

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

switchport access {vlan-id}

Parameter

Parameter	Directions
Vlan-id	Vlan ID, value range: 1-4094.

Default

All ports are members of vlan1 and do not belong to other vlans

Command mode

port configuration mode

This command can add port settings to one or more vlans

eg.

The following command is to add trunk mode port to one vlan or multiple vlans

switch(config)# interface G1

switch(config-if)# switchport mode trunk

switch(config-if)# switchport trunk tag 2

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

The following command is to add a hybrid mode port to one vlan or multiple vlans

switch(config-if)# switchport mode hybrid

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

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

The following command is to add the access mode port to vlan2

switch(config-if)# switchport access 2

4.1.4 show vlan

Command description

show vlan [vlan-id]

Parameter

Parameter	Directions
vlan-id	Displays the given VLAN. Value range: 1-4094.

Default

N/A

Command mode

User mode

Use Command mode

This command can view vlan members

eg.

Show all VLAN information

Switch# show vlan all

Vid Status Name Tag_port Utag_port

---

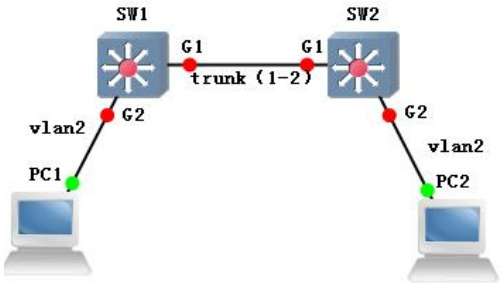
1 static vlan1 G1 G2 G3 G4 G5 G6 G7 G8 G9 G10 G11 G12 G13 G14 G15 G16 G17 G18 G19 G20 G21 G22 G23 G24 G25 G26 G27 G28

2 static vlan2

3 static vlan3

example

Realize vlan communication across switches (pc1 and pc2 can access normally)



SW1/SW2： switch# configure terminal
switch(config)# interface G1
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk tag 2
switch(config-if)# exit
switch(config)# interface G2
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 2

Phenomenon

pc1 (192.168.222.107) and pc2 (192.168.222.94) ping each other

4.2 MAC config

The configuration commands are:

mac-address aging-time

show mac-addres

The reason why the switch can directly send data packets to the destination node, instead of sending data packets to all nodes in a broadcast mode like a hub, is that the most critical technology is that the switch can identify the MAC addresses of the network cards of the nodes connected to the network, and place them. to a place called the MAC Address Table. This MAC address table is stored in the cache of the switch, and these addresses are remembered, so that when data needs to be sent to the destination address, the switch can look up the node location of this MAC address in the MAC address table, and then directly to this location sent by the node. The so-called number of MAC addresses refers to the maximum number of MAC addresses that can be stored in the MAC address table of the switch. The greater

the number of stored MAC addresses, the higher the speed and efficiency of data forwarding.

4.2.1 mac-address aging-time

Command description

mac-address aging-time {10-1000000}

no mac-address aging-time

Configure the Mac aging time, use the no form of this command to restore the default setting

Parameter

Parameter	Directions
time	MAC address aging time in seconds.

Default

300

Command mode

Global configuration mode

Use Command mode

Configuring the aging time of mac addresses in global configuration mode

eg.

Configure the MAC address aging time to 100 seconds

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

Restore the MAC address aging time to the default 300 seconds

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

4.2.2 show mac-address

Command description

show mac-addres{ aging-time}

Parameter

N/A

Default

N/A

Command mode

User mode or global mode

Use Command mode

After using this command, you can view the aging time of the mac address and mac address

eg.

The following command can check the aging time of mac address and mac address

switch# show mac-address

MAC	Vlan	Port	Type
94-de-80-dc-cf-38	1	G4	dynamic
60-92-17-9d-30-c3	1	G4	dynamic

Switch# show mac-address aging-time

Mac address aging-time : 100

4.3 ARP config

The configuration commands are:

show arp

arp static

arp timeout

This function module can view the arp entry information learned by the switch, add static arp entries to prevent illegal host access, and modify the aging time of arp entries.

4.3.1 show arp

Command description

show arp

If you want to view dynamic ARP entries, you can use this command.

Parameter

N/A

Default

N/A

Command mode

Configure this command in global configuration mode

eg.

Check dynamic ARP entries.

Switch(config)# show arp

4.3.2 arp static

Command description

arp static ip_addr mac_addr

no arp static ip_addr

If you want to add static ARP, you can configure it through this command. Use the no form of this command to cancel this configuration.

Parameter

Parameter	Directions
ip_addr	IP address, the value range is X.X.X.X.
mac_addr	mac address, value range: H.H.H

Default

N/A

Command mode

Global configuration mode.

eg.

Add static ARP entry

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

4.3.3 arp timeout

Command description

arp timeout seconds

no arp timeout

If you want to set the ARP aging time, you can use this command to configure it. Use the no form of this command to cancel this configuration.

Parameter

Parameter	Directions
seconds	Unit: second, the value range is 1-2147483.

Default

N/A

Command mode

Interface mode

eg.

Set the ARP aging time to 3000 seconds.

switch(config)# interface eth0

switch(config-vlanif1)# arp timeout 3000

4.4 MSTP config

The configuration commands are:

spanning-tree

spanning-tree mode

spanning-tree max-age

spanning-tree hello-time

spanning-tree forward-delay

spanning-tree max-hop

spanning-tree instance

show spanning-tree

show spanning-tree interface brief

STP (Spanning Tree Protocol, Spanning Tree Protocol) is a protocol established according to the IEEE 802.1D standard for eliminating physical loops at the data link layer in a local area network. Devices running this protocol discover loops in the network by exchanging information with each other, selectively block certain ports, and finally prune the loop network structure into a tree structure of N/A loops, thereby preventing packets In the loop network, the number of loops and N/A limit loops are constantly increased, so as to avoid the problem that the packet processing capability is reduced due to the repeated reception of the same packet by the device.

4.4.1 spanning-tree

Command description

spanning-tree

no spanning-tree

To configure the STP enable setting, use the no form of this command to disable STP.

Parameter

N/A

Default

Disable

Command mode

Global mode

eg.

switch(config)# spanning-tree

switch(config)# no spanning-tree

4.4.2 spanning-tree mode

Command description

spanning-tree mode {stp|rstp|mstp}

Parameter

Stp	Enable STP mode
rstp	Enable RSTP mode
mstp	Enable MSTP mode

Default

Default enable STP mode

Command mode

Global mode

Use Command mode

Configure spanning-tree operation mode

eg.

The following command will enable RSTP mode:

switch(config)# spanning-tree mode rstp

4.4.3 spanning-tree max-age

Command description

spanning-tree max-age {6-40}

Parameter

seconds	BPDU maximum lifetime. Value range: 6-40s.

Default

20s

Command mode

Global mode

Use Command mode

Configure the maximum time to live for STP BPDUs

eg.

The following command will configure the maximum time-to-live for STP to 24 seconds:

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

4.4.4 spanning-tree hello-time

Command description

spanning-tree hello-time { 1-10 }

Parameter

Time	Interval for sending hello packets, value range: 1-10s.

Default

2s

Command mode

Global configuration mode

eg.

The following command will configure the interval for sending STP hello packets to 10 seconds:

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

4.4.5 spanning-tree forward-delay

Command description

spanning-tree forward-delay { 4-30 }

Parameter

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

Default

15 seconds

Command mode

Global configuration mode

eg.

The following command will configure the STP forwarding delay to 20 seconds:

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

4.4.6 spanning-tree max-hop

Command description

spanning-tree max-hop { 1-40 }

Parameter

Hop count	The maximum number of hops valid for a BPDU protocol packet. Value range: 1-40.

Default

20

Command mode

Global configuration mode

eg.

The following command will configure the maximum number of hops valid for BPDU protocol packets to be 40:

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

4.4.7 spanning-tree instance

Command description

spanning-tree instance configures the mapping relationship between MSTP vlan and instance

Parameter

N/A

Default

N/A

Command mode

Global configuration mode

eg.

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

4.4.8 spanning-tree mstp name

Command description

spanning-tree mstp name, Configure the domain name of mstp

Parameter

N/A

Default

N/A

Command mode

Global configuration mode

eg.

switch(config)# spanning-tree mstp name 2

4.4.9 spanning-tree mstp revision

Command description

spanning-tree mstp revision ,Configure the revision number of mstp

Parameter

N/A

Default

N/A

Command mode

Global configuration mode

eg.

switch(config)# spanning-tree mstp revision 2

4.4.10 show spanning-tree

Command description

show spanning-tree

Parameter

N/A

Default

N/A

Command mode

Privileged Mode/Global Mode

Use Command mode

After using this command, can view mstp information

eg.

The following command can view mstp information:

switch# show spanning-tree

Spanning-tree is disable:

max age 20 bridge forward delay 20

forward delay 15 max hops 20

hello time 2 orce protocol version mstp

4.4.11 show spanning-tree interface brief

Command description

show spanning-tree interface brief

Parameter

N/A

Default

N/A

Command mode

Privileged Mode/Global Mode

Use Command mode

After using this command, you can view mstp information

eg. switch(config)# show spanning-tree interface brief

```
Switch# show spanning-tree interface brief
MSTID Port        Role              State
--------------------------------------------
0     G1          Disabled          forwarding
0     G2          Disabled          forwarding
0     G3          Disabled          forwarding
0     G4          Disabled          forwarding
0     G5          Disabled          forwarding
0     G6          Disabled          forwarding
0     G7          Disabled          forwarding
0     G8          Disabled          forwarding
0     G9          Disabled          forwarding
0     G10         Disabled          forwarding
```

4.5 IGMP-snooping

The configuration commands are:

igmp-snooping

igmp-snooping host-age-time

igmp-snooping fast-leave

igmp-snooping static-group

show igmp-snooping group

IGMP Snooping is the abbreviation of Internet Group Management Protocol Snooping (Internet Group Management Protocol Snooping). It is a multicast constraint mechanism running on Layer 2 devices to manage and control multicast groups.

4.5.1 igmp-snooping

Command description

igmp-snooping

no igmp-snooping

Configure to enable the IGMP snooping function, use the no form of this command to disable this function.

Parameter

N/A

Default

Disable

Command mode

Global mode

eg.

The following commands will configure eanble and disable

igmp-snooping：

Switch(config)# igmp-snooping

Switch(config)#no igmp-snooping

4.5.2 igmp-snooping host-age-time

Command description

igmp-snooping host-age-time｛200-1000｝

Parameter

Parameter	Directions
time	Host aging time. Value range: 200-1000s.

Default

300

Use Command mode

Configure the host aging time

Command mode

Global configuration mode

eg.

The following command will configure the host aging time to 200s:

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

4.5.3 igmp-snooping fast-leave

Command description

igmp-snooping fast-leave

no igmp-snooping fast-leave

Configure to enable the port fast leave function, and use the no form of this command to disable this function.

Parameter

N/A

Default

Disable

Command mode

Interface mode

eg.

switch(config)# vlan 1

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

4.5.4 igmp-snooping static-group

Command description

igmp-snooping static-group, Add static multicast group

no igmp-snooping static-group, Delete an added static multicast group

Parameter

N/A

Default

Disable

Command mode

Interface mode

eg.

switch(config)# interface G1

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

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

4.5.5 show igmp-snooping group

Command description

show igmp-snooping group

Parameter

N/A

Default

N/A

Command mode

User mode

eg.

The following command will view multicast group information:

switch# show igmp-snooping group

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

4.6 DHCP snooping

Command description:

dhcp-snooping

4.6.1 dhcp-snooping

Command description

dhcp-snooping

no dhcp-snooping

To enable the DHCP snooping function, use the no form of this command to disable this function

Parameter

N/A

Default

Disable

Command mode

Global mode

eg.

N/A

4.6.2 dhcp-snooping

Command description

dhcp-snooping untrust

no dhcp-snooping untrust

To set the port mode to untrust, use the no form of this command to configure the port mode to trust.

Parameter

N/A

Default

untrust

Command mode

Interface mode

eg.

Set the mode of port 1 to trust

Switch(config-if)# no dhcp-snooping untrust

4.6.3 show dhcp-snooping

Command description

show dhcp-snooping

Parameter

N/A

Default

N/A

Command mode

Privileged mode

eg.

switch# show dhcp-snooping

4.7 QoS config

Command description:

qos

cos default

cos map

dscp map

scheduler police

Function introduction

QoS (Quality of Service) refers to a network that can use various basic technologies to provide better service capabilities for specified network communications. It is a security mechanism of the network and is used to solve problems such as network delay and congestion. a technology. Under normal circumstances, if the network is only used for a specific N/A time-limited application system, QoS is not required, such as Web applications, or E-mail settings. But it is necessary for critical applications and multimedia applications. When the network is overloaded or congested, QoS ensures that important traffic is not delayed or dropped, while maintaining the efficient operation of the network.

4.7.1 QOS

Command description

Qos remask<all/cos/dscp>

Change QoS Trust Mode Weight.

Parameter

N/A

Default

cos

Command mode

Interface mode

eg.

Modify the qos trust mode of the optimal G1 port to dscp

switch(config)# interface G1

switch(config-if)# qos trust dscp

4.7.2 cos default

Command description

cos default<0-7>

Parameter

N/A

Default

0

Command mode

Interface mode

eg.

Modify the default cos priority of the G1 port

switch(config)# interface g1

switch(config-if)# cos default 6

4.7.3 cos map

Command description

cos map

Set the mapping relationship between cos priority and queue

Parameter

N/A

Default

One-to-one mapping between priorities and queues

Command mode

Global mode

eg.

Map cos priority 0 to queue 3

switch(config)# cos map 0 3

4.7.4 dscp map

Command description

dscp map

Set the mapping relationship between dscp priority and cos priority

Parameter

N/A

Default

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

Command mode

global mode

eg.

Map dscp priority 45 to cos priority 7

switch(config)# dscp map 45 7 7

4.7.5 scheduler policy

Command description

scheduler police

Set QoS scheduling algorithm

Parameter

sp	Strict priority mode: the queue with the highest priority is served first until the priority is empty, then the queue with the next highest priority is served, and so on.
wrr	Weighted round robin scheduling algorithm: supports different bandwidth requirements, and can allocate different proportions

	of output bandwidth to different queues.

Default

sp

Command mode

Global mode

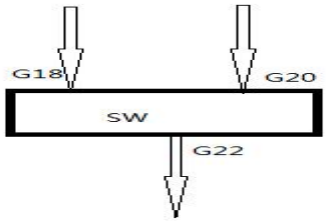
eg.

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

4.7.6 example

Test topology (test port-based QoS)

The 1-3 ports of the Ixia tester correspond to the G18-G22 of the switch respectively



（一）configuration

// When the data packet of the ingress port does not carry any priority flag, it will enter the corresponding queue with the priority set by the port.

Set the priority of 7 to the data packets entering port 18 of the switch, and the priority of 6 to the data packets of port 20.

switch(config)#interface G18

switch(config-if)cos default 7

switch(config-if)no qos trust

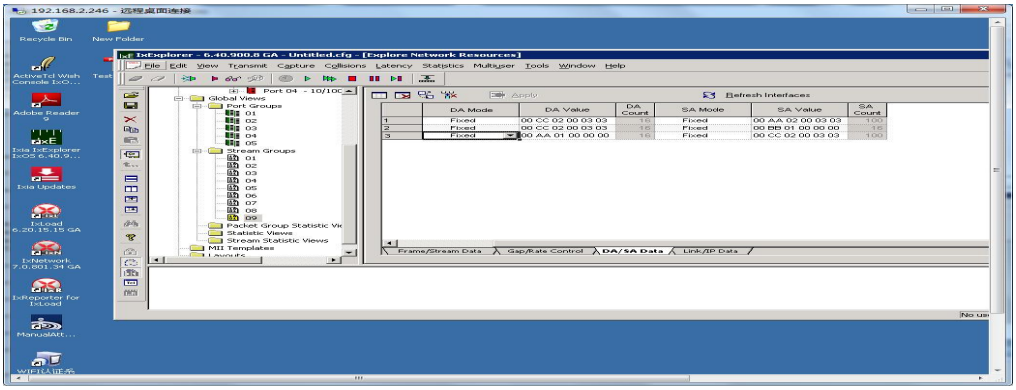
switch(config-if)exit

switch(config)#interface G20

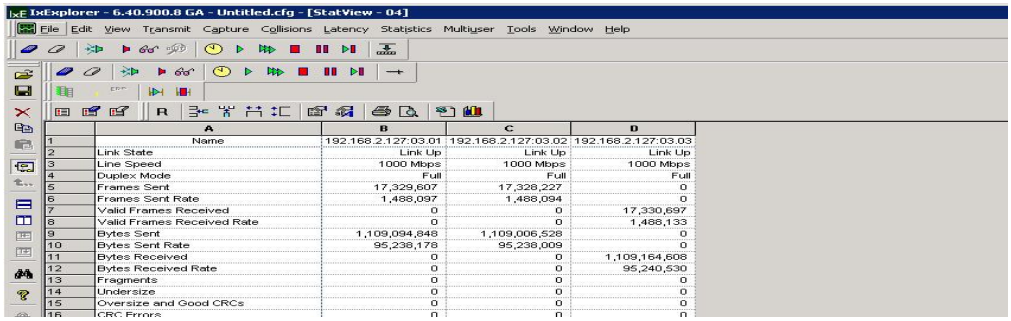
switch(config-if)cos default 6

switch(config-if)no qos trust

b、Set the destination address of Ixia1-2 to Ixia3



c、After learning the MAC address, start the packet sending action of 1-2 ports



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

（二）Test Results

Result：pass

Capture the packet on port 3 and observe the original MAC address. You can see that the received packet is from the packet with the highest priority queue on port 1.

Chapter 5 Network Security Commands

5.1 Anti-attack

Command descriptio：

system ignore icmp-echo

system protection syn-ack

system rate-limit

function Introduction

The anti-attack configuration is used to ignore the ICMP request of the device, defend against the TCP SYN attack to the device, and control the threshold value of the data received by the CPU.

5.1.1 system ignore icmp-echo

Command description

If you want to ignore ICMP requests destined for this device, you can use this command to configure. Use the no form of this command to cancel this configuration.

system ignore icmp-echo

no system ignore icmp-echo

Parameter

N/A

Default

N/A

Command mode

Global configuration mode.

eg.

Configure to ignore ICMP requests destined for this device.

switch(config)# system ignore icmp-echo

5.1.2 system protection ddos

Command description

If you want to defend against ddos attacks on the device, you can configure it through this command. Use the no form of this command to cancel this configuration.

system protection ddos

no system protection ddos

Parameter

N/A

Default

N/A

Command mode

Global mode

eg.

Configure defense against ddos attacks on the device

switch(config)# system protection ddos

5.1.3 system rate-limit

Command description

If you want to control the threshold of CPU receiving data, you can configure it through this command. Use the no form of this command to cancel this configuration.

system rate-limit value

no system rate-limit

Parameter

parameter	Directions
value	<0-100000> pps , Default value 0:disable limited。

Default

N/A

Command mode

Global mode

eg.

Configure the threshold for the CPU to receive data as 1000.

switch(config)# system rate-limit 1000

Disable the threshold control function of the CPU receiving data

switch(config)# no system rate-limit

5.2 MAC binding

Command description:

mac-address static

5.2.1 mac-address static

Command description

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

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

If you want to add a static MAC address, you can configure it through this command. Use the no form of this command to cancel this configuration.

Parameter

Parameter	Directions
mac-addr	MAC address. Value range: H.H.H.
vlan-id	The VLAN to which the MAC address belongs. Value range: 1-4094.
interface-id	The physical port to which the MAC address belongs.

Default

N/A

Command mode

global configuration mode.

eg.

Configure the MAC address 00-00-0 0-00-00-01 to be bound to port

G10 belonging to VLAN2.

switch(config)# mac-address static 00-00-00-00-00-01 vlan 2 interface G10

5.3 ARP binding

Command description:

arp

function Introduction

In order to better manage the computers in the network, you can use the ARP binding function to control the access (IP binding) between the computers in the network.)

5.3.1 arp static

Command description

arp static

Parameter

N/A

Default

N/A

Command mode

Global configuration mode.

eg.

switch(config)# arp static 192.168.1.1 50-46-5D-E2-D5-50

5.3.2 show arp

Command description:

View the binding of the arp address

show arp

Parameter

N/A

Default

N/A

Command mode

Privileged configuration mode.

eg.

Show ARP binding list

switch(config)# show arp

5.4 ACL config

Command description:

mac acl

ip acl

rule

ip/mac access-group

function Introduction

The Access Control List (ACL) is used to control the data packets entering and leaving the port.

The communication between information points and the communication between internal and external networks are essential business requirements in the enterprise network. In order to ensure the security of the internal network, it is necessary to use security policies to ensure that unauthorized users can only access specific network resources, so as to achieve access to specific network resources. purpose of control. In short, ACL can filter traffic in the network and is a network technical means to control access.

After configuring an ACL, you can restrict network traffic, allow access to specific devices, specify to forward packets on specific ports, and so on. For example, ACL can be configured to prohibit devices in the LAN from accessing the external public network, or only FTP service can be used. ACLs can be configured on routers or service software with the ACL function.

ACL is an important technology to ensure system security in the Internet of Things. Based on the security of the device hardware layer, it controls the communication between devices at the software layer and uses programmable methods to specify access rules to prevent illegal devices from destroying system security. Get system data.

5.4.1 mac acl

Command description

mac acl <1-99>

no mac acl <1-99>

If you want to add a mac acl group, you can configure it through this

command. Use the no form of the command to delete the group.

Parameter

Parameter	Directions
<1-99>	mac acl group number, range: 1-99

Default

N/A

Command mode

Global mode

After using this command, you can add a mac acl group

eg.

switch(config)#mac acl 1

5.4.2 ip acl

Command description

ip acl <100-999>

no ip acl <100-999>

If you want to add an ip acl group, you can configure it through this command. Use the no form of the command to delete the group.

Parameter

Parameter	Directions
<100-999>	ip acl group number, range: 100-999

Default

N/A

Command mode

Global mode

eg.

switch(config)#ip acl 100

5.4.3 rule

Command description

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

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

no rulel <1-127>

If you want to add an acl rule, you can configure it through this command. Use the no form of the command to delete the group.

Parameter

Parameter	Directions
<1-127>	Rule number, range: 1-127
source mac	Source mac address, any means any
destination mac	Destination mac address, any means any
1-4094	vlan number, range: 1-4094
ETHTYPE	Ether type, the range is 0x0000-0xFFFF; 0x0000 or not filled means it does not match the Ether type field,
source ip	Source IP address, any means any
destination ip	Destination IP address, any means any
<0-7>	IP precedence to match, range 0-7
<0-15>	TOS to match, range 0-15
<0-63>	DSCP to match, range 0-63

Default

N/A

Command mode

Global mode

After using this command, you can add an acl rule

eg.

Add a rule 1 of mac acl 1

switch(config)#mac acl 1

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

5.4.4 ip/mac access-group

Command description

ip access-group <100-999>

no ip access-group <100-999>

mac access-group <1-99>

no mac access-group <1-99>

After using this command, you can bind the acl rules used by the port

Parameter

Parameter	Directions
<100-999>	ip acl group number, range: 100-999
<1-99>	mac acl group number, range: 1-99

Default

N/A

Command mode

Interface mode

eg.

Switch(config-if)# ip access-group <100-999>

5.5 802.1X config

Command description:

dot1x auth-port system-auth-ctrl

dot1x initialize interface IFNAME

dot1x radius-client source-interface HOSTNAME PORT

dot1x radius-server deadtime MIN

dot1x radius-server host HOSTNAME auth-port PORTNO key STRING retransmit RETRIES timeout SEC

dot1x re-authenticate interface IFNAME

function Introduction

The 802.1x protocol is an access control and authentication protocol based on Client/Server. It can restrict unauthorized users/devices from accessing LAN/WLAN through the access port. 802.1x authenticates users/devices connected to a switch port before obtaining various services provided by the switch or LAN. Before passing the authentication, 802.1x only allows EAPoL (Extensible Authentication Protocol over Local Area Network) data to pass through the switch port connected to the device; after passing the authentication, normal data can pass through the Ethernet port smoothly.

5.5.1 dot1x auth-port system-auth-ctrl

Command description

dot1x auth-port system-auth-ctrl

no dot1x auth-port system-auth-ctrl

Enable and disable the port-based Dot1x function.

Parameter

N/A

Default

N/A

Command mode

Global mode

After using this command, you can enable the 802.1X function, and use the no form of this command to disable this function.

eg.

switch(config)# dot1x auth-port system-auth-ctrl

5.5.2 dot1x initialize interface IFNAME

Command description

dot1x initialize interface IFNAME

Initializes 802.1X authentication for the port.

Parameter

Parameter	Directions
IFNAME	Specify the interface name, such as G1, X1, etc.

Default

N/A

Command mode

Global mode

After using this command, the initial session is authenticated, and the connected session will be disconnected.

eg.

switch(config)# dot1x initialize interface G1

5.5.3 dot1x radius-client source-interface HOSTNAME PORT

Command description

dot1x radius-client source-interface HOSTNAME PORT

Parameter

Parameter	Directions
HOSTNAME	RADIUS client (hostname or IP)
PORT	Client port number (default 1812)

Default

N/A

Command mode

Global mode

After using this command, you can set the IP and port number of the radius client

eg.

Switch(config)#dot1x radius-client source-interface 192.168.200.200 1812

5.5.4 dot1x radius-server deadtime MIN

Command description

dot1x radius-server deadtime MIN

Configure the IP address of the accounting server and the IP address and secret key of the backup server

Parameter

Parameter	Directions
MIN	RADIUS server death time (in minutes) <0-1440>, default is 0

Default

N/A

Command mode

Global mode

After using this command, you can set the death time of the Radius server

eg.

switch(config)# dot1x radius-server deadtime 5

5.5.5 dot1x radius-server

Command description

dot1x radius-server host HOSTNAME auth-port PORTNO key STRING retransmit RETRIES timeout SEC

Configure the update interval/maintain authentication time of the authentication server.

Parameter

Parameter	Directions
HOSTNAME	RADIUS server (hostname or IP)
PORTNO	Radius server port number (default 1812)
STRING	RADIUS server keystring
RETRIES	Number of retransmissions (range 1-100)
SEC	RADIUS server timeout (in seconds) <1-1000>

Default

N/A

Command mode

Global mode

After using this command, you can set the parameters related to the Radius server

eg.

switch(config)#Dot1x radius-server host 192.168.200.1 auth-port 1812 key 123456 retransmit 3 timeout 5

5.5.6 dot1x re-authenticate

Command description

dot1x re-authenticate interface IFNAME

Manually re-authenticate the specified port.

Parameter

IFNAME	Specify the interface name, such as G1, X1, etc.

Default

N/A

Command mode

Global mode

After using this command, re-authenticate the specified port

eg.

Configure re-authentication on port G1

Switch(config)# dot1x re-authenticate interface

5.5.7 dot1x initialize

Command description

dot1x initialize

Initialize the specified port, i.e. disable the port and try to re-authenticate

Parameter

N/A

Default

N/A

Command mode

Interface mode

After using this command, re-authenticate the specified port

eg.

Port G1 initialization

Switch(config)# interface G1

Switch(config-if)# dot1x initialize

5.5.8 dot1x keytxenabled

Command description

dot1x keytxenabled enable/disable

Enable/disable the password transmission switch for the specified port.

Parameter

N/A

Default

N/A

Command mode

Interface mode

After using this command, enable the password transmission switch of the specified port

eg.

Port G1 initialization

Switch(config)# interface G1

Switch(config-if)# dot1x keytxenabled enable

5.5.9 dot1x port-control

Command description

dot1x port-control auto

dot1x port-control dir both/in

dot1x port-control force-authorized

dot1x port-control unforce-authorized

Configure the authentication mode of the specified port

Parameter

N/A

Default

N/A

Command mode

Interface mode

Use this command to set the authentication mode of the specified port

eg.

Configure the G1 port authentication mode to be automatic and the control direction to be bidirectional

Switch(config)# interface G1

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

Switch(config-if)# dot1x port-control dir both

5.5.10 dot1x protocol-version

Command description

dot1x protocol-version 1/2

Configure the authentication protocol version of the specified port, the default is 2.

Parameter

N/A

Default

N/A

Command mode

Interface mode

Use this command to set the authentication protocol version of the specified port

eg.

Configure the G1 port authentication protocol version to 1

Switch(config)# interface G1

Switch(config-if)#dot1x protocol-version 1

5.5.11 dot1x quiet-period

Command description

dot1x quiet-period <1-65535>

The time to be in the N/A prompt state after the authentication fails, the default is 60s

Parameter

N/A

Default

N/A

Command mode

Interface mode

Use this command to set the time in the N/A prompt state after authentication failure

eg.

Configure the silent time of the G1 port to 60s

Switch(config)# interface G1

Switch(config-if)#dot1x quiet-period 60

5.5.12 dot1x re-authenticate

Command description

dot1x re-authenticate

Re-authenticate the specified port.

Parameter

N/A

Default

N/A

Command mode

Interface mode

Use this command to re-authenticate the specified port

eg.

Configure G1 re-authentication

Switch(config)# interface G1

Switch(config-if)#dot1x re-authenticate

5.5.13 dot1x reauthMax

Command description

dot1x reauthMax <1-10>

Number of reauthentication attempts before authorization (default 2).

Parameter

N/A

Default

N/A

Command mode

Interface mode

Use this command to set the number of re-authentication attempts before the specified port is unauthorized

eg.

Configure the number of re-authentications for G1 to 5

Switch(config)# interface G1

Switch(config-if)#dot1x reauthMax 5

5.5.14 dot1x reauthentication

Command description

dot1x reauthentication

To enable re-authentication on the specified port, add the no command in front to disable it.

Parameter

N/A

Default

N/A

Command mode

Interface mode

Use this command to set the specified port re-authentication switch

eg.

Enable G1 re-authentication

Switch(config)# interface G1

Switch(config-if)#dot1x reauthentication

5.5.15 dot1x timeout

Command description

dot1x timeout re-authperiod <1-4294967295>

seconds between reauthorization attempts (default 3600 seconds)

dot1x timeout server-timeout <1-65535>

Authentication server response timeout (default 30 seconds)

dot1x timeout supp-timeout <1-65535>

Requester response timeout (default 30 seconds)

dot1x timeout tx-period <1-65535>

The number of seconds between consecutive request id attempts (default 30 seconds)

Parameter

N/A

Default

N/A

Command mode

Interface mode

Use this command to set the timeout period

eg.

N/A

5.6 Port isolation

Command description

switchport protected

function Introduction

Port isolation is to achieve Layer 2 isolation between packets. Different ports can be added to different VLANs, but limited VLAN resources will be wasted. With the port isolation feature, isolation between ports in the same VLAN can be achieved. Users only need to add ports to the isolation group to achieve Layer 2 data isolation between ports in the isolation group. The port isolation function provides users with a safer and more flexible networking solution.

5.6.1 switchport protected

Command description

switchport protected

no switchport protected

If you want to configure port isolation, you can configure it through this command. Use the no form of this command to cancel this configuration.

Parameter

N/A

Default

N/A

eg.

Configure G1 port isolation.

switch(config)# interface G1

switch(config-if)# switchport protected

5.7 Storm control

Command description:

storm-control broadcast pps

storm-control multicast pps

storm-control unicast pps

function Introduction

Storm suppression means that users can limit the amount of broadcast traffic that is allowed to be received on a port. When this type of

traffic exceeds the threshold set by the user, the system will discard the data frames that exceed the traffic limit to prevent the occurrence of storms and ensure the normal operation of the network.

5.7.1 storm-control broadcast pps

Command description

storm-control broadcast pps vlaue

no storm-control broadcast

If you want to suppress the broadcast packets of the port, you can use this command to configure. Use the no form of this command to cancel this configuration.

Parameter

Parameter	Directions
Value	Value range: 0-1000000 unit pps, the default value is 0, which means no suppression.

Default

N/A

Command mode

Interface mode

eg.

Suppress the rate of broadcast packets on port G1 to 1000pps.

switch(config)# interface G1

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

5.7.2 storm-control multicast pps

Command description

storm-control multicast pps vlaue

no storm-control multicast

If you want to suppress the multicast packets of the port, you can use this command to configure. Use the no form of this command to cancel this configuration.

Parameter

Parameter	Directions
value	Value range: 0-1000000 unit pps, the default value is 0, which means no suppression.

Default

N/A

Command mode

Interface mode

eg.

Suppress the rate of multicast packets on port G1 to 1000pps.

switch(config)# interface G1

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

5.7.3 storm-control unicast pps

Command description

storm-control unicast pps vlaue

no storm-control unicast

If you want to suppress the unicast packets of the port, you can use this command to configure. Use the no form of this command to cancel this configuration.

Parameter

Parameter	Directions
value	Value range: 0-1000000 unit pps, the default value is 0, which means no suppression.

Default

N/A

Command mode

Interface mode

eg.

Value range: 0-1000000 unit pps, the default value is 0, which means no suppression.

switch(config)# interface G1

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

5.8 ERPS config

Function Introduction

ERPS (Ethernet Ring Protection Switching): Ethernet multi-ring protection technology, the protocol standard is the ITU-TG.8032 multi-ring standard. ERPS pursues higher performance and more security, which is the permanent development direction of the network. The Ethernet ring network technology has become an important redundancy protection method in the Layer 2 network.

In the Layer 2 network, the STP protocol is generally used for

network reliability, as well as the loop protection protocol mentioned in the previous section. The STP protocol is a standard ring network protection protocol developed by IEEE and has been widely used. The application is limited by the size of the network, and the convergence time is affected by the network topology. Generally, the convergence time of STP is in the second level. When the network diameter is large, the convergence time is longer. Although RSTP/MSTP can reduce the convergence time to the millisecond level, it still cannot meet the requirements for services with high service quality requirements such as 3G/NGN voice. In order to shorten the convergence time and eliminate the influence of network size, the ERPS protocol came into being.

ERPS is a link layer protocol specially applied to the Ethernet ring. It can prevent the broadcast storm caused by the data loop in the Ethernet ring; when a link on the Ethernet ring is disconnected, it can quickly enable the backup link to Communication between nodes on the ring network is restored. Compared with the STP protocol, the ERPS protocol has the characteristics of fast topology convergence speed (less than 20ms) and the convergence time is related to the number of nodes on the ring N/A.

5.8.1 erps

Command description

Erps enable/disable

Parameter

N/A

Default

Disable

Command mode

Global mode

After using this command, you can perform Global mode on erps

eg.

Switch(config)# erps enable

Switch(config)# erps disable

5.8.2 erps xx

Command description

erps physical-ring Ring ID east-interface PORT(A) west-interface

PORT(B)

erps instance Instance ID

ring type major-ring/sub-ring

raps-cannel-vlan VLAN ID

node-role owner/neighbour/normal/interconnection

data-traffic-vlan reference-stg STG ID

Parameter

Parameter	Directions
Ring ID	1-255
PORT(A)	any port
PORT(B)	Except for the ports filled in above
Instance ID	1-64
VLAN ID	Protocol vlan, range 2-4094, cannot be duplicated with business vlan
node-role	There is one and only one Owner node in an ERPS ring
STG ID	business vlan instance

Default

Dsiable

Command mode

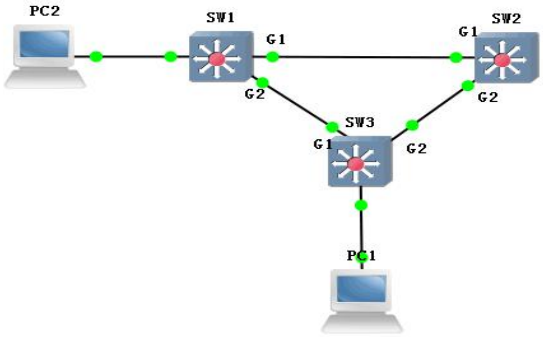
Global mode

5.8.3 example

Three devices group erps ring, set G1 on sw1 as the main port (responsible for controlling the forwarding state, that is, this port will be blocked when there is a loop)

During the loop, pc1 and pc2 access normally

When other links other than the link where the blocked port is located fails, erps can achieve faster switching



sw1：switch(config)#erps enable

switch(config)#erps physical-ring 1 east-interface G1 west-interface G2

swtich(config)#erps instance 1

swtich(config-erps-instance)#physical-ring 1

swtich(config-erps-instance)#ring-type major-ring

swtich(config-erps-instance)#node-role owner east-interface

swtich(config-erps-instance)#raps-channel-vlan 3001

swtich(config-erps-instance)#data-traffic-vlan reference-stg 0

swtich(config-erps-instance)#erps enable

sw2/sw3：switch(config)#erps enable

switch(config)#erps physical-ring 1 east-interface G1 west-interface G2

swtich(config)#erps instance 1

swtich(config-erps-instance)#physical-ring 1

swtich(config-erps-instance)#ring-type major-ring

swtich(config-erps-instance)#node-role normal

swtich(config-erps-instance)#raps-channel-vlan 3001

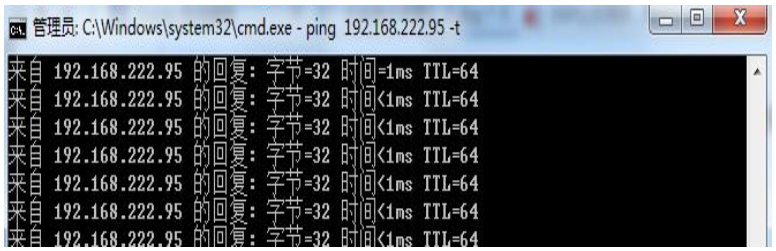
swtich(config-erps-instance)#data-traffic-vlan reference-stg 0

swtich(config-erps-instance)#erps enable

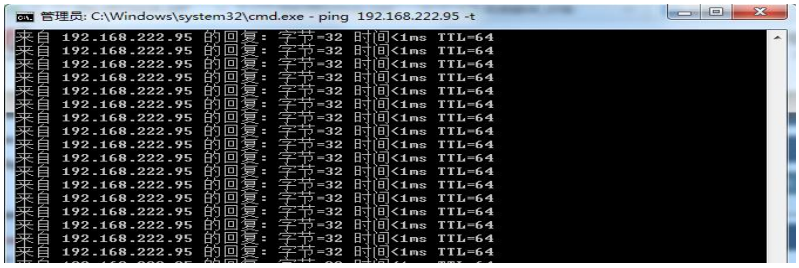
Phenomenon

Block G1 port on SW1

pc1（192.168.222.107） ping pc2（192.168.222.95）



Manually cut off the link other than the link where the blocked port is located, which can realize fast switchover without interruption of ping



5.9 IP source guard

Command description:

ip source-guard

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

ip dhcp-snooping binding

function Introduction

Through the IP source protection function, you can filter and control the packets forwarded by the port to prevent illegal packets from passing through the port, thereby restricting the illegal use of network resources (such as illegal hosts imitating legitimate users' IP access to the network), and improving the port's security. Safety.

If the port of the switch is configured with IP source protection, when a packet arrives at the port, the device will check the IP source protection entry, and the packet that conforms to the entry can be forwarded or enter the subsequent process, and the packet that does not conform to the entry can be forwarded. will be discarded. The binding function is for ports. After a port is bound, only the port is restricted, and other ports are not affected by the binding.

5.9.1 ip source-guard

Command description

ip source-guard

no ip source-guard

Configure to enable IP source protection function, use the no form of this command to disable this function

Parameter

N/A

Default

Disable

Command mode

Global mode

After using this command, you can enable the IP source protection function

eg.

Switch(config)#Ip source-guard

5.9.2 ip source-guard trust

Command description

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

no ip ip source-guard trust

Parameter

Parameter	Directions
0/1/2/3	The maximum number of dynamic clients is 0/1/2, 3 means N/A limit

Default

Disable

Command mode

Interface mode

After using this command, you can enable the port IP source protection function, and use the no form of this command to restore the default value of the port.

eg.

Switch(config-if)#Ip source-guard trust 1

5.9.3 ip dhcp-snooping binding

Command description

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

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

Parameter

Parameter	Directions

MAC	Statically bound MAC address
VLANID	Statically bound VLAN number
A.B.C.D	Statically bound IP address
Msak	The mask of the statically bound IP address
IFNAME	The port number

Default

N/A

Command mode

User mode

After using this command, you can enable the IP source protection static binding function, and use the no form of this command to release the binding.

eg.

switch(config)#ip dhcp-snooping binding 40-50-11-11-11-11 vlan 1 ip 192.168.1.1 mask 255.255.255.0 interface G1

Chapter 6 Network Management Commands

6.1 HTTP config

Command description:

ip http-server http

ip http-server https

Function Introduction

HTTP configuration commands are described. This command can configure the switch to accept HTTP/HTTPS service requests on the specified port, process the request and return the processing result to the browser

6.1.1 ip http-server http

Command description

ip http-server http

no ip http-server

If you want to start the switch http service, you can configure it through this command. Use the no form of this command to cancel this configuration, and use the N/A method to manage the switch in http mode.

Parameter

N/A

Default

N/A

Command mode

global configuration mode

eg.

Start the switch http service.

Switch(config)# ip http-server http

6.1.2 ip http-server https

Command description

ip http-server https

no ip http-server

If you want to start the switch https service, you can configure it through this command. Use the no form of this command to cancel this configuration, and use the N/A method to manage the switch in https mode.

Parameter

N/A

Default

N/A

Command mode

Global configuration mode.

eg.

Enable the switch https service.

Switch(config)# ip http-server https

6.2 SNMP config

Command description:

community

syscontact

syslocation

sysname

trap

trap2sink

trapsink

user

Function Introduction

Simple Network Management Protocol (SNMP) consists of a set of

network management standards, including an application layer protocol, a database schema and a set of data objects. This protocol enables network management systems to monitor devices connected to the network for any management concerns. This protocol is part of the internet protocol suite defined by the Internet Engineering Task Force (IETF).

6.2.1 snmp

Command description

snmp

no snmp

If you want to enable the snmp function, you can configure it through this command. Use the no form of the command to disable this feature.

Parameter

N/A

Default

Enable

Command mode

Global mode

eg.

Enable the switch snmp function.

switch(config)# snmp

6.2.2 snmp-server trap2sink

Command description

snmp-server trap2sink ip

snmp-server trapsink ip

Select the version of snmp and the configuration of the receiving address, which can be configured by this command.

Parameter

N/A

Default

snmp

Command mode

Global mode

eg.

Configure the SNMP protocol version of the switch.

switch(config)# snmp-server trap2sink 192.168.1.1

6.2.3 snmp-server trap

Command description

snmp-server trap

no snmp-server trap

Enable/disable snmp trap function.

Parameter

N/A

Default

Disable

Command mode

Global mode

eg.

switch(config)# snmp-server trap

6.2.4 snmp-server community

Command description

community

// Set the authentication name and permissions

Parameter

ro；read only

rw：read and write

Default

public

Command mode

Global mode

eg.

Configure the switch

switch(config)#snmp-server community ro 111

// The authentication name is 111, and the permission is read-only

6.2.5 snmp host

Command description

snmp-server sysname

// set hostname

Parameter

N/A

Default

N/A

Command mode

Global mode

eg.

switch(config)#snmp-server sysname 1111

// The hostname is 1111

6.2.6 snmp-server user

Command description

snmp-server

Parameter

N/A

Default

N/A

Command mode

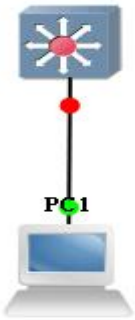
Global mode

eg.

switch(config)#snmp-server user ro 111

6.2.7 example

The switch enables snmp, and the MIB Browser is installed on pc1 to obtain the switch node information



sw： 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

//snmp version and read-write community configuration

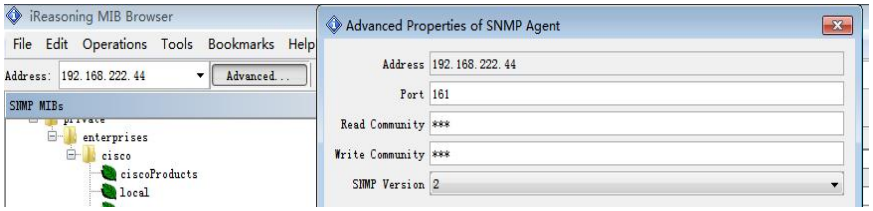
switch(config)# snmp-server host aa

switch(config-snmps-host)# no shutdown

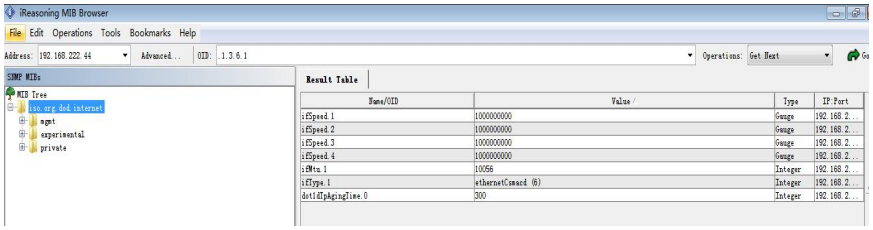
switch(config-snmps-host)# host 192.168.222.107

// snmp trap information configuration

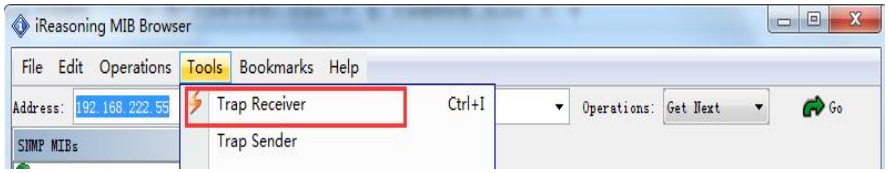
pc： Open MIB Browser on the PC, and add the switch ip with the corresponding community name



Right-click iso.org.dod.internet, click work, and relevant information will be displayed on the information display page.



Click trap receive under tools to view the uploaded trap information



Chapter 7 System Maintenance Commands

7.1 Reboot

Command description

If you want to restart the device, you can configure it through this command.

reboot

Parameter

N/A

Default

N/A

Command mode

Privileged mode.

eg.

Reboot the device after saving the configuration.

switch# system config save

switch# reboot

7.2 System config restore

Command description

If you want to restore the switch to factory settings, you can use this command to configure it, and it will take effect after restarting.

Parameter

N/A

Default

N/A

Command mode

Privileged mode.

eg.

It will take effect after restoring the factory configuration and restarting.

switch# system config restore

swtich# reboot

7.3 System config save

Command description

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

Parameter

N/A

Default

N/A

Command mode

Privileged mode

eg.

Save switch configuration

switch# system config save

7.4 PING test

function Introduction

PING (Packet Internet Groper), Internet Packet Explorer, a program for testing the amount of network connections. Ping sends an ICMP (Internet

Control Messages Protocol), that is, the Internet Message Control Protocol; the echo request message is sent to the destination and reports whether the desired ICMP echo (ICMP echo response) is received. It is a command used to check whether the network is smooth or the speed of the network connection.

Command description

Ping ip

Test reachability with the host.

Parameter

N/A

Default

N/A

Command mode

Privileged mode

eg.

Test the reachability of switches and hosts

switch# ping 192.168.1.100