# XonTel XT-1600G/XT-2400G PoE Switches

# CLI Management User-Guide

# Contents

# Chapter 1 General Command

## 1.1 Mode Command

### 1.1.1 configure terminal

Command

**configure terminal**

Mode

Privileged Mode

Parameter

Without

Description

**configure terminal** command enter into config mode.

Example

#enter into configuration mode.

**Switch#configure terminal**

**Switch(config)#**

### 1.1.2 disable

Command

**disable**

Mode

Privileged mode

Parameters

Without

Description

**disable** command is used to close the privileged mode, back to normal mode.

Example

# Close and return to normal mode:

**Switch#disable**

**Switch>**

### 1.1.3 enable

Command

**enable**

Mode

normal mode

Parameters

Without

Description

When Password right, enter privileged mode.

Example

From common mode into privileged mode:

**Switch> enable**

**password:******

**switch#**

### 1.1.4 exit

Command

**exit**

Mode

all modes

Parameter

Without

Description

**exit** command is used to end the current mode, return to the previous model..

Example

# From the privileged mode back to Normal Mode.

**Switch#exit**

**Switch>**

## 1.2 File Manager command

### 1.2.1 copy running-config startup-config

Command

**copy running-config startup-config**

Mode

privileged mode

Parameter

Without

Description

**copy running-config startup-config** command to save the current configuration of the system boot configuration file.

Example

# Copy the current configuration as the restart for next time .

**Switch#copy running-config startup-config**

**Building and writing configuration ...**

## 1.2.2 delete startup-config

Command

**delete startup-config**

Mode

Privileged mode

Parameters

without

Description

Delete the startup configuration file. The implementation of the command to restart the switch, will be restored to factory settings.

Example

# Remove the startup configuration

**Switch#delete startup-config**

**Do you wish to continue? [Y/N]:**

## 1.2.3 download configure

Command

**download configure <ip-address> <file-name>**

Mode

Privileged mode

Parameters

**ip-address:** TFTP server ip address.

**file-name:** TFTP server's configuration file name.

Description

Configuration file from the TFTP server will be downloaded to the switch as the startup configuration file, restart the switch after the entry into force of the downloaded configuration file.

Example

#downloaded the configuration file- conf.txt from the host 172.16.0.1.to the switch.

**Switch#download configure 172.16.0.1 conf.txt**

## 1.2.4 download image

Command

**download image <ip-address> <file-name>**

Mode

Privileged mode

Parameters

**ip-address:** TFTP server ip address.

**file-name:** TFTP server's configuration file name.

Description

download the Image file from the TFTP server to the switch as an image file and restart the switch after the image file to take effect.

Example

# switch.img the image files downloaded to the switch from the host 172.16.0.1

**Switch#download image 172.16.0.1 switch-0v13.img**

## 1.2.5 upload configure

Command

**upload configure <ip-address> <file-name>**

Mode

Privileged mode

Parameters

**ip-address:** show The purpose of that file upload TFTP server's IP address.

**file-name:** save to TFTP server configuration file name.

Description

Save The switch startup configuration file to the TFTP server.

Example

# saved the start configuration file to the host 172.16.0.200 , named conf:

**Switch#upload configure 172.16.0.200 conf**

## 1.2.6 write

Command

**write**

Mode

Privileged mode

Parameters

without

Description

To save the current user configuration settings.

Example

without

## 1.3 System Management Command

### 1.3.1 enable password

Command

**enable password <password>**

**no enable password**

Mode

Configuration Mode

Parameters

**password:** Password string. The default password is blank.

Description

**enable password** command is used to modify the password of the switch from normal mode to enter privileged mode.

no enable password command is used to cancel password.

Example

# Modify the switch password is admin:

**Switch(config)#enable password admin**

### 1.3.2 exec-timeout

Command

**exec-timeout <minutes> [<seconds>]**

**no exec-timeout**

Mode

Terminal Configuration Mode

Parameters

**minutes:** minutes, range 0-35791.

**seconds:** seconds, range 0-59.

Description

**exec-timeout** command is used to configure the telnet terminal idle timeout. The default value is 10 minutes.

no exec-timeout command is used to cancel configuration, restore the default value.

Example

# Configure the timeout to 15 minutes:

**Switch(config-line)#exec-timeout 15**

## 1.3.3 hostname

Command

**hostname <name>**

**no hostname**

Mode

Configuration Mode

Parameters

**name:** the name of the system, start with a letter. The default system name :Switch.

Description

**hostname** command is used to modify the system's name.

no hostname name of the system restore factory settings.

Example

# The system name was changed to Name:

**Switch(config)#hostname Name**

**Name(config)#**

## 1.3.4 password

Command

**password <password>**

**no password**

Mode

Configuration Mode

Parameters

**password:** Password string. The default is no password

Description

**password** command is used to set the Telnet connection password.

no password command is used to cancel password settings and restore default values.

Example

without

## 1.3.5 reset

Command

reset

Mode

Privileged mode

Parameters

Without

Description

The command reset to re-start switch.

Example

Without

## 1.3.6 show history

Command

**show history**

Mode

Normal mode/privileged mode

Parameters

Without

Description

Show history command to display the command history can be displayed before the implementation of this Order 20 Order

Example

without

## 1.3.7 show version

Command

**show version**

Mode

Normal mode/privileged mode

Parameters

Without

Description

Show version command is used to display system image file information

Example

#show version

**Switch#show version**

**switch 1.0.1**

**Build time:Jun 16 2008, 15:28:25**

## 1.3.8 terminal

command

**terminal{length <number>|no length}**

Mode

Normal mode/privileged mode

Parameters

**length:** number of rows that Every time displays to the screen. The default 25-line

**no length:** Cancel the settings of shows the number of rows, return to the default settings

Description

**terminal** command used configuration terminal once the number of rows to the screen

Example

# Configuration terminal displays 10 lines per

**Switch>terminal length 10**

## 1.3.9 who

Command

**who**

Mode

Normal mode/privileged mode

Parameters

without

Description

**who** command is used to display the current vty users

Example

`# Display the current VTY users.

**Switch#who**

**vty[0] connected from**

**vty[34] connected from 172.20.2.104**

## 1.3.10 line vty

Command

**line vty**

Mode

Configuration Mode

Parameters

Without

Description

The command line vty enter terminal config mode.

Example

# Enter terminal mode.

**Switch(config)#line vty**

**Switch(config-line)#**

## 1.4 View Configuration Command

### 1.4.1 show running-config

Command

**show running-config [access-list | interface | ip {igmp | route} | vlan]**

Mode

privileged mode

Parameters

**access-list:** ACL relevant configuration.

**interface:** The interface-related configuration, including the physical interface and virtual interface.

**ip {igmp snooping}:** igmp snooping-related configuration.

**ip {route}:** route-related configuration.

**vlan:** vlan-related configuration.

Description

**show running-config** command is used to display the current configuration info.

Example

without

### 1.4.2 show startup-config

Command

**show startup-config**

Mode

privileged mode

Parameters

without

Description

**show startup-config** command is used to display the file contents of system start configuration.

Example

without

# 1.5 Mac address table command

## 1.5.1 bridge ageing-time

Command

bridge ageing-time <time>

no bridge ageing-time

Mode

Configuration Mode

Parameters

**time:** mac table aging time，range：10-1000000 second. Default 300 seconds.

Description

**bridge ageing-time** command is used to show mac address table aging time.

**no bridge ageing-time** command is to restore the ageing time of mac address table to the factory values

Example

# Set the aging time is: 100 seconds

**Switch(config)#bridge ageing-time 100**

## 1.5.2 show bridge fdb

Command

show bridge fdb [dynamic | interface <ifname> | static | vlan <vlan-id>]

Mode

Normal mode/privileged mode

Parameters

**ifname:** interface name.

**vlan-id :** Vlan id number

Description

Display the corresponding mac address table information

Example

#show all mac address table

**Switch>show bridge fdb**

| Bridge | VLAN | port | mac | fwd static |
|---|---|---|---|---|
| 1 | 1 | fe1/12 | 00ca.0009.0001 1 | 1 |

**Total of Entry 1**

### 1.5.3 clear mac address-table dynamic

Command

**clear mac address-table dynamic [ interface <ifname> ]**

Mode

Normal mode/privileged mode

Parameters

**ifname:** Interface name

Description

Delete dynamic mac address table

Example

#Clear all dynamic mac address-talble:

**Switch>clear mac address-table dynamic**

## 1.6 network debugging command

### 1.6.1 ping

Command

**ping <ip-address> [-n <count> | -l <size> | -r <count> | -s <count> | -j <count> <ip-address>* | -k <count> <ip-address>* | -w <timeout>]***

Mode

privileged mode

Parameters

**ip-address:** target IP address.

**-n:** the number of requests sent.

**-l:** send the packet's length.

**-r:** record the specified number of hops of the route.

**-s:** records of the hops tim of specified number.

**-j:** Source with a loose routing, enter the routing hops and the associated IP address of jump. Enter multiple IP addresses can be repeated.

**-k:** Source with a strict routing, enter the routing hops and the associated IP address of jump. Enter multiple IP addresses can be repeated.

**-w:** wait for each response timeout, unit seconds.

Description

**ping** is a network debugging tool to test up to another host. Simple application simply enter the target host's IP address; if you use ping as a diagnostic tool, you can enter more details of the parameters

Example

#Send 5 request packet to the host 172.16.0.1:

**Switch#ping 172.16.0.1 -n 5**

## 1.6.2 trace-route

Command

**trace-route <ip-address> [-h <maximum-hops> | -j <count> <ip-address>* | -w <timeout>]***

Mode

privileged mode

Parameters

**ip-address:** target IP address.

**-h:** maximum number of hops.

**-j:** Source with a loose routing, enter the routing hops and the associated IP address of jump. multiple IP addresses can be repeated.

**-w:** timeout time (seconds).

Description

**trace-route** can detect route of the data packets from one host to another host. If you just want to achieve this functionality, users only need to enter the target IP address on it. If you want to Diagnosis can be entered as a network-related parameters.

Trace-route way to achieve this is the case, from the host to the purpose of this TTL incremental host sends UDP packets. If the TTL is zero, the router will be sent through the TTL runs out, host unreachable ICMP packets; If you get to host, but the host does not have the UDP packets of the port, the host will respond to the ICMP port unreachable packets. traceroute according to the response of the ICMP packets through the host or the port does not reach up to determine whether the destination host. If the host is not up to shows that, after the router, print this router IP address, continue to send TTL plus 1 of the UDP packet until the TTL is equal to Maxmum time to live. If the port is not up to explain the purpose to reach the host, print the host's IP address, and stop sending UDP packets.

Example

# Test the purpose of 192.168.10.2, the routing of the largest number of 10-hop :

**Switch#trace-route 192.168.10.2 -n 10**

## 1.6.3 telnet

Command

telnet <ip-address>

mode

privileged mode

Parameters

**ip-address:** Target IP Address.

Description

Remote login to another switch or host.

Example

#Login to the switch that manage ip is 172.16.0.1：

**Switch#telnet 172.16.0.1**

# 1.7 Multi-user manager command

## 1.7.1 username

Command

**username <username> password <password> {normal | privilege}**

**no username [username]**

Mode

Configuration Mode

Parameters

**username:** user name string, maximum length of 20.

**password:** Password string, maximum length of 20.

**normal:** normal permissions.

**privilege:** privileged access.

Description

**username** command can add users, modify existing user's password or permission. without the default user, can add up to 10 users. Multi-user can be used for telnet terminal, http users, and login to use.

no username command be used to delete an existing user or all users.

Example

# Add a user named abc, password is abc, permissions for normal users

**Switch(config)#username abc password abc normal**

# 1.8 User Security Control command

## 1.8.1 security-manage http

Command

security-manage http {access-group < group-id> | disable | enable }

Mode

configuration mode Configuration Mode

Parameters

**group-id:** Reference number of rules, the scope is "1-99"

Description

Used to set whether to support the web login

Example

#Set to support web mode login

**Switch(config)#security-manage http enable**

## 1.8.2 security-manage snmp

Command

**security-manage snmp {access-group < group-id> | disable | enable }**

Mode

Configuration Mode

Parameters

**group-id:** Reference number of rules, the scope is "1-99"

Description

Used to set whether to support the snmp login

Example

#Set to support snmp login

**Switch(config)#security-manage snmp enable**

## 1.8.3 security-manage telnet

Command

**security-manage telnet {access-group < group-id> | disable | enable | number <number> }**

Mode

Configuration Mode

Parameters

**group-id:** reference group number of rules, rules, the scope of "1-99"

**number:** the number of support telnet login

Description

Used to set whether to support telnet login.

Example

#Set to support telnet mode login：

**Switch(config)#security-manage telnet enable**

## 1.8.4 show security-manage

Command

show security-manage

Mode

Normal mode / privileged mode

Parameters

without

Description

**show security-manage** command is used to display system security information.

Example

# show the system security manage information

**Switch#show security-manage**

| Service type | Admin state | Access-list name |
|---|---|---|
| ---------- | ---------- | ---------- |
| **http** | **enable** | **0** |
| **snmp** | **enable** | **0** |
| **telnet** | **enable** | **88** |

# Chapter 2 Port command

## 2.1 Port General configuration

### 2.1.1 interface

Command

interface <if-name> [if-name]

Mode

Configuration Mode / Interface Configuration Mode

Parameters

**if-name:** port name. Fast port to fe as a prefix, Gigabit port to ge the prefix aggregation port to trunk as a prefix. Port number is a suffix. Example: the first port is expressed as fe1 / 1; aggregation port 1 is expressed as trunk1.

if-range: port range configuration. Range of parameters such as port configuration which mean enter multi-physical ports at the same time. Enter into the multiple physical ports At the same time, each port must be have the same prefix, separated by blank. Cases of interface fe1 / 1 fe1/10 or interface ge1/25 ge1/26.

Note: does not support aggregation port or vlan interface range configuration.

Description

interface command is used to enter one or more of the port configuration mode.

Example

# Incoming port 24

**Switch(config)#interface fe1/24**

#incoming trunking port

**Switch(config)#interface trunk1**

# Into the port range 1-24

**Switch(config)#interface fe1/1 fe1/24**

## 2.1.2 description

command

**description <line>**

**no description**

Mode

interface configuration mode.

Parameters

**line:** port description string.

Description

**description** command to set the port description can do the description for port.

no description order the cancellation of the port described configuration.

Example

# Set the description of the port fe1 / 1 as:

**Switch(config-fe1/1)#description bulid 1 floor 5**

## 2.1.3 show interface

command

**show interface [<if-name> | statistics <if-name>]**

Mode

Normal mode / privileged mode

Parameters

**if-name:** Interface name

**statistics:** Show port send and receive packet statistics.

Description

**show interface** command without parameters to display all of the lay2 and lay3 interface information. Specify the interface name displays the specified lay2 or lay3 interface information. show interface statistics show the specified interface send and receive packet statistics.

Example

#display the info of vlan1 interface

**Switch>show interface vlan1**

**Interface vlan1**

**Hardware Type: VLAN**

**MAC Address:** **0009.ca1b.a011**
**Flags:** **<UP,BROADCAST,MULTICAST>**
**Admin Status:** **UP**
**Operate Status:** **DOWN**
**Index:** **3**
**Metric:** **1**
**MTU:** **1500**
**IP Address:** **192.168.0.1/24**

**Switch#show interface fe1/11**
**Interface fe1/11**
**Hardware Type:** **Ethernet**
**MAC Address:** **0625.0000.004a**
**Flags:** **<UP,BROADCAST,RUNNING,MULTICAST>**
**Admin Status:** **UP**
**Operate Status:** **UP**
**Index:** **2011**
**Metric:** **1**
**MTU:** **1500**
**Duplex:** **full**
**Config Duplex:** **AutoNego**
**Bandwidth:** **100m**
**Config Bandwidth:** **AutoNego**
**Switchport Mode:** **access**
**Default Vlan:** **1**

## 2.1.4 shutdown

command
**shutdown**
**no shutdown**
Mode
Interface Configuration Mode
parameters:
without
Descroption
shutdown-close port, The state of managed port is DOWN.
no shutdown-open port, The state of managed port is UP.
Example:
#shutdown the port:fe1/1：
**Switch(config-fe1/1)#shutdown**
**Switch(config-fe1/1)#**

### 2.1.5 speed

command

**speed {autonegtiate | full-10 | full-100 | full-1000 | half-10 | half-100}**

mode

interface configuration mode

parameters

**autonegtiate:** duplex status is anto-negotiation.

**full-10:** speed 10M full-duplex status.

**full-100:** speed 100M full-duplex status.

**full-1000:** speed status 1000M full duplex.

**half-10:** 10M half-duplex status.

**half-100:** 100M half-duplex status.

description

Configure the speed of port as duplex status

Example

#change the port-fe1/1into 100Mfull-duplex status：

**Switch(config-fe1/1)#speed full-100**

## 2.2 MIRROR command

### 2.2.1 mirror

command

**mirror interface <if-name> direction {both | receive | transmit}**

**no mirror interface <if-name> direction [receive | transmit]**

mode

interface configuration mode.

parameters

**if-name:** monitor port.

**both:** monitor the specified port’s out of data streams

**receive:** monitor the specified ports received data streams

**transmit:** Monitor the specified port output data streams

description

**mirror interface** command specify the monitor port, used to monitor the data stream from other ports.

**no mirror interface** command cancel the configuration of monitor ports.

Example

#Use port fe1/1 to monitor the input data stream from port fe1/12:

**Switch(config-fe1/1)#mirror interface fe1/12 direction receive**

### 2.2.2 show mirror

command

**show mirror [interface <if-name>]**

mode

normal mode/privileged mode

parameters

**interface <if-name>：** port name.

description

**show mirror** command is used to display the info of mirror configuration.

Example

without .

## 2.3 broadcast storm-control command

### 2.3.1 storm-control

command

**storm-control {broadcast | dlf | multicast | ratelimit <rate-num>}**

**no storm-control {broadcast | dlf | multicast}**

mode

interface configuration mode

parameters

**broadcast:** control the broadcast packet.

**dlf:** control purposes unknown unicast packets.

**multicast:** multicast control packets.

**ratelimit:** control rate.

description

**storm-control** command used to set forwarding restrictions the port to the broadcast packet, dlf packet, multicast packet. Set the port storm-control settings received in accordance with the data streams will limit the forward speed.

no storm-control command used to cancel settings.

Example

# Restrict port fe1 / 1 for broadcasting, multicast, unknown packet forwarding rate of 20971 kbits

**Switch(config-fe1/1)#storm-control ratelimit 20971**

**Switch (config-fe1/1)#end**

**Switch#show storm-control fe1/1**

| Port | Bcast | Mcast | Dlf | Limit(kbits) |
|---|---|---|---|---|
| fe1/1 | set | unset | unset | 20971 |

### 2.3.2 show storm-control

command

show storm-control [<if-name>]

mode

normal mode/privileged mode

parameters

**if-name:** port name.

description

**show storm-control** command is used to show storm-control states，Display the content including broadcast packets, dlf packets, multicast packet control value and the number of discarded packets.

Example

#display fe1/1's storm-control config info

**Switch>show storm-control fe1/1**

| Port | Bcast | Mcast | Dlf | Limit(kbits) |
|---|---|---|---|---|
| fe1/1 | set | unset | unset | 64 |

## 2.4 Flow-Control Command

### 2.4.1 flowcontrol

command

flowcontrol

no flowcontrol

mode

interface configuration mode

parameters

without

description

**flowcontrol** command is uesd to open the flow control functiom of port

**no flowcontrol** command is used to close the flow control function of port.

Example

Without.

### 2.4.2 show flowcontrol

command

**show flowcontrol [interface <if-name>]**

mode

normal mode/privileged mode

parameters

**if-name:** interface name.

description

Check the configuration of the port flow control.

Example

Without.

## 2.5 Port Bandwidth command

### 2.5.1 portrate

command

**portrate egress <rate>**

**portrate ingress <rate>**

mode

interface configuration mode.

parameters

**egress:** the port output rate.

**ingress:** the port input rate.

**rate:** the rate of setting the value, range :1-1024000 kbits.

description

Set the maximum input and output rate of the port. 1000M trillion for the mouth, the smallest particle size is 8MB; for 100M port, under the speed limit at the 1.792MB, the particle size is 64kb, on top of this, the particle size is 1MB.

Example

# Set the port fe1 / 2 input speed limits 128Kbps:

**Switch(config-fe1/2)#portrate ingress 128**

### 2.5.2 show portrate

command

**show portrate [interface <if-name>]**

mode

normal mode/privileged mode

parameters

**if-name：** port name.

description

**show portrate** command Is used to display the speed limit specified port configuration.

Example

without .

## 2.6 Port Trunking command

### 2.6.1 trunk

command

trunk <trunk-id>

no trunk <trunk-id>

mode

configuration mode.

parameters

**trunk-id:** Link trunk number, the scope is"1-3". In which 1,2 for 100M port trunk group, 3-port trunk groups for the 1000M. default for no link trunk configuration

description

**trunk** command is used to create a link trunking, the system make a link trunk as a logical port link trunkt. Need to first create a link trunk only after trunk port configuration. Each 100M port trunk group of up to four ports, 1000M-port trunk group to support two ports. no trunk command is used to delete a link trunk. Remove trunk group must be removed before the members of the port

Example

# configure a group number is an trunk link:

**Switch(config)#trunk ?**

**<1-3> Trunk ID: <1-2>100M port trunk, <3>1G port trunk**

**load-balance load-balance commands**

**Switch(config)#trunk 1**

### 2.6.2 trunk interface

command

**trunk interface <if-name>**

**no trunk interface [<if-name>]**

mode

interface configuration mode.

parameters

**if-name:** port name.

description

**trunk interface <if-name>** command make the physical port trunk groups to join and become trunk port.

no trunk interface command delete the trunk group from physical port；If the input port name only delete the specified port, if no enter the port name will delete all the physical ports within the trunk group.

Example

#configure the port fe1/1as trunk1port's member:

**Switch(config-trunk1)#trunk interfae fe1/1**

## 2.6.3 trunk load-balance

command

**trunk load-balance { dst-mac | src-dst-mac | src-mac}**

**no trunk load-balance**

mode

configuration mode.

parameters

**dst-mac:** According to the target MAC addresses out of the port direction of data flow load balancing.

**src-dst-mac:** According to the source MAC address and destination MAC addresses out of the port on the direction of data flow load balancing. This is the default load balancing strategy.

**src-mac:** According to the source MAC address of a port on the direction of data flow load balancing.

description

**trunk load-balance** command configure TRUNK group's Load balancing strategy.

**no trunk load-balance** command cancel configuration Load balancing strategy , restore src-dst-mac strategy.

Example

#Configuration trunk according to the target MAC address do the load balancing strategy：

**Switch(config)#trunk load-balance dst-mac**

## 2.6.4 show trunk

command

**show trunk [<trunk-id>]**

mode

normal mode/privileged mode.

parameters

**trunk-id:** query TRUNK group ID number

description

Show link trunk configuration, including the trunk group name, load balancing strategy

and members of the port. If not specify runk group ID number is displayed all of the aggregate port configuration

Example

#display all link trunk configuration：

**Switch#show trunk**

**% Trunk name: trunk1**

**% Load-balance: Source and Destination Mac address**

**% Member:**

**fe1/1**

**fe1/11**

## 2.7 Port Protection command

### 2.7.1 switchport port-security protect

command

**switchport port-security protect**

**no switchport port-security protect**

mode

interface configuration mode.

parameters

without

description

**switchport port-security protect** command configuration port is the port-protect. protect ports can not inter-connected PC, protect the port can only communicate with non-protected port

**no switchport port-security protect** command cancel the protect port.

Example

#Configure port fe1/1 as protect port

**Switch(config-fe1/1)#switchport port-security protect**

**Switch(config-fe1/1)#**

### 2.7.2 show port-security protect

command

show port-security protect

mode

Normal mode / privileged mode.

parameters

without .

description

Show protect port’s info.

Example

#show all the protect port configuration：

**Switch#show port-security protect**

| Port | Port protected |
|---|---|
| ----- | ---------- |
| fe1/22 | ON |

## 2.8 Jumbo Frame command

### 2.8.1 Jumbo Frame

command

**jumbo frame{1518|1536|2000|2044}**

**no jumbo frame**

mode

interface configuration mode.

parameters

**1518:** allow 1518-byte none vlan tag packets and 1522-byte vlan tag the packets through

**1536:** allow package through a length of 1536 bytes of data

**2000:** allow package through a length of 2000 bytes of data

**2044:** allow 2044-byte none vlan tag packets and 2048-byte vlan tag of packet through

description

**jumbo frame** command to configure global forwarding packet's length.

**no jumbo frame** command to revert to the default value of 1518 bytes.

Example

# Configure port forwarding packets of 2044 bytes in length:

**Switch (config) # jumbo frame 2044**

### 2.8.1 show Jumbo Frame

command

**show jumbo frame**

mode

normal mode/privileged mode.

parameters

without .

description

**show jumbo frame** to view the configuration of the large frame

Example

# View the configuration of the large frame:

**Switch#show jumbo frame**

**jumbo frame(bytes): 1518**

# Chapter 3 MAC security command

## 3.1 MAC binding command

### 3.1.1 switchport port-security mac-bind

command

**switchport port-security mac-bind <mac-address> vlan <vlan-id>**

**no switchport port-security mac-bind [mac-address]**

mode

interface configuration mode.

parameters

**mac-address:** Binding of the physical address, using 12-bit 16 hexadecimal to express; mac address, format HHHH.HHHH.HHHH;

**vlan-id:** on the mac-bind the vlan id number, range 1-4094.

description

**switchport port-security mac-bind** command is to mac binding the ports..

**no switchport port-security mac-bind** command cancel mac binding.

Example

#Configuration port fe1/1 at vlan1 to do the MAC binding 00ca.0009.0001.

**Switch(config-fe1/1)switchport port-security mac-bind 00ca.0009.0001 vlan 1**

### 3.1.2 switchport port-security mac-bind auto-conversion

command

**switchport port-security mac-bind auto-conversion [number <number> | vlan <vlan-id> ]**

**no switchport port-security mac-bind [<macaddr> vlan vlan <vlan-id>]**

mode

interface configuration mode.

parameters

**number:** number of mac auto- bind，range is 1-1891.

**vlan-id:** which vlan to mac binding,1range 1-4094.

description

**switchport port-security mac-bind auto-conversion** command to anto-binding the learnt dynamic mac address.

**no switchport port-security mac-bind [<macaddr> vlan vlan <vlan-id>]** command is used to delete the corresponding MACbind configuration.

Example

# Configuration port fe1 / 1 the dynamics of learning to automatically translate into a static mac address mac address binding

**Switch(config-fe1/1)#switchport port-security mac-bind auto-conversion**

### 3.1.3 show port-security mac-bind

command

**show port-security mac-bind [ifname]**

mode

normal mode/privileged mode

parameters

**ifname:** Need to specify the interface name of lay2.

description

Display the specified port's mac bind info.

Example

Switch# show port-security mac-bind

| VLAN ID | MAC ADDRESS | IFNAME |
|---|---|---|
| 1 | 00ca.0009.0001 | fe1/12 |

## 3.2 MAC filtering command

### 3.2.1 switchport port-security mac-filter

command

**switchport port-security mac-filter <mac-address> vlan <vlan-id>**

**no switchport port-security mac-filter [mac-address]**

mode

interface configuration mode.

parameters

**mac-address:** Filtered physical address, using 12-bit 16 hexadecimal, format HHHH.HHHH.HHHH

**vlan-id:** vlan's id no that mac－bind，range 1-4094.

description

**switchport port-security mac-filter** command do the port's mac filter..

**no switchport port-security mac-filter** command cancel mac filter.

Example

#configuration port fe1/1 at vlan1 to do MAC filter 00ca.0009.0001.

**Switch(config-fe1/1)# switchport port-security mac-filter 00ca.0009.0001 vlan 1**

## 3.2.2 switchport port-security mac-filter auto-conversion

command

**switchport port-security mac-filter auto-conversion [number <number> | vlan <vlan-id> ]**

**no switchport port-security mac-filter [macaddr vlan <vlan-id> ]**

mode

interface configuration mode.

parameters

**number:** number of do the mac anto filter .range 1-8191.

**vlan-id:** which vlan need do the mac filter， range 1-4094.

description

**switchport port-security mac-filter auto-conversion** command is to leanrt dynamic mac address transfer automatically into mac address fliter.

**no switchport port-security mac-filter** command is used to delete the corresponding ma filter configuration.

Example

#configuration port fe1/1 learnt dynamic mac address transfer to the static mac address filter.

**Switch(config-fe1/1)#switchport port-security mac-filter auto-conversion**

## 3.2.3 show port-security mac-filter

command

**show port-security mac-filter [ifname]**

mode

normal mode/privileged mode

parameters

**ifname:** need to specified lay2 interface name..

description

Show the specified mac filter info.

Example

**Switch# show port-security mac-filter**

**VLAN ID MAC ADDRESS IFNAME**

**1 0009.ca00.0009 fe1/20**

## 3.3 MAC address learning control command

### 3.3.1 switchport port-security learn-limit

command

**switchport port-security learn-limit <number>**

**no switchport port-security learn-limit**

mode

interface configuration mode.

parameters

**number:** restrict the no of learning MAC.range 0-8191.

description

**switchport port-security learn-limit** command is Restrictions on the number of ports to learn MAC.

**no switchport port-security learn-limit** command is to cancel learn Mac restrictions.

Example

#configure port fe1/1only learnt 50 MAC address.

**Switch(config-fe1/1)#switchport port-security learn-limit 50**

### 3.3.2 show port-security learn-limit

command

**Switch#show port-security learn-limit [ifname]**

mode

normal mode/privileged mode

parameters

**ifname:** need to specified lay2 interface name.

description

Show the specified port learn mac’s no.

Example

**Switch#show port-security learn-limit**

**interface fe1/21 dynamic learn limit is 50**

# Chapter 4 Loop Detection command

## 4.1.1 loopback-detection detection-time

command

**loopback-detection detection-time <detection-time>**

**no loopback-detection detection-time**

mode

configuration mode.

parameters

**detection-time:** the interval of Port forwarding loop detection protocol packet, the range 1~65535, default value is 5.

description

**loopback-detection detection-time** command: Configuration of this machine is used to enable single-port loop detection time interval to send protocol packets. This value must be less than twice the time automatic recovery (resume-time)

no loopback-detection detection-time command is used to delete the configuration to detection-time，Back to the default values.

Example

#Detection of loop configuration protocol packets to send interval is 10 seconds

**Switch#conf t**

**Switch(config)#loop-detection detection-time 10**

## 4.1.2 loopback-detection protocol-safety

command

**loopback-detection protocol-safety**

**no loopback-detection protocol-safety**

mode

configuration mode.

parameters

without .

description

**loopback-detection protocol-safety** command: Single-port configuration of this machine is used to loop detection Initiation Protocol security checks, start the feature after the protocol port will detect the same protocol packets Whenever the number of auxiliary groups as a basis for judging. To enable this feature, respond-packets configuration to take effect.

**no loopback-detection protocol-safety** command is used to prohibit Protocol security checks.

Example

#configure single-port loop Detection protocol security features

**Switch#conf t**

**Switch(config)#loop-detection protocol-safety**

## 4.1.3 loopback-detection respond-packets

command

**loopback-detection respond-packets <packets number>**

**no loopback-detection respond-packets**

mode

configuration mode.

parameters

**packets number:** Port to receive the same number of protocol packets, the range 2 ~ 100, default value is 10

description

**loopback-detection respond-packets** command: Configuration of this machine is used to enable single-port port forwarding loop detection protocol packet as a basis to determine existence of the loop the number of the receiving protocol packets, if you believe that there is to achieve this number of loops. This configuration is only security feature is enabled only when the agreement entered into force.

**no loopback-detection respond-packets** command is used to delete the configuration to respond-packets，Back to the default values.

Example

#configure the Single-Port Loop Detection when making judgments based on the protocol packet format 5

**Switch#conf t**

**Switch(config)#loop-detection respond-packets 5**

## 4.1.4 loopback-detection resume-mode

command

**loopback-detection resume-mode <automation | manual>**

**no loopback-detection resume-mode**

mode

configuration mode.

parameters

**automation:** Auto (default value)

**manual:** manual.

description

**loopback-detection resume-mode** command: Configuration of this machine is used to

detect the loop recovery port communication mode: automatic or manual. Automatic mode, the port will be made every "resume-time" time to re-enabled and send the protocol packet detect the presence of loops. Manual mode, the port and then entered the ring to detect blocked state, since the user believe that intervention.

no loopback-detection resume-mode command is used to delete the configuration of resume-mode，Back to the default values（auto）.

Example

#configure the single-port loop test recoveryy as manual mode

**Switch#conf t**

**Switch(config)#loop-detection resume-mode manual**

## 4.1.5 loopback-detection resume-time

command

**loopback-detection resume-time < resume-time >**

**no loopback-detection resume-time**

mode

configuration mode.

parameters

**resume-time:** the intervel of recovery of port，Range 10 ~ 65536, default value is 600..

description

**loopback-detection resume-time** command :Configuration port is used to detect the loop and enters blocking state after the automatic recovery time. The parameters can only resume-mode for the automation when effective, value must be greater than the detection-time of 2 times..

**no loopback-detection resume-time** command is used to delete the configuration of resume-mode，Back to the default values.

Example

#configure port to detect the loop and blocks the re-enable after 30 seconds：

**Switch#conf t**

**Switch(config)#loop-detection resume-time 30**

## 4.1.6 loopback-detection enable

command

**loopback-detection enable**

**no loopback-detection**

mode

interface configuration mode.

parameters

without

description

**loopback-detection enable** command is used to configure the port start to loop detection.

**no loopback-detection** command is to prohibit the loop detection.

Example

#Configure port fe1/2 start to singnal port looping detection.:

**Switch(config)#inter fe1/2**

**Switch(config-fe1/2)#loopback-detection enable**

### 4.1.7 loopback-detection resume

command

**loopback-detection resume**

mode

interface configuration mode.

parameters

without

description

**loopback-detection resume** command is used to manually restart to detect the loop and enters the state of the port blocking.

Example

#Restart port fe1/2:

**Switch(config)#inter fe1/2**

**Switch(config-fe1/2)#loopback-detection resume**

## 4.2 Single-Port Loop Detection viewing command

### 4.2.1 show loopback-detection

command

**show loopback-detection [ifname]**

mode

privileged mode.

parameters

**ifname:** interface name，here is the physical port.

**null:** when parameters is blank,display loopback-detection protocal configuration.

description

**show loopback-detection** command is used to viewing loopback-detectionprotocal’s configuration and port list and the loop detection.

Example

#View loopback-detection protocal and port fe1/1detection：

**Switch#show loop-detection fe1/1**

**Loop detection configuration information**

| | | |
|---|---|---|
| **detection interval** | **: [10 Secs.]** | **Default[5 Secs.]** |
| **Resume mode** | **: [Automation]** | **Default[Automation]** |
| **Resume interval** | **: [600 Secs.]** | **Default[600 Secs.]** |
| **Execute operate** | **: [Shutdown]** | **Default[Shutdown]** |
| **Protocol safety** | **: [Disable]** | **Default[Disable]** |
| **Respond packets** | **: [10]** | **Default[10]** |
| **Dected Port List** | **: fe1/1** | |
| **fe1/1** | **: Not Loop** | |
| **Detect VLAN list** | **: 1** | |

## 4.3 Single-Port Loop Detection Debugging command

### 4.3.1 debug loopback-detection

command

**debug loopback-detection [all | events | packets [send | recv]]**

**no debug loopback-detection [all | events | packets [send | recv]]**

mode

privilegaed mode.

parameters

**all:** the agreement that all debugging switches.

**events:** the event under the agreement protocol debugging switch.

**packets:** protocol packets debugging switch

**null:** The parameters for the space-time deal with all the same.

description

**debug loopback-detection** command: Loopback-detection is used to open the specified under the debugging switches. Opens the corresponding debug information is output in the control terminal.

Example

#Open loop-detecion protocol packets debugging switch, and see open or not：

**Switch#debug loop-detection packets**

**Switch#show debug loop-detection**

**loopback-detection debugging status:**

**loopback-detection packets receive debugging is on**

**loopback-detection packets send debugging is on**

# Chapter 5 ip mac-bind command

## 5.1 Ip mac-bind command

command

**ip mac-bind <source-ip> <mac-address>**

**no ip mac-bind <source-ip> <mac-address>**

mode

interface configuration mode

parameters

**source-ip：** source-IP format: A.B.C.D.

**mac-address：** macaddress，format: HHHH.HHHH.HHHH。

description

**ip mac-bind** command to bind the port ip and mac address.

Example

**Switch(config-fe1/3)#ip mac-bind 192.168.0.2 0009.ca00.0002**

## 5.2 show IP mac-bind command

command

**show ip mac-bind [if-name]**

mode

normal mode/privileged mode

parameters

**if-name:** interface name

description

**show ip mac-bind** command to view the ip mac-bind information.

Example

```
Switch#show ip mac-bind
[fe1/4]   sum: 1
        MAC                 IP
        0009.ca00.0020 192.168.0.200
```

# Chapter 6 vlan command

## 6.1 vlan Create command

### 6.1.1 vlan database

command

vlan database

mode

configuration mode

parameters

without .

description

Enter vlan configuration mode.

Example

#enter into vlanconfigurationmode：

**Switch(config)#vlan database**

**Switch(config-vlan)#**

### 6.1.2 vlan

command

**vlan <vlan-id>**

**no vlan <vlan-id>**

mode

vlan configuration mode

parameters

**vlan-id:** to create one or more vlan. VLAN ID range is 1-4094. vlan-id, there are two expressions, one is a comma-separated multiple VLAN number, such as 1,3,5,10, and the other one is a VLAN range, such as 2-10, but can not exist in two ways . A command to create the vlan number can not be more than 100，

description

**vlan** command is used to create the VLAN. Note that VLAN 1 is the default method VLAN without removed.

**no vlan** command is used to delete a vlan.

Example

#Create vlan 2-10：

**Switch(config-vlan)#vlan 2-10**

# 6.2 vlan port configuration command

## 6.2.1 switchport access

command

**switchport access vlan <vlan-id>**

**no switchport access vlan**

mode

interface configuration mode

parameters

**vlan-id:** port default VID, range 2-4094.

The default switch only VLAN 1, all ports are untagged member of VLAN1.

description

**switchport access** command: VLAN mode is used to set the L2 ACCESS interface for the specified VLAN. This command is only L2 interface VLAN mode is ACCESS mode effective. After you set this command, this L2 interface PVID is specified VLAN, this L2 interface belongs only to the specified VLAN of the UNTAG members.

no switchport access vlan command to the interface access vlan back to the default VLAN, that is VLAN1. This command setting, this interface pvid into one, and only belongs to the untagged member of VLAN1

Example

#Make port fe1/1configuration into vlan2 untagged port：

**Switch(config-fe1/1)#switchport access vlan 2**

## 6.2.2 switchport hybrid allowed vlan add

command

**switchport hybrid allowed vlan add <vlan-list> egress-tagged { disable | enable}**

mode

interface configuration mode

parameters

**vlan-list:** the no of join into vlan，range:1-4094.

description

**switchport hybrid** command Used to specify the port to join one or more VLAN, if egress-tagged enable, is a TAG member, if the egress-tagged disable, it is UNTAG member

**<vlan-list>** there are two kinds of expression, one is a comma-separated multiple VLAN number, such as 1,3,5,10, and the other one is a VLAN range, such as 2-10, but can not exist in two ways.

1,3-5 expression is wrong (, and - only the existence one) ,2-4 ,6-7 is also wrong (- only exist once)

Example

#Configure port fe1/1to vlan1-3 tagged port:

**Switch(config-fe1/1)#switchport mode hybrid**

**Switch(config-fe1/1)#switchport hybrid allowed vlan add 1-3 egress-tagged enable**

## 6.2.3 switchport hybrid allowed vlan all

command

**switchport hybrid allowed vlan all**

mode

interface configuration mode

parameters

without

description

**switchport hybrid allowed vlan all** command only effective on lay2 interface's hybrid mode. The interface to join all of the VLAN in the (VLAN1 excluded), is that all of the tagged members of VLAN. After the newly created VLAN, the port will be added to the new VLAN in the VLAN membership of the TAG. Perform this command, the original belongs to activate the vlan the port of UNTAG members will become TAG members)

Example

# The port fe1 / 1 is set to vlan1 of untagged member of vlan all the other members of the tagged:

**Switch(config-fe1/1)#switchport mode hybrid**

**Switch(config-fe1/1)#switchport hybrid allowed vlan all**

:

## 6.2.4 switchport hybrid allowed vlan none

command

**switchport hybrid allowed vlan none**

mode

interface configuration mode

parameters

without

description

This command is only valid hybridmode L2 interface. This interface is no longer a member of VLAN of all (VLAN1 exception). The implementation of this command, the native vlan of the port will revert to 1

Example

# Port fe1 / 1 was originally vlan1 a tagged port, vlan2, vlan3 the untagged , vid = 2; Delete fe1 / 1 from the outside vlan remove vlan1:

**Switch(config-fe1/1)#switchport hybrid allowed vlan none**

**After the implementation of the command, the port fe1 / 1 of the tagged port is vlan1，vid=1.**

## 6.2.5 switchport hybrid allowed vlan remove

command

**switchport hybrid allowed vlan remove <vlan-id>**

mode

interface configuration mode

parameters

**vlan-id:** Need to remove the vlan number ,range 1-4094.

description

This command is only valid hybrid mode l2 interface. This interface is no longer the designated one or more VLAN members.

If the specified VLAN has enabled vlan, then the native vlan to return to 1

Example

# The port fe1 / 1 removed from the vlan2：

**Switch(config-fe1/1)#switchport hybrid allowed vlan remove 2**

## 6.2.6 switchport hybrid vlan

command

**switchport hybrid vlan <vlan-id>**

**no switchport hybrid vlan**

mode

interface configuration mode

parameters

**vlan-id:** join the vlan no.

description

**switchport hybrid vlan** command is only valid hybrid mode l2 interface. For the hybrid interface for the native vlan of the interface is set to the specified VLAN. After you set this command, this two-story interface pvid for the specified VLAN, and that the interface belongs to the specified VLAN in untagged members (if you set this command before the port has already belong to the VLAN of the TAG members, then perform this command after the port remain the TAG members, PVID or for the specified VLAN).

**no switchport hybrid vlan** command the native vlan of the interface is restored to the default VLAN (VLAN1). The implementation of this command, the original native vlan deleted (no longer belong to the original native vlan of the UNTAG or TAG members), the new native vlan is 1, the UNTAG belonging to VLAN1 members (if you perform this command before the port is already VLAN1 The TAG members, then continued after the implementation of this command to VLAN1 a TAG member), PVID revised to

1.

Example

#Configuration port fe1 / 1 for the vlan2's untagged member, vlan1 of the tagged members, and the vid 2：

**Switch(config-fe1/1)#switchport mode hybrid**

**Switch(config-fe1/1)#swi hybrid vlan 2**

**Switch(config-fe1/1)#switchport hybrid allowed vlan add 1 egress-tagged enable**

## 6.2.7 switchport mode

command

**switchport mode { access | hybrid | trunk}**

**no switchport { access | hybrid | trunk}**

mode

interface configuration mode

parameters

**access:** interface vlan mode is access mode. The default is access mode. If the l2 interface is set to access mode, the interface of the UNTAG default VLAN1 members, PVID is 1.

**hybrid:** interface vlan mode for hybrid mode. If the interface is set to HYBRID mode, the interface of the UNTAG default VLAN1 members, PVID is 1.

**trunk:** interface vlan mode for trunk mode. If the interface is set to TRUNK mode, the interface is the default for the VLAN1 a TAG member, PVID 1

description

Set the l2 interface VLAN mode, is one of access, hybrid or trunk

**no switchport** command will revert interface mode to the default value, returned to access mode, and access vlan is VLAN1

Example

# Set the port fe1 / 1 as the trunk port:

**Switch(config-fe1/1)#switchport mode trunk**

## 6.2.8 switchport trunk allowed vlan add

command

**switchport trunk allowed vlan add <vlan-list>**

mode

interface configuration mode

parameters

**vlan-id:** The interface to join one or more of the VLAN number. VLAN ID range is 1-4094. <vlan-id> there are two kinds of expression, one is a comma-separated multiple VLAN number, such as 1,3,5,10, and the other one is a VLAN range, such as 2-10, but

the two methods can not be exist at the same time.

description

This command is only valid trunk mode l2 interface. The interface is added to the specified one or more of the VLAN in a VLAN's tagged as a designated member

Example

# Port fe1/1configuration for vlan1-10 of the tagged members:

**Switch(config-fe1/1)#switchport trunk allowed vlan add 1-10**

## 6.2.9 switchport trunk allowed vlan all

command

**switchport trunk allowed vlan all**

mode

interface configuration mode

parameters

without

description

switchport trunk allowed vlan all command only effective.l2 interface trunk mode .The interface to join all of the VLAN in the (VLAN1 excluded), all of the tagged members of VLAN. After the newly created VLAN, the port will be added to the new VLAN in the VLAN membership of the TAG

Example

# Port fe1/1configuration for vlan1-10 of the tagged members:

**Switch(config-fe1/1)#switchport trunk allowed vlan all**

## 6.2.10 switchport trunk allowed vlan none

command

**switchport trunk allowed vlan none**

mode

interface configuration mode

parameters

without

description

**switchport trunk allowed vlan none** command just effective of l2 trunkmode. The interface is not the membership of any VLAN. (VLAN1 excluded).

Example

# Remove trunk ports fe1 / 1 from the outside vlan1 other vlan:

**Switch(config-fe1/1)#switchport trunk allowed vlan none**

## 6.2.11 switchport trunk allowed vlan remove

command

**switchport trunk allowed vlan remove <vlan-list>**

mode

interface configuration mode

parameters

**vlan-list:** the interface to delete one or more of the VLAN number. VLAN ID range is 1-4094. vlan-list, there are two expressions, one is a comma-separated multiple VLAN number, such as 1,3,5,10, and the other one is a VLAN range, such as 2-10, but can not exist in two ways

description

**switchport trunk allowed vlan remove** command only effective of l2 interface trunk mode. This interface is no longer the designated one or more VLAN members.

Example

#delete port fe1/1 from vlan 2、vlan3：

**Switch(config-fe1/1)#switchport trunk allowed vlan remove 2,3**

# 6.3 vlan view command

## 6.3.1 show vlan

command

**show vlan [<vlan-id>]**

mode

normal mode/privileged mode

parameters

**vlan-id:** need to display vlan no，range 1-4094.

description

Display VLAN information, including VLAN the port information. When you specify the vlan id show only the information specified vlan

Example

# View the current division of vlan：

**Switch#show vlan**

| VLAN | Name | State | Member ports ([u]-Untagged, [t]-Tagged) |
|---|---|---|---|
| 1 | vlan1 | active | [u]fe1/1 [u]fe1/2 [u]fe1/3 [u]fe1/4 [u]fe1/5 [u]fe1/6 [u]fe1/7 [u]fe1/8 [u]fe1/9 [u]fe1/10 [u]fe1/11 [u]fe1/12 [u]fe1/13 [u]fe1/14 [u]fe1/15 [u]fe1/16 [u]fe1/17 [u]fe1/18 [u]fe1/19 [u]fe1/20 [u]fe1/21 [u]fe1/22 |

**[u]fe1/23 [u]fe1/24 [u]ge1/25 [u]ge1/26**
**[u]trunk1**

# Chapter 7 QOS

## 7.1 QOS Configuration Command

### 7.1.1 qos dscp-map-qp

Command

**qos dscp-map-qp <dscp-value> qosprofile <qp-value>**

**no qos dscp-map-qp <qp-value>**

mode

configuration mode.

parameters

**dscp-value：** dscp's value，range 0-63，

**qp-value：** Packet to the column, the value of qp0, qp1, qp2, qp3.

description

**qos dscp-map-qp** command said dscp value mapped to the column.

**no qos dscp-map-qp** command back to the default mapping

Example

# configuration dscp value of 50 mapped to the column qp1.

**Switch(config)#qos dscp-map-qp 50 qosprofile qp1**

### 7.1.2 qos qosprofile

command

**qos qosprofile <qp-value> weight <weitht>**

**no qos qosprofile <qp-value> weight**

mode

configuration mode.

parameters

**qp-value：** Packet to the column, the value of qp0, qp1, qp2, qp3.

**Weight:** to express the value of the column data packets.

description

**qos qosprofile** command configuration is the value of the data packets.

**no qos dscp-map-qp** command back to the default mapping

Example

# configuration dscp value of 50 mapped to the column qp1.

**Switch(config)#qos qosprofile qp1 weight 50**

## 7.1.3 qos wrr-hqp

command

**qos wrr-hqp**

**no qos wrr-hqp**

mode

configuration mode.

parameters

without .

description

**qos wrr-hqp** command to start the highest priority column.

**no qos wrr-hqp** command to remove the maximum priority to the column.

Example

**Switch(config)#qos wrr-hqp**

## 7.1.4 qos cos-based

command

**qos cos-based**

**no qos cos-based**

mode

interface configuration mode.

parameters

without .

description

**qos cos-based** command configuration based cos’ sqos.

**no qos cos-based** command cancel qos.

Example

# on the port fe1/1configure cos-based qos.

**Switch(config-fe1/1)#qos cos-based**

## 7.1.5 qos dscp-based

command

**qos dscp-based**

**no qos dscp-based**

mode

interface configuration mode.

parameters

without .

description

**qos dscp-based** command configuration dscp-based qos.

**no qos dscp-based** command cancel qos.

Example

#Set port fe1/1configure dsc-based qos.

**Switch(config-fe1/1)#qos dscp-based**

## 7.1.6 qos port-based

command

**qos port-based**

**no port-based**

mode

interface configuration mode.

parameters

without .

description

**port-based** command configuration: port-based qos.

**no port-based** command cancel qos.

Example

#at the port fe1/1configuration port-based qos.

**Switch(config-fe1/1)#qos port-based**

## 7.1.7 qos user-priority

command

**qos user-priority <pri-value>**

**no qos user-priority**

mode

interface configuration mode.

parameters

**Pri-value:** Priority value.

description

**qos user-priority** command express no-tag packet's value of cos.

**no qos user-priority** command back to the default value.

Example

#at the port fe1/1configurationuser-priority's value is 5.

**Switch(config-fe1/1)#qos user-priority 5**

## 7.2 QOS View command

### 7.2.1 show qos

command

**show qos**

mode

normal mode/privileged mode.

parameters

without .

description

**show qos** command displays the global QoS configuration information..

Example

without

### 7.2.2 show qos interface

command

**show qos interface [if-name]**

mode

normal mode/privileged mode.

parameters

**if-name：** interface name .

description

**show qos interface** command view port qos's info.

Example

**Switch#show qos interface fe1/1**

**Port-Based QoS : Disable**
**SCP-Based QoS : Disable**
**COS-Based QoS : Enable**
**Default Priority : 0/QP0**

# Chapter 8 STP command

## 8.1 STP configuration command

### 8.1.1 spanning-tree mst cisco-interoperability

command

**spanning-tree mst cisco-interoperability {disable | enable}**

mode

configuration mode

parameters

**disable:** closing function. Off by default.

**enable:** Open function.

description

Enable or disable the Spanning Tree Protocol and cisco compatible.

Heavenly Creations network switch 802.1s based STP protocol for each STI message length is 16 bytes; and CISCO switches, BPDU length of each of STI message is 26 bytes. Household in order, and CISCO switches, configuration tico to start when the network switches and CISCO compatible switch

Example

without .

### 8.1.2 spanning-tree mst enable

command

**spanning-tree mst enable**

mode

configuration mode

parameters

without

description

Start stp calculation.

Example

without .

### 8.1.3 spanning-tree mst errdisable-timeout

command

**spanning-tree mst errdisable-timeout {enable | interval <seconds>}**

**no spanning-tree mst errdisable-timeout {enable | interval}**

mode

configuration mode

parameters

**seconds:** Time-out time, the scope 10-1000000 seconds. Default 300 seconds.

description

**spanning-tree mst errdisable-timeout enable** command start errdisable mechanism, when the start of the port BPDU gurad received BPDU, it will start errordisable timer. errordisable will be in the system configuration of the timeout time to re-activate the port.

**spanning-tree mst errdisable-timeout interval** command set errordisable timeout.

**no spanning-tree mst errdisable-timeout** command be used to cancel the configuration, restore the default value.

Example

without .

## 8.1.4 spanning-tree mst forward-time

command

**spanning-tree mst forward-time <seconds>**

**no spanning-tree mst forward-time**

mode

configuration mode.

parameters

**seconds:** port from discarding to learning, and learning to the forwarding number of seconds to wait. Range is 4-30 seconds. The default is 15 seconds.

According to the agreement generated a few forward-time must meet the following conditions：2*(forward-time - 1) >= max-age.

description

**spanning-tree mst forward-time** command is used to configure forward delay time.

**no spanning-tree mst forward-time** command is used to cancel configure forward delay time，back to the default value.

Example

without .

## 8.1.5 spanning-tree mst hello-time

command

s**panning-tree mst hello-time <seconds>**

**no spanning-tree mst hello-time**

mode

configuration mode

parameters

**seconds:** the generated intervals with the switch. Range is 1-10 seconds. Defaults is 2 seconds.

According to generate the number of agreements hello-time must meet the following conditions: 2*(hello-time + 1) =< max-age.

description

**spanning-tree mst hello-time** configuration STP hello packet send interval time.

**no spanning-tree mst hello-time** command cancel the configuration，back to the default value.

Example

#Configuration hello packet send interval time is 10 seconds：

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

## 8.1.6 spanning-tree mst max-age

command

**spanning-tree mst max-age <seconds>**

**no spanning-tree mst max-age**

mode

configuration mode

parameters

**seconds:** the switch trigger a re-configuration before waiting to receive spanning tree configuration information in seconds. Range of 6-40 seconds. Default 20 seconds

description

configure the maximum time of trunk the root bridge

no command cancel configuration, restore the default value

Example

without .

## 8.1.7 spanning-tree mst max-hops

command

**spanning-tree mst max-hops <hops>**

**no spanning-tree mst max-hops**

mode

configuration mode

parameters

**hops：** In a field in the BPDU is discarded before the specified number of hops. Range of 1-40. Default is 20 jump.

description

configure BPDU protocal packet effective the maximum hops.

no command cancel configuration, restore the default value.

Example

without .

## 8.1.8 spanning-tree mst portfast

command

**spanning-tree mst portfast**

**no spanning-tree mst portfast**

mode

interface configuration mode

parameters

without

description

**spanning-tree mst portfast** command configuration :one port as portfast port, enable the port from blocking state to forwarding state, bypassing the listening and learning state.

no command cancel configuration, restore the default value.

Example

#configure port fe1/1as portfast interface：

**Switch(config-fe1/1)#spanning-tree mst portfast**

## 8.1.9 spanning-tree mst portfast bpdu-filter

command

**spanning-tree mst portfast bpdu-filter [default | disable | enable]**

**no spanning-tree mst portfast bpdu-filter**

mode

configuration mode/interface configuration mode

parameters

**default:** default state

**disable:** closing function.

**enable:** Enable feature.

description

To prevent the portfast port to receive or send BPDU.

On configuration mode，spanning-tree mst portfast bpdu-filter command start portfast bpdu-filter default status's port BPDU filtering functions. At interface configuration mode，spanning-tree mst portfast bpdu-filter enable open the BPDU filter in any port.

no command cancel configuration, restore the default value.

Example

#configure port fe1/1as portfast interface， do not send stp bpdu packet：

**Switch(config-fe1/1)#spanning-tree mst portfast**

**Switch(config-fe1/1)#spanning-tree mst portfast bpdu-filte enable**

## 8.1.10 spanning-tree mst portfast bpdu-guard

command

**spanning-tree mst portfast bpdu-guard [default | disable | enable]**

**no spanning-tree mst portfast bpdu-guard**

mode

configuration mode/interface configuration mode

parameters

**default:** default state

**disable:** closing function.

**enable:** Enable feature.

description

When the configuration of the port BPDU gurad received BPDU when, spanning tree will be shutdown this port. In a valid configuration, Port Fast-enabled ports do not receive BPDU. In a portfast enabled port receives a BPDU that without an efficient configuration, for example, an unauthorized device connections, BPDU guard into an error-disabled state.

No commandcancel configuration, restore the default value.

Example

#configure port fe1/1as portfast interface ， start BPDU protect functions：

**Switch(config-fe1/1)#spanning-tree mst portfast**

**Switch(config-fe1/1)#spanning-tree mst portfast bpdu-guard enable**

## 8.1.11 spanning-tree mst priority

command

**spanning-tree mst priority <value>**

mode

configuration mode

parameters

**value：**CIST bridge priority ，range 0-61440，default value 32768. CIST priority values can only be in multiples of 4096.

description

configure bridge priority. Bridge low priority devices are more likely to become the root bridge

Example

#Configuration CIST bridge priority is 36862：

**Switch#configure terminal**

**Switch(config)#spanning-tree mst priority 36862**

## 8.1.12 spanning-tree mst force-version

command

**spanning-tree mst force-version <version>**

**no spanning-tree mst force-version**

mode

interface configuration mode

parameters

**version：** protocal’ s type，Range 0-3，

0 - express STP protocal，

1 - stand that not support spanning tree.，

2 - stand RSTP protocal，

3 - stand STP protocal .

default protocal type is 0.

description

configuration send protocal packet type.

No command cancel configuration, restore the default value.

Example

#configure port fe1/1send stp protocal packet：

**Switch(config-fe1/1)# spanning-tree mst force-version 0**

## 8.1.13 spanning-tree mst guard root

command

**spanning-tree mst guard root**

**no spanning-tree mst guard root**

mode

interface configuration mode

parameters

without

description

configure start root guard function，Not to receive the bridge priority higher than their BPDU packets, specify the switch as the root switch. Off by default.

No command cancel configuration, restore the default value.

Example

without .

## 8.1.14 spanning-tree mst link-type

command

**spanning-tree mst link-type { point-to-point | shared}**

**no spanning-tree mst link-type**

mode

interface configuration mode

parameters

**point-to-point:** point to point connection type, allowing the port state of rapid transformation. As the default type.

**shared:** Connection type is shared, does not allow port status quickly transform the process to go through 802.1D calculations to determine the status of the port. .

description

configue interface the type of connection.

No command cancel configuration, restore the default value.

Example

without .

## 8.1.15 spanning-tree mst path-cost

command

**spanning-tree mst path-cost <cost>**

**no spanning-tree mst path-cost**

mode

interface configuration mode

parameters

**cost:** cist path cost value, range 1-200000000. The default value is 20000000. A lower path cost is more likely to be the root.

The following is the path bandwidth and overhead mapping table:

| Bandwidth (bps) | Path overhead |
|---|---|
| 100,000(100K) | 200000000 |
| 1,000,000(1M) | 20000000 |
| 10,000,000(10M) | 2000000 |
| 100,000,000(100M) | 200000 |
| 1,000,000,000(1G) | 20000 |
| 10,000,000,000(10G) | 2000 |
| 100,000,000,000(100G) | 200 |
| 1,000,000,000,000(1T) | 20 |
| >1000000000000 | 2 |

description

Configure cist path overhead.

No command cancel configuration, restore the default value.

Example

# configuration example 2-port fe1 / 1 path cost of 200 of the cist:

**Switch(config-fe1/1)#spanning-tree mst path-cost 200**

**Switch#show spanning-tree mst instance 2 interface fe1/1**

**% fe1/1: Port 2001 - Id 87d1 - Role Disabled - State Forwarding**

**% fe1/1: Designated Internal Path Cost 0 - Designated Port Id 0**

**% fe1/1: Configured Internal Path Cost 20000000**

**% fe1/1: Configured CST External Path cost 200**

**% fe1/1: CST Priority 128 - MSTI Priority 128**

**% fe1/1: Designated Root 0000000000000207**

**% fe1/1: Designated Bridge 0000000000000207**

**% fe1/1: Message Age 0 - Max Age 0**

**% fe1/1: Hello Time 0 - Forward Delay 0**

**% fe1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0**

## 8.1.16 spanning-tree mst priority

command

**spanning-tree mst priority <value>**

mode

interface configuration mode

parameters

**value:** cist port priority, the scope of 0-240, only a multiple of 16. The default value is 128.

description

configuration interface cist priority.

Example

# configuration examples of two-port fe1 / 1 of the cist priority 240:

**Switch(config-fe1/1)#spanning-tree mst priority 240**

**Switch#show spanning-tree mst instance 2 interface fe1/1**

**% fe1/1: Port 2001 - Id f7d1 - Role Disabled - State Forwarding**

**% fe1/1: Designated Internal Path Cost 0 - Designated Port Id 0**

**% fe1/1: Configured Internal Path Cost 10**

**% fe1/1: Configured CST External Path cost 20000000**

**% fe1/1: CST Priority 240 - MSTI Priority 160**

**% fe1/1: Designated Root 0000000000000207**

**% fe1/1: Designated Bridge 0000000000000207**

**% fe1/1: Message Age 0 - Max Age 0**

**% fe1/1: Hello Time 0 - Forward Delay 0**

**% fe1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0**

## 8.1.17 clear spanning-tree detected protocols

command

**clear spanning-tree detected protocols [interface <if-name>]**

mode

privileged mode

parameters

**if-name:** need to reset the port STP protocol detection feature.

description

In order to, and is compatible with 802.1D STP protocol, the system can automatically detect each other's system operation agreement, according to the agreement to run the other side to determine the port operation agreement. clear spanning-tree detected protocols command reset it to the task of protocol negotiation to renegotiate the agreement between it and the host.

Example

# Close Module 1-port one of the STP protocol detection feature

**Switch#clear spanning-tree detected protocols interface fe1/1**

# 8.2 STP VIEW command

## 8.2.1 show spanning-tree mst

command

**show spanning-tree mst [config | detail | instance <instance-id> [interface <if-name>] | interface <if-name>]**

mode

normal mode/privileged mode

parameters

**instance-id:** instance number, range 0-15.

**if-name:** port number

description

**show spanning-tree mst** command show vlan and cist information as well as the corresponding form instance.

**show spanning-tree mst config** command show stp the configuration information.

**show spanning-tree mst detail** command show stp detailed information, including the cist interface information, examples of information and examples of interface information.

**show spanning-tree mst instance <instance-id>** command displays an example of information.

**show spanning-tree mst instance <instance-id> interface <if-name>** command displays a cist interface information.

**show spanning-tree mst interface <if-name>** displays a stp interface information.

Example

#show stpconfiguration info：

**Switch#show spanning-tree mst config**

**%**

**% MSTP Configuration Information for bridge 1 ：**

**%----------**

**% Format Id : 0**

**% Name : Switch**

**% Revision Level :1**

**% Digest : 0xD042DCDBBC60C63B623C157F60A37A6F**

**%----------**

**Switch#**

# Show examples of an interface within the fe1 / 1 of the stp Information：

**Switch#show spanning-tree mst instance 1 interface fe1/1**

**% fe1/1: Port 2001 - Id 87d1 - Role Disabled - State Discarding**

**% fe1/1: Designated Internal Path Cost 0 - Designated Port Id 0**

**% fe1/1: Configured Internal Path Cost 20000000**

**% fe1/1: Configured CST External Path cost 20000**

**% fe1/1: CST Priority 128 - MSTI Priority 128**

**% fe1/1: Designated Root 0000000000000000**

**% fe1/1: Designated Bridge 0000000000000000**

**% fe1/1: Message Age 0 - Max Age 0**

**% fe1/1: Hello Time 0 - Forward Delay 0**

**% fe1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0**

## 8.3 STP debugging command

### 8.3.1 debug mstp

command

**debug mstp**

**no debug mstp**

mode

privileged mode.

parameters

without .

description

**debug mstp** command to open stp revelent protocal timer debugging switch, the relevant logs written to the log table.

**no debug mstp** command be used to turn off debugging stp timer switch.

Example

# Open stp debugging switch timer

**Switch#debug mstp**

## 8.3.2 debug mstp all

command

**debug mstp all**

**no debug mstp all**

mode

privileged mode.

parameters

without .

description

**debug mstp all** command to open stp revelent protocal timer debugging switch, the relevant logs written to the log table

**no debug mstp all** command be used to turn off debugging stp timer switch.

Example

# Open all stp debugging switch timer：

**Switch#debug mstp all**

## 8.3.3 debug mstp cli

command

**debug mstp cli**

**no debug mstp cli**

mode

privileged mode.

parameters

without .

description

**debug mstp cli** command to open stp command timer debugging switch, the relevant logs written to the log table.

**no debug mstp cli** command be used to turn off debugging stp command timer switch.

Example

# Open the stp command debugging switch timer：

**Switch#debug mstp cli**

## 8.3.4 debug mstp packet

command

**debug mstp packet [recv | send]**

**no debug mstp packet [recv | send]**

mode

privileged mode.

parameters

without .

description

**debug mstp packet** command to open stp timer debugging switch, the relevant logs written to the log table.

**no debug mstp packet** command be used to turn off debugging stp timer switch.

Example

# Open the stp protocol debugging switch timer:

**Switch#debug mstp packet recv**

## 8.3.5 debug mstp protocol

command

**debug mstp protocol [detail]**

**no debug mstp protocol [detail]**

mode

privileged mode.

parameters

without .

description

**debug mstp timer** command agreement to open stp timer debugging switch, the relevant logs written to the log table.

**no debug mstp timer** command be used to turn off debugging stp timer switch.

Example

# Open the stp protocol debugging switch timer:

**Switch#debug mstp protocol detail**

## 8.3.6 debug mstp timer

command

**debug mstp timer [detail]**

**no debug mstp timer [detail]**

mode

privileged mode.

parameters

without .

description

**debug mstp timer** command agreement to open stp timer debugging switch, the relevant logs written to the log table.

**no debug mstp timer** command be used to turn off debugging stp timer switch.

Example

#Open the stp protocol debugging switch timer：

**Switch#debug mstp timer detail**

# Chapter 9 AAA Command

## 9.1 802.1x Command

### 9.1.1 dot1x

Command

**dot1x**

**no dot1x**

Mode

Configuration mode

Parameters

Without

Description:

**dot1x** command to open the switch 802.1x protocol to establish a AAA environment, we must first implement this command to open the 802.1x protocol.

**no dot1x** command close the protocal of switch- 802.1x, 802.1x protocol can not be established after the closure of AAA environment.

Example

# open 802.1x protocal.

**Switch# dot1x**

# close 802.1x protocal.

**Switch# no dot1x**

## 9.1.2 dot1x default

Command

**dot1x default**

Mode

Configuration mode

Parameters

Without

Description

Let 802.1x protocol configuration to return to the default state .

Example

#Let 802.1x protocol configuration to return to the default state .

**Switch# dot1x default**

## 9.1.3 dot1x control auto

Command

**dot1x control auto**

Mode

interface Configuration mode

Parameters

Without

Description

Configure a port on auto state, all user who under the port to access the network should through authentication

Example

# configure port fe1/1 as the Auto Status:

**Switch(config-fe1/1)dot1x control auto**

## 9.1.4 dot1x control force-authorized

Command

**dot1x control force-authorized**

Mode

interface Configuration mode

Parameters

Without

Description

Configure a port on force-authorized state, all user who under the port to will access the network without authentication

Example

# configure port fe1/1 as Force-authorized Status:

**Switch(config-fe1/1)dot1x control force-authorized**

## 9.1.5 dot1x control force-unauthorized

Command

**dot1x control force-unauthorized**

Mode

interface Configuration mode

Parameters

Without

Description

Configure a port to force-unauthorized state, the user who under this port always can not access the network.

Example

# configure port fe1/1 as Force-authorized Status:

**Switch(config-fe1/1)dot1x control force-unauthorized**

## 9.1.6 no dot1x control

Command

**no dot1x control**

Mode

Interface configuration mode.

Parameters

without

Description

Configure a port as N / A state, the useers under the port be able to access network without authenticate.

Example

# Configure fe1/1 as N / A state

**Switch(config-fe1/1)no dot1x control**

**Switch(config-fe1/1)**

## 7.1.7 dot1x reauthenticate

Command

**dot1x reauthenticate**

**no dot1x reauthenticate**

Mode

configuration mode.

Parameters

without

Description

**dot1x reauthenticate** to open the 802.1x protocal's renewed authentication mechanisms.

**no dot1x reauthenticate** to close the 802.1x protocal's renewed authentication mechanisms.

Example

# Open the re-authentication mechanism

**Switch# dot1x reauthenticate**

# close the re-authentication mechanism

**Switch# no dot1x reauthenticate**

## 9.1.8 dot1x timeout re-authperiod

Command

**dot1x timeout re-authperiod <interval>**

Mode

configuration mode.

Parameters

**interval:** specifies the time re-certification interval in seconds.

Description

Configure the 802.1x protocol to re-certification time interval.

Example

# Configure the re-certification of the time interval 1000 seconds

**Switch# dot1x timeout re-authperiod 1000**

## 9.1.9 dot1x support-host

Command

**dot1x support-host <number>**

Mode

Interface configuration mode.

Parameters

**number:** specified port 's maximum certified hosts number.

Description

Configure port's maximum certified hosts number.

Example

# Configure port fe1 / 1 the largest number access to the hosts 100:

**Switch(config-fe1/1) #dot1x support-host 100**

## 9.1.10 dot1x timeout tx-period

Command

**dot1x timeout tx-period <interval>**

Mode

configuration mode

Parameters

**interval:** specifies the switch resend EAP-Request protocol packet interval time, in seconds.

Description

Configure the switch resend EAP-Request protocol packet interval time,

Example

Configure the switch resend EAP-Request protocol packet interval time, in 20 seconds.

**Switch(config)#dot1x timeout tx-period 20**

## 9.1.11 dot1x max-req

Command

**dot1x max-req <number>**

Mode

configuration mode

Parameters

**number:** the times of Specifies the switch resend EAP-Request protocol packets

Description

the times of configure the switch resend EAP-Request protocol packets.

Example

# Configure the switch resend EAP-Request protocol package’s time as 2 times:

**Switch(config)#dot1x max-req 2**

## 9.1.12 dot1x timeout quiet-period

Command

**dot1x timeout quiet-period <interval>**

Mode

configuration mode

Parameters

**interval:** specifies user authentication fails, wait for the re-certification interval, in seconds.

Description

Configure user authentication fails, to wait for re-certification intervals.

Example

# Configure the user authentication fails, to wait for the re-certification interval time of 20 seconds

**Switch(config)#dot1x timeout quiet-period 20**

## 9.1.13 dot1x timeout server-timeout

Command

**dot1x timeout server-timeout <interval>**

Mode

configuration mode

Parameters

**interval:** Specifies the switch to the authentication server RADIUS packet retransmission interval, in seconds

Description

Configure the switch to the authentication server RADIUS packet retransmission interval.

Example

# Configure the switch to the RADIUS packet authentication server retransmission interval time of 20 seconds:

**Switch(config)#dot1x timeout server-timeout 20**

## 9.1.14 dot1x timeout supp-timeout

Command

**dot1x timeout supp-timeout <interval>**

Mode

configuration mode

Parameters

**interval:** Specifies the switch to the client re-send eap request packet interval, in seconds.

Description

Configure the switch to the client re-send eap request packet interval,

Example

# Configure the switch to the client re-send eap request packet interval in 30 seconds

**Switch(config)#dot1x timeout supp-timeout 30**

## 9.1.15 dot1x transmit-port

Command

**dot1x transmit-port**

**no dot1x transmit-port**

Mode

configuration mode

Parameters

without

Description

Configure the switch to connect the client and the authentication switch port transmit port, the client and the 802.1x authentication exchange between the forward eapol certification package.

Configure switch contact clients

Example

# Configure port fe1/1 for the transfer port:

**Switch(config-fe1/1)#dot1x transmit-port**

# Configure port fe1/1 for non-transfer port:

**Switch(config-fe1/1)#no dot1x transmit-port**

## 9.1.16 dot1x client-version

command

**dot1x client-version <string>**

mode

configuration mode.

parameters

**string:** Specifies 802.1x client version number.

description

configuration 802.1x client version number

Example

#configuration 802.1x Client's version number

**Switch(config)# dot1x client-version 2.0**

## 9.1.17 dot1x check-client

command

**dot1x check-client**

mode

configuration mode.

parameters

without .

description

configuration check the existence of the client.

Example

**Switch (config)#dot1x check-client**

## 9.1.18 dot1x check-version

command

**dot1x check-version {open | close }**

mode

configuration mode.

parameters

**open:** Check the client version numbers.

**close:** Does not check the client version numbers.

description

Configure whether to check the version of the client.

Example

Without

## 9.1.19 show dot1x

command

**show dot1x**

**show dot1x interface**

mode

Privileges mode.

parameters

without .

description

When the command is when the show dot1x to show all of the 802.1xconfiguration information, including all ports of the configuration information; show dot1x interface when the command is displayed when all access to the port under the user's information.

Example

# Show all 802.1xconfiguration information:

**Switch#show dot1x**

# Show all the access port under the user's information:

**Switch#show dot1x interface**

## 9.2 radius-servercommand

### 9.2.1 radius-server host

command

**radius-server host <ip-address>**

mode

configuration mode.

parameters

**ip-address:** Specifies the primary authentication server's IP address.

description

configuration primary authentication server's IP address.

Example

#configuration the primary authentication server is198.168.80.111:

**Switch(config)#radius-server host 198.168.80.111**

### 9.2.2 radius-server option-host

command

**radius-server option-host <ip-address>**

mode

configuration mode.

parameters

**ip-address:** Specify the backup authentication server's IP address.

description

Configure the backup authentication server's IP address.

Example

# Configure the backup authentication server for 198.168.80.110:

**Switch(config)#radius-server option-host 198.168.80.110**

### 9.2.3 radius-server key

command

**radius-server key <string>**

mode

configuration mode.

parameters

**string:** Specifies the switch's shared secret key.

description

Configuration between the switch and authentication server shared key authentication.

Example

# Configure the switch shared key for abcdef:

**Switch(config)#radius-server key abcdef**

## 9.2.4 radius-server accounting

command

**radius-server accounting**

**no radius-server accounting**

mode

configuration mode.

parameters

without .

description

**radius-server accounting** billing functions to open the switch.

**no radius-server accounting** off switch billing functions.

Example

# Open the billing function:

**Switch (config) # radius-server accounting**

# Close the billing functions:

**Switch(config)#no radius-server accounting**

## 9.2.5 radius-server udp-port

command

**radius-server udp-port <port-number>**

mode

configuration mode.

parameters

**port-number:** Specifies the switch and the authentication server authentication packets between the UDP port number.

description

Configure the switch with the authentication server authentication packets between the UDP port number. Under normal circumstances the user do not need to modify the authentication UDP port number.

Example

# Configure the authentication packets UDP port number is 1812:

**Switch(config)#radius-server udp-port 1812**

## 9.2.6 radius-server attribute nas-portnum

command

**radius-server attribute nas-portnum <number>**

mode

configuration mode.

parameters

**Number:** Specifies NAS Port property values.

description

Configuration NAS Port property values.

Example

# Configure NAS Port property value 1000:

**Switch(config)#radius-server attribute nas-portnum 1000**

## 9.2.7 radius-server attribute nas-porttype

command

**radius-server attribute nas-porttype <number>**

mode

configuration mode.

parameters

**number:** Specifies NAS Port Type property values.

description

Configuration NAS Port Type property values.

Example

# Configure NAS Port Type property value of 10:

**Switch(config)#radius-server attribute nas-porttype 10**

## 9.2.8 radius-server attribute service-type

command

radius-server attribute service-type <number>

mode

configuration mode.

parameters

**number:** Specifies NAS Port Server property values.

description

Configuration NAS Port Server property values.

Example

# Configure NAS Port Server property value of 3:

**Switch(config)#radius-server attribute service-type 3**

## 9.2.9 radius-server vsa

command

**radius-server vsa <string>**

mode

configuration mode.

parameters

**string:** Specify vendor-specific information.

description

configure RADIUS Property of the vendor-specific information.

Example

**Switch(config)# radius-server vsa Switch**

## 9.2.10 adius-server roam

command

**adius-server roam**

**no radius-server roam**

mode

configuration mode.

parameters

without .

description

**adius-server roam** open RADIUSR roaming.

**no radius-server roam** close RADIUS roaming.

Example

#configuration RADIUS roaming：

**Switch(config)#radius-server roam**

#close RADIUS roaming：

**Switch(config)#no radius-server roam**

## 9.2.11 show radius-server

command

**show radius-server**

mode

normal mode/privileged mode.

parameters

without .

description

show RADIUS relevant configuration info.

Example

# show RADIUS configuration info：

**Switch# show radius-server**

# Chapter 10 IGMP SNOOPING command

## 10.1 IGMP SNOOPING configuration commands

### 10.1.1 ip igmp snooping

Command

**ip igmp snooping**

**no ip igmp snooping**

Mode

Configuration Mode

Parameters

Without

Description

**ip igmp snooping** command is used to start all vlan's igmp snooping capabilities.

**no igmp snooping** command is used to close all vlan's igmp snooping capabilities.

Example

Without

### 10.1.2 ip igmp snooping fast-leave

Command

**ip igmp snooping fast-leave vlan <vlan-id>**

**no ip igmp snooping fast-leave vlan <vlan-id>**

Mode

Configuration Mode

Parameters

**vlan-id:** to start fast-leave vlan number.

Description

Start a vlan fast-leave function of IGMP V2.

no command to close a vlan fast -leave functions of IGMP V2 .

Example

# Start vlan2 multicast members immediately leave the function:

**Switch(config)#ip igmp snooping fast-leave vlan 2**

## 10.1.3 ip igmp snooping fast-leave-timeout

Command

**ip igmp snooping fast-leave-timeout <interval> vlan <vlan-id>**

**no ip igmp snooping fast-leave-timeout vlan <vlan-id>**

Mode

Configuration mode

Parameters

**Interval:** Delay time, unit ms, no range restriction. The default is 300000 ms.

**vlan-id:** The configuration of the vlan number, range 1-4094.

Description:

To set up a vlan multicast members fast-leave-timeout, to delete the members after the receipt of leave packets waiting to the specified time interval.

no command cancel fast-leave-timeout, interval to restore the default value

Example

# Configure vlan1 is used to delete the members immediately after received leave packet from igmp snooping members

**Switch(config)#ip igmp snooping fast-leave vlan 1**

**Switch(config)#ip igmp snooping fast-leave-timeout 0 vlan 1**

## 10.1.4 ip igmp snooping group-membership-timeout

Command

**ip igmp snooping group-membership-timeout <interval> vlan <vlan-id>**

**no ip igmp snooping group-membership-timeout vlan <vlan-id>**

Mode

Configuration mode

Parameters

**interval:** members survival time, units ms, no range restriction. By default 400000 ms.

**vlan-id:** The configuration of the vlan number, range 1-4094.

Description

Configuration after receiving report package to join the igmp snooping group’s survival time.

no command cancel the configuration of members of the survival time, restore the

default value.

Example

# Configure igmp snooping members vlan2 survival time of 600 seconds:

**Switch(config)#ip igmp snooping group-membership-timeout 600000 vlan 2**

## 10.1.5 ip igmp snooping mrouter

Command

**ip igmp snooping mrouter vlan <vlan-id>**

**no ip igmp snooping mrouter vlan <vlan-id>**

Mode

Interface Configuration Mode

parameters

**vlan-id:** interface vlan number belongs

Description

Configure the query port, other ports which received the igmp snooping join to the leave packet will be forwarded to the port; the port would join the igmp snooping group.

no command to delete the query port of configure.

Example

# Configure port fe1 / 1 for the vlan2 query port:

**Switch(config-fe1/1)#no ip igmp snooping mrouter vlan 2**

## 10.1.6 ip igmp snooping query-membership-timeout

Command

**ip igmp snooping query-membership-timeout <interval> vlan <vlan-id>**

**no ip igmp snooping query-membership-timeout vlan <vlan-id>**

Mode

Configuration Mode

parameters

**interval:** Query port survival time, units ms, range 60000-300000ms. Default is 300000 ms.

**vlan-id:** The configuration of the vlan of the vlan number, range 1-4094.

Description

configuration received of QUERY packets and join QUERY group survival time.

no command is used to cancelled Inquiry survival time configuration, restore the default value.

Examle:

# Configure Query port vlan2 survival time of 600 seconds:

**Switch(config)#ip igmp snooping query-membership-timeout 600000 vlan 2**

## 10.1.7 ip igmp snooping vlan

Command

**ip igmp snooping vlan <vlan-id>**

**no ip igmp snooping vlan <vlan-id>**

Mode

Configuration Mode

parameters

**vlan-id:** vlan number.

Description

Start a vlan's igmp snooping feature, you must first implementation of the ip igmp snooping before configure a vlan features.

no ordered the closure of a vlan's igmp snooping capabilities.

Example

# Close the igmp snooping feature of vlan3, the other vlan open igmp snooping features:

**Switch(config)#no ip igmp snooping vl**

**Switch(config)#no ip igmp snooping vlan 3**

## 10.1.8 ip igmp snooping explicit-tracking

Command

**ip igmp snooping explicit-tracking vlan <vlan-id>**

**no ip igmp snooping explicit-tracking vlan <vlan-id>**

Mode

Configuration Mode

parameters

.**vlan-id:** vlan number.

Description

Start a vlan's igmp snooping explicit-tracking capabilities.

no command close a vlan's igmp snooping explicit-tracking capabilities.

Example:

#open the igmp snooping explicit-tracking functions of vlan1.

**Switch(config)# ip igmp snooping explicit-tracking vlan 1**

#Close the igmp snooping explicit-tracking functions of vlan3

**Switch(config)#no ip igmp snooping explicit-tracking vlan 3**

## 10.1.9 ip igmp snooping ssm-safe-reporting

Command

**ip igmp snooping ssm-safe-reporting vlan <vlan-id>**

**no ip igmp snooping ssm-safe-reporting vlan <vlan-id>**

Mode

Configuration Mode

parameters

**vlan-id:** vlan number.

Description

Start a vlan's igmp snooping ssm-safe-reporting capabilities.

no command close a vlan's igmp snooping ssm-safe-reporting capabilities.

Example:

#open the igmp snooping ssm-safe-reporting functions of vlan1.

**Switch(config)# ip igmp snooping ssm-safe-reporting vlan 1**

#close vlan3’s s igmp snooping ssm-safe-reporting functions

**Switch(config)#no ip igmp snooping ssm-safe-reporting vlan 3**

# 10.2 IGMP SNOOPING VIEW COMMAND

## 10.2.1 show ip igmp snooping

Command

**show ip igmp snooping [fast-leave [vlan <vlan-id>] | fast-leave-timeout [vlan <vlan-id>] | forwarding-table | group-membership-timeout [vlan <vlan-id>] | interface [vlan <vlan-id>] | query-membership-timeout [vlan <vlan-id>] | vlan <vlan-id> ]**

Mode

Normal Mode/Privileged mode

parameters

**fast-leave:** showing the case of opening fast-leave function

**vlan <vlan-id>:** displays the specified vlan configuration.

**fast-leave-timeout:** Display fast-leave-timeout configuration.

**forwarding-table:** display IGMP snooping forwarding table, including the IGMP snooping group and the corresponding vlan, port.

**group-membership-timeout:** Show group membership survival time configuration.

**interface:** display the relationship between the workable port and vlan.

**query-membership-timeout:** Display query survival time configuration.

**vlan:** Display the specified vlan's igmp snooping configuration.

Description

Display igmp snooping configuration.

Example

#show vlan1’s igmp snooping configuration：

**Switch#show ip igmp snooping vlan 1**

**Bridge 1 VLAN 0:**

**IGMP Snooping is globally enabled**

**Bridge 1: VLAN 1**
**IGMP Snooping is enabled**
**IGMP Snooping fast-leave is enabled**
**IGMP Snooping fast-leave-timeout is 300000 ms**
**IGMP snooping query membership timeout is 300000 ms**
**IGMP snooping group membership timeout is 400000 ms**

## 10.2.2 show ip igmp snooping age-table

Command

**show ip igmp snooping age-table { group-membership | query-membership}**

Mode

Normal Mode/Privileged mode

parameters

**group-membership:** show members group's age time.

**query-membership:** display the query group's age time.

Description

Showing the IMGP snooping group 's age time, and surrounding of ports.

Example

**Switch#show ip igmp snooping age-table group-membership**

| VLAN | Address | Port | Seconds |
|---|---|---|---|
| 3 | 239.255.255.250 | fe1/2 | 340000 ms |

## 10.2.3 show ip igmp snooping mrouter

Command

**show ip igmp snooping mrouter [interface <if-name> | vlan <vlan-id>]**

Mode

Normal Mode/Privileged mode

parameters

**interface <if-name>:** displays the specified port

**vlan <vlan-id>:** displays the specified vlan query port.

Description

Display the query port information.

Example

# Show vlan3 query port:

**Switch#show ip igmp snooping mrouter vlan 3**

| Bridge | VLAN | Ports |
|---|---|---|
| 1 | 3 | fe1/2, |

## 10.2.4 show ip igmpv2

Command

**show ip igmpv2 snooping statistics [vlan <vlan-id>]**

Mode

Normal Mode/Privileged mode

parameters

**vlan <vlan-id>:** showing specified vlan's circumstances.

Description

show the statistics of igmpv2 protocol packet.

Example

# Show the Statistics of igmpv2 protocol packets of vlan1 .

**Switch#show ip igmpv2 snooping statistics vlan 1**

**IGMP-V2 Snooping Statistics: Bridge 1 VLAN default**
**Total valid pkts rcvd : 0**
**Total invalid pkts rcvd : 0**
**Number of Reports rcvd : 0**
**Number of Leaves rcvd : 0**
**Number of Membership Queries rcvd : 0**
**Number of Reports tx : 0**
**Number of Leaves tx : 0**
**Number of Group-Specific Queries tx : 0**
**Number of General Queries tx : 0**

## 10.2.5 show ip igmp snooping explicit-tracking

Command

**show ip igmp snooping explicit-tracking vlan <vlan-id>**

Mode

Normal Mode/Privileged mode

parameters

**vlan-id:** vlan number.

Description

Display vlan's igmp snooping explicit-tracking of functional status and details.

Example

#show the igmp snooping explicit-tracking function of vlan1

**Switch#show ip igmp snooping explicit-tracking vlan 1**

## 10.2.6 show ip igmp snooping ssm-safe-reporting

Command

**show ip igmp snooping ssm-safe-reporting vlan <vlan-id>**

Mode

Normal Mode/Privileged mode

parameters

**vlan-id:** vlan number.

Description

Display vlan's igmp snooping ssm-safe-reporting of functional status

Example

Display vlan1's igmp snooping ssm-safe-reporting of functional status

**Switch#show ip igmp snooping ssm-safe-reporting vlan 1**

## 10.2.7 show ip igmpv3

Command

**show ip igmpv3 snooping statistics [vlan <vlan-id>]**

Mode

Normal Mode/Privileged mode

parameters

**vlan <vlan-id>:** display of the specified vlan

Description

Show igmpv3 protocol packet statistics.

Example

# show igmpv3 protocol packtet statistics of vlan1

**Switch#show ip igmpv3 snooping statistics vlan 1**

# 10.3 IGMP SNOOPING debug commands

## 10.3.1 debug igmp snooping

Command

**debug igmp snooping [all] | [cli] | [events] | [packet] | [timer]**

**no debug igmp snooping [all] | [cli] | [events] | [packet] | [timer]**

Mode

Privileged mode

parameters

**all:** Open all debug igmp snooping switches.

**cli:** cli command prompt.

**events:** Open igmp snooping time debug switch.

**packet:** Open the igmp snooping packets debugging switch.

**timer:** Open the igmp snooping timer debug switch.

Description

**debug igmp snooping** command is used to open the relevant debugging igmp snooping switch, allowing users to see the relevant events and igmp snooping packet send and receive cases.

**no debug igmp snooping** command is used to close corresponding debug igmp snooping switch

Example

# Open the igmp snooping packet debugging switch

**Switch#debug igmp snooping packet**

# Chapter 11 ACL command

## 11.1 ACL Configuration Command

### 11.1.1 Standard IP ACL rules

Command

**access-list {<group-id>} {permit | deny | remark} {<source-ip>}**

Mode

Configuration Mode

Parameters

**group-id:** rule group, range: <1-99> | <1300-1999>.

**permit:** to allow compliance with the rules of the packet forwarding.

**deny:** to prohibit compliance with the rules of the packet forwarding.

**remark:** add comments to a specified set of rules.

**source-ip:** source IP, there are three input methods:

1) ABCD wildcard IP address can be controlled from a segment;

2) any equivalent A.B.C.D 255.255.255.255

3) host A.B.C.D equivalent to A.B.C.D 0.0.0.0

**wildcard:** reverse mask to decide which bits need to match, '0 'indicates the need to match, '1' do not need to match.

description

IP-ACL configuration standards-based access control rules. This type of rule is to determine whether the source IP address of the packet matches the configured ACL rules

or not; if matched according to deny / permit for the appropriate treatment. Of all the ACL rules have a hidden rule in the deny all IP packets, as long as the user configured an ACL rule, the system will generate this rule automatically. Therefore, users do not need to go to deny any configuration manually. Based on the expansion of IP rules and the rules based on MAC address as well.

Example

# Configure a set of rules that allow the data packet forwarding for the source address of 192.168.0.0 network segment, to prohibit the packet forwarding of the source address of 192.168.0.11, and other address .

**Switch(config)#access-list 1 deny host 192.168.0.11**

**Switch(config)#access-list 1 permit 192.168.0.0 0.0.0.255**

**Switch(config)#access-list 1 deny any**

## 11.1.2 Extended IP ACL rules

Command

**access-list {<group-id>} {permit | deny | remark} {protocol} {<source-ip>} [<source-port>] {<dest-ip>} <dest-port > [<type>]**

Mode

Configuration Mode

Parameters

**group-id:** Rule group number, range <100-199> <2000-2699>.

**permit:** to allow compliance with the rules of the packet forwarding.

**deny:** to prohibit compliance with the rules of the packet forwarding.

**remark:** add comments to a specified set of rules.

**protocol:** the protocol type in the IP layer on top, such as: ip, tcp, udp, enter the appropriate numbers, such as the six representatives of the tcp. If you do not control these agreements, you can enter ip or (0).

**source-ip:** source IP, there are three input methods:

1) ABCD wildcard IP address can be controlled from a segment;

2) any equivalent A.B.C.D 255.255.255.255

3) host A.B.C.D equivalent to A.B.C.D 0.0.0.0

**wildcard:** to decide which bits need to match, '0 'indicates the need to match, '1' do not need to match.

**source-port:** protocol is tcp or udp, you can control the data packet source port, the input mode can be familiar with the port service name, such as: www is a number such as 80 on behalf of the www port.

**dest-ip:** destination IP address. There are three input methods:

1) ABCD wildcard IP address can be controlled from a segment;

2) any equivalent A.B.C.D 255.255.255.255

3) host A.B.C.D equivalent to A.B.C.D 0.0.0.0

**dest-port:** protocol is tcp or udp, you can control the data packet destination port, the same input mode and srcPort.

**type:** You can control the message type, the input mode is the name of the message type can also be a number.

description

Configure an extended IP rules to match the specified protocol packets, according to the packet source and destination IP address, message type, or port the decision to forward or discard.

Example

# Configuration rules to prohibit packets ip from 192.168.0.2 to 192.168.1.0 network segment,

**Switch (config) # access-list 100 deny the ip host 192.168.0.2 192.168.1.0 0.0.0.255**

# Configure a set of rules, to the address of 10.1.0.0 255.255.0.0 network segment can not access any www server, but 10.1.1.1 above restrictions; can be configured as follows:

**Switch (config) # access - list 199 deny the tcp 10.1.0.0 0.0.255.255 any www**

**Switch (config) # access-list 199 permit tcp host 10.1.1.1 any www**

## 11.1.3 MAC IP ACL rules

Command

**access-list <groupId> {deny | permit | remark} <source-mac> <destination -mac> ip <source-ip> <destination-ip>**

Mode

Configuration Mode

Parameters

**group-id:** rule group, ranging from 700 to 799.

**permit:** to allow compliance with the rules of the packet forwarding.

**deny:** to prohibit compliance with the rules of the packet forwarding.

**remark:** add comments to a specified set of rules.

**source-mac:** Source MAC. There are three input methods:

1) HHHH.HHHH.HHHH wildcard can be controlled from a segment of the MAC address;

2) any equivalent HHHH.HHHH.HHHH FFFF.FFFF.FFFF

3) is equivalent to the host ABCD HHHH.HHHH.HHHH 0000.0000.0000

**destination-mac:** the MAC. The source MAC. There are three input methods:

1) HHHH.HHHH.HHHH wildcard can be controlled from a segment of the MAC address;

2) any equivalent HHHH.HHHH.HHHH FFFF.FFFF.FFFF

3) is equivalent to the host ABCD HHHH.HHHH.HHHH 0000.0000.0000

**source-ip:** source IP, there are three input methods:

1) ABCD wildcard IP address can be controlled from a segment;

2) any equivalent A.B.C.D 255.255.255.255

3) host A.B.C.D equivalent to A.B.C.D 0.0.0.0

**wildcard:** to decide which bits need to match, '0 'indicates the need to match, '1' do not

need to match.

**dest-ip:** destination IP address. There are three input methods:

1) ABCD wildcard IP address can be controlled from a segment;

2) any equivalent A.B.C.D 255.255.255.255

3) host A.B.C.D equivalent to A.B.C.D 0.0.0.0

description

Configure a MAC-based ip rules, according to the packet source and destination IP address, source and destination MAC decided to forward or discard.

Example

# Configuration rules from the source MAC address 0009.ca10.0907 and IP 192.168.0.2 to the destination MAC address to 0009.ca10.0908 and IP address is 192.168.2.3 the IP packet is prohibited.

**Switch (config) # access-list 700 deny host 0009.ca10.0907 host 0009.ca10.0908 ip host 192.168.0.2 host 192.168.0.3**

## 11.1.4 MAC ARP ACL rules

Command

**access-list <groupId> {deny | permit | remark} arp <arp-operation> <sender-mac> <sender-ip>**

Mode

Configuration Mode

Parameters

**group-id:** rule group, ranging from 1100 to 1199.

**permit:** to allow compliance with the rules of the packet forwarding.

**deny:** to prohibit compliance with the rules of the packet forwarding.

**remark:** add comments to a specified set of rules.

**arp-operation:** the arp protocol packet type of operation.

**sender-mac:** MAC address of the sender.

**sender-ip:** the sender's IP address.

description

Configure a MAC ARP ACL rules to match the specified protocol packets can be forwarded or discarded according to the packet's source IP address, source MAC decisions.

Example

# configure ACL rules for 1100 allow mac source address 0009.ca10.1122 source IP 192.168.0.10 hair arp request packet.

**Switch (config) # access-list 1100 permit arp request host 0009.ca10.1122 host 192.168.0.10**

## 11.1.5 Access-group

Command

**access-group <group-id>**

Mode

interface configuration mode

Parameters

**group-id:** reference to the rule group, the standard IP rules range <1-99> | <1300-1999> Extended IP scope of the rules <100-199> <2000-2699> Mac arp rules range <1100-1199> Mac ip rule range <700-799>

description

Make use of a ACL rules on ports.

Example

# Port fe1 / 1 reference rule group 1:

**Switch (config-fe1 / 1) # access-group 1**

## 11.1.6 Delete ACL rules

Command

**no access-list <group-id>**

Mode

Configuration mode

Parameters

**group-id:** ACL group number

description

Delete ACL rules.

Example

# Delete ACL list 1：

**Switch(config)#no access-list 1**

# 11.2 ACL ACL view command

## 11.2.1 show access-group

Command

**show access-group**

Mode

privileged mode

Parameters

without

Description

Display configuration of ACL

Example

**Switch#show access-group**

**Interface fe1/1**

**access-list 100 is set**

### 11.2.2 show access-list

Command

**show access-list [<group-id>]**

Mode

privileged mode

Parameters

**group-id:** to show the rule number

Description

Display configuration acl rules

Example

# showing ACL configuration information.

**Switch#show access-list**

**Standard IP access list 1, Remark acl1**

**deny 192.168.1.0, wildcard bits 0.0.0.255**

**permit any**

# Chapter 12 TCP / IP commands

## 12.1 Configure Command

### 12.1.1 arp

Command

**arp <ip-address> <mac-address> [if-name]**

**no arp {<ip-address> | <ip-prefix> | all | dynamic | static}**

Mode

Configuration Mode

parameter

**ip-address:** bound IP address, using 32-bit dotted decimal

**mac-address:** physical address binding, using 12-bit 16 hexadecimal, said; mac address, format HHHH.HHHH.HHHH;

**if-name:** interface name, specify the IP and MAC binding interface, which must be the second layer interface;

**ip-prefix:** ip prefix, use the ip address / mask forms, that a network;

**dynamic:** Dynamic Learning arp table entry;

**static:** static configuration or dynamic learning and converted into a static arp table entry type.

Description:

**arp** command used to configure a static arp table entry, with the [if-name] parameter can be binding IP, MAC address and layer 2 interfaces, , after the success of configuration with the IP and MAC address of the host only from the second layers of the specified port and Switch Communications.

**no arp** command to delete the corresponding arp table entry or a static configuration.

Example

# Configure the ip address of 192.168.1.1 with MAC address 0003.0010.1011 mapped.

**Switch(config)#arp 192.168.1.1 0003.0010.1011**

# Configure the IP address of 192.168.8.3, MAC address 0009.ca10.0011 host only through the interface fe1 / 4 uplink:

**Switch(config)#arp 192.168.8.3 0009.ca10.0011 fe1/4**

## 12.1.2 arp static

Command

**arp static {<ip-prefix> | all}**

**no arp static**

Mode

Configuration Mode

parameters

**ip-prefix:** ip address segment， form: A.B.C.D/M.

**all:** all static arp table.

description

**arp static** command used to within the parameters specified by the dynamic arp static arp table entry into bits;

**no arp static** command be used to delete the static arp table entry.

Example

# All dynamic arp table entry is set to a static table entry:

**Switch(config)#arp static all**

## 12.1.3 ip address

command

**ip address <address/mask>**

**no ip address [<address/mask>]**

mode

interface configuration mode

parameters

**address / mask:** ip address and mask length. Range address: 0.0.0.0 ~ 223.255.255.255; mask: 0 ~ 32.

description

**ip address** command used to configure the IP address of a three-tier interface. The command is currently only in the three-tier interface (vlan) effectively. Assigned to the command with the ip interface vlan command before the first start the three-tier interface.

**no ip address** command be used to remove the interface IP address configured.

Example

# configuration interface vlan4 the ip address of 192.168.192.32, mask length of 24-bit:

**Switch#conf ter**

**Switch(config)#inter vlan24**

**Switch(config-vlan24)#ip addr 192.168.192.32/24**

**Switch(config-vlan24)#end**

**Switch#show ip interface vlan24 brief**

| Interface | IP-Address | Status | Protocol |
|---|---|---|---|
| vlan24 | 192.168.192.32 | up | up |

## 12.1.4 ip route

command

**ip route {<ip-address>/<mask-length> | <ip-address> <mask>} <gateway >**

**no ip route {<ip-address>/<mask-length> | <ip-address> <mask>}**

mode

configuration mode

parameters

**ip-address:** the purpose of IP address, 32-bit dotted-decimal format.

**mask-length:** mask length, decimal.

**mask:** IP address mask, the dotted-decimal format.

**gateway:** the specified route next hop gateway IP address dotted-decimal format.

description

**ip route** command used to configure a static route.

**no ip route** command be used to remove the static route, in the presence of more than one route to reach the same network when you do not specify the gateway to delete all

with the purpose of the network matches the static route.

Example

# Configure a route to the 210.1.1.0/24 network segment, the next hop to 172.20.2.2:

**Switch#configure terminal**

**Switch(config)#ip route 210.1.1.0/24 172.20.2.2**

#Canlcel a static router

**Switch#configure terminal**

**Switch(config)#no ip route 210.1.1.0/24**

## 12.1.5 ip interface vlan

command

**ip interface vlan <vlan-id>**

**no ip interface vlan <vlan-id>**

mode

configuration mode

parameters

**vlan-id:** vlan id number.

description

**ip interface vlan** command to start lay3 interface

**no ip interface vlan** command to cancel lay3 interface.

Example

#To enable vlan 2 the lay3 interface：

**Switch(config)#ip interface vlan 2**

# 12.2 show command

## 12.2.1 show arp

command

**show arp [<ip-address> | dynamic | static]**

mode

normal mode/privileged mode

parameters

**ip-address:** ip address segment.

**dynamic:** dynamic leanrt arp table.

**static:** static arp table.

description

**show arp** command Used to display the Address Resolution Table.

Example

# Show dynamic learning the arp table:

**Switch#show arp**

**ARP TABLE**

| Internet Address | Physical Address | Type |
|---|---|---|
| 172.20.2.104 | 0040.cac9.e135 | dynamic |
| 192.168.1.3 | 0009.ca10.1005 | dynamic |

**Total Number: 2**

## 12.2.2 show ip interface

command

**show ip interface [<ifname>] brief**

mode

normal mode/privileged mode

parameters

**ifname:** Need to specify the interface name interface name, can be a layer interface, can also be a lay3 interface. The default display all two, three-layer interfaces.

description

show ip interface command Is used to display a summary of interface information.

Example

# Show interface vlan24 information：

**Switch#show ip interface vlan24 brief**

| Interface | IP-Address | Status | Protocol |
|---|---|---|---|
| vlan24 | 192.168.192.32 | up | up |

## 12.2.3 show ip route

command

**show ip route [<network>]**

mode

normal mode/privileged mode

parameters

The default parameters: Shows the current routing table to activate the routing

**network:** the specified display relevant network routing, using 32-bit dotted-decimal or address of the prefix / mask is expressed.

description

**show ip route** command used to display routing information. Including destination address, mask length, protocol, priority, weight, the next hop and output interface.

The command only displays the current active route (best route).

Example

#show the current routing

**Switch#show ip route**

**Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP**
**O - OSPF, IA - OSPF inter area**
**N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2**
**E1 - OSPF external type 1, E2 - OSPF external type 2**
**i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area**
*** - candidate default**
**Gateway of last resort is 192.168.1.3 to network 0.0.0.0**
**S*  0.0.0.0/0 [1/0] via 192.168.1.3, vlan5**
**C  172.20.1.0/24 is directly connected, vlan2**
**C  172.20.2.0/24 is directly connected, vlan3**
**C  192.168.1.0/24 is directly connected, vlan5**

## 12.2.4 show ip route database

command

**show ip route database**

mode

normal mode/privileged mode

parameters

**The default parameters:** Display the routing table of all routes, including the activation and non-active route.

description

**show ip rout database** command Is used throughout the routing table in the routing information, including non-active route..

Example

# Show all the routing

**Switch#show ip route database**

**Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP**
**O - OSPF, IA - OSPF inter area**
**N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2**
**E1 - OSPF external type 1, E2 - OSPF external type 2**
**i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area**
**> - selected route, * - FIB route, p - stale info**
**S  *> 0.0.0.0/0 [1/0] via 192.168.0.200, vlan1**
**C  *> 192.168.0.0/24 is directly connected, vlan1**

# Chapter 13 SNMP commands

## 13.1 SNMP configuration commands

### 13.1.1 snmp community

Command:

**snmp community <community-name> {ro | rw}**

**no snmp community <community-name>**

Mode

Configuration Mode

Parameters

**community-name:** SNMP shared body name. Character Length: 1 ~ 20.

**ro:** read-only attribute.

**rw:** read-write attribute.

Description

**snmp community** command is configured SNMP shared body names and associated attributes of the shared body.

**no snmp community** command is to delete the specified SNMP shared body..

Example

# Configure a shared body called the private read-write property.

**Switch(config)#snmp community private rw**

# Remove a body called the shared private

**Switch(config)#no snmp community private**

### 13.1.2 snmp trap

Command

**snmp trap <notify-name> host <ipaddress> version {1 | 2c | 3}**

**no snmp trap <notify-name>**

Mode

Configuration Mode

Parameters

**notify-name:** SNMP trap name. Character Length: 1 ~ 32.

**ipaddress:** The purpose of IP addresses to send trap.

1: SNMP version 1.

2: SNMP version 2.

3: SNMP version 3.

Description

**snmp trap** command is to configure SNMP trap and the trap of the relevant attributes.

no snmp trap command is to delete the specified SNMP trap.

Example

# Configure a test called the SNMP trap and send the purpose of IP-192.168.0.10; using SNMP version 1.

**Switch (config) # snmp trap test host 192.168.0.10 version 1**

# Delete a named test the SNMP trap

**Switch (config) # no snmp trap test**

## 13.1.3 snmp system information contact

Command

**snmp system information <contact | location | name> <information string>**

**no snmp system information <contact | location | name >**

Mode

Configuration Mode

Parameter

**Information string:** appointed content. Character length:1~255.

Description:

**snmp system information** command is a configuration system information.

**no snmp system information** command is to delete the system information.

Example

# Configure the system to contact specific content: E-mail: networks@quickte.com

**Switch(config)#snmp system information contact E-mail: networks@quickte.com**

# Configure the system location specific content is: Shennan Road,Shenzhen,China

**Switch(config)#snmp system information location Shennan Road,Shenzhen,China**

# Configure the system name specific content is: Switch

**Switch(config)#snmp system information name Switch**

# Remove the system name

**Switch(config)#no snmp system information name**

## 13.1.4 snmp engine-id local

Command

**snmp engine-id local < engine-id>**

Mode

Configuration Mode

Parameters

**engine-id:** SNMP version 3 used in engine id

Description

**snmp engine-id local** command is used to configure SNMP version 3 of the engine id. The ID for a 24-bit hexadecimal numbers; and the importation of less than 24,

automatically padded with 0.

Example:

# Configure SNMP engine ID as: 00002ffc0000226c7f000022

**Switch(config)#snmp engine-id local 00002ffc0000226c7f000022**

## 13.1.5 snmp user

Command

**snmp user <user-name> <group-name> v3 [auth {md5 | sha} <auth-key>]**

**no snmp user <user-name> <group-name> v3**

Mode

Configuration Mode

Parameters

**user-name:** Setting snmpv3 engine ID corresponding to a user name. Character Length: 1 ~ 32.

**group-name:** set the user name corresponding to the group name. Character Length: 1 ~ 32.

**auth:** use the user name of the security level is identifiable.

**md5:** use of identification hmac md5 authentication protocol

**sha:** the use of identification hmac sha authentication protocol

**auth-key:** enter the identification password, md5 for the 16-byte long string of 16 hexadecimal numbers, sha for the 20-byte long string of 16 hexadecimal numbers.

Description

**snmp user** command is to set snmpv3 local engine ID corresponding to a user name. And the user name corresponding to the group name, if the user name to support authentication, you need to set authentication protocol (md5 or sha) and the corresponding identification password.

**no snmp user** command is to delete the snmpv3 local engine ID corresponding to a user name

Example

# Set up a support md5 authentication user name initialmd5, group called the initia, identify password 047b473f93211a17813ce5fff290066b:

**Switch(config)# snmp user initialmd5 initial v3 auth md5 047b473f93211a17813ce5fff290066b**

# Set the user name without identifying initialnone, group called the initial:

**Switch(config)# snmp user initialnone initial v3**

#Delete the user name initialmd5, called the initial group of users.

**Switch(config)# no snmp user initialmd5 initial v3**

### 13.1.6 snmp group

Command

**snmp group <group-name> v3 {auth | noauth} [notify <notify-view-name> | write <write-view-name> | read <read-view-name>]**

**no snmp group <group-name> v3 {auth | noauth}**

Mode

Configuration Mode

Parameters

**group-name:** configure the group name. Character Length: 1 ~ 32.

**auth:** This access control is needed identification.

**noauth:** The access control does not require identification.

**notify:** Specifies can generate notification mib view.

**notify-view:** Specifies can generate notification mib view view's name.

**write:** specify the write mib view.

**write-view:** specify the write mib view view name.

**read:** Specifies readable mib view.

**read-view:** the specified readable mib view view 'sname.

Description

**snmp group** command is set snmp group name and information.

**no snmp group** command to delete snmp group name and information.

Example

# Set group called the initial, security level is the (auth), security mode (v3) specified in the notice may be written or read the name of the view were internet, internet, internet.

**Switch(config)# snmp group initial v3 auth read internet write internet notify internet**

# Delete group called the initial group.

**Switch(config)# no snmp group initial v3 auth**

## 13.2 SNMP view the command

### 13.2.1 show snmp community

Command

**show snmp community**

Mode

Normal mode / privileged mode

Parameters

Without

Description

**show snmp community** command is to show all of the current name of the public body.

Example

# Show all the common body name:

**Switch# show snmp community**

## 13.2.2 show snmp trap

Command

**show snmp trap**

Mode

Normal mode / privileged mode

Parameters

Without

Description

**show snmp trap** command is used to display all of the current trap names.

Example

# Show all of the trap name:

**Switch#show snmp trap**

## 13.2.3 show snmp system information

Command

**show snmp system information**

Mode

Normal mode / privileged mode

Parameters

Without

Description

**show snmp system information** is displayed SNMP commands to set system information.

Example

#Display the current system information:

**Switch#show snmp system information**

## 13.2.4 show snmp engine-id

Command

**show snmp engine-id**

Mode

Normal mode / privileged mode

Parameters

Without

Description

**show snmp engine-id** command is to show SNMP used engine-id.

Example

# Display SNMP uses engine-id:

**Switch#show snmp engine-id**

## 13.2.5 show snmp user

Command

**show snmp user [specify-name-of-user]**

Mode

Normal mode / privileged mode

parameters Parameters

Without

Description

**show snmp user** command is to show SNMP uses user and its properties.

Example

# Display SNMP-use user initialnone its attributes:

**Switch#show snmp user initialnone**

## 13.2.6 show snmp group

Command

**show snmp group**

Mode

Normal mode / privileged mode

Parameters

Without

Description

**show snmp group** command is to show all of the group to use SNMP information

Example

# Display SNMP information on the use of all of the group

**Switch#show snmp group**

# Chapter 14 System Log Command

## 14.1 Common Log Command

### 14.1.1 debug ip

Command

**debug ip [all | arp | icmp | recv | send | tcp | udp]**

**no debug ip [all | arp | icmp | tcp | udp]**

Mode

Privileged mode.

Parameters

**all:** debug all ip, arp, icmp, udp, tcp and other protocol packets. Resolve the important field of IP header, including the protocol type, packet length, and four lays messages, such as port number.

**arp:** debug arp protocol packets, can be resolved is the ARP request or response, can be resolved ARP content, sender IP and MAC address information and so on the receiving end.

**icmp:** debug icmp protocol for sending and receiving of data packets. This command is mainly by parsing the source of header and destination address.

**recv:** received ip packets.

**send:** send ip packet.

**tcp:** Debugging transport layer protocol TCP, send and receive packets situation, you can see the send and receive packet window size, should be

By-layer packet size of the port and the source and destination address.

**udp:** debugging udp transport layer protocol for sending and receiving packets situation, you can see the port and the application layer packet size, and send and receive packets source and destination address.

Description

**debug ip to ip** command is used to open the first package, the related packets debugging switch, allowing users to be able to see specific types of ip packet sending and receiving of messages.

**no debug ip** ordered the closure of the corresponding debug ip packet switching.

Example:

# Open the icmp message debug switch

**Switch#debug ip icmp**

### 14.1.2 log display

Command

**log display [critical | debugging | informational | warning]**

**no log display [critical | debugging | informational | warning]**

Mode

Privileged mode

Parameters

**critical:** output critical-level information.

**debugging:** output debugging -level debugging information.

**informational:** output information-level debugging information.

**warning:** output warning- level debugging information

Example:

# Output of all opened debug switch debugging information:

**Switch#log display**

## 14.1.3 no debug all

Command

**no debug all**

Mode

Privileged Mode

parameters

without

Description

no debug all command is used to close all opened debug switch

Example:

# Close all opened debugg switch

**Switch#no debug all**

## 14.1.4 show debugging

Command

**show debugging [igmp | ip]**

Mode

Privileged mode / normal mode

Parameters:

**igmp:** igmp related debugging switches.

**ip:** ip related debugging switches.

Description

show debug command is used to check those current opening debug switch.

Example

#Show debugging switch information

**Switch#show debugging**

**IP debugging status:**

**IP receive packets debugging is on.**

**IP send packets debugging is on.**

**IGMP SNOOPING debugging status:**

## 14.1.5 show log

Command

**show log [critical | debugging | informational | warning]**

Mode

Privileged mode / normal mode.

Parameters

**critical:** output of critical-level log information.

**debugging:** output debugging- level log information.

**informational:** output information-level log information.

**warning:** output warning- level log information

Description

**show log** command to display the log information which in the log list.

Example:

# Display information-level log information

**Switch#show log informational**

**2089/08/10 11:01:24 Informational: ICMP: SEND: Destination IP: 172.20.10.54 Source IP: 172.20.10.2 ICMP Type: 11 ICMP Code: 0**

**2089/08/10 11:01:21 Informational: ICMP: SEND: Destination IP: 172.20.10.54 Source IP: 172.20.10.2 ICMP Type: 11 ICMP Code: 0**

**2089/08/10 11:01:18 Informational: ICMP: SEND: Destination IP: 172.20.10.54 Source IP: 172.20.10.2 ICMP Type: 11 ICMP Code: 0**

**2089/08/10 11:00:13 Informational: ICMP: SEND: Destination IP: 172.20.3.3 Source IP: 172.20.14.2 ICMP Type: 3 ICMP Code: 3**

**2089/08/10 11:00:13 Informational: ICMP: SEND: Destination IP: 172.20.3.3 Source IP: 172.20.14.2 ICMP Type: 3 ICMP Code: 3**

**2089/08/10 10:59:38 Informational: ICMP: SEND: Destination IP: 172.20.10.54 Source IP: 172.20.10.2 ICMP Type: 11 ICMP Code: 0**

**2089/08/10 10:53:21 Informational: ICMP: SEND: Destination IP: 172.20.3.3 Source IP: 172.20.10.2 ICMP Type: 3 ICMP Code: 3**

### 14.1.6 show log display

Command

**show log display [critical | debugging | informational | warning]**

Mode

Privileged mode / normal mode

Parameters

**critical:** Serious-level output log information

**debugging:** Output debugging information

**informational:** General Tips-level output log information

**warning:** General warning-level output log information.

Description

**show log display** command is to display the four priority real-time monitoring of end-switch configuration (Open or closed)

Example

# Showing the monitoring configuration information

**Switch#show log display**

**Log display configuration:**

**Critical log: OFF**

**Warning log: OFF**

**Informational log: OFF**

**Debugging log: OFF**

# Chapter 15 EAPS Command

## 15.1 STP configuration command

### 15.1.1 Creating an EAPS Domain

Command

**eaps create <ring-id>**

Mode

Privileged Mode

Parameter

Without

Description

Create an EAPS Domain

Example

Without

## 15.1.2 Configure an EAPS Domain Control VLAN

Command

**eaps control-vlan <ring-id> <vlan-id>**

Mode

Privileged Mode

Parameter

Without

Description

Configure an EAPS Domain Control VLAN

Example

Without

## 15.1.3 to add a protected VLAN to EAPS Domain

Command

**eaps protected-vlan <ring-id> <vlan-id>**

Mode

Privileged Mode

Parameter

Without

Description

Add a protected VLAN to EAPS Domain

Example

Without

## 15.1.4 Configure an EAPS Domain node mode of operation

Command

**eaps mode <ring-id> <master|transit>**

Mode

Privileged Mode

Parameter

Without

Description

Configure an EAPS Domain node mode of operation

Example

Without

## 15.1.5 Configure an EAPS Domain's Primary Port

Command

**eaps primary-port <ring-id> <ifname>**

Mode

Privileged Mode

Parameter

Without

Description

Configure an EAPS Domain's Primary Port

Example

Without

## 15.1.6 Configure an EAPS Domain of Secondary Port

Command

**eaps secondary-port <ring-id> <ifname>**

Mode

Privileged Mode

Parameter

Without

Description

Configure an EAPS Domain of the Secondary Port.

Example

Without

## 15.1.7 Configure fail-period timer timeout time

Command

**eaps fail-time <ring-id> <secs>**

Mode

Privileged Mode

Parameter

Without

Description

Configure an EAPS Domain of the fail-period timer timeout time. The default is 3 seconds. Units of seconds.

Example

Without

## 15.1.8 configured to send an EAPS Domain regular HEALTH packet time

Command

**eaps fail-time <ring-id> <secs>**

Mode

Privileged Mode

Parameter

Without

Description

Configure an EAPS Domain from time to time to send HEALTH packet time. The default is 1 second. Units of seconds. Hello-timer must be less than fail-time.

Example

Without

## 15.1.9 On or Off and Extreme equipment is compatible

Command

**eaps extreme-interoperability <ring-id> <enable|disable>**

Mode

Privileged Mode

Parameter

Without

Description

Start or shut down and Extreme equipment is compatible, the default is to start compatible

Example

Without

## 15.1.10 start an EAPS Domain

Command

**eaps enable <ring-id>**

Mode

Privileged Mode

Parameter

Without

Description

Start an EAPS Domain

Example

Without

### 15.1.11 Close an EAPS Domain

Command

**eaps disable <ring-id>**

Mode

Privileged Mode

Parameter

Without

Description

Close an EAPS Domain

Example

Without

## 15.2 EAPS show command

### 15.2.1 shows the EAPS Domain information

Command

**show eaps**

Mode

Privileged Mode

Parameter

Without

Description

Display system was launched in the EAPSDomain information

Example

Without

### 15.2.2 shows a EAPSDomain details

Command

**Show eaps <ring-id>**

Mode

Privileged Mode

Parameter

Without

Description

Shows a EAPSDomain details

Example

Without

# Chapter 16 PoE Command

## 16.1 PoE configuration command

### 16.1.1 PoE enable

Command

**poe enable <if-name> [if-name]**

Mode

Configuration Mode / Interface Configuration Mode

Parameters

**if-name:** port name. Fast port to fe as a prefix, Gigabit port to ge the prefix aggregation port to trunk as a prefix. Port number is a suffix. Example: the first port is expressed as fe1 / 1; aggregation port 1 is expressed as trunk1.

**if-range:** port range configuration. Range of parameters such as port configuration which mean enter multi-physical ports at the same time. Enter into the multiple physical ports At the same time, each port must be have the same prefix, separated by blank. Cases of interface fe1 / 1 fe1/10 or interface ge1/25 ge1/26.

Note: does not support aggregation port or vlan interface range configuration.

Description

Enable PoE function

Example

#Enable port 1 PoE function

**Switch#poe enable fe1/1**

## 16.1.2 PoE disable

Command

**poe disable <if-name> [if-name]**

Mode

Configuration Mode / Interface Configuration Mode

Parameters

**if-name:** port name. Fast port to fe as a prefix, Gigabit port to ge the prefix aggregation port to trunk as a prefix. Port number is a suffix. Example: the first port is expressed as fe1 / 1; aggregation port 1 is expressed as trunk1.

**if-range:** port range configuration. Range of parameters such as port configuration which mean enter multi-physical ports at the same time. Enter into the multiple physical ports At the same time, each port must be have the same prefix, separated by blank. Cases of interface fe1 / 1 fe1/10 or interface ge1/25 ge1/26.

Note: does not support aggregation port or vlan interface range configuration.

Description

Disable PoE function

Example

#Disable port 1 PoE function

**Switch# poe disable fe1/1**

## 16.1.3 Show PoE details

Command

**show poe**

Mode

Privileged Mode

Parameter

Without

Description

Show PoE details

Example

# show the PoE details

**Switch#sh poe**

| Port | Status | Operation |
|---|---|---|
| ge1 | Enable | Off |
| ge2 | Enable | Off |
| ge3 | Enable | Off |

| | | |
|---|---|---|
| ge4 | Enable | Off |
| ge5 | Enable | Off |
| ge6 | Enable | Off |
| ge7 | Enable | Off |
| ge8 | Enable | Off |
| ge9 | Enable | Off |
| ge10 | Enable | Off |
| ge11 | Enable | Off |
| ge12 | Enable | Off |
| ge13 | Enable | Off |
| ge14 | Enable | Off |
| ge15 | Enable | Off |
| ge16 | Enable | Off |
| ge17 | Enable | Off |
| ge18 | Enable | Off |
| ge19 | Enable | Off |
| ge20 | Enable | Off |
| ge21 | Enable | Off |
| ge22 | Enable | Off |
| ge23 | Enable | Off |
| ge24 | Enable | Off |