User’s Manual

GPON OLT Command Line

English

Contant

Chapter 1 Switch Logging in Command

1.1 Switch Logging in Command

Switch logging in command includes:

- **cls**
- **configure terminal**
- **enable**
- **end**
- **exit**
- **help**
- **hostname**
- **interface**
- **muser**
- **quit**
- **show muser**
- **show username**
- **stop**
- **terminal language**
- **timeout**
- **username**
- **username change-password**

1.1.1 cls

Use **cls** command to clear current screen displaying

cls

【Command configuration mode】

Any configuration mode

【Example】

！Clear current screen displaying

Optiway>cls

1.1.2 configure terminal

Use **configure terminal** command to enter global configuration mode from privileged mode.

configure terminal

【Command configuration mode】

Privileged mode

【Example】

Optiway#configure terminal

Optiway(config)#

【Related command】

exit,end

1.1.3 enable

Use **enable** command to enter privileged mode from user mode.

enable

【Command configuration mode】

User mode

【Example】

！ Enter from user mode to privileged mode

Optiway>enable

Optiway#

【Related command】

exit,end

1.1.4 end

Use **end** command to be back from global configuration mode or other superior mode to privileged mode.

end

【Command configuration mode】

Any configuration mode except user mode and privileged mode

【Usage】

5 levels of command line configuration mode, from inferior to superior are:

- User mode
- Privileged mode
- Global configuration mode
- Interface configuration mode, VLAN configuration mode, and AAA configuration mode
- Domain configuration mode and radius configuration mode

End command can back from global configuration mode or other superior mode to privileged mode.

【Example】

！Back from global configuration mode to privileged mode

Optiway(config-if-ethernet-2/1)#end

Optiway#

【Related command】

exit

1.1.5 **exit**

Use **exit** command to be back to inferior mode. For the user mode, exit.

exit

【Command configuration mode】

Any configuration mode

【Usage】

Use exit command can be back to inferior mode

【Example】

！Back to global configuration mode from interface configuration mode

Optiway(config-if-ethernet-2/1)#exit

Optiway(config)#

【Related command】

end

1.1.6 **help**

Use **help** command to display command help information.

help

【Command configuration mode】

Any configuration mode

【Usage】

Use help command can display any command in current mode, and user can key in “?” at any moment.

【Example】

Optiway(config)#help

1.1.7 **hostname**

Use **hostname** command to configure host name. Use **no hostname** command to restore default host name.

hostname hostname

no hostname

【Parameter】

hostname:character strings range from 1 to 32, these strings can be printable, excluding such wildcards as '/',':','*','?','\\','<','>','|',""etc.

【Default】

Default hostname is OptiWay

【Command configuration mode】

Global configuration mode

【Usage】

Modify system hostname. If the hostname is OptiWay,the hostname in global configuration mode is OptiWay(config)#.

【Example】

！Configure hostname to be OptiWayEL8600-04

Optiway(config)#hostname OptiwayEL8600-04

OptiwayEL8600-04(config)#

1.1.8 **interface**

Use **interface** command to enter interface configuration mode.

interface ethernet *interface-num*

【Parameter】

interface-num:The number of the interface

【Command configuration mode】

Global configuration mode

【Usage】

Interface-number is in the form of slot-num/port-num, in which slot-num is in the range of 0 to 2, and port-num is in the range of 1 to 24.

【Example】

！Enter from clobal configuration mode to interface configuration mode

Optiway(config)#interface ethernet 2/1

1.1.9 **interface range**

Use this command to enter Ethernet interface group configuration mode.

interface range *interface-list*

【Parameter】

interface-list:interface list

【Command configuration mode】

Global configuration mode

【Usage】

After entering Ethernet interface group mode, inputting command once can configure all interface members of this group and failure in halfway will not affect the configuration o following interfaces. All command which can be used in Ethernet interface mode can be used in this mode. This is a dynamic mode.the current group will not be existed after exit. All configuration command in this mode can generate anticompile for single interface.

【Example】

!Enter Ethernet interface group configuration mode which includes Ethernet 1 - 3

Optiway(config)#interface range ethernet 2/1 to e 2/3

1.1.10 muser

Use muser command to enable user's RADIUS/TACACS+ remote authentication.

muser { **local** | { **radius** *radiusname* { **pap** | **chap** } [**local**] } }| { tacacs+ [author] [account] [local] } }

【Parameter】

radiusname:RADIUS server configuration name

【Command configuration mode】

Global configuration mode

【Usage】

Configure authentication of RADIUS/TACACS+ remote authentication only or using RADIUS/TACACS+ remote authentication first, if RADIUS/TACACS+ fails, local database authentication is used.

RADIUS authentication supports PAP or CHAP ways.

Enable RADIUS/TACACS+ remote authentication needs correct RADIUS/TACACS+ server configuration.

If it is TACACS+ remote authentication, when the authorization is not used, the privilege after authentication is administrator; when the authorization is used, the privilege after authentication is determined by the replied priv_lvl from remote server, if there is no reply, it is administrator; if the authorization fails, it is normal user.

The accounting of TACACS+ is from the beginning to the end.

【Example】

！ Enable RADIUS authentication with the way of PAP

Optiway(config)#muser radius radiusserver1 pap

！ Enable TACACS+ authentication

Optiway(config)#muser tacacs+ author

1.1.11 **quit**

Use **quit** command to disconnect with switch and exit.

quit

【Command configuration mode】

Any configuration mode

【Usage】

If the current connect is in telnet, use quit command to disconnect with the switch and exit. If the current connect is in serial port, after using quit command, you will re-log in.

【Example】

！Disconnect with the switch and exit

Optiway#quit

1.1.12 show muser

Use **show muser** command to display user's authentication.

show muser

【Command configuration mode】

Any configuration mode

【Example】

！Display user's authentication

Optiway(config)#show muser

1.1.13 show tacacs+

Use this command to show TACACS+ server configuration.

show tacacs+

【Command configuration mode】

Any configuration mode

【Example】

！ show TACACS+ server configuration

Optiway(config)#show tacacs+

1.1.14 show username

Use **show username** command to display all the users or the user's privilege or the existed user and his privilege.

show username [*username*]

【Parameter】

username:existed username ranges from 1 to 32 printable characters such wildcards as '/',':','*','?','\\','<','>','|',"".

【Command configuration mode】

Any configuration mode

【Example】

！ Display the privilege of user "green"

Optiway(config)#show username green

1.1.15 stop

Use **stop** command to stop the session between user and telnet forcibly, that is, after using this command, telnet user with the username of "username" will force to disconnect with telnet.

stop username

【Parameter】

username:Telnet user who has logged in

【Command configuration mode】

Privileged mode

【Usage】

Only administrator can use this command

【Example】

！Force user “green” to disconnect with telnet

Optiway#stop green

1.1.16 tacacs+

use this command to configure TACACS+ server.

tacacs+ { priamary | secondary } server *ipaddress* [key *keyvalue*] [port *portnum*] [timeout *timevalue*]

no tacacs+ { priamary | secondary } server

【Parameter】

ipaddress:ip address of primary and secondary server which cannot be the same.

keyvalue:the key between switch and server, which is in the length of 1～16 characters.

portnum:TACACS+ is tcp and this value is defaulted to be 49, which is in the range of 1～65535

timevalue:the timeout of tcp connection, which is defaulted to be 5 seconds and in the range of 1～120 seconds.

【Command configuration mode】

Global configuration mode

【Usage】

Only administrators can use this command.

【Example】

！ Configure primary server

Optiway#tacacs+ priamary server key 123

1.1.17 terminal language

Use this command to shift language mode of command line interface.

terminal language { chinese | english }

【Parameter】

It is defaulted to be English

【Command configuration mode】

Privileged mode

【Usage】

System command line interface supports both English and Chinese.

【Example】

！ Shift English into Chinese

Optiway#terminal language chinese

1.1.18 timeout

Use **timeout** command to configure the overtime of user's logging in. Use no timeout command to configure overtime to be non-over timing.

timeout [*minute*]

no timeout

【Parameter】

minute:Range from 1 to 480 minutes

【Default】

Default time is 20 minutes

【Command configuration mode】

User mode, privileged mode

【Usage】

If timeout command without parameter, it configures to be default time. No timeout command means non-overtime. Use **no timeout** command in telnet, if the user doesn't exit and the net is smooth, telnet user is non-overtime; if the net is disconnected, the link to telnet will be disconnected in 2 hours.

This command is effective for command line users.

【Example】

！Configure the overtime to be 30 minutes

Optiway#timeout 30

！Configure user to be non-overtime

Optiway#no timeout

1.1.19 username username privilege

Use **username username privilege** command to add a user or modify the privilege or password of the existed user. Use **no username username privilege** command to remove specified user.

username *username* [**privilege** *level*] { **password** *encryption-type password* }

no username *username*

【Parameter】

username:User name of new users and existed users ranges from 1 to 32 printable characters excluding such wildcards as '/',':','*','?','\\','<','>','|','"" etc.

privilege:Privilege of new user or the modified privilege of existed user ranges from 0 to 15. 0 to 1 means user while 2 to 15 means administrator. Caution: the privilege of administrator cannot be modified.

encryption-type: the value of it is 0 or 7. 0 means non-encryption and 7 means encryption(It is not supported now).

password:Log in password for new user and modified password of the existed user ranges from 1 to 16 characters or numbers.

【Command configuration mode】

Global configuration mode

【Usage】

When inputting the privilege of the new user, 0 to 1 means ordinary user and 2 to 15 means administrator. If the privilege doesn't configure, the default privilege is ordinary user.

If inputting nothing to modify the privilege of existed user, the privilege doesn't modify. The privilege of Admin cannot be modified.

【Example】

！ Add a new administrator “green”, configure privilege to be 15,and password to be 123456

Optiway(config)#username green privilege 15 password 0 123456

！ Modify the privilege of administrator “green” to be 1,and password to be 1234

Optiway(config)#username green privilege 1 password 0 1234

1.1.20 username change-password

Administrator “admin” can use username change-password to modify the password of him and others, and other users can use this command to modify his own password. After inputting this command, user will be asked to input as following: original password, the username of the password needs modifying, new password and confirm new password.

username change-password

【Parameter】

Username must be existed.

【Command configuration mode】

Global configuration mode

【Usage】

Only administrator “admin”can modify other user’s password, while others only can modifies his own. If a user forgets his password, administrator “admin” can use this command to give him a new one.

【Example】

！ Modify the password of user “green” to be 123456

Optiway(config)#username change-password

please input you login password : ******

please input username :green

Please input user new password :******

Please input user comfirm password :******

chang user green password success.

Chapter 2 Port Configuration Command

2.1 Ethernet Interface Configuration Command

Ethernet interface configuration command includes:

- **clear interface**
- **combo**
- **description**
- **duplex**
- **flow-control**
- **ingress acceptable-frame**
- **ingress filtering**
- **link-aggregation**
- **priority**
- **show description**
- **show interface**
- **show statistics interface**
- **shutdown**
- **speed**
- **switchport access**
- **switchport mode**
- **switchport trunk allowed vlan**
- **switchport trunk**
- **tag**

- **show statistics dynamic interface**
- **show utilization interface**

2.1.1 clear interface

Use **clear interface** command to clear the information of the interface.

clear interface [*interface-num* | slot-num]

【Parameter】

interface-num:Means Ethernet port. Interface-num is in the form of interface-type + interface-number. Interface-type is Ethernet and interface-number is slot-num/port-num, in which slot-num is in the range of 0 to 2, and port-num is in the range of 1 to 24.

slot-num:Means slot number which is in the form of ethernet + slot-num, and ranges from 0 to 2

【Command configuration mode】

Global configuration mode, interface configuration mode

【Usage】

The information of the interface includes: numbers of unicast, multicast and broadcast message etc.

Using **clear interface** command in global mode, if the interface-num and slot-num are not assigned, the information of all interfaces is cleared. If the slot-num is assigned, the port information of the assigned slot is cleared. In interface mode, only the information of the current port can be cleared.

【Example】

！Clear information of all interfaces

Optiway(config)#clear interface

！ Clear information of interface 5 in global and interface mode

Optiway(config)#clear interface ethernet 2/5

Optiway(config-if-ethernet-2/5)#clear interface

2.1.2 combo

Use this command to configure combo attribute of Ethernet interface.

combo { fiber | copper }

【Parameter】

fiber:FX attribution

copper:TX arrtibution

【Default】

fiber

【Command configuration mode】

Interface configuration mode

【Usage】

Only Ethernet interface 1～4 are combo interfaces. If combo interface is configured to be TX mode, FX cannot be used. If combo interface is configured as FX, TX cannot be used.

【Example】

！ Configure combo attribution of current Ethernet interface 1 to be TX

Optiway(config-if-ethernet-2/1)#combo copper

2.1.3 description

Use **description** command to configure a port description string. Use **no description** command to remove the port description string.

description description-list

no description

【Parameter】

description-list:Port description string ranges from 1 to 32 characters

【Command configuration mode】

Interface configuration mode

【Example】

！Configure description string “green” for the Ethernet 2/3

Optiway(config-if-ethernet-2/3)#description green

！Clear description of Ethernet 2/3

Optiway(config-if-ethernet-2/3)#no description

【Related command】

show description

2.1.4 duplex

Use **duplex** command to configure the duplex mode of the current port. Use **no duplex** command to restore the default duplex mode, that is, auto-negotiation.

duplex { half | full | auto }

no duplex

【Parameter】

half:Half duplex mode

full:Full duplex mode

auto:Auto-negotiation mode

【Default】

auto

【Command configuration mode】

Interface configuration mode

【Usage】

When configuring duplex mode, full duplex means receiving and sending messages at the same time; half duplex means receiving or sending message at one time, and auto means the duplex mode negotiating by each port.

100 BASE-FX only supports full duplex.

【Example】

！Configure ethernet 0/5 port to full duplex

Optiway(config-if-ethernet-2/5)#duplex full

2.1.5 **flow-control**

Use **flow-control** command to enable flow control on the Ethernet port. Use **no flow-control** command to disable flow control on the port.

flow-control

no flow-control

【Default】

Disable

【Command configuration mode】

Interface configuration mode

【Usage】

If the port is crowded, it needs controlling to avoid congestion and data loss. Use flow-control command to control the flow.

【Example】

！ Enable flow control on Ethernet 2/5

Optiway(config-if-ethernet-2/5)#flow-control

！ Disable flow control on Ethernet 2/5

Optiway(config-if-ethernet-2/5)#no flow-control

2.1.6 ingress acceptable-frame

Use **ingress acceptable-frame** command to configure ingress acceptable frame mode. Use **no ingress acceptable-frame** command to restore the default ingress acceptable frame.

ingress acceptable-frame { all | tagged }

no ingress acceptable-frame

【Default】

All types of frame is acceptable

【Command configuration mode】

Interface configuration mode

【Usage】

When ingress acceptable-frame enables, frame of other type are dropped. When ingress acceptable-frame disables, all types of frames are received.

【Example】

！Configure Ethernet 2/5 only to receive tagged frame

Optiway(config-if-ethernet-2/5)#ingress acceptable-frame tagged

！Restore default ingress acceptable-frame Ethernet 2/5

Optiway(config-if-ethernet-2/5)#no ingress accetable-frame

2.1.7 ingress filtering

Use **ingress filtering** command to enable interface ingress filtering. Use **no ingress filtering** command to disable interface ingress filtering.

ingress filtering

no ingress filtering

【Default】

Ingress filtering enables.

【Command configuration mode】

Interface configuration mode

【Usage】

When interface ingress filtering enables, the frame with the VLAN ID being different from the VLAN ID of the interface which the frame is received will be dropped; when interface ingress filtering disables, the frame will not be dropped.

【Example】

！ Enable the ingress filtering of ethernet 2/5

Optiway(config-if-ethernet-2/5)#ingress filtering

！ Disable the ingress filtering of ethernet 2/5

Optiway(config-if-ethernet-2/5)#no ingress filtering

2.1.8 **priority**

Use **priority** command to assign priority of the port. Use **no priority** command to restore default priority.

priority priority-value

no priority

【Parameter】

priority-value:Ranges from 2 to 7

【Default】

Default priority-value is 2

【Command configuration mode】

Interface configuration mode

【Usage】

The larger priority-value is, the higher the priority is.

【Example】

！ Configure priority-value of Ethernet 2/3 to be 1

Optiway(config-if-ethernet-2/3)#priority 1

2.1.9 **show description**

Use **show description** command to display interface description.

show description interface [*interface-list*]

【Parameter】

interface-list:List of interfaces means many Ethernet ports

【Command configuration mode】

Any configuration mode

【Usage】

When displaying interface description, if interface-list is not specified, description of all interfaces is displayed. If interface is specified, the description of the specified interface is displayed.

【Example】

！Display description of Ethernet 2/3

Optiway(config)#show description interface ethernet 2/3

【Related command】

description

2.1.10 show interface

Use **show interface** command to display port configuration.

show interface [*interface-num*]

【Parameter】

interface-num:Means Ethernet port. Interface-num is in the form of interface-type + interface-number. Interface-type is Ethernet and interface-number is slot-num/port-num, in which slot-num is in the range of 2

to 2, and port-num is in the range of 1 to 24.

【Command configuration mode】

Any configuration mode

【Usage】

If port type and port number are not specified, the command displays information about all ports. If both port type and port number are specified, the command displays information about the specified port.

【Example】

！Display the configuration information of Ethernet 2/1

Optiway#show interface ethernet 2/1

2.1.11 show statistics interface

Use **show statistics interface** command to display the statistic information of specified port or all ports.

show statistics interface [*interface-num*]

【Parameter】

interface-num:Means Ethernet port. Interface-num is in the form of interface-type + interface-number. Interface-type is Ethernet and interface-number is slot-num/port-num, in which slot-num is in the range of 2 to 2, and port-num is in the range of 1 to 24.

【Command configuration mode】

Any mode

【Usage】

If port type and port number are not specified, the command displays statistic

information about all ports. If both port type and port number are specified, the command displays statistic information about the specified port.

【Example】

！ Display statustic information of Ethernet 2/1

Optiway#show statistics interface ethernet 2/1

2.1.12 show statistics higig

Use **show statistics** higig **[unit** unit **higig-port** higig-port] command in any mode to show port info.

Use **show statistics dynamic higig** to show dynamic statictics.

show statistics higig [unit unit higig-port higig-port]

show statistics dynamic higig

【Parameter】

dynamic:dynamic statistics

unit:chip unit

higig-port:port number

【Command configuration mode】

Any mode

【Usage】

If no unit and higig port is specified, show all.

【Example】

！ Show higig-statistics unit 2 higig-port1

Optiway(diag)%% show statistics higig unit 2 higig-port 1

2.1.13 clear higig-statistics

Use **clear statistics** [all | **unit** unit **higig-port** higig-port] command to clear info.

clear higig-statistics [all | unit unit higig-port higig-port]

【Parameter】

all: all ports

unit:chip unit

higig-port:port number

【Command configuration mode】

Global configuration mode

【Usage】

Use this command in global configuration mode, if no higig port is specified, clear all.

【Example】

！Clear higig-statistics unit 2 higig-port1

Optiway(diag)%% clear higig-statistics unit 2 higig-port 1

2.1.14 shutdown

Use **shutdown** command to disable an Ethernet port. Use **no shutdown** command to enable an Ethernet port.

shutdown

no shutdown

【Default】

Ethernet port enables

【Command configuration mode】

Interface configuration mode

【Usage】

Use **no shutdown** command to enable an Ethernet port after related parameter and protocol are configured. Disable a port and then enable it when there is a failure, which can recover the port.

【Example】

！Disable Ethernet 2/1, then enable it.

Optiway(config-if-ethernet-2/1)#shutdown

Optiway(config-if-ethernet-2/1)#no shutdown

2.1.15 port-control mode

Use this command to configure port-control mode. Use **no** command to restore to slave mode.

port-control mode *master* | *slave*

no port-control mode

【Default】

slave

【Command configuration mode】

Interface configuration mode

【Usage】

When two extended GE electric ports connect to each other and speed is in force, and the two sides are master and slave, the connection is successful.

【Example】

！Set e2/2 to be master and restore to be slave

Optiway(config-if-ethernet-2/2)# port-control mode master

Optiway(config-if-ethernet-2/2)# no port-control mode

2.1.16 **show port-control mode**

Use this command to show port-control mode.

show port-control mode

【Command configuration mode】

Any configuration mode

【Usage】

Only extended GE electric port needs this configuration.

【Example】

！Show port-control mode

Optiway# show port-control mode

2.1.17 **speed**

Use **speed** command to configure the port speed. Use **no speed** command to restore the port speed to the defaulting setting.

speed { 12 | 12auto | 122 | 122auto | auto }

no speed

【Parameter】

12:Means the port speed is 12Mbps

122:Means the port speed is 122Mbps

12auto: means the maximum port speed is 12Mbps,and duplex mode is auto-negotiation

122auto: means the maximum port speed is 122Mbps,and duplex mode is auto-negotiation

auto: means both port speed and duplex mode are auto-negotiation

【Default】

auto

【Command configuration mode】

Interface configuration mode

【Usage】

122 BASE TX supports the speed of 12Mbps and 122Mbps and the duplex mode of half, full duplex and auto-negotiation mode. 122 BASE FX supports the speed of 122Mbps and the duplex mode of full duplex.

【Example】

！Configure the speed of Ethernet 2/1 to 122Mbps

Optiway(config-if-ethernet-2/1)#speed 122

2.1.18 **switchport mode**

Use **switchport mode** command to configure port type. Use **no switchport mode** command to restore default port type, that is, access port.

switchport mode { access | trunk }

no switchport mode

【Parameter】

access:Configure port to be non-trunk port.

trunk:Configure port to be trunk port.

【Default】

Default port mode is access port.

【Command configuration mode】

Interface configuration mode

【Usage】

Use switchport mode command to configure a port to be trunk port or access port. If a port configures to be a trunk port, the vlan mode changes untagged into tagged, and if a port configures to be an access one, the vlan mode changes tagged into untagged. In addition, configure a port to be a trunk one, then create a vlan, this port will automatically be added to the vlan.

【Example】

！ Configure Ethernet 2/1 to be trunk port

Optiway(config-if-ethernet-2/1)#switchport mode trunk

2.1.19 switchport trunk allowed vlan

Use **switchport trunk allowed vlan** command to add trunk port to specified VLAN. Use **no switchport trunk allowed vlan** command to remove trunk port from specified vlan.

switchport trunk allowed vlan { *vlan-list* | all }

no switchport trunk allowed vlan { *vlan-list* | all }

【Parameter】

vlan-list: vlan-list*vlan-list* can be discrete numbers, sequential numbers or both. Discrete numbers are separated by ",", and sequential numbers use "-", such as: 2, 5,8,12-22. Vlan-list in the following context expresses the same.

all:Add trunk ports to all VLAN.

【Command configuration mode】

Interface configuration mode

【Usage】

Use this command to add trunk port to specified VLAN. Trunk port can belong to more VLANs. If use **switchport trunk allowed vlan** command in many times, VLAN allowed by the trunk port is the congregation of these vlan-list.

【Example】

! Add trunk port Ethernet2/1 to VLAN 3,4,72～152

Optiway(config-if-ethernet-2/1)#switchport trunk allowed vlan 3,4,72-152

2.1.20 switchport trunk default vlan

Use this command to configure port default vlan-id (pvid),with no command is to revert the default vlan-id.

switchport default vlan *vlan-id*

no switchport default vlan

【Parameter】

vlan-id range is 1～4094

【Default】

vlan-id default value is 1

【Command mode】

Interface configuration mode

【Example】

！Configure port 1 the default VLAN id is 100

OptiWay(config-if-ethernet-2/1)#switchport default vlan 100

2.1.21 show statistics dynamic interface

Use **show statistic dynamic interface** command to display the statistic information of all interfaces.

show statistics dynamic interface

【Command configuration mode】

Any configuration mode

【Usage】

Statistic information refreshes automatically every 3 seconds.

【Example】

！Display statistic information of the port

Optiway#show statistics dynamic interface

2.1.22 show utilization interface

Use **show utilization interface** command to display the utilization information of all ports, including receiving and sending speed, bandwidth utilization rate, etc.

show utilization interface

【Command configuration mode】

Any configuration mode

【Usage】

Receiving and sending rate and bandwidth utilization rate refresh every 3 seconds.

【Example】

！Display utilization interface of the port

Optiway#show utilization interface

2.1.23 **local-switch**

Use this command to enable local switching feature of Ethernet interface. Use the **no** command to disable it.

local-switch

no local-switch

【Default】

Disable

【Command configuration mode】

Interface configuration mode

【Usage】

Enabling local switching feature of Ethernet interface can transmit the packet from the port where it is in.

It is useful when a interface downlinking a WAP.

【Example】

！ Enable local switching feature of e2/5

Optiway(config-if-ethernet-2/5)#local-switch

！ Disable local switching feature of e2/5

Optiway(config-if-ethernet-2/5)#no local-switch

2.2 Interface Mirror Configuration Command

Interface Mirror configuration command includes:

- **mirror destination-interface**
- **mirror source-interface**
- **show mirror**

2.2.1 **mirror destination-interface**

Use **mirror destination-interface** command configure mirror destination interface. Use **no mirror destination-interface** command to remove mirror interface.

mirror destination-interface *interface-num*

no mirror destination-interface *interface-num*

【Parameter】

interface-num:Means Ethernet port. Interface-num is in the form of interface-type + interface-number. Interface-type is Ethernet and interface-number is slot-num/port-num, in which slot-num is in the range of 2 to 2, and port-num is in the range of 1 to 24.

【Command configuration mode】

Global configuration mode

【Example】

！ Configure Ethernet 2/1 to be mirror destination-interface

Optiway(config)#mirror destination-interface ethernet 2/1

2.2.2 mirror source-interface

Use **mirror source-interface** command to configure mirror source-interface. Use **no mirror source-interface** command to remove mirror source-interface.

mirror source-interface { *interface-list* | cpu } { both | egress | ingress }

no mirror source-interface { *interface-list* | cpu }

【Parameter】

interface-list:List of interfaces provides in the form of interface-num [to interface-num], this can be repeated for 3 times.

cpu:Means CPU port

both:Means both egress and ingress can be mirrored

egress:Means egress mirror

ingress:Means ingress mirror

【Command configuration mode】

Global configuration mode

【Example】

！ Configure Ethernet 2/1 to ethernet 2/12 to be mirror source-interface

Optiway(config)#mirror source-interface ethernet 2/1 to ethernet 2/12 both

2.2.3 show mirror

Use **show mirror** command to display system configuration of current mirror

interface, including monitor port and mirrored port list.

show mirror

【Command configuration mode】

Any configuration mode

【Example】

！Display monitor port and mirrored port list

Optiway(config)#show mirror

2.3 Port CAR Configuration Command

Port CAR configuration command includes:

- **port-car**
- **port-car-open-time**
- **port-car-rate**
- **show port-car**

2.3.1 **port-car**

Use **port-car** command to enable port CAR of global system or port. Use **no port-car** command to disable port CAR of global system or port.

port-car

no port-car

【Default】

Port-car globally enables

【Command configuration mode】

Global configuration mode, interface configuration mode

【Example】

！Enable port-car globally

Optiway(config)#port-car

！Enable port-car of Ethernet 2/8

Optiway(config-if-ethernet-2/8)#port-car

2.3.2 port-car-open-time

Use **port-car-open-time** command to configure the reopen time of the port shutdown by port-car. Use **no port-car-open-time** command to restore the default port-car-open-time.

port-car-open-time *port-car-open-time*

no port-car-open-time

【Parameter】

port-car-open-time:The reopen time of the port shutdown by port-car. It ranges from 1 to 3622

【Default】

Default port-car-open-time is 482 seconds

【Command configuration mode】

Global configuration mode

【Example】

！Configure port-car-open-time to be 12 seconds

Optiway(config)#port-car-open-time 12

2.3.3 port-car-rate

Use **port-car-rate** command to configure the port-car-rate. Use **no port-car-rate** command to restore the default port-car-rate.

port-car-rate *port-car-rate*

no port-car-rate

【Parameter】

port-car-rate:Port-car-rate ranges from 1 to 2622

【Default】

Default port-car-rate is 322 packet/second

【Command configuration mode】

Global configuration mode

【Example】

！Configure port-car-rate to be 122 packet/second

Optiway(config)#port-car-rate 122

2.3.4 show port-car

Use **show port-car** command to display port-car information.

show port-car

【Command configuration mode】

Any configuration mode

【Example】

！Display port-car information

Optiway(config)#show port-car

2.4 Port LACP Configuration Command

Port LACP configuration command includes:

- **channel-group**
- **channel-group mode**
- **channel-group load-balance**
- **higig-trunk load-balance**
- **lacp system-priority**
- **lacp port-priority**
- **show higig-trunk load-balance**
- **show utilization higig**
- **show lacp sys-id**
- **show lacp internal**
- **show lacp neighbor**
- **show statistics channel-group**
- **clear channel-group**
- **show statistics dynamic channel-group**
- **show utilization channel-group**

2.4.1 channel-group

Use **channel-group** command to create channel group, but there is no member in the group. To remove the group, all the members of the group must be removed first. Use **no channel-group** command to remove the group.

channel-group channel-group-number

no channel-group channel-group-number

【Parameter】

channel-group-number:Range from 2 to 5

【Default】

Non

【Command configuration mode】

Global configuration mode

【Example】

！Create channel group 1

Optiway(config)#channel-group 1

2.4.2 channel-group mode

Use **channel-group mode** command to add port members to the group, and specify the mode.

channel-group *channel-group-number* mode {active | passive | on}

no channel-group channel-group-number

【Parameter】

channel-group-number:Range from 2 to 5

【Default】

Non

【Command configuration mode】

Interface /Interface group configuration mode

【Example】

！ Add Ethernet 2/3 to channel-group 3 and specify the port to be active mode

Optiway(config-if-ethernet-2/3)#channel-group 3 mode active

！ Add Ethernet 2/6 to ethernet 2/8 to channel-group 2 and specify the ports to be on mode

Optiway(config)#interface range ethernet 2/6 to ethernet 2/8

Optiway(config-if-range)#channel-group 2 mode on

2.4.3 **channel-group load-balance**

Use **channel-group load-balance** command to configure channel-group load-balance, that is, choose physical link program when message sending.

channel-group *channel-group-number* load-balance

{dst-ip|dst-mac|src-dst-ip|src-dst-mac|src-ip|src-mac}

【Parameter】

channel-group-number:Range from 2 to 5

【Default】

Source MAC mode

【Command configuration mode】

Global configuration mode

【Example】

！ Specify load-balance of channel-group 2 is destination mac

Optiway(config)#channel-group load-balance dst-mac

2.4.4 **higig-trunk load-balance**

Use this command to configure load-balance of static channel-group between two chips. Use no command to restore to default configuration.

higig-trunk load-balance

{dst-ip|dst-mac|src-dst-ip|src-dst-mac|src-ip|src-mac}

【Default】

Source MAC

【Command configuration mode】

Global configuration mode

【Example】

！Specify load-balance of static channel-group between two chips to be destination MAC

Optiway(config)#higig-trunk load-balance dst-mac

2.4.5 lacp system-priority

Use **lacp system-priority** command to configure lacp system priority. Use **no lacp system-priority** command to restore default priority.

The redundancy influence made by LACP system and port priority shows: LACP providing redundancy system needs guarantee the consistency of the choosing redundancy for conterminous switches, and user can configure redundancy link, which is realized by system and port priority. Choose redundancy in following steps:

1,Make sure which switch is the standard of choice. For exchanging the message, two switches know each other's LACP system priority and system mac. They compare local LACP system priority, the smaller one is the standard; if they have the same priority, compare the system MAC, the smaller is the standard.

2,Choose redundancy link with the port parameter of the standard switch. Compare the port LACP priority first, the inferior is the redundant; if they have the same priority, the larger number of the port is redundant.

lacp system-priority *priority*

no lacp system-priority *priority*

【Parameter】

*priority:*Range from 1 to 65535

【Default】

default priority is 32768

【Command configuration mode】

Global configuration mode

【Example】

！Configure LACP system priority is 42222

Optiway(config)#lacp system-priority 42222

2.4.6 **lacp port-priority**

Use **lacp port-priority** command to configure lacp port-priority. When the port backup exists, the inferior one backups. Use no lacp port-priority command to restore default lacp port-priority.

lacp port-priority *priority*

【Parameter】

*priority:*Range from 1 to 65535

【Default】

Default priority is 128

【Command configuration mode】

Interface /Interface group configuration mode

【Example】

！Configure lacp port-priority of Ethernet 2/2 to be 12345

Optiway(config-if-ethernet-2/2)#lacp port-priority 12345

2.4.7 show higig-trunk load-balance

Use this command to show higig-trunk load balance

show higig-trunk load-balance

【Parameter】

None

【Default】

None

【Command mode】

All modes

【Example】

！Show higig-trunk load balance

OptiWay(config)#show higig-trunk load-balance

2.4.8 show utilization higig

Use this command to show all HiGig port utilization, including HiGig port receive and send rate, port bandwidth occupancy rate etc.

show utilization higig

【Command mode】

All command mode

【Usage】

When displaying HiGig port,informaton of HiGig port receive and send rate, port bandwidth occupancy rate refreshes every 3s.

【Example】

！ Show real-time all HiGig port utilization

OptiWay#show utilization higig

2.4.9 **show lacp sys-id**

Use **show lacp sys-id** command to display lacp system id, which is in the form of 16 characters of system priority and 32 characters of system MAC address.

show lacp sys-id

【Parameter】

Non

【Default】

Non

【Command configuration mode】

Any configuration mode

【Example】

！ Display lacp system id

Optiway(config)#show lacp sys-id

2.4.10 show lacp internal

Use **show lacp interval** command to display the information of group members, if the there is no keywords, all groups are displayed.

show lacp internal [*channel-group-number*]

【Parameter】

channel-group-number:Range from 2 to 5

【Default】

Non

【Command configuration mode】

Any configuration mode

【Example】

！ Such as:

Optiway#show lacp internal

2.4.11 show statistics channel-group

Use this command to display statistic channel-group, it shows current all channel group if no parameter enters.

show statistics channel-group [*channel-group-number*]

【Parameter】

channel-group-number:channel index is 0～5

【Default】

None

【Command mode】

All modes

【Example】

！For example:

OptiWay#show statistics channel-group

2.4.12 clear channel-group

Use this command to delete statistic channel-group, it deletes current all channel group if no parameter enters.

clear channel-group [*channel-group-number*]

【Parameter】

channel-group-number:channel index is 0～5

【Default】

None

【Command mode】

All modes

【Example】

！For example:

OptiWay#clear channel-group

2.4.13 show statistics dynamic channel-group

Use this command to display dynamic channel-group.

show statistics dynamic channel-group

【Default】

None

【Command mode】

All modes

【Example】

！For example:

OptiWay#show statistics dynamic channel-group

2.4.14 show utilization channel-group

Use this command to display all channel utilization, including receive and send rate, port bandwidth occupancy rate etc.

show utilization channel-group

【Parameter】

None

【Default】

None

【Command mode】

All modes

【Example】

！For example:

OptiWay#show utilization channel-group

2.4.15 show lacp neighbor

Use **show lacp neighbor** command to display the information of the neighbour port in the group. If there is no keyword, the neighbor ports of all the groups are displayed.

show lacp neighbor [*channel-group-number*]

【Parameter】

channel-group-number:Range from 2 to 5

【Default】

Non

【Command configuration mode】

Any configuration mode

【Example】

！Such as:

Optiway#show lacp neighbor

2.5 Port Alarm Configuration Command

Port alarm configuration command includes:

- **alarm all-packets**
- **alarm all-packets threshold**
- **show alarm all-packets**

2.5.1 alarm all-packets

Use **alarm all-packets** command to enable global or port all-packets alarm.

Use **no alarm all-packets** command to disable global or port all-ports alarm.

alarm all-packets

no alarm all-packets

【Default】

Alarm all-packets enable

【Command configuration mode】

Global/interface configuration mode

【Example】

！ Enable global alarm all-packets

Optiway(config)#alarm all-packets

！Enable alarm all-packets of Ethernet 2/8

Optiway(config-if-ethernet-2/8)#alarm all-packets

2.5.2 alarm all-packets threshold

Use **alarm all-packets threshold** command to configure alarm all-packets exceed and normal threshold.

alarm all-packets threshold [exceed *exceed*] [normal *normal*]

no alarm all-packets

【Parameter】

exceed:Exceed threshold. 122BASE ranges from 2 to 12222

normal: normal threshold. 122BASE ranges from 2 to 12222

【Default】Default GE exceed threshold is 852,normal threshold is 622.

Default 12GE exceed threshold is 8522,normal threshold is 6222.

【Command configuration mode】

Interface configuration mode

【Usage】

Exceed > normal

【Example】

！Configure alarm all-packets exceed threshold to be 52,and normal threshold to be 32

Optiway(config)#alarm all-packets threshold exceed 522 normal 322

2.5.3 show alarm all-packets

Use **show alarm all-packets** command to display the information of global alarm all-packets.

show alarm all-packets

【Command configuration mode】

Any configuration mode

【Example】

！ Display global alarm all-packets information

Optiway(config)#show alarm all-packets

Port alarm global status : enable

Port alarm exceed port

2.5.4 show alarm all-packets interface

Use **show alarm all-packets interface** command to display port alarm all-packets information.

show alarm all-packets interface [*interface-list*]

【Parameter】

interface-num:List of Ethernet ports to be added to or removed from a VLAN. This keyword needed to be provided in the form of interface-type + interface-number. Interface-type is Ethernet and interface-number is slot-num/port-num, in which slot-num is in the range of 2 to 2, and port-num is in the range of 1 to 24. Seriate interfaces with the same type can be linked by to keyword, but the port number to the right of the to keyword must be larger than the one to the left of the keyword, and this argument only can be repeated for up to 3 times.

【Command configuration mode】

Any configuration mode

【Usage】

Keyword “interface-list” is alternative. If there is no keyword, the alarm all-packets of all the interfaces are displayed, or the information of specified port is displayed.

【Example】

！Display the alarm all-packets interface information of Ethernet 2/1

Optiway(config)#show alarm all-packets interface ethernet 2/1

2.6 Interface shutdown-control Configuration Command

Interface shutdown-control Configuration Command includes:

- **shutdown-control**

- **shutdown-control-open-time**
- **show shutdown-control**

2.6.1 shutdown-control

Use **shutdown-control** command to configure interface shutdown-control.

shutdown-control [broadcast | multicast | unicast] *target-rate*

no shutdown-control [broadcast | multicast | unicast]

【Parameter】

broadcast:configure broadcast shutdown-control

multicast:configure multicast shutdown-control

unicast:configure unicast shutdown-control

target-rate:disable target rate

【Command configuration mode】

Global configuration mode

【Example】

！Enable shutdown-control of e2/8 for broadcast and speed rate is 122pps

Optiway(config-if-ethernet-2/8)#shutdown-control broadcast 122

2.6.2 shutdown-control-open-time

Use **shutdown-control-open-time** command to configure shutdown-control reopen time. Use **no** command to restore to default shutdown-control-open-time.

Shutdown-control-open-time *open-time*

no shutdown-control-open-time

【Parameter】

open-time:shutdown-control reopen time which is in the range of 1～3622

【Default】

The default shutdown-control open-time is 482 seconds.

【Command configuration mode】

Global configuration mode

【Example】

！Configure shutdown-control-open-time of CAR is 12 seconds.

Optiway(config)#shutdown-control-open-time 12

2.6.3 no shutdown-control-recover

Use this command to recover port shutdown-control as default configuration.

no shutdown-control-recover mode | automatic-open-time

【Command mode】

Global configuration mode

【Example】

！Recover port shutdown-control mode as default manual mode

OptiWay(config)# no shutdown-control-recover mode

2.6.4 show shutdown-control

Use **show shutdown-control** command to display interface shutdown-control information.

show shutdown-control

【Command configuration mode】

Any configuration mode

【Example】

！ Display interface shutdown-control information

Optiway(config)#show shutdown-control

Chapter 3 VLAN Configuration Command

3.1 VLAN Configuration

VLAN(Virtual Local Area Network) configuration includes:

- **description**
- **show vlan**
- **switchport**
- **vlan**

3.1.1 description

Use **description** command to assign a description string to the current VLAN.
Use **no description** command to delete the description of the current VLAN.

description *string*

no description

【Parameter】

string:It is in the range of 1 to 32 characters to describe the current VLAN. The characters can be printable, excluding such wildcards as '/',':','*','?','\\','<','>','|',""etc.

【Command configuration mode】

VLAN configuration mode

【Usage】

This command can assign a description to the current VLAN.

【Example】

！ Specify the description string of the current VLAN as “market”

Optiway (config-if-vlan)#description market

3.1.2 show vlan

Use **show vlan** command to display the information about the specified VLAN

show vlan [*vlan-id*]

【Parameter】

vlan-id:Specified the VLAN ID is in the range of 1 to 4294.

【Command configuration mode】

Any configuration mode

【Usage】

This command is used to display the information about the specified VLAN, including VLAN ID, VLAN description, and member ports.

If the VLAN with specified keyword exists, this command displays the information of the specified VLAN. If no keyword is specified, this command displays the list of all the existing VLANs.

【Example】

！ Display the information of all the existing VLANs

Optiway(config)#show vlan

3.1.3 switchport

Use **switchport** command to add a port or multiple ports to a VLAN. Use **no switchport** command to remove a port or multiple ports from a VLAN.

switchport { *interface-list* | all }

no switchport { *interface-list* | all }

【Parameter】

interface-list:List of Ethernet ports to be added to or removed from a VLAN. This keyword needed to be provided in the form of interface-type + interface-number. Interface-type is Ethernet and interface-number is slot-num/port-num, in which slot-num is in the range of 2 to 2, and port-num is in the range of 1 to 24. Seriate interfaces with the same type can be linked by to keyword, but the port number to the right of the to keyword must be larger than the one to the left of the keyword, and this argument only can be repeated for up to 3 times.

all:Means all the interfaces. When the keyword all is specified, all the interfaces in the system are added to a VLAN by using the **switchport** command, and all the interfaces are removed from a VLAN by using the no **switchport** command.

【View】

VLAN configuration view

【Usage】

In no switchport command, all the interfaces would be removed from a VLAN when the interface-list is unspecified. When removing the interface from VLAN 1 (default VLAN), if the PVID of the interface is 1, the PVID must be changed into other VLAN ID, or the removing fails. When removing interface from other VLANs, if the PVID of the interface is the same as the VLAN ID, and the interface is also in VLAN 1, the removing succeeds, and the PVID of the interface default to 1, or the removing fails

【Example】

！ Add Ethernet 1, 3, 4, 5, 8 to current VLAN

Optiway(config-if-vlan)#switchport ethernet 2/1 ethernet 2/3 to ethernet 2/5 ethernet 2/8

！ Remove Ethernet 3, 4, 5, 8 from current VLAN

Optiway(config-if-vlan)#no switchport ethernet 2/3 to ethernet 2/5 ethernet 2/8

3.1.4 **vlan**

Use **vlan** command to enter VLAN mode. If the VLAN identified by the vlan-id argument does not exist, this command creates the VLAN and then enters VLAN mode. Use the **no vlan** commands to remove a VLAN.

vlan vlan-list

no vlan { *vlan-list* | all }

【Parameter】

vlan-list:The VLAN which you want to create and whose view you want to enter. Each id ranges from 1 to 4294.

all:Specifying all when removing VLAN, all created VLANs are removed except the default VLAN.

【Command configuration mode】

Global configuration mode

【Usage】

Use the vlan command to enter VLAN configuration view. If the vlan identified by the vlan-id keyword exists, enter VLAN configuration view. If not, this command creates the VLAN and then enters VLAN configuration view. Use the no vlan command to remove a VLAN. Caution: Default VLAN (VLAN 1) cannot be removed. If there is some port with the same default vlan-id as

VLAN 1, the port's VLAN will become VLAN 1 after using the no vlan command. If the VLAN to be removed exists in the multicast group, remove the related multicast group first.

【Example】

！Enter VLAN 1 configuration view

Optiway(config)#vlan 1

3.2 GVRP Configuration Command

GVRP command includes:

- **gvrp**
- **show gvrp**
- **show gvrp interface**

3.2.1 **gvrp**

Use the **gvrp** command to enable GVRP globally in global configuration mode or a port in Ethernet port configuration mode. Use **no gvrp** command to disable GVRP globally in global configuration mode or a port in Ethernet port configuration mode.

gvrp

no gvrp

【Default】

Disable GVRP globally

【Command configuration mode】

Globally configuration mode, Ethernet port configuration mode

【Usage】

You can enable GVRP only on trunk ports.

【Example】

！ Enable GVRP globally

Optiway(config)#gvrp

！ Enable GVRP on Ethernet port 8

Optiway(config-if-ethernet-2/8)#gvrp

3.2.2 **show gvrp**

Use **show gvrp** command to display the information about GVRP globally.

show gvrp

【Command configuration mode】

Any configuration mode

【Example】

！ Display the information about GVRP globally

Optiway(config)#show gvrp

GVRP state : enable

3.2.3 **show gvrp interface**

Use **show gvrp interface** command to display GVRP information on Ethernet port.

show gvrp interface [*interface-list*]

【Parameter】

interface-list:List of Ethernet ports to be added to or removed from a VLAN.

This keyword needed to be provided in the form of interface-type + interface-number. Interface-type is Ethernet and interface-number is slot-num/port-num, in which slot-num is in the range of 2 to 2, and port-num is in the range of 1 to 24. Seriate interfaces with the same type can be linked by to keyword, but the port number to the right of the to keyword must be larger than the one to the left of the keyword, and this argument only can be repeated for up to 3 times.

【Command configuration mode】

Any configuration mode

【Usage】

Interface-list keyword is optional. If this keyword unspecified, the command displays GVRP information for all the Ethernet ports. If specified, the command displays GVRP information on specified Ethernet port.

【Example】

！Display GVRP information on Ethernet port 3, 25, 26

Optiway(config)#show gvrp interface ethernet 2/3 ethernet 2/5 ethernet 2/6

3.2.4 garp permit vlan

Use **garp permit vlan** command to add configured static vlan to GVRP module for other switches to learn.

garp permit vlan *vlan-list*

no garp permit vlan [*vlan-list*]

【Parameter】

vlan-list:List of VLANs to be entered or to be created and entered. The single VLAN is in the range of 1 to 4294. The list is in the form of number, -, such as:

2, 5, 8, 12-22.

【Command configuration mode】

Global configuration mode

【Example】

!Add vlan 2, 3, 7 to GVRP

Optiway(config)#garp permit vlan 2-3,7

3.2.5 show garp permit vlan

Use **show garp permit vlan** command to display current static vlan permitted learning by GVRP

show garp permit vlan

【Command configuration mode】

Global configuration mode

【Example】

Display current static vlan permitted learning by GVRP

Optiway(config)#show garp permit vlan

3.3 QinQ command

QinQ command includes:

- **dtag**
- **dtag inner-tpid**
- **dtag outer-tpid**
- **dtag mode**
- **show dtag**

- **dtag insert**
- **show dtag insert**
- **dtag swap**
- **show dtag swap**
- **dtag pass-through**

3.3.1 dtag

Use this command to configure global QinQ.

dtag

no dtag

【Command configuration mode】

Global configuration mode

【Example】

！Enable QinQ

Optiway(config)dtag

3.3.2 dtag inner-tpid

Configure TPID of internal tag in global configuration mode:

dtag inner-tpid *tpid*

no dtag inner-tpid

【Parameter】

tpid:TPID value of internal tag which is defaulted to be 2x8122.

【Command configuration mode】

Global configuration mode

【Example】

！Configure internal TPID to be 2x9122

Optiway(config)#dtag inner-tpid 9122

3.3.3 dtag outer-tpid

Configure TPID of external tag in interface configuration mode:

dtag outer-tpid *tpid*

no dtag outer-tpid

【Parameter】

tpid:TPID value of external tag which is defaulted to be 2x8122.

【Command configuration mode】

Interface configuration mode

【Example】

！Configure external TPID of e2/1 to be 2x7122

Optiway(config-if-ethernet-2/1)#dtag outer-tpid 7122

3.3.4 dtag mode

Use **dtag mode** command to configure interface QinQ mode.

dtag mode { customer | service-provider }

no dtag mode

【Parameter】

customer: In this mode, the original tag head will be ignored and a new one

will be added.

service-provider: In this mode, when the vlan protocol number of ingress packet is different from the configured parameter of the interface, a new tag head will be added.

【Command configuration mode】

Interface configuration mode

【Example】

Configure interface to be customer interface.

Optiway(config-if-ethernet-2/1)#dtag mode customer

3.3.5 **show dag**

Display the QinQ configurationof the switch.

show dtag

【Command configuration mode】

Any configuration mode

【Example】

!Display the QinQ configuration

Optiway(config)#show dtag

3.3.6 **dtag insert**

Add vlan tag head in QinQ in interface configuration mode.

dtag insert startvlanid endvlanid targetvlanid

no dtag insert startvlanid endvlanid

【Parameter】

startvlanid:the start vlan id which needs new tag head.

endvlanid:the end vlan id which needs new tag head.

targetvlanid:tag vlan added new tag head and it is transferred according to the new tag vlan.

【Command configuration mode】

Interface configuration mode

【Example】

Configure all vlans from vlan1 to vlan2 in e2/1 to add new tag head with the tag vlan to be vlan3

Optiway(config-if-ethernet-2/1)#dtag insert 1 2 3

3.3.7 **show dag insert**

Display vlan insert configuration.

show dtag insert

【Command configuration mode】

Any configuration mode

【Example】

Display current vlan insert configuration

Optiway(config)#show dtag insert

3.3.8 **dtag swap**

Configure switching vlan in interface mode.

dtag swap startvlanid endvlanid targetvlanid

no dtag swap startvlanid endvlanid

【Parameter】

startvlanid:start vlan needed to be replaced

endvlanid:end vlan needed to be replaced

targetvlanid:the vlan used to replace original vlan ID.

【Command configuration mode】

Interface configuration mode

【Example】

Configure tag packet from vlan1 to vlan 3 in e2/1 is replaced by vlan5

Optiway(config-if-ethernet-2/1)#dtag swap 1 3 5

3.3.9 **show dag swap**

Display current vlan swap configuration.

show dtag swap

【Command configuration mode】

Any configuration mode

【Example】

Display current vlan swap configuration

Optiway(config)#show dtag swap

3.3.10 **dtag pass-through**

Configure vlan transparent transmission in interface mode:

dtag pass-through startvlanid endvlanid

no dtag pass-through startvlanid endvlanid

【Parameter】

startvlanid:the start vlan needed to be transparent transmision

endvlanid:the end vlan needed to be transparent transmision

【Command configuration mode】

Interface configuration mode

【Example】

Configure tag packet transparent transmission from vlan 1 to vlan 3 in e2/1

Optiway(config-if-ethernet-2/1)#dtag pass-through 1 3

3.3.11 **show dag pass-through**

Display vlan pass-through configuration.

show dtag pass-through

【Command configuration mode】

Any configuration mode

【Example】

Display vlan pass-through configuration

Optiway(config)#show dtag pass-through

3.4 l2-tunnel Configuration

In VPN network, it needs encapsulating some protocol packets received in service-provider network edge according to a certain form. The internal device of SP network can recognize this encapsulation and guarantee the packet pass through SP network without any change. The encapsulation will

be released on the other side of SP network for the normal session of the peer entity connected on the edge of SP network.

L2-tunnel command include:

- **l2-tunnel**
- **show l2-tunnel interface**
- **l2-tunnel drop-threshold**
- **show l2-tunnel drop-threshold**

3.4.1 l2-tunnel

Use this command to configure l2-tunnel status.

l2-tunnel [cdp | pagp | lacp | stp | udld | vtp]

no l2-tunnel [cdp | pagp | lacp | stp | udld | vtp]

【Parameter】

cdp:tunnel cisco cdp packet

pagp:tunnel cisco pagp packet

lacp: tunnel lacp packet

stp: tunnel stp packet

udld:tunnel cisco udld packet

vtp:tunnel cisco vtp packet

【Command configuration mode】

Interface configuration mode

【Example】

Configure l2-tunnel stp on e2/1.

Optiway(config-if-ethernet-2/1)#l2-tunnel stp

3.4.2 show l2-tunnel interface

Use this command to display l2-tunnel configuration.

show l2-tunnel interface *interface-list*

【Parameter】

interface-list :refer to 'interface range'

【Command configuration mode】

Any configuration mode

【Example】

Display l2-tunnel configuration

Optiway(config-if-ethernet-2/1)#show l2-tunnel interface

3.4.3 l2-tunnel drop-threshold

Use this command to configure l2-tunnel drop-threshold.

l2-tunnel drop-threshold[cdp | pagp | lacp | stp | udld | vtp] target-rate

no l2-tunnel drop-threshold[cdp | pagp | lacp | stp | udld | vtp]

【Parameter】

cdp:tunnel cisco cdp packet

pagp:tunnel cisco pagp packet

lacp: tunnel lacp packet

stp: tunnel stp packet

udld:tunnel cisco udld packet

vtp:tunnel cisco vtp packet

target-rate:target rate of packet

【Command configuration mode】

Global configuration mode

【Example】

Configure the speed rate of cpu receiving stp packet to be 12pps

Optiway(config)#l2-tunnel drop-threshold stp 12

3.4.4 show l2-tunnel drop-threshold

Use this command to display l2-tunnel drop-threshold.

show l2-tunnel drop-threshold

【Command configuration mode】

Any configuration mode

【Example】

Display l2-tunnel drop-threshold configuration

Optiway(config)#show l2-tunnel drop-threshold

Chapter 4 IP Interface Configuration Command

4.1 IP Interface Configuration Command

IP Interface Configuration Command includes:

- **arp-proxy**
- **interface vlan-interface**
- **interface supervlan-interface**
- **ip address**
- **ip address primary**
- **ip address range**
- **ip def cpu**
- **show ip interface supervlan-interface**
- **show ip interface vlan-interface**
- **subvlan**

4.1.1 arp-proxy

Use **arp-proxy** command to enable ARP proxy to make arp of all subvlan can intercommunicate. Use **no arp-proxy** command to disable ARP proxy.

arp-proxy

no arp-proxy

【Default】

ARP proxy disables.

【Command configuration mode】

Global configuration mode

【Example】

！ Enable ARP proxy

Optiway(config)#arp-proxy

！ Disable ARP proxy

Optiway(config)#no arp-proxy

4.1.2 interface vlan-interface

Use **interface vlan-interface** command to create VLAN interface or enter VLAN interface configuration mode. Use **no interface vlan-interface** command to delete a VLAN interface.

interface vlan-interface *vlan-id*

no interface vlan-interface *vlan-id*

【Parameter】

vlan-id:VLAN interface ID which is in the range of 1～4294

【Command configuration mode】

Global configuration mode

【Usage】

This command is used to create VLAN interface. Create corresponded VLAN interface only when VLAN has existed.

【Example】

！ Enter configuration mode of VLAN interface 2

Optiway(config)# interface vlan-interface 2

4.1.3 interface supervlan-interface

Use **interface supervlan-interface** command to create super VLAN interface or enter super VLAN interface mode. Use **no interface supervlan-interface** command to delete a super VLAN interface.

interface supervlan-interface *supervlan-id*

no interface supervlan-interface *supervlan-id*

【Parameter】

supervlan-id:super VLAN interface ID which is in the range of 1～128

【Command configuration mode】

Global configuration mode

【Usage】

Use this command to create super VLAN interface.

【Example】

！Enter configuration mode of supervlan-interface 2

Optiway(config)#interface supervlan-interface 2

4.1.4 ip address

Use **ip address** command to specify IP address and netmask for VLAN or superVLAN interface. Use **no ip address** command to delete IP address and netmask for VLAN or superVLAN interface.

ip address ip-address mask

no ip address

【Parameter】

ip-address:IP address of VLAN interface

mask:netmask of VLAN interface

【Command configuration mode】

Interface configuration mode

【Usage】

Specify IP address and netmask for VLAN or superVLAN interface after corresponded VLAN or superVLAN interface created.

【Example】

！Specify IP address for VLAN interface 22

Optiway(config-if-vlanInterface-22)#ip address 192.168.2.122 255.255.2.2

！Delete IP address for VLAN interface 22

Optiway(config-if-vlanInterface-22)#no ip address

4.1.5 ip address primary

Use **ip address primary** command to specify primary IP address for VLAN or superVLAN interface.

ip address primary *ip-address*

【Parameter】

ip-address:configured IP address of interface

【Command configuration mode】

Interface configuration mode

【Example】

！ Specify primary IP address for VLAN interface 22

Optiway(config-if-vlanInterface-22)#ip address primary 192.168.2.122

4.1.6 ip address range

Use **ip address range** command to specify accessing range for VLAN or superVLAN interface.

ip address range *startip endip*

【Parameter】

startip:start IP address

endip:end IP address

【Command configuration mode】

Interface configuration mode

【Example】

！ Specify accessing range for VLAN interface

Optiway(config-if-vlanInterface-22)#ip address range 192.168.2.122 192.168.2.222

4.1.7 ip def cpu

Use **ip def cpu** command to allow hardware to search failed routing or failed destination host routing sending to CPU to shift to flow transmission mode and network topology transmission mode.

ip def cpu

no ip def cpu

【Command configuration mode】

Global configuration mode

【Example】

！Enter to network topology transmission mode

Optiway(config)#ip def cpu

4.1.8 ip def cpu vlan

In topological transmitting mode, it can specify to send the routing packet from a specific vlaninterface to an unreachable host to cpu.

ip def cpu vlan *vlan-id*

no ip def cpu vlan *vlan-id*

【Parameter】

vlan-id:VLAN interface ID which is in the range of 1～4294

【Command configuration mode】

Global configuration mode

【Example】

！send the routing packet from vlan 2 to an unreachable host to cpu

Optiway(config)#ip def cpu vlan 2

4.1.9 show ip interface supervlan-interface

Use **show ip interface supervlan-interface** command to display specified superVLAN interface information.

show ip interface supervlan-interface *supervlan-id*

【Parameter】

supervlan-id:super VLAN interface ID which is in the range of 1～128

【Command configuration mode】

Any configuration mode

【Usage】

show ip interface can display all VLAN or superVLAN interface.

【Example】

！Display information of superVLAN 1

Optiway(config)#show ip interface supervlan-interface 1

4.1.10 show ip interface vlan-interface

Use **show ip interface vlan-interface** command to display information of specified or all VLAN interface.

show ip interface vlan-interface *vlan-id*

【Parameter】

vlan-id:specified VLAN interface id to be displayed.

【Command configuration mode】

Any configuration mode

【Usage】

show ip interface can display all VLAN or superVLAN interface.

【Example】

！Display information of VLAN interface 2.

Optiway(config)#show ip interface vlan-interface 2

4.1.11 show ip def cpu

Use this command to display packet transmitting mode.

show ip def cpu

【Command configuration mode】

Any configuration mode

【Usage】

show ip def cpu can display packet transmitting mode

【Example】

！Display packet transmitting mode

Optiway(config)#show ip def cpu

4.1.12 subvlan

Use **subvlan/ no subvlan** command to add or delete subvlan of superVLAN.

subvlan *vlan-id*

no subvlan [*vlan-id*]

【Parameter】

vlan-id:subvlan id of superVLAN to be added or deleted which is intherange of 1～4294,**no** command will delete all subVLAN if there si no keyword.

【Command configuration mode】

super VLAN interface configuration mode

【Usage】

The subVLAN of superVLAN to be added cannot correspond to corresponded VLAN interface or other added superVLAN interface.

【Example】

！ Add VLAN 8 to superVLAN interface 1

Optiway(config-if-superVLANInterface-1)#subvlan 8

4.1.13 urpf

Use this command to enable URPF of VLAN interface and configure the mode. Use the **no** command to disable it.

urpf { strict | loose }

no urpf

【Parameter】

strict:use URPF strict mode

loose:use URPF loose mode

【Command configuration mode】

interface configuration mode

【Usage】

Only after creating corresponded VLAN interface, URPF can be configured. Interface URPF is defaulted to be disabled.

【Example】

！ Enable URPF of VLAN interface 1 and configure to be strict

Optiway(config-if-vlanInterface-1)#urpf strict

！ Disable URPF of VLAN interface 1

Optiway(config-if-vlanInterface-1)#no urpf

4.1.14 **show urpf**

Use this command to display URPF.

show urpf

【Command configuration mode】

interface configuration mode

【Example】

！Display URPF of VLAN interface 1

Optiway(config-if-vlanInterface-1)#show urpf

Chapter 5 ARP Configuration Command

5.1 ARP Configuration Command

ARP Configuration Command includes:

- **arp**
- **arp bind dynacmic**
- **arp aging**
- **show arp**
- **show arp aging**
- **arp-attack-protect**
- **show arp-attack-protect**
- **arp anti-flood**
- **arp anti-flood action**
- **arp anti-flood recover-time**
- **arp anti-flood recover**
- **show arp anti-flood**
- **arp anti-spoofing**
- **arp unknown**
- **arp anti-spoofing valid-check**
- **arp anti-spoofing deny-disguiser**
- **show arp anti-spoofing**
- **arp-dos-protect**
- **show arp-dos-protect**

- **arp** overwrite
- **show** arp overwrite

5.1.1 **arp**

Use **arp** command to adda a static arp table item. Use **no arp** command to delete a specified arp item.

arp ip-address mac [vlan-id interface-num]

arp ip-address **mac** mac [**vid** vlan-id][**port** interface-num]

no arp { all | dynamic | static | *ip-address* }

【Parameter】

ip-address:IP address of ARP maping item.

mac:MAC address of ARP maping item.

vlan-id:local VLAN ID which the frame with the destination address to be mac passed. It is in the range of 1～4294

interface-num:interface ID which the frame with the destination address to be mac passed.

static:static arp item

dynamic:dynamic arp item

all:all arp item

【Command configuration mode】

Global configuration mode

【Usage】

This command can add or delete a static arp item. Vlan-id must be the ID of created VLAN and the following interface interface must belong to this vlan. In

no command, if IP address is specified, delete the corresponded item; if choose static, delete all static arp item; if choose dynamic, delete all dynamic arp item; if choose all, delete all arp item. Above command cannot delete interface corresponded arp item.

【Example】

！Configure MAC address 22:21:22:23:24:25 corresponded to IP address 192.168.2.122 and passed through VLAN 1 interface 1

Optiway(config)#arp 192.168.2.122 22:21:22:23:24:25 1 2/1

！Delete arp item corresponded to IP address 192.168.2.122

Optiway(config)#no arp 192.168.2.122

5.1.2 arp bind dynamic

Use this command to bind static arp table item to be dynamic arp item.

arp bind dynamic { *ip-address* | all }

【Parameter】

ip-address : binding effective dynamic arp of specified ip address.

all : binding all dynamic arp item

【Command configuration mode】

Global configuration mode

【Usage】

Use this command to bind effective dynamic arp item. Effective here means valid and mac address cannot be all 2,multicast address or broadcast address.

【Example】

! Bind dynamic arp whose ip being 192.168.2.1 to be static arp

Optiway(config)#arp bind dynamic 192.168.2.1

! Bind all **effective** dynamic arp item to be static arp

Optiway(config)#arp bind dynamic all

5.1.3 arp aging

Use **arp aging** command to modify arp aging time. Use **no** command to restore it.

arp aging *time*

no arp aging-time

【Parameter】

time:new aging time with the unit being minute which is in the range of 3 to 2882. The default value is 22.

【Command configuration mode】

Global configuration mode

【Example】

！Configure ARP aging time to be 22 minutes.

Optiway(config)#arp aging 22

5.1.4 show arp

Use **show arp** command to display arp information.

show arp { all | dynamic | static | *ip-address* }

【Parameter】

all:display all arp item

dynamic:display all dynamic arp item

static:display all static arp item

ip-address:IP address of ARP maping item.

【Command configuration mode】

Any configuration mode

【Usage】

This command is used to display information of arp item,including: the corresponding relationship between IP address and MAC address, the ID of passed vlan, interface number and item type.

【Example】

！Display corresponded item of IP address 192.168.2.122

Optiway(config)#show arp 192.168.2.122

！Display all arp information

Optiway(config)#show arp all

！Display all static arp information

Optiway(config)#show arp static

！Display all dynamic arp information

Optiway(config)#show arp dynamic

5.1.5 **show arp aging-time**

Use **show arp aging** command to display ARP aging.

show arp aging

【Command configuration mode】

Any configuration mode

【Example】

！Display arp aging-time

Optiway(config)#show arp aging-time

5.1.6 **arp-attack-protect**

Use this command to configure ARP packet of specified IP address can be stopped through switch.

[no] arp-attack-protect *ip mask*

【Parameter】

ip:source ip address of stopped arp packet.

mask:mask of the above ip address

【Command configuration mode】

Global configuration mode

【Example】

！Configure to stop arp packet with the source IP address being 1.1.1.1 255,255,255,255 to go through switch

Optiway(config)#arp-attack-protect 1.1.1.1 255.255.255.255

5.1.7 **show arp-attack-protect**

Use his command to display the ARP packet with configured IP address to be stopped.

show arp-attack-protect

【Parameter】

Non

【Command configuration mode】

Any configuration mode

【Example】

！ Display the ARP packet with configured IP address to be stopped.

Optiway(config)#show arp-attack-protect

5.1.8 arp anti-flood

Use this command to enable arp anti-flood. Use **no** command to disable arp anti-flood.

arp anti-flood

no arp anti-flood

【Command configuration mode】

Global configuration mode

【Example】

! Enable arp anti-flood

Optiway(config)#arp anti-flood

! Disable arp anti-flood

Optiway(config)#no arp anti-flood

5.1.9 arp anti-flood action

Use this command to configure deny action and threshold of ARP anti-flood.

arp anti-flood action { deny-arp | deny-all } threshold *rate-limit*

【Parameter】

deny-arp : deny arp packet and filtrate all arp packets from this mac.

deny-all : deny all packets and filtrate all L2 frame from this mac.

rate-limit: rate threshold. Start deny when beyond it.

【Command configuration mode】

Global configuration mode

【Default】

Default deny action is deny-arp and the rate-limit is 16 pps.

【Example】

! Configure deny action to be banning all packets and rate-limit to be 12 pps

Optiway(config)#arp anti-flood action deny-all threshold 12

5.1.10 arp anti-flood recover-time

Use this command to configure ARP anti-flood recover time.

arp anti-flood recover-time *time*

【Parameter】

time:recover time which is in the range of 2-1442 minutes,if it is 2,it means never recover.

【Command configuration mode】

Global configuration mode

【Default】

Default time is 12 minutes

【Example】

! Configure recover time to be 22 minutes

Optiway(config)#arp anti-flood recover-time 22

5.1.11 arp anti-flood recover

use this command to recover MAC banned by ARP anti-flood manually.

arp anti-flood recover { *mac* | all }

【Parameter】

mac : banned mac address

all: recover all banned mac address

【Command configuration mode】

Global configuration mode

【Example】

! Recover banned mac:22:2a:5a:22:22:22

Optiway(config)#arp anti-flood recover 22:2a:5a:22:22:22

! Recover all banned mac

Optiway(config)#arp anti-flood recover all

5.1.12 show arp anti-flood

Use this command to show ARP anti-flood.

show arp anti-flood

【Command configuration mode】

Any configuration mode

【Example】

! Show arp anti-flood

Optiway(config)#show arp anti-flood

5.1.13 arp anti-flood bind blackhole

Use this command to bind blackhole address generated by arp anti-flood to be manually added.

arp anti-flood bind blackhole { *mac* | all }

【Parameter】

mac : blackhole generated by arp anti-flood

all: restore blackhole generated by arp anti-flood

【Command configuration mode】

Global configuration mode

【Example】

! Bind all blackhole generated by arp anti-flood

Optiway(config)#arp anti-flood bind balckhole all

5.1.14 arp anti-spoofing

Use this command to enable arp anti-spoofing. Use the **no** command to disable it.

arp anti-spoofing

no arp anti- spoofing

【Command configuration mode】

Global configuration mode

【Usage】

After enabling this function, all ARP through switch will be redirected to CPU. If source IP, source MAC,interface number,vlan id and static ARP are totally matched, it is thought to be valid and permitted normal handling and transmit. If not, drop it. If there is not corresponded static ARP table item, handle it as strategy of configuring unknown arp packet:drop it or flood（send to each interfce）.

【Example】

! Enable arp anti-spoofing

Optiway(config)#arp anti-spoofing

! Disable arp anti-spoofing

Optiway(config)#no arp anti-spoofing

5.1.15 arp anti-spoofing unknown

Use this command to configure unknown ARP packet handling strategy.

arp anti-spoofing unknown { discard | flood }

【Parameter】

discard : discard this unknown arp packet.

flood:flood （send to each interfce）this arp packet

【Command configuration mode】

Global configuration mode

【Default】

The default is discard.

【Example】

! Configure arp anti-spoofing unknown to be flood

Optiway(config)#arp anti-spoofing unknown flood

5.1.16 arp anti-spoofing valid-check

Use this command to enable check the validity of source MAC of ARP packet. Use **no** command to disable it.

arp anti-spoofing valid-check

no arp anti-spoofing valid-check

【Command configuration mode】

Global configuration mode

【Usage】

After enabling this function,it will check whether the source mac of arp packet sending to cpu is the as that in arp protocol packet. Drop it if they are different.

【Example】

! Enable ARP anti-spoofing valid-check:

Optiway(config)#arp anti-spoofing valid-check

! Disable ARP anti-spoofing valid-check:

Optiway(config)#no arp anti-spoofing valid-check

5.1.17 arp anti-spoofing deny-disguiser

Use this command to enable ARP anti-spoofing deny-disguiser. Use **no** command to disable it.

arp anti-spoofing deny-disguiser

no arp anti-spoofing deny-disguiser

【Command configuration mode】

Global configuration mode

【Usage】

After enabling this function, when switch cpu receives the ARP packet which is conflict with gateway address, push source mac of arp protocol packet to mac blackhole and send its own free arp. It will check arp broadcast packet. Those arp unicast packet not only for arp will not be checked for no uplink cpu.

【Example】

! Enable ARP anti-spoofing deny-disguiser:

Optiway(config)#arp anti-spoofing deny-disguiser

! Disable ARP anti-spoofing deny-disguiser:

Optiway(config)#no arp anti-spoofing deny-disguiser

5.1.18 show arp anti-spoofing

Use this command to show arp anti-spoofing.

show arp anti-spoofing

【Command configuration mode】

Any configuration mode

【Example】

Optiway(config)#show arp anti-spoofing

5.1.19 arp anti trust

Use this command to set the port to be trust and ARP packet from this port will not be check attacking and spoofing.

[no] arp anti trust

【Command configuration mode】

Interface configuration mode

【Example】

！Configure e2/1 to be trust

Optiway(config-if-ethernet-2/1)#arp anti trust

5.1.20 arp-dos-protect

Use this command to configure ARP packet rate, which is to limit ARP packet through switch.

arp-dos-protect *rate*

【Parameter】

rate:the max rate of ARP packet through switch. The speed rate is in the unit of kbps and in the range of 64kbps--16384kbps (16mbps). In addition, the rate configured here can only be the multiple of 64kbps(it is restricted by hardware).

【Command configuration mode】

Global configuration mode

【Example】

！Restrict the max speed rate of ARP packet through switch to be 128

Optiway(config)#arp-dos-protect 128

5.1.21 **show arp-dos-protect**

Use this command to display the restriction to the speed rate of ARP packet.

show arp-dos-protect

【Parameter】

Non

【Command configuration mode】

Any configuration mode

【Example】

！Display the restriction to the speed rate of ARP packet.

Optiway(config)#show arp-dos-protect

5.1.22 **arp overwrite**

Use this command to enable and disable ARP overwrite and configure arp conflict. When this function is enabled, the table will be update with arp conflict.

[no] arp overwrite

【Parameter】

Non

【Command configuration mode】

Global configuration mode

【Example】

！Enable ARP overwrite

Optiway(config)#arp overwrite

5.1.23 show arp overwrite

Use this command to display arp overwrite configuration.

show arp overwrite

【Parameter】

Non

【Command configuration mode】

Any configuration mode

【Example】

！Display arp overwrite configuration

Optiway(config)#show arp overwrite

Chapter 6 DHCP Configuration Command

6.1 DHCP Configuration Command

- **dhcp-relay**
- **dhcp-relay hide server-ip**
- **dhcp-server**
- **dhcp-snooping**
- **dhcp-snooping trust**
- **dhcp-snooping max-clients**
- **dhcp option82**
- **dhcp option82 strategy**
- **dhcp option82 format**
- **dhcp option82 circuit-id string**
- **dhcp option82 remote-id string**
- **ip-source-guard**
- **ip-source-guard bind ip**
- **show dhcp-relay**
- **show dhcp-relay hide server-ip**
- **show dhcp-server**
- **show dhcp-server interface**
- **show dhcp-snooping**
- **show dhcp-snooping clients**

6.1.1 dhcp-relay

Use **Dhcp-relay** command to enable DHCP relay. Use **no dhcp-relay** command to disable DHCP relay.

Dhcp-relay

no dhcp-relay

【Command configuration mode】

Global configuration mode

【Usage】

Enable DHCP relay before enabling DHCP server.

【Example】

！Enable DHCP relay

Optiway(config)#dhcp-relay

！Disable DHCP relay

Optiway(config)#no dhcp-relay

6.1.2 dhcp-relay hide server-ip

Use **dhcp-relay hide server-ip** command to enable hide server address in DHCP relay. Use **no dhcp-relay hide server-ip** command to disable hide of DHCP.

dhcp-relay hide server-ip

no dhcp-relay hide server-ip

【Command configuration mode】

Global configuration mode

【Default】

Disable

【Usage】

Enable DHCP relay before enabling DHCP hide server. Only after enabling all DHCP, network can operate normally.

【Example】

！Enable hide DHCP server of DHCP relay

Optiway(config)#dhcp-relay hide server-ip

！Disable hide DHCP server of DHCP relay

Optiway(config)#no dhcp-relay hide server-ip

6.1.3 **dhcp-server**

Use following command to configure DHCP server. Use its **no** command to delete configured DHCP server. Configure in global configuration mode:

dhcp-server dhcp-num **ip** ip-addres

no dhcp-server *dhcp-num*

Followings are specified DHCP server of layer 3 interface. Use its **no** command to cancel it. Configure it in interface configuration mode.

dhcp-server *dhcp-num*

no dhcp-server

【Parameter】

dhcp-num:DHCP server number which is in the range of 1～32

ip-addres:IP address of DHCP server

【Command configuration mode】

Global configuration mode, interface configuration mode

【Usage】

Use this command in global configuration mode to configure DHCP server. Specify DHCP server in layer 3 interface in interface configuration mode. If configuring IP address of DHCP server to be the IP address of some layer 3 interface, built-in DHCP server will be used.

【Example】

! Configure IP address of DHCP server 2 to be 192.168.2.122

Optiway(config)#dhcp-server 2 ip 192.168.2.122

! Delete DHCP server 2

Optiway(config)#no dhcp-server 2

! Specify VLAN interface 2 to use DHCP server 1

Optiway(config-if-vlanInterface-2)#dhcp-server 1

! Cancel specified DHCP server of VLAN interface 2

Optiway(config-if-vlanInterface-2)#no dhcp-server

6.1.4 dhcp-snooping

Use **dhcp-snooping** command to configure DHCP SNOOPING. Use **no dhcp-snooping** command to delete this configuration. Configure it in global configuration mode.

dhcp-snooping

no dhcp-snooping

【Command configuration mode】

Global configuration mode

【Example】

！Enable DHCP SNOOPING

Optiway(config)#dhcp-snooping

6.1.5 dhcp-snooping trust

Use **dhcp-snooping trust** command to configure DHCPSNOOPING interface to be trust interface. Use **no dhcp-snooping trust** command to restore it to be non-trust interface.

dhcp-snooping trust

no dhcp-snooping trust

【Command configuration mode】

Interface configuration mode

【Usage】

Interface is defaulted to be nontrust. Valid DHCP server must connect to trust interface.

【Example】

！Configure ethernet 2/1 to be trust interface.

Optiway(config-if-ethernet-2/1)#dhcp-snooping trust

6.1.6 dhcp-snooping max-clients

Followings are used to configure interface or the max DHCP client number permitted by VLAN.

dhcp-snooping max-clients *num*

no dhcp-snooping max-clients

【Parameter】

num:the max number which is in the range of 2 to 2248. it is defaulted to be 2248.

【Command configuration mode】

Interface configuration mode, VLAN configuration mode

【Example】

！Configure the max learning number of Ethernet 2/1 to be 33

Optiway(config-if-ethernet-2/1)#dhcp-snooping max-clients 33

！Configure the max learning number of VLAN 2 to be 33

Optiway(config-if-vlan)#dhcp-snooping max-clients 33

6.1.7 dhcp option82

Use **dhcp option82** command to enable DHCP relay and option82 of DHCP relay. Use **no dhcp option82** command to disable option82 of DHCP.

dhcp option82

no dhcp option82

【Command configuration mode】

Global configuration mode

【Default】

Disable

【Usage】

This command will be effective after DHCP relay enabling.

【Example】

！ Enable option82 of DHCP relay.

Optiway(config)#dhcp option82

6.1.8 dhcp option82 strategy

Use **dhcp option82 strategy** command to configure strategy of request packet which includes option82.

dhcp option82 strategy {drop|keep|replace}

no dhcp option82 strategy

【Command configuration mode】

Global configuration mode

【Parameter】

drop:drop request packet

keep:keep original option82

replace:replace original option82

【Default】

Replace

【Usage】

This command will be effective after DHCP relay enabling.

【Example】

！ Configure strategy to be drop

Optiway(config)#dhcp option82 strategy drop

6.1.9 dhcp option82 format

Use this command to configure dhcp option82 format.

dhcp option82 format {normal | verbose [node-identifier { mac | hostname | user-defined *node-identifier* }] }

no dhcp option82 format

no dhcp option82 format verbose node-identifier

【Command configuration mode】

Global configuration mode

【Parameter】

nomal:the format is normal.

verbose:the format is verbose.

node-identifier { mac | hostname| user-defined *node-identifier*}:accessing node identifier. By default,the node-identifier is mac address.

mac:use mac as node-identifier

hostname:use hostname as node-identifier

user-defined *node-identifier* use specific string as node-identifier. node-identifier ranges from 1-52 byte

【Default】

normal

【Usage】

1)dhcp option82 format is for Option 82 format. no dhcp relay information

format is for restore to default format.

2)when using no dhcp option82 format, if *verbose node-identifier* is empty, it will restore to normal； if not, it will restore to be mac in verbose format.

3）if hostname is node-identifier, there cannot be space in the hostname, or, option82 will be added fail.

【Example】

！Set format as verbose

Optiway(config)#dhcp option82 format verbose

6.1.10 dhcp option82 circuit-id string

Use this command to configure user-defined Circuit ID. Use no command to restore to default configuration.

dhcp option82 circuit-id string *circuit-id*

no dhcp option82 circuit-id string

【Command configuration mode】

Global configuration mode

【Parameter】

circuit-id:user-defined Circuit ID , which is in the range of 1～64.

【Default】

Empty.Circuit ID is determined by Option 82 format.

【Usage】

After configuring user-defined Circuit ID, it will be used in normal mode, but not, in verbose mode.

【Example】

！Configure Circuit ID of Option 82 to be company221

Optiway(config)#dhcp option82 circuit-id company221

6.1.11 dhcp option82 remote-id string

Use this command to configure user-defined Remote ID. Use no command to restore to default configuration.

dhcp option82 remote-id string {*remotet-id* | hostname}

no dhcp option82 remote-id string

【Command configuration mode】

Global configuration mode

【Parameter】

remote-id:user-defined Remote ID , which is in the range of 1～64.

hostname: hostname is as Remote ID

【Default】

Empty. Remote ID is determined by Option 82 format.

【Usage】

After configuring user-defined Remote ID, user-defined Circuit ID can be used in normal and verbose mode.

【Example】

！Configure Remote ID of Option 82 to be device221

Optiway(config)#dhcp option82 circuit-id device221

6.1.12 ip-source-guard

Use this command to enable interface IP source guard. Use **no** command to disable it.

ip-source-guard

no ip-source-guard

【Command configuration mode】

Interface configuration mode, VLAN configuration mode

【Example】

！Enable IP source guard of e2/1

Optiway(config-if-ethernet-2/1)#ip-source-guard

6.1.13 ip-source-guard bind ip

Use this command to configure IP source guard to static bind entry, use **no** to delete IP source guard static bind entry

ip-souce-guard bind ip *ip-address* [mac *mac* [interface ethernet *interface-num*]]

no ip-source-guard bind ip { *ip-address* | all }

【Command mode】

Global configuration mode

【Example】

！Configure IP source guard static bind entry

OptiWay(config-if-ethernet-2/1)#ip-source-guard bind ip 192.168.0.1 mac 0:0:0:0:0:1 interface ethernet 2/1

6.1.14 show dhcp-relay

Use **show dhcp-relay** command to display DHCP relay configuration.

show dhcp-relay

【Command configuration mode】

Any configuration mode

【Example】

！Display DHCP relay configuration

Optiway(config)#show dhcp-relay

DHCP relay is enabled!

6.1.15 show dhcp-relay hide server-ip

Use **show dhcp-relay hide server-ip** command to display hide server IP configuration of DHCP relay.

show dhcp-relay hide server-ip

【Command configuration mode】

Any configuration mode

【Example】

！Display hide server-ip of DHCP relay

Optiway(config)#show dhcp-relay hide server-ip

DHCP RELAY hide server-ip is enabled!

6.1.16 show dhcp-server

Use **show dhcp-server** command to display specified or all DHCP server

configuration.

show dhcp-server [*server-id*]

【Parameter】

server-id:DHCP server number

【Command configuration mode】

Any configuration mode

【Example】

！Display all DHCP server configuration

Optiway(config)#show dhcp-server

6.1.17 **show dhcp-server inerface**

Use **show dhcp-server inerface** command to display Dhcp server configuration specified for layer 3 interface.

show dhcp-server inerface [{ supervlan-interface *supervlan-id* } | { vlan-interface *vlan-id* }]

【Parameter】

supervlan-id:id of superVLAN interface which is in the range of 1～11

vlan-id:VLAN id which is in the range of 1～4294

【Command configuration mode】

Any configuration mode

【Usage】

This command displays Dhcp server configuration specified for layer 3 interface. Interface ID is optional. If it is vacant, all Dhcp server configuration

specified for layer 3 interface will be displayed.

【Example】

！Display all Dhcp server configuration specified for layer 3 interface.

Optiway(config)#show dhcp-server interface

6.1.18 show dhcp-snooping interface

Use **show dhcp-snooping interface** command to show DHCP SNOOPING configuration.

show dhcp-snooping interface [*interface-num*]

【Parameter】

interface-num:consist of port type + port num,port type is ethernet,port num is device/slot-num/port-num,device means stack device num,the range is 0～7,slot-num is slot num,the range is 0～1,port-num is the port num,the range is 1～48.

【Command configuration mode】

Any configuration mode

【Usage】

When displaying port information, if not appoints the port type and port num,it displays all ports information；if appoints to port type and port num, it displays select port information.

【Example】

！Display port 1 DHCP SNOOPING configuration

OptiWay(config)#show dhcp-snooping interface ethernet 2/1

6.1.19 show dhcp-snooping vlan

Use this command to display VLAN DHCP SNOOPING configuration.

show dhcp-snooping vlan [*vlan-id*]

【Command mode】

All command mode

【Usage】

When displaying vlan,it diplays configured vlan if without selected vlan-id,it diplays selected vlan if with vlan-id.

【Example】

！ Display configured all vlan DHCP SNOOPING configuration

OptiWay(config)#show dhcp-snooping vlan

6.1.20 **show ip-source-guard bind ip**

Use this command to display ip-source-guard static bind entry

show ip-source-guard bind ip { *ip-address*| all }

【Command mode】

All command mode

【Example】

！ Display ip as 192.168.0.1 ip-source-guard static bind entry

OptiWay(config)#show ip-source-guard bind ip 192.168.0.1

6.1.21 **show dhcp-snooping clients**

Use **show dhcp-snooping clients** command to display user information.

show dhcp-snooping clients

【Command configuration mode】

Any configuration mode

【Example】

！Display user information

Optiway(config)#show dhcp-snooping clients

Chapter 7 Local IP Address Pool Configuration Command

7.1 Local IP Address Pool Configuration Command

Local IP Address Pool Configuration Command:

- **dhcp-client**
- **dns primary-ip**
- **dns second-ip**
- **dns suffix**
- **gateway**
- **ip**
- **ip-bind**
- **ip pool**
- **lease**
- **section**
- **show dhcp-client**
- **show ip-bind**
- **show ip pool**
- **wins primary-ip**
- **wins second-ip**

7.1.1 dhcp-client

Use this command to configure dhcp client. When ip-bind enables, only configured dhcp client can apply specified IP address.

dhcp-client mac ip vlanid

no dhcp-client *mac vlanid*

【Parameter】

mac: mac address of client

ip:the ip address distributed to client

vlanid:the vlan the client is in

【Command configuration mode】

Global configuration mode

【Example】

！Add client with mac address being 21:22:5e:22:22:22,vlan being 2,ip addrss being 5.5.1.2

Optiway(config)#dhcp-client 21:22:5e:22:22:22 5.5.1.2 2

！Delete client with mac address being 21:22:5e:22:22:22,vlan being 2

Optiway(config)#no **dhcp-client** 21:22:5e:22:22:22 2

7.1.2 dns primary-ip

Use **dns primary-ip** command to configure IP address of primary DNS server of local IP address pool. Use **no dns primary-ip** command to delete IP address of primary DNS server.

dns primary-ip *ip-address*

no dns primary-ip

【Parameter】

ip-address:IP address of primary DNS server.

【Command configuration mode】

Local IP address pool configuration mode

【Example】

！Configure primary DNS server of local IP address pool to be 192.168.2.122

Optiway(config-ip-pool-green)#dns primary-ip 192.168.2.122

！Delete primary DNS server of local IP address pool green

Optiway(config-ip-pool-green)#no dns primary-ip

7.1.3 dns second-ip

Use **dns second-ip** command to configure IP address of second DNS server of local IP address pool. Use **no dns second-ip** command to delete IP address of second DNS server.

dns second-ip *ip-address*

no dns second-ip

【Parameter】

ip-address:IP address of second DNS server.

【Command configuration mode】

Local IP address pool configuration mode

【Example】

！Configure second DNS server of local IP address pool to be 192.168.2.222

Optiway(config-ip-pool-green)#dns second-ip 192.168.2.222

！Delete second DNS server of local IP address pool green

Optiway(config-ip-pool-green)#no dns second-ip

7.1.4 dns third-ip

Use dns third-ip command to configure IP address of third DNS server of local IP address pool. Use **no dns third-ip** command to delete IP address of third DNS server.

dns third-ip *ip-address*

no dns third-ip

【Parameter】

ip-address:IP address of fourth DNS server.

【Command configuration mode】

Local IP address pool configuration mode

【Example】

！Configure third DNS server of local IP address pool to be 192.168.2.322

Optiway(config-ip-pool-green)#dns third-ip 192.168.2.322

！Delete third DNS server of local IP address pool green

Optiway(config-ip-pool-green)#no dns third-ip

7.1.5 dns fourth-ip

Use **dns fourth-ip** command to condifure IP address of fourth DNS server of local IP address pool. Use **no dns fourth-ip** command to delete IP address of fourth DNS server.

dns fourth-ip *ip-address*

no dns fourth-ip

【Parameter】

ip-address:IP address of fourth DNS server.

【Command configuration mode】

Local IP address pool configuration mode

【Example】

！Configure fourth DNS server of local IP address pool to be 192.168.2.422

Optiway(config-ip-pool-green)#dns fourth-ip 192.168.2.422

！Delete fourth DNS server of local IP address pool green

Optiway(config-ip-pool-green)#no dns fourth-ip

7.1.6 **dns suffix**

Use **dns suffix** command to configure DNS suffix of local IP address pool.
Use **no dns suffix** command to delete DNS suffix of local IP address pool.

dns suffix *suffix-name*

no dns suffix

【Parameter】

suffix-name:DNS suffix

【Command configuration mode】

Local IP address pool configuration mode

【Example】

！Configure DNS suffix of address pool green to be greennet.com.cn

Optiway(config-ip-pool-green)#dns suffix greennet.com.cn

！Delete DNS suffix of address pool green

Optiway(config-ip-pool-green)#no dns suffix

7.1.7 gateway

Use **gateway** command to configure gateway and netmask.

gateway ip-address mask

【Parameter】

ip-address:gateway of local IP address pool.

mask:netmask of local IP address pool.

【Command configuration mode】

Local IP address pool configuration mode

【Usage】

All addresses must be in the area determined by gateway and netmask of local IP address pool, and address in address pool cannot include gateway address.

【Example】

！Configure gateway of address pool to be 192.168.2.122, netmask to be 255.255.255.2

Optiway(config-ip-pool-green)#gateway 192.168.2.122 255.255.255.2

7.1.8 ip

Use **ip** command to enable/disable Ip address in local IP address pool.

ip { disable | enable } *ip-address*

【Parameter】

ip-address: must include some network interface in local IP address pool.

【Command configuration mode】

Local IP address pool configuration mode

【Example】

！Disable specified address in local IP address pool network

Optiway(config-ip-pool-green)#ip disable 192.168.2.122

！Enable specified address in local IP address pool network

Optiway(config-ip-pool-green)#ip enable 192.168.2.122

7.1.9 ip-bind

Use this command to enable or disable ip-bind. After enabling ip-bind,only configured dhcp client can apply specified IP address.

ip-bind

no ip-bind

【Parameter】

non

【Command configuration mode】

Global configuration mode

【Example】

！Enable ip bind

ip-bind

！Disable ip-bind

no ip-bind

7.1.10 ip pool

Use **ip pool** command to enter local IP address pool configuration mode. Use **no ip pool** command to delete specified address pool.

ip pool ippoolname

no ip pool *ippoolname*

【Parameter】

ippoolname:character string of address pool name which is in the range of 1～32 characters.

【Command configuration mode】

Global configuration mode

【Usage】

If the IP address pool in ippoolname doesn't exist, create it.

【Example】

！Create and enter local IP address pool green

Optiway(config)#ip pool green

Optiway (config-ip-pool-green)#

7.1.11 lease

Use **lease** command to configure lease of local IP address pool.

lease day:hour:min

【Parameter】

day:hour:min:lease time which is accurated to minute. The shortest is 2:2:1 and the longest is 999:23:59. The default time is 1 day.

【Command configuration mode】

Local IP address pool configuration mode

【Example】

！Configure lease of local IP pool green is 1 day 1 hour 1 minute

Optiway(config-ip-pool-green)#lease 1:1:1

7.1.12 section

Use **section** command to configure local IP pool network interface. Use **no section** command to delete specified IP address pool network interface.

section section-id from-ip to-ip

no section *section-id*

【Parameter】

section-id is the section number of this address pool and at most 8 groups. from-ip is the start address of this address section. to-ip is the end address of this address section. This two ip must be in the address area determined by gateway and netmask excluding gateway address.

【Command configuration mode】

Local IP address pool configuration mode

【Example】

！Configure network interface of local IP address pool

Optiway(config-ip-pool-green)#section 2 192.168.2.122 192.168.2.222

！Delete local IP pool network interface 2

Optiway(config-ip-pool-green)#no section 2

7.1.13 show dhcp-client

Use this command to display specified IP address,MAC or all client configuration.

show dhcp-client [mac | ip]

【Parameter】

mac:mac address of dhcp client

ip:ip address of dhcp client

【Command configuration mode】

Any configuration mode

【Example】

！Display all dhcp client configuration

Optiway(config)#show dhcp-client

7.1.14 show ip-bind

Use this command to display ip-bind configuration.

show ip-bind

【Parameter】

non

【Command configuration mode】

Any configuration mode

【Example】

！Display ip-bind configuration

Optiway(config)#show ip-bind

7.1.15 show ip pool

Use **show ip pool** command to display specified or all IP pool configuration.

show ip pool [ippool-name [section-num]]

【Parameter】

ippool-name:name of specified IP pool

section-num: section number of specified IP pool

【Command configuration mode】

Any configuration mode

【Example】

！Display all local IP pool configuration

Optiway(config)#show ip pool

7.1.16 wins primary-ip

Use **wins primary-ip** command to configure primary WINS server IP address of this IP pool. Use **no wins primary-ip** command to delete primary WINS server IP address of this IP pool.

wins primary-ip *ip-address*

no wins primary-ip

【Parameter】

ip-address: IP address of primary WIN server.

【Command configuration mode】

Local IP address pool configuration mode

【Example】

！Configure primary WIN server of local IP pool green to be 192.168.2.122

Optiway(config-ip-pool-green)#wins primary-ip 192.168.2.122

！Delete primary WINS server IP address of local IP pool green.

Optiway(config-ip-pool-green)#no wins primary-ip

7.1.17 **wins second-ip**

Use **wins second-ip** command to configure second WINS server IP address of this IP pool. Use **no wins second-ip** command to delete second WINS server IP address of this IP pool.

wins second-ip *ip-address*

no wins second-ip

【Parameter】

ip-address: IP address of second WIN server.

【Command configuration mode】

Local IP address pool configuration mode

【Example】

！Configure second WIN server of local IP pool green to be 192.168.2.222

Optiway(config-ip-pool-green)#wins second-ip 192.168.2.222

！Delete second WINS server IP address of local IP pool green.

Optiway (config-ip-pool-green)#no wins second-ip

Chapter 8 Static Routing Configuration Command

8.1 Static Routing Configuration Command

Static Routing Configuration Command includes:

- **ip route**
- **show ip route**

8.1.1 ip route

Use **ip route** command to add a static route. Use **no ip route** command to delete a specified static route. Use no ip route static all command to delete all static route.

ip route dst-ip mask gate-ip

no ip route dst-ip mask [gate-ip]

no ip route static all

【Parameter】

dst-ip:static route destination address to be added which is in the form of dotted decimal

mask:destination address mask which is in the form of dotted decimal

gate-ip:static route next hop address which is in the form of dotted decimal

【Command configuration mode】

Global configuration mode

【Usage】

This command can add or delete a static routing table item. If destination IP and mask are 2, the added route is default route. Gateway address may not be input when deleting route, if it is inputted, it must be the same as that in routing table.

【Example】

！Add a route to 192.168.2.122 network interface, the next hop address is 12.11.2.254

Optiway(config)#ip route 192.168.2.122 255.255.2.2 12.11.2.254

！Delete route which is to 192.168.2.122 network interface

Optiway(config)#no ip route 192.168.2.122 255.255.2.2

！Delete all static route

Optiway(config)#no ip route static all

8.1.2 **show ip route**

Use **show ip route** command to display information of specified route.

show ip route [*ip-address* [*mask*] | static | rip |ospf]

【Parameter】

ip-address:destination address to be displayed which is in the form of dotted decimal.

mask:destination address mask which is in the form of dotted decimal

static:display all statuc routing item.

rip: display all rip routing item.

ospf: display all ospf routing item.

【Command configuration mode】

Any configuration mode

【Usage】

This command is used to display related information of specified routing table item, including the next hop address and routing type. It can be displayed as route to specified deatination address, all static route and all routes. If there is no keyword, all routes will be displayed.

【Example】

！ Display route information to IP address 192.168.2.122

Optiway(config)#show ip route 192.168.2.122

！ Display all routing table

Optiway(config)#show ip route

！ Display all rip routing table

Optiway(config)#show ip route rip

！ Display all ospf routing table

Optiway(config)#show ip route ospf

Chapter 9 RIP Configuration Command

9.1 RIP Configuration Command

RIP configuration command includes:

- **auto-summary**
- **host-route**
- **ip rip authentication**
- **ip rip input**
- **ip rip metricin**
- **ip rip metricout**
- **ip rip output**
- **ip rip split**
- **ip rip version**
- **ip rip work**
- **network**
- **router rip**
- **ip prefix-list**
- **ip prefix-list default**
- **show ip prefix-list**
- **redistribute**
- **distribute-list**
- **show ip rip**
- **show ip rip interface**

9.1.1 auto-summary

Use **auto-summary** command to configure to auto-summary routing when running RIP-2. Use **no auto-summary** command to cancel auto-summary of RIP-2.

auto-summary

no auto-summary

【Default】

RIP-2 is defaulted to auto-summary. For RIP-1,it always summary for it doesn't send network mask when sending routing packet.

【Command configuration mode】

RIP protocol configuration mode

【Example】

！Configure system auto-summary when running RIP-2

Optiway(config-router-rip)#auto-summary

9.1.2 host-route

Use **host-route** command to configure RIP receive host routing. Use **no host-route** command to configure to refuse to receive host routing in RIP packet.

host-route

no host-route

【Default】

RIP receive host routing.

【Command configuration mode】

RIP protocol configuration mode

【Example】

！Configure RIP refuse to receive host routing

Optiway(config-router-rip)#no host-route

9.1.3 ip rip authentication

Use **ip rip authentication simple** command to configure RIP-2 plain text authentication and the password or configure RIP-2 being MD5 authentication and configure MD5 key id and key string.

ip rip authentication { simple *password* | md5 key-id *key-id* key-string *key-string* }

no ip rip authentication

【Parameter】

password:RIP-2 plain text authentication password which is in the range of 1～16

key id: key id for MD5 authentication of RIP-2

key-string: key string for MD5 authentication of RIP-2

【Default】

RIP-2 authentication disables.

【Command configuration mode】

Interface configuration mode

【Usage】

RIP-1 doesn't support packet authentication and RIP-2 supports authentication.

【Example】

！Enable plain text authentication of VLAN interface 3 with the keyword to be Optiway

Optiway(config-if-vlanInterface-3)#ip rip authentication Optiway

9.1.4 ip rip input

Use **ip rip input** command to permit interface receiving RIP packet. Use **no ip rip input** command to configure interface refuse to receive RIP packet.

ip rip input

no ip rip input

【Default】

Interface receives RIP packet.

【Command configuration mode】

Interface configuration mode

【Example】

！Configure VLAN interface 3 not to receive RIP packet

Optiway(config-if-vlanInterface-3)#no ip rip input

9.1.5 ip rip metricin

Use **ip rip metricin** command to configure the added metricin value of router when receiving RIP packet. Use **no ip rip metricin** command to restore the default metricin value.

ip rip metricin *value*

no ip rip metricin

【Parameter】

Value: the added metricin value of router when receiving RIP packet which is in the range of 2 to 16.

【Default】

It is defaulted to be 2.

【Command configuration mode】

Interface configuration mode

【Example】

！Configure the added metricin value of router when receiving RIP packet of VLAN interface 3 to be 1

Optiway(config-if-vlanInterface-3)#ip rip metric 1

9.1.6 ip rip metricout

Use **ip rip metricout** command to configure the added metricout value of router when sending RIP packet. Use **no ip rip metricout** command to restore the default metricout value.

ip rip metricout *value*

no ip rip metricout

【Parameter】

Value: the added metricout value of router when sending RIP packet which is in the range of 2 to 16.

【Default】

It is defaulted to be 2.

【Command configuration mode】

Interface configuration mode

【Example】

！Configure the added metricout value of router when sending RIP packet of VLAN interface 3 to be 1

Optiway(config-if-vlanInterface-3)#ip rip metricout 1

9.1.7 ip rip output

Use **ip rip output** command to permit interface sending RIP packet. Use **no ip rip output** command to forbid interface sending RIP packet.

ip rip output

no ip rip output

【Default】

It is defaulted not to send RIP packet to the outside.

【Command configuration mode】

Interface configuration mode

【Example】

！Forbid VLAN interface 3 sending RIP outside

Optiway(config-if-vlanInterface-3)#no ip rip output

9.1.8 ip rip split

Use **ip rip split** command to enable the split when interface sending RIP packet. Use **no ip rip split** command to disable it.

ip rip split

no ip rip split

【Default】

Enable the split when interface sending RIP packet.

【Command configuration mode】

Interface configuration mode

【Usage】

To prevent routing ring, it is necessary to split. For some special situation, to guarantee the correctly running of protocol, split disables.

【Example】

！Configure VLAN interface 3 to use split when sending RIP packet.

Optiway(config-if-vlanInterface-3)#ip rip split

9.1.9 ip rip version

Use **ip rip version** command to configure RIP version of layer 3 interface. Use **no ip rip version** command to restore the default RIP version.

ip rip version 1

ip rip version 2 [bcast | mcast]

no ip rip version

【Parameter】

1:Configure the RIP version to be RIP-1

2:Configure the RIP version to be RIP-2

bcast:use broadcast when RIP-2 receiving and sending RIP

mcast:use multicast when RIP-2 receiving and sending RIP

【Default】

It is defaulted to run RIP-1. If configuring to be RIP-2, it is defaulted to use multicast.

【Command configuration mode】

Interface configuration mode

【Usage】

Running RIP-1, it can receive and send RIP-1 broadcast packet; when running RIP-2 and using broadcast, it can receive RIP-1 packet and RIP-2 broadcast packet not RIP-2 multicast packet; when running RIP-2 and using multicast, it can only send and receive RIP-2 multicast packet.

【Example】

！ Configure VLAN interface 3 to run RIP-2 and use multicast

Optiway(config-if-vlanInterface-3)#ip rip version 2 mcast

9.1.10 ip rip work

Use **ip rip work** command to permit sending and receiving RIP packet. Use **no ip rip work** command to refuse to send and receive RIP packet.

ip rip work

no ip rip work

【Default】

Receive and send RIP packet is permitted.

【Command configuration mode】

Interface configuration mode

【Usage】

This command equals to **ip rip input** and **ip rip output** command. The latter two control the receiving and sending RIP packet of interface.

【Example】

！Permit VLAN interface 3 receiving and sending RIP packet.

Optiway(config-if-vlanInterface-3)#ip rip work

9.1.11 **network**

Use **network** command to specify the IP network interface to run RIP protocol. Use **no network** command to cancel IP network interface to run RIP protocol.

network ip-address

no network ip-address

【Default】

All network interface will not run RIP protocol.

【Command configuration mode】

RIP protocol configuration mode

【Usage】

After enabling RIP, use this command to specify the IP network interface to run RIP protocol. Attribution of all interface will be effective after running RIP. Because the mask has been configured when creating this IP network

interface, this command needs not input mask.

【Example】

！ Specify network interface 192.1.1.1/24 to run RIP

Optiway(config-router-rip)#network 192.1.1.1

9.1.12 router rip

Use **router rip** command to enable RIP protocol and enter RIP mode. Use **no router rip** command to disable RIP protocol.

router rip

no router rip

【Default】

RIP disables.

【Command configuration mode】

Global configuration mode

【Example】

！ Enable RIP protocol

Optiway(config)#router rip

！ Disable RIP protocol

Optiway(config)#no router rip

9.1.13 ip prefix-list

Use this command to configure an address prefix list or item. Use the no command to remove it.

ip prefix-list prefix-list-name [**seq** seq-number] {**deny** nework len | **permit** network len} [**ge** ge-value] [**le** le-value]

no ip prefix-list *prefix-list-name* [**seq** *seq-number* | **deny** | **permit**]

【Parameter】

prefix-list-name:name of prefix-list

seq:Use seq number to the prefix acl item to be created or deleted.

seq-number:It is used for the order of handling the filtrated.

deny:deny it when matching

permit:permit it when matching

network:giving the prefix to be matched

len:giving the length of prefix to be matched

ge:applying “ge-value”to the given arrange

ge-value:match the range of mask length for the more concrete prefix than“network/len”. If only “ge” is specified, the range is from “ge-value”（larger than or equal to ge-value）to 32（smaller or equal to 32）

le:apply “le-value”to specified range

le-value:match the range of mask length for the more concrete prefix than“network/len”. If only “le” is specified, the range is from “length”（larger than or equal to length）to“le-value”（smaller or equal to le-value）

【Default】

when the seq number is not specified, the default adding value is 12,that is, the first seq number in a prefix acl is 12,and the second and the third is 22 and 32. If the specified seq number is 24,the following is 34, 44 etc. The adding value is not 1 is convenient to insert sentence in configured ones.

【Command configuration mode】

Global configuration mode

【Usage】

ge-value and le-value must satisfy:

length<ge-value<=le-value<=32

length is the length of prefix of the IP address to be matched; ge-value and le-value specify the range of the prefix of the mask to be matched.If ge-value and le-value are not specified, the range is from length to 32；if specified, they are from ge-value to le-value；if only one is specified, refer to the above discription.

Example:

Optiway(config)#ip prefix-list prefix221 permit 192.2.2.2 8 le 24

Optiway(config)#ip prefix-list prefix221 deny 192.2.2.2 8 ge 25

The above commands will check whether the first byte of the toute destination address is 192；then, check the route mask length. The mask with the length larger than and equal to 8 and smaller than and equal to 24 matches “permit”, and the mask with the length larger than and equal to 25 and smaller than and equal to 24 matches “deny”.

Specially, the form with prefix being 2.2.2.2/32can match the route with the destination address and mask being 2（not matching the route with destination being 2 and mask being 1）；2.2.2.2 matches all routes.

【Example】

！Configure prefix ACL to deny route with destination address being 192.168.1.2/24（including all subnetwork route）

Optiway(config)#ip prefix-list pflst221 deny 192.168.1.2 24

Optiway(config)#ip prefix-list pflst221 permit 2.2.2.2 2

9.1.14 ip prefix-list default

Use this command to configure the matching mode when the item does not exist in current prefix list or has no matching item in prefix list.Use the no command to restore the default matching mode.

ip prefix-list default { tab-rule { deny | permit } | entry-rule { deny | permit } }

no ip prefix-list default { tab-rule | entry-rule }

【Parameter】

tab-rule:configure the matching mode with the prefix is not exist.

entry-rule:configure the matching mode when there is no matching item in prefix list.

deny:deny matching mode

permit:permit matching mode

【Default】

By default, the matching mode that the prefix list does not exist is permit and the other is deny.

【Command configuration mode】

Global configuration mode

【Example】

！Configure the matching mode without matching item in prefix list to be permit

Optiway(config)#ip prefix-list default entry-rule permit

9.1.15 show ip prefix-list

Use this command to display some or all prefix list.

show ip prefix-list [prefix-list-name]

【Parameter】

prefix-list-name:name of prefix list

【Command configuration mode】

Any configuration mode

【Example】

！Display all prefix list

Optiway(config)#show ip prefix-list

9.1.16 redistribute

Use **redistribute** command to introduce external static routing or routing information found by other routing protocol. Use **no redistribute** command to cancel the introduction.

redistribute *protocol* [**metric** *metric*] [**type** { 1 | 2 }] [**tag** *tag-value*]

no redistribute [*protocol*]

【Parameter】

protocol:introduced source routing protocol which can be connected, rip and static.

【Default】

None introduction.

【Command configuration mode】

OSPF protocol configuration mode

【Usage】

Each dynamic routing protocol can share routing information. Because of OSPF, router found by other routing protocol always be handled as external routing information of autonomy.

OSPF uses following 4 kinds of different router which as priority order are:

□ □·Inter Area Routing

□ □·Area Border Routing

□ □·The first category external routing

□ □·The second category external routing

The description of routing in or between areais for network structurein Autonomy system. External routingdescribes how to choose destination routing out of Autonomy system.

The first category external routing is received IGP router (such as: RIP and STATIC). This kind of router is more credible, so the cost volume of external router and autonomy system is the same and can compare with the router of OSPF itself, that is, the cost to external router= the cost to its ASBR +the cost of ASBR to destination address.

The second category external routing is the received EGP router. This kind of router is less credible, so the cost volume of ASBR to the outside of autonomy system is far more expensive than that of autonomy system to ASBR, so the former is mainly considered, that is, the cost to the second external router = the cost of ASBR to destination address. If the cost is the same, consider the cost of this router to corresponded ASBR.

【Example】

！ Configure OSPF introduce RIP router

Optiway(config-router-ospf)#redistribute rip

9.1.17 distribute-list

Use this command to configure to filtrate receiving or sending route or configure to receive specified neighbor route. Use the no command to delete filtration rule.

distribute-list { **gate-way** *prefix-list-name* **in** | **prefix-list** *prefix-list-name* { **in** | **out** } }

no distribute-list { gate-way in | prefix-list { in | out } }

【Parameter】

gatway:Configure to receive specified neighbor route. The specified neighbor is the address permitted by prefix list.

prefix-list:Configure to filtrate route applied prefix list.

prefix-list-name:the name of prefix list

in:configure route filtration applied to receive route

out:configure route filtration applied to send route

【Command configuration mode】

RIP protocol configuration mode

【Example】

！Configure to filtrate send route applied to prefix list pflst221

Optiway(config-router-rip)#distribute-list prefix-list pflst221 out

9.1.18 show ip rip

Use **show ip rip** command to display RIP statistics, such as received error RIP packet number and error routing number.

show ip rip

【Command configuration mode】

Any configuration mode

【Example】

！Display RIP information in layer 3

Optiway(config)#show ip rip

9.1.19 show ip rip interface

Use **show ip rip interface** command to display RIP information of interface, such as RIP version or authentication.

show ip rip interface [vlan-interface *vlan-id* | supervlan-interface *supervlan-id*]

【Parameter】

vlan-id:the vlan interface numberto be displayed.

supervlan-id:the supervlan interface numberto be displayed

【Command configuration mode】

Any configuration mode

【Example】

！Display RIP configuration of layer 3 interface

Optiway(config-router-rip)#show ip rip interface

！Display RIP configuration of layer 3 interface 1

Optiway(config-router-rip)#show ip rip interface vlan-interface 1

Chapter 10 OSPF Configuration Command

10.1 OSPF configuration command

OSPF configuration command includes:

- **area authentication**
- **area default-cost**
- **area range**
- **area stub**
- **area virtual-link**
- **default-information originate**
- **default redistribute metric**
- **default redistribute type**
- **ip ospf authentication-key**
- **ip ospf cost**
- **ip ospf dead-interval**
- **ip ospf hello-interval**
- **ip ospf message-digest-key**
- **ip ospf network**
- **ip ospf priority**
- **ip ospf retransmit-interval**
- **ip ospf transmit-delay**
- **network area**
- **redistribute**

- **router id**
- **router ospf**
- **show ip ospf**
- **show ip ospf border-routers**
- **show ip ospf cumulative**
- **show ip ospf database**
- **show ip ospf error**
- **show ip ospf interface**
- **show ip ospf neighbor**
- **show ip ospf request-list**
- **show ip ospf retrans-list**
- **show ip ospf virtual-link**
- **show ip route ospf**
- **show router id**

10.1.1 area authentication

Use **area authentication** command to specify a domain in OSPF to support authentication attribution. Use **area authentication** command to cancel it.

area *area-id* **authentication** [message-digest]

no area *area-id* authentication

【Parameter】

area-id:ID in OSPF domain which is in the form of IP address.

message-digest:use MD5 encryption authentication.

【Default】

None authentication.

【Command configuration mode】

OSPF protocol configuration mode

【Usage】

The authentication type of all routers in a domain must be the same(it supports plain text authentication and MD5 encryption authentication or non authentication.) The authentication password of all routers in the same network interface must be the same. Use **ip ospf authentication** command to configure plain text authentication password. If this domain is configured to support MD5 encryption authentication, use **ip ospf message-digest** command to configure it.

【Example】

！Use MD5 authentication in OSPF domain 1

Optiway(config-router-ospf)#area 2.2.2.1 authentication message-digest

10.1.2 area default-cost

Use **area default-cost** command to specify the cost sending to default router in STUB domain. Use **no area default-cost** command to restore it to default value.

area *area-id* default-cost *cost*

no area *area-id* default-cost

【Parameter】

area-id:ID in OSPF domain which is in the form of IP address.

cost:the cost sending to default router in STUB domain which is in the range of 2～16777215

【Default】

The cost sending to default router in STUB domain is 1.

【Command configuration mode】

OSPF protocol configuration mode

【Usage】

This command is for edge router connected to STUB domain. STUB domain configuration command are: **area stub** and **area default-cost**. All routers connected to STUB domain must use **area stub** command to configure to be stub. Command **area default-cost** is for edge router connected to this STUB domain. This command specify the cost sending to default router in STUB domain.

【Example】

！Specify the cost sending to default router in STUB domain 192.168.2.122 to be 12

Optiway(config-router-ospf)#area 192.168.2.122 default-cost 12

10.1.3 area range

Use **area range** command to configure routing convergence in area border router. Use **no area range** command to cancel convergence in area border router.

area *area-id* **range** *address mask* [advertise | notadvertise]

no area area-id **range** address mask

【Parameter】

area-id:ID in OSPF domain which is in the form of IP address.

address:network interface address

mask:net mask

advertise:sent convergent summary LSAs to other domain

notadvertise:not to sent convergent summary LSAs to other domain

【Default】

None configuration of routing convergence.

【Command configuration mode】

OSPF protocol configuration mode

【Usage】

This command is for Area Border Router（ABR）to convergent routing insomearea. ABR only sends a convergent routing to other area. Convergent routing means: when ABR handling routing information, only one routing is sent to other area for each network interface which has configured convergent routing. One area can configure more convergent network interface, so OSPF can convergent many network interface.

【Example】

！Convergent 222.38.162.2/24 and 222.38.182.2/24 to be 222.38.2.2/16

Optiway(config-router-ospf)#network 222.38.162.2 255.255.255.2 area 1.1.1.1

Optiway(config-router-ospf)#network 222.38.182.2 255.255.255.2 area 1.1.1.1

Optiway(config-router-ospf)#area 1.1.1.1 range 222.38.2.2 255.255.2.2

10.1.4 **area nssa**

Use this command to set NSSA area,with command **no to** delete this configuration.

area *area-id* **nssa** [not-summery]

no area *area-id* nssa

【Parameter】

area-id:area identifier,can be as decimal integer or IP address mode

no-summary:forbid ABR to sending NSSA area with Summary LSAs

【Default】

No configure NSSA area

【Command mode】

OSPF protocol configuration mode

【Usage】

Two configuration commands about NSSA area:area nssa and area default-cost,routers which all connect to NSSA area must use **area nssa** to configure this area as NSSA.**area default-cost** is only effective in the area border router and also appoint the default cost of area border router which sends to NSSA area .

To decrease the LSA quantity of sending to NSSA area, it configures in ABR with no-summary attribute, it forbids ABR to sending NSSA area with summary LSAs（LSA type 3）.

【Example】

！ Configuer area 1.1.1.1 to be NSSA area

OptiWay(config-router-ospf)#area 1.1.1.1 nssa

10.1.5 **area stub**

Use **area stub** command to configure one area to be STUB area. Use **no area stub** command too cancel this configuration.

area *area-id* **stub** [not-summery]

no area *area-id* stub

【Parameter】

area-id:ID of area which is in the form of decimal integeral number or IP address.

no-summary:Forbid ABR sending Summary LSAs to STUB area.

【Default】

Do not configure Stub area.

【Command configuration mode】

OSPF protocol configuration mode

【Usage】

There are two configuration command in STUB area: area stub and area default-cost. All routers connected to STUB area must use **area stub** command to configure to be STUB attribution. Command **area default-cost** only be effective in ABR configuration. This command can specify the cost for ABR to send default routing to STUB area.

For reducing the number of Link State Advertisement (LSA) sent to STUB,configure no-summary in ABR to forbid ABR to send summary LSAs （LSA type 3）to STUB area.

【Example】

！ Configure area 1.1.1.1 to be STUB area.

Optiway(config-router-ospf)#area 1.1.1.1 stub

10.1.6 area virtual-link

Use **area virtual-link** command to create and configure a virtual link. Use **no area virtual-link** command to delete a existed virtual link.

area *area-id* virtual-link *router-id* [{ hello-interval *seconds* | retransmit- interval *seconds* | transmit-delay *seconds* | dead-interval *seconds* | { authentication-key *key* | message-digest-key *keyid* md5 *key* } } *]

no area *area-id* virtual-link *router-id*

【Parameter】

area-id:the ID of virtual link transferring area which can be decimal integeral number or in the form of IP address.

router-id:router ID of virtual link neighbor.

hello-interval *seconds*:specified time interval for sending Hello packet in interface which is in the range of 1～8192 seconds. This value must be the same as the **hello-interval** *seconds* established in virtual link router.

retransmit-interval *seconds*:The specified time interval for resending LSA packet in interface which is in the range of 1～8192 seconds.

transmit-delay *seconds*:The specified time interval for delaying sending LSA packet in interface which is in the range of 1～8192 seconds.

dead-interval *seconds*:specified time interval of dead timer which is in the range of 4～32768 seconds. This value must be equal to the value of **dead-interval** *seconds* and at least 4 times of hello-interval *seconds*.

authentication-key *password*:specified interface plain authentication key which is at most 8 characters and the value of it must be the same as virtual

link neighbor authentication key.

message-digest-key *keyed* **md5** *key*:MD5 authentication key and its identifier of specified interface. Keyed is in the range of 1～255 and key is at most character string of 16 characters. They must be the same as the authentication key and its identifier of the virtual link neighbor.

【Default】

area-id has no defaulted value；router-id has no defaulted value；**hello-interval** *seconds* is defaulted to be 12 seconds；**retransmit-interval** *seconds* is defaulted to be 5 seconds；**transmit-delay** *seconds* is defaulted to be 1seconds；**dead-interval** *seconds* is defaulted to be 42 seconds；authentication-key *password* has no defaulted value；message-digest-key *keyid* md5 *key* has no defaulted value

【Command configuration mode】

OSPF protocol configuration mode

【Usage】

In OSPF protocol, all areas must connect with bone area（area 2）. If there cannot be connected with bone area physically in some area, it can establish virtual link logically.

The smaller the hello-interval value is, the fastest the network change will be noticed, but more network resources will be cost.

Don't configure the value of retransmit-interval tooo small, or it may cause the unnecessary retransmission. Change the value bigger when the speed of the network is slow.

Consider the delay of interface sending when configure the value of transmit-delay.

Two authentication way (plain text authentication and MD5 authentication)

are repellent. Specify one of it or none.

【Example】

！Configure a virtual link with the transmission domain to be 1.1.1.1 and the opposite router at to be 12.11.5.2

Optiway(config-router-ospf)#area 1.1.1.1 virtual-link 12.11.5.2

10.1.7 default-information originate

Use **default-information originate** command to introduce default router to OSPF routing domain. Use **redistribute static** command cannot introduce default routing. Use **no default-information originate** command to cancel introduce default routing.

default-information originate [always] [metric *metric-value*] [type

type-value]

no default-information originate

【Parameter】

always:if default routing hasn't configured, this parameter will cause ase LSA to describe default routing and publish it. If there is no keyward, it must configure default routing to introduce ase LSA.

metric-value:metric value of ase LSA which is in the range of 2～16777215.If it is not configured, it is defaulted to be 1.

type-value :metric type of ase LSA which is in the range of 1～2. If it is not configured, it is defaulted to be 2

【Default】

Not to introduce default routing.

【Command configuration mode】

OSPF protocol configuration mode

【Usage】

Use **redistribute static** command cannot introduce default routing. If introducing default routing, use always keyward to produce default ase LSA.

【Example】

！Produce ase Lsa of default routing if there is; don't produce it if there isn't.

Optiway(config-router-ospf)#default-information originate

！Produce ase Lsa of default routing and publish to OSPF routing area.

Optiway(config-router-ospf)#default-information originate always

10.1.8 default redistribute metric

Use **default redistribute metric** command to configure OSPF introducing the default routing metric of external routing. Use **no default redistribute metric** command to restore the default default routing metric value of external routing.

default redistribute metric *metric*

no default redistribute metric

【Parameter】

metric:default routing metric value of external routing introduced by OSPF which is in the range of 2～16777215.

【Default】

It is defaulted to be 1.

【Command configuration mode】

OSPF protocol configuration mode

【Usage】

OSPF can introduce external routing and publish the information to the autonomous system, so it is necessary to introduce default routing metric of external routing.

【Example】

！ Specify the default routing metric of external routing to be 12

Optiway(config-router-ospf)#default redistribute metric 12

10.1.9 default redistribute type

Use **default redistribute type** command to configure the default type of external routing introduced by OSPF. Use **no default redistribute type** command to restore it to be the default value.

default redistribute type { 1 | 2 }

no default redistribute type

【Parameter】

type 1:the first type of external routing

type 2:the second type of external routing

【Default】

The second type of external routing.

【Command configuration mode】

OSPF protocol configuration mode

【Usage】

OSPF can introduce external routing and publish the information to the autonomous system, so it is necessary to introduce default routing type of external routing.

【Example】

！ Specify default routing type of external routing to be the first type.

Optiway(config-router-ospf)#default redistribute type 1

10.1.10 ip ospf authentication-key

Use **ip ospf authentication-key** command to configure the plain text authentication key between neighbor routers. Use **no ip ospf authentication-key** command to delete configured plain text authentication key.

ip ospf authentication-key *password*

no ip ospf authentication-key

【Parameter】

password:the character string with the length less than 8

【Default】

Interface will not authenticate OSPF packet.

【Command configuration mode】

Interface configuration mode

【Usage】

The router authentication key in the same interface must be the same. Only using **area authentication** command to specify the authentication key type being plain text, this configuration can be effective.

【Example】

！Configure the plain text authentication key password to be abc123

Optiway(config-if-vlanInterface-3)#ip ospf authentication-key abc123

10.1.11 ip ospf cost

Use **ip ospf cost** command to configure the cost of interface sending packet. Use **no ip ospf cost** command to restore the default cost.

ip ospf cost *cost*

no ip ospf cost

【Parameter】

cost:cost for operating OSPF protocol which is in the range of 1～65535.

【Default】

It is defaulted to be 1.

【Command configuration mode】

interface configuration mode

【Usage】

Use this command to configure cost of interface manually, or OSPF will calculate the cost of interface according to the bandwidth of current interface.

【Example】

！Configure cost of VLAN interface 3 by operating OSPF to be 12

Optiway(config-if-vlanInterface-3)#ip ospf cost 12

10.1.12 ip ospf dead-interval

Use **ip ospf dead-interval** command to configure the dead interval of OSPF neighbor. Use **no ip ospf dead-interval** command to restore it to the default value.

ip ospf dead-interval *seconds*

no ip ospf dead-interval

【Parameter】

seconds:the dead interval of OSPF neighbor which is in the range of 1～65535 seconds.

【Default】

The dead interval of OSPF neighbor for Point-to-point and broadcast is 42 seconds; The dead interval of OSPF neighbor for point-to-multipoint,non-broadcast is 122seconds.

【Command configuration mode】

Interface configuration mode

【Usage】

The dead interval of OSPF neighbor is: in the time interval, if the Hello packet hasn't received, it is thought the neighbor is ineffective. dead-interval *seconds* must be 4 times of Hello-interval *seconds*, and the **dead-interval** *seconds* must be the same in the same network interface.

【Example】

！Configure the dead interval of interface 3 to be 62seconds

Optiway(config-if-vlanInterface-3)#ip ospf dead-interval 62

10.1.13 ip ospf hello-interval

Use **ip ospf hello-interval** command to configure time interval of sending Hello packet of interface. Use **no ip ospf hello-interval** command to restore it to the default time interval.

ip ospf hello-interval *seconds*

no ip ospf hello-interval

【Parameter】

seconds:The time interval of sending Hello packet of interface which is in the range of 1～255 seconds.

【Default】

The time interval of sending Hello packet of interface for Point-to-point and broadcast is 12 seconds; The time interval of sending Hello packet of interface for point-to-multipoint,non-broadcast is 32seconds.

【Command configuration mode】

Interface configuration mode

【Usage】

The value of **hello-interval** *seconds* will write to Hello packet and send with it.

The smaller the value of **hello-interval** *seconds* is, the faster the change of network topology is found, but it will cost more routing cost. This interface must be the same as neighbor router.

【Example】

！Configure the time interval of sending Hello packet for vlan interface 3 is 15 seconds.

Optiway(config-if-vlanInterface-3)#ip ospf hello-interval 15

10.1.14 ip ospf message-digest-key

Use **ip ospf message-digest-key** command to configure MD5 authentication key between neighbor routers. Use **no ip ospf message-digest-key** command to delete configured MD5 authentication.

ip ospf message-digest-key *key-id* md5 *key*

no ip ospf message-digest-key

【Parameter】

key-id:it is integeral number in the range of 1～255

key:the character string is in the range of 1～16

【Default】

None authentication.

【Command configuration mode】

Interface configuration mode

【Usage】

The authentication key password in the same network interface must be the same. Only after using **area authentication** command to specify the authentication key type is MD5, this configuration can be effective.

【Example】

！Configure MD5 authentication password of vlan interface 3 to be abc123

Optiway(config-if-vlanInterface-3)#ip ospf message-digest-key 12 md5 abc123

10.1.15 ip ospf network

Use **ip ospf network** command to configure network type of OSPF interface. Use **no ip ospf network** command to restore the default network type.

ip ospf network { broadcast | non-broadcast | point-to-multipoint | point-to-point }

no ip ospf network

【Parameter】

broadcast:configure network type of interface to be broadcast.

non-broadcast:configure network type of interface to be NBMA

point-to-multipoint:configure network type of interface to be poit-to- multipoint

point-to-point:configure network type of interface to be poit-to- point

【Default】

Default network type of interface is broadcast.

【Command configuration mode】

Interface configuration mode

【Usage】

It is advised not to modify network type.

【Example】

！Configure Vlan interface 2 to be non-broadcast

Optiway(config-if-vlanInterface-2)#ip ospf network non-broadcast

10.1.16 ip ospf priority

Use **ip ospf priority** command to configure the priority of interface to select “designated router”. Use **no ip ospf priority** command to restore it to the

default value.

ip ospf priority *value*

no ip ospf priority

【Parameter】

value:the priority of interface to select “designated router” is in the range of 2～255

【Default】

The default priority of interface to select “designated router”is 1.

【Command configuration mode】

Interface configuration mode

【Usage】

The priority of router interface determines the competency in selecting“designated router”. The superior priority is firstly considered in conflict. Designated router (DR) is not determined by human, but selected by all routers in the network interface. The router in this network interface whose Priority > 2 can be the candidate. Choose the one with the superior priority to be the so called DR. If the priority is the same, choose the one with larger router ID. The vote is the Hello packet. Each router writes its own DR into Hello and sends it to each router in the network interface. When two of them declairing that they are the DR, choose the one with superior priority. If they have the same priority, choose the one with the larger router ID. The one with the priority being 2, he will not be selected to be DR or BDR.

If DR is failure because of some fault, routers must select DR again at the same time. It costs a long time. During this time, the calculation of router is not correct. In order to shorten it, BDR（Backup Designated Router）is brought up. BDR is a abackup for DR. Select BDR at the same time as DR. It

establishes neighborship and exchange routing information with the routers in the network interface. After the failure of DR, BDR is about to be DR because the neighborship has been established. There will be reselected a new BDR which will not be effected the calculation of router though it needs a long time.

Caution:

DR is not always the router with the superlative priority and BDR is not always the one with the second superlative priority. After selecting DR and BDR, a new router adds, no matter how superlative its priority is, it will not be DR.

DR is the definition in a network interface which is for router interface. A router may be DR in an interface and may be BDR or DRother in another interface.

Selecting DR in broadcast or NBMA interface, it is unnecessary to select DR in poit-to-poit or poit-to-multipoit interface.

【Example】

！Configure priority of VLAN interface 3 to be 122

Optiway(config-if-vlanInterface-3)#ip ospf priority 122

10.1.17 ip ospf retransmit-interval

Use **ip ospf retransmit-interval** command to configure time interval of interface retransmit LSA. Use **no ip ospf retransmit-interval** command to trstore it to the default value.

ip ospf retransmit-interval *seconds*

no ip ospf retransmit-interval

【Parameter】

seconds:time interval of interface retransmit LSA which is in the range of 1～65535s

【Default】

5 seconds

【Command configuration mode】

Interface configuration mode

【Usage】

When a router sending “Link Status Advertisement”（LSA）, it needs to receive the confirm. If the confirm hasn’t received in LSA retransmit interval, this LSA will be retransmit.

Don’t configure the LSA retransmit interval too short, or it will cause unnecessary retransmission.

【Example】

！Configure the retransmit interval of sending LSA between neighbor routers and VLAN interface 3 to be 8 seconds.

Optiway(config-if-vlanInterface-3)#ip ospf retransmit-interval 8

10.1.18 ip ospf transmit-delay

Use **ip ospf transmit-delay** command to configure transmit delay of LSA. Use **no ip ospf transmit-delay** command to restore the default LSA transmit delay.

ip ospf transmit-delay *seconds*

no ip ospf transmit-delay

【Parameter】

seconds:time interval of LSA transmit delay which is in the range of 1～65535 秒

【Default】

1 second

【Command configuration mode】

Interface configuration mode

【Usage】

LSA will be aging (1 more minute per second) with time in Link Status DateBase(LSDB) of this router but it will not be aging in network transmission, so it is necessary to add the configured time before sending LSA. This configuration is very important in network with low speed.

【Example】

！Configure LSA delay interval of VLAN interface 3 to be 3 seconds.

Optiway(config-if-vlanInterface-3)#ip ospf transmit-delay 3

10.1.19 **network area**

Use **network area** command to specify the area where interface locates.

network ip-address wildcard-mask **area** area-id

no network ip-address wildcard-mask **area** area-id

【Parameter】

ip-address:network interface adress where interface locates.

wildcard-mask:IP address mask or IP address wildcard shield (it is in the form of NOT calculation of IP address mask in which “1”means ignoring the bit corresponded in IP address and “2”means this bit must be reserved).

area-id: the area ID number this address belonged to. In order for the normal working OSPF, area ID number of all router interface in the same specified

area must be matching. The way of identifying is: in the form of IP address or integer number.

【Default】

Interface doesn't belong to any area.

【Command configuration mode】

OSPF protocol configuration mode

【Usage】

Use keywork ip-address and wildcard-mask can configure an interface to be some area. For running OSPF protocol in an interface, the primary IP address must locate in the specified network range. If the second IP address locates in specified network interface, OSPF protocol will not run.

【Example】

！Specify OSPF run in interface with primary IP address to be 192.168.2.122, mask to be 255.255.255.2 and OSPF area number to be 1.1.1.1

Optiway(config-router-ospf)#network 192.168.2.122 255.255.255.2 area 1.1.1.1

10.1.20 redistribute

Use **redistribute** command to introduce external static routing or routing information found by other routing protocol. Use **no redistribute** command to cancel the introduction.

redistribute *protocol* [**metric** *metric*] [**type** { 1 | 2 }] [**tag** *tag-value*][**prefix-list** *prefix-list-name*]

no redistribute [*protocol*]

【Parameter】

protocol:introduced source routing protocol which can be connected, rip and static.

【Default】

None introduction.

【Command configuration mode】

OSPF protocol configuration mode

【Usage】

Each dynamic routing protocol can share routing information. Because of OSPF, router found by other routing protocol always be handled as external routing information of autonomy.

OSPF uses following 4 kinds of different router which as priority order are:

- Inter Area Routing
- Area Border Routing
- The first category external routing
- The second category external routing

The description of routing in or between areais for network structurein Autonomy system. External routingdescribes how to choose destination routing out of Autonomy system.

The first category external routing is received IGP router (such as: RIP and STATIC). This kind of router is more credible, so the cost volume of external router and autonomy system is the same and can compare with the router of OSPF itself, that is, the cost to external router= the cost to its ASBR +the cost of ASBR to destination address.

The second category external routing is the received EGP router. This kind of router is less credible, so the cost volume of ASBR to the outside of autonomy

system is far more expensive than that of autonomy system to ASBR, so the former is mainly considered, that is, the cost to the second external router = the cost of ASBR to destination address. If the cost is the same, consider the cost of this router to corresponded ASBR.

【Example】

！Configure OSPF introduce RIP router

Optiway(config-router-ospf)#redistribute rip

10.1.21 ip ospf distribute-list

Under specific layer 3 iterface, configure strategy rules on ingress and egress route by specifying OSPF address prefix list to filtrate route on OSPF learning. In addition, it also can specify neighbor Ethernet switch to learn specific OSPF route of Ethernet switch. Use no command to delete configured prefix list.

ip ospf distribute-list { gate-way *prefix-list-name* in | prefix-list *prefix-list-name* { in | out } }

no ip ospf distribute-list { gate-way in | prefix-list { in | out } }

【Parameter】

gatway:Configure to receive route from specific neighbor. Specific neighbor is the permit address in prefix list

prefix-list:Configure filtration to route prefix-list

prefix-list-name:define prefix-list name （string）

in:Configure route filtration in receiving route

out:Configure route filtration in sending route

【Default】

By default, this function is disabled.

【Command configuration mode】

interface configuration mode

【Example】

！Configure ip ospf distribute-list prefix-list check in vlan interface2

Optiway(config-if-vlanInterface-2)#ip ospf distribute-list prefix-list check in

10.1.22 ip ospf bfd

Use this command to enable OSPF to use BFD to monitor link status. use **no** command to disable OSPF to use BFD to monitor link status.

ip ospf bfd

no ip ospf bfd

【Default】

By default, it is disabled.

【Command configuration mode】

Interface configuration mode

【Usage】

The switches on both sides of the monitor link enable this funtion, it can be enabled. Enable BFD to improve OSPF to detect link failure and break up neighbourhood and update routing speed.

【Example】

！Enable OSPF to use BFD on VLAN interface 2

Optiway(config-if-vlanInterface-2)#ip ospf bfd

10.1.23 router id

Use **router id** command to configure the router ID when running OSPF. Use **no router id** command to cancel configured router ID.

router id router-id

no router id

【Parameter】

router-id:integeral number without symbols which is the unique identifier in autonomy system.

【Default】

Choose the one with smaller IP address to be router ID from interface.

【Command configuration mode】

Global configuration mode

【Usage】

When configuring router ID, the router ID of any two routers in autonomy are not the same. Generally, configure router ID to be the same as that of the IP address in some interface of the router. To make sure of the stability operation of OSPF, be sure the division of router ID and manually configure it.

【Example】

！Configure router ID to be 192.168.2.122

Optiway(config)#router id 192.168.2.122

10.1.24 **router ospf**

Use **router ospf** command to enable OSPF protocol. Use **no router ospf** command to disable OSPF protocol.

router ospf

no router ospf

【Default】

OSPF disables.

【Command configuration mode】

Global configuration mode

【Example】

！ Enable OSPF

Optiway(config)#router ospf

！ Disable OSPF

Optiway(config)#no router ospf

10.1.25 **show ip ospf**

Use **show ip ospf** command to display OSPF information.

show ip ospf [*area-id*]

【Parameter】

area-id:ID in OSPF domain which is in the form of IP address or integeral number.

【Command configuration mode】

Any configuration mode

【Usage】

Diagnose OSPF failure according to the command output.

【Example】

！ Display OSPF information

Optiway(config)#show ip ospf

10.1.26 **show ip ospf border-routers**

Use **show ip ospf border-routers** command to display OSPF edge router information.

show ip ospf border-routers

【Command configuration mode】

Any configuration mode

【Usage】

Diagnose OSPF failure according to the command output.

【Example】

！ Display OSPF edge router information.

Optiway(config)#show ip ospf border-routers

10.1.27 **show ip ospf cumulative**

Use **show ip ospf cumulative** command to display OSPF statistic information.

show ip ospf cumulative

【Command configuration mode】

Any configuration mode

【Usage】

Diagnose OSPF failure according to the command output.

【Example】

Optiway(config-if-vlanInterface-2)#show ip ospf cumulative

10.1.28 show ip ospf database

Use **show ip ospf database** command to display LSDB information of OSPF.

show ip ospf database

【Command configuration mode】

Any configuration mode

【Usage】

Diagnose OSPF failure according to the command output.

【Example】

！Display LSDB information of OSPF

Optiway(config)#show ip ospf database

10.1.29 show ip ospf error

Use **show ip ospf error** command to display OSPF error information.

show ip ospf error

【Command configuration mode】

Any configuration mode

【Usage】

Diagnose OSPF failure according to the command output.

【Example】

！ Display OSPF error information.

Optiway(config-if-vlanInterface-2)#show ip ospf error

10.1.30 **show ip ospf interface**

Use **show ip ospf interface** command to display OSPF interface information.

show ip ospf interface [interface-type interface-num]

【Parameter】

interface-type:interface type which is VLAN or superVLAN type.
interface-number:interface number. VLAN interface number is in the range of 1～4294 and superVLAN interface is in the range of 1～11.

【Command configuration mode】

Any configuration mode

【Usage】

Diagnose OSPF failure according to the command output.

【Example】

！ Display OSPF interface information

Optiway(config)#show ip ospf interface

10.1.31 **show ip ospf neighbor**

Use **show ip ospf neighbor** command to display all neighbor information of OSPF.

show ip ospf neighbor

【Command configuration mode】

Any configuration mode

【Usage】

Diagnose OSPF failure according to the command output.

【Example】

！Display all neighbor information of OSPF.

Optiway(config)#show ip ospf neighbor

10.1.32 **show ip ospf request-list**

Use **show ip ospf request-list** command to display OSPF request list.

show ip ospf request-list

【Command configuration mode】

Any configuration mode

【Usage】

Diagnose OSPF failure according to the command output.

【Example】

！Display OSPF request list.

Optiway(config)#show ip ospf request-list

10.1.33 **show ip ospf retrans-list**

Use **show ip ospf retrans-list** command to display OSPF retransmit list.

show ip ospf retrans-list

【Command configuration mode】

Any configuration mode

【Usage】

Diagnose OSPF failure according to the command output.

【Example】

！Display OSPF retransmit list.

Optiway(config)#show ip ospf retrans-list

10.1.34 show ip ospf virtual-link

Use **show ip ospf virtual-link** command to display OSPF virtual link information.

show ip ospf virtual-link

【Command configuration mode】

Any configuration mode

【Usage】

Diagnose OSPF failure according to the command output.

【Example】

！Display OSPF virtual link information.

Optiway(config)#show ip ospf virtual-link

show ospf virtual link information

area 1.1.1.1 neighbor 193.1.1.2

state Point To Point event 1

auth type Simple auth key abc123

Timer interval HInterval 12 DInterval 42 TrDelay 1 RtInterval 5

Total entries: 1 ospf virtual link

10.1.35 show ip route ospf

Use **show ip route ospf** command to display routing information learnt by OSPF.

show ip route ospf

【Command configuration mode】

Any configuration mode

【Usage】

Diagnose OSPF failure according to the command output.

【Example】

！Display routing table information.

Optiway(config)#show ip route ospf

10.1.36 show router id

Use **show router id** command to display configured router ID.

show router id

【Command configuration mode】

Any configuration mode

【Usage】

Diagnose OSPF failure according to the command output.

【Example】

！ Display configured router ID.

Optiway(config)#show router id

current router id :192.168.2.122

10.1.37 **show ip ospf distribute-list**

Use **show ip ospf distribute-list** command to display configured prefix list.

show ip ospf distribute-list

【Command configuration mode】

Any configuration mode

【Usage】

Diagnose OSPF failure according to the command output.

【Example】

！ Display configured prefix list

Optiway(config)#show ip ospf distribute-list

Chapter 11 BGP Configuration Command

11.1 BGP Configuration Command

BGP Configuration Command includes:

- **aggregate-address**
- **bgp always-compare-med**
- **bgp default local-preference**
- **bgp router-id**
- **default-metric**
- **ip as-path access-list**
- **ip distribute-list**
- **neighbor advertisement-interval**
- **neighbor distribute-list**
- **neighbor ebgp-multihop**
- **neighbor filter-list**
- **neighbor next-hop-self**
- **neighbor remote-as**
- **neighbor timers**
- **network**
- **redistribute**
- **router bgp**
- **show ip as-path access-list**
- **show ip bgp**

- **show ip bgp neighbors**
- **show ip bgp summary**
- **show ip distribute-list**
- **timers bgp**

11.1.1 aggregate-address

Use this command to create a convergent route in BGP table. Use the no command to delete a convergent route.

aggregate-address { *address mask* | *A.B.C.D/M* } [**summary-only**]

no aggregate-address { *address mask* | *A.B.C.D/M* } [**summary-only**]

【Parameter】

address:IP address of convergent route;

mask:netmask of convergent route;

A.B.C.D/M:convergent route address and length of netmask;

summary-only:only summary convergent route.

【Default】

Not to configure any convergent route.

【Command configuration mode】

BGP configuration mode

【Usage】

Use this command to realize BGP route convergency and reduce memory cost of BGP table.

If there is concrete route in specified range available in BGP table, use

aggregate-address command without parameter to create specified convergent route in BGP table and inform it to BGP neighbor without suppressing the notification of the covered concrete route. Generated convergent route is local convergent and is configured atomic-aggregateion which means it may lose information in convergency.

Supress all notification of the covered concrete route when generating and informing convergent route by using keyword “summary-only”.

Use neighbor distribute-list command to suppress some concrete route.

【Example】

Optiway(config-router-bgp)# aggregate-address 192.168.2.2 255.255.2.2

11.1.2 bgp always-compare-med

Use this command to compare MED from different AS route path. Use the no command to deny comparison.

bgp always-compare-med

no bgp always-compare-med

【Default】

Only compare MED from the same AS route path.

【Command configuration mode】

BGP configuration mode

【Usage】

MED is used for choosing the best path. The smaller MED value will be chosen.

It is recommended to use this command when the IGP and route choosing

method are the same in the corresponded AS.

【Example】

Optiway(config-router-bgp)# bgp always-compare-med

11.1.3 bgp default local-preference

Use this command to configure local preference. Use the no command to restore to default loacal preference.

bgp default local-preference *localprefvalue*

no bgp default local-preference

【Parameter】

localprefvalue:configured default local preference whish is in the range of 2 - 4294967295.

【Default】

The default local preference is 122.

【Command configuration mode】

BGP configuration mode

【Usage】

Configuring different local preference can influence the route choosing of BGP.

The larger the local preference value is, the more chance for coorsponded route to be chosen.

【Example】

Optiway(config-router-bgp)# bgp default local-preference 222

11.1.4 bgp router-id

Use this command to configure BGP route id.

bgp router-id *ip-address*

no bgp router-id

【Parameter】

ip-address:BGP router id of IP address which is in the form of dotted decimal.

【Default】

By default, BGP can choose an interface address from current available interfacesto be BGP route id.

【Command configuration mode】

BGP configuration mode

【Usage】

By default, BGP will use dynamic router id which will influence BGP running. Using this command to specify BGP route id can guarantee the unchangement of router id. The configured router id is unique in the network.

【Example】

Optiway(config-router-bgp)# bgp router-id 192.168.3.4

11.1.5 default-metric

Use this command to configure system metric value. Use no command to restore to default metric value.

default-metric *metric*

no default-metric

【Parameter】

metric:Specific metric value which is in the range of 1 to 4294967295.

【Default】

Default metric value is 2.

【Command configuration mode】

BGP configuration mode

【Usage】

Multi-exit discriminate is the external metric of route which is different from local preference. MED exchanges between AS, but the EMD entered AS will not leave it. MED is used for choosing the best route and the smaller one will be chosen. When a router running BGP which gains the route with the same destination address and different next hop through different External Peer, it will preferentially make a decision according to MED value of different route. The route will smaller MED will be chosen the external route of AS with the same condition.

【Example】

Optiway(config-router-bgp)# default-metric 12

11.1.6 ip as-path access-list

Use this command to configure the list that BGP AS path matches. Use the no command to delete it.

ip as-path access-list *aspath-list-number* { **permit** | **deny** } *as-regular-expression*

no ip as-path access-list *aspath-list-number* { **permit** | **deny** } *as-regular-expression*

【Parameter】

aspath-list-number:AS path list id which is in the range of 1～199;

as-regular-expression:used for matching regular expression of AS path

【Default】

None control list is configured.

【Command configuration mode】

Global configuration mode

【Usage】

AS path matching is completed by AS path regular expression which matches AS-PATH in BGP route as ASCII string and determines to accept or deny route by deny or permit command for successfully matched AS path. After defining BGP route distribute list, it can realize BGP strategy function by applying neighbor filter-list command.

For the same list number, user can define multiple distribute list, that is, one distribute list number represents a group of distribute list. Each AS path list uses numbers to be their id.

If ip as-path access-list command is configured, there must be at least one command with ip as-path access-list permit for the items with the same list number, or all route will be filtered when using neighbor filter-list command.

In the process of matching, the relationship between *aspath-list-number* is ”or”,that is, route information matching one item of this list group means it matches the filtration of the distribute list of the as-path list id.

Special symbol and its meanings in regular expression are in the following:

Symbol	Description
.	Any single character, including space.
*	Leader character never appears or continuely appears many times in target object.
-（hyphen）	Any character in the range formed by the characters before or behind hyphen.
_（underline）	Match comma, {, }, (,), the beginning of the string, the end of the string or a space
[ ]	Any character in square brackets.
[^]	Any character except listing in square brackets.(^ is in the front of the character)
|	Alternation, matches either left side or right side
^	Match the beginning of the string
$	Match the end of the string

【Example】

Optiway(config)# ip as-path access-list 12 deny ^722$

Optiway(config)# ip as-path access-list 12 permit .*

【Related Command】

neighbor filter-list,show ip as-path access-list

11.1.7 ip distribute-list

Use this command to configure BGP route filter list. Use the no command to delete it.

ip distribute-list *list-number* { **permit** | **deny** } *net-addr wildcard-netmask*

no ip distribute-list *list-number* { **permit** | **deny** } *net-addr wildcard-netmask*

【Parameter】

list-number:BGP route filter list id which is in the range of 1～199;

net-addr:network address;

wildcard-netmask:wildcard netmask address

【Default】

None distribute list is configured.

【Command configuration mode】

Global configuration mode

【Usage】

BGP route matching is completed by *net-addr* and *wildcard-netmask*. For those successfully matched, determine to accept route or not through deny or permit command. After defining BGP route distribute list, it can realize BGP strategy function by applying neighbor distribute-list command.

For the same list number, user can define multiple distribute list, that is, one distribute list number represents a group of distribute list. Each AS path list uses numbers to be their id.

If ip distribute-list command is configured, there must be at least one command with ip distribute-list permit for the items with the same list number, or all route will be filtered when using neighbor distribute-list command.

In the process of matching, the relationship between distribute list number is ”or”,that is, route information matching one item of this list group means it matches the filtration of the distribute list of the distribute list id.

【Example】

Optiway(config)# ip distribute-list 3 deny 192.168.9.2 2.2.2.255

Optiway(config)# ip distribute-list 3 permit 2.2.2.2 255.255.255.255

【Related Command】

neighbor filter-list,show ip as-path access-list

11.1.8 neighbor advertisement-interval

Use this command to configure neighbor's advertisement interval. Use the no command to restore the default value.

neighbor *ip-address* advertisement-interval *seconds*

no neighbor *ip-address* advertisement-interval

【Parameter】

ip-address:configured neighbor's IP address.

seconds:the minimum interval for sending Update advertisement which is in the range of 1～65535 seconds.

【Default】

By default, IBGP neighbor is 15 seconds and EBGP neighbor is 32 seconds.

【Command configuration mode】

BGP configuration mode

【Example】

Optiway(config-router-bgp)# neighbor 192.168.3.3 advertisement-interval 12

11.1.9 neighbor distribute-list

Use this command to apply distribute list to specified neighbor. Use the no command to cancel it.

neighbor *ip-address* **distribute-list** *list-number* { **in** | **out** }

no neighbor *ip-address* **distribute-list** *list-number* { **in** | **out** }

【Parameter】

ip-address:configured neighbor's IP address.

list-number:IP accessing control list nukber which is in the range of 1～199.

in:ingress filter

out:Egress filter

【Default】

Neighbors will not apply any filter list.

【Command configuration mode】

BGP configuration mode

【Usage】

Use this command to complete BGP route strategy for filtration of BGP sending and receiving route. Using this commanf together with **ip distribute-list** to apply distribute list to specific neighbor. Distribute list can only match IP address, therefore, this command can only filtrate AS number in path of sending and receiving route.

【Example】

Optiway(config-router-bgp)# neighbor 192.168.3.3 distribute-list 3 in

【Related Command】

ip distribute-list,neighbor filter-list

11.1.10 neighbor ebgp-multihop

Use this command to permit establishing connection with EBGP neighbor not

directly connected to network. Use the no command to cancel the configuration.

neighbor *ip-address* ebgp-multihop

no neighbor *ip-address* ebgp-multihop

【Parameter】

ip-address:configured neighbor's IP address.

【Default】

By default, only directly connected neighbors can establish connection for EBGP.

【Command configuration mode】

BGP configuration mode

【Usage】

Usually, EBGP neighbors are directly connected. It can use this command to make them not connect directly when necessary.

【Example】

Optiway(config-router-bgp)# neighbor 192.168.3.7 ebgp-multihop

11.1.11 neighbor filter-list

Use this command to apply filter list to specified neighbor. Use no command to cancel it.

neighbor *ip-address* **filter-list** *aspath-list-number* { **in** | **out** }

no neighbor *ip-address* **filter-list** *aspath-list-number* { **in** | **out** }

【Parameter】

ip-address:configured neighbor's IP address

aspath-list-number:AS regular expression filter list number which is in the range of 1～199.

in:ingress filter

out:Egress filter

【Default】

By default, neighbor will not apply any filter list.

【Command configuration mode】

BGP configuration mode

【Usage】

Use this command to complete BGP route strategy for filtration of BGP sending and receiving route. Using this commanf together with **ip as-path access-list** to apply filter list to specific neighbor. Filer list can only match AS-PATH, therefore, this command can only filtrate AS number in path of sending and receiving route.

【Example】

Optiway(config-router-bgp)# neighbor 192.168.3.3 filter-list 3 out

【Related Command】

ip as-path access-list,neighbor distribute-list

11.1.12 neighbor next-hop-self

Use this command to cancel the calculation of the next-hop in route distributed to neighbors and make the self-address next hop. Use the no command to cancel the configuration.

neighbor *ip-address* next-hop-self

no neighbor *ip-address* next-hop-self

【Parameter】

ip-address:configured neighbor's IP address

【Default】

Disable

【Command configuration mode】

BGP configuration mode

【Usage】

In non-full connect network, router in the same network interface may not connect directly. Use this command to configure the next hop of BGP route to be local interface address.

【Example】

Optiway(config-router-bgp)# neighbor 192.168.3.3 next-hop-self

11.1.13 neighbor remote-as

Use this command to create BGP neighbor. Use no command to remove it.

neighbor *ip-address* **remote-as** *as-number*

no neighbor *ip-address* **remote-as** *as-number*

【Parameter】

ip-address:IP address of neighbors.

as-number:AS number of the AS which neighbor is in.

【Default】

Not any neighbor is configured.

【Command configuration mode】

BGP configuration mode

【Usage】

This command is necessary for running BGP for creating BGP neighbors. If as-number value and local AS number specified in **router bgp** command are the same, IBGP neighbor is established, or is EBGP neighbor.

【Example】

! Establish neighbor 192.168.3.7 to be EBGP neighbor

Optiway(config-router-bgp)# router bgp 422

Optiway(config-router-bgp)# neighbor 192.168.3.7 remote-as 722

11.1.14 neighbor timers

Use this command to configure Keepalive packet sending-interval with specific neighbors and holdtime. Use no command to restore default value.

neighbor ip-address **timers** keepalive-interval holdtime

no neighbor *ip-addres* timers

【Parameter】

ip-address:configured neighbor IP address;

keepalive-interval:Keepalive interval which is in the range of 2～21845;

holdtime:holdtime which is in the range of 2～65535.

【Default】

The default keepalive is 32 seconds and holdtime is 182 seconds.

【Command configuration mode】

BGP configuration mode

【Usage】

The priority of the timer configured by this command is superior than that configured by **timers bgp** command.

【Example】

Optiway(config-router-bgp)# neighbor 192.168.3.3 timers 62 182

11.1.15 network

Use this command to configure network route announced by local BGP. Use no command to cancel the announced network route.

network { ip-address [**mask** address-mask] | A.B.C.D/M }

no network { ip-address [**mask** address-mask] | A.B.C.D/M }

【Parameter】

ip-address:ip address announced by BGP.

address-mask:mask of network address.

A.B.C.D/M:network address and mask length announced by BGP

【Default】

Not announce any route.

【Command configuration mode】

BGP configuration mode

【Usage】

Only completely matched route can use network announcememt, that is, the route whose prefix and mask completely matches will be published to neighbors. If the mask is not specified, it should be accurately matched according to natural network interface.

【Example】

Optiway(config-router-bgp)# network 12.1.2.2 mask 255.255.2.2

11.1.16 redistribute

Use this command to introduce route information of other protocol to BGP. Use the no command to cancel introducing route information of other protocol.

redistribute { connected | static | rip | ospf } [metric *metric*]

no redistribute { connected | static | rip | ospf }

【Parameter】

connected:introduce connected route;

static:introduce static route;

rip:introduce RIP route;

ospf:introduce OSPF route;

metric: metric value.

【Default】

Not introduce route information of other protocol to BGP

【Command configuration mode】

BGP configuration mode

【Usage】

A route protocol can introduce (or learn) route information collected by other route protocol.

【Example】

Optiway(config-router-bgp)# redistribute ospf

11.1.17 router bgp

Use this command to enable BGP and enter BGP configuration mode. Use no command to disable BGP.

router bgp *as-number*

no router bgp *as-number*

【Parameter】

as-number:specified local AS number.

【Default】

BGP disables.

【Command configuration mode】

Global configuration mode

【Usage】

Use this command to enable and disable BGP and specify local AS number.

【Example】

Optiway(config)# router bgp 422

11.1.18 show ip as-path access-list

Use this command to show AS path information.

show ip as-path access-list [*aspath-list-number*]

【Parameter】

aspath-list-number:AS path list number which is in the range of 1～199.

【Command configuration mode】

Any configuration mode

【Usage】

Use this command to show AS path information.

【Example】

Optiway# show ip as-path 4

ip as path access list 4, 1 rule:

2 permit ^422$

11.1.19 **show ip bgp**

Use this command to show route information in BGP table.

show ip bgp [*A.B.C.D* | *A.B.C.D/M* [**longer-prefix**]]

【Parameter】

A.B.C.D:the network interface to be displayed；

A.B.C.D/M:the network interface and mask length to be displayed；

longer-prefix:show matched route whose mask is the same or longer than the specific one.

【Command configuration mode】

Any configuration mode

【Usage】

Show route information in BGP table. It is used to show the learnt route of BGP and also show part of it by using keywords.

【Example】

Optiway# show ip bgp

New GreenNet BGP Module Version 2.5.2

Autonomous System number 422, local router ID 192.168.3.3 Status codes: s suppressed, * valid, > best, i internal

Origin codes: i - IGP, e - EGP, ? – incomplete

	Network	NextHop	Metric	LocalPref	Path
*>	192.168.5.2/24	2.2.2.2		122	i

11.1.20 **show ip bgp neighbors**

Use this command to show neighbors.

show ip bgp neighbors [*neighbor-address*]

【Parameter】

neighbor-address:IP address of neighbors.

【Command configuration mode】

Any configuration mode

【Usage】

Use this command to show neighbor information which displays detail information and **show ip bgp neighbors summary** command displays

summary information.

【Example】

Optiway# show ip bgp neighbors

BGP Neighbor 192.168.3.3 Status ENABLED remote AS 422, internal link

Local host 192.168.3.4 Mask 255.255.255.2 AS 422

Configured Timers: Hold 32 Keepalive 182 Connect Retry 32

Update 32 Update For IntraAS Route 15

Param: Local Preference 122 OutBound Metric 2

Route Reflector Client is DISABLED

BGP State = Established Socket State = ESTAB Remote Initialized

Remote Router ID = 192.168.3.3 Connection Up Times 2

Running Timers: Hold 182 Keepalive 32 Connect Retry DISABLED

Update 32 Update For IntraAS Route 15

11.1.21 **show ip bgp summary**

Use this command to show all BGP summary.

show ip bgp summary

【Command configuration mode】

Any configuration mode

【Usage】

Use this command to show all BGP summary.

【Example】

Optiway# show ip bgp summary

Neighbor	V	AS	MsgRcvd	MsgSent	Up/Down	State/PfxRcd
192.168.3.3	4	422	1	2	24:41:13	Established
192.168.3.7	4	722	2	2	22:44:15	Established
192.168.3.8	4	422	4	1	26:27:29	Established

11.1.22 **show ip distribute-list**

Use this command to show distribute list.

show ip distribute-list [*list-number*]

【Parameter】

list-number:distribute list number which is in he range of 1 to 199.

【Command configuration mode】

Any configuration mode

【Usage】

Use this command to show distribute list.

【Example】

Optiway# show ip distribute-list 3

ip distribute-list 3, 2 rule:

2 deny 192.168.9.2 2.2.2.255

1 permit 2.2.2.2 255.255.255.255

11.1.23 timers bgp

Use this command to configure global Keepalive of BGP and Holdtime timer. Use no command to restore default Keepalive and Holdtime timer.

timers bgp keepalive-interval holdtime

no timers bgp

【Parameter】

keepalive-interval:the time interval of sending Keepalive notification which is in the range of 2 to 21845.

holdtime:BGP hold time which is in the range of 2 to 65535.

【Default】

The default value of keepalive-interval and holdtime are 32 and 182 seconds.

【Command configuration mode】

BGP configuration mode

【Usage】

Configure BGP global timer parameter.

【Example】

Optiway(config-router-bgp)# timers bgp 32 182

Chapter 12 Multicast Protocol Configuration Command

12.1 Static Multicast Configuration Command

Static multicast configuration command includes:

- **multicast mac-address**
- **multicast mac-address vlan interface**
- **show multicast**

12.1.1 multicast mac-address

Use **multicast mac-address** command to create a multicast group. Use **no multicast mac-address** command to remove multicast group formed by specified mac address and related vlan-id.

multicast mac-address *mac* vlan *vlan-id*

no multicast [mac-address *mac* vlan *vlan-id*]

【Parameter】

mac:The mac address of multicast group displayed in the form of multicast address, such as: 21:22:5e:**:**:**

vlan-id:Range from 1 to 4294

【Command configuration mode】

Global configuration mode

【Usage】

To create multicast group, MAC address should be multicast group address, and vlan-id must be existed. If there is no parameter in any multicast mac-address command, all multicast group are removed.

【Example】

！Create a multicast group

Optiway(config)#multicast mac-address 21:22:5e:21:22:23 vlan 1

12.1.2 multicast mac-address vlan interface

Use **multicast mac-address vlan interface** command to add interface to existed multicast group. Use no multicast mac-address vlan interface command to remove interface.

multicast mac-address *mac* **vlan** *vlan-id* **interface** { all | *interface-list* }

no multicast mac-address *mac* **vlan** *vlan-id* **interface** { all | *interface-list* }

【Parameter】

mac:Means mac address of existed multicast which is in the form of multicast mac-address, such as: 21:22:5e:**:**:**

vlan-id:Range from 1 to 4294. Multicast group is assembled by vlan-id and mac-address.

interface-list:List of Ethernet ports to be added to or removed from a VLAN. This keyword needed to be provided in the form of interface-type + interface-number. Interface-type is Ethernet and interface-number is slot-num/port-num, in which slot-num is in the range of 2 to 2, and port-num is in the range of 1 to 24. Seriate interfaces with the same type can be linked by to keyword, but the port number to the right of the to keyword must be larger than the one to the left of the keyword, and this argument only can be repeated for up to 3 times.

all:means all interfaces in system in multicast mac-address vlan interface command, and means all the interfaces of the multicast group in the no multicast mac-address vlan interface command.

【Command configuration mode】

Global configuration mode

【Example】

！Remove ethernet 2/2 from existed multicast group.

Optiway(config)#no multicast mac-address 21:22:5e:21:22:23 vlan 1 interface ethernet 2/2

12.1.3 show multicast

Use **show multicast** command to display the information of the specified or all existed multicast group.

show multicast [mac-address *mac*]

【Parameter】

mac:MAC address existed in multicast group

【Command configuration mode】

Any configuration mode

【Usage】

If mac-address is not specified, information of the entire multicast group is displayed.

【Example】

！Display the information of multicast group with the MAC address to be 21:22:5e:21:22:23

Optiway(config)#show multicast mac-address 21:22:5e:21:22:23

12.2 IGMP snooping and GMRP Configuration Command

IGMP snooping and GMRP configuration command includes:

- **gmrp**
- **igmp-snooping**
- **igmp-snooping host-aging-time**
- **igmp-snooping max-response-time**
- **igmp-snooping fast-leave**
- **igmp-snooping group-limit**
- **igmp-snooping permit/deny group**
- **igmp-snooping route-port forward**
- **igmp-snooping multicast vlan**
- **show gmrp**
- **show gmrp interface**
- **show igmp-snooping**

12.2.1 gmrp

Use **gmrp** command to enable GMRP globally or for a port. Use **no GMRP** command to disable GMRP globally or for a port.

gmrp

no gmrp

【Default】

GMRP disables globally

【Command configuration mode】

Global configuration mode,Interface configuration mode

【Usage】

GMRP for a port must be enabling in trunk mode

【Example】

！ Enable GMRP globally

Optiway(config)#gmrp

！ Disable the GMRP of Ethernet 2/3

Optiway(config-if-ethernet-2/3)#no gmrp

12.2.2 igmp-snooping

Use **igmp-snooping** command to enable IGMP snooping. Use **no IGMP-snooping** command to disable IGMP snooping.

igmp-snooping

no igmp-snooping

【Default】

IGMP snooping disable

【Command configuration mode】

Global configuration mode

【Example】

！ Enable IGMP snooping

Optiway (config)#igmp-snooping

12.2.3 igmp-snooping host-aging-time

Use **igmp-snooping host-aging-time** command to configure the host-aging-time of dynamic multicast group learnt by igmp-snooping. Use **no igmp-snooping host-aging-time** command to restore the default host-aging-time.

igmp-snooping host-aging-time *seconds*

no igmp-snooping host-aging-time

【Command configuration mode】

Global configuration mode

【Parameter】

seconds:range from 12 to 1222222 seconds

【Example】

！Configure host-aging-time of the dynamic multicast group learnt by igmp-snooping to be 12 seconds

Optiway(config)#igmp-snooping host-aging-time 12

12.2.4 igmp-snooping max-response-time

When receiving a leave message, igmp-snooping will wait for some time to see whether to remove interface of igmp-snooping multicast group. The time is the response time.

igmp-snooping max-reponse-time *seconds*

no igmp-snooping max-reponse-time

【Command configuration mode】

Global configuration mode

【Parameter】

seconds:Range from 1 to 122 seconds. The default time is 12 seconds

【Usage】

This command is effective when fast leave disables

【Example】

！Configure the max-response-time of igmp-snooping is 99 seconds

Optiway(config)#igmp-snooping max-response-time 99

12.2.5 igmp-snooping fast-leave

Use **igmp-snooping fast-leave** command to configure fast-leave of the interface. When fast-leave enables, if the fast-leave message is received, the interface leaves the aging group, or the time to leave is determined by the max-response-time.

igmp-snooping fast-leave

no igmp-snooping fast-leave

【Command configuration mode】

Interface configuration mode

【Default】

Fast-leave disables

【Example】

！Enable igmp-snooping fast-leave

Optiway(config-if-ethernet-2/1)#igmp-snooping fast-leave

12.2.6 igmp-snooping group-limit

Use **igmp-snooping group-limit** command to configure the number of the

multicast group allowed learning.

igmp-snooping group-limit *limit*

no igmp-snooping group-limit

【Command configuration mode】

Interface configuration mode

【Parameter】

limit:Range from 2 to 128. The default number is 128

【Example】

！Configure the igmp-snooping group-limit to be 99

Optiway(config-if-ethernet-2/1)#igmp-snooping group-limit 99

12.2.7 igmp-snooping permit/deny group

Use **igmp-snooping permit/deny group** command to configure the permit and deny group, and the learning regulations of the group which is not permit or deny group (We call it default group).

igmp-snooping permit/deny group [all | *group-address*]

no igmp-snooping permit/deny group [*group-address*]

【Command configuration mode】

Interface configuration mode for permit/deny group

Global configuration mode for the learning regulations of default group

【Parameter】

group-address:Multicast MAC address is in the form of 21:22:5e:21:22:23

【Example】

！Configure the learning regulation of default group to allow all multicast group

Optiway(config)#igmp-snooping permit group all

！ Configure Ethernet 2/3 not to learn multicast 21:22:5e:22:21:21

Optiway(config-if-ethernet-2/3)#igmp-snooping deny group 21:22:5e:22:21:21

12.2.8 igmp-snooping route-port forward

Multicast routers interface is the interface received IGMP inquiring message (It is also called mix router interface.).

Use **igmp-snooping route-port forward** command to configure whether to add router interface to IGMP snooping learning group.

igmp-snooping route-port forward

no igmp-snooping route-port forward

【Command configuration mode】

Global configuration mode

【Default】

Disable

【Example】

！ Enable igmp-snooping route-port forward

Optiway(config)#igmp-snooping route-port forward

12.2.9 igmp-snooping multicast vlan

Use **igmp-snooping multicast vlan** command to specify a VLAN for a port to learn and transmit multicast message. IGMP message intercepted by

IGMP Snooping will modify its VID to be specified VLAN to transmit. Descendent multicast message is transmitted in VLAN, and separated with unicast message VLAN.

igmp-snooping multicast vlan *vlan-id*

no igmp-snooping multicast vlan

【Command configuration mode】

Interface configuration mode

【Parameter】

vlan-id:Range from 1 to 4294

【Default】

No multicast VLAN configuration for port

【Example】

！Configure multicast vlan of Ethernet 2/1 to be vlan 2

Optiway(config-if-ethernet-2/1)#igmp-snooping multicast vlan 2

12.2.10 **show gmrp**

Use **show gmrp** command to display GMRP globally.

show gmrp

【Command configuration mode】

Any configuration mode

【Example】

！Display GMRP information globally

Optiway(config)#show gmrp

GMRP state : enable

12.2.11 show gmrp interface

Use **show gmrp interface** command to display GMRP information of an interface.

show gmrp interface [*interface-list*]

【Parameter】

interface-list:List of Ethernet ports to be added to or removed from a VLAN. This keyword needed to be provided in the form of interface-type + interface-number. Interface-type is Ethernet and interface-number is slot-num/port-num, in which slot-num is in the range of 2 to 2, and port-num is in the range of 1 to 24. Seriate(sequential?) interfaces with the same type can be linked by to keyword, but the port number to the right of the to keyword must be larger than the one to the left of the keyword, and this argument only can be repeated for up to 3 times.

【Command configuration mode】

Any configuration mode

【Usage】

Key word “interface-list” is optional. If this keyword is lacking, all the information of the interfaces is displayed, or information of only specified interfaces is displayed.

【Example】

！Display information of gmrp interface Ethernet 2/1, ethetnet 2/2, Ethernet 2/3, Ethernet 2/1

Optiway(config)#show gmrp interface ethernet 2/1 to ethernet 2/3 ethernet 3/2

port GMRP status

e2/1 enable

e2/2 enable

e2/3 enable

e3/2 enable

Total entries: 4

12.2.12 garp permit multicast mac-address

Use **garp permit multicast mac-address** command to add configured static multicast group to GMRP to be dynamic learned by other switches.

garp permit multicast [mac-address *mac* vlan *vlan-id*]

【Parameter】

mac:MAC address of existed multicast group in the form of multicast MAC address, such as: 21:22:5e:**:**:**

vlan-id:Range from 1 to 4294. Multicast group is combined by vlan-id and mac

【Command configuration mode】

Global configuration mode

【Example】

! Add multicast group 21:22:5e:22:21:21 vlan 1 to GMRP

Optiway(config)#garp permit multicast mac-address 21:22:5e:22:21:21 vlan 1

12.2.13 show garp permit multicast

Use **show garp permit multicast** command to display static multicast group permitted learning by GMRP.

show garp permit multicast

【Command configuration mode】

Any configuration mode

【Example】

! Display the static multicast permitted by GMRP

Optiway(config)#show garp permit multicast

12.2.14 show igmp-snooping

Use **show igmp-snooping** command to display the information of IGMP snooping

show igmp-snooping

【Command configuration mode】

Any configuration mode

【Example】

！Display IGMP snooping information

Optiway(config)#show igmp-snooping

12.3 IGMP Configuration Command

IGMP configuration command includes:

- **ip igmp**

- **igmp-proxy**
- **ip igmp access-group**
- **ip igmp last-member-query-interval**
- **ip igmp query-interval**
- **ip igmp query-max-response-time**
- **ip igmp static-group**
- **ip igmp create-group**
- **ip igmp robustness-varible**
- **ip igmp limit-group**
- **ip igmp version**
- **ip multicast-routing**
- **show igmp-proxy**
- **show ip igmp groups**
- **show ip igmp interface**
- **ip igmp ssm-mapping**
- **mroute igmp**
- **ssm-mapping static**
- **show ip igmp ssm-mapping**

12.3.1 ip igmp

Use **ip igmp** command to enable IGMP. Use **no ip igmp** command to disable IGMP.

ip igmp

no ip igmp

【Default】

IGMP is not run.

【Command configuration mode】

Interface configuration mode (including VLAN interface and super VLAN interface configuration mode)

【Usage】

Only interface IGMP enables, IGMP packet can be sent and received.

【Example】

！Enable IGMP of VLAN-interface1

Optiway(config-if-vlanInterface-1)#ip igmp

12.3.2 igmp-proxy

Use this command to enable IGMP proxy. Use **no** command to disable IGMP proxy.

igmp-proxy

no igmp-proxy

【Default】

Disable

【Command configuration mode】

VLAN interface mode

【Usage】

After enabling IGMP proxy, switch is a master for uplink multicast router which transfer the collected multicast information from user out through report packet. Multicast router will transfer multicast flow to switch and switch will

transfer it to downlink user. When there is no master in some multicast, switch will send leave packet to multicast router and multicast router will stop transferring multicast data to switch. This function is applied to switch in network end and it is unnecessary to enable multicast routing protocol to finish multicast transmission to save switch resources.

【Example】

！Enable IGMP proxy

Optiway(config-if-vlanInterface-1)#igmp-proxy

12.3.3 ip igmp access-group

Use **ip igmp access-group** command to restrict host in the subnetwork connected to Ethernet switch interface to add to multicast group. Use **no ip igmp access-group** command to cancel this restriction.

ip igmp access-group access-list-number [port-list]

no ip igmp access-group *[port-list]*

【Parameter】

access-list-number:standard IP ACL number which is in the range of 1～99. It defines a group range in which host can only add to the multicast group.

ports-list:List of Ethernet ports. This keyword needed to be provided in the form of interface-type + interface-number. Interface-type is Ethernet and interface-number is device/slot-num/port-num, in which device is stack device number which is in the range of 2 to 7, slot-num is in the range of 2 to 1, and port-num is in the range of 1 to 12. Seriate interfaces with the same type can be linked by to keyword, but the port number to the right of the to keyword must be larger than the one to the left of the keyword, and this argument only can be repeated for up to 3 times and it cannot configure all ports to be port isolation downlink ports.

【Default】

Non-restriction for the host to add to multicast group.

【Command configuration mode】

Interface configuration mode (including VLAN interface and super VLAN interface configuration mode)

【Usage】

Ethernet switch sends host-query message to be sure the multicast group members existed in local network which connected with this Ethernet switch. The packets sent to the milticast group will be transferred to these members. User can restrict the host in sunnetwork connected to interface in each interface adding to multicast group.

【Example】

！Configure access-list 1

Optiway (config)# access-list 1 permit 225.2.2.2 2.255.255.255

！Specify host in VLAN interface 1 can only be added to the multicast grou pwhich satisfied rules in access-list 1

Optiway(config-if-vlanInterface-1) # ip igmp access-group 1

12.3.4 ip igmp last-member-query-interval

Use **ip igmp last-member-query-interval** command to configure query interval of last member.

ip igmp last-member-query-interval *seconds*

no ip igmp last-member-query-interval

【Parameter】

Seconds the query interval of last member which is in the range of 1 to 64.

【Default】

The query interval of last member is 1 second.

【Command configuration mode】

Interface configuration mode (including VLAN interface and super VLAN interface configuration mode)

【Usage】

This command can only be effected in the network of IGMP V2/V3.
the query of last member is to know whethern there is multicast group member and reduce delitescence, so this time period cannot be too long.

【Example】

！Configure the query interval of last member of interface 1 to be 2 seconds.

Optiway(config-if-vlanInterface-1)#ip igmp last-member-query-interval 2

12.3.5 ip igmp query-interval

Use **ip igmp query-interval** command to configure the query interval of host members. Use **no ip igmp query-interval** command to restore the default query interval.

ip igmp query-interval *seconds*

no ip igmp query-interval

【Parameter】

Seconds : the query interval of host member which is in the range of 1 to 32222 seconds.

【Default】

The query interval of host member is 125 second.

【Command configuration mode】

Interface configuration mode (including VLAN interface and super VLAN interface configuration mode)

【Usage】

Ethernet switch sends host-query message to be sure the multicast group members existed in local network which connected with this Ethernet switch. The packets sent to the milticast group will be transferred to these members. User can restrict the host in sunnetwork connected to interface in each interface adding to multicast group.

In a LAN, Designated Router is the only one which sends host-query message. For IGMP V1, choose specified router according to the multicast routing protocol run in LAN; for IGMP V2, choose specified router according to the smallest IP address in LAN. Ethernet switch supported PIM can also be specified router.

If Ethernet switch doesn't receive query packet from any host member after overtime（configured by ip igmp querier-timeout command）, this switch becomes the Querier（the switch sending host-query message）

【Example】

！Configure query interval of VLAN 1 to be 122 seconds

Optiway(config-if-vlanInterface-1)# ip igmp query-interval 122

12.3.6 ip igmp query-max-response-time

Use **ip igmp query-max-response-time** command to configure the max response time of query packet of host members. Use **no ip igmp query-max-response-time** command to restore the default max response

time.

ip igmp query-max-response-time *seconds*

no ip igmp query-max-response-time

【Parameter】

Seconds : the max response time in query packet of host member which is in the range of 1 to 32222 seconds.

【Default】

The max response time in query packet of host member is 12 seconds.

【Command configuration mode】

Interface configuration mode (including VLAN interface and super VLAN interface configuration mode)

【Usage】

Use this command when running IGMP V2/V3.

This command can control the time interval for host to response the query packet of host members. The small time interval can make switch master the existence of group members. If the response to the query packet of host members is not quickly, they may be deleted from multicast group though user doesn't want. User must configure the interval larger than the shortest response time.

【Example】

！ Configure the max response time in query packet is 8 seconds.

Optiway(config-if-vlanInterface-1)# ip igmp query-max-response-time 8

12.3.7 ip igmp static-group

Use **ip igmp static-group** command to configure Ethernet switch interface to add to multicast group. Use **no ip igmp static-group** command to delete interface from multicast group.

ip igmp static-group groups-address port-list sourcelist sourcelist

no ip igmp static-group *groups-address port-list* sourcelist *sourcelist*

【Parameter】

groups-address: the muilticast group address to be added.

ports-list:List of Ethernet ports. This keyword needed to be provided in the form of interface-type + interface-number. Interface-type is Ethernet and interface-number is device/slot-num/port-num, in which device is stack device number which is in the range of 2 to 7, slot-num is in the range of 2 to 1, and port-num is in the range of 1 to 12. Seriate interfaces with the same type can be linked by to keyword, but the port number to the right of the to keyword must be larger than the one to the left of the keyword, and this argument only can be repeated for up to 3 times and it cannot configure all ports to be port isolation downlink ports.

sourcelist: multicast source address list which is to add to specified source address list. There will be at most 8 multicast source address list.

【Default】

Interface will not statistically add to any multicast group.

【Command configuration mode】

VLAN interface

【Usage】

After adding to multicast statically, no matter there is multicast memberor not, multicast flow will transferred to this interface.

【Example】

！Add interface 1 of VLAN interface 1 to multicast group 224.1.1.1 and the multicast source address add to specified source address is 12.2.2.1

Optiway(config-if-vlanInterface-1)# ip igmp static-group 224.1.1.1 ethernet 2/1

12.3.8 ip igmp create-group

Use this command together with ip igmp static-group command to configure ingress vlan ID of static multicast route table item. Use the no command to delete it.

Vlan interface configuration mode:

ip igmp create-group *groups-address*

no ip igmp create-group *groups-address*

supervlan interface configuration mode:

ip igmp create-group *groups-address* vlan *vlanid*

no ip igmp create-group *groups-address* vlan *vlanid*

【Parameter】

groups-address:multicast group address to be configured

vlanid: ingress vlanid of static multicast group member

【Default】

No static multicast route table item

【Command configuration mode】

interface mode（including VLAN and superVlan interface mode）

【Usage】

This command is used with ip igmp static-group command. ip igmp static-group command only creates static multicast group members but not specifies ingress vlanid, so the multicast packet transferring cannot finished. This command specifies ingress vlan and creates a complete static multicast member table to realize the packet transmission of static multicast members. In VLAN mode, ingress vlanid value is the id of vlan interface.

【Example】

！Configure ingress vlanid of static multicast group 224.2.1.5 in vlan interface 1

Optiway(config-if-vlanInterface-1)# ip igmp create-group 224.2.1.5

12.3.9 ip igmp robustness-varible

Use **ip igmp robustness-varible** command to configure robustness-varible of Ethernet switch. Use **no ip igmp robustness-varible** command to restore it to default value.

ip igmp robustness-varible *num*

no ip igmp robustness-varible

【Parameter】

num:the robustness-varible which is in the range of 1 to 7.

【Default】

The default robustness-varible value is 2.

【Command configuration mode】

Interface configuration mode (including VLAN interface and super VLAN interface configuration mode)

【Usage】

The robustness-varible is a very important parameter to express the operation of IGMP which is used to control the numberof sending packetto prevent the loss of the packet in network to strengthen the operation of network protocol. For example, after receiving the message of the leaving of the multicast group members, switch need send special group query and the robustness varible will specifies the number of the special query packet sent in a certain time interval. In addition, robustness varible is an important parameter to calculate other variables, such as: existing time of other queries and group membes are all use robustness variable to calculate.

【Example】

！Configure robustness variable of vlan interface 1 to be 5

Optiway(config-if-vlanInterface-1)# ip igmp robustness-varible 5

12.3.10 ip igmp limit-group

Use **ip igmp limit-group** command to configure the number of the multicast group restricted switch interface to add. Use **no ip igmp limit-group** command to restore the default number of the multicast group restricted switch interface to add.

ip igmp limit-group *num*

no ip igmp limit-group

【Parameter】

num:the number of the multicast group restricted to add.

【Default】

The number of the multicast group restricted to add is 1224.

【Command configuration mode】

Interface configuration mode (including VLAN interface and super VLAN interface configuration mode)

【Usage】

Use this command to restrict the number of IGMP group added in interface, the router will not handle IGMP adding packet if it is beyond the restriction. By default, the max number of IGMP group added in interface is the max number of multicast group number (that is max hardware table item, considering it can use up all hareware table items through one interface). In configuration, if the added number of IGMP group is beyond the configuration, the added IGMP group will not be deleted. Repeat this command, the new configuration will cover the original.

【Example】

！Configure the number of the multicast group restricted to add of vlan interface 1 to be 5

Optiway(config-if-vlanInterface-1)# ip igmp limit-group 5

12.3.11 ip igmp version

Use **ip igmp version** command to configure the IGMP version run in Ethernet switch. Use **no ip igmp version** command to restore the default IGMP version.

ip igmp version { 1 | 2 | 3}

no ip igmp version

【Parameter】

1:IGMP Version 1.

2:IGMP Version 2.

3:IGMP Version 3.

【Default】

Run IGMP version 2.

【Command configuration mode】

Interface configuration mode (including VLAN interface and super VLAN interface configuration mode)

【Usage】

All system run in the same subnetwork must support the same IGMP version.switch can find the switch with other version automatically and inform sys-log, but it cannot shift it automatically.

Some command needs IGMP V2/V3 to be effective, such as: ip igmp query-max-response-time and ip igmp query-timeout command.

【Example】

！Run IGMP version 1 in VLAN interface 1.

Optiway(config-if-vlanInterface-1)# ip igmp version 1

12.3.12 ip multicast-routing

Use **ip multicast-routing** command to enable multicast router. Use **no ip multicast-routing** command to disable multicast router.

ip multicast-routing

no ip multicast-routing

【Default】

Multicast router disables.

【Command configuration mode】

Global configuration mode

【Usage】

Only after enabling multicast router, ethernet switch can receive multicast packet.

Caution: after enabling layer 3 multicast, layer 2 multicast and IGMP Snooping table item are ineffective.

【Example】

！ Enable multicast router

Optiway(config)#ip multicast-routing

12.3.13 **show igmp-proxy**

Use this command to display IGMP proxy information.

show igmp-proxy

【Command configuration mode】

Any configuration mode

【Usage】

Use this command to display IGMP proxy status, configuration of uplink multicast router and IGMP proxy interface.

【Example】

！ Display IGMP proxy information

Optiway(config)#show igmp-proxy

12.3.14 **show ip igmp groups**

Use **show ip igmp groups** command to display multicast group information

learnt by IGMP and statically configured multicast group member information.

show ip igmp groups [*multicast-ip*]

【Parameter】

multicast-ip:multicast group address.

【Command configuration mode】

Any configuration mode

【Usage】

If the parameter is omitted, group address and interface type information of all multicast group members will be displayed.

【Example】

！ Displyay IGMP multicast group information.

Optiway(config)#show ip igmp group

12.3.15 show ip igmp interface

Use **show ip igmp interface** command to display interface information which runs IGMP.

show ip igmp interface [interface-type interface-number]

【Parameter】

interface-type:includes VLAN interface and superVlan interface.

interface-number:intwerface ID

【Command configuration mode】

Any configuration mode

【Usage】

If the parameter is omitted, all interface information which runs IGMP will be displayed.

【Example】

！ Display all IGMP interface information.

Optiway#show ip igmp interface

12.3.16 ip igmp ssm-mapping

Enable SSM Mappingin configured SSM address range. Use **no** command to disable SSM Mapping.

ip igmp ssm-mapping

no ip igmp ssm-mapping

【Parameter】

Non

【Default】

SSM Mapping disables.

【Command configuration mode】

Interface configuration mode (including VLAN interface and superVlan interface)

【Usage】

Enable SSM Mapping in interface before configuring SSM source/group address mapping table item, or IGMP will not support SSM Mapping.

When router enabled SSM Mapping receives IGMPv1/v2 report packet, it will gain mapping source address S through group address G to form （S,G） channel.

SSM Mapping only needs configuring on device connected to receiving host.

【Example】

Enable SSM Mapping:

ip igmp ssm-mapping

12.3.17 mroute igmp

Enter igmp configuration mode.

mroute igmp

【Command configuration mode】

Any configuration mode

【Usage】

Use mroute pim command to enter IGMP mode to configure IGMP global parameter without enabling IGMP protocol. Use exit command to exit to last mode and use quit to exit to preivileged mode.

【Example】

！Enter igmp mode

Optiway(config)#mroute igmp

12.3.18 ssm-mapping static

Enable static SSM Mapping. Use **no** command to cancel it.
ssm-mapping static { *access-control-list source-address* }
no ssm-mapping static { *access-control-list source-address* | **all** }

【Parameter】

access-control-list:used in static SSM Mapping ACL
source-address:source address mapping from group address in *access-control-list*
all:（option）all ssm-mapping configuration

【Default】

Non

【Command configuration mode】

IGMP global configuration mode

【Usage】

Static SSM Mapping can be configured many times. Group G belongs to Permit item of multiple ACL,the *source-address* parameter of multiple ACL are all mapping source of Group G. The max number of static SSM Mapping is 8.

【Example】

Enable static SSM Mapping:

mroute igmp

ssm-mapping static 11 172.16.8.11

ssm-mapping static 12 172.16.8.12

12.3.19 **show ip igmp ssm-mapping**

Display SSM Mapping of specific group address.

show ip igmp ssm-mapping [*group-address*]

【Parameter】

group-address:（option）corresponded SSM Mapping of group address.

【Default】

Display all ssm-mapping.

【Command configuration mode】

Any configuration mode

【Usage】

Display SSM Mapping of specific group address. If there is no mapping information, it will prompt resolve error.

【Example】

Display SSM Mapping of specific group address:

Optiway# **show ip igmp ssm-mapping 232.1.1.4**

Group address: 232.1.1.4

Database : Static

Source list : 172.16.8.5
: 172.16.8.6

Display SSM Mapping of specific group address(If there is no mapping information):
Optiway # **show ip igmp ssm-mapping 232.1.1.4**

Can't resolve 232.1.1.4 to source-mapping

12.4 PIM Configuration Command

PIM configuration command includes:

- **ip pim dense-mode**
- **ip pim neighbor-limit**
- **ip pim neighbor-policy**
- **ip pim query-interval**
- **ip pim sparse-mode**
- **ip pim bsr-border**
- **mroute pim**
- **show ip mroute**
- **show ip pim neighbor**
- **show ip pim interface**
- **show ip pim rp-info**
- **show ip pim bsr**
- **source-policy**
- **static-rp**
- **bsr-candidate**
- **rp-candidate**

- **spt-threshold**
- **ssm**
- **show ip pim ssm range**

12.4.1 ip pim dense-mode

Use **ip pim dense-mode** command to enable PIM-DM in interface. Use **no ip pim dense-mode** command to disable PIM-DM.

ip pim dense-mode

no ip pim dense-mode

【Default】

PIM-DM is not run in interface.

【Command configuration mode】

Interface configuration mode (including VLAN interface and superVlan interface)

【Usage】

Before enabling PIM-DM protocol,enable multicast routing protocol.

【Example】

! Run PIM-DM in VLAN interface 1

Optiway(config-if-vlanInterface-1)#ip pim dense-mode

12.4.2 ip pim neighbor-limit

Use **ip pim neighbor-limit** command to restrict PIM neighbour number of router interfaces. If it is beyond the configured restriction, new neighbours cannot be added. Use **no ip pim neighbor-limit** command to restore it to the

default configuration.

ip pim neighbor-limit *limit*

no ip pim neighbor-limit

【Parameter】

limit:the max limit of PIM neighbor in interface which is in the range of 2～128.

【Default】

The max limit of PIM neighbor in interface is 128.

【Command configuration mode】

Interface configuration mode (including VLAN interface and superVlan interface)

【Usage】

Only enable PIM-DM protocol before configure PIM interfqace attribution.

【Example】

！Configure the max limit of PIM neighbor in VLAN-interface 1 is 16

Optiway(config-if-vlanInterface-1)#ip pim neighbor-limit 16

12.4.3 ip pim neighbor-policy

Use **ip pim neighbor-policy** command to configure filreation to PIM neighbor in current interface. Use **no ip pim neighbor-policy** command to cancel filreation.

ip pim neighbor-policy *access-list-number*

no ip pim neighbor-policy

【Parameter】

access-list-number:standard IP ACL which is in the range of 1 to 99.

【Default】

Not to filtrate neighbors.

【Command configuration mode】

Interface configuration mode (including VLAN interface and superVlan interface)

【Usage】

Ethernet switch sends host-query message to be sure the multicast group members existed in local network which connected with this Ethernet switch. The packets sent to the milticast group will be transferred to these members. User can restrict the host in sunnetwork connected to interface in each interface adding to multicast group.

【Example】

！Configure access-list 1

Optiway (config)# access-list 1 permit 12.2.2.2 2.255.255.255

！Learn the neighbor which is in in VLAN interface 1 and satisfies the rules in access-list 1

Optiway(config-if-vlanInterface-1) # ip pim neighbor-policy 1

12.4.4 ip pim query-interval

Use **ip pim query-interval** command to configure the query interval of Hello packet. Use **no ip pim query-interval** command to restore the default value.

ip pim query-interval *seconds*

no ip pim query-interval

【Parameter】

seconds:the query interval of Hello packet which is in the range of 1 to 65535 seconds.

【Default】

The default query interval of Hello packet is 32s.

【Command configuration mode】

Interface configuration mode (including VLAN interface and superVlan interface)

【Usage】

After enabling PIM-SM protocol, for finding neighbors, switch will send Hello packet for all network devices supported PIM periodically. If the Hello packet is received, there is neighbor network device supported PIM, and this interface will add this neighbor to its interface neighbor list; if interface hasn't received the Hello packet from neighbour in its neighbour list, the neighbour is thought to leave multicast group.

【Example】

！Configure query interval of the last member in VLAN interface 1 is 62 seconds

Optiway(config-if-vlanInterface-1)#ip pim query-interval 62

12.4.5 ip pim sparse-mode

Use **ip pim sparse-mode** command to enable PIM-SM in interface. Use **no ip pim sparse-mode** command to disable PIM-SM.

ip pim sparse-mode

no ip pim sparse-mode

【Default】

PIM-DM is not run in interface.

【Command configuration mode】

Interface configuration mode (including VLAN interface and superVlan interface)

【Usage】

Before enabling PIM-DM protocol,enable multicast routing protocol

【Example】

！Run PIM-SM in VLAN interface 1.

Optiway(config-if-vlanInterface-1)#ip pim sparse-mode

12.4.6 ip pim bsr-border

Us this command to enable bsr domain border in interface. Use the no command to disable it.

ip pim bsr-border

no ip pim bsr-border

【Default】

bsr-border disables

【Command configuration mode】

Interface configuration mode (including VLAN interface and superVlan interface)

【Usage】

User can divide the network operating PIM-SM into many areas and use

different Bootstrap Router in each area. Caution: This command cannot establish multicast border but a PIM Bootstrap Router border.

【Example】

！Enable bsr-border in PIM-SM interface

Optiway(config-if-vlanInterface-1)#ip pim bsr-border

12.4.7 **mroute pim**

Use mroute **pim** command to enter pim configuration.

mroute **pim**

【Command configuration mode】

Any configuration mode

【Usage】

mroute PIM command is used to enter PIM to configure the global parameter of PIM but not enable PIM protocol. Use exit to be back to the last mode and use quit to be back to privileged mode.

【Example】

！Enter pim mode

Optiway(config)# mroute pim

12.4.8 **show ip mroute**

Use **show ip mroute** command to display multicast routing table and current version only supports PIM multicast routing table.

show ip mroute [*group-address*]

【Parameter】

group-address:multicast address.

【Command configuration mode】

Any configuration mode

【Usage】

If there is no parameter, all multicast routing items are displayed. If the address is specified, all all multicast routing tables are displayed, including （S,G）and（*,G）.

【Example】

！Display multicast routing table

Optiway(config-if-vlanInterface-1)#show ip mroute

12.4.9 show ip pim neighbor

Use **show ip pim neighbor** command to display neighbor list learnt by PIM.

show ip pim neighbor [interface vlan-interface *vid*]

【Parameter】

Vid: it is in the range of 1 to 4294.

【Command configuration mode】

Any configuration mode

【Usage】

If there is no parameter, all neighbors will be displayed. Display neighbor in the specified interface after specification.

【Example】

！ Display neighbor list

Optiway(config-if-vlanInterface-1)# show ip pim neighbor

12.4.10 show ip pim interface

Use **show ip pim interface** command to display operation and configuration information of PIM interface.

show ip pim interface [interface-type interface-number]

【Parameter】

interface-type:interface type. Here means VLAN interface.

interface-number:interface number which is in the range of 1～4294.

【Command configuration mode】

Any configuration mode

【Usage】

If there is no parameter, all interfaces information will be displayed. Display information in the specified interface after specification.

【Example】

！ Display PIM interface information

Optiway(config-if-vlanInterface-1)#show ip pim interface

12.4.11 show ip pim rp-info

Uer **show ip pim rp-info** command to display RP information of PIM-SM.

show ip pim rp-info

【Parameter】

group-address:the multicast group address. If it is not specified,display all, including dynamically learnt and static configured RP.

【Command configuration mode】

Any configuration mode

【Usage】

The effecting RP information is displayed.

【Example】

！Display RP information of PIM interface.

Optiway(config-if-vlanInterface-1)#show ip pim rp-info

12.4.12 **show ip pim bsr**

Use this command to display BSR information.

show ip pim bsr

【Command configuration mode】

Any configuration mode

【Usage】

Use this command to display BSR information including selected BSR information and candidate BSR.

【Example】

！Display current BSR information

Optiway(config-if-vlanInterface-1)#show ip pim bsr

12.4.13 **source-policy**

Use **source-policy** command to configure router to filtrate multicast data packet according to source address. Use **no source-policy** command to cancel it.

source-policy access-list-number

no source-policy

【Parameter】

access-list-number:standard IP ACL number which is in the range of 1～99.

【Default】

Not to filtrate the source address of multicast data packet.

【Command configuration mode】

PIM configuration mode

【Usage】

After configuring source address filtration, the data packet which is not satisfying filtration rules will be dropped.

Repeat this command, new configuration will cover the last one.

【Example】

！Configure switch multicast packet with the source address to be 192.168.1.1

Optiway (config)# access-list 1 permit 192.168.1.1 2

Optiway(config-pim) # source-policy 1

12.4.14 **static-rp**

Use **static-rp** command to configure static RP used by PIM-SM.

static-rp *address*

no static-rp

【Parameter】

address:RP address

【Default】

Static RP is not configured.

【Command configuration mode】

PIM configuration mode

【Usage】

Static RP is used for backup of dynamic RP to improve the strength of network. In the effection of RP selected by BSR mechanism, static RP is unaffected.

All routers in PIM domain must configure this command and specify the same RP address at the same time.

Repeat this command, new configuration will cover the last one.

Related configuration refers to show ip pim rp-info.

【Example】

！ Configure static RP to be 192.168.1.1

Optiway(config-pim) # static-rp 192.168.1.1

12.4.15 **bsr-candidate**

Use this command to configure switch to be Candidate Bootstrap Router,(C-BSR). Use the **no** command to delete C-BSR.

bsr-candidate interface-type interface-number hash-mask-length [priority]

no bsr-candidate

【Parameter】

interface-type:interface type which can be VLAN-interface or Super VLAN-interface；

interface-number:interface number；

hash-mask-len:matching mask length in HASH which is in the range of 2～32. The longer the mask is, the smaller the discrete of C-BSR is; the shorter the mask is, the larger the discrete of C-BSR is.

priority:C-BSR priority which is in the range of 2～255. The candidate BSR with superior priority will be selected to be BSR； the one with larger IP address with the same priority will be selected to be BSR. The default *priority* is 2.

【Default】

Non candidate BSR is specified.

【Command configuration mode】

PIM configuration mode

【Usage】

Repeat excuting this command ,new configuration will cover the last one.

【Example】

！ Configure VLAN interface 1 to be candidate BSR

Optiway(config-pim) # bsr-candidate vlan-interface 1 12 12

12.4.16 **rp-candidate**

Use this command to configure switch to be Candidate Rendezvous Point,(C-RP). Use the **no** command to cancel this configuration. If there is no group-list parameter, C-RP serves for all groups.

rp-candidate interface-type interface-number [**group-list** access-list-number [priority]]

no rp-candidate interface-type interface-number [**group-list** access-list-number]

【Parameter】

i interface-type:interface type which can be VLAN-interface or Super VLAN-interface；

interface-number:interface number

access-list-number:standard IP accessing list number which is in the range of 1～99. It defines the range of a group which is the service range of RP.

priority:C-RP priority which is in the range of 2～255. The C-RP with superior priority will be selected to be RP；the one with larger IP address with the same priority will be selected to be RP.

【Default】

Non C-RP is specified.

【Command configuration mode】

PIM configuration mode

【Usage】

Repeat excuting this command ,new configuration will cover the last one.

【Example】

！ Configure VLAN interface 1 to be C-RP

Optiway(config-pim) # rp-candidate vlan-interface 1 group-list 1 12

12.4.17 spt-threshold

Use this command to configure switch threshold shift from RPT to adding to SPT which is shown as the rate of received multicast packet with the unit of bps. It supports 2 kinds of fixed thresholds : immediately and infinity,and immediately is the defult one. Use **no** command to restore it to immediately.

spt-threshold { *immediately* | *infinity* }

no spt-threshold

【Parameter】

immediately:adding to SPT as soon as receiving multicast packet

infinity:Never adding to SPT

【Default】

immediately

【Command configuration mode】

PIM configuration mode

【Usage】

Repeatly excute this command, new configuration will cover the last one.

【Example】

！ Configure SPT threshold to be infinity

Optiway(config-pim) # spt-threshold infinity

12.4.18 ssm

Define IP multicast address range of SSM. Use **no** command to cancel it.

ssm {**default** | **range** *access-list*}

no ssm {**default** | **range** *access-list*}

【Parameter】

default:Define IP multicast address range to be 232/8.

range:Specify IP collection based on standard ACL number or name to be SSM multicast address range.

【Default】

Do not configure SSM multicast address range.

【Command configuration mode】

PIM configuration mode

【Usage】

When excuting this command, in configured SSM multicast address range,router will not need receive and generate MSDP SA news to predigest network topology.

Multiple configuration is not permit. The next configuration will cover the previous one.

The condition for enabling SSM mode:

If multicast group address is in SSM group range, router interface runs IGMPv3,receiver's host runs IGMPv3,source address is specified in Report news, enable SSM mode.

If multicast group address is in SSM group range, router interface runs IGMPv3,receiver's host runs IGMPv1 or IGMPv2,SSM Mapping is enabled in router and there is matched SSM source group mapping rule, enable SSM mode.

【Example】

Configure SSM through ACL address range:

access-list 4 permit 224.2.151.141

mroute pim

ssm range 4

12.4.19 show ip pim ssm range

Display SSM Mapping of specific group address.

show ip pim ssm range

【Command configuration mode】

Any configuration mode

【Usage】

Display configured SSM group address range.

【Example】

Display configured SSM group address range.

Optiway# **show ip pim ssm range**

Group Address	Mask Length	ACL
237.2.2.2	8	1

Totle ssm group range entries:1.

Display default SSM group address range.

Optiway# **show ip pim ssm range**

Group Address	Mask Length	Desc
232.2.2.2	8	default

Display non-configured SSM group address range.

Optiway # **show ip pim ssm range**

No configged ssm group range

Chapter 13 ACL Configuration Command

13.1 ACL configuration command list

ACL command includes:

- **absolute**
- **access-group**
- **access-list**
- **access-list extended**
- **access-list link**
- **access-list match-order**
- **access-list standard**
- **access-list user**
- { **permit | deny** }
- **periodic**
- **port-isolation**
- **show access-list config**
- **show access-list config statistic**
- **show access-list runtime all**
- **show access-list runtime statistic**
- **show port-isolation**
- **show time-range**
- **time-range**

13.1.1 absolute

Use **absolute** command to create absolute time range. Use **no absolute** command to delete the configuration of absolute time range.

absolute [**start** *time date*] [**end** *time date*]

no absolute [**start** *time date*] [**end** *time date*]

【Parameter】

start *time date*:optional choice. Configure the start absolute time. The form of *time* is hh:mm:ss,using 24 hours. hh is in the range of 2～23,mm is in the range of 2－59, and ss is in the range of 2－59. The form of *date* is YYYY/MM/DD. day is in the range of 1～31,month is in the range of 1～12,year is 4 numbers. If the start time is not configured, it means there is no restriction to the start time but the end time.

end *time date*:optional choice. Configure the end absolute time. The form of *time* and *date* is the same as the start time and it must be larger than the start time. If the end time is not configured, it is the max time of system.

【Command configuration mode】

time-range configuration mode

【Usage】

Absolute time range can determine a large scale of effective time and restrict the time range of periodic time. Each time period can define 12 absolute time range. In the period of configuring absolute time and periodic time, only when the absolute time range is satisfied, periodic time range can be judged. When the staart time and end time are not specified, the specified time range is the earlist time the switch can be recognized to the inferior time.

【Example】

！ The following time range will be effective from 2:2 Jan 1st, 2222.

Optiway(config)#time-range tm1

Optiway(config-timerange-tm1)#absolute start 2:2 1-1-2222

Optiway(config-timerange-tm1)#exit

！ The following time range will be effective from 22:22 December 12, 2222 to 22:21

Optiway(config)#time-range tm2

Optiway(config-timerange-tm2)#absolute end 22:22 12-12-2222

Optiway(config-timerange-tm2)#exit

！ The following time range will be effective from 14:22 to 16:22 in each weekend from 22:22 December 31, 1999 to 22:22 December 12, 2222.（The configuration of periodic time range refers to periodic command.）

Optiway(config)# time-range testall

Optiway(config-timerange-testall)#absolute start 22:22 12-31-1999 end 22:22 12-12-2222

Optiway(config-timerange-testall)#periodic weekend 14:22 to 16:22
Optiway(config-timerange-testall)#exit

13.1.2 **access-group**

Use **access-group** command to activate accessing control list. Use **no access-group** command to cancel activate.

access-group { [**ip-group** { access-list-number | access-list-name }
[**subitem** subitem]] [**link-group** { access-list-number | access-list-name }
[**subitem** subitem]] } }

no access-group { **all** | [**ip-group** { *access-list-number* | *access-list-name* }
[**subitem** *subitem*]] [**link-group** { *access-list-number* | *access-list-name* }

[**subitem** *subitem*]] } }

【Parameter】

access-list-number:accessing control list number which is in the range of 1 to 399. access-list-name:the name of accessing list which is the character string and in the form of initial capitalized characters ([a-z, A-Z]), excluding space and quotation mark； **subitem** *subitem*:optional parameter, specifies the subitem in accessing list which is in the range of 2～127. If it is not specified, all subitems are activated.

Instruction:

Followings are the parameter of **no** command.

all:all the activated accessing list must be cancel.（including number and name ID）

【Usage】

This command supports activating accessing control list of layer 2 and layer 3 at the same time, but the action of each accessing control list should not be conflict, if there is conflict (such as one is permit, the other is deny), the activation fails. It can support at most 127 l2 and l3 ACL.

【Command configuration mode】

Global configuration mode

【Example】

！ Activate accessing control list 1 and 222 at the same time.

Optiway(config)#access-group ip-group 1 link-group 222

13.1.3 **access-list**

Use **access-list** command to configure a ACL with number ID, which can be:

standard ACL, extended ACL, Layer 2 ACL and user-defined ACL. Use **no access-list** command to delete all the subitems or one subitem in one ACL with number ID or name ID or all ACLs.

1. Define standard ACL with number ID.

access-list *access-list-number1* { permit | deny } { *source-addr source-wildcard* | any } [**fragments**] [**time-range** *time-range-name*]

2. Define extended ACL with number ID.

access-list *access-list-number2* { permit | deny } [*protocol*] [established]

{ *source-addr source-wildcard* | any } [*port* [*portmask*]] { *dest-addr dest-wildcard* | any } [*port* [*portmask*]] [*icmp-type* [*icmp-code*] | *icmp-packet*] [fragments] { [**precedence** *precedence*] [**tos** tos] | [**dscp** *dscp*] } [**time-range** *time-range-name*]

3. Define Layer 2 ACL with number ID.

access-list access-list-number3 { permit | deny } [protocol] [**cos** vlan-pri] **ingress** { { [source-vlan-id] [source-mac-addr source-mac-wildcard] [**interface** interface-num] } | any } **egress** { { [dest-mac-addr dest-mac-wildcard] [**interface** interface-num | **cpu**] } | any } [**time-range** time-range-name]

4. Delete ACL or its subitem.

no access-list { **all** | { access-list-number | **name** access-list-name } [subitem] }

【Parameter】

access-list-number1:standard ACL rules in the range of 1～99
access-list-number2:extended ACL rules in the range of 122～199
access-list-number3:Layer 2 ACL rules in the range of 222～299

permit:permit the packet which satisfied the condition passing.

deny:deny the packet which satisfied the condition passing.

time-range *time-range-name*:the name of time range whichh is optional parameter, and it will be efective in this time period.

Instruction:

Followings are all kinds of attribution with packet. ACL is the rules determined by the value of these parameter.

source-addr source-wildcard | any:*source-addr source-wildcard* means source IP address and source address wildcard which is in the form of dotted decimal notation; any means all source address which is used to establish standard or extended ACL.

fragments:means this rule is effective to the fragment packets, and non-fragment packet will ignore this rule. This parameter is used in standard or extended ACL.

protocol:the protocol with the name of numbers and names. The name of numbers is in the range of 1～255; the name of names is in the range of icmp, igmp, tcp, udp, gre, ospf and ipinip. This parameter is used in extended ACL.

established:means this rule is effective to the first SYN packet after the successful connection of TCP. This is the optional parameter which appears when the parameter of protocol is tcp. This parameter is used in extended ACL.

[Port [portmask]]: means the interface range of TCP/UDP. Port:means the tcp or udp port used by packet which is the optional parameter by using symbols oe numbers. The number is in the range of 2～65535,and the symbol refers to symbol table helped to remembered by port number. Portmask is port mask which is optional and is in the range of 2～65535. When the protocol is tcp or udp, it can support the configuration in the range of protocol ports. When configuring port number and mask, user can input octal, decimal or hex not port to permit all ports; portmask can be 2 or none to express the port

itself, or it can be determined by port and portmask according to the port range. This rule can support single port configuration which can support the configuration of larger or equal to the port range (accurate to 2^n).

dest-addr dest-wildcard | any:*dest-addr dest-wildcard* means destination IP address and destination address wildward which is in the form of decimal; any means all destination address. This parameter can be used in extended ACL.

[*icmp-type* [*icmp-code*] | *icmp-packet*]:*icmp-type* [*icmp-code*] specified — ICMP packet. icmp-type means ICMP packey type which is in the form of characters and numbers. The number is in the range of 2～255；icmp-code means ICMP code which appears when the protocol is icmp and there is no character to express ICMP. The range of it is 2～255；icmp-packet is the ICMP packet with the name of name, which is specified by icmp-type and icmp-code. This parameter can be used in extended ACL.

precedence *precedence*:optional parameter which means IP priority. It can be number and name which is in the range of 2～7. This parameter can be used in extended ACL.

dscp *dscp*:optional parameter which can be categoried according to DSCP, it is number or name which is in the range of 2～63. This parameter can be used in extended ACL.

tos *tos*:optional parameter which can be categoried according to TOS, it is number or name which is in the range of 2～15. This parameter can be used in extended ACL.

[**cos** *vlan-pri*]: 822.1p priority which is in the range of 2～7. This parameter can be used in layer 2 ACL.

ingress { { [*source-vlan-id*] [*source-mac-addr source-mac-wildcard*] [**interface** interface-num] } | any }:the source information of packet. source-vlan-id means source VLAN of data packet. [*source-mac-addr source-mac-wildcard*] means the source MAC address and MAC address

wildcard of packet. These two parametes can determine the range of source MAC address, such as: when source-mac-wildcard is 2:2:2:2:ff:ff,user is interested in the first 32 bit of source MAC address (that is the bit position corresponded to the number 2 in wildcard) **interface** *interface-num* means the layer 2 ports receiving this packet, any means all packets received by all ports. This parameter can be used in layer 2 ACL.

egress { { [*dest-mac-addr dest-mac-wildcard*] [**interface** *interface-num* | **cpu**] } | any }:destination information of packet.*dest-mac-addr dest-mac-wildcard* means destination MAC address and destination MAC address wildcard. These two parametes can determine the range of destination MAC address range, such as: when dest-mac-wildcard is 2:2:2:2:ff:ff,user is interested in the first 32 bit of source MAC address (that is the bit position corresponded to the number 2 in wildcard),**interface** *interface-num* means the layer 2 ports transferring this packet,**cpu** means cpu port,any means all packets transferred from all ports. This parameter can be used in layer 2 ACL.

{ *rule-string rule-mask offset* }&<1-22>:rule-string is the character string for users to define rules which must be in the form of hex with even numbers of characters; *rule-mask offset* is used for distilling packet information, rule-mask is inerratic mask which is used to collation operation of data packet, offset is sideplay mount which is with the standard of the packet head and specifies to collation operate from which bit, *rule-mask offset* effects together which will compare the character string distilled from packet with *rule-string* defined by user itself to find the matched packet before handling. &<1-22> means at most 22 rules can be defined. **ingress interface** *interface-num*,**egress interface** *interface-num* :the name of layer 2 interface, interface-num means one interface, **cpu** means cpu interface. This parameter can be used in user-determined ACL.

Instructions:

Followings are the parameter of **no** command.

all:means all accessing list will be deleted (including number ID and name ID).

access-list-number:the ACL number to be deleted which is a number between 1～399

name access-list-name:the ACL name to be deleted which is character string parameter with initial English letters (that is [a-z,A-Z]) with any kind, excluding space and quotation mark; **all**,**any** are not allowed.

subitem:optional parameter which specifies which subitem to be deletedinthe list. It is in the range of 2～127. If it is unspecified, all subitems will be deleted.

【Command configuration mode】

Global configuration mode

【Example】

！Configure ACL 1 to deny the packet with the source IP to be 192.168.3.1

Optiway(config)#access-list 1 deny 192.168.3.1 2

！Configure ACL 122 to deny packet with the 2xff of TCP source port number to be 2

Optiway(config)# access-list 122 deny tcp any 2 2xff any

13.1.4 access-list extended

Use **access-list extended** command to create an extended ACL with name ID, then enter extended ACL configuration mode. Use **no access-list** command to delete one or all subitems of ACL with number ID or name ID or delete all ACL.

access-list extended *name* [match-order { config | auto }]

no access-list { **all** | { *access-list-number* | **name** *access-list-name* } [**subitem** *subitem*] }

【Parameter】

name : character string parameter with initial English letters (that is [a-z,A-Z]) with any kind, excluding space and quotation mark; **all**,**any** are not allowed.

config:means the configuration order of user when matching ACL.

auto:means the configuration order of deep precedency when matching ACL.

Instruction:

Followings are the parameters of **no** command.

all:means all accessing list will be deleted (including number ID and name ID).

access-list-number:the ACL number to be deleted which is a number between 1～399

name access-list-name:the ACL name to be deleted which is character string parameter with initial English letters (that is [a-z,A-Z]) with any kind, excluding space and quotation mark; **all**,**any** are not allowed.

subitem *subitem*:optional parameter which specifies which subitem to be deletedinthe list. It is in the range of 2～127. If it is unspecified, all subitems will be deleted.

【Default】

The default order is config order.

【Command configuration mode】

Global configuration mode

【Usage】

This command creates an extended ACL with the name of “name”. After entering the extended ACL configuration mode, use { **permit** | **deny** }command to add subitem of this ACL (use exit command to exit ACL mode). Each ACL consists of many subitems, and the specified range of the flow category rules of each subitem is different, and if a packet can match many rules, there must be a matching order. Use **match-order** to specify the matching order, whether it is according to user configuration or deep precedency (precedent to match the rule with the small range). If it is not specified, it is defaulted to be user configuration order. Once user specifies the matching order of an ACL, it cannot be changed, unless delete all subitems of this ACL before respecify the order.

【Example】

！Create an extended ACL with the name to be example and specify the order to be deep precedency.

Optiway(config)#access-list extended example match-order auto

13.1.5 access-list link

Use **access-list link** command to create a layer 2 ACL with a name ID and enter layer 2 ACL configuration mode. Use **no access-list** command to delete one or all subitems of ACL with number ID or name ID or delete all ACL.

access-list link *name* [**match-order** { config | auto }]

no access-list { **all** | { *access-list-number* | **name** *access-list-name* } [**subitem** *subitem*] }

【Parameter】

name : character string parameter with initial English letters (that is [a-z,A-Z]) with any kind, excluding space and quotation mark; **all**,**any** are not allowed.

config:means the configuration order of user when matching ACL.

auto:means the configuration order of deep precedency when matching ACL.

Instruction:

Followings are the parameters of **no** command.

all:means all accessing list will be deleted (including number ID and name ID).

access-list-number:the ACL number to be deleted which is a number between 1～399

name access-list-name:the ACL name to be deleted which is character string parameter with initial English letters (that is [a-z,A-Z]) with any kind, excluding space and quotation mark; **all**,**any** are not allowed.

subitem *subitem*:optional parameter which specifies which subitem to be deletedinthe list. It is in the range of 2～127. If it is unspecified, all subitems will be deleted.

【Default】

The default order is config order.

【Command configuration mode】

Global configuration mode

【Usage】

This command creates a layer 2 ACL with the name of “name”. After entering the laye 2 ACL configuration mode, use { **permit** | **deny** }command to add subitem of this ACL (use exit command to exit ACL mode). Each ACL consists of many subitems, and the specified range of the flow category rules of each subitem is different, and if a packet can match many rules, there must be a matching order. Use **match-order** to specify the matching order,

whether it is according to user configuration or deep precedency (precedent to match the rule with the small range). If it is not specified, it is defaulted to be user configuration order. Once user specifies the matching order of an ACL, it cannot be changed, unless delete all subitems of this ACL before respecify the order.

【Example】

！Create a layer 2 ACL with the name to be example and specify the order to be deep precedency.

Optiway(config)#access-list link example match-order auto

13.1.6 access-list match-order

Use **access-list** command to specify rule matching order of an ACL with number ID.

access-list *access-list-number* **match-order** { config | auto }

【Parameter】

access-list-number:the ACL number which is a number between 1～399

config:means the configuration order of user when matching ACL.

auto:means the configuration order of deep precedency when matching ACL.

【Default】

The default order is config order.

【Command configuration mode】

Global configuration mode

【Usage】

Each ACL consists of many subitems, and the specified range of the flow

category rules of each subitem is different, and if a packet can match many rules, there must be a matching order. Use this command to specify the matching order, whether it is according to user configuration or deep precedency (precedent to match the rule with the small range). If it is not specified, it is defaulted to be user configuration order. Once user specifies the matching order of an ACL, it cannot be changed, unless delete all subitems of this ACL before respecify the order.

【Example】

！ Specify the order to be deep precedency.

Optiway(config)#access-list 1 match-order auto

13.1.7 access-list standard

Use **access-list standard** command to create a standard ACL with a name ID and enter standard ACL configuration mode. Use **no access-list standard** command to delete one or all subitems of ACL with number ID or name ID or delete all ACL.

access-list standard *name* [match-order { config | auto }]

no access-list { **all** | { *access-list-number* | **name** *access-list-name* } [**subitem** *subitem*] }

【Parameter】

name : character string parameter with initial English letters (that is [a-z,A-Z]) with any kind, excluding space and quotation mark; **all**,**any** are not allowed.

config:means the configuration order of user when matching ACL.

auto:means the configuration order of deep precedency when matching ACL.

Instruction:

Followings are the parameters of **no** command.

all:means all accessing list will be deleted (including number ID and name ID).

access-list-number:the ACL number to be deleted which is a number between 1～399

name access-list-name:the ACL name to be deleted which is character string parameter with initial English letters (that is [a-z,A-Z]) with any kind, excluding space and quotation mark; **all**,**any** are not allowed.

subitem *subitem*:optional parameter which specifies which subitem to be deletedinthe list. It is in the range of 2～127. If it is unspecified, all subitems will be deleted.

【Default】

The default order is config order.

【Command configuration mode】

Global configuration mode

【Usage】

This command creates a standard ACL with the name of “name”. After entering the standard ACL configuration mode, use { **permit** | **deny** }command to add subitem of this ACL (use exit command to exit ACL mode). Each ACL consists of many subitems, and the specified range of the flow category rules of each subitem is different, and if a packet can match many rules, there must be a matching order. Use **match-order** to specify the matching order, whether it is according to user configuration or deep precedency (precedent to match the rule with the small range). If it is not specified, it is defaulted to be user configuration order. Once user specifies the matching order of an ACL, it cannot be changed, unless delete all subitems of this ACL before respecify the order.

【Example】

！Create a standard ACL with the name to be example and specify the order to be deep precedency.

Optiway(config)#access-list standard example match-order auto

13.1.8 { permit | deny }

Use this command to add a subitem to ACL with the name ID.

1. Add a subitem to standard ACL with the name ID.

{ **permit** | **deny** } { *source-addr source-wildcard* | **any** } [**fragments**] [**time-range** *time-range-name*]

2. Add a subitem to extended ACL with the name ID.

{ **permit** | **deny** } [*protocol*] [**established**] { *source-addr source-wildcard* |

any } [port [portmask]] { dest-addr dest-wildcard | **any** } [port [portmask]]

[*icmp-type* [*icmp-code*]] { [**precedence** *precedence*] [**tos** *tos*] |

[**dscp** *dscp*] [**fragments**] [**time-range** *time-range-name*]

3. Add a subitem to layer 2 ACL with the name ID.

{ **permit** | **deny** } [*protocol*] [**cos** *vlan-pri*] **ingress** { { [*source-vlan-id*] [*source-mac-addr source-mac-wildcard*] [**interface** *interface-num*] } | **any** } **egress** { { [*dest-mac-addr dest-mac-wildcard*] [**interface** *interface-num* | **cpu**] } | **any** } [**time-range** *time-range-name*]

【Parameter】

permit:permit the packet which satisfied the condition passing.

deny:deny the packet which satisfied the condition passing.

time-range *time-range-name*:the name of time range whichh is optional

parameter, and it will be efective in this time period.

Instruction:

Followings are all kinds of attribution with packet. ACL is the rules determined by the value of these parameter.

source-addr source-wildcard | any:*source-addr source-wildcard* means source IP address and source address wildcard which is in the form of dotted decimal notation; any means all source address which is used to establish standard or extended ACL.

fragments:means this rule is effective to the fragment packets, and non-fragment packet will ignore this rule. This parameter is used in standard or extended ACL.

protocol:the protocol with the name of numbers and names. The name of numbers is in the range of 1～255; the name of names is in the range of icmp, igmp, tcp, udp, gre, ospf and ipinip. This parameter is used in extended ACL.

established:means this rule is effective to the first SYN packet after the successful connection of TCP. This is the optional parameter which appears when the parameter of protocol is tcp. This parameter is used in extended ACL.

[Port [portmask]]: means the interface range of TCP/UDP. Port:means the tcp or udp port used by packet which is the optional parameter by using symbols oe numbers. The number is in the range of 2～65535,and the symbol refers to symbol table helped to remembered by port number. Portmask is port mask which is optional and is in the range of 2～65535. When the protocol is tcp or udp, it can support the configuration in the range of protocol ports. When configuring port number and mask, user can input octal, decimal or hex not port to permit all ports; portmask can be 2 or none to express the port itself, or it can be determined by port and portmask according to the port range. This rule can support single port configuration which can support the

configuration of larger or equal to the port range (accurate to 2^n).

dest-addr dest-wildcard | any:*dest-addr dest-wildcard* means destination IP address and destination address wildward which is in the form of decimal; any means all destination address. This parameter can be used in extended ACL.

[*icmp-type* [*icmp-code*] | *icmp-packet*]:*icmp-type* [*icmp-code*] specified ICMP packet. icmp-type means ICMP packey type which is in the form of characters and numbers. The number is in the range of 2～255；icmp-code means ICMP code which appears when the protocol is icmp and there is no character to express ICMP. The range of it is 2～255；icmp-packet is the ICMP packet with the name of name, which is specified by icmp-type and icmp-code. This parameter can be used in extended ACL.

precedence *precedence*:optional parameter which means IP priority. It can be number and name which is in the range of 2～7. This parameter can be used in extended ACL.

dscp *dscp*:optional parameter which can be categoried according to DSCP, it is number or name which is in the range of 2～63. This parameter can be used in extended ACL.

tos *tos*:optional parameter which can be categoried according to TOS, it is number or name which is in the range of 2～15. This parameter can be used in extended ACL.

[**cos** *vlan-pri*]: 822.1p priority which is in the range of 2～7. This parameter can be used in layer 2 ACL.

ingress { { [*source-vlan-id*] [*source-mac-addr source-mac-wildcard*] [**interface** interface-num] } | any }:the source information of packet. source-vlan-id means source VLAN of data packet. [*source-mac-addr source-mac-wildcard*] means the source MAC address and MAC address wildcard of packet. These two parametes can determine the range of source MAC address, such as: when source-mac-wildcard is 2:2:2:2:ff:ff,user is

interested in the first 32 bit of source MAC address (that is the bit position corresponded to the number 2 in wildcard) **interface** *interface-num* means the layer 2 ports receiving this packet, any means all packets received by all ports. This parameter can be used in layer 2 ACL.

egress { { [*dest-mac-addr dest-mac-wildcard*] [**interface** *interface-num* | **cpu**] } | any }:destination information of packet.*dest-mac-addr dest-mac-wildcard* means destination MAC address and destination MAC address wildcard. These two parametes can determine the range of destination MAC address range, such as: when dest-mac-wildcard is 2:2:2:2:ff:ff,user is interested in the first 32 bit of source MAC address (that is the bit position corresponded to the number 2 in wildcard),**interface** *interface-num* means the layer 2 ports transferring this packet,**cpu** means cpu port,any means all packets transferred from all ports. This parameter can be used in layer 2 ACL.

{ *rule-string rule-mask offset* }&<1-22>:rule-string is the character string for users to define rules which must be in the form of hex with even numbers of characters; *rule-mask offset* is used for distilling packet information, rule-mask is inerratic mask which is used to collation operation of data packet, offset is sideplay mount which is with the standard of the packet head and specifies to collation operate from which bit, *rule-mask offset* effects together which will compare the character string distilled from packet with *rule-string* defined by user itself to find the matched packet before handling. &<1-22> means at most 22 rules can be defined. **ingress interface** *interface-num*,**egress interface** *interface-num* :the name of layer 2 interface, interface-num means one interface, **cpu** means cpu interface. This parameter can be used in user-determined ACL.

Instructions:

Followings are the parameter of **no** command.

all:means all accessing list will be deleted (including number ID and name

ID).

access-list-number:the ACL number to be deleted which is a number between 1～399

name access-list-name:the ACL name to be deleted which is character string parameter with initial English letters (that is [a-z,A-Z]) with any kind, excluding space and quotation mark; **all**,**any** are not allowed.

subitem:optional parameter which specifies which subitem to be deletedinthe list. It is in the range of 2～127. If it is unspecified, all subitems will be deleted.

【Parameter】

ACL configuration mode (including 4 configuration modes as: standard, extended, layer 2, interface)

【Parameter】

Entering ACL configuration mode, user this command to establish an ACL subitem. This command can be used repeatedly. Establish many subitems for an ACL. There can be 128 subitems in total. If this ACL has activated, add subitems are not allowed.

【Example】

！ Create a standard ACL with the name to be example and specify the matching order to be deep precedency.

Optiway(config)#access-list standard example match-order auto

Create ACL item successfully!

Optiway(config-std-nacl-example)#permit 192.168.3.1 2

Config ACL subitem successfully!

Optiway(config-std-nacl-example)#

13.1.9 **periodic**

Use **periodic** command to create periodic time range. Use **no periodic** command to delete periodic time range.

periodic days-of-the-week hh:mm:ss **to** [day-of-the-week] hh:mm:ss

no periodic days-of-the-week hh:mm:ss **to** [day-of-the-week] hh:mm:ss

【Parameter】

days-of-the-week:means this time period will be effected in the day of the week or will be effected from the day of week. More than one parameter can be input at one time. The range of this parameter is as following:

2～6（number which means from Monday to Sunday）；

mon,tue,wed,thur,fri,sat,sun（special character string which means Monday to Sunday）；

weekdays（special character string which means weekday from Monday to Friday）；

weekend（the time for rest, including Saturday and Sunday）；

daily（special character string which means all days, including 7 days of a week).

day-of-the-week behind **to**:means the time period will not be effected in the day of week. It defines a time range with the day-of-the-week before **to**. The day-of-the-week before or after **to** can only have one value, that is, the day between Monday and Sunday, and the one chosen before **to** must be earlier than the day chosen after it, such as: if the first day-of-the-week is wed,day-of-the-week after to can only be wed, thu, fri or sat. If there are two or more values before **to**, there will not be any value of day-of-the-week after it.

hh:mm:ss :The first is the start time and the second is the end time.

【Command configuration mode】

time-range configuration mode

【Usage】

The effective time of periodic time range is a week. According to the configuration, there are different expression, such as:the configuration of 8:22 to 18:22 in every weekday is:

OPTIWAY(config-timerange-test)#periodic weekdays 8:22 to 18:22

Or:

OPTIWAY(config-timerange-test)#periodic Monday Tuesday Wednesday Thursday Friday 8:22 to 18:22

The configuration of 8:22 to 18:22 from Monday to Friday is:

OPTIWAY(config-timerange-test)#periodic Monday 8:22 to Friday 18:22

【Example】

！ The time range is effective in 8:22 to 18:22 from Monday to Friday

Optiway(config)#time-range 1to5

Optiway(config-timerange-1to5)#periodic weekdays 8:22 to 18:22

Optiway(config-timerange-1to5)#exit

！ The time range is effective in 8:22 to 18:22 every day

Optiway(config)#time-range all_day

Optiway(config-timerange-all_day)#periodic daily 8:22 to 18:22

Optiway(config-timerange-all_day)#exit

！ The time range is effective in 8:22 to 18:22 from every Monday to Friday

Optiway(config)#time-range 1to5

Optiway(config-timerange-1to5)#periodic monday 8:22 to friday 18:22

Optiway(config-timerange-1to5)#exit

！The time range is effective in every weekend

Optiway(config)#time-range wend2

Optiway(config-timerange-wend2)#periodic weekend 2:2 to 23:59

Optiway(config-timerange-wend2)#exit

！The time range is effective in every weekend afternoon

Optiway(config)#time-range wendafternoon

Optiway(config-timerange-wendafternoon)#periodic weekend 14:22 to 18:22

Optiway(config-timerange-wendafternoon)#exit

13.1.10 port-isolation

Use **port-isolation** command to add one or a group of port isolation downlink port. Use **no port-isolation** command to delete one or a group of port isolation downlink port.

port-isolation { *interface-list* }

no port-isolation { *interface-list* | all }

【Parameter】

interface-list:List of Ethernet ports. This keyword needed to be provided in the form of interface-type + interface-number. Interface-type is Ethernet and interface-number is device/slot-num/port-num, in which device is stack device number which is in the range of 2 to 7, slot-num is in the range of 2 to 1, and port-num is in the range of 1 to 12. Seriate interfaces with the same type can be linked by to keyword, but the port number to the right of the to keyword

must be larger than the one to the left of the keyword, and this argument only can be repeated for up to 3 times and it cannot configure all ports to be port isolation downlink ports.

all:Means all the interfaces. When the keyword all is specified, all the interfaces in the system are added to a VLAN by using the **switchport** command, and all the interfaces are removed from a VLAN by using the no **switchport** command.

【Command configuration mode】

Global configuration mode

【Example】

！Add Ethernet 2/1 ethernet 2/3 to ethernet 2/5 ethernet 2/8 to be port isolation downlink port

Optiway(config)#port-isolation ethernet 2/1 ethernet 2/3 to ethernet 2/5 ethernet 2/8

！ Delete ethernet 2/3 to ethernet 2/5 ethernet 2/8 from port isolation downlink port

Optiway(config)#no port-isolation ethernet 2/3 to ethernet 2/5 ethernet 2/8

13.1.11 port-isolation group

Use this command to add a port member to a port group. Use the **no** commandtodelete a or some member.

port-isolation group *groupid* { *interface-list* }

no port-isolation group { all | *groupid* { *interface-list* } }

【Parameter】

groupid: the number of the group to be added.

interface-list:List of Ethernet ports. This keyword needed to be provided in the form of interface-type + interface-number. Interface-type is Ethernet and interface-number is device/slot-num/port-num, in which device is stack device number which is in the range of 2 to 7, slot-num is in the range of 2 to 1, and port-num is in the range of 1 to 12. Seriate interfaces with the same type can be linked by to keyword, but the port number to the right of the to keyword must be larger than the one to the left of the keyword, and this argument only can be repeated for up to 3 times

all:means all port group isolation

【Command configuration mode】

Global configuration mode

【Example】

！Add e2/1 and e2/3 to port isolation 1

Optiway(config)#port-isolation group 1 ethernet 2/1 ethernet 2/3

！Delete port isolation 1

Optiway(config)#no port-isolation group 1

13.1.12 show access-list config

Use **show access-list config** command display detaol configuration of ACL.

show access-list config { **all** | *access-list-number* | **name** *access-list-name* }

【Parameter】

all means all ACL (including the one with number ID and name ID)

access-list-number means the number of ACL to be displayed which is a number in the range of 1～399

name *access-list-name* character string parameter with initial English letters

(that is [a-z,A-Z]) with any kind, excluding space and quotation mark; **all**,**any** are not allowed.

【Command configuration mode】

Any configuration mode

【Usage】

This command is used to display detail configuration of ACL, including each { **permit | deny** } syntax, its sequence number and the number and bytes of packet matched this syntax.

【Example】

！Display all ACL

Optiway#show access-list config all

13.1.13 show access-list config statistic

Use **show access-list config statistic** command to display statistics information of ACL.

show access-list config statistic

【Command configuration mode】

Any configuration mode

【Example】

！Display statistics information of ACL.

Optiway(config)#show access-list config statistic

13.1.14 show access-list runtime

Use **show access-list runtime** command to display runtime application

information of ACL.

show access-list runtime { **all** | *access-list-number* | **name** *access-list-name* }

【Parameter】

all means all ACL (including the one with number ID and name ID)

access-list-number means the number of ACL to be displayed which is a number in the range of 1～399

name *access-list-name* character string parameter with initial English letters (that is [a-z,A-Z]) with any kind, excluding space and quotation mark; **all**,**any** are not allowed.

【Command configuration mode】

Any configuration mode

【Usage】

This command is used to display ACL runtime application information which includes ACL name, subitem name and deliver status.

【Example】

！Display runtime application of ACL of all interfaces.

Optiway#show access-list runtime all

13.1.15 show access-list runtime statistic

Use **show access-list runtime statistic** command to display ACL statistics information.

show access-list runtime statistic

【Command configuration mode】

Any configuration mode

【Example】

！Display ACL statistics information.

Optiway(config)#show access-list runtime statistic

13.1.16 show port-isolation

Use **show port-isolation** command to display port isolation and port isolation configuration.

show port-isolation

【Command configuration mode】

Any configuration mode

【Example】

！Display port isolation configuration

Optiway(config)#show port-isolation

13.1.17 show time-range

Use **show time-range** command to display time range.

show time-range [all | statistic | **name** *time-range-name*]

【Parameter】

all:all time range

statistic:all statistics information of all time range.

time-range-name:the name of time range with initial English letters (that is [a-z,A-Z]) with any kind which is in the range of 1 to 32 characters.

【Command configuration mode】

Any configuration mode

【Usage】

show time-range command is used to display the configuration and status of current time period. The time range which is activated will be displayed as active, and the one which is inactivated will be displayed as inactive.

⚠Caution: Because there is a time error when updating access-list status for about 1 minute, and show time-range will judge it through current time, the fact that show time-range saw a time range has been activated, but its access-list hasn't is normal.

【Example】

! Display all time range

Optiway(config-timerange-tm2)#show time-range all

! Display time range with the name of tm1

Optiway(config)#show time-range name tm1

! Display statistic information of all time range:

Optiway(config)#show time-range statistic

13.1.18 time-range

Use **time-range** command to enter **time-range** configuration mode. Use **no time-range** command to delete configured time range.

time-range time-range-name

no time-range { all | **name** *time-range-name* }

【Parameter】

time-range-name:the name of time range with initial English letters (that is [a-z,A-Z]) with any kind which is in the range of 1 to 32 characters.

【Command configuration mode】

Global configuration mode

【Example】

！Create time range tm1 and enter it.

Optiway(config)#time-range tm1

Optiway(config-timerange-tm1)#

Chapter 14 QOS Configuration Command

14.1 QoS Configuration Command

QoS configuration command includes:

- **clear traffic-statistic**
- **line-rate**
- **mirrored-to**
- **queue-scheduler**
- **queue-scheduler cos-map**
- **queue-scheduler dscp-map**
- **rate-limit**
- **show qos-info all**
- **show qos-info mirrored-to**
- **show qos-info statistic**
- **show qos-info traffic-copy-to-cpu**
- **show qos-info traffic-priority**
- **show qos-info traffic-redirect**
- **show qos-info traffic-statistic**
- **show qos-interface all**
- **show qos-interface line-rate**
- **show qos-interface rate-limit**
- **show qos-interface statistic**
- **show queue-scheduler**

- **show queue-scheduler cos-map**
- **show queue-scheduler dscp-map**
- **storm-control**
- **traffic-copy-to-cpu**
- **traffic-priority**
- **traffic-redirect**
- **traffic-statistic**

14.1.1 clear traffic-statistic

Use **clear traffic-statistic** command to clear traffic-statistic.

clear traffic-statistic { **all** | { [**ip-group** { *access-list-number* | *access-list-name* } [**subitem** *subitem*]] [**link-group** { *access-list-number* | *access-list-name* } [**subitem** *subitem*]] } }

【Parameter】

all:clear all the traffic statistic list (including combination item).**ip-group** { *access-list-number* | *access-list-name* } [**subitem** *subitem*] :means standard or extended accessing control list. access-list-number:sequence number of accessing list which is in the range of 1～199；access-list-name:the name of accessing list which is the character string and in the form of initial capitalized characters ([a-z, A-Z]), excluding space and quotation mark；**subitem** *subitem*:optional parameter, specifies the subitem in accessing list which is in the range of 2～127. If it is not specified, all subitems will be clear.

link-group { *access-list-number* | *access-list-name* } [**subitem** *subitem*] :means layer 2 accessing control list. access-list-number:accessing list serial number which is in the range of 222～299； access-list-name:name of accessing list. Character string is in the form of initial capitalized characters ([a-z, A-Z]), excluding space and quotation mark； **subitem** *subitem*:optional

parameter, specifies the subitem in accessing list which is in the range of 2～127. If it is not specified, all subitems will be clear.

【Command configuration mode】

Any configuration mode

【Usage】

Use this command to clear all or specified traffic statistics information.

【Example】

！Clear traffic statistics information of accessing list 1

Optiway#clear traffic-statistic ip-group 1

14.1.2 bandwidth egress

Use **line-rate** command to limit port speed and the total speed of sending packet. Use **no line-rate** command to cancel the configuration of speed limitation.

Bandwidth egress *target-rate*

no bandwidth egress

【Parameter】

target-rate:the total speed of sending packet which is in the range of 1～122,with the unit of Mbps

【Command configuration mode】

Interface configuration mode

【Usage】

Use this command to limit port speed and the total speed of sending packet.

【Example】

！Configure the speed of Ethernet 21 to be 12

Optiway(config-if-fastEthernet-1)#line-rate 12

14.1.3 mirrored-to

Use **mirrored-to** command to enable ACL identified flow. Use **no mirrored-to** command to cancel flow mirror.

mirrored-to { [**ip-group** access-list-number | access-list-name [**subitem** subitem]] [**link-group** access-list-number | access-list-name [**subitem** subitem]] } } [**interface** interface-num]

no mirrored-to {[**ip-group** access-list-number | access-list-name [**subitem** subitem]] [**link-group** access-list-number | access-list-name [**subitem** subitem]] } }

ip-group { *access-list-number* | *access-list-name* } [**subitem** *subitem*] :means standard or extended accessing control list. access-list-number:sequence number of accessing list which is in the range of 1～199；access-list-name:the name of accessing list which is the character string and in the form of initial capitalized characters ([a-z, A-Z]), excluding space and quotation mark；**subitem** *subitem*:optional parameter, specifies the subitem in accessing list which is in the range of 2～127. If it is not specified, all subitems will be clear.

link-group { *access-list-number* | *access-list-name* } [**subitem** *subitem*] :means layer 2 accessing control list. access-list-number:accessing list serial number which is in the range of 222～299；access-list-name:name of accessing list. Character string is in the form of initial capitalized characters ([a-z, A-Z]), excluding space and quotation mark；**subitem** *subitem*:optional parameter, specifies the subitem in accessing list which is in the range of 2～127. If it is not specified, all subitems will be clear.

interface { *interface-num* }:specified data flow destination mirror interface. interface-num is the interface number.

【Command configuration mode】

Global configuration mode

【Usage】

Use this command to flow mirror the data packet which matched specified accessing list regulations (it is only be effective for permit rules of accessing list). The interface of destination mirror cannot be Trunk or convergent interface. Switch can only support one destination mirror port. Mirror destination port must be specified when using this command to configure flow mirror for the first time.

【Example】

!Mirror flow the data packet which matches the permit rules of accessing list 1 to ethernet 1

Optiway(config)#mirrored-to ip-group 1 interface ethernet 2/1

14.1.4 queue-scheduler

Use **queue-scheduler** command to configure queue-scheduler mode and parameter. Use **no queue-scheduler** command to disable queue-scheduler.

queue-scheduler { **sp-wrr** queue1-weight queue2-weight queue3-weight | **wrr** queue1-weight queue2-weight queue3-weight queue4-weight }

no queue-scheduler

【Parameter】

sp-wrr *queue1-weight queue2-weight queue3-weight*:means the strict priority and weighted round robin. *Queue4* is strict-priority, others are weighted round

robin, and their default weight are: 22,32,52. queue1-weight:means the weight of the queue 1, that is the percentage of bandwidth of distribution；queue2-weight:means the weight of the queue 2, that is the percentage of bandwidth distribution；queue3-weight:means the weight of the queue 3, that is the percentage of bandwidth distribution.

wrr *queue1-weight queue2-weight queue3-weight queue4-weight*:Means the weighted round robin. queue1-weight:means the weight of queue 1, that is the percentage of bandwidth distribution；queue2-weight:means the weight of queue 2,that is the percentage of bandwidth distribution；queue3-weight:means the weight of queue 3, that is the percentage of bandwidth distribution；queue4-weight:Means the weight of queue 4, that is the percentage of bandwidth distribution

【Command configuration mode】

Global configuration mode

【Usage】

For weighted configuration, the sum of all the weighted is 122.

【Example】

！Configure queue-scheduler to be weighted round robin, and 4 weights to be 22,22,32,32

Optiway(config)#queue-scheduler wrr 22 22 32 32

14.1.5 queue-scheduler cos-map

Use **queue-scheduler cos-map** command to configure 4 queue numbers and cos-map to 8 packed-priority of IEEE822.1p.

queue-scheduler cos-map [*queue-number*] [*packed-priority*]

【Parameter】

queue-number:Range from 2 to 3

packed-priority:The priority defined by IEEE 822.1p ranges from 2 to 7

【Default】

The default mapping is the mapping defined by 822.1p:

822.1p:	2	1	2	3	4	5	6	7
packed-priority:	2	2	1	1	2	2	3	3

【Command configuration mode】

Global configuration mode

【Usage】

There are 4 default packed-priorities from 2 to 3. 3 is superlative. The superlative data in the buffer is preferential to send.

【Example】

！ Configure packed-priority 1 to mapped priority 6 of IEEE 822.1p

Optiway(config)#queue-scheduler cos-map 1 6

14.1.6 queue-scheduler dscp-map

Use this command to configure the mapping relationship between DSCP and 8 priority in IEEE 822.1p.

queue-scheduler dscp-map [*dscp-value*] [*packed-priority*]

【Parameter】

dscp-value:DSCP in ToS which is in the range of 2～63

packed-priority:The priority defined by IEEE 822.1p ranges from 2 to 7

【Default】

The default mapping relationship is that all DSCP map to priority 2.

【Command configuration mode】

Global configuration mode

【Usage】

Use this command together with queue-scheduler cos-map, which can get the mapping between dscp and hardware queue.

【Example】

！Configure dscp 2 to map to priority 5

Optiway(config)#queue-scheduler dscp-map 2 5

14.1.7 rate-limit

Use **rate-limit input** command to enable ACL flow identification to control flow, and different action for internal and external packet. Use **no rate-limit input** command to cancel flow control.

rate-limit input {[**ip-group** { *access-list-number* | *access-list-name* } [**subitem** *subitem*]] [**link-group** { *access-list-number* | *access-list-name* } [**subitem** *subitem*]] } } **target-rate** [**exceed-action** *action*]

no rate-limit input {[**ip-group** { *access-list-number* | *access-list-name* } [**subitem** *subitem*]] [**link-group** { *access-list-number* | *access-list-name* } [**subitem** *subitem*]] } }

【Parameter】

input:means to flow control the received packet of the port.

user-group { *access-list-number* | *access-list-name* } [**subitem** *subitem*]:means accessing control list defined by user.
access-list-number:accessing list serial number which is in the range of 322～

399；access-list-name:name of accessing list. Character string is in the form of initial capitalized characters ([a-z, A-Z]), excluding space and quotation mark；**subitem** *subitem*:optional parameter, specifies the subitem in accessing list which is in the range of 2～127. If it is not specified, all subitems will be clear.

ip-group { *access-list-number* | *access-list-name* } [**subitem** *subitem*] :means standard or extended accessing control list. access-list-number:sequence number of accessing list which is in the range of 1～199；access-list-name:the name of accessing list which is the character string and in the form of initial capitalized characters ([a-z, A-Z]), excluding space and quotation mark；**subitem** *subitem*:optional parameter, specifies the subitem in accessing list which is in the range of 2～127. If it is not specified, all subitems will be clear.

link-group { *access-list-number* | *access-list-name* } [**subitem** *subitem*] :means layer 2 accessing control list. access-list-number:accessing list serial number which is in the range of 222～299；access-list-name:name of accessing list. Character string is in the form of initial capitalized characters ([a-z, A-Z]), excluding space and quotation mark；**subitem** *subitem*:optional parameter, specifies the subitem in accessing list which is in the range of 2～127. If it is not specified, all subitems will be clear.

target-rate:configured normal flow with the unit of mbps. It is defaulted to be 64kpbs.

exceed-action *action*:optional parameter. Following actions will be adopted when the flow of data packet is beyond the configuration:

drop:drop the packet；

set-dscp-value value:configure new DSCP value.

【Command configuration mode】

Global configuration mode

【Usage】

Use this command to flow mirror the data packet which matched specified accessing list regulations (it is only be effective for permit rules of accessing list).

【Example】

！Flow control the data packet which matches the permit rules of accessing list 1. The normal flow is 64kbps. The data packet beyond this flow will be dropped.

Optiway(config)#rate-limit input ip-group 1 64 exceed-action drop

14.1.8 two-rate-policer mode

Use this command to configure two rate policer mode.

two-rate-policer mode { color-aware | color-blind }

【Parameter】

color-aware:aware the color of incoming packet.

color-blind:cannot aware the color of incoming packet.

【Default】

The default mode is color-blind mode.

【Command configuration mode】

Global configuration mode

【Usage】

Use this command to configure two rate policer mode. When color-aware

mode enables, dscp-map is enabled.

【Example】

！Configure two rate policer mode to be color-blind

Optiway(config)#two-rate-policer mode color-blind

14.1.9 two-rate-policer set-pre-color

Use this command to configure two rate policer to traffic monitor the color of incoming packet.

two-rate-policer set-pre-color *dscp-value* {green | yellow | red }

【Parameter】

dscp-value:dscp of the packet color to be configured.

green:mark packet to be green.

yellow:mark packet to be yellow.

red:mark packet to be red.

【Default】

The default color is green

【Command configuration mode】

Global configuration mode

【Usage】

Use this command to configure two rate policer to traffic monitor the color of incoming packet which can only worked in color-aware mode,when the incoming packet is configured to be green,the outputting packet color is the same as that in color-blind mode；when the incoming packet is configured to

be yellow,the speed of which is beyond pir, packet will turn to red and others are yellow;when configuring to be red,outputting packet is still red.

【Example】

！Configure packet whose incoming dscp is 4 to be yellow

Optiway(config)#two-rate-policer set-pre-color 4 yellow

14.1.10 **show qos-info all**

Use **show qos-info all** command to display all QoS configuration.

show qos-info all

【Command configuration mode】

Any configuration mode

【Usage】

Use this command to display all QoS configuration, including priority,redirection, flow statistics, flow mirror and copy packet to CPU.

【Example】

！Display all QoS configuration

Optiway#show qos-info all

14.1.11 **show qos-info mirrored-to**

Use **show qos-info mirrored-to** command to display flow mirror configuration.

show qos-info mirrored-to

【Command configuration mode】

Any configuration mode

【Usage】

Use this command to display flow mirror configuration, including flow mirror accessing list,flow mirror interface.

【Example】

！Display all flow mirror configuration

Optiway#show qos-info mirrored-to

14.1.12 show qos-info statistic

Use **show qos-info statistic** command to display all QoS statistics information.

show qos-info statistic

【Command configuration mode】

Any configuration mode

【Usage】

Use this command to display all QoS statistics information, including priority, redirection, flow statistics, flow mirror, and copy packet to CPU.

【Example】

！Display all QoS statistics information

Optiway(config)#show qos-info statistic

14.1.13 show qos-info traffic-copy-to-cpu

Use **show qos-info traffic-copy-to-cpu** command to display configuration of copying packet to CPU.

show qos-info traffic-copy-to-cpu

【Command configuration mode】

Any configuration mode

【Usage】

Use this command to display copying packet to CPU configuration, including copying packet to CPU accessing list.

【Example】

！Display copy packet to CPU configuration

Optiway#show qos-info traffic-copy-to-cpu

14.1.14 show qos-info traffic-priority

Use **show qos-info traffic-priority** command to display priority configuration.

show qos-info traffic-priority

【Command configuration mode】

Any configuration mode

【Usage】

Use this command to display copying packet to CPU configuration, including copying packet to CPU accessing list.

【Example】

！Display priority configuration

Optiway#show qos-interface traffic-priority

14.1.15 show qos-info traffic-redirect

Use **show qos-info traffic-redirect** command to display redirection configuration.

show qos-info traffic-redirect

【Command configuration mode】

Any configuration mode

【Usage】

Use this command to display redirection configuration, including accessing list of redirection flow and redirection port.

【Example】

！Display redirection configuration

Optiway#show qos-info traffic-redirect

14.1.16 show qos-info traffic-statistic

Use **show qos-info traffic-statistic** command to display flow statistics information.

show qos-info traffic-statistic

【Command configuration mode】

Any configuration mode

【Usage】

Use this command to display flow statistics, including accessing list of flow statistics and packet number.

【Example】

！Display the flow statistics information

Optiway#show qos-info traffic-statistic

14.1.17 show qos-interface all

Use **show qos-interface all** command to display QoS configuration of all ports.

show qos-interface [*interface-num*] all

【Parameter】

interface-num:the interface of switch.

【Command configuration mode】

Any configuration mode

【Usage】

If no parameter is input, this command will display all QoS configuration, includes: speed limit and rate limit.

【Example】

！Display all QoS configuration

Optiway#show qos-info all

14.1.18 show qos-interface line-rate

Use **show qos-interface line-rate** command to display line rate configuration of egress port.

show qos-interface [*interface-num*] line-rate

【Parameter】

interface-num:the interface of switch.

【Command configuration mode】

Any configuration mode

【Usage】

If no parameter is input, this command will display line rate configuration of egress port. If interface is input, this command will display line rate configuration of egress port of specified interface, includes: egredd port and its rate limit.

【Example】

！Display interface limit configuration

Optiway(config-if-ethernet-24)#show qos-interface line-rate

14.1.19 show qos-interface rate-limit

Use **show qos-interface rate-limit** command to display flow rate limit configuration.

show qos-interface [*interface-num*] rate-limit

【Parameter】

interface-num:the interface of switch.

【Command configuration mode】

Any configuration mode

【Usage】

If no parameter is input, this command will display interface flow speed limit. If interface is input, this command will display interface flow speed limit of specified interface, includes: interface flow speed limit accessing list, average speed rate and related monitor configuration.

【Example】

！Display interface flow speed limit configuration

Optiway#show qos-interface rate-limit

14.1.20 show qos-interface statistic

Use **show qos-interface statistic** command to display flow monitor statistics of all ports.

show qos-interface statistic

【Command configuration mode】

Any configuration mode

【Example】

！Display flow monitor statistics

Optiway(config)#show qos-interface statistic

14.1.21 show queue-scheduler

Use **show queue-scheduler** command to display the mode and the parameter of queue-scheduler.

show queue-scheduler

【Command configuration mode】

Any configuration mode

【Example】

！Display the mode and parameter of the queue-scheduler

Optiway#show queue-scheduler

Queue scheduling mode: strict-priority

14.1.22 show queue-scheduler cos-map

Use **show queue-scheduler cos-map** command to display the queue-scheduler cos-map.

show queue-scheduler cos-map

【Command configuration mode】

Any configuration mode

【Example】

！Display the queue-scheduler cos-map

Optiway(config)#show queue-scheduler cos-map

14.1.23 show queue-scheduler dscp-map

Display mapping relationship between queue scheduler and dscp.

show queue-scheduler dscp-map

【Command configuration mode】

Any configuration mode

【Example】

！Display mapping relationship between queue scheduler and dscp

Optiway(config)#show queue-scheduler dscp-map

14.1.24 show two-rate-policer

Use this command to display specified or all two rate policer

show two-rate-policer [*two-rate-policer-id*]

【Parameter】

two-rate-policer-id:two rate policer ID which is in the range of 2～255

【Command configuration mode】

Any configuration mode

【Example】

！Display all two rate policer

Optiway#show two-rate-policer

14.1.25 storm-control

Use **storm-control** command to configure broadcast/known multicast/unknown unicast/unknown multicast storm-control. Use **show interface** command to display storm-control information.

storm-control rate *target-rate*

storm-control { broadcast | multicast | dlf }

no storm-control { broadcast | multicast | dlf }

【Parameter】

broadcast:Configure broadcast storm-control

multicast:Configure known multicast storm-control

dlf:Configure unknown multicast storm-control

target-rate:The target rate of storm-control with the unit of Kbps

【Command configuration mode】

Interface configuration mode

【Example】

！ Configure storm-control rate of Ethernet 2/5 to be 1Kpps

Optiway(config-if-ethernet-2/5)#storm-control broadcast 1224

14.1.26 traffic-copy-to-cpu

Use **traffic-copy-to-cpu** command to enable ACL identification and copy the matched packet to CPU. Use **no traffic-copy-to-cpu** command to cancel the copy.

traffic-copy-to-cpu { [**ip-group** { *access-list-number* | *access-list-name* } [**subitem** *subitem*]] [**link-group** { *access-list-number* | *access-list-name* } [**subitem** *subitem*]] } }

no traffic-copy-to-cpu { [**ip-group** { *access-list-number* | *access-list-name* } [**subitem** *subitem*]] [**link-group** { *access-list-number* | *access-list-name* } [**subitem** *subitem*]] } }

【Parameter】

ip-group { *access-list-number* | *access-list-name* } [**subitem** *subitem*] :means standard or extended accessing control list. access-list-number:sequence number of accessing list which is in the range of 1～199；access-list-name:the name of accessing list which is the character string and in the form of initial capitalized characters ([a-z, A-Z]), excluding space and quotation mark；**subitem** *subitem*:optional parameter, specifies the subitem in accessing list which is in the range of 2～127. If it is not specified, all subitems will be clear.

link-group { *access-list-number* | *access-list-name* } [**subitem** *subitem*] :means layer 2 accessing control list. access-list-number:accessing list serial number which is in the range of 222～299；access-list-name:name of accessing list. Character string is in the form of initial capitalized characters ([a-z, A-Z]), excluding space and quotation mark；**subitem** *subitem*:optional parameter, specifies the subitem in accessing list which is in the range of 2～

127. If it is not specified, all subitems will be clear.

【Command configuration mode】

Global configuration mode

【Usage】

Use this command to copy specified accessing list packet to CPU (it is only be effective for permit rules of accessing list).

【Example】

！Copy the data packet which matches the permit rules of accessing list 1 to CPU

Optiway(config)#traffic-copy-to-cpu ip-group 1

14.1.27 traffic-priority

Use **traffic-priority** command to enable ACL to mark priority. Use **no traffic-priority** command to cancel priority.

traffic-priority { [**ip-group** { *access-list-number* | *access-list-name* } [**subitem** *subitem*]] [**link-group** { *access-list-number* | *access-list-name* } [**subitem** *subitem*]] } { [**dscp** *dscp-value* | **precedence** { *pre-value* | from-cos }] [**cos** { *pre-value* | from-ipprec }] [**local-precedence** *pre-value*] }

no traffic-priority { { [**ip-group** { *access-list-number* | *access-list-name* } [**subitem** *subitem*]] [**link-group** { *access-list-number* | *access-list-name* } [**subitem** *subitem*]] } }

【Parameter】

input:means to flow control the received packet of the port.

ip-group { *access-list-number* | *access-list-name* } [**subitem** *subitem*] :means standard or extended accessing control list.

access-list-number:sequence number of accessing list which is in the range of 1～199；access-list-name:the name of accessing list which is the character string and in the form of initial capitalized characters ([a-z, A-Z]), excluding space and quotation mark；**subitem** *subitem*:optional parameter, specifies the subitem in accessing list which is in the range of 2～127. If it is not specified, all subitems will be clear.

link-group { *access-list-number* | *access-list-name* } [**subitem** *subitem*] :means layer 2 accessing control list. access-list-number:accessing list serial number which is in the range of 222～299；access-list-name:name of accessing list. Character string is in the form of initial capitalized characters ([a-z, A-Z]), excluding space and quotation mark；**subitem** *subitem*:optional parameter, specifies the subitem in accessing list which is in the range of 2～127. If it is not specified, all subitems will be clear.

dscp *dscp-value*:configure DSCP priority which is in the range of 2～63.

precedence { *pre-value* | from-cos }:configure IP priority. pre-value is IP priority which is in the range of 2～7；from-cos means configure IP priority to be the same as 822.1p priority.

cos { *pre-value* | from-ipprec }:configure 822.1p priority. *pre-value* is 822.1p priority which is in the range of 2～7；from-ipprec means the priority of 822.1p and IP is the same.

local-precedence *pre-value*:configure local priority which is in the range of 2～7.

【Command configuration mode】

Global configuration mode

【Usage】

Use this command to mark priority to specified ACL.(it is only be effective for permit rules of accessing list). There are three types of priority (dscp, cos, IP

priority and local priority). Switch can locate packet to interface outputting queue according to the cos value (that is 822.1p priority) and also can locate packet to corresponding outputting queue according to the specified local priority. If both 822.1p priority and local priority are configured, 822.1p priority will be precedent to use.

【Example】

！Configure the priority of data packet which matches the permit rules of accessing list 1 to be 2

Optiway(config)#traffic-priority ip-group 1 local-precedence 2

14.1.28 **traffic-redirect**

【Parameter】

ip-group { *access-list-number* | *access-list-name* } [**subitem** *subitem*] :means standard or extended accessing control list. access-list-number:sequence number of accessing list which is in the range of 1～199；access-list-name:the name of accessing list which is the character string and in the form of initial capitalized characters ([a-z, A-Z]), excluding space and quotation mark；**subitem** *subitem*:optional parameter, specifies the subitem in accessing list which is in the range of 2～127. If it is not specified, all subitems will be clear.

link-group { *access-list-number* | *access-list-name* } [**subitem** *subitem*] :means layer 2 accessing control list. access-list-number:accessing list serial number which is in the range of 222～299；access-list-name:name of accessing list. Character string is in the form of initial capitalized characters ([a-z, A-Z]), excluding space and quotation mark；**subitem** *subitem*:optional parameter, specifies the subitem in accessing list which is in the range of 2～127. If it is not specified, all subitems will be clear.

cpu:means redirect to CPU.

interface *interface-num*:The interface the packet to be redirect to. interface-num is interface number.

【Command configuration mode】

Global configuration mode

【Usage】

Use this command to redirect the data packet which matched specified accessing list regulations (it is only be effective for permit rules of accessing list). The redirect can be used in some protocol packet needed handle by CPU or the packet needed CPU to find routing.

【Example】

！Redirect the data packet which matches the permit rules of accessing list 1 to ethernet 1

Optiway(config)#traffic-redirect ip-group 1 interface ethernet 2/1

14.1.29 traffic-statistic

Use **traffic-statistic** command to enable ACL identification to statistic traffic. Use **no traffic-statistic** command to cancel traffic statistics.

traffic-statistic {[**ip-group** { access-list-number | access-list-name } [**subitem** subitem]] [**link-group** { access-list-number | access-list-name } [**subitem** subitem]] } }

no traffic-statistic { [**ip-group** { *access-list-number* | *access-list-name* } [**subitem** *subitem*]] [**link-group** { *access-list-number* | *access-list-name* } [**subitem** *subitem*]] } }

【Parameter】

ip-group { *access-list-number* | *access-list-name* } [**subitem**

subitem] :means standard or extended accessing control list. access-list-number:sequence number of accessing list which is in the range of 1～199；access-list-name:the name of accessing list which is the character string and in the form of initial capitalized characters ([a-z, A-Z]), excluding space and quotation mark；**subitem** *subitem*:optional parameter, specifies the subitem in accessing list which is in the range of 2～127. If it is not specified, all subitems will be clear.

link-group { *access-list-number* | *access-list-name* } [**subitem** *subitem*] :means layer 2 accessing control list. access-list-number:accessing list serial number which is in the range of 222～299；access-list-name:name of accessing list. Character string is in the form of initial capitalized characters ([a-z, A-Z]), excluding space and quotation mark；**subitem** *subitem*:optional parameter, specifies the subitem in accessing list which is in the range of 2～127. If it is not specified, all subitems will be clear.

【Command configuration mode】

Global configuration mode

【Usage】

Use this command to statistic traffic the data packet which matched specified accessing list regulations (it is only be effective for permit rules of accessing list). The new configuration of traffic statistics will eliminate corresponding traffic statistics.

【Example】

！Statistic traffic of the data packet which matches the permit rules of accessing list 1

Optiway(config)#traffic-statistic ip-group 1

Chapter 15 STP Configuration Command

15.1 STP Configuration Command

STP（Spanning Tree protocol）configuration command includes:

- **show spanning-tree interface**
- **show spanning-tree remote-loop-detect interface**
- **spanning-tree**
- **spanning-tree cost**
- **spanning-tree forward-time**
- **spanning-tree hello-time**
- **spanning-tree max-age**
- **spanning-tree port-priority**
- **spanning-tree mcheck**
- **spanning-tree point-to-point**
- **spanning-tree portfast**
- **spanning-tree transmit**
- **spanning-tree priority**
- **spanning-tree mode**
- **clear spanning-tree**

15.1.1 show spanning-tree interface

Use **show spanning-tree interface** command to display the information of current STP protocol.

show spanning-tree interface [*interface-list*]

show spanning-tree interface [*interface-list*]

【Parameter】

interface-list:List of Ethernet ports to be added to or removed from a VLAN. This keyword needed to be provided in the form of interface-type + interface-number. Interface-type is Ethernet and interface-number is slot-num/port-num, in which slot-num is in the range of 2 to 2, and port-num is in the range of 1 to 24. Seriate(sequential?) interfaces with the same type can be linked by to keyword, but the port number to the right of the to keyword must be larger than the one to the left of the keyword, and this argument only can be repeated for up to 3 times.

【Command configuration mode】

Any configuration mode

【Usage】

Show spanning-tree interface [*interface-list*] command to display the information of spanning-tree. Keyword “interface-list” is optional. If it is lacked, information of interfaces is displayed, or only the information of specified interface is displayed.

【Example】

！Display the information of spanning-tree

Optiway#show spanning-tree interface ethernet 2/7

15.1.2 show spanning-tree remote-loop-detect interface

Use this command to display remote loop detect.

Show spanning-tree remote-loop-detect interface [*interface-list*]

【Parameter】

interface-list:the interface list to be displayed which means manyethernet interface

interface-list :List of Ethernet ports to be added to or removed from a VLAN. This keyword needed to be provided in the form of interface-type + interface-number. Interface-type is Ethernet and interface-number is slot-num/port-num, in which slot-num is in the range of 2 to 2, and port-num is in the range of 1 to 24. Seriate(sequential) interfaces with the same type can be linked by to keyword, but the port number to the right of the to keyword must be larger than the one to the left of the keyword, and this argument only can be repeated for up to 3 times.

【Command configuration mode】

Any configuration mode

【Usage】

Use this command to display remote loop detect and whether interface is block caused by loop

【Example】

！Display remote loop detect of interface 1

Optiway(config)#show spanning-tree remote-loop-detect interface e 2/1

15.1.3 spanning-tree

Use **spanning-tree** command to enable STP globally or on a port.

Use **no spanning-tree** command disable STP globally or on a port.

spanning-tree

no spanning-tree

【Default】

STP is enabled globally

【Command configuration mode】

Global configuration mode, interface configuration mode

【Example】

！ Enable STP globally

Optiway(config)#spanning-tree

！ Disable STP on Ethernet 2/8

Optiway(config-if-ethernet-2/8)#no spanning-tree

15.1.4 spanning-tree cost

Use **spanning-tree cost** command to configure the path cost of the current port in a specified spanning tree. Use **no spanning-tree cost** command to restore to the default path cost of the current port in the specified spanning tree.

spanning-tree cost *cost*

no spanning-tree cost

【Parameter】

cost:Path cost to be configured for the port. This keyword ranges from 1 to 65535

【Default】

In IEEE 822.1D protocol, the default cost is determined by the speed of the port. The port with the speed 12M have the cost of 122,122M, 19.

【Command configuration mode】

Interface configuration mode

【Usage】

Default cost is suggested to use.

【Example】

！Configure path cost of Ethernet 2/8 to 22

Optiway(config-if-ethernet-2/8)#spanning-tree cost 22

15.1.5 spanning-tree forward-time

Use **spanning-tree forward-time** command to configure the Forward delay of the switch. Use **no spanning-tree forward-time** command to restore to the default forward delay.

spanning-tree forward-time *seconds*

no spanning-tree forward-time

【Parameter】

seconds: Forward Delay in seconds to be configured. This keyword ranges from 4 to 32 seconds

【Default】

The default forward delay is 15 seconds

【Command configuration mode】

Global configuration mode

【Usage】

When this switch is the root bridge, port state transition period is the Forward Delay time, which is determined by the diameter of the switched network. The

longer the diameter is, the longer the time is. The default forward delay time, 15 seconds is suggested to use.

 Caution:Forward Delay ≥ Hello Time + 2.

【Example】

！Configure forward delay to 22 seconds

Optiway(config)#spanning-tree forward-time 22

15.1.6 spanning-tree hello-time

Use **spanning-tree hello-time** coammand to configure the hello time of the switch. Use **no spanning-tree hello-time** command to restore to the default hello time.

spanning-tree hello-time *seconds*

no spanning-tree hello-time

【Parameter】

seconds:Hello Time in seconds to be configured. This keyword ranges from 1 to 12 seconds.

【Default】

The default hello time is 2 seconds

【Command configuration mode】

Global configuration mode

【Usage】

The system periodically sents STP messages. The period of a root bridge sending STP messages is the hello time. Hello time is suggested to use 2

seconds.

 Caution:Hello Time ≤ ForwardDelay – 2.

【Example】

！ Configure Hello Time to 8 seconds

Optiway(config)#spanning-tree hello-time 8

15.1.7 spanning-tree max-age

Use **spanning-tree max-age** command to configure Max Age of the switch. Use **no spanning-tree max-age** command to restore to the default Max Age.

spanning-tree max-age *seconds*

no spanning-tree max-age

【Parameter】

seconds:Means Max Age in seconds to be configured. This keyword ranges from 6 to 42 seconds

【Default】

The default Max Age is 22 seconds

【Command configuration mode】

Global configuration mode

【Usage】

Max Age is used to configure the longest aging interval of STP. Dropping message when overtiming. The STP will be frequently accounts and take crowded network to be link fault, if the value is too small. If the value is too large, the link fault cannot be known timely. Max Age is determined by

diameter of network, and the default time of 22 seconds is suggested.

 Caution:2*(Hello Time + 1) ≤ Max Age ≤ 2*(ForwardDelay – 1)

【Example】

！Configure the Max Age to 12 seconds

Optiway(config)#spanning-tree max-age 12

15.1.8 spanning-tree port-priority

Use **spanning-tree port-priority** command to configure the port priority of the current port in the specified spanning tree. Use **no spanning-tree port-priority** command to restore the current port to the default port priority in the specified spanning tree.

spanning-tree port-priority *port-priority*

no spanning-tree port-priority

【Parameter】

port-priority:Configure the port priority. It ranges from 2 to 255

【Default】

The default port priority of a port in any spanning tree is 128

【Command configuration mode】

Interface configuration mode

【Usage】

The smaller the value of priority is, the superior the priority is, and the port is easier to be a root port.

【Example】

！Configure the port priority of Ethernet 2/1 in STP to 64

Optiway(config-if-ethernet-2/1)#spanning-tree port-priority 64

15.1.9 spanning-tree mcheck

When operation RSTP protocol, and port is in the compatible mode. Use **spanning-tree mcheck** command to force the port sent RSTP message.

spanning-tree mcheck

【Command configuration mode】

Interface configuration mode

【Example】

！Configure Ethernet 2/7 to send RSTP message

Optiway(config-if-ethernet-2/7)#spanning-tree mcheck

15.1.10 spanning-tree point-to-point

Use **spanning-tree point-to-point** command to configure the link connected to the current Ethernet port to be a point-to-point link.

spanning-tree point-to-point { auto | forcefalse | falsetrue }

no spanning-tree point-to-point

【Parameter】

auto:Network bridge auto-detect whether or not the link connected to the current Ethernet port is a point-to-point link.

forcefalse:Specifies that the link connected to the current Ethernet port is not a point-to-point link.

forcetrue: Specifies that the link connected to the current Ethernet port is a point-to-point link.

【Default】

Auto

【Command configuration mode】

Interface configuration mode

【Example】

！ Configure the link connected to Ethernet 2/7 as a point-to-point link

Optiway(config-if-ethernet-2/7)#spanning-tree point-to-point forcetrue

15.1.11 spanning-tree portfast

Use **spanning-tree portfast** command to configure the current port as an edge port.

spanning-tree portfast

no spanning-tree portfast

【Default】

All Ethernet ports of a switch are non-edge ports.

【Command configuration mode】

Interface configuration mode

【Usage】

Edge port can be in transmitting state in linkup in 3 seconds, and it changes into non-edge port after receiving STP message.

【Example】

！ Configure Ethernet 2/7 as a non-edge port.

Optiway(config-if-ethernet-2/7)#spanning-tree portfast

15.1.12 spanning-tree transit-limit

Use **spanning-tree transit-limit** command to configure the maximum number of configuration BPDUs the current port can transmit in each Hello time.

spanning-tree transit-limit *max-bpdus*

no spanning-tree transit-limit

【Parameter】

max-bpdus:the number of BPDU ranges from 1 to 255.

【Default】

3

【Command configuration mode】

Interface configuration mode

【Example】

！ Configure the maximum number of configuration BPDUs that can be transmitted by the Ethernet 2/7 in each Hello time to 5

Optiway(config-if-ethernet-2/7)#spanning-tree transit-limit 5

15.1.13 spanning-tree priority

Use **spanning-tree priority** command to configure the priority of the switch in the specified spanning tree. Use **no spanning-tree priority** command to restore to the default priority in the specified spanning tree.

spanning-tree priority *bridge-priority*

no spanning-tree priority

【Parameter】

bridge-priority:Switch priority to be configured. This keyword rsnges from 2 to 61442,and must be a multiple of 4296.

【Default】

32768

【Command configuration mode】

Global configuration mode

【Usage】

Configure STP priority when STP enables, and the inferior priority of the switch can be the root bridge.

【Example】

！Configure the priority of the switch in spanning tree to 4296

Optiway(config)#spanning-tree priority 4296

15.1.14 **spanning-tree mode**

Use **spanning-tree mode** command to configure the STP operation mode.

spanning-tree mode { rstp | stp }

no spanning-tree mode

【Parameter】

rstp:Enable the rstp-campatible mode

stp:Enable the STP-compatible mode

【Default】

rstp

【Command configuration mode】

Global configuration mode

【Example】

！Configure the switch to operation in STP-compatible mode

Optiway(config)#spanning-tree mode stp

15.1.15 spanning-tree remote-loop-detect

Use **spanning-tree remote-loop-detect** command to enable remote loop detect. Use **no spanning-tree remote-loop-detect** command to disable remote loop detect.

spanning-tree remote-loop-detect

no spanning-tree remote-loop-detect

【Command configuration mode】

Global configuration mode and interface configuration mode

【Usage】

Batch processthe interface in global configuration mode needed keyword.

【Example】

！Enable spanning-tree remote-loop-detect interface of Ethernet 2/1, and ethernet 2/3

Optiway(config)#spanning-tree remote-loop-detect interface ethernet 2/1 ethernet 2/3

！ Disable remote-loop-detect of Ethernet 2/1

Optiway(config-if-ethernet-2/1)#no spanning-tree remote-loop-detect

15.1.16 clear spanning-tree

Use **clear spanning-tree** command to clear STP information

clear spanning-tree

clear spanning-tree interface *interface-list*

【Parameter】

interface-list:List of Ethernet ports to be added to or removed from a VLAN. This keyword needed to be provided in the form of interface-type + interface-number. Interface-type is Ethernet and interface-number is slot-num/port-num, in which slot-num is in the range of 2 to 2, and port-num is in the range of 1 to 24. Seriate(sequential?) interfaces with the same type can be linked by to keyword, but the port number to the right of the to keyword must be larger than the one to the left of the keyword, and this argument only can be repeated for up to 3 times.

【Command configuration mode】

Global configuration mode

【Example】

！ Clear spanning-tree information

Optiway(config)#clear spanning-tree

15.2 MSTP Cconfiguration Command

MSTP（Multiple spanning Tree protocol）configuration command includes:

- **spanning-tree mst forward-time**

- **spanning-tree mst hello-time**
- **spanning-tree mst max-age**
- **spanning-tree mst max-hops**
- **spanning-tree mst name**
- **spanning-tree mst revision**
- **spanning-tree mst instance vlan**
- **spanning-tree mst instance priority**
- **spanning-tree mst portfast**
- **spanning-tree mst link-type**
- **spanning-tree mst external cost**
- **spanning-tree mst instance cost**
- spanning-tree mst instance port-priority
- show spanning-tree mst config-id
- **show spanning-tree mst instance interface**

Following commands:

- **spanning-tree mst forward-time；**
- **spanning-tree mst hello-time；**
- **spanning-tree mst max-age；**
- **spanning-tree mst portfast；**
- **spanning-tree mst link-type**

Please refer to corresponding commands in SST:

- **spanning-tree forward-time；**
- **spanning-tree hello-time；**
- **spanning-tree max-age；**

- **spanning-tree portfast**;
- spanning-tree point-to-point

Here will not explain detailedly.

15.2.1 spanning-tree mst max-hops

Use **spanning-tree mst max-hops** command to configure the max-hops of MSTP packet.

spanning-tree mst max-hops *max-hops*

no spanning-tree mst max-hops

【Parameter】

max-hops:the hops of MSTP packet which is in the range of 2-255

【Default】

The default hops is 22

【Command configuration mode】

Global configuration mode

【Example】

！Configure the max-hops of MSTP packet to be 12

Optiway(config)#spanning-tree mst max-hops 12

15.2.2 spanning-tree mst name

Use **spanning-tree mst name** command to configure MST name of MSTP.

spanning-tree mst name *name*

no spanning-tree mst name

【Parameter】

Name: district name of MSTP which is one part of MSTP configuration. It is a character string of 32 bytes.

【Default】

It is defaulted to have no name.

【Command configuration mode】

Global configuration mode

【Example】

！Configure MSTP name to be greennet

Optiway(config)#spanning-tree mst name greennet

15.2.3 spanning-tree mst revision

Use **spanning-tree mst revision** command to configure the revision level of MSTP.

spanning-tree mst revision *revision-level*

no spanning-tree mst revision

【Parameter】

revision-level:MSTP revision level which is one of MSTP and it is the integer number between 2 to 65535.

【Default】

The default value is 2.

【Command configuration mode】

Global configuration mode

【Example】

！Configure revision level of MSTP to be 12

Optiway(config)#spanning-tree mst revision 12

15.2.4 spanning-tree mst instance vlan

Use **spanning-tree mst instance** command to configure the mapping relations between MSTP instance and VLAN.

spanning-tree mst instance *instance-num* vlan *vlan-list*

no spanning-tree mst instance *instance-num* vlan *vlan-list*

【Parameter】

instance-num:MSTP instance number which is in the range of 1-15

vlan-list:vlan-list can be discrete number, a sequential number, and the mixture of both. Discrete number can be separated by comma, and sequential number can be separated by “-”, such as: 2, 5, 8, 12-22

【Default】

All vlan mapped to MSTP instance 2

【Command configuration mode】

Global configuration mode

【Example】

！Configure vlan 2-7 mapping to MSTP instance 2

Optiway(config)#spanning-tree mst instance 2 vlan 2-7

15.2.5 spanning-tree mst instance *instance-num* priority

Use **spanning-tree mst instance** command to configure the priority of

networkbridge in some MSTP instance.

spanning-tree mst instance *instance-num* priority *priority*

no spanning-tree mst instance *instance-num* priority

【Parameter】

instance-num:MSTP instance number which is in the range of 2-15

priority:the priority of network bridge which is the integer times of 4296 in the range of 2-61442

【Default】

The priority of network bridge in each instance is 32768.

【Command configuration mode】

Global configuration mode

【Example】

！Configure the priority of network bridge in instance 2 is 4296

Optiway(config)#spanning-tree mst instance 2 priority 4296

15.2.6 spanning-tree mst external cost

Use **spanning-tree mst external cost** command to configure external cost of port.

spanning-tree mst external cost *external-cost*

no spanning-tree mst external cost

【Parameter】

external-cost:external cost of port which is in the range of 1-222222222.

【Default】

The external cost of port is 222222.

【Command configuration mode】

Interface configuration mode

【Example】

！Configure the external cost of port 2 to be 222

Optiway(config-if-ethernet-2/2)#spanning-tree mst external cost 222

15.2.7 spanning-tree mst instance cost

Use **spanning-tree mst instance** command to configure cost for port in each instance.

spanning-tree mst instance *instance-num* cost *cost*

no spanning-tree mst instance *instance-num* cost

【Parameter】

instance-num:MSTP instance number which is in the range of 2-15

cost:port cost which is in the range of 1-222222222

【Default】

The cost for port in each instance is 222222

【Command configuration mode】

Interface configuration mode

【Example】

！Configure the cost for port 2 in instance 1 to be 222

Optiway(config-if-ethernet-2/2)#spanning-tree mst instance 1 cost 222

15.2.8 spanning-tree mst instance port-priority

Use **spanning-tree mst instance port-priority** command to configure the priority of port in STP instance.

spanning-tree mst instance *instance-num* port-priority *priority*

no spanning-tree mst instance *instance-num* port-priority

【Parameter】

instance-num:MSTP instance number which is in the range of 2-15

priority:port priority which is the integer times of 16 and is in the range of 1-242

【Default】

The priority of port in each instance is 128

【Command configuration mode】

Interface configuration mode

【Example】

！Configure the priority of port 2 in instance 1 to be 16

Optiway(config-if-ethernet-2/2)#spanning-tree mst instance 1 port-priority 16

15.2.9 show spanning-tree mst config-id

Use **show spanning-tree mst config-id** command to display MSTP config-id. MSTP config-id includes: MSTP revision level, MSTP config-name and the mapping relations between STP instance and VLAN.

show spanning-tree mst config-id

【Command configuration mode】

Any configuration mode

【Example】

！Display the config-id

Optiway(config)#show spanning-tree mst config-id

15.2.10 show spanning-tree mst instance interface

Use **show spanning-tree mst instance** command to display port information in some instance.

show spanning-tree mst instance *instance-num* interface [*interface-list*]

【Parameter】

interface-num:List of Ethernet ports to be added to or removed from a VLAN. This keyword needed to be provided in the form of interface-type + interface-number. Interface-type is Ethernet and interface-number is device/slot-num/port-num, in which device is stackable device number whichi is in the range of 2 to 7, slot-num is in the range of 2 to 2, and port-num is in the range of 1 to 24. Seriate interfaces with the same type can be linked by to keyword, but the port number to the right of the to keyword must be larger than the one to the left of the keyword, and this argument only can be repeated for up to 3 times.

【Command configuration mode】

Any configuration mode

【Example】

！Display the information of port 1 in MSTP instance 2

Optiway(config)#show spanning-tree mst instance 2 interface ethernet 2/1

Chapter 16 822.1X Configuration Command

16.1 Domain Configuration Command

Domainn configuration command includes:

- **aaa**
- **access-limit**
- **default domain-name enable**
- **domain**
- **show domain**
- **radius host binding**
- **state**

16.1.1 aaa

Use **aaa** command to enter AAA configuration mode

aaa

【Command configuration mode】

Global configuration mode

【Usage】

Enter AAA configuration mode to do related configuration

【Example】

！Enter AAA configuration mode

Optiway(config)#aaa

Optiway(config-aaa)#

16.1.2 access-limit

Use **access-limit enable** command to configure the maximum number of access user that can be contained in current domain.

access-limit enable *max-link*

access-limit disable

【Parameter】

max-link: the maximum number of access user that can be contained in current domain ranges from 1 to 642

【Default】

disable,means no limitation

【Command configuration mode】

Domain configuration mode

【Usage】

A domain can limit the maximum number of access user that can be contained in current domain. The related link with the domain is the domain name of the authenticate username must be the current domain and using its authentication, authorization and accounting. If there is no related link to the domain, the number of access user can be modified; if there are several related link, the new limitation cannot be conflict with the syatem operation, such as: there are 8 related links, the new limitatiom of the link number must be larger or qual to 8 or non-limitation. Use state command to change it into smaller one after shutdown related link.

【Example】

！ Configure the maximum number of access user that can be contained in domain green.com to 522

Optiway(config-aaa-green.com)#access-limit enable 522

16.1.3 default domain-name enbale

Use **default domain-name enable** command to configure a existed domain to be default domain. If the domain doesn't exist, the configuration fails. Use **default domain-name disable** command to disable the default domain.

default domain-name enable *domain-name*

default domain-name disable

【Parameter】

domain-name: the name of the domain

【Command configuration mode】

AAA configuration mode

【Usage】

When the default domain name is disabled, switch will not deal with the invalid message, if the username goes without the domain name. After the default domain name is enabling, switch will add @ and default domain name to a username wothout a domain name to authenticate. To configure a default domain which must be existed, or the configuration fails.

【Example】

！ Configure default domain name to be green.com and enable the default domain

Optiway(config-aaa)#default domain-name enable green.com

！ Disable default domain name

Optiway(config-aaa)#default domain-name disable

【Related command】

domain

16.1.4 **domain**

Use **domain** command to enter AAA configuration mode. If it doesn't exist, create it. Use **no domain** command to remove the domain.

domain domain-name

no domain domain-name

【Parameter】

domain-name: the name of the domain ranges from 1 to 24 charaters, no difference in upper-case type and lower case letters, and without space.

【Command configuration mode】

AAA configuration mode

【Usage】

Enter domain configuratuin mode to configure authtication and accounting. If the domain doesn't exist, create it, and then enter it. At most 8 domains are allowed. The configuration of each domain can be different, to realise multiple ISP operation.

Add a domian in term of the need, no domain existed by default.

After the creation of a domain, use state active to activate it before use.

【Example】

！ Create domain with the name of green.com

Optiway(config-aaa)#domain green.com

Optiway(config-aaa-green.com)#

！Remove domain with the name of green.com

Optiway(config-aaa)#no domain green.com

【Related command】

radius host, state

16.1.5 **show domain**

Use **show domain** command to display the configuration of the domain, such as: domain name, corresponding RADIUS server, and domain activation.

show domain [*domain-name*]

【Parameter】

domain-name:The name of the domain

【Command configuration mode】

Any configuration mode

【Example】

！Display the configuration of green.com

Optiway(config-aaa-green.com)#show domain

16.1.6 **radius host binding**

Use **radius host binding** command to configure RADIUS authtication and accounting.

radius host binding *radius-scheme*

【Parameter】

radius-scheme: the name of RADIUS authentication and accounting. It must be existed.

【Command configuration mode】

Domain configuration mode

【Example】

！Configure current domain to use RADIUS configuration of “green”

Optiway(config-aaa-green.com)#radius host binding green

【Related command】

radius host（RADIUS configuration mode）

16.1.7 **state**

Use **state** command to configure the state of the domain to be active or block.

state { active | block }

【Parameter】

active:active state,allow the authentication of the domain user.

block:block stste,not allow the authentication of the domain user.

【Default】

The default state of the created domain is block, and uses this command to activate it before use. It is to avoid using the unconfigured domain in configuring. Activate it after all configuration finished.

【Command configuration mode】

Domain configuration mode

【Usage】

Use state active command to activate domain before used.

【Example】

！Activate green.com

Optiway(config-aaa-green.com)#state active

【Related command】

domain

16.2 RADIUS Server Configuration Command

RADIUS server configuration command includes:

- **accounting-on**
- **acct-secret-key**
- **auth-secret-key**
- **dnrate-value**
- **h3c-cams**
- **nas-ipaddress**
- **primary-acct-ip**
- **primary-auth-ip**
- **show radius attribute**
- **show radius config-attribute**
- **show radius host**
- **uprate-value**
- **radius 8021p**
- **radius accounting**
- **radius attribute**

- **radius bandwidth-limit**
- **radius config-attribute**
- **radius host**
- **radius mac-address-number**
- **radius server-disconnect drop 1x**
- **radius vlan**
- **realtime-account**
- **second-acct-ip**
- **second-auth-ip**
- **username-format**

16.2.1 accounting-on

This command is to configure to send Accounting-On packets to RADIUS server after device reboots, it requires users to off line to solve on line users can't logo in with authentication after device reboots.

accounting-on *{ disable | enable }*

【Parameter】

enable:start function

disable:close function

【Default】

By default, it disables

【Command mode】

AAA configuration mode

【Example】

！ Enable

OptiWay(config-aaa)# accounting-on enable

16.2.2 **acct-secret-key**

This command is to configure accounting key of RADIUS server, with command **no** means to delete this operation.

acct-secret-key *key*

no acct-secret-key

【Parameter】

key: 1~16 characters

【Default】

By default, it is none

【Command mode】

RADIUS server configuration mode

【Example】

！ Configure accounting key of RADIUS server as 123

OptiWay(config-aaa-radius-green)#acct-secret-key 123

16.2.3 **auth-secret-key**

This command is to configure authenticate key of RADIUS server, with command **no** means to delete this operation.

auth-secret-key *key*

no auth-secret-key

【Parameter】

key: 1~16 characters

【Default】

By default, it is none

【Command mode】

RADIUS server configuration mode

【Example】

！ Configure authenticate key of RADIUS server as 123

OptiWay(config-aaa-radius-green)#auth-secret-key 123

16.2.4 **dnrate-value**

Campatible with H3C Cams RADIUS server,use this command to configure downlink bandwidth about Vendor Specific attribute id in RADIUS packets.

dnrate-value *value*

【Parameter】

vlaue:attribute id,the range is 1~32

【Default】

By default, it is 5

【Command mode】

AAA configuration mode

【Example】

！ Configure downlink bandwidth attribute id 7 compatible with H3C Cams

OptiWay(config-aaa)#dnrate-value 7

【Commands】

h3c-cams

16.2.5 h3c-cams

When RADIUS server uses H3C Cams , this command to configure compatible mode to finish some special operation.

h3c-cams *{ disable | enable }*

【Parameter】

enable:start function

disable:close function

【Default】

By default , it disables

【Command mode】

AAA configuration mode

【Example】

！Enable H3C Cams compatible mode

OptiWay(config-aaa)#h3c-cams enable

16.2.6 nas-ipaddress

This command is to configure to send packets about NAS IPAddress attribute id, with command **no** means to delete the operation.

nas-ipaddress *nas-ip*

no nas-ipaddress

【Parameter】

nas-ip: IP address

【Default】

By default, it is none, it means device IP address

【Command mode】

RADIUS server configuration mode

【Example】

！Configure the value as 192.168.0.100

OptiWay(config-aaa-radius-green)# nas-ipaddress 192.168.0.100

16.2.7 primary-acct-ip

This command is to configure accounting IP address and port in RADIUS server, with command **no** means to delete related configuration.

primary-acct-ip *server-ip accounting-port*

no primary-acct-ip

【Parameter】

server-ip:accounting RADIUS server IP address

accounting-port:authentication port ,the range is :1～65535

【Default】

By default, accounting port is 1813

【Command mode】

RADIUS server configuration mode

【Example】

！Configure accounting RADIUS server primary IP address is 192.168.0.100,accouting port is 1813

OptiWay(config-aaa-radius-green)#primary-acct-ip 192.168.0.100 1813

16.2.8 primary-auth-ip

This command is to configure IP address and port for primary authentication, with command **no** means to delete related configuration.

primary-auth-ip *server-ip authentication-port*

no primary-auth-ip

【Parameter】

server-ip:primary RADIUS server IP address

authentication-port:authentication port,the range is :1～65535

【Default】

By default, authentication port is 1812

【Command mode】

RADIUS server configuration mode

【Example】

！Configure IP address as 192.168.0.100 for primary authentication, authentication port is 1812

OptiWay(config-aaa-radius-green)#primary-auth-ip 192.168.0.100 1812

16.2.9 show radius attribute

This command is to display attribution configuration compatible with H3C Cam, now it only displays to send H3C client version to RADIUS server or not.

show radius attribute

【Parameter】

None

【Command mode】

All command mode

【Example】

！Display sending H3C client version to RADIUS server or not

OptiWay(config)# show radius attribute

16.2.10 show radius config-attribute

This command is to display attribution configuration about RADIUS,such as accounting , priority, VLAN etc.

show radius config-attribute

【Parameter】

None

【Command mode】

All command mode

【Example】

！Display attribution configuration about RADIUS

OptiWay(config)# show radius config-attribute

16.2.11 show radius host

This command is to display RADIUS server information, including RADIUS server primary IP address, secondary IP address, authentication port, accounting port, accounting key etc.

show radius host [*radius-scheme*]

【Parameter】

radius-scheme:RADIUS server name

【Command mode】

All command mode

【Example】

！Display RADIUS server information

OptiWay(config-aaa-radius-default)#show radius host

16.2.12 uprate-value

Campatible with H3C Cams RADIUS server,use this command to configure uplink bandwidth about Vendor Specific attribute id in RADIUS packets

uprate-value *value*

【Parameter】

vlaue: attribution id,the range is 1~32

【Default】

By default, it is 2

【Command mode】

AAA configuration mode

【Example】

！ Configure attribution id as 7 of uplink bandwidth compatible with H3C Cams

OptiWay(config-aaa)# uprate-value 7

【Commands】

h3c-cams

16.2.13 **radius 8021p**

This command is to verify port priority after configuring user authentication, with command **no** means to delete related configuration.

radius 8021p enable

no radius 8021p

【Parameter】

None

【Default】

Close function

【Command mode】

AAA configuration mode

【Usage】

Priority value passes through RADIUS packets Vendor Specific attribution id 77 , this attribution can modify with radius config-attribute command.

【Example】

！ Enable function

OptiWay(config-aaa)# radius 8021p enable

16.2.14 radius accounting

This command is to configure to start accounting or not after users authenticate in order to isolate from authentication and acconting.If disable accounting, users access to the internet without accounting after users pass the authentication.

[no]radius accounting

【Parameter】

None

【Default】

Enable authentication

【Command mode】

AAA configuration mode

【Example】

！Disable accounting

OptiWay(config-aaa)#no radius accounting

16.2.15 radius attribute

This command is to send H3C client version to RADIUS server or not compatible with H3C Cams, with command **no** means to delete related configuration.

[no] radius attribute client-version

【Parameter】

None

【Default】

Disable the function

【Command mode】

AAA configuration mode

【Example】

！Send H3C client version to RADIUS server

OptiWay(config-aaa)# radius attribute client-version

16.2.16 radius bandwidth-limit

This command is to modify user port bandwidth control after configuring user authentication, with command **no** means to delete related configuration.

radius bandwidth-limit enable

no radius bandwidth-limit

【Parameter】

None

【Default】

Disable the function

【Command mode】

AAA configuration mode

【Usage】

Uplink/downlink bandwidth value passes through RADIUS packets Vendor

Specific attribution id 75/76, this attribution id can modify by radius config-attribute command.

【Example】

！ Start function

OptiWay(config-aaa)# radius bandwidth-limit

16.2.17 radius config-attribute

This command is to configure RADIUS expansion value through RADIUS packets Vendor Specific attribution id.

radius config-attribute { access-bandwidth { downlink | uplink } | dscp | mac-address-number } type

【Parameter】

access-bandwidth downlink: configure downlink bandwidth, the default value is 75

access-bandwidth uplink: onfigure uplink bandwidth, the default value is 76

dscp:configure priority, the default value is 77

mac-address-number:MAC address quantity limitation, the default value is 50

type: attribution id

【Command mode】

AAA configuration mode

【Example】

！ Configure priority value attribution id as 80

OptiWay(config-aaa)# radius config-attribute dscp 80

16.2.18 radius host

This command is to create RADIUS server and enter into the configuration mode of RADIUS server. If RADIUS server exists, enter into the configuration mode of server. With command **no** means delete radius-scheme selected RADIUS server.

radius host *radius-scheme*

no radius *radius-scheme*

【Parameter】

radius-scheme:RADIUS server name, the range is 1～32 character,no matter capital or low case without space

【Command mode】

AAA configuration mode

【Example】

！Create and enter into RADIUS server myScheme

OptiWay(config-aaa)#radius host myScheme

OptiWay(config-aaa-radius-myScheme)#

【Commands】

radius host (or configuration mode)

16.2.19 radius mac-address-number

This command is to modify MAC address learning quantity limitation after configuring user authentication, with command **no** means delete the operation.

radius mac-address-number enable

no radius mac-address-number

【Parameter】

None

【Default】

Disable the function

【Command mode】

AAA configuration mode

【Usage】

MAC address learning quantity limitation value passes through RADIUS packets Vendor Specific attribution id 50, this attribution id can modify through radius config-attribute command.

【Example】

！Start function

OptiWay(config-aaa)# radius mac-address-number enable

16.2.20 radius server-disconnect drop 1x

This command is to configure user off line or not in the accounting system, with command **no** means delete the operation.

radius server-disconnect drop 1x

no radius server-disconnect drop 1x

【Parameter】

None

【Default】

Disable the function

【Command mode】

AAA configuration mode

【Example】

！ Enable function

OptiWay(config-aaa)# radius server-disconnect drop 1x

16.2.21 **radius vlan**

This command is to modify port PVID after configuring user authentication, with command **no** means delete the operation.

radius vlan enable

no radius vlan

【Parameter】

None

【Default】

Disable the function

【Command mode】

AAA configuration mode

【Usage】

PVID value passes through RADIUS packets Tunnel-Pvt-Group-ID attribution id.

【Example】

！ Start function

OptiWay(config-aaa)# radius vlan enable

16.2.22 realtime-account

This command is to configure current RADIUS server intermediate accounting function, configure to send intermediate accounting packets or not, if sending ,how munch is the interval. With command **no** means disable intermediate accounting function

realtime-account interval *minute*

no realtime-account

【Parameter】

minute: intermediate accounting packets interval,the range is :1～255,unit is minute

【Default】

By default, enable intermediate accounting, sending interval is 12 minutes

【Command mode】

RADIUS server configuration mode

【Example】

！ Enable RADIUS server intermediate accounting packets sending, sending interval is 30 minutes

OptiWay(config-aaa-radius-green)#realtime-account interval 30

！ Disable intermediate accounting packets sending

OptiWay(config-aaa-radius-green)#no realtime-account

16.2.23 second-acct-ip

This command is to configure IP address and port of secondary accounting RADIUS server, with command **no** means delete configuration.

second-acct-ip *server-ip accounting-port*

no second-acct-ip

【Parameter】

server-ip: secondary accounting RADIUS server IP address

accounting-port: authentication port ,the range is :1～65535

【Default】

By default, accounting port is 1813

【Command mode】

RADIUS server configuration mode

【Example】

！ Configure secondary accounting RADIUS server IP address as 192.168.0.100, accounting port is 1813

OptiWay(config-aaa-radius-green)# second-acct-ip 192.168.0.100 1813

16.2.24 **second-auth-ip**

This command is to configure IP address and port of secondary authentication RADIUS server , with command **no** means delete configuration..

second-auth-ip *server-ip authentication-port*

no second-auth-ip

【Parameter】

server-ip: secondary authentication RADIUS server IP address

authentication-port: authentication port,the range is :1～65535

【Default】

By default,authentication port is 1812

【Command mode】

RADIUS server configuration mode

【Example】

！ Configure secondary authentication RADIUS server IP address as 192.168.0.100, ,authentication port is 1812

OptiWay(config-aaa-radius-green)# second-auth-ip 192.168.0.100 1812

16.2.25 username-format

Use **username-format** command to configure the format of the usernames to be sent to RADIUS servers.

username-format with-domain

username-format without-domain

【Parameter】

with-domain:User name with domain name

without-domain:User name without domain name

【Default】

With domain

【Command configuration mode】

RADIUS configuration mode

【Usage】

In application, some RADIUS servers support username with domain name, butsome not, so according to the real situation to configure the RADIUS server.

【Example】

！Configure the username sent to the RADIUS server with the name of green not to carry domain name.

Optiway(config-aaa-radius-green)#username-format without-domain

【Related command】

radius host

16.3 822.1X Related Configuration Command

822.1X related configuration command include:

- **dot1x**
- **dot1x daemon**
- **dot1x eap-finish**
- **dot1x eap-transfer**
- **dot1x max-user**
- **dot1x port-control**
- **dot1x re-authenticate**
- **dot1x re-authentication**
- **dot1x timeout re-authperiod**
- **dot1x user cut**
- **show dot1x**

- **show dot1x daemon**
- **show dot1x interface**
- **show dot1x session**

16.3.1 dot1x method

Use **dot1x method** command to enable 822.1x. Use **no dot1x** command to disable 822.1x.

dot1x method [macbased portbased]

no dot1x

【Default】

802.1X disables

【Command configuration mode】

Global configuration mode

【Usage】

802.1x configuration can be effective only after 802.1x is enable. Some command can be used after 822.1x enables.

【Example】

！Enable 802.1X based on user authentication mode

Optiway(config)#dot1x method macbased

！Disable 802.1X

Optiway(config)#no dot1x

16.3.2 dot1x daemon

When 822.1x enables, configure whether a port send 822.1x daemon and

sending period.

dot1x daemon [time *time-value*] [interface *interface-list*]

no dot1x daemon

【Parameter】

time-value:the intervals of 822.1x daemon sending ranges from 12 to 622 seconds.

interface-list:List of Ethernet ports to be added to or removed from a VLAN. This keyword needed to be provided in the form of interface-type + interface-number. Interface-type is Ethernet and interface-number is slot-num/port-num, in which slot-num is in the range of 2 to 2, and port-num is in the range of 1 to 24. Sequential interfaces with the same type can be linked by to keyword, but the port number to the right of the to keyword must be larger than the one to the left of the keyword, and this argument only can be repeated for up to 3 times. There is no keyword in interface configuration mode.

【Default】

822.1x daemon is not sent by default. When 822.1x enables, default interval to send daemon is 62seconds.

【Command configuration mode】

Interface configuration mode, global configuration mode

【Usage】

This command is effective after 822.1x enables.

After 822.1x enables, configure according to the real situation.

【Example】

！ Enable dot1x daemon on ethernet 2/5 with the period time of 22 seconds

Optiway(config-if-ethernet-2/5)#dot1x daemon time 22

！ Configure dot1x daemon of ethernet 2/5 globally with the period time of 22 seconds

Optiway(config)# dot1x daemon time 22 interface ethernet 2/5

！ Restore the default dot1x daemon configuration on ethernet 2/5

Optiway(config-if-fastethernet-5)#no dot1x daemon

！ Restore the default dot1x daemon configuration of ethernet 2/5 globally

Optiway(config)#no dot1x daemon interface ethernet 2/5

16.3.3 dot1x eap-finish

After using dot1x eap-transfer command, 822.1 authentication message encapsulated by EAP frame from user is sent to RADIUS server after transfering to data frame encapsulated by other high level protocol.

After using **dot1x eap-finish** command,

dot1x eap-finish

【Default】

Use eap-finish way to transmit authentication message.

【Command configuration mode】

Global configuration mode

【Usage】

Choose dot1x eap-finish or dot1x eap-transfer command according to RADIUS server configuration. If authentication message transmitting way is different from RADIUS server authentication message receiving way,

authentication fails.

【Example】

！ Configure authentication message tramsitting to be eap-finish

Optiway(config)#dot1x eap-finish

【Related command】

dot1x eap-transfer

16.3.4 dot1x eap-transfer

After using **dot1x eap-transfer** command, 822.1 authentication message encapsulated by EAP frame from user is sent to RADIUS server without any changes.

dot1x eap-transfer

【Default】

Use eap-finish way to transmit authentication message.

【Command configuration mode】

Global configuration mode

【Usage】

Choose dot1x eap-finish or dot1x eap-transfer command according to RADIUS server configuration. If authentication message transmitting way is different from RADIUS server authentication message receiving way, authentication fails.

【Example】

！ Configure authentication message tramsitting to be eap-transfer

Optiway(config)#dot1x eap-transfer

【Related command】

dot1x eap-finish

16.3.5 dot1x max-user

Use **dot1x max-user** command to configure the maximum number of supplicant systems an ethernet port can accommodate. Use **no dot1x max-user** command to configure the maximum number to be 1.

dot1x max-user *host-num*

no dot1x max-user

【Parameter】

host-num:The integer between 1 and 16

【Default】

The max-user of 122M ethernet port is 16

【Command configuration mode】

Interface configuration mode or global configuration mode

【Usage】

This command is effective after 822.1X authentication.

After 822.1X enables, max-user of a port is determined by the real situation. The max-user of 122M ethernet port is 16

【Example】

！Configure the max-user of ethernet 2/5 is 12 in interface configuration mode

Optiway(config-if-ethernet-2/5)#dot1x max-user 122

! Configure the max-user of ethernet 2/5 is 12 globally

Optiway(config)#dot1x max-user 122 interface ethernet 2/5

! Restore the default max-user of ethernet 2/5 in interface configuration mode

Optiway(config-if-fastethernet-5)#no dot1x max-user

! Restore the default max-user of ethernet 2/5 globally

Optiway(config)#no dot1x max-user interface ethernet 2/5

16.3.6 dot1x port-control

Use **dot1x port-control** command to configure port control mode. Use **no dot1x port-control** command to restore the default port control.

dot1x port-control { auto | forceauthorized | forceunauthorized }

no dot1x port-control

【Parameter】

auto:Means needing authentication. User of this type of interface can get the resource from the LAN after authentication.

forceauthorized:Means forcing authorization. User of this type of interface can get the resource from the LAN without authentication.

forceunauthorized:Means forcing unauthorization. User of this type of interface cannot get the resource from the LAN.

【Default】

Port control mode is auto by default.

【Command configuration mode】

Interface configuration mode or global configuration mode

【Usage】

This command is effective after 822.1X authentication.

After 822.1X enables, the port control mode of RADIUS server is configured to be forceauthorized, so that the information of authenticator can be delivered to RADIUS server for authentication.

The port for user can be configured to be auto. User of this type of interface can get the resource from the LAN after authentication.

【Example】

！Ethernet 2/5 is RADIUS server port. Configure port-control mode of ethernet 2/5 to be forceauthorized in interface configuration mode

Optiway(config-if-ethernet-2/5)#dot1x port-control forceauthorized

！ Configure port-control mode of ethernet 2/5 to be forceauthorized globally.

Optiway(config)#dot1x port-control forceauthorized interface ethernet 2/5

【Related command】

dot1x

16.3.7 dot1x re-authenticate

Use **dot1x re-authenticate** command to re-authenticate current interface.

dot1x re-authenticate

【Command configuration mode】

Interface configuration mode or global configuration mode

【Usage】

This command is effective after 822.1X authentication.

822.1X re-authenticate only supports the message transmitting way of dot1x eap-transfer.

【Example】

！ Re-authenticate ethernet 2/5 in interface configuration mode

Optiway(config-if-ethernet-2/5)#dot1x re-authenticate

！ Re-authenticate ethernet 2/5 globally

Optiway(config)#dot1x re-authenticate interface ethernet 2/5

16.3.8 dot1x re-authentication

Use **dot1x re-authentication** command to enable 822.1x re-authentication. Use **no dot1x re-authentication** command to disable 822.1x re-authentication.

dot1x re-authentication

no dot1x re-authentication

【Default】

822.1X re-authentication disable

【Command configuration mode】

Interface configuration mode, global configuration mode

【Usage】

This command is effective after 822.1x authentication enables.

822.1X authentication only supports the message sending of dot1x eap-transfer.

【Example】

！ Enable re-authentication of ethernet 2/5

Optiway(config-if-ethernet-2/5)#dot1x re-authentication

Optiway(config)#dot1x re-authentication interface ethernet 2/5

【Related command】

dot1x,dot1x eap-finish,dot1x eap-transfer

16.3.9 dot1x timeout re-authperiod

Use **dot1x timeout re-authperiod** command to configure 822.1x re-authperiod. Use **no dot1x timeout re-authperiod** command to restore the default 822.1x re-authperiod.

dot1x timeout re-authperiod *seconds* [interface *interface-num*]

no dot1x timeout re-authperiod [interface *interface-num*]

【Parameter】

seconds: 822.1X re-authperiod ranges from 1 to 65535 seconds

interface-num:Optional interface number

【Default】

The default 822.1X re-authperiod is 3622 seconds

【Command configuration mode】

Global configuration mode

【Usage】

This command is effective after 822.1X authentication enables.

When no port is specified, use dot1x timeout re-authperiod command to modify 822.1x re-authperiod of all ports,or specified port is modified.

【Example】

！ Configure 822.1x re-authperiod of ethernet 2/3 to be 1822

Optiway(config)#dot1x timeout re-authperiod 1822 interface ethernet 2/3

！Restore all the re-authperiod to the default of 822.1x re-authperiod

Optiway(config)#no dot1x timeout re-authperiod

16.3.10 dot1x user cut

Use **dot1x user cut** command to remove specified online user.

dot1x user cut { { **username** *username* } | { **mac-address** *mac-address* [**vlan** *vlan-id*] } }

【Parameter】

username: the username to be removed

mac-address:Mac address of user to be removed

vlan-id:The vlan of user to be removed

【Command configuration mode】

Global configuration mode

【Example】

！Remove user with username of aaa@gnnet.com

Optiway(config)#dot1x user cut username aaa@gnnet.com

16.3.11 dot1x detect

Configure 802.1x user heartbead detection and interval time .

dot1x detect [interval *time-value*] [**interface** *interface-num*]

no dot1x detect

【Parameter】

time-value:send interval time of 1x heartbeat packets, unit is second

【Default】

By default, close 1x heartbeat ,when opening, send the packets every 25s

【Command mode】

Port configuration mode or all global configuration mode

【Usage】

This command is effective after it only enables 802.1X authentication..

Enable 802.1X uthentication, operators control to send heartbead detection packets and interval time to 1x authentication user according to the actual situation.

【Example】

！ Enable 1x heartbeat detection, interval time is 50s

OptiWay(config)# dot1x detect interval 50

16.3.12 dot1x quiet-period-value

Configure static function, when 802.1x users fail the authentication, it can't continue to verify in some period .

dot1x quiet-period-value *time-value*

【Parameter】

time-value:default interval time ,unit is second, default 0 means disable

【Default】

By default, it disables.

【Command mode】

All global configuration mode

【Usage】

This command is effective after it only enables 802.1X authentication..

【Example】

！ Enable static function, the configuration time is 50s

OptiWay(config)# dot1x quiet-period-value 50

16.3.13 **show dot1x**

Use **show dot1x** command to display 822.1x authentication information, such as: 822.1x authentication is enable or not, which authentication is used.

show dot1x

【Command configuration mode】

Any configuration mode

【Usage】

Use show command to display related information before configuration.

【Example】

！ Display 822.1x authentication information

Optiway(config)#show dot1x

16.3.14 **show dot1x daemon**

Use **show dot1x daemon** command to display 822.1x daemon configuration.

show dot1x daemon [interface *interface-num*]

【Parameter】

interface-num:Optioned interface number

【Command configuration mode】

Any configuration mode

【Example】

！Display the 822.1x daemon of all the ports

Optiway(config)#show dot1x daemon

16.3.15 **show dot1x interface**

Use **show dot1x interface** command to display such configuration of interface as control mode, re-authenticate, re-authperiod, max-user, etc.

show dot1x interface [*interface-num*]

【Parameter】

interface-num:Optioned interface number

【Command configuration mode】

Any configuration mode

【Usage】

Use this command to display related information before configuration. Use show command to display the changes.

【Example】

！Display port-control, re-authentication, re-authperiod and max-user configuration of ethernet 2/5

Optiway(config)#show dot1x interface ethernet 2/5

16.3.16 **show dot1x session**

Use **show dot1x session** command to display 822.1x session, including online information: interface number, mac-address, username, etc.

show dot1x session [{ interface *interface-num* } | { mac-address *mac* }]

【Parameter】

interface-num:The interface number

mac:The optioned mac-address

【Command configuration mode】

Any configuration mode

【Usage】

Use this command to display and detect the information of onlined user

【Example】

！Display all the onlined authentication users

Optiway(config)#show dot1x session

Chapter 17 SNTP Client Configuration Command

17.1 SNTP client configuration command list

SNTP client configuration command includes:

- **show sntp client**
- **sntp client**
- **sntp client authenticate**
- **sntp client authentication-key**
- **sntp client broadcastdelay**
- **sntp client mode**
- **sntp client multicast ttl**
- **sntp client poll-interval**
- **sntp client retransmit**
- **sntp client retransmit-interval**
- **sntp client valid-server**
- **sntp server**
- **sntp trusted-key**

17.1.1 show sntp client

Use the **show sntp client** command to display the information about SNTP client configuration and running.

show sntp client

【Command configuration mode 】

Any configuration mode

【Example】

！ Display the information about SNTP client configuration and running

Optiway(config)#show sntp client

17.1.2 sntp client

Use **sntp client** command to enable SNTP client. Use no sntp client command to disable SNTP client.

sntp client

no sntp client

【Usage】

If SNTP client has been enabled, sntp client command fails.

【Command configuration mode】

Global configuration mode

【Example】

！ Enable SNTP client

Optiway(config)#sntp client

17.1.3 sntp client authenticate

Use **sntp client authenticate** command to enable MD5 authentication of SNTP client. Use **no SNTP client authenticate** command to disable MD5 authentication of SNTP client.

sntp client authenticate

no sntp client authenticate

【Default】

SNTP client authenticate disables

【Command configuration mode】

Global configuration mode

【Example】

！ Enable SNTP client authenticate

Optiway(config)#sntp client authenticate

17.1.4 sntp client authentication-key

Use **sntp client authentication-key** command to configure MD5 authentication-key. More than one authentication-key can be configured.

sntp client authentication-key *number* md5 *value*

no sntp client authentication-key *number*

【Parameter】

number:Authentication-key ID ranges from 1to 4294967295

value:Authentication-key of 16 characters at most, which can be numbers, letters, space and other symbols.

【Default】

No authentication-key

【Usage】

Use sntp client authentication-key command to configure MD5 authentication-key. If the configuration is successful, the authentication-key should be effective after sntp client authentication-key command configures it

reliable or to be the key of unicast and anycast.

【Command configuration mode】

Global configuration mode

【Example】

！Configure SNTP client MD5 authentication-key, with the key ID being 12,and the key being abc

Optiway(config)#sntp client authentication-key 12 md5 abc

17.1.5 sntp client broadcastdelay

Use **sntp client broadcastdelay** command to configure the transmission delay of the SNTP client in broadcast or multicast. Use **no sntp client broadcastdelay** command to restore default transmission delay.

sntp client broadcastdelay *milliseconds*

no sntp client broadcastdelay

【Parameter】

milliseconds:This keyword ranges from 1 to 9999

【Default】

3 milliseconds

【Command configuration mode】

Global configuration mode

【Usage】

Transmission delay is necessary because client cannot time transmission delay and local time compensation in broadcast and multicast.

【Example】

！ Configure broadcastdelay to be 1 second

Optiway(config)#sntp client broadcastdelay 1222

17.1.6 sntp client mode

Use **sntp client mode** command to configure the operation mode of SNTP client. Use **no sntp client mode** command to restore the default operation mode of SNTP client.

sntp client mode { unicast | broadcast | multicast | anycast [**key** *number*] }

no sntp client mode

【Parameter】

unicast:Unicast mode

broadcast:Broadcast mode

multicast:Multicast mode

anycast:Anycast mode

number: ID of anycast ranges from 2 to 4294967295,2 means unauthentication.

【Default】

Broadcast mode

【Usage】

Use sntp client mode command to configure the operation mode of SNTP client. Only when SNTP client enables, this command is effective.

【Command configuration mode】

Global configuration mode

【Example】

！Configure SNTP client to operate in anycast

Optiway(config)#sntp client mode anycast

17.1.7 sntp client multicast ttl

Use **sntp client multicast ttl** command to configure ttl-value of multicast message. Use **no sntp client multicast ttl** command to restore default ttl-value.

sntp client multicast ttl *ttl-value*

no sntp client multicast ttl

【Parameter】

ttl-value:Ttl in multicast message sending ranges from 1 to 255

【Default】

Default ttl-value is 255

【Command configuration mode】

Global configuration mode

【Usage】

This command should be effective by sending message through multicast address in anycast operation mode. In order to restrict the range of sending multicast message, TTL-value setting is suggested.

【Example】

！Configure TTTL-value of sending multicast message to be 5

Optiway(config)#sntp client multicast ttl 5

17.1.8 sntp client poll-interval

Use **sntp client poll-interval** command to configure poll-interval of SNTP client in unicast or anycas. Use **no sntp client poll-interval** command to restore default poll-interval.

sntp client poll-interval *seconds*

no sntp client poll-interval

【Parameter】

seconds:Resending interval ranges from 64 to 1224 seconds

【Default】

1222 seconds

【Command configuration mode】

Global configuration mode

【Usage】

SNTP client sends requirement message regularly to the server in unicast and anycast operation mode. System time will be revised after receiving the message.

【Example】

！Configure poll-interval to be 122 seconds

Optiway(config)#sntp client poll-interval 122

17.1.9 sntp client retransmit

Use **sntp client retransmit** command to configure retransmit times inunicast

and anycast operation mode. Use **no sntp client retransmit** command to configure SNTP client not to retransmit requirement message.

sntp client retransmit *times*

no sntp client retransmit

【Parameter】

times:Times of retransmit ranges from 1 to 12

【Default】

non-retransmit（2）

【Command configuration mode】

Global configuration mode

【Usage】

In order to guarantee reliable transmission of SNTP client, overtime retransmission system is adopted. The requirement message will be resent if there's no reply in a certain time until the retransmit times limits. This command is effective in unicast and anycast operation mode, because these modes need send requirement message and overtime retransmission.

【Example】

！Configure overtime retransmission to be twice

Optiway(config)#sntp client retransmit 2

17.1.10 sntp client retransmit-interval

Use **sntp client retransmit-interval** command to configure retransmit-interval of SNTP client in unicast and anycast operation mode.

sntp client retransmit-interval *seconds*

no sntp client retransmit-interval

【Parameter】

seconds:Retransmit-interval ranges from 1 to 32 seconds

【Default】

5 seconds

【Command configuration mode】

Global configuration mode

【Usage】

Overtime retransmit system is used to guarantee reliable transmission of the requirement message. When there is no reply in retransmit-interval, the requirement message will be resent.

【Example】

！Configure retransmit-interval to be 12 seconds.

Optiway(config)#sntp client retransmit-interval 12

17.1.11 sntp client valid-server

Use **sntp client valid-server** command to add a filtration list item of valid -server. Use **no sntp client valid-server** command to remove a filtration list item of valid-server.

sntp client valid-server *ip-address wildcard*

no sntp client valid-server *ip-address wildcard*

【Parameter】

ip-address:Means valid-server interface. Mainframe cannot be 2

wildcard:Similar to reverse the mask

【Command configuration mode】

Global configuration mode

【Usage】

In the mode of broadcast and multicast, SNTP client checks time by receiving protocol messages sent by all servers. And it cannot filtrate the servers when spiteful attack exists. To solve this problem, a series of valid servers can be listed to filtrate source address of the message.

【Example】

！ Add a valid-server list

Optiway(config)#sntp client valid-server 12.1.2.2 2.2.255.255

17.1.12 sntp server

Use **sntp server** command to configure server ip-address in unicast mode. Use **no sntp server** command to remove server ip-address.

sntp server ip-address [**key** number]

no sntp server

【Parameter】

ip-address:Server ip-address.

number: To encrypt message when sending requirement to server. Use the key-number to decipher the message when the reply is received. The key-number ranges from 2 to 4294967295. 2 means unauthentication.

【Command configuration mode】

Global configuration mode

【Usage】

In unicast mode, server ip-address must be configured, or SNTP client cannot work smoothly.

【Example】

！Configure unicast server ip-address to be 192.168.2.122

Optiway(config)#sntp server 192.168.2.122

17.1.13 sntp client summer-time

This command is to configure SNTP client summer-time.

sntp client summer-time { **dayly** start-month start-day start-time end-month end-day end-time | **weekly** start-month start-week start-weekday start-time end-month end-week end-weekday end-time}

no sntp client summer-time

【Parameter】

start-month:start month, the range is 1～12

end-month: end month,the range is 1～12

start-day: start day, the range is 1～31

end-day:end day, the range is 1～31

start-time:start time, the range is 00:00:00～23:59:59

end-time:end time, the range is 00:00:00～23:59:59

start-week:start week, the range is 1～4

end-week:end week, the range is 1～4

start-weekday:start weekday, the range is sun～sat

end-weekday:end weekday, the range is sun～sat

【Default】

By default, no configure summer-time

【Usage】

Normally, end time of summer time is bigger than start time,it corresponds to the northern hemisphere's summer-time; start time of summer time is bigger than end time,it corresponds to the southern hemisphere's summer-time.Then the range of summer-time is from start time to year end plus from the beginning time to the end time.

【Command mode】

All global configuration mode

【Example】

！ Configure summer time as 0 clock April 1st to 23:59:59 Oct 31st

OptiWay(config)#sntp client summer-time dayly 4 1 00:00:00 10 31 23:59:59

17.1.14 **sntp trusted-key**

Use **sntp trusted-key** command to configure a trusted-key.

sntp trusted-key *number*

no sntp trusted-key *number*

【Parameter】

number:Key ID ranges from 1 to 4294967295

【Default】

All key number is reliable

【Usage】

In broadcast and multicast, the authentication is valid only when key-number is configured. The authentication is invalid when receiving the message encrypt by untrusty-key.

【Command configuration mode】

Global configuration mode

【Example】

！Configure trusted-key to be 12

Optiway(config)#sntp trusted-key 12

Chapter 18 Syslog Configiration Command

18.1 Syslog Configuration Command

Syslog configuration command includes:

- **show logging**
- **show logging buffered**
- **show logging flash**
- **show logging filter**
- **show debug**
- **logging**
- **logging sequence-numbers**
- **logging timestamps**
- **logging language**
- **logging monitor**
- **terminal monitor**
- **logging buffered**
- **clear logging buffered**
- **logging flash**
- **clear logging flash**
- **logging host**
- **logging facility**
- **logging source**
- **logging snmp-agent**

- **debug**
- **upload logging**

18.1.1 show logging

Use **show logging** command to display Syslog configuration, state, and statistical information.

show logging

【Command configuration mode】

Any configuration mode

【Example】

！Display Syslog configuration, state, and statistical information.

Optiway(config)#show logging

18.1.2 show logging buffered

Use **show logging buffered** command to display buffered log.

show logging buffered [*level* | level-list { *level* [to *level*] } &<1-8>] [module { xxx | … } *]

【Parameter】

level:Level of information ranges from 2 to 7

xxx:Means the name of the module. … means other modules are omitted.

【Command configuration mode】

Any configuration mode

【Usage】

Use keyword “level-list” to display the specified level information in list. If the “level-list” is not specified, the information of the higher level (The smaller the level number is, the higher the level is.) and the equal level will be displayed.

【Example】

！Display the buffered log of level 7

Optiway(config)#show logging buffered level-list 7

18.1.3 show logging flash

Use **show logging flash** command to display flash log.

show logging flash [*level* | level-list { *level* [to *level*] } &<1-8>] [module { xxx | … } *]

【Parameter】

level:Level of information ranges from 2 to 7

xxx:Means the name of the module. … means other modules are omitted.

【Command configuration mode】

Any configuration mode

【Usage】

Use keyword “level-list” to display the specified level information in list. If the “level-list” is not specified, the information of the higher level (The smaller the level number is, the higher the level is.) and the equal level will be displayed.

【Example】

！Display the flash log of module vlan

Optiway(config)#show logging flash module vlan

18.1.4 show logging filter

Use **show logging filter** command to display filter log.

show logging filter { monitor *monitor-no* | buffered | flash | host *ip-address* | snmp-agent }

【Parameter】

monitor-no:Means terminal number. 2 means console, and 1 to 5 means Telnet terminal.

ip-address:ip address of log host（Syslog server）

【Command configuration mode】

Any configuration mode

【Example】

！Display buffered filter log

Optiway(config)#show logging filter buffered

18.1.5 show debug

Use **show debug** command to display the debug of the module.

show debug

【Command configuration mode】

Any configuration mode

【Example】

！Display the debug of module

Optiway(config)#show debug

18.1.6 logging

Use **logging** command to enable Syslog. Use no logging command to disable Syslog.

logging

no logging

【Default】

Syslog enables

【Command configuration mode】

Global configuration mode

【Example】

！Enable Syslog

Optiway(config)#logging

18.1.7 logging sequence-numbers

Use **logging sequence-numbers** command to configure global sequence number to be displayed in Syslog. Use **no logging sequence-numbers** command to configure global sequence number not to be displayed in Syslog.

logging sequence-numbers

no logging sequence-numbers

【Default】

Not display global sequence number

【Command configuration mode】

Global configuration mode

【Example】

！Configure global sequence number to be displayed in Syslog outputting information.

Optiway(config)#logging sequence-numbers

18.1.8 logging timestamps

Use **logging timestamps** command to configure the type of timestamps in Syslog. Use **no logging timestamps** command to restore the default type of timestamps.

logging timestamps { notime | uptime | datetime }

no logging timestamps

【Parameter】

notime:Timestamps are not displayed

uptime:Uptime is the timestamps

datetime:Datetime is the timestamps

【Default】

Uptime is the default timestamps

【Command configuration mode】

Global configuration mode

【Example】

！Configure datetime to be the timestamps

Optiway(config)#logging timestamps datetime

18.1.9 logging language

Use **logging language** command to configure the language in Syslog.

logging language { english | chinese }

【Parameter】

english:Use English to be logging language

chinese:Use Chinese to be logging language

【Default】

Use English to be logging language

【Command configuration mode】

Global configuration mode

【Example】

！Configure Chinese to be logging language

Optiway(config)#logging language chinese

18.1.10 logging monitor

Use **logging monitor** command to enable monitor logging and configure filter regulation. Use **no logging monitor** command to disable monitor logging and restore default filter regulation.

logging monitor { all | *monitor-no* }

no logging monitor { all | *monitor-no* }

logging monitor { **all** | *monitor-no* } { *level* | **none** | **level-list** { *level* [**to** *level*] } &<1-8> } [**module** { **xxx** | **…** } *]

no logging monitor { all | *monitor-no* } filter

【Parameter】

all:All terminals

monitor-no:Means terminal number. 2 means console, and 1 to 5 means Telnet terminal.

level:Level of information ranges from 2 to 7

none:Any level is not allowed

xxx:Means the name of the module. … means other modules are omitted.

【Default】

All monitor logging disable.

Filter regulations of all terminals are to allow all modules of all levels except level 6 to output information

【Command configuration mode】

Global configuration mode

【Usage】

Use keyword “level-list” to display the specified level information in list. If the “level-list” is not specified, the information of the higher level (The smaller the level number is, the higher the level is.) and the equal level will be displayed.

【Example】

！Enable monitor logging

Optiway(config)#logging monitor 2

！Configure filter regulations of all terminals to allow all module of levels 2 to 6 to output information

Optiway(config)#logging monitor 2 6

18.1.11 terminal monitor

Use **terminal monitor** command to enable current terminal information displaying. Use **no terminal monitor** command to disable current terminal information displaying.

terminal monitor

no terminal monitor

【Default】

Current terminal information displaying enables,all Telnetterminal information displaying disables.

【Command configuration mode】

Any configuration mode

【Usage】

This command has influence on current terminal and current log in.

【Example】

！Enable current terminal information displaying

Optiway(config)#terminal monitor

18.1.12 logging buffered

Use **logging buffered** command to enable buffered logging and configure filter regulations. Use **no logging buffered** command to disable buffered logging and restore to default filter regulations.

logging buffered

no logging buffered

logging buffered { *level* | **none** | **level-list** { *level* [**to** *level*] } &<1-8> } [**module** { **xxx** | **…** } *]

no logging buffered filter

【Parameter】

level:Level of information ranges from 2 to 7

none:Any level is not allowed.

xxx:Means the name of the module. … means other modules are omitted.

【Default】

All buffered logging enable.

Filter regulations of all terminals are to allow all modules of levels 2 to 6 to output information

【Command configuration mode】

Global configuration mode

【Usage】

Use keyword “level-list” to display the specified level information in list. If the “level-list” is not specified, the information of the higher level (The smaller the level number is, the higher the level is.) and the equal level will be displayed.

【Example】

！ Disable buffered logging

Optiway(config)#no logging buffered

！ Configure filter regulations of all terminals to allow all module of level 2,1,2 and 6 to output information

Optiway(config)#logging buffered level-list 2 to 2 6

18.1.13 **clear logging buffered**

Use **clear logging buffered** command to clear buffered logging.

clear logging buffered

【Command configuration mode】

Any configuration mode

【Example】

！Clear buffered logging

Optiway(config)#clear logging buffered

18.1.14 logging flash

Use **logging flash** command to enable flash logging and configure filter regulations. Use **no logging flash** command to disable flash logging and restore to default filter regulations.

logging flash

no logging flash

logging flash { *level* | **none** | **level-list** { *level* [**to** *level*] } &<1-8> } [**module** { **xxx** | **…** } *]

no logging flash filter

【Parameter】

level:Level of information ranges from 2 to 7

none:Any level is not allowed.

xxx:Means the name of the module. … means other modules are omitted.

【Default】

All flash logging enable.

Filter regulations of all terminals are to allow all modules of levels 2 to 6 to output information

【Command configuration mode】

Global configuration mode

【Usage】

Use keyword “level-list” to display the specified level information in list. If the “level-list” is not specified, the information of the higher level (The smaller the level number is, the higher the level is.) and the equal level will be displayed.

【Example】

！Disable flash logging

Optiway(config)#no logging flash

！Configure filter regulations of all terminals to allow all vlan module to output information

Optiway(config)#logging flash none

Optiway(config)#logging flash 7 module vlan

18.1.15 clear logging flash

Use **clear logging flash** command to clear flash logging.

clear logging flash

【Command configuration mode】

Any configuration mode

【Example】

！Clear flash logging

Optiway(config)#clear logging flash

18.1.16 logging host

Use **logging host** command to configure host ip address, and enable host logging, and configure filter regulation of Syslog server. Use **no logging host** command to remove host ip address, disable host logging, and configure default filter regulation.

logging ip-address

no logging *ip-address*

logging host { all | *ip-address* }

no logging host { all | *ip-address* }

logging host { **all** | *ip-address* } { *level* | **none** | **level-list** { *level* [**to** *level*] } &<1-8> } [**module** { **xxx** | **…** } *]

no logging host { all | *ip-address* } filter

【Parameter】

all:All logging host

ip-address:IP address of Syslog server

level:Level of information ranges from 2 to 7

none:Any level is not allowed.

xxx:Means the name of the module. … means other modules are omitted.

【Default】

All logging host enable.

Filter regulations of all terminals are to allow all modules of levels 2 to 6 to output information

【Command configuration mode】

Global configuration mode

【Usage】

At most 15 logging hosts are allowed to configure.

Use keyword “level-list” to display the specified level information in list. If the “level-list” is not specified, the information of the higher level (The smaller the level number is, the higher the level is.) and the equal level will be displayed.

【Example】

！ Add a new logging host with the ip address of 1.1.1.1

Optiway(config)#logging 1.1.1.1

！ Enable logging host 1.1.1.1

Optiway(config)#logging host 1.1.1.1

！Configure filter regulations of logging host 1.1.1.1 to allow all module of level 2 to 6 to output information

Optiway(config)#logging host 1.1.1.1 6

18.1.17 **logging facility**

Use logging facility command to configure logging facility used by logging host. Use **no logging facility** command to restore the default logging facility.

logging facility { xxx | … } *

no logging facility

【Parameter】

xxx:The name of logging facilities.… means other logging facilities are omitted.

【Default】

Default logging facility is localuse7

【Command configuration mode】

Global configuration mode

【Example】

！Configure logging facility to be localuse2

Optiway(config)#logging facility localuse2

18.1.18 logging source

Use **logging source** command to configure logging host to use fixed source ip address outputting. Use **no logging source** command to configure logging host not to use fixed source ip address outputting.

logging source *ip-address*

no logging source

【Parameter】

ip-address:Fixed source ip address

【Default】

Not to use fixed source ip address

【Command configuration mode】

Global configuration mode

【Usage】

The fixed source ip address must be the ip address of some port in facility to be configured, or configuration fails. If the fixed source ip address is not used,

egress interface is used as the fixed source ip address.

【Example】

！Configure the fixed source ip address of logging host to be 1.1.1.2

Optiway(config)#logging source 1.1.1.2

18.1.19 logging snmp-agent

Use **logging snmp-agent** command to enable SNMP Agent logging and configure filter configuration. Use **no logging snmp-agent** command to disable SNMP Agent logging and restore to default filter configuration.

logging snmp-agent

no logging snmp-agent

logging snmp-agent { *level* | **none** | **level-list** { *level* [**to** *level*] } &<1-8> } [**module** { **xxx** | **…** } *]

no logging snmp-agent filter

【Parameter】

level: information level, 2～7

none: no any level

xxx: module mode,…ignore other module name

【Parameter】

level:Level of information ranges from 2 to 7

none:Any level is not allowed.

xxx:Means the name of the module. … means other modules are omitted.

【Default】

By default , information output power switch disables

By default, filter rule is that permit all module output information with level 2～5

【Default】

All SNMP Agent logging enable.

Filter regulations of all terminals are to allow all modules of levels 2 to 5 to output information

【Command mode】

All global configuration mode

【Command configuration mode】

Global configuration mode

【Usage】

Use key word evel-list to configure selected level information output in permited level list; Without level-list configuration permit , it equals higher（the small value with higher level） and this level information output

Configure Trap host address if Syslog information with Trap packets sends to SNMP Workstation, it also configures Trap host address ,see SNMP configuration.

【Usage】

Use keyword “level-list” to display the specified level information in list. If the “level-list” is not specified, the information of the higher level (The smaller the level number is, the higher the level is.) and the equal level will be displayed.

Configure Trap host ip address for Syslog information to send to SNMP Workstation by Trap message. (Refer to SNMP configuration)

【Example】

！ Enable SNMP Agent logging

Optiway(config)#logging snmp-agent

！ Configure SNMP Agent outputting filtration rule to be permitting 2 to 3 levels of information

Optiway(config)#logging snmp-agent 3

【Related command】

snmp-server host

18.1.20 **debug**

Use **debug** command to enable debug of a module. Use **no debug** command to disable debug of a module.

debug { all | { xxx | … } * }

no debug { all | { xxx | … } * }

【Parameter】

all:All module

xxx:Means the name of the module. … means other modules are omitted.

【Default】

All debug disable.

【Command configuration mode】

Global configuration mode

【Example】

！ Enable debug of module vlan

Optiway(config)#debug vlan

18.1.21 upload logging

Use **upload logging** command to upload Flash storage to ftp or tftp server.

upload logging tftp *ip-address file-name*

upload logging ftp ip-address file-name user-name password

【Parameter】

ip-address:IP address of server

file-name:The filename saved to server

user-name:Ftp username

password:Ftp password

【Command configuration mode】

Privileged mode

【Example】

！Upload Flash storage to tftp server 1.1.1.1,and saved file is aaa.txt

Optiway(config)#upload logging tftp 1.1.1.1 aaa.txt

Chapter 19 SSH Configuration Command

19.1 SSH configuration command list

SSH configuration command includes:

- **show ssh**
- **show keyfile**
- **ssh**
- **crypto key generate rsa**
- **crypto key zeroize rsa**
- **crypto key refresh**
- **load keyfile**
- **upload keyfile**

19.1.1 show ssh

Use **show ssh** command to display SSH configuration information, including version number, enabling/disabling SSH and SSH keyfile.

show ssh

【Command configuration mode】

Any configuration mode

【Example】

！Display SSH information

Optiway#show ssh

19.1.2 show keyfile

Use **show keyfile** command to display keyfile in Flash storage.

show keyfile { public | private }

【Command configuration mode】

Privileged configuration mode

【Example】

！Display SSH keyfile

Optiway#show keyfile public

19.1.3 ssh

Use this command to enable/disable SSH.

ssh

no ssh

【Default】

Disable

【Command configuration mode】

Global configuration mode

【Example】

！Enable SSH

Optiway(config)#ssh

19.1.4 crypto key generate rsa

Use **crypto key generate rsa** command to configure SSH to be generate

rsa.

crypto key generate rsa

【Command configuration mode】

Privileged configuration mode

【Example】

！Configure SSH key to be generate rsa.

Optiway#crypto key generate rsa

19.1.5 crypto key zeroize rsa

Use **crypto key zeroize rsa** command to clear the keyfile in Flash storage.

crypto key zeroize rsa

【Command configuration mode】

Privileged configuration mode

【Example】

！Clear keyfile in Flash storage

Optiway#crypto key zeroize rsa

19.1.6 crypto key refresh

Use **crypto key refresh** command to load SSH key from Flash storage.

crypto key refresh

【Command configuration mode】

Privileged configuration mode

【Example】

！ Load SSH key from Flash storage.

Optiway#crypto key refresh

19.1.7 load keyfile

Use **load keyfile** command to download keyfile to device from tftp or ftp server.

load keyfile { public | private } tftp *server-ip filename*

load keyfile { **public** | **private** } **ftp** *server-ip filename username passwd*

【Parameter】

server-ip:IP address of tftp or ftp server

filename:file name of keyfile.

username:ftp username

passwd:ftp password

【Command configuration mode】

Privileged configuration mode

【Example】

！ Download keyfile pub.txt from tftp server 1.1.1.1 as public keyfile

Optiway#load keyfile public tftp 1.1.1.1 pub.txt

19.1.8 upload keyfile

Use **upload keyfile** command to upload keyfile to device from tftp or ftp server.

upload keyfile { public | private } tftp *server-ip filename*

upload keyfile { **public** | **private** } **ftp** *server-ip filename username passwd*

【Parameter】

server-ip:IP address of tftp or ftp server

filename:file name of keyfile.

username:ftp username

passwd:ftp password

【Command configuration mode】

Privileged configuration mode

【Example】

！ Upload keyfile to tftp server 1.1.1.1 and saved as pub.txt

Optiway#upload keyfile public tftp 1.1.1.1 pub.txt

Chapter 20 VRRP Configuration Command

20.1 VRRP configuration command list

VRRP configuration command includes:

- **ip vrrp**
- **show vrrp**
- **vrrp ping-enable**
- **vrrp preempt**
- **vrrp priority**
- **vrrp timer**

20.1.1 ip vrrp

Use **ip vrrp** command to assign an IP address of the current interface to a virtual switch (also called a backup group). Use **no ip vrrp** command to remove a virtual IP address from a backup group.

ip vrrp *vrid vip*

no ip vrrp *vrid* [*vip*]

【Parameter】

vrid:Backup group id which is in the range of 1 to 255

vip:Virtual IP address of backup group.

【Command configuration mode】

VLAN interface configuration mode

【Usage】

Backup id is in the range of 1 to 255. Virtual address can be undistributed IP address in the interface where the backup group is in, and also can be IP address of backup group interface. At most 8 backup groups can be configured. If this address is the one the switch has used, it also can be configured. Now, this switch is called an IP Address Owner. When specify the first IP address to a backup group, system will create this backup group, and add virtual IP address to this backup group from that on, system will only add the address to the backup group. At most 8 IP address can be configured to each backup group. When deleting the last IP address, the backup group will be deleted at the same time, that is, there is no this backup group in this interface and all configurations are not valid.

【Example】

！Configure a virtual group in interface 1 of VLAN with the virtual IP to be 192.168.1.1

Optiway(config-if-vlanInterface-1)#ip vrrp 1 192.168.1.1

20.1.2 **show vrrp**

Use **show vrrp** command to display VRRP status information.

show vrrp [vlan-interface *num*] [*vrid*]

【Parameter】

num:interface number, here is vid of vlan interface.

vrid:ID of backup group.

【Command configuration mode】

Any configuration mode

【Example】

！ Display configured VRRP information

Optiway#show vrrp

20.1.3 **vrrp ping-enable**

Use **vrrp ping-enable** command to enable/disable the ping command is not responded by the device which is not the IP address owner.

vrrp ping-enable

no vrrp ping-enable

【Default】

Disable the ping command is not responded by the device which is not the IP address owner.

【Command configuration mode】

Global configuration mode

【Usage】

According to the protocol, the device which is not the IP address ownerm has to drop the packet with the destination IP address being virtual IP adress. When main-control switch is not the IP address owner, the ping packet (ICMP echo requiring packet) which is sent to virtual IP address will be dropped. Using this command to enable the responding to the ping function of the device which is not the IP address owner, the ping packet to the virtual IP address can be responded when the main-control switch is not the IP address owner.

【Example】

！ Enable ping response of the device which is not the IP address owner.

Optiway(config)#vrrp ping-enable

20.1.4 **vrrp preempt**

Use **vrrp preempt** command to configure the preemption of backup group.

vrrp preempt *vrid* [delay *delay*]

no vrrp preempt *vrid*

【Parameter】

vrid:virtual group ID which is in the range of 1～255

delay:preempt delay which is in the range of 1～255,and the unit is second.

【Default】

It is defaulted to be preempt with the delay time being 2

【Command configuration mode】

VLAN interface configuration mode

【Usage】

Once there is a Master in the backup group,and there is no failure, and other switch though has configured to prossess superior priority,it will not be Master unless the preemption is configured. If the switch is configured to be preempt, once it prossesses its priority is superior than the Master, it will be the Master. Accordingly, the original Master will be the backup. The delay time can be configured at the same time as the preemption, which can delay backup being Master. The aim of delay time is: In unstable network, if Backup doesn't receive the packet from Master on time, it will become Master (the reson why Backup cannot receive the packet is because of the congestion of the network, not the abnormal working of Master). So waiting for a certain time, the packet will be received from Master, which avoids frequent changes.

Cancelling preemption of backup group, the delay time will be 2.

【Example】

！Configure preemption and delay time of backup group.

Optiway(config-if-vlanInterface-1)#vrrp preempt 1 delay 3

20.1.5 vrrp priority

Use **vrrp priority** command to configure the priority of backup group. Use **no priority** command to restore the default value.

vrrp priority *vrid priority*

no priority *vrid*

【Parameter】

vrid:virtual group ID which is in the range of 1～255

priority:virtual group priority which is in the range of 1～254

【Default】

The priority defaulted value is 122.

【Command configuration mode】

VLAN interface configuration mode

【Usage】

In VRRP, the status of each switch in backup group is determined by priority. The switch with the superior priority is the Master, and the range of it is from 2 to 255 (the larger the value is, the superior the priority is). The configured priority is from 1 to 254. Priority 2 is reserved for special use, and 255 is reserved for IP address owner.

【Example】

！ Configure the priority of the switch in backup group 1 to be 222

Optiway(config-if-vlanInterface-1)#vrrp priority 1 222

20.1.6 vrrp track

This command is to configure or delete backup monitor interface

vrrp track *vrid* { **vlan-if** *vlan-id* | **supervlan-if** *supervlan-id* } [**reduced** *pri-value*]

no vrrp track *vrid* { all | vlan-if *vlan-id* | supervlan-if *supervlan-id* }

【Parameter】

vrid:virtual group ID,the range is 1～255

vlan-id:vlan id belongs to vlan port

supervlan-id: supervlan id belongs to supervlan

pri-value: need to reduce the priority when being monitored interface is down

【Default】

By default, no configure any monitor interfaces

By default, the priority is low to 10 when being monitored interface is down

【Command mode】

VLAN/superVlan interface configuration mode

【Example】

！Configure monitor interface in backup group 1 as vlan interface 2, the priority value is low to 20

OptiWay(config-if-vlanInterface-1)#vrrp track 1 vlan-if 2 reduced 20

20.1.7 vrrp timer

Use **vrrp timer** command to configure VRRP timer. Use **no vrrp timer** command to restore the default VRRP timer.

vrrp timer vrid adver_interval

no vrrp timer

【Parameter】

vrid:virtual group ID which is in the range of 1～255

adver_interval:The interval of sending VRRP packet by Master which is in the range of 1 to 255 with the unit being second.

【Default】

The default adver_interval is 1 second.

【Command configuration mode】

VLAN interface configuration mode

【Usage】

Master switch in VRRP backuo group will send VRRP packet timely (the interval is adver-interval) to inform switches in the backup group that it can work normally. If Backup hasn't received the VRRP packet from Master for a acertain time (the time interval is master_down_interval), it thinks that the Master cannot work normally, and it will turn to Master. User can adjust the adver_interval of VRRP packet sending by the Master through this command. The master_down_interval of Backup is three times of adver_interval. The overlarge of network flow or the different timer of the switch may cause the abnormal overtime of the master_down_interval to change the status. Prolong the adver_interval and configure delay time can solve this problem. The unit of adver_interval is second.

【Example】

```
! Configure the adver-interval of backup group 1 is 1 second.
Optiway(config-if-vlanInterface-1)#vrrp timer 1 1
```

Chapter 21 Switch Manage and Maintenance Command

21.1 Configuration Files Management

Configuration files management includes:

- **buildrun mode continue**
- **buildrun mode stop**
- **clear startup-config**
- **copy nm-interface-config startup-config**
- **copy running-config startup-config**
- **copy startup-config running-config**
- **show running-config**
- **show startup-config**

21.1.1 buildrun mode continue

Use **buildrun mode continue** command to configure buildrun mode to be continune.

buildrun mode continue

【Command configuration mode】

Privileged mode

【Example】

！Configure buildrun mode to be continune

OPTIWAY#buildrun mode continue

21.1.2 buildrun mode stop

Use **buildrun mode stop** command to configure buildrun mode to be stop.

buildrun mode stop

【Command configuration mode】

Privileged mode

【Example】

！Configure buildrun mode to be stop.

OPTIWAY#buildrun mode stop

21.1.3 clear startup-config

Use **clear startup-config** command to clear saved configuration.

clear startup-config

【Command configuration mode】

Privileged mode

【Usage】

Use this command to clear saved configuration and reboot switch. The switch will restore to original configuration.

【Example】

！Restore the original configuration

OPTIWAY#clear startup-config

21.1.4 copy nm-interface-config startup-config

Use **copy nm-interface-config startup-config** command to save minmum

manageable configuration of network administration.

copy nm-interface-config startup-config [vlan-interface-id [ip-address mask gateway-address]]

【Parameter】

vlan-interface-id: VLAN interface number

ip-address:IP address

mask:netmask

gateway-address:gateway address

【Command configuration mode】

Privileged configuration mode

【Usage】

If no keyword is configured, vlan-interface-id is defaulted to be the id of VLAN interface 1,ip-address is IP address of VLAN interface 1,mask is netmask of VLAN interface 1,gateway-address is the gateway address of VLAN interface 1；

If only imputed vlan-interface-id, ip-address is defaulted to be IPaddress of imputed VLAN interface,mask is netmask of VLAN interface,gateway-address is defaulted route gateway；

If all keywords are imputed, it will be saved as inputting.

【Example】

！ Save configuration of VLAN interface 1

OPTIWAY#copy nm-interface-config startup-config

！ Save configuration of VLAN interface 2

OPTIWAY#copy nm-interface-config startup-config 2

！ Save configuration of user-defined interface

OPTIWAY#copy nm-interface-config startup-config 2 192.168.2.122 255.255.255.2 192.168.2.1

21.1.5 copy running-config startup-config

Use **copy running-config startup-config** command to save current configuration.

copy running-config startup-config

【Command configuration mode】

Privileged mode

【Example】

！ Save current configuration

OPTIWAY#copy running-config startup-config

21.1.6 copy startup-config running-config

Use **copy startup-config running-config** command to execute saved configuration, and executed configuration is the same as the saved one.

copy startup-config running-config

【Command configuration mode】

Privileged mode

【Example】

！ Execute saved configuration

OPTIWAY#copy startup-config running-config

21.1.7 show running-config

Use **show running-config** command to display current configuration.

show running-config [module-list]

【Parameter】

module-list:Optional module. The module name can be changed with the version.

【Command configuration mode】

Any configuration mode

【Example】

！Display all configurations

OPTIWAY#show running-config

！Display configuration of GARP and OAM module

OPTIWAY#show running-config garp oam

21.1.8 show startup-config

Use **show startup-config** command to display saved configuration.

show startup-config [module-list]

【Parameter】

module-list:Optional module. The module name can be changed with the version.

【Command configuration mode】

Any configuration mode

【Example】

！Display all saved configuration

OPTIWAY#show running-config

！Display saved configuration of GARP and OAM module

OPTIWAY#show running-config garp oam

21.2 Online Loading Upgrade Program

Online Loading Upgrade Program includes:

- **load application ftp**
- **load application tftp**
- **load application xmodem**
- **load configuration ftp**
- **load configuration tftp**
- **load configuration xmodem**
- **load whole-bootrom ftp**
- **load whole-bootrom tftp**
- **load whole-bootrom xmodem**
- **upload alarm ftp**
- **upload alarm tftp**
- **upload configuration ftp**
- **upload configuration tftp**
- **upload logging ftp**
- **upload logging tftp**

21.2.1 load application ftp

Use **load application ftp** command to load application program by FTP protocol.

load application ftp ftpserver-ip filename username userpassword

【Parameter】

ftpserver-ip:IP address of FTP server

filename:Filename to be loaded

username,userpassword:Username and password of FTP server

【Command configuration mode】

Privileged mode

【Usage】

Open FTP server and set username, password and file download path before use this command. Reboot the switch after successful download and run new application program.

【Example】

！Download application program app.arj to 192.168.2.122 by FTP

OPTIWAY#load application ftp 192.168.2.122 app.arj username password

21.2.2 load application tftp

Use **load application tftp** command to load application program by TFTP protocol.

load application tftp *tftpserver-ip filename*

【Parameter】

tftpserver-ip:IP address of TFTP server

filename:Filename to be loaded

【Command configuration mode】

Privileged mode

【Usage】

Open TFTP server and set file download path before use this command. Reboot the switch after successful download and run new application program.

【Example】

！Download application program app.arj to 192.168.2.122 by TFTP

OPTIWAY#load application tftp 192.168.2.122 app.arj

21.2.3 load application xmodem

Use **load application xmodem** command to load application program by Xmodem protocol.

load application xmodem

【Command configuration mode】

Privileged mode

【Usage】

Choose “send” -> “send file” in super terminal, and input full path and filename of the file in filename dialog box, and choose Xmodem protocol in “protocol” , then click 【send】.

Reboot the switch after successful download and run new application program.

【Example】

！Download application program by Xmodem protocol

OPTIWAY#load application xmodem

21.2.4 load configuration ftp

Use **load configuration ftp** command to load configuration program by FTP protocol.

load configuration ftp ftpserver-ip filename username userpassword

【Parameter】

ftpserver-ip:IP address of FTP server

filename:Filename to be loaded

username,userpassword:Username and password of FTP server

【Command configuration mode】

Privileged mode

【Usage】

Open FTP server and set username, password and file download path before use this command. Reboot the switch after successful download and run new configuration program.

【Example】

！Download configuration program abc to 192.168.2.122 by FTP

OPTIWAY#load configuration ftp 192.168.2.122 abc username password

21.2.5 load configuration tftp

Use **load configuration tftp** command to load configuration program by TFTP protocol.

load configuration tftp *tftpserver-ip filename*

【Parameter】

tftpserver-ip:IP address of TFTP server

filename:Filename to be loaded

【Command configuration mode】

Privileged mode

【Usage】

Open TFTP server and set file download path before use this command. Reboot the switch after successful download and run new configuration program.

【Example】

！Download configuration program abc to 192.168.2.122 by TFTP

OPTIWAY#load configuration ftp 192.168.2.122 abc

21.2.6 load configuration xmodem

Use **load configuration xmodem** command to load configuration program by Xmodem protocol.

load configuration xmodem

【Command configuration mode】

Privileged mode

【Usage】

Choose “send” -> “send file” in super terminal, and input full path and filename of the file in filename dialog box, and choose Xmodem protocol in “protocol”, then click 【send】.

Reboot the switch after successful download and run new application program.

【Example】

！Download configuration program by Xmodem protocol

OPTIWAY#load configuration xmodem

21.2.7 load whole-bootrom ftp

Use **load whole-bootrom ftp** command to load whole bootrom by FTP protocol.

load whole-bootrom ftp ftpserver-ip filename username userpassword

【Parameter】

ftpserver-ip:IP address of FTP server

filename:Filename to be loaded

username,userpassword:Username and password of FTP server

【Command configuration mode】

Privileged mode

【Usage】

Open FTP server and set username, password and file download path before use this command.

【Example】

！Download whole-bootrom abc to 192.168.2.122 by FTP

OPTIWAY#load whole-bootrom ftp 192.168.2.122 abc username password

21.2.8 load whole-bootrom tftp

Use **load whole-bootrom tftp** command to load whole bootrom by TFTP protocol.

load whole-bootrom tftp *tftpserver-ip filename*

【Parameter】

tftpserver-ip:IP address of TFTP server

filename:Filename to be loaded

【Command configuration mode】

Privileged mode

【Usage】

Open TFTP server and set file download path before using this command.

【Example】

！Download whole-bootrom abc to 192.168.2.122 by TFTP

OPTIWAY#load whole-bootrom tftp 192.168.2.122 abc username password

21.2.9 load whole-bootrom xmodem

Use **load whole-bootrom xmodem** command to load whole bootrom by xmodem protocol.

load whole-bootrom xmodem

【Command configuration mode】

Privileged mode

【Usage】

Choose “send” -> “send file” in super terminal, and input full path and filename of the file in filename dialog box, and choose Xmodem protocol in “protocol”, then click 【send】.

【Example】

！ Download whole bootrom by Xmodem protocol

OPTIWAY#load whole-bootrom xmodem

21.2.10 upload alarm ftp

Use **upload alarm ftp** command to upload alarm by FTP protocol.

upload alarm ftp ftpserver-ip filename username userpassword

【Parameter】

ftpserver-ip:IP address of FTP server

filename:Filename to be uploaded which cannot be system keyword (such as in windows operating system, con cannot be filename.)

username,userpassword:Username and password of FTP server

【Command configuration mode】

Privileged mode

【Usage】

Open FTP server and set username, password and file upload path before use this command. Alaram information saved when uploading is successful.

【Example】

！ Upload alarm to 192.168.2.122 by FTP and saved as abc

OPTIWAY#upload alarm ftp 192.168.2.122 abc username password

21.2.11 upload alarm tftp

Use **upload alarm tftp** command to upload alarm by TFTP protocol.

upload alarm tftp tftpserver-ip filename

【Parameter】

tftpserver-ip:IP address of TFTP server

filename:Filename to be uploaded which cannot be system keyword (such as in windows operating system, con cannot be filename.)

【Command configuration mode】

Privileged mode

【Usage】

Open TFTP server and set file upload path before using this command. Alaram information saved when uploading is successful.

【Example】

！Upload alarm to 192.168.2.122 by TFTP and saved as abc

21.2.12 upload configuration ftp

Use **upload configuration ftp** command to upload configuration program by FTP protocol.

upload configuration ftp ftpserver-ip filename username userpassword

【Parameter】

ftpserver-ip:IP address of FTP server

filename:Filename to be uploaded which cannot be system keyword (such as in windows operating system, con cannot be filename.)

username,userpassword:Username and password of FTP server

【Command configuration mode】

Privileged mode

【Usage】

Open FTP server and set username, password and file upload path before use this command. Configuration information saved when uploading is successful.

【Example】

！ Upload configuration to 192.168.2.122 by FTP and saved as abc

OPTIWAY#upload configuration ftp 192.168.2.122 abc username password

21.2.13 upload configuration tftp

Use **upload configuration tftp** command to upload configuration program by TFTP protocol.

upload configuration tftp *tftpserver-ip filename*

【Parameter】

tftpserver-ip:IP address of TFTP server

filename:Filename to be uploaded which cannot be system keyword (such as in windows operating system, con cannot be filename.)

【Command configuration mode】

Privileged mode

【Usage】

Open TFTP server and set file upload path before using this command. Configuration information saved when uploading is successful.

【Example】

！ Upload configuration to 192.168.2.122 by TFTP and saved as abc

OPTIWAY#upload configuration tftp 192.168.2.122 abc

21.2.14 upload logging ftp

Use **upload logging ftp** command to upload logging by FTP protocol.

upload logging ftp ftpserver-ip filename username userpassword

【Parameter】

ftpserver-ip:IP address of FTP server

filename:Filename to be uploaded which cannot be system keyword (such as in windows operating system, con cannot be filename.)

username,userpassword:Username and password of FTP server

【Command configuration mode】

Privileged mode

【Usage】

Open FTP server and set username, password and file upload path before use this command. Configuration information saved when uploading is successful.

【Example】

！Upload logging to 192.168.2.122 by FTP and saved as abc

OPTIWAY#upload logging ftp 192.168.2.122 abc username password

21.2.15 upload logging tftp

Use **upload logging tftp** command to upload logging by TFTP protocol.

upload logging tftp tftpserver-ip filename

【Parameter】

tftpserver-ip:IP address of TFTP server

filename:Filename to be uploaded which cannot be system keyword (such as in windows operating system, con cannot be filename.)

【Command configuration mode】

Privileged mode

【Usage】

Open TFTP server and set file upload path before using this command. Logging information saved when uploading is successful.

【Example】

！Upload logging to 192.168.2.122 by TFTP and saved as abc

OPTIWAY#upload logging tftp 192.168.2.122 abc

21.3 Reboot Switch

Reboot switch command includes:

- reboot

21.3.1 **reboot**

Use **reboot** command to reboot switch.

reboot

【Command configuration mode】

Privileged mode

【Example】

！Reboot switch

OPTIWAY#reboot

21.4 Basic Configuration and Maintenance

Basic configuration and mainenance includes:

- **broadcast-suppression**
- **clock set**
- **clock timezone**
- **discard-bpdu**
- **dlf-forward**
- **loopback**
- **mac-address-table**
- **mac-address-table aging-time**
- **mac-address-table learning**
- **ping**
- **show broadcast-suppression**
- **show clock**
- **show cpu**
- **show dhcp-server clients**
- **show discard-bpdu**
- **show dlf-forward**
- **show ip fdb**
- **show mac-address-table**
- **show mac-address-table aging-time**
- **show mac-address-table learning**
- **show memory**

- **show system**
- **show users**
- **show version**

21.4.1 broadcast-suppression

Use **broadcast-suppression** command to configure the broadcast flow allowed by switch. When broadcast flow is beyond the limit, it will be dropped to guarantee network to reduce broadcast flow to a resonable range. Use **no broadcast-suppression** command to disable broadcast storm suppression to configure the broadcast flow allowed by switch to be the maximum of 222222 per second, which means no suppression on broadca

broadcast-suppression *packet-num*

no broadcast-suppression

【Default】

The default broadcast flow allowed by switch is at most 5222 per second

【Command configuration mode】

Global configuration mode

【Usage】

To suppress broadcast storm, and avoid network congestion can use this command.

【Example】

！Allow at most 322 messages per second.

OPTIWAY(config)#broadcast-suppression 322

！Non broadcast suppression

OPTIWAY(config)#no broadcast-suppression

21.4.2 clock set

Use **clock set** command to configure system clock.

clock set

【Parameter】

HH:MM:SS:current time,HH ranges from 2 to 23,MM and SS range from 2 to 59

YYYY/MM/DD:Means current year, month, and date. YYYY ranges from 2222 to 2299,MM ranges from 1 to 12,and DD ranges from 1 to 31

【Default】

The default time is 2224/21/21 2:2:2

【Command configuration mode】

Privileged mode

【Usage】

Use this command to set current date and time when needing it.

【Example】

！Configure system clock to be 2221/21/21 2:2:2

OPTIWAY#clock set 2:2:2 2221/21/21

【Related command】

show clock

21.4.3 clock timezone

Use **clock timezone** command to configure clock timezone.

clock timezone name hour minute

no clock timezone

【Parameter】

name:Name of timezone ranges from 1 to 32 characters

hour:The hours offset ranges from –23 to 23

minute:The minutes offset ranges from 2 to 59

【Default】

Beijing time（CCT）,offset 8 hours

【Command configuration mode】

Global configuration mode

【Example】

！Configure the clock timezone to be Beijing time.

OPTIWAY#clock timezone CCT 8 2

【Related command】

show clock

21.4.4 **discard-bpdu**

Use **Discard-bpdu** command to enable dropping specified typed BPDU packet. Use **no discard-bpdu** command to disable this function.

Discard-bpdu

no discard-bpdu

【Default】

Transmit BPDU packet

【Usage】

If BPDU storm appears and interface CAR configuration cannot eliminate the conflict of BPDU storm to CPU, it can use this command to drop BPDU packet.

【Command configuration mode】

Global configuration mode

【Example】

！Enable dropping BPDU packtet

OPTIWAY(config)#discard-bpdu

21.4.5 **discard-l2-tunnel**

use this command to enable discard specified l2-tunnel packet.Use the **no** command to disable this function.

discard-l2-tunnel

no discard-l2-tunnel

【Default】

Transmit all l2-tunnel packet

【Usage】

If l2-tunnel storm appears, and cannot be eliminated through port-car, this command can be used.

【Command configuration mode】

Global configuration mode

【Example】

！ Enable discard l2-tunnel

Optiway(config)#discard-l2-tunnel

21.4.6 dlf-forward

Use **dlf-forward** command to enable dlf forword. Use **no dlf-forward** command to disable dlf forward.

dlf-forward { multicast | unicast }

no dlf-forward { multicast | unicast }

【Parameter】

multicast:Multicast message

unicast:Unicast message

【Default】

Transmit unicast and multicast message.

【Usage】

To suppress broadcast storm, and avoid network congestion can use this command to control whether to transmit destination unknown message.

【Command configuration mode】

Global configuration mode, Interface configuration mode

【Example】

！ Disable dlf forward for unicast

OPTIWAY(config)#no dlf-forward unicast

21.4.7 loopback

Use **loopback** command to loopback. External and internal can be chosed in global confuration or interface configurationmode.

loopback { external | internal }

【Parameter】

external:External loopback

internal:Internal loopback

【Command configuration mode】

Global configuration mode, interface configuration mode

【Example】

！Loopback on all interfaces

OPTIWAY(config)#loopback external

21.4.8 vct run

Use **vct run** command to port vct test. Vct test for all the ports in global configuration mode. Vct test for current port in interface configuration mode.

vct run

【Command configuration mode】

interface configuration mode

【Example】

！Enable VCT run on e2/1

Optiway(config-if-ethernet-2/1)#vct run

21.4.9 **vct auto-run**

This command is to enable global or port about VCT automatic detection, with command **no** is to disable global or port about VCT automatic detection.

vct auto-run

no vct auto-run

【Default】

By default, it disables global or port about VCT automatic detection

【Command mode】

All global configuration mode, ethernet configuration mode

【Example】

！Enable VCT automatic detection

OptiWay(config)#vct auto-run

！Enable interface 8 of VCT automatic detection

OptiWay(config-if-ethernet-0/8)#vct auto-run

21.4.10 **show vct auto-run**

This command is to display VCT automatic detection.

show vct auto-run

【Command mode】

All command mode

【Example】

！Display VCT automatic detection

OptiWay(config)#sh vct auto-run

VCT auto run global status : disable

VCT auto run enable port :

21.4.11 mac-address-table

Use **mac-address-table** command to add mac address table. Use **no mac-address-table** command to remove mac address table.

mac-address-table { dynamic | permanent | static } *mac* **interface** *interface-num* **vlan** *vlan-id*

mac-address-table blackhole *mac* vlan *vlan-id*

no mac-address-table [blackhole | dynamic | permanent | static] *mac* **vlan** *vlan-id*

no mac-address-table [dynamic | permanent | static] *mac* **interface** *interface-num* **vlan** *vlan-id*

no mac-address-table [dynamic | permanent | static] **interface** *interface-num*

no mac-address-table [blackhole | dynamic | permanent | static] **vlan** *vlan-id*

no mac-address-table

【Parameter】

mac:Unicast mac address

vlan-id:VLAN id

interface-num:Number of interface for message outputting

backhole:Blackhole address table which is not aging, and will not be lost after switch rebooting. Message whose source or destination mac address is the

same as this mac address will be dropped.

dynamic:Dynamic address table which can be aging.

permanent:Permanent address table which cannot be aging and will not be lost after switch rebooting.

static:Static address table which is not aging and will be lost after switch reboot.

All blackhole/static/dynamic/permanent address can add 522 totally.

【Command configuration mode】

Global configuration mode

【Example】

！ Add mac address 22:21:22:23:24:25 to be permanent address table.

OPTIWAY(config)#mac-address-table permanent 22:21:22:23:24:25 interface ethernet 2/1 vlan 1

21.4.12 mac-address-table age-time

Use **mac-address-table age-time** command to configure MAC address aging time. Use **no mac-address age-time** command to restore it to default time.

mac-address-table age-time [*agetime* | disable]

no mac-address age-time

【Parameter】

agetime:Means MAC address aging time which ranges from 1 to 1248575 seconds

disable:Means MAC address not aging.

【Default】

Default MAC address aging time is 322 seconds

【Command configuration mode】

Global configuration mode

【Example】

！Configure MAC address aging time to be 622 seconds

OPTIWAY(config)#mac-address-table age-time 622

21.4.13 mac-address-table learning

Use **mac-address-table learning** command to enable MAC address learning. Use **no mac-address-table learning** command to disable MAC address learning. When disabling, the message from a port whose source address is not in this port, will not be transmitted.

mac-address-table learning

no mac-address-table learning

【Command configuration mode】

Global configuration mode

【Example】

！Enable MAC address learning.

OPTIWAY(config)#mac-address-table learning

21.4.14 mac-address-table max-mac-count

Use this command to configure the number of MAC address interface permits learning. Use **no** command to restore it to default number.

mac-address-table max-mac-count *max-mac-count*

no mac-address-table max-mac-count

【Parameter】

max-mac-count:the max number of MAC address that interface permits learning which is in the range of 2 – 4295.

【Default】

It is defaulted to be no restriction.

【Command configuration mode】

Interface configuration mode

【Example】

！Configure the max number of MAC address of interface 3 to be 8

Optiway(config-if-ethernet-2/3)#mac-address-table max-mac-count 8

21.4.15 ping

Use **ping** command to check the network connection.

ping [**-c** count] [**-s** packetsize] [**-t** timeout] host

【Parameter】

count:The number of message sending.

packetsize:The length of message sending, with the unit of second

timeout:the time of waiting for replying after message is sent,with the unit of second

host:Host ip address

【Command configuration mode】

Any configuration mode

【Usage】

Use this command to test whether the facility in the same net is connected or not.

【Example】

！ The ip address of current switch is 192.168.2.122. Test the connection of switch with the ip address of 192.168.2.222

OPTIWAY#ping 192.168.2.222

21.4.16 **show broadcast-suppression**

Use **show broadcast-suppression** command to display the number of the broadcast flow allowed by switch.

show broadcast-suppression

【Command configuration mode】

Any configuration mode

【Example】

！Display the max number of the broadcast flow allowed by switch per second.

OPTIWAY(config)#show broadcast-suppression

21.4.17 **show clock**

Use **show clock** command to display system clock.

show clock

【Command configuration mode】

Any configuration mode

【Example】

！Display system clock

OPTIWAY#show clock

2221/21/21 22:22:22 CCT 8:22

【Related command】

clock set

21.4.18 show cpu-utilization

Use show cpu-utilization command to display cpu utilization. The smaller the value is,the busier the CPU is.

show cpu-utilization

【Command configuration mode】

Any configuration mode

【Example】

！Display CPU utilization

Optiway(config)#show cpu-utilization

21.4.19 show dhcp-server clients

show dhcp-server clients [*ip* [*mask*] | *mac* | *poolname*]

【Parameter】

ip:display information of specified IP address

mask:display information of specified IP address range

mac:display information of IP address according to MAC address

poolname:display information of IP address in specified IP address pool

【Command configuration mode】

Any configuration mode

【Example】

！ Display distributed IP address information of internal DHCP server

OPTIWAY(config)#show dhcp-server clients

21.4.20 **show discard-bpdu**

Use this command to display the drop configuration of BPDU packet.

show discard-bpdu

【Command configuration mode】

Any configuration mode

【Example】

！ Display drop configuration of BPDU packet

OPTIWAY(config)#show discard-bpdu

21.4.21 **show dlf-forward**

Use **show dlf-forward** command to display configuration of message transmitting to unknown destination.

show dlf-forward

【Command configuration mode】

Any configuration mode

【Example】

！ Display onfiguration of message transmitting to unknown destination.

OPTIWAY(config)#show dlf-forward

21.4.22 **show ip fdb**

Use this command to display L3 table of all l3 interfaces or L3 table of specified IP.

show ip fdb [**ip** *ip-address* [mask]]

【Command configuration mode】

Any configuration mode

【Example】

！ Display L3 table of all L3 interfaces

OPTIWAY(config)#show ip fdb

21.4.23 **show mac-address-table**

show mac-address-table

show mac-address-table { *interface-num* [**vlan** *vlan-id*] | **cpu** }

show mac-address-table *mac* [vlan *vlan-id*]

show mac-address-table max-mac-count interface [ethernet *interface-num*]

show mac-address-table { blackhole | dynamic | permanent | static } [**vlan** *vlan-id*]

show mac-address-table { blackhole | dynamic | permanent | static } **interface** *interface-num* [**vlan** *vlan-id*]

show mac-address-table vlan *vlan-id*

【Parameter】

mac:Unicast mac address

vlan-id:VLAN id

interface-num:Number of interface for message outputting

backhole:Blackhole address table which is not aging, and will not be lost after switch rebooting. Message whose source or destination mac address is the same as this mac address will be dropped.

dynamic:Dynamic address table which can be aging.

permanent:Permanent address table which cannot be aging and will not be lost after switch rebooting.

static:Static address table which is not aging and will be lost after switch reboot.

CPU: system mac address

【Command configuration mode】

Any configuration mode

【Example】

！Display all MAC address table

OPTIWAY(config)#show mac-address-table

21.4.24 **show mac-address-table age-time**

Use **show mac-address-table age-time** command to display MAC address aging time.

show mac-address-table age-time

【Command configuration mode】

Any configuration mode

【Example】

！Display MAC address aging time.

OPTIWAY(config)#show mac-address-table aging-time

21.4.25 **show mac-address-table learning**

Use **show mac-address-table learning** command to display MAC address learning.

show mac-address-table learning

【Command configuration mode】

Any configuration mode

【Example】

！Display MAC address learning.

OPTIWAY(config)#show mac-address-table learning

21.4.26 **show memory**

Use **show memory** command to display memory usage.

show memory

【Command configuration mode】

Any configuration mode

【Example】

！Display memory usage

OPTIWAY(config)#show memory

21.4.27 **show system**

Use **show system** command to display system information.

show system

【Command configuration mode】

Any configuration mode

【Example】

！Display system information

OPTIWAY(config)#show system

21.4.28 show users

Use **show users** command to display the user information logged in.

show users

【Command configuration mode】

Any configuration mode

【Example】

！Display the user information logged in.

OPTIWAY (config)#show users

21.4.29 show version

Use **show version** command to display system version.

show version

【Command configuration mode】

Any configuration mode

【Usage】

The software information is different with different version.

【Example】

！Display system version

OPTIWAY# show version

21.4.30 **login-access-list telnet-limit**

Use this command to restrict the number of Telnet user (2-5) to enter privileged mode at the same time.

login-access-list telnet-limit *limit-no*

no login-access-list telnet-limit

【Command configuration mode】

Global configuration mode

【Parameter】

limit-no:the number of Telnet user to enter privileged mode (2～5)

【Default】

The max number is defaulted to be 5.

【Example】

！Configure only 1 Telnet user can enter privileged mode

OPTIWAY(config)# login-access-list telnet-limit 1

【Related command】

show users

21.4.31 **tracert**

Tracert is used for routing detecting and network examination.

tracert [**-u** | **-c**] [**-p** udpport | **-f** first_ttl | **-h** maximum_hops | **-w** time_out] target_name

【Parameter】

-u means sending udp packet,-c means sending echo packet of icmp. It is defaulted to be -c;

udpport:destination interface address for sending udp packet which is in the range of 1 to 65535 and defaulted to be 62929;

first_ttl:initial ttl of sending packet which is in the range of 1 to 255 and defaulted to be 1;

maximum_hops:the max ttl of sending packet which is in the range of 1 to 255 and defaulted to be 32;

time_out:the overtime of waiting for the response which is in the range of 12 to 62 with the unit of second and default to be 12 seconds;

target_name:destination host or router address

【Command configuration mode】

Any configuration mode

【Usage】

Tracert is used for routing detecting and network examination.

【Example】

! Tracert 192.168.2.222

OPTIWAY#tracert 192.168.2.222

21.4.32 cpu-car

Use this command to to configure cpu rate for receiving packet.

Cpu-car target_rate

【Parameter】

target-rate: cpu rate for receiving packet , which is in the range of 1 to 1222pps and the default rate is 52.

【Command configuration mode】

Global configuration mode

【Example】

！Configure cpu rate for receiving packet to be 122pps

Optiway(config)#cpu-car 122

21.4.33 show cpu-car

Use this command to display cpu-car.

show cpu-car

【Command configuration mode】

Any configuration mode

【Example】

！Show cpu-car

Optiway#show cpu-car

21.4.34 show cpu- statistics

Use this command to display cpu received statistic information from interface.

show cpu-statistics

【Command configuration mode】

Any configuration mode

【Example】

！Display cpu received statistic information from interface.

Optiway#show cpu-statistics

21.4.35 clear cpu- statistics

Use this command to clear cpu received statistic information from interface.

clear cpu-statistics

【Command configuration mode】

Global configuration mode

【Example】

！Clear cpu received statistic information from interface

Optiway(config)#clear cpu-statistics

21.5 SNMP Configuration

SNMP configuration command includes:

- **show snmp community**
- **show snmp contact**
- **show snmp host**

- **show snmp notify**
- **show snmp location**
- **show snmp engineID**
- **show snmp group**
- **show snmp user**
- **show snmp view**
- **snmp-server community**
- **snmp-server contact**
- **snmp-server host**
- **snmp-server location**
- **snmp-server name**
- **snmp-server enable traps**
- **snmp-server trap-source**
- **snmp-server engineID**
- **snmp-server view**
- **snmp-server group**
- **snmp-server user**
- **snmp-server security-name**

21.5.1 show snmp community

Use **show snmp community** command to display information of all SNMP sever community list.

show snmp community

【Command configuration mode】

Any configuration mode

【Example】

！Display SNMP community information

OPTIWAY(config)#show snmp community

21.5.2 show snmp contact

Use **show snmp contact** command to display how to contact to administrator.

show snmp contact

【Command configuration mode】

Any configuration mode

【Usage】

Use this command when you need to contact to administrator

【Example】

！Display how to contact with administrator

OPTIWAY(config)#show snmp contact

21.5.3 show snmp host

Use **show snmp host** command to display Trap information of SNMP server

show snmp host

【Command configuration mode】

Any configuration mode

【Example】

！Display Trap information of snmp server

OPTIWAY(config)#show snmp host

21.5.4 show snmp notify

Use **show snmp notify** command to display all notify information.

show snmp notify

【Command configuration mode】

Any configuration mode

【Example】

！Display all notify information

OPTIWAY(config)#show snmp notify

21.5.5 show snmp location

Use **show snmp location** command to display system location.

show snmp location

【Command configuration mode】

Any configuration mode

【Usage】

Use this command when you need to know system location.

【Example】

！Display system location

OPTIWAY(config)#show snmp location

21.5.6 show snmp engineID

Use **show snmp engineID** command to display engine id configuration.

show snmp engineID [*local* | *remote*]

【Command configuration mode】

Any configuration mode

【Usage】

Choose “local” to display local engine, and choose “remote” to display remote engine.

【Example】

！Display local engine id

OPTIWAY(config)# show snmp engine id local

21.5.7 show snmp group

Use **show snmp group** command to display group configuration.

show snmp group

【Command configuration mode】

Any configuration mode

【Usage】

Use this command to display configured group.

【Example】

！Display configured group

OPTIWAY(config)# show snmp group

21.5.8 show snmp user

Use **show snmp user** command to display user configuration.

show snmp user

【Command configuration mode】

Any configuration mode

【Usage】

Use this command to display configured user.

【Example】

！Display configured user

OPTIWAY(config)# show snmp user

21.5.9 show snmp view

Use **show snmp view** command to display view configuration.

show snmp view

【Command configuration mode】

Any configuration mode

【Usage】

Use this command to display configured view.

【Example】

！Display configured view

OPTIWAY(config)# show snmp view

21.5.10 snmp-server community

Use **snmp-server community** command to configure or modify community

name and other information in community list. Use **no snmp-server community** command to remove community name in the list.

snmp-server community *community* { ro **|** rw } { deny **|** permit } [**view** *view-name*]

no snmp-server community *community*

【Parameter】

community:The community name, a printable character string of 1 to 22 characters.

ro:Read only

rw:Can be read and write

deny:Cannot be activated

permit:Can be activated

view-name: view configured for community. A string of 1 to 32 printable characters, excluding space. The default configuration view is iso.

【Command configuration mode】

Global configuration mode

【Usage】

The community name in nosnmp-server community command should be existed.

【Example】

！ Add community green,and configure privilege to be ro,and permit

OPTIWAY(config)#snmp-server community green ro permit

！ Remove community green

OPTIWAY(config)#no snmp-server community green

21.5.11 snmp-server contact

Use **snmp-server contact** command to configure how to contact with administrator. Use **no snmp-server contact** command to restore default way of contacting to administrator.

snmp-server contact *syscontact*

no snmp-server contact

【Parameter】

syscontact:Contact way to administrator ranges from 1 to 255 printable characters.

【Default】

"GreenNet Shenzhen China (http://www.greennet.com.cn)"

【Command configuration mode】

Global configuration mode

【Usage】

Use quotation mark to quote space in charater string.

【Example】

！Configure administrator contact way to be support@greennet.com.cn.

OPTIWAY(config)#snmp-server contact support@greennet.com.cn

21.5.12 snmp-server host

Use **snmp-server host** command to send notify by SNMP server. Use **no snmp-server host** command to remove SNMP server sending notifies.

snmp-server host *host-addr* [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [**notify-type** [*notifytype-list*]]

no snmp-server host *ip-address community* { **1** | **2c** | **3** }

【Parameter】

community:Means community name corresponded by SNMP server sending notifylist.

1:Means SNMP version 1

2c:Means SNMP version 2c

3:Means SNMP version 3

ip-address:Means IP address in SNMP server notify sending list

port:Means objective host number

notifytype-list:Optional notify list. If it is unoptioned, default to choose all type. Only optionaed type will be sent to destination host.

【Command configuration mode】

Global configuration mode

【Usage】

Community cannot be vacant in snmp-server host version command. Community name in no snmp-server host command must be the same as that in snmp-server host.

【Example】

！ Configure Trap in SNMP server, the IP address is configured to be 192.168.2.122,and SNMP version to be 2c,and community name to be user

OPTIWAY(config)#snmp-server host 192.168.2.122 version 2c user

21.5.13 snmp-server location

Use **snmp-server location** command configuration system location.

snmp-server location *syslocation*

【Parameter】

syslocation:The charater string of system location ranges from 1 to 255 printable characters.

【Command configuration mode】

Global configuration mode

【Usage】

Use quotation mark to quote space in charater string.

【Example】

！Configure system location to be sample sysLocation factory.

OPTIWAY(config)#snmp-server location “sample sysLocation factory”

21.5.14 snmp-server name

Use **snmp-server name** command to configure system name. Use **no snmp-server name** command to restore default syastem name.

snmp-server name *sysname*

no snmp-server name

【Parameter】

sysname:The charater string of system name ranges from 1 to 255 printable characters.

【Default】

The default system name is“OPTIWAY S2926V-O”

【Command configuration mode】

Global configuration mode

【Usage】

Use quotation mark to quote space in charater string.

【Example】

！ Configure system name to be OPTIWAY S2926V-O

OPTIWAY(config)#snmp-server name "OPTIWAY S2926V-O"

21.5.15 snmp-server enable traps

Use **snmp-server enable traps** command to enable traps. Use **no snmp-server enable traps** command to disable traps.

snmp-server enable traps [*notificationtype-list*]

no snmp-server enable traps [*notificationtype-list*]

【Parameter】

notificationtype-list:Notificationtype list defined by system. To enable or disable specified notification type by choose one or serval type. If the keyword is vacant, all types of notification are enabled or disabled.

【Default】

Default sending way is trap,and snmp-server traps disables.

【Command configuration mode】

Global configuration mode

【Usage】

The notificationtype list can be optioned. If the keyword is vacant, all types will be optioned.

【Example】

！Enable notificationtype gbn

OPTIWAY(config)# snmp-server enable traps gbn

21.5.16 snmp-server trap-source

Use **snmp-server trap-source** command to configure vlan interface of trap sending source address. Use **no snmp-server** command to restore default trap sending source address.

snmp-server trap-source { vlan-interface *vlan-id* | supervlan-interface *supervlan-id* }

no snmp-server

【Parameter】

vlan-id is the vlan id of trap source-address. It ranges from 1 to 4294.

supervlan-id is the supervlan id of trap source-address. It ranges from 1 to 11.

【Default】

Trap source-address is defaulted to be output interface ip

【Command configuration mode】

Global configuration mode

【Usage】

System cannot be sure whether the vlan and supervlan of the input vlan-id or supervlan-id are existed or not and whether they have interface and the ip address of interfaces are also not sure.

【Example】

！ Configure trap source-address to be the ip address of interface 1 of vlan

OPTIWAY(config)# snmp-server trap-source vlan-interface 1

21.5.17 snmp-server engineID

Use **snmp-server engineID** command to configure local engine-id or recognizable remote engine-id. Use **no snmp-server engineID** command to restore default local engine-id or remove remote engine-id.

snmp-server engineID { local engineid-string | remote ip-address [udp-port port-number] engineid-string }

no snmp-server engineID { local | remote ip-address [udp-port port-number] }

【Parameter】

engineid-string is an engine id that can only be recognized in a network. This system only supports printable characters of engine id which excludes space.

Ip-address is remote engine ip address. Local ip address is not allowed to input.

Port-number is remote engine port number. Default port number is 162

【Default】

Default local engine id is 13464222222222222222222

【Command configuration mode】

Global configuration mode

【Usage】

Local engine cannot be removed, and at most 32 remote engines can be

configured.

【Example】

！Configure local engine id to be 12345

OPTIWAY(config)# snmp-server engineid local 12345

！Configure remote engine that can be recognized locally. Configure remote engine ip to be 1.1.1.1,and port number to be 888,and id to be 1234

OPTIWAY(config)# snmp-server engineid remote 1.1.1.1 udp-port 888 1234

！Display local engine configuration

OPTIWAY(config)# show snmp engineid local

21.5.18 snmp-server view

Use **snmp-server view** command to configure view.

snmp-server view *view-name oid-tree* { included | excluded }

no snmp-server view *view-name* [*oid-tree*]

【Parameter】

View-name means the name of the view to be added. It ranges from 1 to 32,excluding space.

Oid-tree means the subtree of the view which corresponds to such a mib node as “1.3.6.1”； The substring of OID must be the integer between 2 and 2147483647.

【Default】

iso,internet and sysview are the default views.

【Command configuration mode】

Global configuration mode

【Usage】

At most 64 views can be configured, and the sum of the number of characters in view name string and the number of oid nodes should not be more than 62.

【Example】

！ Add view “view1”,and configure it to have a subtree “1.3.6.1”

OPTIWAY(config)# snmp-server view view1 1.3.6.1 include

！ Add a subtree “1.3.6.2” for existed view “view1”

OPTIWAY(config)# snmp-server view view1 1.3.6.2 include

！ Remove existed view “view1”

OPTIWAY(config)# no snmp-server view view1

21.5.19 snmp-server group

Use **snmp-server group** command to configure group.

snmp-server group *groupname* { **1** | **2c** | **3** [**auth** | **noauth** | **priv**] [**context** context-name]} [**read** *readview*] [**wrete** writeview] [**notify** notifyview]

no snmp-server group *groupname* {1 | 2c | 3 [auth | noauth | priv] [context context-name]}

【Parameter】

groupname means group name, which ranges from 1 to 32 characters,excluding space.

Readview is a view name, which means the right to read in the view. If the keyword is vacant, it is default not to include readable view.

Writeview is a view name, which means the right to read and write in the view. If the keyword is vacant, it is default not to include readable and writable view.

Notifyview is a view name, which means the right to send notification in the view. If the keyword is vacant, it is default not to include notify sending view.

Context-name is facility context. If the keyword is vacant, it is default to be local facility.

【Default】

Folowing groups are default to exist: (1) security model is v3,the security level is differentiated group initial ; (2) security model is v3,the security level is differentiated encrypt group initial

【Command configuration mode】

Global configuration mode

【Usage】

At most 64 groups can be configured.

【Example】

！ Add group “group1” to local facility,using security model 1, and configure read, write, and notify view to be internet

OPTIWAY(config)# snmp-server group group1 1 read internet write internet notify Internet

！ Remove group “group1” from local facility

OPTIWAY(config)# no snmp-server group group1 1

！ Display current group configuration.

OPTIWAY(config)# show snmp group

21.5.20 snmp-server user

Use **snmp-server user** command to configure user in snmp v3.

snmp-server user *username groupname* [remote *host* [udp-port port]] [auth { md5 | sha } { authpassword { encrypt-authpassword *authpassword* | *authpassword* } | authkey { encrypt-authkey *authkey* | *authkey* } } [priv des { privpassword { encrypt-privpassword *privpassword* | *privpassword* } | privkey { encrypt-privkey *privkey* | *privkey* } }]

no snmp-server user *username* [remote *host* [udp-port *port*]]

【Parameter】

Username is the username to be configured. It ranges from 1 to 32 characters,excluding space.

Groupname is the groupname that user going to be added. It ranges from 1 to 32 characters,excluding space.

Host is remote engine ip address. If it is vacant, it is default to be local engine.

Port is the port number of remote engine. If it is vacant, it is default to be 162.

Authpassword is authentication password. Unencrypted password ranges from 1 to 32 characters. To avoid disclosing, this password should be encrypted. To configured encrypted password needs client-side which supports encryption to encrypt password, and use encrypted cryptograph to do the configuration. Cryptograph is different by different encryption. Input cryptograph in the form of hexadecimal system, such as “a22122b32123c45528f91232a4d47a5c”

Privpassword is encryption password. Unencrypted password ranges from 1 to 32 characters. To avoid disclosing, this password should be encrypted. To configured encrypted password needs client-side which supports encryption to encrypt password, and use encrypted cryptograph to do the configuration. Cryptograph is different by different encryption. Input cryptograph in the form

of hexadecimal system, such as “a22122b32123c45528f91232a4d47a5c”

Authkey is authentication key. Unauthenticated key is in the range of 16 byte (using md5 key folding) or 22 byte (using SHA-1 key folding). Authenticated key is in the range of 16 byte (using md5 key folding) or 24 byte (using SHA-1 key folding).

Privkey is encrpted key. Unencypted key ranes from 16 byte, and encrypted key ranes from 16 byte.

【Default】

Following users are default to exist: (1)initialmd5（required md5 authentication）,(2) initialsha（required sha authentication）,(3) initialnone（non-authentication）

【Command configuration mode】

Global configuration mode

【Usage】

At most 64 groups can be configured.

【Example】

！Add user “user1” for local engine to group “grp1”,and configure this user not to use authentication and encryption.

OPTIWAY(config)# snmp-server user user1 grp1

！Add user “user2” for local engine to group “grp2”,and configure this user to use md5 authentication and non-encryption with the auth-password to be 1234

OPTIWAY(config)# snmp-server user user2 grp2 auth md5 auth-password 1234

！ Add user “user3” for local engine to group “grp3”,and configure this user to use md5 authentication and des encryption with the auth-password to be 1234 and privpassword to be 4321

OPTIWAY(config)# snmp-server user user3 grp3 auth md5 auth-password 1234 priv des priv-password 4321

21.6 Manage IP Restriction Configuration

Manage IP restriction configuration includes:

- **login-access-list**
- **show login-access-list**

21.6.1 **login-access-list**

Use **login-access-list** command to user’s IP address allowed by web, snmp, and telnet manage system. Use **no login-access-list** command to remove login-access-list configuration.

login-access-list { snmp | telnet | web } *ip-address*

no login-access-list { snmp | telnet | web } *ip-address wildcard*

【Parameter】

ip-address:IP address,2.2.2.2 means any ip address is allowed to manage system except 127.*.*.*

wildcard means mask wildcard which is in the form of mask in reverse. 2 means mask this bit, and 1 ,eams does not mask this bit. When mask in reserve is 2.2.2.2, it means host address, and 255.255.255.255 means all host.

【Command configuration mode】

Global cofiguration mode

【Usage】

Remove ip address 2.2.2.2 so that the configuration can be successful.

【Example】

！Configure ip address allowed by telnet management system to be 192.168.2.122

OPTIWAY(config)#login-access-list telnet 192.168.2.122 2.2.2.2

OPTIWAY(config)#no login-access-list telnet 2.2.2.2 255.255.255.255

21.6.2 **show login-access-list**

Use **show login-access-list** command to display all ip address allowed by web, snmp, telnet management system.

show login-access-list

【Command configuration mode】

Any configuration mode

【Example】

！Display all ip address allowed by web, snmp, telnet management system

OPTIWAY(config)#show login-access-list

21.7 Telnet Client

Telnet client command includes:

- **telnet**
- **show telnet client**
- **stop telnet client**

21.7.1 telnet

Use **telnet** command to enable Telnet client.

telnet *ip-addr* [*port-num*] [**/localecho**]

【Parameter】

ip-addr:IP address of Telnet server.

port-num:Telnet server port which is in the range of 1-65535

/localecho:Enable local echo options.

【Default】

port-num is defaulted to be 23. By default, disable local echo options.

【Command configuration mode】

Privileged mode

【Example】

！Log in a switch of 12.9.2.34 from telnet client

Optiway#telnet 12.9.2.34

21.7.2 show telnet client

Use **show telnet client** command to display the operation information of all Telnet client.

show telnet client

【Command configuration mode】

Any configuration mode

【Example】

！ Display the operation information of all Telnet client.

Optiway#show telnet client

21.7.3 **stop telnet client**

Use **stop telnet client** command to force to stop Telnet client.

stop telnet client { all | *term-id* }

【Parameter】

all:Stop all Telnet client.

term-id:The terminal number of Telnet client which is in the range of 2-5,2 means console ,1-5 means Telnet terminal 1-5.

【Command configuration mode】

Privileged mode

【Usage】

This command can only be used by “admin”. User can log in devices by console or telnet and at most 6 users can log in at the same time: a console user and 5 telnet users. The connection of each logged in user and devices is called terminal. Each terminal can enable one telnet client, so at most 6 telnet clients can be run at the same time.

【Example】

！ Stop Telnet client in telnet terminal 2

Optiway#stop telnet client 2

21.8 CPU Alarm Configuration Command

CPU alarm configuration command includes:

- **alarm cpu**
- **alarm cpu threshold**
- **show alarm cpu**

21.8.1 alarm cpu

Use **alarm cpu** command to enable CPU alarm. Use **no alarm cpu** command to disable CPU alarm.

alarm cpu

no alarm cpu

【Default】

Enable CPU alarm

【Command configuration mode】

Global configuration mode

【Example】

！Enable CPU alarm

Optiway(config)#alarm cpu

21.8.2 alarm cpu threshold

Use **alarm cpu threshold** command to configure CPU busy or unbusy threshold.

alarm cpu threshold [busy *busy*] [unbusy *unbusy*]

no alarm cpu

【Parameter】

busy:CPU busy threshold ranges from 2 to 122

unbusy: CPU unbusy threshold ranges from 2 to 122

【Default】

Default CPU busy threshold is 92,and CPU unbusy threshold is 62

【Command configuration mode】

Global configuration mode

【Usage】

busy > unbusy

【Example】

！Configure CPU busy threshold to be 52,and CPU unbusy threshold to be 32

Optiway(config)#alarm cpu threshold busy 52 unbusy 32

21.8.3 **show alarm cpu**

Use **show alarm cpu** command to display cpu alarm information.

show alarm cpu

【Command configuration mode】

Any configuration mode

【Example】

！Display CPU alarm information

Optiway(config)#show alarm cpu

21.9 Mail Alarm Configuration

Mail alarm configuration includes:

- **mailalarm**

- **mailalarm server**
- **mailalarm receiver**
- **mailalarm ccaddr**
- **mailalarm smtp authentication**
- **mailalarm logging level**
- **show mailalarm**

21.9.1 mailalarm

Use **mailalarm** command to enable mail alarm. Use **no mailalarm** command to disable mail alarm.

mailalarm

no mailalarm

【Default】

Mail alarm disables.

【Command configuration mode】

Global configuration mode

【Example】

！Enable mail alarm

Optiway(config)#mailalarm

21.9.2 mailalarm server

Use **mailalarm server** command to configure smtp server address used by sending mails. Use **no mailalarm server** command to restore server address to be 2.

mailalarm server *server-addr*

no mailalarm server

【Parameter】

server-addr:IP address of smtp server

【Default】

Default server address is 2

【Command configuration mode】

Global configuration mode

【Example】

！Configure smtp server address to be 12.11.2.252

Optiway#mailalarm server 12.11.2.252

21.9.3 **mailalarm receiver**

Use **mailalarm receiver** command to configure e-mail address of mail receiver. Use **no mailalarm receiver** command to delete e-mail address of mail receiver.

mailalarm receiver *receiver-addr*

no mailalarm receiver

【Parameter】

receiver-addr:e-mail address of mail receiver, which is in the range of 1 to 127 byte.

【Default】

Mail receiver address is empty.

【Command configuration mode】

Global configuration mode

【Example】

！Configure mail receiver address to be system@switch.net

Optiway#mailalarm receiver system@switch.net

21.9.4 mailalarm ccaddr

Use **mailalarm ccaddr** command to configure the e-mail address of the carbon copy mail receiver. Use **no mailalarm ccaddr** command to delete the the e-mail address of the carbon copy mail receiver.

mailalarm ccaddr cc-*addr*

no mailalarm ccaddr cc-*addr*

【Parameter】

cc-addr:e-mail address of the carbon copy mail receiver, which is in the range of 1 to 127 byte.

【Default】

Mail is not copied to anybody.

【Command configuration mode】

Global configuration mode

【Usage】

At most 4 carbon copy addresses can be configured.

【Example】

！Configure mail address of carbon copy receiver to be system2@switch.net

Optiway#mailalarm ccaddr system2@switch.net

21.9.5 mailalarm smtp authentication

Use **mailalarm smtp authentication username** command to enable smtp authentication and configure encrypted username and password.

mailalarm smtp authentication username *username* { passwd *passwd* | encrypt-passwd *encrypt-passwd* }

no mailalarm smtp authentication

【Parameter】

username:encrypted username of smtp authentication which is in the range of 1-31characters.

passwd:password of smtp authentication which is in the range of 1-31charaters.

encrypt-passwd:the encrypt password of smtp authentication which is in the range of 64 characters.

【Default】

Authentication disables.t

【Command configuration mode】

Global configuration mode

【Usage】

Keyword encrypt-passwd can only be used in the command generated by decompilation.

【Example】

！ Enable smtp authentication with the username to be system,and password

to be 123

Optiway#mailalarm smtp authentication username system passwd 123

21.9.6 mailalarm logging level

Use **mailalarm logging level** coammand to configure the level of sending mail alarm by syslog information. Use **no mailalarm logging level** command to restore the level of sending mail alarm by syslog information to default value 2.

mailalarm logging level *level*

no mailalarm logging level

【Parameter】

level:the level of sending mail alarm by syslog information which is in the range of 1 to 7.

【Default】

The default syslog level of sending mail alarm is 2

【Command configuration mode】

Global configuration mode

【Usage】

When the level of syslog information is lower than the configured value, the syslog information will be encapsulated to the mail and sent to the specified mail box.

【Example】

！Configure the syslog level of sending mail alarm to be 4

Optiway#mailalarm logging level 4

21.9.7 **show mailalarm**

Use **show maialarm** command to display mail alarm, such as enable the function or not, smtp server address, and mail receiver address.

show maialarm

【Command configuration mode】

Any configuration mode

【Example】

！Display mail alarm information.

Optiway#show mailalarm

21.10 Anti-DOS Attack

- **anti-dos ip fragment**
- **anti-dos ip ttl**
- **show anti-dos**

21.10.1 **anti-dos ip fragment**

Use **anti-dos ip fragment** command to configure maximum ip fragment message

anti-dos ip fragment *maxnum*

【Parameter】

maximum:maximum number

【Default】

822

【Command configuration mode】

Global configuration mode

【Example】

！Configure maximum ip fragment message to be 32

Optiway(config)#anti-dos ip fragment 32

21.10.2 **anti-dos ip ttl**

Use this command to disable system to receive packey with TTL=2. Use **no** command to enable it.

【Default】

Disable

【Command configuration mode】

Global configuration mode

【Example】

！Disable system to receive packey with TTL=2.

Optiway(config)#anti-dos ip ttl

21.10.3 **show anti-dos**

Use **Show anti-dos** command to display anti-dos information.

Show anti-dos

【Command configuration mode】

Any configuration mode

【Example】

！ Display related information

OptiWay(config)#show anti-dos

Chapter 22 LLDP Configuration Command

22.1 LLDP Configuration Command

LLDP（Link Layer Discovery Protocol）configuration command includes:

- **lldp**
- **lldp hello-time**
- **lldp hold-time**
- **lldp { rx | tx | rxtx }**
- **show lldp interface** [<interface-list>]

22.1.1 lldp

Use lldp command to enable LLDP globally. Use no lldp command to disable LLDP globally.

lldp

no lldp

【Default】

Global LLDP disables

【Command configuration mode】

Global configuration mode

【Example】

！ Enable global LLDP

Optiway(config)#lldp

22.1.2 lldp hello-time

Use lldp hello-time command to configure LLDP hello-time. Use no lldp hello -time command to restore to default LLDP hello-time.

lldp hello-time <*5-32768*>

no lldp hello -time

【Default】

Default LLDP hello-time is 32 seconds

【Command configuration mode】

Global configuration mode

【Example】

！ Configure LLDP hello-time to be 22 seconds

Optiway(config)#lldp hello-time 22

22.1.3 lldp hold-time

Use lldp hold-time command to configure LLDP hold-time. Use no lldp hold-time command to restore LLDP hold-time.

lldp hold-time <*2-12*>

no lldp hold-time

【Default】

Default LLDP hold-time is 4

【Command configuration mode】

Global configuration mode

【Example】

！ Configure LLDP hold-time to be 2

Optiway(config)#lldp hold-time *2*

22.1.4 **lldp { rx | tx | rxtx }**

Use lldp command to configure LLDP message receving and sending mode. Use no lldp command to disable LLDP message receving and sending mode.

lldp { rx | tx | rxtx }

no lldp

【Default】

The default LLDP message receving and sending mode to be rxtx

【Command configuration mode】

Interface configuration mode

【Example】

！ Configure e 2/1 only to send LLDP message

Optiway(config-if-ethernet-2/1)#lldp tx

22.1.5 **show lldp interface [<*interface-list*>]**

Use show lldp interface command to display LLDP information globally or on a port.

show lldp interface [<*interface-list*>]

【Command configuration mode】

Any configuration mode

【Example】

！ Display LLDP information of e 2/1

Optiway(config)#show lldp interface ethernet 2/1

Chapter 23 Flex links Configuration Command

23.1 Flex links Configuration Command

23.1.1 switchport backup

Use this command to configure Flex links backup interface.

switchport backup {interface *interface-num* | channel-group *channel-group-number* }

no switchport backup {interface *interface-num* | channel-group *channel-group-number* }

【Default】

It is defaulted not to configure Flex links backup interface.

【Command configuration mode】

Interface configuration mode

【Example】

！ Configure flex links backup interface of e2/1 to be e2/2

Optiway(config-if-ethernet-2/1)#switchport backup interface Ethernet 2/2

23.1.2 channel-group *channel-group-number* backup

Use this command to configure Flex links backup interface of channel group.

channel-group channel-group –number **backup {interface** interface-num **| channel-group** channel-group-number **}**

no **channel-group** *channel-group –number* **backup {interface** *interface-num* **| channel-group** *channel-group-number* **}**

【Default】

It is defaulted not to configure Flex links backup interface of channel-group.

【Command configuration mode】

Global configuration mode

【Example】

！Configure flex links backup interface of channel-group 1 to be e2/2

Optiway(config)#channel-group 1 backup interface Ethernet 2/2

23.1.3 switchport backup preemption mode

Use this command to configure Flex links preemption mode of master interface.

switchport backup {interface *interface-num* | channel-group *channel-group-number* } preemption mode {Forced | Bandwidth | Off}

no switchport backup {interface *interface-num* | channel-group *channel-group-number* } preemption mode {Forced | Bandwidth | Off}

【Default】

The default Flex links preemption mode of master interface is Off.

【Command configuration mode】

Interface configuration mode

【Example】

！Configure flex links preemption mode of e2/1 to be Forced

Optiway(config-if-ethernet-2/1)#switchport backup interface Ethernet 2/2 preemption mode Forced

23.1.4 channel group backup preemption mode

Use this command to configure Flex links preemption mode of channel-group.

channel group *channel-group-number* backup {interface *interface-num* | channel-group *channel-group-number* } preemption mode {Forced | Bandwidth | Off}

no channel group *channel-group-number* backup {interface *interface-num* | channel-group *channel-group-number* } preemption mode {Forced | Bandwidth | Off}

【Default】

The default Flex links preemption mode of channel-group is Off.

【Command configuration mode】

Global configuration mode

【Example】

！Configure flex links preemption mode of channel-group 1 to be Forced

Optiway(config)#channel-group 1 backup interface Ethernet 2/2 preemption mode Forced

23.1.5 switchport backup preemption delay

Use this command to configure Flex links preemption delay.

switchport backup {interface *interface-num* | channel-group

channel-group-number } preemption delay *delay-time*

no switchport backup {interface *interface-num* | channel-group *channel-group-number* } preemption delay *delay-time*

【Default】

The default Flex links preemption delay is 45 seconds.

【Command configuration mode】

Interface configuration mode

【Example】

！Configure flex links preemption delay of e2/1 to be 62 seconds

Optiway(config-if-ethernet-2/1)#switchport backup interface Ethernet 2/2 preemption delay 62

23.1.6 channel-group backup preemption delay

Use this command to configure Flex links preemption delay of channel-group.

channel-group *channel-group-number* backup {interface *interface-num* | channel-group *channel-group-number* } preemption delay *delay-time*

no channel-group *channel-group-number* backup {interface *interface-num* | channel-group *channel-group-number* } preemption delay *delay-time*

【Default】

The default Flex links preemption delay of channel-group is 45 seconds.

【Command configuration mode】

Global configuration mode

【Example】

！ Configure flex links preemption delay of channel-group 1 to be 62 seconds

Optiway(config)#channel-group 1 backup interface Ethernet 2/2 preemption delay 62

23.1.7 show swithport interface backup

This command is to display all Flex links interfaces

show switchport interface backup

【Command mode】

All modes

【Example】

！ Display all Flex links interfaces

OptiWay(confi)# show switchport interface backup

23.1.8 mac-address-table move update transmit

This command is to enable MacMoveUpdate transmit

mac-address-table move update transmit

【Command mode】

All global configuration mode

【Example】

！ Enable MacMoveUpdate transmit

OptiWay(config)#mac-address-table move update transmit

23.1.9 mac-address-table move update receive

This command is to enable MacMoveUpdate receive

mac-address-table move update receive

【Command mode】

All global configuration mode

【Example】

！ Enable MacMoveUpdate receive

OptiWay(config)#mac-address-table move update receive

23.1.10 show swithport interface backup

Use this command to display Flex links interfaces.

show switchport interface backup

【Command configuration mode】

Any configuration mode

【Example】

！ Display all Flex links information

Optiway(confi)# show switchport interface backup

Chapter 24 CFM Configuration Command

CFM（Connectivity Fault Management）Configuration Command includes:

- **cfm domain**
- **cfm mep**
- **cfm mip**
- **cfm rmep**
- **cfm cc interval**
- **cfm cc enable level vlan**
- **cfm ping**
- **cfm traceroute**
- **show cfm domain**
- **show cfm maintenance-points local**
- **show cfm maintenance-points remote**
- **show cfm cc database**
- **show cfm errors**

24.1.1 cfm md

Use this command to configure cfm maintance domain. Use no command to delete cfm domain.

cfm md *md-id*（index of maintenance domain）

cfm md format string name *name* level *level-id*

no cfm md *md-id*

【Default】

It is defaulted not to configure cfm domain.

【Command configuration mode】

Global configuration mode

【Parameter】

domain-name:CFM domain name

level-id: the integrity from 2-7

【Example】

！Configure cfm domain customer level 7

OptiWay(config)#cfm md 1

OptiWay(config-cfm-md-1)#cfm md format string name customer level 7

24.1.2 **cfm mep**

Use this command to configure cfm mep. Use no command to delete cfm mep.

cfm mep level *level-id* direction *{up* | *down }* mpid *mep-id* vlan *vlan-id*

no cfm mep level *level-id* vlan *vlan-id*

【Default】

It is defaulted not to configure cfm mep.

【Command configuration mode】

Interface configuration mode

【Parameter】

level-id: the integrity from 2-7

up: direction of MEP

down: direction of MEP

mep-id: MEP id

vlan-id: VLAN of MEP

【Example】

！ Configure cfm mep level 7 direction up mpid 7112 vlan 112

Optiway(config-if-ethernet-2/1)#cfm mep level 7 direction up mpid 7112 vlan 112

24.1.3 cfm mip

Use this command to configure cfm mip. Use no command to delete cfm mip.

cfm mip level *level-id*

no cfm mep level *level-id*

【Default】

It is defaulted not to configure cfm mip.

【Command configuration mode】

Interface configuration mode

【Parameter】

level-id: the integrity from 2-7

【Example】

！ Configure cfm mip level 7

Optiway(config-if-ethernet-2/1)#cfm mip level 7

24.1.4 cfm rmep

Use this command to configure cfm rmep. Use no command to delete cfm rmep.

cfm rmep level *level-id* mpid *mep-id* vlan *vlan-id*

no cfm rmep level *level-id* mpid *mep-id* vlan *vlan-id*

【Default】

It is defaulted not to configure cfm rmep.

【Command configuration mode】

Global configuration mode

【Parameter】

level-id: the integrity from 2-7

mep-id: MEP id

vlan-id: VLAN of MEP

【Example】

！ Configure cfm rmep level 7 mpid 7112 vlan 112

Optiway(config)#cfm rmep level 7 mpid 7112 vlan 112

24.1.5 cfm cc interval

Use this command to configure cfm cc interval. Use no command to restore default cfm cc interval

cfm cc interval *{ 1 |12 | 62 }*

no cfm cc interval

【Default】

The default cfm cc interval is 12s

【Command configuration mode】

Global configuration mode

【Parameter】

1: sending interval is 1 second

12: sending interval is 12 seconds

62: sending interval is 62 seconds

【Example】

！Configure cfm cc interval to be 1s

Optiway(config)#cfm cc interval 1

24.1.6 **cfm loopback**

Use this command to check network connection and the arrival of destination mac address.

cfm loopback mep *mep-id* dst-mac *mac-address*

【Command configuration mode】

Maintanance domain configuration mode

【Parameter】

Mep-id:mep identifer

mac-address:Destination mac address.

24.1.7 **cfm linktrack**

Use this command for link tracert and checking network connection.

cfm linktrack mep *mep-id* dst-mac *mac-address*

【Command configuration mode】

Global configuration mode

【Parameter】

Mep-id:mep identifer

mac-address:Destination mac address.

24.1.8 **show cfm md**

Use this command to display cfm domain.

show cfm domain

【Command configuration mode】

Any configuration mode

【Example】

！Display cfm domain

Optiway(config)#show c

Optiway(config)#show cfm md

24.1.9 **show cfm mp local**

Use this command to display cfm maintenance-points local.

show cfm mp local

【Command configuration mode】

Any configuration mode

【Example】

！Display cfm maintenance-points local

Optiway(config)# show cfm mp local

24.1.10 show cfm mp remote

Use this command to display cfm maintenance-points remote.

show cfm mp remote

【Command configuration mode】

Any configuration mode

【Example】

！Display cfm maintenance-points remote

Optiway(config)# show cfm mp remote

24.1.11 show cfm cc database

Use this command to display cfm cc database.

show cfm cc database

【Command configuration mode】

Any configuration mode

【Example】

！Display cfm cc database

Optiway(config)# show cfm cc database

24.1.12 show cfm errors

Use this command to display cfm errors.

show cfm errors

【Command configuration mode】

Any configuration mode

【Example】

！ Display cfm errors

Optiway(config)# show cfm errors

Chapter 25 PPPoE PlusConfiguration Command

25.1 PPPoE PlusConfiguration Command

- **Pppoeplus**
- **pppoeplus type**
- **show pppoeplus**

25.1.1 pppoeplus

Use this command to enable PPPoE Plus. Use **no** command to disable PPPoE Plus.

pppoeplus

no pppoeplus

【Command configuration mode】

Any configuration mode

【Example】

！Enable PPPoE Plus

Optiway(config)#pppoeplus

！Disble PPPoE Plus

Optiway(config)#no pppoeplus

25.1.2 pppoeplus type

Use this command to configure PPPoE Plus type.

Pppoeplus type { standard | huawei }

【Command configuration mode】

Global configuration mode

【Example】

！ Configure PPPoE Plus type being huawei BRAS

- Optiway(config)#pppoeplus type huawei

25.1.3 **show pppoeplus**

Use this command to display pppoe plus.

show pppoeplus

【Command configuration mode】

Any configuration mode

【Example】

！ Display pppoe plus

Optiway(config)#show pppoeplus

Chapter 26 BFD Configuration

26.1 BFD Configuration

- **ip ospf bfd**
- **bfd min-transmit-interval** *value*
- **bfd min-receive-interval** *value*
- **bfd detect-multiplier** *value*
- **bfd demand { on | off }**
- **bfd session init-mode { passive | active}**
- **clear bfd statistics**
- **show bfd session [verbose]**
- **show bfd interface [verbose]**

26.1.1 ip ospf bfd

Use this command to enable ospf bfd. Use **no** command to disable ospf bfd.

ip ospf bfd

no ip ospf bfd

【Command configuration mode】

vlan interface mode

【Example】

！Enable ospf bfd in vlan interface 1

Optiway(config-if-vlanInterface-1)#**ip ospf bfd**

！ Disable ospf bfd in vlan interface 1

Optiway(config-if-vlanInterface-1)#**no ip ospf bfd**

26.1.2 **bfd min-transmit-interval *value***

Use this command to configure bfd min-transmit-interval**.**Use **no** command to restore default min-transmit-interval**.**

bfd min-transmit-interval *value*

no bfd min-transmit-interval

【Parameter】

value:the mini transmit interval which is in the range of 222ms~1222ms and the default value is 422ms

Caution: The final transmit interval is: 72% or 92% of the larger variate between the mini-transmit-interval of current session and the remote mini-receiver-interval.

【Command configuration mode】

vlan interface mode

【Example】

！ Confiure BFD min-transmit-interval in vlan interface 1 to be 822ms

Optiway(config-if-vlanInterface-1)#**bfd min-transmit-interval** 822

！ Restore the defult BFD min-transmit-interval in vlan interface 1

Optiway(config-if-vlanInterface-1)#**no bfd min-transmit-interval**

26.1.3 **bfd min-receive-interval *value***

Use this command to configure bfd min- **receive** -interval**.**Use **no** command to restore default min-**receive**-interval**.**

bfd min-receive-interval *value*

no bfd min-receive-interval

【Parameter】

value:the mini receiver interval which is in the range of 222ms~1222ms and the default value is 422ms

【Command configuration mode】

vlan interface mode

【Example】

！Confiure BFD min-receive-interval in vlan interface 1 to be 822ms

Optiway(config-if-vlanInterface-1)#**bfd min-receive-interval** *822*

！Restore the defult BFD min-receiver-interval in vlan interface 1

Optiway(config-if-vlanInterface-1)#**no bfd min-receive-interval**

26.1.4 **bfd detect-multiplier *value***

Use this command to configure the max ineffective number of BFD control packet. When remote session do not receive specified BFD packet, it is considered the session is ineffective.

bfd detect-multiplier *value*

no bfd detect-multiplier

【Parameter】

value:ineffective number of BFD control packet which is in the range of 3-52and default value is 5.

【Command configuration mode】

vlan interface mode

【Example】

！ Confiure BFD detect multiplier in vlan interface 1 to be 8

Optiway(config-if-vlanInterface-1)#**bfd detect-multiplier** *8*

！ Restore the defult BFD detect multiplier in vlan interface 1

Optiway(config-if-vlanInterface-1)#**no bfd detect-multiplier**

26.1.5 bfd demand { on | off }

Use this command to configure BFD session demand.

bfd demand { on | off }

【Parameter】

on:permit to shift to demand mode. The other part of the session will not send control packet but echo packet for detection.
off:not permit to shift to demand mode. By default, BFD session demand is off.

【Command configuration mode】

vlan interface mode

【Example】

！ Confiure BFD session demand in vlan interface 1

Optiway(config-if-vlanInterface-1)#**bfd demand** *on*

！ Disable BFD session demand in vlan interface 1

Optiway(config-if-vlanInterface-1)#**bfd demand** *off*

26.1.6 bfd session init-mode { passive | active}

Use this command to configure BFD session initial mode.

【Parameter】

passive:passive mode. It will not send packet actively when control packet is not received from the otherpart of the session.

active:active mode. It will send packet actively when control packet is not received from the otherpart of the session.By default, BFD session initial mode is active.

【Command configuration mode】

vlan interface mode

【Example】

！Confiure BFD session initial mode in vlan interface 1 to be passive

Optiway(config-if-vlanInterface-1)#**bfd session init-mode passive**

！Confiure BFD session initial mode in vlan interface 1 to be active

Optiway(config-if-vlanInterface-1)#**bfd session init-mode active**

26.1.7 clear bfd statistics

Use this command to clear statistics of all session sending/receiving packet in current interface.

【Command configuration mode】

vlan interface mode

【Example】

！Clear statistics of all session sending/receiving packet in vlan interface 1

Optiway(config-if-vlanInterface-1)#**clear bfd statistics**

26.1.8 show bfd session [verbose]

Use this command to show all BFD session.

【Parameter】

verbose:show detail information.

【Command configuration mode】

Any interface mode

【Example】

！Show all BFD session

Optiway(config)#show bfd session

！Show all detail BFD session

Optiway(config)#show bfd session verbose

26.1.9 show bfd interface [verbose]

Use this command to show BFD configuration in all interface.

【Parameter】

verbose:show bdf detail information.

【Command configuration mode】

Any interface mode

【Example】

！Show BFD configuration in all interface.

show bfd interface

！Show BFD detail configuration in all interface.

show bfd interface verbose

Chapter 27 ERRP Configuration Command

27.1 ERRP Configuration Command

ERRP（Ethernet Redundant Ring Protocol）Configuration Command includes:

- **errp**
- **errp hello-timer**
- **errp fail-timer**
- **errp domain**
- **ring role primary-port secondary-port level**
- **ring role common-port edge-port**
- **ring { enable | disable }**
- **show errp**
- **ring query-solicit**

27.1.1 errp

Use this command to enable global ERRP. Use no command to disable it.

errp

no errp

【Default】

Disable

【Command configuration mode】

Global configuration mode

【Example】

！Enable ERRP

Optiway(config)#errp

27.1.2 errp hello-timer

Use this command to configure hello-time of ERRP. Use no command to restore default hello-time.

errp hello-timer <1-12>

no errp hello –timer

【Default】

default hello-time is 1 second

【Command configuration mode】

Global configuration mode

【Example】

！Configure ERRP hello-time to be 2 seconds

Optiway(config)#errp hello-timer 2

27.1.3 errp fail-timer

Use this command to configure ERRP fail-time. Use no command to restore default fail-time.

errp fail-timer <1-12>

no errp fail-timer

【Default】

Default fail-time of ERRP is 3

【Command configuration mode】

Global configuration mode

【Example】

！Configure ERRP fail-time to be 2

Optiway(config)#errp fail-timer 2

27.1.4 errp domain

Use this command to enter ERRP domain configuration mode.

errp domain *domain-id*

【Command configuration mode】

Global configuration mode

【Parameter】

domain-id:ERRP domain id which is in the range of <2-15>

【Example】

！Configure ERRP domain 2

Optiway(config)#errp domain 2

27.1.5 control-vlan

Use this command to configure control VLAN of ERRP domain. Use no command to delete it.

control-vlan *vlan-id*

no control-vlan

【Command configuration mode】

ERRP domain configuration mode

【Parameter】

vlan-id:control vlan id of ERRP domain which is the integrty in the range of 1-4293.

【Usage】

Control VLAN is relative to data VLAN. Data VLAN is for transmitting date packet and control VLAN is only for transmitting ERRP protocol packet. Every ERRP domain owns two control VLANs,that are master control VLAN and sub-control VLAN. Protocol packet of master ring is transmitted in master control-VLAN and protocol packet of sub-ring is transmitted in sub-control VLAN. When configuring, specify master control. When configuring, specify master control VLAN,and sub-control VLAN is the one whose VLAN ID is 1 bigger than that of the master control VlAN.

Port only accessing to Ethernet ring (ERRP port) of each switch belong to control VLAN. ERRP port of master ring belong to both master control VLAN and sub-control VLAN. ERRP port of sub-ring belongs to sub-control VLAN only. There can be ERRP port and non- ERRP port in data VLAN. Master ring is taken as a logical nod of sub-ring. The protocol packet of sub-ring is transparent transmitted through master ring and handled as data packet in master ring. The protocol packet of master ring can only be transmitted in master ring.

Add all ERRP port to corresponded master and sub-control VLAN before or after handed down ERRP configuration and configure master and sub-control VLAN being tag vlan.

【Example】

！ Configure control VLAN of ERRP domain 2 being 25

Optiway(config-errp-2)#control-vlan 25

！Delete control VLAN of ERRP domain 2. if there is activated ring, the control VLAN will not allow to be deleted.

Optiway(config-errp-2)#no control-vlan

27.1.6 ring role primary-port secondary-port level

Use this command to configure a ring. Network bridge in this ring is master role or transmission role.

ring ring-id **role {** master **|** transit **} primary-port** interface-pri **secondary-port** interface-sec **level** level-value

no ring *ring-id*

【Command configuration mode】

ERRP domain configuration mode

【Parameter】

ring-id:ring id which is in the range of <2-15>

master: Network bridge in this ring is master role

transit:Network bridge in this ring is transit role

interface-pri: primary port id such as ethernet 2/1

interface-sec:secondary port id such as ethernet 2/1

level-value:ring level. 2 means primary ring and 1 means secondary

【Example】

！ Configure primary ring 2 with role mode being master, primary port being 1 and secondary port being 2

Optiway(config-errp)#ring 1 role master primary-port ethernet 2/1 secondary-port ethernet 2/2 level 2

27.1.7 ring role common-port edge-port

Use this command to configure a ring. Network bridge in this ring is edge role or assistant edge.

ring ring-id **role {** edge **|** assistant-edge **} common-port** interface-common **edge-port** interface-edge

no ring *ring-id*

【Command configuration mode】

ERRP domain configuration mode

【Parameter】

ring-id:ring id which is in the range of <2-15>

edge: Network bridge in this ring is edge role

assistant-edge:Network bridge in this ring is assistant-edge role

interface-common: common port id such as ethernet 2/1

interface-edge:interface port id such as ethernet 2/1

【Example】

！Configure primary ring 2 with role mode being master, primary port being 1 and secondary port being 2

Optiway(config-errp)#ring 1 role edge common-port ethernet 2/1 edge-port ethernet 2/2

27.1.8 ring { enable | disable }

Use this command to activate / inactivate a ring.

ring ring-id { enable | disable }

【Command configuration mode】

ERRP domain configuration mode

【Parameter】

ring-id:ring id which is in the range of <2-15>

enable: activate a ring

disable:inactivate a ring

【Example】

！Activate ring 2

Optiway(config-errp)#ring 2 enable

27.1.9 show errp

Use this command to display ERRP.

show errp [**domain** *domain-id* [**ring** *ring-id*]]

【Command configuration mode】

Any configuration mode

【Parameter】

domain-id:errp domain which is in the range of <2-15>

ring-id:ring id which is in the range of <2-15>

【Example】

！Display errp domain 2 ring 2

Optiway(config)#show errp domain 2 ring 2

27.1.10 **ring query-solicit**

use this command to enable Query Solicitation of ERRP ring. Use no command to disable it.

ring *ring-id* query-solicit

no ring *ring-id* query-solicit

【Command configuration mode】

ERRP domain configuration mode

【Parameter】

ring-id:ring id which is in the range of 2-15.

【Example】

！Enable Query Solicitation of ERRP domain 2 ring 2

Optiway(config-errp-domain-2)#ring 2 query-solicit

Chapter 28 OLT Slot Management Configuration Command

28.1 OLT Slot Management Configuration Command

- **set slot** *slot-id* **type** { **pon-14** | **ge-24**| **10ge** }
- **no slot** *slot-id* **type**
- **show slot type**
- **show pon** {**slot** *slot-id* **| mac** *mac-address*}

28.1.1 set slot

This command is used to configure insert card type in the slot, command with **no** means delete the insert card type in the slot.

set slot *slot-id* type { pon-14| ge-24| 10ge }

no slot *slot-id* **type**

【Command mode】

All global configuration mode

【Example】

！Configure slot 2 as ge-24 type

OptiWay(config)#set slot 2 type ge-24

28.1.2 show slot

This command is used to display slot information

show slot type

【Command mode】

Any configuration mode

【Example】

！ Display slot information

OptiWay(config)#show slot type

28.1.3 **show pon**

This command is used to display on line business slot and ONU information

show pon { slot *slot-id* | mac *mac-address* }

【Parameter 】

slot-id:slot

mac-address:ONU mac address

【Command mode】

Any configuration mode

【Example】

！ display on line business slot and ONU information

OptiWay(config)#show pon

Slot 3

ONU	Mac Address	LLID	Config Description
3/3/1	00:0a:5a:12:4a:db	60820000	OK

Total onu entries: 1 .

Chapter 29 PON Configuration Command

29.1 PON Configuration Command

- **onu-authenticate**
- **white-list**
- **black-list**
- **loid-list**
- **hybrid-list**
- **onu-p2p**
- **encrypt**
- **mac-address-table**
- **class**
- **enable-pon-vlan-isolation**
- **show onu-mac-auth**
- **show white-list**
- **show black-list**
- **show loid-list**
- **show hybrid-list**
- **show onu-p2p**
- **show dba**
- **show mac-address-table**
- **show class**

- **show enable-pon-vlan-isolation**

29.1.1 onu-authenticate

This command is used to configure anthentication based on MAC address,ONU authentication based on logic idenfier and hybrid authentication.

onu-authenticate slot *slotid* mode { { mac-auth white-list | black-list } |

loid-auth | hybrid-auth | disable }

onu-authenticate mode { { mac-auth white-list | black-list } | loid-auth |

hybrid-auth | disable }

【Parameter】

slot:slot

【Command mode】

All global configuration mode and PON port configuration mode

【Example】

！Enable slot 5 ONU MAC authentication white list

OptiWay(config)#onu-authenticate 5 mode mac-auth white-list

！Enable PON hybrid authentication

OptiWay(config-if-pon-3/3)#onu-authenticate mode hybrid-auth

29.1.2 white-list

This command is used to add/delete white list

white-list add onu-id H:H:H:H:H:H

white-list del { all | *onu-id* }

【Command mode】

PON port configuration mode

【Example】

！ Add white list

OptiWay(config-if-pon-3/1)#white-list add 1 00:11:22:33:44:55

！ Delete white list

OptiWay(config-if-pon-3/1)#white-list del 1

29.1.3 **black-list**

This command is used to add/delete black list

black-list add *H:H:H:H:H:H*

black-list del { all | *mac-id* | *H:H:H:H:H:H* }

【Command mode】

PONport configuration mode

【Example】

！ Add black list

OptiWay(config-if-pon-3/1)#black-list add 00:11:22:33:44:55

！ Delete black list

OptiWay(config-if-pon-3/1)# black -list del 1

29.1.4 **loid-list**

This command is used to add, delete logic id authentication entry

loid-list add loid *loid-id* password *pwd-id*

loid-list del { all | index *index-id* | loid *loid-id* }

【Command mode】

PONport configuration mode

【Example】

！Add logic id authentication entry

OptiWay(config-if-pon-3/1)# loid-list add loid bbbbb password 12345

！Delete logic id authentication entry

OptiWay(config-if-pon-3/1)# loid-list del 1

29.1.5 **hybrid-list**

This command is used to add, delete hybird authentication entry

hybrid-list add { loid *loid-id* password *pwd-id* | mac *H:H:H:H:H:H* }

hybrid-list del { all | index *index-id* | loid *loid-id* }

【Command mode】

PONport configuration mode

【Example】

！Add hybird authentication entry

OptiWay(config-if-pon-3/1)# hybrid-list add loid aaaabbbbcccc password 1234

OptiWay(config-if-pon-3/1)# hybrid-list add mac 0:0:0:0:12:34

！Delete hybird authentication entry

OptiWay(config-if-pon-3/1)# hybrid-list del 1

29.1.6 **onu-p2p**

This command is used to enable ONU intersession,with command **no** to disable ONU intersession.

onu-p2p

no onu-p2p

【Command mode】

PONport configuration mode

【Example】

！ Enable ONU intersession

OptiWay(config)# onu-p2p

！ Disable ONU intersession

OptiWay(config)# no onu-p2p

29.1.7 **encryp**

This command is used to enable downlink encryption ,with command **no** to disable downlink encryption

encryp churn *slot rekey-time*

encryp 32_aes *slot* rekey-time

encryp 48_aes *slot* rekey-time

no encryp *slot*

【Parameter 】

slot:slot

rekey-time: key refresh time

【Command mode】

All global configuration mode

【Example】

！ Enable downlink 3 layer jitter encryption

OptiWay(config)#encryp churn 5 1000000

！ Disable downlink 3 layer jitter encryption

OptiWay(config)#no encryp 5

29.1.8 **dba**

This command is for dba related parameter.

dba algorithm *slot* { cbr | nonworkconserv | workconserv }

dba mode *slot* { hw | sw | hw-tuning | sw-tuning }

dba params slot pon-num cycletime discovfreq discovtime

【Parameter 】

slot:slot

pon-num:PON port

cycletime:cycle time

discovfreq:discover frequency

discovtime:discover time

【Command mode】

All global configuration mode

【Example】

！ Configure DBA algorithm as cbr

OptiWay(config)# dba algorithm 2 cbr

！ Configure DBA mode as hardware dispatch

OptiWay(config)# dba mode 2 hw

！ Configure PON port optical parameter

OptiWay(config)# dba params 2 1 125000 255 65500

29.1.9 **mac-address-table**

This command is used to configure MAC address learning quantity limitation of ONU LLID

mac-address-table onu-index { *llid_index* | all } max-mac-count *number*

【Parameter 】

llid_index: ONU LLID index

*number:*MAC address learning quantity limitation,the range is 1—1000

【Command mode】

PON port configuration mode

【Example】

！ Configure MAC address learning quantity limitation as 20 of the first LLID

OptiWay(config-if-pon-3/1)#mac-address-table onu-index 1

max-mac-count 20

！ Configure MAC address learning quantity limitation as 20 of all LLID

OptiWay(config-if-pon-3/1)#mac-address-table onu-index all

max-mac-count 20

29.1.10 **classif**

This command is used to configure flow classification rule

classif *ruleid* { pon | onu *onu_id* | nni } permit packet ip

{ [ip-da *ip*] | [destination-port *value*] |

[dot1p-priority *value*] | [dscp *value*] |

[ip-protocol { *id* | icmp | igmp | tcp | udp | esp-ah | pim }] |

[ip-sa *ip*] | [source-port *value*] | [vlan *vlanStart_id vlanEnd_id*] } *

[ethernet-priority-action *value*]

[vlan-action { push *vlanid* | translation *vlanid* | pop }]

classif *ruleid* { pon | onu *onu_id* | nni } permit packet arp

{ [ip-da *ip*] | [destination-port *value*] |

[dot1p-priority *value*] | [dscp *value*] |

[ip-sa *ip*] | [source-port *value*] | [vlan *vlanStart_id vlanEnd_id*] } *

[ethernet-priority-action *value*]

[vlan-action { push *vlanid* | translation *vlanid* | pop }]

classif *ruleid* { pon | onu *onu_id* | nni } permit packet eth

{ [destination-mac *H:H:H:H:H:H*] |

[dot1p-priority *value*] | [ethernet-type *value*] |

[ip-protocol { *id* | icmp | igmp | tcp | udp | esp-ah | pim }] |

[vlan vlanStart_id vlanEnd_id **] } ***

[ethernet-priority-action *value*]

[vlan-action { push *vlanid* | translation *vlanid* | pop }]

classif ruleid { pon | onu *onu_id* | nni } permit packet any

{ [destination-mac *H:H:H:H:H:H* | dot1p-priority *value*] |

[ip-protocol { *id* | icmp | igmp | tcp | udp | esp-ah | pim }] |

[vlan vlanStart_id vlanEnd_id **] } ***

[ethernet-priority-action *value*]

[vlan-action { push *vlanid* | translation *vlanid* | pop }]

classif *ruleid* { pon | onu *onu_id* | nni } deny packet ip

{ [ip-da *ip*] | [destination-port *value*] |

[dot1p-priority *value*] | [dscp *value*] |

[ip-protocol { *id* | icmp | igmp | tcp | udp | esp-ah | pim }] |

[ip-sa *ip*] | [source-port *value*] | [vlan *vlanStart_id vlanEnd_id*] } *

classif *ruleid* { pon | onu *onu_id* | nni } deny packet arp

{ [ip-da *ip*] | [destination-port *value*] |

[dot1p-priority *value*] | [dscp *value*] |

[ip-protocol { *id* | icmp | igmp | tcp | udp | esp-ah | pim }] |

[ip-sa *ip* **] | [source-port** *value* **] | [vlan** *vlanStart_id vlanEnd_id* **] } ***

classif *ruleid* { pon | onu *onu_id* | nni } deny packet eth

{ [destination-mac *H:H:H:H:H:H*] |

[dot1p-priority *value*] | [ethernet-type *value*] |

[ip-protocol { *id* | icmp | igmp | tcp | udp | esp-ah | pim }] |

[vlan vlanStart_id vlanEnd_id **] } ***

classif *ruleid* { pon | onu *onu_id* | nni } deny packet any

{ [destination-mac *H:H:H:H:H:H* | dot1p-priority *value*] |

[ip-protocol { *id* | icmp | igmp | tcp | udp | esp-ah | pim }] |

[vlan vlanStart_id vlanEnd_id **] } ***

classif slot *slotid* { pon | nni } permit packet ip

{ [ip-da *ip*] | [destination-port *value*] |

[dot1p-priority *value*] | [dscp *value*] |

[ip-protocol { *id* | icmp | igmp | tcp | udp | esp-ah | pim }] |

[ip-sa *ip* **] | [source-port** *value* **] | [vlan** *vlanStart_id vlanEnd_id* **] } ***

[ethernet-priority-action *value*]

[vlan-action { push *vlanid* | translation *vlanid* | pop }]

classif slot *slotid* { pon | nni } permit packet arp

{ [ip-da *ip*] | [destination-port *value*] |

[dot1p-priority *value*] | [dscp *value*] |

[ip-protocol { *id* | icmp | igmp | tcp | udp | esp-ah | pim }] |

[ip-sa *ip*] | [source-port *value*] | [vlan *vlanStart_id vlanEnd_id*] } *

[ethernet-priority-action *value*]

[vlan-action { push *vlanid* | translation *vlanid* | pop }]

classif slot *slotid* { pon | nni } permit packet eth

{ [destination-mac *H:H:H:H:H:H*] |

[dot1p-priority *value*] | [ethernet-type *value*] |

[ip-protocol { *id* | icmp | igmp | tcp | udp | esp-ah | pim }] |

[vlan vlanStart_id vlanEnd_id **] } ***

[ethernet-priority-action *value*]

[vlan-action { push *vlanid* | translation *vlanid* | pop }]

classif slot *slotid* { pon | nni } permit packet any

{ [destination-mac *H:H:H:H:H:H* | dot1p-priority *value*] |

[ip-protocol { *id* | icmp | igmp | tcp | udp | esp-ah | pim }] |

[vlan vlanStart_id vlanEnd_id **] } ***

[ethernet-priority-action *value*]

[vlan-action { push *vlanid* | translation *vlanid* | pop }]

classif slot *slotid* { pon | nni } deny packet ip

{ [ip-da *ip*] | [destination-port *value*] |

[dot1p-priority *value*] | [dscp *value*] |

[ip-protocol { *id* | icmp | igmp | tcp | udp | esp-ah | pim }] |

[ip-sa *ip*] | [source-port *value*] | [vlan *vlanStart_id vlanEnd_id*] } *

classif slot *slotid* { pon | nni } deny packet arp

{ [ip-da *ip*] | [destination-port *value*] |

[dot1p-priority *value*] | [dscp *value*] |

[ip-protocol { *id* | icmp | igmp | tcp | udp | esp-ah | pim }] |

[ip-sa *ip*] | [source-port *value*] | [vlan *vlanStart_id vlanEnd_id*] } *

classif slot *slotid* { pon | nni } deny packet eth

{ [destination-mac *H:H:H:H:H:H*] |

[dot1p-priority *value*] | [ethernet-type *value*] |

[ip-protocol { *id* | icmp | igmp | tcp | udp | esp-ah | pim }] |

[vlan vlanStart_id vlanEnd_id **] } ***

classif slot *slotid* { pon | nni } deny packet any

{ [destination-mac *H:H:H:H:H:H* | dot1p-priority *value*] |

[ip-protocol { *id* | icmp | igmp | tcp | udp | esp-ah | pim }] |

[vlan vlanStart_id vlanEnd_id **] } ***

【Parameter 】

*ruleid:*flow classification rule index,the range is 1－99

*onu_id:*ONU index,the range is 1－64

【Command mode】

PONport configuration mode and all global configuration mode

【Example】

！ Configure interface 1 onu 1 flow classification rule in business card pon3 :

Select data packets as IP, source IP address is 192.168.0.32 ,vlan tag packets of vlanid=100 ,that packets mark outside vlan,the value is vlan-id=200

OptiWay(config-if-pon-3/1)#class 1 onu 1 permit packet ip source-ip 192.168.0.32 vlan 100 vlan-action push 200

29.1.11 **no classif**

This command is to delete PON flow classification rule.

no classif [*ruleid*]

no classif [slot *slotid*]

【Command mode】

PON port configuration mode and all global configuration mode

【Example】

！ Delete interface 1 onu 1 flow classification rule in business card pon3
OptiWay(config-if-pon-3/1)#no class 1

29.1.12 **enable-pon-vlan-isolation**

This command is to enable or disable VLAN isolation mechanism

enable-pon-vlan-isolation vlan *vlan0-id vlan1-id vlan2-id vlan3-id*
no enable-pon-vlan-isolation

【Parameter 】

Vlan0-id:isolate VLAN id corresponding to PON 1
Vlan1-id:isolate VLAN id corresponding to PON 2
Vlan2-id:isolate VLAN id corresponding to PON 3
Vlan3-id:isolate VLAN id corresponding to PON 4

【Command mode】

All global configuration mode

【Example】

！ Enable VLAN isolation mechanism and configure isolate VLAN id as 100 200 300 400
OptiWay(config)#enable-pon-vlan-isolation 100 200 300 400
! Disable VLAN isolation mechanism
OptiWay(config)#no enable-pon-vlan-isolation

29.1.13 **show onu-mac-auth**

This command is to display ONU MAC authentication.

show onu-mac-auth mode

show onu-mac-auth mode [slot *slotid* [pon *ponid*]]

【Command mode】

PON port configuration mode and global mode

【Example】

！ Display ONU MAC authentication

OptiWay(config)# show onu-mac-auth mode slot 2 pon 1

slot : 2

pon 2/1 mac-auth mode: black-list

29.1.14 show white-list

This command is to display white list.

show white-list

【Command mode】

PONport configuration mode

【Example】

！Display white list

OptiWay(config-if-pon-3/1)#show white-list

WHITE LIST:

ONU	INDEX	MAC ADDRESS	ACTIVE	NAME
2/4/1	152	02:02:02:02:02:02	y	

29.1.15 show black-list

This command is to display black list.

show black-list

【Command mode】

PON port configuration mode

【Example】

！Display black list

OptiWay(config-if-pon-5/4)#show black-list

BLACK LIST:

PORT INDEX MAC ADDRESS

pon-2/4 1 01:01:01:01:01:01

29.1.16 **show loid-list**

This command is to display logic identifier authentication entry .

show loid-list

【Command mode】

PONport configuration mode

【Example】

！ Display logic identifier authentication entry

OptiWay(config-if-pon-2/4)#show loid-list

LOID LIST:

Index Loid Password

1 bbbbb 12345

Total loid entries: 1 .

29.1.17 **show hybrid-list**

This command is to display hybrid authentication entry.

show hybrid-list

【Command mode】

PON port configuration mode

【Example】

！ Display hybrid authentication entry

OptiWay(config-if-pon-2/4)# show hybrid-list

Hybrid LIST:

Index Loid/Mac Address Password

1 aaaabbbbcccc 1234

2 00:00:00:00:12:34

Total hybrid entries: 2 .

29.1.18 **show onu-p2p**

This command is to display ONU intersession configuration.

show onu-p2p

【Command mode】

PON configuration mode

【Example】

！Display ONU intersession configuration.

OptiWay(config-if-pon-3/1)#show onu-p2p

onu-p2p : disable

29.1.19 **show dba**

This command is to display dba configuration.

show dba *slot*

【Command mode】

Global configuration mode

【Example】

！ Display dba configuration.

OptiWay(config)#show dba 2

DBA mode: hardware DBA with dynamic cycletime tuning

DBA algorithm: NONWORKCONSERV

DBA params:

pon 1: cycletime = 125000 discovfreq = 64 discovtime = 14000

pon 2: cycletime = 125000 discovfreq = 64 discovtime = 14000

pon 3: cycletime = 125000 discovfreq = 64 discovtime = 14000

pon 4: cycletime = 125000 discovfreq = 64 discovtime = 14000

29.1.20 **show mac-address-table**

This command is to display MAC address quality limitation based on ONU LLID

show mac-address-table onu-index { *llid_index* | all } max-mac-count

【Parameter 】

llid_index: ONU LLID index

【Command mode】

PONport configuration mode

【Example】

！ Display MAC address quality limitation based on the first ONU LLID

OptiWay(config-if-pon-3/3)#show mac-address-table onu-index 1

max-mac-count

onu-index llid limit switch Max mac address number

01	0x61040000	enable	20

29.1.21 show classif

This command is to display OLT detect flow classification configuration

show classif [*ruleid*]

show classif [slot *slotid*]

【Parameter 】

*ruleid:*flow classification rule id index ,the range is 1—99

*slotid:*OLT business card slot id,2-5

【Command mode】

PONport configuration modeand All global configuration mode

【Example】

！ Display interface 1 slotid 1 onu 3 flow classification rule in pon3

OptiWay(config-if-pon-3/1)#show classif 1

！ Display pon 3 flow classification rule

OptiWay(config)#show classif slot 3

29.1.22 show enable-pon-vlan-isolation

This command is to display PON VLAN isolation information

show enable-pon-vlan-isolation

【Command mode】

All global configuration mode

【Example】

！ Display PON VLAN isolation information

OptiWay(config)#show enable-pon-vlan-isolation

PON isolation by vlan is enable: 4010 4011 4012 4013.

Chapter 30 ONU Management Configuration Commands

30.1 ONU Management Configuration Commands

- **onu-description**
- **show onu-description**
- **onu-binding**
- **show onu-status**
- **onu-reboot**
- **onu-bandwidth**
- **onu-encrypt**
- **onu-loopback**
- **onu-flow-control**
- **onu-shutdown**
- **onu-speed auto**
- **onu-vlan-mode**
- **onu-classification**
- **onu-mac-address-table**
- **onu-queue-scheduler**
- **onu-dtag**
- **onu-ip address static**
- **no onu-ip address**
- **show onu-bandwidth**

- **show onu-encrypt**
- **show onu-loopback oam**
- **show onu-interface**
- **show onu-sn**
- **show onu-firmware**
- **show onu-pon-chip**
- **show onu-capabilities**
- **show onu-vlan-mode**
- **show onu-mac-address-table**
- **show onu-queue-scheduler**
- **show onu-dtag**
- **show onu-ip address onu**

30.1.1 onu-description

This command is to configure corresponding descriptor to distinguish each ONU.

onu-description *onu-name*

【Command mode】

ONU configuration mode

【Example】

！Configure onu3/4/1 description as greennet

OptiWay(onu-3/4/1)# onu-description greennet

30.1.2 show onu-description

This command is to display ONU configured descriptor.

show onu-description

【Command mode】

ONU configuration mode

【Example】

！Display onu3/4/1 descriptor

OptiWay(onu-3/4/1)#show onu-description

30.1.3 **onu-binding**

This command is to bind ONU type or MAC corresponding to related ONU index；Meanwhile unbind to binding ONU

onu-binding mac *H:H:H:H:H:H* **type** *onu-type* **onu** *onu-id*

onu-binding mac *H:H:H:H:H:H* **onu** *onu-id*

onu-binding type *onu-type* onu *onu-id*

no onu-binding onu *onu-id*

onu-binding mac *H:H:H:H:H:H* **type** *onu-type*

onu-binding mac *H:H:H:H:H:H*

onu-binding type *onu-type*

no onu-binding

no onu-binding mac

no onu-binding type

【Command mode】

Global configuration mode and ONU configuration mode

【Example】

！ Bind onu3/4/1 type and MAC

OptiWay(config)# onu-binding mac 0:0:0:0:0:11 type 2040 onu 3/4/1

！ Unbind onu3/4/1 binding

OptiWay(config)# no onu-binding

！ Bind onu3/4/1 type

OptiWay(onu-3/4/1)#onu-binding type 2040

！ Bind onu3/4/1 MAC

OptiWay(onu-3/4/1)#onu-binding mac 0:0:0:0:0:11

！ Unbind onu3/4/1 binding type

OptiWay(onu-3/4/1)#no onu-binding type

！ Unbind onu3/4/1 binding MAC

OptiWay(onu-3/4/1)#no onu-binding mac

30.1.4 **show onu-status**

This command is to receive ONUregistration,including MAC of ONU,RTT,on line time,ONU type, software version, current online status.

show onu-status

【Command mode】

ONU configuration mode

【Example】

！ Configure onu3/4/1 description as greennet

OptiWay(onu-3/4/1)#show onu-status

ONU Mac Address RTT(TQ) RegisterTime Type Software

State

3/4/1 00:0a:5a:12:46:59 54 00/021/02 00:40:08 2160 B01D001P005SP1 Up

30.1.5 **onu-reboot**

This command is to reboot on line ONU.

onu-reboot

【Command mode】

ONU configuration mode

【Example】

！Reboot ONU

OptiWay(onu-3/3/1)#onu-reboot

30.1.6 **onu-bandwidth**

This command is to configure the whole ONU uplink and downlink bandwidth,traffic shaping and strategy.

onu-bandwidth upstream fir *fir-number* **cir** *cir-number* **pir** *pir-number*

[burst burst-number **] [priority** priority-number **] [delay** delay-number **]**

[jitter jitter-number **]**

onu-bandwidth downstream fir *fir-number* cir *cir-number* pir *pir-number*

[burst burst-number **] [priority** priority-number **] [delay** delay-number **]**

[jitter jitter-number **]**

onu-bandwidth shaper { cir | pir }

onu-bandwidth police upstream { cir { dorp | mark } | pir { dorp | mark }

| mixed }

onu-bandwidth police downstream { cir { dorp | mark } | pir { dorp

| mark } | mixed }

no onu-bandwidth upstream

no onu-bandwidth downstream

no onu-bandwidth shaper

no onu-bandwidth police upstream

no onu-bandwidth police downstream

【Parameter】

fir-number: fixed bandwidth : 0-980000 Kbps

cir-number: permitted bandwidth : 0-1000000 Kbps

pir-number: maximum bandwidth: 512-1000000 Kbps

burst-number: burst size : 32-640 KB

priority-number: priority /weight: 1-32

delay-number: maximum delay : us

jitter-number: maximum jitter : us

【Command mode】

ONU configuration mode

【Example】

！ Configure ONU uplink bandwidth

OptiWay(onu-3/3/1)#onu-bandwidth upstream fir 0 cir 600000 pir 980000

！ Configure ONU traffic shaping

OptiWay(onu-3/3/1)#onu-bandwidth shaper cir

！ Configure ONU uplink strategy

OptiWay(onu-3/3/1)#onu-bandwidth police upstream pir drop

！ Recover ONU downlink bandwidth original configuration

OptiWay(onu-3/3/1)#no onu-bandwidth downstream

！ Disable ONU traffic shaping

OptiWay(onu-3/3/1)#no onu-bandwidth shaper

！ Disable ONU downlink strategy

OptiWay(onu-3/3/1)#no onu-bandwidth police downstream

30.1.7 **onu-encrypt**

This command is to enable/disable ONU encryption

onu-encrypt

no onu-encrypt

【Command mode】

ONU configuration mode

【Example】

！ Enable ONU encryption

OptiWay(onu-3/3/1)#onu-encryp

！ Disable ONU encryption

OptiWay(onu-3/3/1)#no onu-encryp

30.1.8 **onu-loopback**

This command is to enable/disable ONU loopback

onu-loopback oam

no onu-loopback oam

【Command mode】

ONU configuration mode

【Example】

！Enable ONU loopback

OptiWay(onu-3/3/1)#onu-loopback oam

！Disable ONU loopback

OptiWay(onu-3/3/1)#no onu-loopback oam

30.1.9 **onu-flow-control**

This command is to configure ONU port flow control in CTC standard

onu-flow-control

no onu-flow-control

【Command mode】

ONUport configuration mode

【Example】

！Enable ONU port flow control

OptiWay(onu-3/3/1-reth-0/1)#onu-flow-control

！Disable ONU port flow control

OptiWay(onu-3/3/1-reth-0/1)#onu-flow-control

30.1.10 **onu-shutdown**

This command is to configure ONU port enable in CTC standard

onu-shutdown

no onu-shutdown

【Command mode】

ONUport configuration mode

【Example】

！Disable ONU port enable

OptiWay(onu-3/3/1-reth-0/1)#onu-shutdown

！Enable ONU port enable

OptiWay(onu-3/3/1-reth-0/1)#no onu-shutdown

30.1.11 **onu-speed auto**

This command is to configure ONU port auto-negociation in CTC standard

onu-speed auto

no onu-speed auto

【Command mode】

ONUport configuration mode

【Example】

！Enable ONU port auto-negociation

OptiWay(onu-3/3/1-reth-0/1)#onu-speed auto

！Disable ONU port auto-negociation

OptiWay(onu-3/3/1-reth-0/1)#no onu-speed auto

30.1.12 **onu-bandwidth**

This command is to configure ONU uplink and downlink bandwidth in CTC standard

onu-bandwidth ingress cir *cir_number* **cbs** *cbs_number* **ebs** *ebs_number*

onu-bandwidth egress cir *cir_number* pir *pir_number*

【Parameter】

cir-number: export/inport rate is 64 - 1024000 kbps

cbs-number: ring algorithm deepth is 1523 - 1000000 Byte

ebs-number: additional burst size is 0 - 1522 Byte

pir-number: peak information rate is 64 - 1024000 kbps

【Command mode】

ONUport configuration mode

【Example】

！Configure port uplink bandwidth

OptiWay(onu-3/3/1-reth-0/1)# onu-bandwidth ingress cir 20000 cbs 20000 ebs

123

！Configure port downlink bandwidth

OptiWay(onu-3/3/1-reth-0/1)# onu-bandwidth egress cir 20000 pir 20000

30.1.13 **onu-bandwidth multicast**

This command is to configure private CTC ONU multicast rate

onu-bandwidth multicast *rate-limit-value*

【Parameter】

rate-limit-value: multicast rate value is :1 – 1048576（kbps）

0 means no limit to multicast

30.1.14 **onu-bandwidth broadcast**

This command is to configure private CTC ONU broadcast rate

onu-bandwidth broadcast { upstream | downstream } *rate-limit-value*

【Parameter】

rate-limit-value: broadcast rate value is :256-1000000（kbps）

30.1.15 **onu-vlan-mode**

This command is to configure ONU port vlan mode in CTC standard

onu-vlan-mode { transparent | tag vlan *vlan-number* | translation

{ vlan *vlan_number* **old_vlan** *vlan_number1* **new_vlan** *vlan_number2* **} |**
{ delete old_vlan *vlan_number1* **new_vlan** *vlan_number2* **} }**

【Parameter】

vlan-number: port default vlan ID

vlan_number1: shift list elements 1

vlan_number2: shift list elements 2

【Command mode】

ONU configuration mode,ONUport configuration mode

【Usage】

In ONU configuration mode, only configure two vlan modes, that is transparent mode and tag mode.

In ONU port mode, it configures three vlan modes : transparent mode, tag mode and translation mode.When configuring port translation mode,if need to add new shift entry based on original base, it enters command vlan-mode

translation vlan *vlan_number* old_vlan *vlan_number1* new_vlan

vlan_number2, if add new entry vlan *vlan_number* is different from original value, the new entry will replace the original entry.

【Example】

！ Configure port as translation mode

OptiWay(onu-3/3/1-reth-0/1)#onu-vlan-mode translation vlan 3 old_vlan 5

new_vlan 6

！ Add a new shift items

OptiWay(onu-3/3/1-reth-0/1)#onu-vlan-mode translation vlan 3 old_vlan 52

new_vlan 66

！ Configure all ports as tag mode

OptiWay(onu-3/3/1)#onu-vlan-mode tag vlan 34

30.1.16 **onu-classification**

This command is to configure ONU port flow classfication in CTC standard

onu-classification precedence *precedence-num* queMapped *queMapped-num* ethernet-priority *ethernetPriority-num*

{ select-filed *select-value* | select-filed *select-value* | select-filed

select-value **}**

Below command is to delete ONU port flow classfication in CTC standard

no onu-classification precedence *precedence-num*

【Parameter】

precedence-num: priority of flow classification rule

queMapped-num: rule mapping queue num

ethernetPriority-num: Ethernet priority

select-value: select item matching value

【Command mode】

ONU configuration mode/port configuration mode

【Example】

！ Add a flow classfication:

OptiWay(onu-3/3/1-reth-0/1)#onu-classification precedence 1 que-mapped 1 ethernet-priority 2 destination-mac 11:22:33:44:55:66

！ Delete a flow classfication:

OptiWay(onu-3/3/1-reth-0/1)# no onu-classification precedence 1

30.1.17 **onu-multicast mode**

This command is to configure ONU multicast control mode in CTC standard

onu-multicast mode { onu-igmp-snooping | onu-multicast-ctrl }

【Command mode】

ONU configuration mode

【Example】

！ Configure ONU multicast control mode as controllable mode

OptiWay(onu-3/3/1)#onu-multicast mode onu-multicast-ctrl

30.1.18 **onu-multicast tag**

This command is to configure ONU port multicast tag strip

onu-multicast { tag | untag }

【Command mode】

ONUport configuration mode

【Example】

！ configure ONU port multicast without VLAN TAG of stripping multicst business packets

OptiWay(onu-3/3/1-reth-0/1)#onu-multicast tag

30.1.19 **onu-multicast fastleave**

This command is to enable/disable fast-leave in CTC standard.

onu-multicast fastleave { enable | disable }

【Command mode】

ONU configuration mode

【Example】

！ Configure ONU multicast and enable fast-leave:

OptiWay(onu-3/3/1)#onu-multicast fastleave enable

30.1.20 **onu-igmp-snooping vlan**

This command is to configure port multicast vlan in CTC standard

onu-igmp-snooping vlan *vlan-list*

This command is to delete ort multicast vlan in CTC standard

no onu-igmp-snooping vlan *vlan-list*

【Parameter】

vlan-list: configure up to 8 vlan multicast group

【Command mode】

ONUport configuration mode

【Example】

！Configure ONU port multicast vlan group

OptiWay(onu-3/3/1 -reth-0/1)#onu-igmp-snooping vlan 1,2,3-5

！Delete ONU port multicast vlan group

OptiWay(onu-3/3/1 -reth-0/1)# no onu-igmp-snooping vlan 1,2

30.1.21 **onu-igmp-snooping group-number**

This command is to configure the maximum view on line multicast group in igmp-snooping mode

onu-igmp-snooping group-number *group-number*

【Command mode】

ONUport configuration mode

【Example】

！Configure ONU view on line multicast group in igmp-snooping mode

OptiWay(onu-3/3/1 -reth-0/1)# onu-igmp-snooping group-number 6

30.1.22 onu-multicast-ctrl

This command is to configure the privileged control table in the control multicast mode.

onu-multicast-ctrl { permit | preview } { *H:H:H:H:H:H portid vlanid* }

【Parameter】

H:H:H:H:H:H :multicast mac address

portid:onu port id

vlanid: multicast vlan num

【Command mode】

ONU configuration mode

【Example】

！ Configure ONU multicast vlan group

OptiWay(onu-3/3/1)# onu-multicast-ctrl permit 01:00:5e:01:01:01 1 5

30.1.23 onu-fec mode

This command is to configure FEC mode in CTC standard

onu-fec mode { enable | disable }

【Command mode】

ONU configuration mode

【Example】

！ Enable fec

OptiWay(onu-3/3/1)# onu-fec mode enable

30.1.24 no onu-classification

This command is to delete ONU port flow classification in CTC standard

no onu-classification precedence *precedence-num*

【Parameter】

precedence-num: priority of flow classification rule

【Command mode】

ONU configuration mode/port configuration mode

【Example】

！Delete a flow classification:

OptiWay(onu-3/3/1-reth-0/1)# no onu-classification precedence 1

30.1.25 no onu-igmp-snooping vlan

This command is to delete multicast vlan in CTC standard

no onu-igmp-snooping vlan *vlan-list*

【Parameter】

vlan-list: configure maximum 8 vlan multicast group

【Command mode】

ONUport configuration mode

【Example】

！Delete ONU port multicasdt vlan group

OptiWay(onu-3/3/1 -reth-0/1)# no onu-igmp-snooping vlan 1,2

30.1.26 **no onu-multicast-ctrl**

This command is to delete port multicast vlan group in CTC standard

no onu-multicast-ctrl { *H:H:H:H:H:H portid vlanid* **}**

【Parameter】

H:H:H:H:H:H : multicast mac address

portid:onu port id

vlanid: multicast vlan id

【Command mode】

ONU configuration mode

【Example】

！ Delete ONU port multicast vlan group

OptiWay(onu-3/3/1)# no onu-multicast-ctrl 01:00:5e:01:01:01 1 5

30.1.27 **no onu-bandwidth multicast**

This command is to recover private CTC ONU multicast default rate :that is no limit to multicast

no onu-bandwidth multicast

30.1.28 **no onu-bandwidth broadcast**

This command is to recover privateCTC ONU broadcast default rate :that is no limit to broadcast

no onu-bandwidth broadcast

30.1.29 **onu-mac-address-table max-mac-count**

This command is to limit ONU port MAC address learning quantity

onu-mac-address-table max-mac-count *number*

no onu-mac-address-table max-mac-count

【Parameter】

*number:*MAC address limitation quantity,the range is 1—1000

【Command mode】

ONU configuration mode, it appoints to all ports

ONUport configuration mode,it appoints to single port

【Example】

！Configure ONU 3/3/1 all ports MAC address limitation quantity is 20

OptiWay(onu-3/3/1)#onu-mac-address-table max-mac-count 20

！Configure ONU 3/3/1port3 MAC address limitation quantity is 40

OptiWay(onu-3/3/1)#interface ethernet 3

OptiWay(onu-3/3/1-reth-3)#onu-mac-address-table max-mac-count 40

！Delete ONU 3/3/1 all ports MAC address limitation quantity is 20

OptiWay(onu-3/3/1)#no onu-mac-address-table max-mac-count

30.1.30 **onu-mac-address-table age-time**

This command is to configure ONU MAC address aging time

onu-mac-address-table age-time { *number* | disable }

no onu-mac-address-table age-time

【Parameter】

number: means MAC address aging time,the range is 1-1048575s

disable: means MAC address table doesn't be aging

【Default】

The default value of MAC address aging time is 300s

【Command mode】

ONU configuration mode

【Example】

！Configure ONU MAC address aging time is 10s

OptiWay(onu-3/3/1)#onu-mac-address-table age-time 10

！Revert ONU MAC address aging time is the default 300s

OptiWay(onu-3/3/1)#no onu-mac-address-table age-time

！Disable ONU MAC address aging time

OptiWay(onu-3/3/1)#onu-mac-address-table age-time disable

30.1.31 **onu-queue-scheduler**

This command is to configure ONU queue scheduler.

onu-queue-scheduler { strict-priority | wrr queue1-weight queue2-weight queue3-weight queue4-weight **}**

no queue-scheduler

【Parameter】

strict-priority: means queue executes strict scheduler

queue1-weight queue2-weight queue3-weight queue4-weight: means queue executes WRR .queue1-weight:num 1 queue weight；queue2-weight: num

2queue weight；queue3-weight: num 3 queue weight；queue4-weight: num 4 queue weight

【Command mode】

ONU configuration mode

【Example】

！ Configure queue scheduler mode as WRR ,the weight of 8 queues is 15, 14,13,12

OptiWay(onu-3/3/1)#onu-queue-scheduler wrr 15 14 13 12

30.1.32 **onu-queue-scheduler cos-map**

This command is to configure the mapping of 8 queues in hardward system and 8 priorites in IEEE 802.1p .

onu-queue-scheduler cos-map { *queue-number packed-priority* }

【Parameter】

queue-number: hardware priority queue, the range is 0～4

packed-priority:IEEE 802.1p defines priority,the range is 0～7

【Default】

By default, the mapping is as below :

802.1p:	0	1	2	3	4	5	6	7
Hardware priority :	0	0	1	1	2	2	3	3

【Command mode】

ONU configuration mode

【Usage】

By default, S8600-04 has 4 hardware priority queues , from 0～4,4 is the highest priority.

S8600-04 sends buffer packets of higher priority in the hardware priority queues.

【Example】

！ Configure hardware priority queues 1 mapping to IEEE 802.1p protocol priority 6

OptiWay(onu-3/3/1)#onu-queue-scheduler cos-map 1 6

30.1.33 onu-queue-scheduler cos-remap

This command is to configure the mapping of 8 priority in IEEE 802.1p.With command **no** means to disable 802.1p re-mapping.

onu-queue-scheduler cos-remap [*old-cos new-cos*]

【Parameter】

old-cos:IEEE 802.1p defined original priority ,the range is 0～7

new-cos:IEEE 802.1p defined new priority,the range is 0～7

【Default】

By default, the mapping disables, when open, COS assigns to different priority.

【Command mode】

ONU configuration mode

【Example】

！ Enable 802.1p re-mapping, configure value 2 IEEE 802.1p protocol priority re-mapping to 5

OptiWay(onu-3/3/1)#onu-queue-scheduler cos-remap

OptiWay(onu-3/3/1)#onu-queue-scheduler cos-remap 2 5

30.1.34 **onu-mac-address-table blackhole**

This command is to configure ONU MAC blackhole

onu-mac-address-table blackhole *H:H:H:H:H:H* [vlan *vlan_id*]

no onu-mac-address-table blackhole { all | *H:H:H:H:H:H* [vlan *vlan_id*] }

【Parameter】

H:H:H:H:H:H:MAC address

*vlan_id:*VLAN id,the range is 1—4094

【Command mode】

ONU configuration mode

【Example】

！ Configure ONU 3/3/1 blackhole items

OptiWay(onu-3/3/1)#onu-mac-address-table blackhole 1:1:1:1:1:1 vlan 1

！ Delete ONU 3/3/1 blackhole items

OptiWay(onu-3/3/1)#no onu-mac-address-table blackhole 1:1:1:1:1:1 vlan 1

！ Delete ONU 3/3/1 all blackhole items

OptiWay(onu-3/3/1)#no onu-mac-address-table blackhole all

30.1.35 **onu-dtag**

This command is to configure ONU QINQ

onu-dtag [flexible-qinq]

no onu-dtag

onu-dtag outer-tpid *tpid_id*

no onu-dtag outer-tpid

onu-dtag mode { customer | uplink }

no onu-dtag mode

onu-dtag insert *start_vlan end_vlan vlan*

no onu-dtag insert [all]

onu-dtag psgg-through *start_vlan end_vlan*

no onu-dtag psgg-through [all]

【Parameter】

*tpid_id:*TPID value,the range is 0x5DD－0xFFFF

start_vlan: start VLAN value,the range is 1－4094

end_vlan: end VLAN value,the range is 1－4094

*vlan:*VLAN value,the range is 1－4094

【Command mode】

In ONU configuration mode,it is for QINQ mode and outside TPID

In ONU port configuration mode, it is for QINQ entity items

【Example】

！ Enable static QINQ

OptiWay(onu-3/3/1)#onu-dtag

！ Enable flexible QINQ

OptiWay(onu-3/3/1)#onu-dtag flexible-qinq

! Disable QINQ

OptiWay(onu-3/3/1)#no onu-dtag

! Configure outside TPID

OptiWay(onu-3/3/1)#onu-dtag outer-tpid 999

! Revert to default TPID

OptiWay(onu-3/3/1)#no onu-dtag outer-tpid

! Configure port mode as CUSTOMER mode

OptiWay(onu-3/3/1-reth-0/1)#onu-dtag mode customer

! Revert port mode is the default UPLINK mode

OptiWay(onu-3/3/1-reth-0/1)#no onu-dtag mode

! Configure port INSERT items

OptiWay(onu-3/3/1-reth-0/1)#onu-dtag insert 3 5 6

! Delete port INSERT item

OptiWay(onu-3/3/1-reth-0/1)#no onu-dtag insert 3 5 6

! Configure port PASSTHROUGH items

OptiWay(onu-3/3/1-reth-0/1)#onu-dtag pass-through 7 9

! Delete port all PASSTHROUGH items

OptiWay(onu-3/3/1-reth-0/1)#no onu-dtag pass-through all

30.1.36 **onu-ip address static**

This command is to configure ONU IP

onu-ip address static *ip-address ip-address-mask ip-address-gateway*

【Command mode】

ONU configuration mode

【Example】

！Configure onu 3/4/1 IP

OptiWay(onu-3/4/1)#onu-ip address static 1.1.1.22 255.255.255.0 1.1.1.1

30.1.37 **no onu-ip address**

This command is to clear ONU IP

no onu-ip address

【Command mode】

ONU configuration mode

【Example】

！Clear onu 3/4/1 的 IP

OptiWay(onu-3/4/1)#no onu-ip address

30.1.38 **onu-vlan**

This command is to enter into VLAN configuration mode or create VLAN then enter into VLAN configuration mode

onu-vlan *vlan-id*

【Command mode】

ONU configuration mode or ONU port mode

【Example】

！Create ONU 3/4/1 VLAN 200

OptiWay(onu-3/4/1)#onu-vlan 200

30.1.39 **no onu-vlan**

This command is to delete all VLAN except existed VLAN 1 or selected VLAN

no onu-vlan { *vlan-id* | all }

【Command mode】

ONU configuration mode

【Example】

！ Delete ONU 3/4/1 VLAN 200

OptiWay(onu-3/4/1)#no onu-vlan 200

30.1.40 **onu-swithport**

This command is to add ONU port in current VLAN.

onu-switchport { *interface-list* | all }

【Command mode】

ONU VLAN mode

【Example】

！ Add ONU3/3/1 port 1,2,3 to current VLAN

OptiWay(onu-3/3/1-rvlan)#onu-switchport ethernet 2/1 to ethernet 2/3

30.1.41 **no onu-swithport**

This command is to add ONU port in current VLAN

no onu-switchport { *interface-list* | all }

【Command mode】

ONU VLAN mode

【Example】

！ Delete ONU3/3/1 port 1 in the current VLAN

OptiWay(onu-3/3/1-rvlan)#no onu-switchport ethernet 2/1

30.1.42 **onu-swithport access vlan**

This command is to add current ports to selected VLAN, port default VLAN ID is selected VLAN

onu-switchport access vlan *vlan-id*

【Command mode】

ONU port mode

【Example】

！ Add ONU3/3/3 access port 3 to VLAN 200

OptiWay(onu-3/3/3-reth-0/3)#onu-switchport access vlan 200

30.1.43 **no onu-swithport access vlan**

This command is to delete current access port in selected VLAN

no onu-switchport access vlan *vlan-id*

【Command mode】

ONU port mode

【Example】

！ Delete ONU3/3/3 access port 3 in VLAN 200

OptiWay(onu-3/3/3-reth-0/3)#no onu-switchport access vlan 200

30.1.44 **onu-tag-mode**

This command is to configure ONU port in tag mode .

onu-tag-mode [tag | untag | unmodify]

【Command mode】

ONU port mode

【Example】

！ Configure ONU3/3/3 access port 3 TAG mode as tag

OptiWay(onu-3/3/3-reth-0/3)#onu-tag-mode tag

30.1.45 **onu-com-session**

This command is to configure electricity power ONU console session parameter.

onu-com-session *comid* { tcpclient | udp } *serverip portid* [*baudrate* [*parity* [*databits* [*stopbits*]]]]

onu-com-session *comid* tcpserver *portid* [*baudrate* [*parity* [*databits* [*stopbits*]]]]

【Parameter】

comid: console id ,the range is 1-4

portid: network id,the range is 1-65535

baudrate: baud rate,the range is 0-10,0 means baud rate is 300,1 means baud rate is 600,2 means baud rate is 1200,3 means baud rate is 2400,4 means baud rate is 4800,5 means baud rate is 9600,6 means baud rate is 14400,7 means baud rate is 19200,8 means baud rate is 38400,9 means baud rate is 57600,10 means baud rate is 115200, it will be the default value 115200 if nothing inputs

parity-type: parity type, the range is 0-4,0 means None parity,1 means even parity,2 means odd parity ,3 means symbol parity ,4 means space parity, it will be the default value None parity if nothing inputs

databits: data bits ,the range is 0-3,0 means data bit as 5 bits,1 means data bit 6 bits, 2 means data bit 7 bits,3 means data bit 8 bits, it will be the default value 8 bits if nothing inputs

*stopbits:*stop bits,the range is 0-2,0 means stop bit as 1bit,1 means stop bit as 1.5 bits,2 means stop bit as 2 bits, it will be the default 1 bit if nothing inputs

【Command mode】

ONU configuration mode

【Example】

！ Configue ONU console 1 session is UDP, session port is 9800,session ip is 192.168.1.1, baud rate is 1200,parity type is even parity, databits is 6 bits, stopbits is 1.5 bits

OptiWay(onu-3/4/1)#onu-com-session 1 udp 192.168.1.1 9800 2 1 1 1

30.1.46 **no onu-com-session**

his command is to disable electricity power ONU console session.

no onu-com-session *comid*

【Command mode】

ONU configuration mode

【Example】

！ Disable console 1 session

OptiWay(onu-3/4/1)#no onu-com-session 1

30.1.47 clear onu-com-statistic

This command is to clear console traffic statistic

clear onu-com-statistic [*comid*]

【Command mode】

ONU configuration mode

【Example】

！ Clear all console traffic statistic

OptiWay(onu-3/4/1)# clear onu-com-statistic

30.1.48 onu-event-alarm loopback

This command is to enable/disable onu loopback alarm

onu-event-alarm loopback enable/disable

【Command mode】

ONU configuration mode,All global configuration mode

【Example】

！ Enable onu loopback alarm

OptiWay(onu-3/3/1)#onu-event-alarm loopback enable

！ Disable onu loopback alarm

OptiWay(onu-3/3/1)#onu-event-alarm loopback disable

30.1.49 onu-ctc-upgrade

This command is to upgrad ONU version based on ctc standard

onu-ctc-upgrade

【Command mode】

ONU configuration mode

【Example】

！ Upgrade onu

OptiWay(onu-3/4/1)#onu-ctc-upgrade

30.1.50 **onu-ctc-upgrade-commit**

This command is to ensure onu upgrade had finished

onu-ctc-upgrade-commit

【Command mode】

ONU configuration mode

【Example】

！ Ensure onu upgrade had finished

OptiWay(onu-3/4/1)#onu-ctc-upgrade-commit

30.1.51 **show onu-port-info**

This command is to display current ONU port PVID and port TAG mode .

show onu-port-info

【Command mode】

Any configuration mode

【Example】

！ Display current ONU3/3/3 port 3 information

OptiWay(onu-3/3/3-reth-0/3)#show onu-port-info

PVID 200

Port mode: Untagged

30.1.52 show onu-status

This command is to display receiving ONUregistration,including MAC of ONU,RTT,on line time,ONU type, software version, current online status.

show onu-status [*onu-id* **|** *onu-mac* **]**

【Command mode】

Any configuration mode

【Example】

！Display current online ONU status

OptiWay(onu-3/4/1)#show onu-status

ONU Mac Address RTT(TQ) RegisterTime Type Software State

3/4/1 00:0a:5a:12:46:59 54 00/021/02 00:40:08 2160 B01D001P005SP1 UP

30.1.53 show statistics onu

This command is to display ONU port traffic statistics

show statistics onu *olt/pon/onu*

【Command mode】

Any configuration mode

【Example】

！Display ONU port 1 traffic statistics

OptiWay(config)#show statistics

OptiWay(onu-3/3/1)#show statistics 3/4/1

SLOT/PON TOTAL(BYTES) UNICASTS(packets)

MULTICASTS(packets) BROADCASTS(packets)

3/4/1 port:pon

input	6389705	511	92443	6176
output	80054	73	0	498

3/4/1 port:uni

input	549817	73	6907	498
output	2354053	10	30565	6176

30.1.54 **show onu-bandwidth**

This command is to display the whole ONU uplink and downlink bandwidth,traffic shaping and strategy.

show onu-bandwidth

show onu-bandwidth shaper

show onu-bandwidth police

【Command mode】

ONU configuration mode

【Example】

！ Display ONU uplink bandwidth

OptiWay(onu-3/3/1)#show onu-bandwidth

upstream: fir=0 cir=1000 pir=100000 burst=100 priority=1 delay=10

jitter=10

downstream: fir=0 cir=1000 pir=100000 burst=100 priority=1 delay=10 jitter=10

ONU port 1 bandwidth ingress is Disable

！Display ONU traffic shaping

OptiWay(onu-3/3/1)#show onu-bandwidth shaper

shaper action: disable

！Display ONU traffic strategy

OptiWay(onu-3/3/1)#show onu-bandwidth police

upstream police: disable

downstream police: disable

30.1.55 **show onu-encrypt**

This command is to display ONU encryption

show onu-encrypt

【Command mode】

ONU configuration mode

【Example】

！Display ONU encryption

OptiWay(onu-3/3/1)#show onu-encrypt

encryp: enable

30.1.56 **show onu-loopback oam**

This command is to display ONU loopback

show onu-loopback oam

【Command mode】

ONU configuration mode

【Example】

！ Display ONU loopback

OptiWay(onu-3/3/1)#show onu-loopback oam

Loopback oam is disable

30.1.57 **show onu-interface**

This command is to display ONU port information

show onu-interface [ethernet *ethernet_number*]

【Parameter 】

ethernet-number:detailed port num

【Command mode】

ONU configuration mode

【Example】

！ Display ONU port1

OptiWay(onu-3/3/1)#show onu-interface ethernet 2/1

onu : 3/3/1

ONU port 1 is Disable, port link is LINK UP

ONU auto negotiate ability :

ability value[1] : 0x00000028

ability value[2] : 0x00000192

ability value[3] : 0x00000142

speed auto is Enable, Flow control is Disable

bandwidth ingress is Disable

bandwidth egress is Disable

30.1.58 **show onu-sn**

This command is to display ONU serial number in CTC standard.

show onu-sn

【Command mode】

ONU configuration mode

【Example】

！ Display ONU serial number

OptiWay(onu-3/3/1)#show onu-sn

Vender ID: IMST

MODEL: 8015

ONUID: 0x00 0x0a 0x5a 0x11 0x49 0x5c

HW: 0x35 0x30 0x31 0x31 0x00 0x00 0x00 0x00

SW: 0x32 0x30 0x33 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

30.1.59 **show onu-firmware**

This command is to display ONU firmware information in CTC standard.

show onu-firmware

【Command mode】

ONU configuration mode

【Example】

！ Display ONU firmware information

OptiWay(onu-3/3/1)#show onu-firmware

onu firmware :

0x48 0xfd 0x97 0x3f 0x00 0x02 0x00 0x00 0x00 0x03 0x00 0x00

30.1.60 **show onu-pon-chip**

This command is to display ONU PON chip information in CTC standard.

show onu-pon-chip

【Command mode】

ONU configuration mode

【Example】

！ Display ONU PON chip information

OptiWay(onu-3/3/1)#show onu-pon-chip

onu chip id : vendor id IM

onu chip id : model Id 0x5 0x11

onu chip id : date 06/17/39

30.1.61 **show onu-capabilities**

This command is to display ONU support in CTC standard

show onu-capabilities

【Command mode】

ONU configuration mode

【Example】

！ Display ONU support

OptiWay(onu-3/3/1)#show onu-capabilities

onu 3/3/1 :

onu capability:	serviceSupported	3
onu capability:	numGEPorts	1
onu capability:	geBitmap	0x10000
onu capability:	numFEPorts	16
onu capability:	feBitmap	0xffff
onu capability:	numPOTSPorts	0
onu capability:	numE1Ports	0
onu capability:	numUSQueues	4
onu capability:	maxQueueUSPort	4
onu capability:	numDSQueues	4
onu capability:	maxQueueDSPort	4
onu capability:	BatteryBackup	0

30.1.62 **show onu-bandwidth**

This command is to display ONU uplink and downlink bandwidth in CTC standard.

show onu-bandwidth ingress [interface ethernet *ethernet_number*]

show onu-bandwidth egress [interface ethernet *ethernet_number*]

【Parameter 】

ethernet-number:detailed port num

【Command mode】

ONU configuration mode

【Example】

```
！ Display ONU port uplink bandwidth configuration
OptiWay(onu-3/3/1)#show onu-bandwidth ingress interface ethernet 2/1
onu : 3/3/1
ONU port 1 bandwidth ingress is Enable
    cir(ingress rate of port)    20000
    cbs(depth of token bucket)    20000
ebs(the extra burst size)    123
！ Display all ports downlink bandwidth configuration
OptiWay(onu-3/3/1)#show onu-bandwidth egress
onu : 3/3/1
ONU port 1 bandwidth egress is Disable
ONU port 2 bandwidth egress is Disable
ONU port 3 bandwidth egress is Disable
ONU port 4 bandwidth egress is Disable
ONU port 5 bandwidth egress is Disable
ONU port 6 bandwidth egress is Disable
```

ONU port 7 bandwidth egress is Disable

ONU port 8 bandwidth egress is Disable

30.1.63 **show vlan-mode**

This command is to display ONU vlan mode in CTC standard

show vlan-mode [interface ethernet *ethernet_num*]

【Parameter 】

ethernet-number: detailed port num

【Command mode】

ONU configuration mode

【Example】

！Display port 1 vlan mode

OptiWay(onu-3/3/1)#show vlan-mode interface ethernet 2/1

onu 3/3/1 :

port ID : 1 ctc vlan mode : transparent

！Display all ports vlan mode

OptiWay(onu-3/3/1)#show vlan-mode

onu 3/3/1 :

port ID : 1 ctc vlan mode : transparent

port ID : 2 ctc vlan mode : transparent

port ID : 3 ctc vlan mode : transparent

port ID : 4 ctc vlan mode : transparent

port ID : 5 ctc vlan mode : transparent

port ID : 6 ctc vlan mode : transparent

port ID : 7 ctc vlan mode : transparent

port ID : 8 ctc vlan mode : transparent

30.1.64 **show onu-classification**

This command is to display ONU port flow classification configuration

show onu-classification

【Command mode】

ONU configuration mode/port configuration mode

【Example】

！Display flow classification configuration

OptiWay(onu-3/3/1)#show onu-classification

Rules 1 Precedence 1 QueMapped 2 ethernet-priority 5

Destination-port 55

Rules 2 Precedence 3 QueMapped 2 ethernet-priority 5

Destination-port 44

Rules 3 Precedence 4 QueMapped 2 ethernet-priority 5

Destination-port 88

Rules 4 Precedence 5 QueMapped 2 ethernet-priority 5

Destination-port 66

30.1.65 **show onu-multicast mode**

This command is to display multicast mode

show onu-multicast mode

【Command mode】

ONU configuration mode

【Example】

！ Display ONU multicast control mode as controllable mode

OptiWay(onu-3/3/1)#show onu-multicast mode

30.1.66 **show onu-multicast tag**

This command is to display multicast mode

show onu-multicast tag

【Command mode】

ONUport configuration mode

【Example】

！ Display ONU port multicast VLAN TAG strip or not

OptiWay(onu-3/3/1-reth-0/1)# show onu-multicast tag

interface 1:tag

30.1.67 **show onu-multicast fast-leave**

This command is to display port fast-leave status and capacity

show onu-multicast fast-leave

【Command mode】

ONU configuration mode

【Example】

！ Display ONU multicast fast-leave function

OptiWay(onu-3/3/1)# show onu-multicast fast-leave

OptiWay(onu-3/3/1 -reth-0/1)# show onu-multicast fastleave

non-fast-leave(igmp-snooping) ability:support

fast-leave(igmp-snooping) ability:support

non-fast-leave(multicast-control) ability:support

fast-leave(multicast-control) ability:support

fase-leave state disable

30.1.68 **show onu-igmp-snooping vlan**

This command is to display multicast vlan group and multicast group quantity on line at the same time.

show onu-igmp-snooping vlan

【Command mode】

ONU configuration mode

【Example】

！ Display igmp-snooping multicast vlan group in the multicast mode

OptiWay(onu-3/3/1 -reth-0/1)#show onu-igmp-snooping vlan

interface 1

multicast-vlan:no vlan

group-number:255

30.1.69 **show onu-multicast-ctrl local-ctrl**

This command is to display privilege control table in the local controllable

mode

show onu-multicast-ctrl local-ctrl

【Command mode】

ONU configuration mode

【Example】

！ Display local controllable multicast configuration

OptiWay(onu-3/3/1)# show onu-multicast-ctrl local-ctrl

Port	Multicast MAC	Multicast Vlan	Type	online
5	01:00:5e:01:01:01	5	permit	N

30.1.70 **show onu-multicast-ctrl**

This command is to display privilege control table in the remote controllable mode

show onu-multicast-ctrl

【Command mode】

ONU configuration mode

【Example】

！ Display remote controllable multicast configuration

OptiWay(onu-3/3/1)# show onu-multicast-ctrl

the channel number at one time : 5

the live time : 300

preview time once : 180

preview interval : 300

preview times : 5

Port	Multicast MAC	Multicast Vlan
5	01:00:5e:01:01:01	5

30.1.71 **show onu-fec**

This command is to display ONU forward error correction

show onu-fec

【Command mode】

ONU configuration mode

【Example】

！ Display fec status and capacity

OptiWay(onu-3/3/1)#show onu-fec

onu fec ability: supported mode:disable

30.1.72 **show onu-mac-address-table max-mac-count**

This command is to display ONU port MAC address limitation quantity

show onu-mac-address-table max-mac-count

【Command mode】

ONU configuration mode, display all port

ONUport configuration mode, display single port

【Example】

！ Display ONU all ports MAC address limitation quantity

OptiWay(onu-3/3/1)#show onu-mac-address-table max-mac-count

Port	limit switch	Max mac address number
1	disable	0
2	disable	0
3	disable	0
4	disable	0
5	disable	0
6	disable	0
7	disable	0

.

.

.

！ Display ONU port 3 MAC address limitation quantity

OptiWay(onu-3/3/1)#interface ethernet 3

OptiWay(onu-3/3/1-reth-0/3)#show onu-mac-address-table max-mac-count

Port	limit switch	Max mac address number
3	disable	0

30.1.73 **show onu-mac-address-table age-time**

This command is to display ONU MAC address aging time

show onu-mac-address-table age-time

【Command mode】

ONU configuration mode

【Example】

！ Display ONU MAC address aging time

OptiWay(onu-3/3/1)#show onu-mac-address-table age-time

mac address table agingtime is 300 second!

30.1.74 **show onu-queue-scheduler**

This command is to display ONU queue scheduler mode and mapping

show onu-queue-scheduler

show onu-queue-scheduler cos-map

show onu-queue-scheduler cos-remap

【Command mode】

ONU configuration mode

【Example】

！ Display ONU queue scheduler mode

OptiWay(onu-3/3/1)# show onu-queue-scheduler

Queue scheduler mode: first come first serve

30.1.75 **show onu-mac-address-table blackhole**

This command is to display ONU MAC blackhole

show onu-mac-address-table blackhole

【Command mode】

ONU configuration mode

【Example】

！ Display ONU 3/3/1 blackhole items

OptiWay(onu-3/3/1)#show onu-mac-address-table blackhole

Show MAC blackhole table information

MAC Address VLAN ID

01:01:01:01:01:01 1

Total entries: 1 .

30.1.76 **show onu-bandwidth multicast**

This command is to display ONU multicast rate

show onu-bandwidth multicast

【Command mode】

ONU configuration mode

【Example】

！Display ONU 3/3/1 multicast rate

OptiWay(onu-3/3/1)#show onu-bandwidth multicast

ONU 4/2/3 Multicast: Downstream = 1000000(kbps) Upstream = 1000000(kbps)

30.1.77 **show onu-bandwidth broadcast**

This command is to display ONU broadcast rate

show onu-bandwidth broadcast

【Command mode】

ONU configuration mode

【Example】

！ Display ONU 3/3/1 broadcast rate

OptiWay(onu-3/3/1)# show onu-bandwidth broadcast

ONU 4/2/3 Broadcast: Downstream = 1000000(kbps) Upstream = 1000000(kbps)

30.1.78 **show onu-dtag**

This command is to display ONU QINQ information

show onu-dtag

show onu-dtag insert

show onu-dtag pass-througn

【Command mode】

ONU configuration mode

ONUport configuration mode

【Example】

！ Display QINQ mode

OptiWay(onu-3/3/1)#show onu-dtag

Current double tag style is : flexible-qinq

Current outer-tpid is : 0x999

Ethernet 01 is a customer port

Ethernet 02 is a uplink port

Ethernet 03 is a uplink port

Ethernet 04 is a uplink port

.

.

.

Ethernet 16 is a uplink port

！ Display port INSERT items

OptiWay(onu-3/3/1-reth-0/1)#show onu-dtag insert

port	inner start vlan	inner end vlan	outer vlan
01	3	5	6

Total entries: 1 .

！ Display port PASSTHROUGH items

OptiWay(onu-3/3/1-reth-0/1)#show onu-dtag pass-through

port	pass through start vlan	pass through end vlan
01	7	9

Total entries: 1 .

30.1.79 **show onu-mac-address-table blackhole**

This command is to display ONU MAC blackhole

show onu-mac-address-table blackhole

【Command mode】

ONU configuration mode

【Example】

！ Display port INSERT items

OptiWay(onu-3/3/1-reth-0/1)#show onu-dtag insert

30.1.80 **show onu-ip address onu**

This command is to display ONU IP

show onu-ip address onu { *onu-id* **|** *mac-address* **}**

【Command mode】

Any configuration mode

【Example】

！Display onu 3/4/1 IP configuration

OptiWay(config)#show onu-ip address onu 3/4/1

ONU	Mac Address	Ipaddress	Subnet Mask	Gateway	Status
3/4/1	11:22:33:44:55:66	1.1.1.22	255.255.255.0	1.1.1.1	static

30.1.81 **show onu-com-session**

This command is to display electricity power ONU console session configuration parameter

show onu-com-session [*comid*]

【Command mode】

ONU configuration mode

【Example】

！Display onu 3/3/1 console session configuration

OptiWay(onu-3/3/1)#show onu-com-session

com1

com session type: udp

com session port: 9800

com session serverip:192.168.1.1

com settings baudrate:1200

com settings parity: even

com settings databits:6 bit

com settings stopbits:2 bit

com2

com session:DISABLE

com3

com session:DISABLE

com4

com session:DISABLE

30.1.82 **show onu-com-statistic**

This command is to display console traffic statistics

show onu-com-statistic [*comid*]

【Command mode】

ONU configuration mode

【Example】

！ Display onu 3/3/1 console traffic statistics

OptiWay(onu-3/3/1)#show onu-com-statistic

com1

com bytesrecv: 0

com bytessend:0

30.1.83 show onu-event-alarm loopback

This command is to display onu loopback alarm status

show onu-event-alarm loopback

【Command mode】

ONU configuration mode,All global configuration mode

【Example】

OptiWay(onu-3/3/1)#show onu-event-alarm loopback

Chapter 31 PSG Management Configuration Command

31.1 PSG Management Configuration Command

PSG(Protection Switching Group) configuration command includes:

- **mpcp-delay-time**
- **admin-enable-pon**
- **psg creat**
- **psg delete**
- **psg switch**
- **admin-enable-psg**
- **show mpcp-delay-time**
- **show admin-enable-pon**
- **show psg**
- **show admin-enable-psg**

31.1.1 mpcp-delay-time

This command is to configure/delete MPCP delay time of ONU registration

mpcp-delay-time slot *slot_id* **pon** *pon_id* **time** *delay_time*

no mpcp-delay-time slot *slot_id* **pon** *pon_id*

【Parameter】

*slot_id:*slot id

*pon_id:*pon port id

*delay_time:*delay time

【Command mode】

All global configuration mode

【Example】

！Configure PON 3 delay time in slot3

OptiWay(config)# mpcp-delay-time slot 3 pon 3 time 10

！Delete PON 3 delay time in slot3

OptiWay(config)# no mpcp-delay-time slot 3 pon 3

31.1.2 admin-enable-pon

This command is to enable/disable PON status

admin-enable-pon slot *slot_id* pon *pon_id*

no admin-enable-pon slot *slot_id* pon *pon_id*

【Parameter】

*slot_id:*slot id

*pon_id:*pon port id

【Command mode】

All global configuration mode

【Example】

！Enable PON 3 status in slot3

OptiWay(config)#admin-enable-pon slot 3 pon 3

！Disable PON 3 status in slot3

OptiWay(config)#no admin-enable-pon slot 3 pon 3

31.1.3 psg creat

This command is to creat PSG group

psg creat slot *slot_id* psg-id *psg_id* active-pon *pon_index* standby-pon *pon_index*

【Parameter】

psg_id:psg id

*slot_id:*slot id

*pon_index:*pon id

【Command mode】

All global configuration mode

【Usage】

Creat PSG, system will assign PSG id automatically in the current PSG.

Before creating PSG, disable PON status.

【Example】

！Creat PSG of master PON 1 backup PON2

OptiWay(config)#psg creat slot 3 active-pon 1 standby-pon 2

31.1.4 psg delete

This command is to delete PSG group

psg delete slot *slot_id* psg-id *psg_id*

【Parameter】

*slot_id:*slot id

*psg_id:*psg id

【Command mode】

All global configuration mode

【Example】

！ Delete PSG group

OptiWay(config)#psg delete slot 3 psg-id 1

31.1.5 **psg switch**

This command is to shift master/backup PON in PSG manually

psg switch slot *slot_id* psg-id *psg_id*

【Parameter】

*slot_id:*slot id,the range is 2--5

*psg_id:*psg id,the range is 1--2

【Command mode】

All global configuration mode

【Example】

！ Shift master/backup PON in PSG 1

OptiWay(config)#psg switch slot 3 psg-id 1

31.1.6 **admin-enable-psg**

This command is to enable/disable PSG group

admin-enable-psg slot *slot_id* psg-id *psg_id*

no admin-enable-psg slot *slot_id* psg-id *psg_id*

【Parameter】

*slot_id:*slot id

*psg_id:*psg id

【Command mode】

All global configuration mode

【Example】

！ Enable PSG group 1

OptiWay(config)#admin-enable-psg slot 3 psg-id 1

！ Disable PSG group 1

OptiWay(config)#no admin-enable-psg slot 3 psg-id 1

31.1.7 **show mpcp-delay-time**

This command is to display MPCP echo delay time in ONU registration

show mpcp-delay-time slot *slot_id* pon *pon_id*

【Parameter】

*slot_id:*slot id

*pon_id:*pon id

【Command mode】

All global configuration mode

【Example】

！ Display PON 3 echo delay time in slot3

OptiWay(config)#show mpcp-delay-time slot 3 pon 3

Port limit delay delay time

pon 3/3: disable 10

31.1.8 show admin-enable-pon

This command is to display PON

show admin-enable-pon slot *slot_id*

【Parameter】

*slot_id:*slot id

【Command mode】

All global configuration mode

【Example】

！ display PON in slot 3

OptiWay(config)#show admin-enable-pon slot 3

PON port administrative status

pon 3/1: admin-up

pon 3/2: admin-up

pon 3/3: admin-down

pon 3/4: admin-up

31.1.9 show psg

This command is to display PSG group

show psg slot *slot_id*

【Parameter】

*slot_id:*slot id,the range is 2--5

【Command mode】

All global configuration mode

【Example】

！ Display PSG 1

OptiWay(config)#show psg slot 3

PSG ID active pon standby pon administrative status

psg-3/1 pon-3/1 pon-3/2 admin-down

31.1.10 **show admin-enable-psg**

This command is to display PSG group enable

show admin-enable-psg slot *slot_id* [psg-id *psg_id*]

【Parameter】

*slot_id:*slot id

*psg_id:*psg id

【Command mode】

All global configuration mode

【Example】

！ Display PSG group enable

OptiWay(config)#show admin-enable-psg slot 3 psg-id 1

PSG port administrative status

psg 3/1: admin-up

Chapter 32 Controllable Multicast Profile Managmenet Commands

32.1 Controllable multicast profile management commands

Controllable multicast profile management commands includs:

- **multicast-ctrl profile**
- **multicast-ctrl**
- **show multicast-ctrl profile**
- **enable/disable multicast-ctrl profile**
- **onu-multicast-ctrl profile-binding**

32.1.1 multicast-ctrl profile

This command is to creat/delete controllable multicast profile

multicast-ctrl profile *profile_id*

no multicast-ctrl profile *profile_id*

【Parameter】

*profile_id:*controllable profile number,the range is 1—32

【Command mode】

All global configuration mode

【Example】

！Creat controllable multicast profile 1

OptiWay(config)# multicast-ctrl profile 1

！Delete controllable multicast profile 1

OptiWay(config)# no multicast-ctrl profile 1

32.1.2 **multicast-ctrl**

This command is to add/delete controllable multicast profile privilege control table

multicast-ctrl { permit | preview } { *H:H:H:H:H:H vlan_id* **}**

no multicast-ctrl { *H:H:H:H:H:H* | *vlan_id* **}**

【Parameter】

H:H:H:H:H:H: means MAC address

*vlan_id:*means VLAN id,the range is 1—4094

【Command mode】

Profile mode

【Example】

！Configure controllable multicast profile privilege:

OptiWay(multicast-profile-1)#multicast-ctrl permit 01:00:5e:01:02:03 2

！Delete controllable multicast profile privilege:

OptiWay(multicast-profile-1)#no multicast-ctrl 01:00:5e:01:02:03

32.1.3 **show multicast-ctrl profile**

This command is to display controllable multicast profile privilege control table

show multicast-ctrl profile *profile_id*

【Parameter】

*profile_id:*controllable multicast profile id,the range is 1—32

【Command mode】

Any configuration mode

【Example】

！Display controllable multicast profile 1 privilege control table

OptiWay(onu-3/3/1)#show multicast-ctrl profile 1

32.1.4 enable multicast-ctrl profile

This command is to enable controllable multicast profile privilege control table

enable multicast-ctrl profile *profile_id*

【Parameter】

*profile_id:*controllable multicast profile id,the range is 1—32

【Command mode】

Profile mode

【Example】

！Enable controllable multicast profile 1:

OptiWay(multicast-profile-1)#enable multicast-ctrl profile 1

32.1.5 onu-multicast-ctrl profile-binding

This command is to bind/delete onu and controllable multicast profile privilege control table

onu-multicast-ctrl profile-binding *profile_id port_id*

no onu-multicast-ctrl profile-binding *profile_id* *port_id*

【Parameter】

profile_id:controllable multicast profile id,the range is 1—32

port_id:onu port id

【Command mode】

ONU configuration mode

【Example】

！ Bind onu3/3/1 controllable multicast profile 1 privilege control table:

OptiWay(onu-3/3/1)#onu-multicast-ctrl profile-binding 1 0/2

！ Delete onu3/3/1 controllable multicast profile 1 privilege control table:

OptiWay(onu-3/3/1)#no onu-multicast-ctrl profile-binding 1 0/2

SHANGHAI SUN TELECOMMUNICATION CO., LTD.
Building No.145 Lane 666, Xianing Rd.
Jinshan Industrial Zone, Jinshan District
ShangHai, China 201506
Tel: +86 21 60138638 Fax: +86 21 60138635-401
E-mail: ics@suntelecom.cn
http://www.suntelecom.cn