QTECH

МИР ДОСТУПНЕЕ

QSW-3900 10GE
Intelligent Routing Switch

User’s Manual

QTECH QSW-3900 10GE

Intelligent Routing Switch

User's Manual

Command Line Reference Manual

Content

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

```
QTECH>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】

```
QTECH#configure terminal
QTECH(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

```
QTECH>enable
QTECH#
```

【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

```
QTECH(config-if-ethernet-0/0/1)#end
QTECH#
```

【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

```
QTECH(config-if-ethernet-0/0/1)#exit
QTECH(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】

```
QTECH(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 QTECH

【Command configuration mode】

Global configuration mode

【Usage】

Modify system hostname. If the hostname is QSW-3900，the hostname in global configuration mode is QSW-3900(config)#.

【Example】

！Configure hostname to be QTECH QSW-3900

```
QTECH(config)#hostname QTECH QSW-3900
QTECH QSW-3900(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

```
QTECH(config)#interface ethernet 0/0/1
```

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

```
QTECH(config)#interface range ethernet 0/0/1 to e 0/0/3
```

1.1.10 muser

Use muser command to enable user’s RADIUS remote authentication.

muser { local | { radius *radiusname* { pap | chap } [local] } }

【Parameter】

radiusname：RADIUS server configuration name

【Command configuration mode】

Global configuration mode

【Usage】

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

RADIUS authentication supports PAP or CHAP ways.

Enable RADIUS remote authentication needs correct RADIUS server configuration.

When the authentication is successful, user’s privilege is normal. Only when the authentication reply message includes the field of “service-type”, and the value of it is “Administrative”, the user is administrator.

【Example】

！Enable RADIUS authentication with the way of PAP

```
QTECH(config)#muser radius radiusserver1 pap
```

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

```
QTECH#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

```
QTECH(config)#show muser
```

1.1.13 **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 "nic"

```
QTECH(config)#show username nic
```

1.1.14 **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 “nic” to disconnect with telnet

```
QTECH#stop nic
```

1.1.15 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

```
QTECH#terminal language chinese
```

1.1.16 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

```
QTECH#timeout 30
```

！Configure user to be non-overtime

```
QTECH#no timeout
```

1.1.17 **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 “nic”， configure privilege to be 15 ,and password to be 123456

```
QTECH(config)#username nic privilege 15 password 0 123456
```

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

```
QTECH(config)#username nic privilege 1 password 0 1234
```

1.1.18 **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 "nic" to be 123456
QTECH(config)#username change-password
please input you login password : ******
please input username :nic
Please input user new password :******
Please input user comfirm password :******
chang user nic 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

```
QTECH(config)#clear interface
```

！Clear information of interface 5 in global and interface mode

```
QTECH(config)#clear interface ethernet 0/0/5

QTECH(config-if-ethernet-0/0/5)#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

```
QTECH(config-if-ethernet-0/0/ 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 “nic” for the Ethernet 0/0/3

```
QTECH(config-if-ethernet-0/0/3)#description nic
```

！Clear description of Ethernet 0/0/3

```
QTECH(config-if-ethernet-0/0/3)#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

```
QTECH(config-if-ethernet-0/0/5)#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 0/5

```
QTECH(config-if-ethernet-0/0/5)#flow-control
```

！Disable flow control on Ethernet 0/5

```
QTECH(config-if-ethernet-0/0/5)#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 0/0/5 only to receive tagged frame

```
QTECH(config-if-ethernet-0/0/5)#ingress acceptable-frame tagged
```

！Restore default ingress acceptable-frame Ethernet 0/0/5

```
QTECH(config-if-ethernet-0/0/5)#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 0/0/5

```
QTECH(config-if-ethernet-0/0/5)#ingress filtering
```

！Disable the ingress filtering of ethernet 0/0/5

```
QTECH(config-if-ethernet-0/0/5)#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 0 to 7

【Default】

Default priority-value is 0

【Command configuration mode】

Interface configuration mode

【Usage】

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

【Example】

！Configure priority-value of Ethernet 0/0/3 to be 1

```
QTECH(config-if-ethernet-0/0/3)#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 0/0/3

QTECH(config)#show description interface ethernet 0/0/3

【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 0 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 0/0/1

```
QTECH#show interface ethernet 0/0/1
```

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 0 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 0/0/1

```
QTECH#show statistics interface ethernet 0/0/1
```

2.1.12 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 0/0/1, then enable it.

```
QTECH(config-if-ethernet-0/0/1)#shutdown
QTECH(config-if-ethernet-0/0/1)#no shutdown
```

2.1.13 speed

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

speed { 10 | 10auto | 100 | 100auto | auto }
no speed

【Parameter】

10：Means the port speed is 10Mbps

100：Means the port speed is 100Mbps

10auto: means the maximum port speed is 10Mbps，and duplex mode is auto-negotiation

100auto: means the maximum port speed is 100Mbps，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】

100 BASE TX supports the speed of 10Mbps and 100Mbps and the duplex mode of half, full duplex and auto-negotiation mode. 100 BASE FX supports the speed of 100Mbps and the duplex mode of full duplex.

【Example】

！Configure the speed of Ethernet 0/0/1 to 100Mbps

```
QTECH(config-if-ethernet-0/0/1)#speed 100
```

2.1.14 switchport access

Use **switchport access** command to add current port to specified VLAN, and the default VLAN-ID is configured to be the specified VLAN.

Use **no switchport access** command to remove current port from specified

VLAN, except VLAN 1, and if the default vlan-id of the current port is the specified VLAN and this port also belongs to VLAN 1, the default vlan-id of the current port restores to be 1.

switchport access vlan *vlan-id*
no switchport access vlan *vlan-id*

【Parameter】

vlan-id：ID of a VLAN ranges from 2 to 4094

【Command configuration mode】

Interface configuration mode

【Usage】

The precondition to use this command is the current port cannot be trunk port and the specified vlan must exist.

【Example】

!Add Ethernet 0/0/1 to VLAN 2. VLAN 2 exists, and Ethernet 0/0/1 is not trunk port.

```
QTECH(config-if-ethernet-0/0/1)#switchport access vlan 2
```

2.1.15 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 0/0/1 to be trunk port

```
QTECH(config-if-ethernet-0/0/1)#switchport mode trunk
```

2.1.16 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, 5,8,10-20. 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 Ethernet0/0/1 to VLAN 3、4、70～150

QTECH(config-if-ethernet-0/0/1)#switchport trunk allowed vlan 3,4,70-150

2.1.17 switchport trunk native vlan

Use switchport trunk native vlan command to configure the default vlan-id (pvid) of trunk port. Use no switchport trunk native vlan command to restore the default vlan-id.

switchport trunk native vlan *vlan-id*

no switchport trunk native

【Parameter】

vlan-id ranges from 1 to 4094

【Default】

Default vlan-id is 1

【Command configuration mode】

Interface configuration mode

【Usage】

Only trunk port can use this command, errors may occur when using this command on access port. This command configures a default VLAN id for trunk port，and the VLAN id must be valid, and the port must be in the vlan.

When restoring the default vlan of the port, this port must be in VLAN 1, or the configuration fails.

【Example】

！Configure default vlan id of trunk ethernet 0/0/1 to be 100

```
QTECH(config-if-ethernet-0/0/1)#switchport trunk native vlan 100
```

2.1.18 tag

Use **tag** command to enable access port to send message with tag vlan. Use

no tag command to disable.

tag vlan vlan-list

no tag vlan *vlan-list*

【Parameter】

vlan-id ranges from 1 to 4094

【Default】

Access port can send message with tag vlan of this port

【Command configuration mode】

Interface configuration mode

【Usage】

This command can only be used for access port.

In interface configuration mode, configuration only can enable this port to send message with specified tag vlan, this vlan can be or cannot be the one the port belongs to, but the vlan must exist. Tag vlan command can be used for many times to enable the port to send message with different types of tag vlans. No tag vlan command has the same way of using, it can enable this port not to message with specified tag vlan.

【Example】

！Enable Ethernet 0/0/1 to send message with tag vlan 100, VLAN 200 to VLAN 220

```
QTECH(config-if-ethernet-0/0/1)#tag vlan 100,200-220
```

2.1.19 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

```
QTECH#show statistics dynamic interface
```

2.1.20 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

```
QTECH#show utilization interface
```

2.1.21 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 e0/0/5

```
QTECH(config-if-ethernet-0/0/5)#local-switch
```

！Disable local switching feature of e0/0/5

```
QTECH(config-if-ethernet-0/0/5)#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 0 to 2, and port-num is in the range of 1 to 24.

【Command configuration mode】

Global configuration mode

【Example】

！Configure Ethernet 0/0/1 to be mirror destination-interface

```
QTECH(config)#mirror destination-interface ethernet 0/0/1
```

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 0/0/1 to ethernet 0/0/12 to be mirror source-interface

```
QTECH(config)#mirror source-interface ethernet 0/0/1 to ethernet 0/0/12 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

```
QTECH(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

```
QTECH(config)#port-car
```

！Enable port-car of Ethernet 0/0/8

```
QTECH(config-if-ethernet-0/0/8)#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 3600

【Default】

Default port-car-open-time is 480 seconds

【Command configuration mode】

Global configuration mode

【Example】

！Configure port-car-open-time to be 10 seconds

```
QTECH(config)#port-car-open-time 10
```

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 2600

【Default】

Default port-car-rate is 300 packet/second

【Command configuration mode】

Global configuration mode

【Example】

！Configure port-car-rate to be 100 packet/second

```
QTECH(config)#port-car-rate 100
```

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

QTECH(config)#show port-car

2.4 Port LACP Configuration Command

Port LACP configuration command includes:

- **channel-group**
- **channel-group mode**
- **channel-group load-balance**
- **lacp system-priority**
- **lacp port-priority**
- **show lacp sys-id**
- **show lacp internal**
- **show lacp neighbor**

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 0 to 5

【Default】

Non

【Command configuration mode】

Global configuration mode

【Example】

！Create channel group 1

```
QTECH(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 0 to 5

【Default】

Non

【Command configuration mode】

Interface /Interface group configuration mode

【Example】

！Add Ethernet 0/0/3 to channel-group 3 and specify the port to be active mode

```
QTECH(config-if-ethernet-0/0/3)#channel-group 3 mode active
```

！Add Ethernet 0/0/6 to ethernet 0/0/8 to channel-group 2 and specify the ports to be on mode

```
QTECH(config)#interface range ethernet 0/0/6 to ethernet 0/0/8
QTECH(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 0 to 5

【Default】

Source MAC mode

【Command configuration mode】

Global configuration mode

【Example】

！Specify load-balance of channel-group 0 is destination mac

```
QTECH(config)#channel-group load-balance dst-mac
```

2.4.4 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 40000

```
QTECH(config)#lacp system-priority 40000
```

2.4.5 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 0/0/2 to be 12345

```
QTECH(config-if-ethernet-0/0/2)#lacp port-priority 12345
```

2.4.6 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

```
QTECH(config)#show lacp sys-id
```

2.4.7 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 0 to 5

【Default】

Non

【Command configuration mode】

Any configuration mode

【Example】

！Such as：

QTECH#show lacp internal

2.4.8 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 0 to 5

【Default】

Non

【Command configuration mode】

Any configuration mode

【Example】

！Such as：

QTECH#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

QTECH(config)#alarm all-packets

！Enable alarm all-packets of Ethernet 0/0/8

```
QTECH(config-if-ethernet-0/0/8)#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. 100BASE ranges from 0 to 100

normal: normal threshold. 100BASE ranges from 0 to 100

【Default】

100 BASE default exceed threshold is 85，normal threshold is 60

【Command configuration mode】

Interface configuration mode

【Usage】

Exceed > normal

【Example】

!Configure alarm all-packets exceed threshold to be 50 ,and normal threshold to be 30

```
QTECH(config)#alarm all-packets threshold exceed 500 normal 300
```

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

```
QTECH(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 0 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 0/0/1

```
QTECH(config)#show alarm all-packets interface ethernet 0/0/1
```

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”

```
QTECH (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 4094.

【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

```
QTECH(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 0 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

```
QTECH(config-if-vlan)#switchport ethernet 0/0/1 ethernet 0/0/3 to ethernet 0/0/5 ethernet 0/0/8
```

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

```
QTECH(config-if-vlan)#no switchport ethernet 0/0/3 to ethernet 0/0/5 ethernet 0/0/8
```

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 4094.

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

```
QTECH(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
QTECH(config)#gvrp
！Enable GVRP on Ethernet port 8
```

```
QTECH(config-if-ethernet-0/0/8)#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

```
QTECH(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 0 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

```
QTECH(config)#show gvrp interface ethernet 0/0/3 ethernet 0/0/5 ethernet
0/0/6
```

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 4094. The list is in the form of number, -, such as: 2, 5, 8, 10-20.

【Command configuration mode】

Global configuration mode

【Example】

!Add vlan 2, 3, 7 to GVRP

```
QTECH(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

```
QTECH(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

```
QTECH(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 0x8100.

【Command configuration mode】

Global configuration mode

【Example】

！Configure internal TPID to be 0x9100

```
QTECH(config)#dtag inner-tpid 9100
```

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 0x8100.

【Command configuration mode】

Interface configuration mode

【Example】

！Configure external TPID of e0/0/1 to be 0x7100

```
QTECH(config-if-ethernet-0/0/1)#dtag outer-tpid 7100
```

3.3.4 dtag mode

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

dtag mode { c*ustomer* | *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.

```
QTECH(config-if-ethernet-0/0/1)#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

```
QTECH(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 e0/0/1 to add new tag head with the tag vlan to be vlan3

```
QTECH(config-if-ethernet-0/0/1)#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

```
QTECH(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 e0/0/1 is replaced by vlan5

```
QTECH(config-if-ethernet-0/0/1)#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

```
QTECH(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 e0/0/1

```
QTECH(config-if-ethernet-0/0/1)#dtag swap 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

```
QTECH(config)#show dtag pass-through
```

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

```
QTECH(config)#arp-proxy
```

！Disable ARP proxy

```
QTECH(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 1～4094

【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

```
QTECH(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

QTECH(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 20

```
QTECH(config-if-vlanInterface-20)#ip address 192.168.0.100 255.255.0.0
```

！Delete IP address for VLAN interface 20

```
QTECH(config-if-vlanInterface-20)#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 20

```
QTECH(config-if-vlanInterface-20)#ip address primary 192.168.0.100
```

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

```
QTECH(config-if-vlanInterface-20)#ip address range 192.168.0.100 192.168.0.200
```

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

```
QTECH(config)#ip def cpu
```

4.1.8 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

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

4.1.9 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.

```
QTECH(config)#show ip interface vlan-interface 2
```

4.1.10 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 1～4094，**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

```
QTECH(config-if-superVLANInterface-1)#subvlan 8
```

Chapter 5 ARP Configuration Command

5.1 ARP Configuration Command

ARP Configuration Command includes:

- arp
- arp aging
- show arp
- show arp aging
- arp-attack-protect
- show arp-attack-protect
- arp-dos-protect
- show arp-dos-protect

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 1～4094

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 00:01:02:03:04:05 corresponded to IP address 192.168.0.100 and passed through VLAN 1 interface 1

```
QTECH(config)#arp 192.168.0.100 00:01:02:03:04:05 1 0/0/1
```

！Delete arp item corresponded to IP address 192.168.0.100

```
QTECH(config)#no arp 192.168.0.100
```

5.1.2 arp aging

Use **arp aging** command to modify arp aging time.

arp aging *time*

【Parameter】

time：new aging time with the unit being minute which is in the range of 1 to 2880. The default value is 20.

【Command configuration mode】

Global configuration mode

【Example】

！Configure ARP aging time to be 20 minutes.

```
QTECH(config)#arp aging 20
```

5.1.3 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 192.168.0.100

```
QTECH(config)#show arp 192.168.0.100
```

！Display all arp information

```
QTECH(config)#show arp all
```

！Display all static arp information

```
QTECH(config)#show arp static
```

！Display all dynamic arp information

```
QTECH(config)#show arp dynamic
```

5.1.4 show arp aging

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

show arp aging

【Command configuration mode】

Any configuration mode

【Example】

！Display arp aging

```
QTECH(config)#show arp aging
```

5.1.5 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

```
QTECH(config)#arp-attack-protect 1.1.1.1 255.255.255.255
```

5.1.6 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.

QTECH(config)#show arp-attack-protect

5.1.7 arp anti-attack limit

Use this command to configure anti-arp attack rate. The user of arp packet with the speed beyond the limit will be forbidden.

[no] arp anti-attack limit *rate-limit*

【Parameter】

rate-limit：arp packet limit

【Command configuration mode】

Global configuration mode

【Example】

！Configure arp anti-attack limit to be 20

QTECH(config)#arp anti-attack limit 20

5.1.8 arp anti-attack permit

Use this command to reopen the user forbidden by anti-arp attack.

arp anti-attack permit *[source-mac]*

【Parameter】

source-mac：the MAC address of forbidden user

【Command configuration mode】

Global configuration mode

【Example】

！Reopen the user forbidden by anti-arp attack whose Mac address is 00:0a:5a:00:02:02

QTECH(config)#arp anti-attack permit 00:0a:5a:00:02:02

5.1.9 **show arp anti-attack**

Use this command to display anti-arp attack information.

show arp anti-attack

【Command configuration mode】

Global configuration mode

【Example】

！Display anti-arp attack information

QTECH(config)#show arp anti-attack

5.1.10 **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

```
QTECH(config)#arp-dos-protect 128
```

5.1.11 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.

```
QTECH(config)#show arp-dos-protect
```

5.1.12 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

```
QTECH(config)#arp overwrite
```

5.1.13 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

```
QTECH(config)#show arp overwrite
```

Chapter 6 DHCP Configuration Command

6.1 DHCP Configuration Command

- **dhcp option82**
- **dhcp option82 strategy**
- **dhcp-relay**
- **dhcp-relay hide server-ip**
- **dhcp-server**
- **dhcp-snooping**
- **dhcp-snooping trust**
- **dhcp-snooping max-clients**
- **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 option82

Use dhcp option82 command to enable 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

```
QTECH(config)#dhcp option82
```

6.1.2 dhcp option82 strategy

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

dhcp option82 strategy {drop|keep|replace}

【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

```
QTECH(config)#dhcp option82 strategy drop
```

6.1.3 **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

QTECH(config)#dhcp-relay

！Disable DHCP relay

QTECH(config)#no dhcp-relay

6.1.4 **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 or the first or the last level of DHCP, network can operate normally.

【Example】

！Enable hide DHCP server of DHCP relay

```
QTECH(config)#dhcp-relay hide server-ip
```

！Disable hide DHCP server of DHCP relay

```
QTECH(config)#no dhcp-relay hide server-ip
```

6.1.5 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 192.168.0.100

```
QTECH(config)#dhcp-server 2 ip 192.168.0.100
```

！Delete DHCP server 2

```
QTECH(config)#no dhcp-server 2
```

！Specify VLAN interface 2 to use DHCP server 1

```
QTECH(config-if-vlanInterface-2)#dhcp-server 1
```

！Cancel specified DHCP server of VLAN interface 2

```
QTECH(config-if-vlanInterface-2)#no dhcp-server
```

6.1.6 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

【Usage】

It cannot enable with DHCP RELAY. It is defaulted to be disable.

【Example】

！Enable DHCP SNOOPING

```
QTECH(config)#dhcp-snooping
```

6.1.7 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 0/0/1 to be trust interface.

```
QTECH(config-if-ethernet-0/0/1)#dhcp-snooping trust
```

6.1.8 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 0 to 2048. it is defaulted to be 2048.

【Command configuration mode】

Interface configuration mode, VLAN configuration mode

【Example】

！Configure the max learning number of Ethernet 0/0/1 to be 33

```
QTECH(config-if-ethernet-0/0/1)#dhcp-snooping max-clients 33
```

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

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

6.1.9 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 e0/0/1

```
QTECH(config-if-ethernet-0/0/1)#ip-source-guard
```

6.1.10 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

```
QTECH(config)#show dhcp-relay
```

DHCP relay is enabled!

6.1.11 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

```
QTECH(config)#show dhcp-relay hide server-ip
DHCP RELAY hide server-ip is enabled!
```

6.1.12 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

QTECH(config)#show dhcp-server

6.1.13 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 1～4094

【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.

```
QTECH(config)#show dhcp-server interface
```

6.1.14 show dhcp-snooping

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

show dhcp-snooping

【Command configuration mode】

Any configuration mode

【Example】

！Display DHCP SNOOPING configuration

```
QTECH(config)#show dhcp-snooping
```

6.1.15 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

```
QTECH(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 01:00:5e:22:22:22，vlan being 2，ip addrss being 5.5.1.2

```
QTECH(config)#dhcp-client 01:00:5e:22:22:22 5.5.1.2 2
```

！Delete client with mac address being 01:00:5e:22:22:22，vlan being 2

QTECH(config)#no **dhcp-client** 01:00:5e: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 192.168.0.100

```
QTECH(config-ip-pool-nic)#dns primary-ip 192.168.0.100
```

！Delete primary DNS server of local IP address pool nic

```
QTECH(config-ip-pool-nic)#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 192.168.0.200

```
QTECH(config-ip-pool-nic)#dns second-ip 192.168.0.200
```

！Delete second DNS server of local IP address pool nic

```
QTECH(config-ip-pool-nic)#no dns second-ip
```

7.1.4 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 nic to be qtech.ru

```
QTECH(config-ip-pool-nic)#dns suffix qtech.ru
```

！Delete DNS suffix of address pool nic

```
QTECH(config-ip-pool-nic)#no dns suffix
```

7.1.5 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 192.168.0.100, netmask to be 255.255.255.0

```
QTECH(config-ip-pool-nic)#gateway 192.168.0.100 255.255.255.0
```

7.1.6 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

```
QTECH(config-ip-pool-nic)#ip disable 192.168.0.100
```

！Enable specified address in local IP address pool network

```
QTECH(config-ip-pool-nic)#ip enable 192.168.0.100
```

7.1.7 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

7.1.8 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 nic

```
QTECH(config)#ip pool nic
```

```
QTECH (config-ip-pool-nic)#
```

7.1.9 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 0:0:1 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 nic is 1 day 1 hour 1 minute

```
QTECH(config-ip-pool-nic)#lease 1:1:1
```

7.1.10 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

```
QTECH(config-ip-pool-nic)#section 0 192.168.0.100 192.168.0.200
```

！Delete local IP pool network interface 0

```
QTECH(config-ip-pool-nic)#no section 0
```

7.1.11 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

```
QTECH(config)#show dhcp-client
```

7.1.12 **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

```
QTECH(config)#show ip-bind
```

7.1.13 **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

QTECH(config)#show ip pool

7.1.14 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 nic to be 192.168.0.100

```
QTECH(config-ip-pool-nic)#wins primary-ip 192.168.0.100
```

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

```
QTECH(config-ip-pool-nic)#no wins primary-ip
```

7.1.15 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 nic to be 192.168.0.200

```
QTECH(config-ip-pool-nic)#wins second-ip 192.168.0.200
```

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

```
QTECH (config-ip-pool-nic)#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.

ip route *dst-ip mask gate-ip*

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

【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 0, 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 192.168.0.100 network interface, the next hop address is 10.11.0.254

```
QTECH(config)#ip route 192.168.0.100 255.255.0.0 10.11.0.254
```

！Delete route which is to 192.168.0.100 network interface

```
QTECH(config)#no ip route 192.168.0.100 255.255.0.0
```

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 192.168.0.100

```
QTECH(config)#show ip route 192.168.0.100
```

！Display all routing table

```
QTECH(config)#show ip route
```

！Display all rip routing table

```
QTECH(config)#show ip route rip
```

！Display all ospf routing table

```
QTECH(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

```
QTECH(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

```
QTECH(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 QTECH

```
QTECH(config-if-vlanInterface-3)#ip rip authentication QTECH
```

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

```
QTECH(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 0 to 16.

【Default】

It is defaulted to be 0.

【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

```
QTECH(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 0 to 16.

【Default】

It is defaulted to be 0.

【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

```
QTECH(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

```
QTECH(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.

```
QTECH(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

```
QTECH(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.

```
QTECH(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

```
QTECH(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

```
QTECH(config)#router rip
```

！Disable RIP protocol

```
QTECH(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 10，that is, the first seq number in a prefix acl is 10，and the second and the third is 20 and 30. 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：

```
QTECH(config)#ip prefix-list prefix001 permit 192.0.0.0 8 le 24
```

```
QTECH(config)#ip prefix-list prefix001 deny 192.0.0.0 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 0.0.0.0/32can match the route with the destination address and mask being 0（not matching the route with destination being 0 and mask being 1）；0.0.0.0/0 matches all routes.

【Example】

！Configure prefix ACL to deny route with destination address being 192.168.1.0/24（including all subnetwork route）

```
QTECH(config)#ip prefix-list pflst001 deny 192.168.1.0 24

QTECH(config)#ip prefix-list pflst001 permit 0.0.0.0 0
```

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

```
QTECH(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

```
QTECH(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

```
QTECH(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 pflst001

```
QTECH(config-router-rip)#distribute-list prefix-list pflst001 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

QTECH(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

```
QTECH(config-router-rip)#show ip rip interface

！Display RIP configuration of layer 3 interface 1

QTECH(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

```
QTECH(config-router-ospf)#area 0.0.0.1 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 0～16777215

【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 192.168.0.100 to be 10

```
QTECH(config-router-ospf)#area 192.168.0.100 default-cost 10
```

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 202.38.160.0/24 and 202.38.180.0/24 to be 202.38.0.0/16

```
QTECH(config-router-ospf)#network 202.38.160.0 255.255.255.0 area
1.1.1.1
QTECH(config-router-ospf)#network 202.38.180.0 255.255.255.0 area
1.1.1.1
QTECH(config-router-ospf)#area 1.1.1.1 range 202.38.0.0 255.255.0.0
```

10.1.4 **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.

```
QTECH(config-router-ospf)#area 1.1.1.1 stub
```

10.1.5 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 1 ~ 8192 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 10 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 40 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 0) . 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 10.11.5.2

```
QTECH(config-router-ospf)#area 1.1.1.1 virtual-link 10.11.5.2
```

10.1.6 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 keyword, it must configure default routing to introduce ase LSA.

metric-value：metric value of ase LSA which is in the range of 0 ~ 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.

```
QTECH(config-router-ospf)#default-information originate
```

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

```
QTECH(config-router-ospf)#default-information originate always
```

10.1.7 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 0～16777215.

【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 10

```
QTECH(config-router-ospf)#default redistribute metric 10
```

10.1.8 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.

```
QTECH(config-router-ospf)#default redistribute type 1
```

10.1.9 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

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

10.1.10 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 10

```
QTECH(config-if-vlanInterface-3)#ip ospf cost 10
```

10.1.11 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 40 seconds; The dead interval of OSPF neighbor for point-to-multipoint、non-broadcast is 120seconds.

【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 s*econds*, and the **dead-interval** *seconds* must be the same in the same network interface.

【Example】

！Configure the dead interval of interface 3 to be 60seconds

QTECH(config-if-vlanInterface-3)#ip ospf dead-interval 60

10.1.12 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 10 seconds; The time interval of sending Hello packet of interface for point-to-multipoint、non-broadcast is 30seconds.

【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.

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

10.1.13 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

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

10.1.14 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

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

10.1.15 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 0～255

【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 > 0 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 0, 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 100

```
QTECH(config-if-vlanInterface-3)#ip ospf priority 100
```

10.1.16 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 1～65535 秒

【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.

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

10.1.17 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.

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

10.1.18 **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 “0”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 192.168.0.100, mask to be 255.255.255.0 and OSPF area number to be 1.1.1.1

```
QTECH(config-router-ospf)#network 192.168.0.100 255.255.255.0 area
1.1.1.1
```

10.1.19 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

QTECH(config-router-ospf)#redistribute rip

10.1.20 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 192.168.0.100

```
QTECH(config)#router id 192.168.0.100
```

10.1.21 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

QTECH(config)#router ospf

！Disable OSPF

QTECH(config)#no router ospf

10.1.22 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

QTECH(config)#show ip ospf

10.1.23 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.

```
QTECH(config)#show ip ospf border-routers
```

10.1.24 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】

```
QTECH(config-if-vlanInterface-2)#show ip ospf cumulative
```

10.1.25 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

```
QTECH(config)#show ip ospf database
```

10.1.26 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.

```
QTECH(config-if-vlanInterface-2)#show ip ospf error
```

10.1.27 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 1～4094 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

```
QTECH(config)#show ip ospf interface
```

10.1.28 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.

```
QTECH(config)#show ip ospf neighbor
```

10.1.29 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.

```
QTECH(config)#show ip ospf request-list
```

10.1.30 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.

```
QTECH(config)#show ip ospf retrans-list
```

10.1.31 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.

```
QTECH(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    10    DInterval    40    TrDelay    1    RtInterval    5

-------------------------------------------------------

Total entries: 1 ospf virtual link
```

10.1.32 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.

```
QTECH(config)#show ip route ospf
```

10.1.33 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.

```
QTECH(config)#show router id

current router id :192.168.0.100
```

Chapter 11 Multicast Protocol Configuration Command

11.1 Static Multicast Configuration Command

Static multicast configuration command includes:

- **multicast mac-address**
- **multicast mac-address vlan interface**
- **show multicast**

11.1.1 **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: 01:00:5e:**:**:**

vlan-id：Range from 1 to 4094

【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

```
QTECH(config)#multicast mac-address 01:00:5e:01:02:03 vlan 1
```

11.1.2 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* i**nterface** { 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: 01:00:5e:**:**:**

vlan-id：Range from 1 to 4094. 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 0 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 0/2 from existed multicast group.

QTECH(config)#no multicast mac-address 01:00:5e:01:02:03 vlan 1 interface ethernet 0/2

11.1.3 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 01:00:5e:01:02:03

```
QTECH(config)#show multicast mac-address 01:00:5e:01:02:03
```

11.2 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**

11.2.1 **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

```
QTECH(config)#gmrp
```

！Disable the GMRP of Ethernet 0/3

```
QTECH(config-if-ethernet-0/3)#no gmrp
```

11.2.2 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

```
QTECH (config)#igmp-snooping
```

11.2.3 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 10 to 1000000 seconds

【Example】

！Configure host-aging-time of the dynamic multicast group learnt by igmp-snooping to be 10 seconds

```
QTECH(config)#igmp-snooping host-aging-time 10
```

11.2.4 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 100 seconds. The default time is 10 seconds

【Usage】

This command is effective when fast leave disables

【Example】

！Configure the max-response-time of igmp-snooping is 99 seconds

```
QTECH(config)#igmp-snooping max-response-time 99
```

11.2.5 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

```
QTECH(config-if-ethernet-0/1)#igmp-snooping fast-leave
```

11.2.6 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 0 to 128.　The default number is 128

【Example】

！Configure the igmp-snooping group-limit to be 99

```
QTECH(config-if-ethernet-0/1)#igmp-snooping group-limit 99
```

11.2.7 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 01:00:5e:01:02:03

【Example】

！Configure the learning regulation of default group to allow all multicast group

```
QTECH(config)#igmp-snooping permit group all
```

！Configure Ethernet 0/3 not to learn multicast 01:00:5e:00:01:01

```
QTECH(config-if-ethernet-0/3)#igmp-snooping deny group 01:00:5e:00:01:01
```

11.2.8 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

```
QTECH(config)#igmp-snooping route-port forward
```

11.2.9 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 4094

【Default】

No multicast VLAN configuration for port

【Example】

！Configure multicast vlan of Ethernet 0/1 to be vlan 2

```
QTECH(config-if-ethernet-0/1)#igmp-snooping multicast vlan 2
```

11.2.10 show gmrp

Use **show gmrp** command to display GMRP globally.

show gmrp

【Command configuration mode】

Any configuration mode

【Example】

！Display GMRP information globally

```
QTECH(config)#show gmrp
GMRP    state : enable
```

11.2.11 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 0 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 0/1, ethetnet 0/2, Ethernet 0/3, Ethernet 2/1

```
QTECH(config)#show gmrp interface ethernet 0/1 to ethernet 0/3 ethernet 3/2
```

```
port   GMRP status

e0/1   enable

e0/2   enable

e0/3   enable

e3/2   enable

Total entries: 4
```

11.2.12 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: 01:00:5e:**:**:**

vlan-id：Range from 1 to 4094. Multicast group is combined by vlan-id and mac

【Command configuration mode】

Global configuration mode

【Example】

! Add multicast group 01:00:5e:00:01:01 vlan 1 to GMRP

```
QTECH(config)#garp permit multicast mac-address 01:00:5e:00:01:01 vlan 1
```

11.2.13 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

```
QTECH(config)#show garp permit multicast
```

11.2.14 **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

QTECH(config)#show igmp-snooping

11.3 IGMP Configuration Command

IGMP configuration command includes:

- **ip igmp**
- **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 ip igmp groups**
- **show ip igmp interface**

11.3.1 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

```
QTECH(config-if-vlanInterface-1)#ip igmp
```

11.3.2 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 0 to 7, slot-num is in the range of 0 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
QTECH (config)# access-list 1 permit 225.0.0.0 0.255.255.255
！Specify host in VLAN interface 1 can only be added to the multicast grou
pwhich satisfied rules in access-list 1
QTECH(config-if-vlanInterface-1) # ip igmp access-group 1
```

11.3.3 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.

```
QTECH(config-if-vlanInterface-1)#ip igmp last-member-query-interval 2
```

11.3.4 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 30000 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 120 seconds

```
QTECH(config-if-vlanInterface-1)# ip igmp query-interval 120
```

11.3.5 **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 30000 seconds.

【Default】

The max response time in query packet of host member is 10 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.

```
QTECH(config-if-vlanInterface-1)# ip igmp query-max-response-time 8
```

11.3.6 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 0 to 7, slot-num is in the range of 0 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 10.0.0.1

```
QTECH(config-if-vlanInterface-1)# ip igmp static-group 224.1.1.1 ethernet 0/1
```

11.3.7 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 224.0.1.5 in vlan interface 1

```
QTECH(config-if-vlanInterface-1)# ip igmp create-group 224.0.1.5
```

11.3.8 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

```
QTECH(config-if-vlanInterface-1)# ip igmp robustness-varible 5
```

11.3.9 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 1024.

【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

```
QTECH(config-if-vlanInterface-1)# ip igmp limit-group 5
```

11.3.10 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.

```
QTECH(config-if-vlanInterface-1)# ip igmp version 1
```

11.3.11 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

```
QTECH(config)#ip multicast-routing
```

11.3.12 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.

```
QTECH(config)#show ip igmp group
```

11.3.13 **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.

```
QTECH#show ip igmp interface
```

11.4 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**
- **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**

11.4.1 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

```
QTECH(config-if-vlanInterface-1)#ip pim dense-mode
```

11.4.2 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 0～128。

【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

```
QTECH(config-if-vlanInterface-1)#ip pim neighbor-limit 16
```

11.4.3 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

```
QTECH (config)# access-list 1 permit 10.0.0.0 0.255.255.255
```

！Learn the neighbor which is in in VLAN interface 1 and satisfies the rules in access-list 1

```
QTECH(config-if-vlanInterface-1) # ip pim neighbor-policy 1
```

11.4.4 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 30s.

【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 60 seconds

```
QTECH(config-if-vlanInterface-1)#ip pim query-interval 60
```

11.4.5 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.

```
QTECH(config-if-vlanInterface-1)#ip pim sparse-mode
```

11.4.6 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

```
QTECH(config-if-vlanInterface-1)#ip pim bsr-border
```

11.4.7 pim

Use **pim** command to enter pim configuration.

pim

【Command configuration mode】

Global configuration mode

【Usage】

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

QTECH(config)# pim

11.4.8 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

```
QTECH(config-if-vlanInterface-1)#show ip mroute
```

11.4.9 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 4094.

【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

```
QTECH(config-if-vlanInterface-1)# show ip pim neighbor
```

11.4.10 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 1～4094.

【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

```
QTECH(config-if-vlanInterface-1)#show ip pim interface
```

11.4.11 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.

```
QTECH(config-if-vlanInterface-1)#show ip pim rp-info
```

11.4.12 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

```
QTECH(config-if-vlanInterface-1)#show ip pim bsr
```

11.4.13 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

```
QTECH (config)# access-list 1 permit 192.168.1.1 0
QTECH(config-pim) # source-policy 1
```

11.4.14 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

```
QTECH(config-pim) # static-rp 192.168.1.1
```

11.4.15 **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 0～32. 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 0～255. 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 0.

【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

```
QTECH(config-pim) # bsr-candidate vlan-interface 1 10 10
```

11.4.16 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 0～255. 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

```
QTECH(config-pim) # rp-candidate vlan-interface 1 group-list 1 10
```

Chapter 12 ACL Configuration Command

12.1 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**

12.1.1 **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 0 ~ 23，mm is in the range of 0 - 59, and ss is in the range of 0 - 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 0:0 Jan 1st, 2000.

```
QTECH(config)#time-range tm1
QTECH(config-timerange-tm1)#absolute start 0:0 1-1-2000
QTECH(config-timerange-tm1)#exit
```

！The following time range will be effective from 22:00 December 10, 2000 to

```
22:01
QTECH(config)#time-range tm2
QTECH(config-timerange-tm2)#absolute end 22:00 12-10-2000
QTECH(config-timerange-tm2)#exit
```

！The following time range will be effective from 14:00 to 16:00 in each weekend from 20:00 December 31, 1999 to 20:00 December 10, 2000.（The configuration of periodic time range refers to periodic command.）

```
QTECH(config)# time-range testall
QTECH(config-timerange-testall)#absolute start 20:00 12-31-1999 end 20:00
12-10-2000
QTECH(config-timerange-testall)#periodic weekend 14:00 to 16:00
QTECH(config-timerange-testall)#exit
```

12.1.2 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 0 ~ 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 200 at the same time.

```
QTECH(config)#access-group ip-group 1 link-group 200
```

12.1.3 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** *preceden*ce] [**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 100 ~ 199

access-list-number3：Layer 2 ACL rules in the range of 200 ~ 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 0～65535,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 0～65535. 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 0 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 一 ICMP packet. icmp-type means ICMP packey type which is in the form of characters and numbers. The number is in the range of 0 ~ 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 0 ~ 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 0 ~ 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 0 ~ 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 0 ~ 15. This parameter can be used in extended ACL.

[**cos** *vlan-pri*]： 802.1p priority which is in the range of 0 ~ 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 0:0:0:0:ff:ff，user is interested in the first 32 bit of source MAC address (that is the bit position corresponded to the number 0 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 0:0:0:0:ff:ff , user is interested in the first 32 bit of source MAC address (that is the bit position corresponded to the number 0 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* }&<1-20> ：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. &<1-20> means at most 20 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 0 ~ 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

```
QTECH(config)#access-list 1 deny 192.168.3.1 0
```

！Configure ACL 100 to deny packet with the 0xff of TCP source port number to be 0

```
QTECH(config)# access-list 100 deny tcp any 0 0xff any
```

12.1.4 **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 0～127. 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.

```
QTECH(config)#access-list extended example match-order auto
```

12.1.5 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 0 ~ 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.

QTECH(config)#access-list link example match-order auto

12.1.6 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.

```
QTECH(config)#access-list 1 match-order auto
```

12.1.7 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 0～127. 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.

QTECH(config)#access-list standard example match-order auto

12.1.8 { **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* [*portmas*k]] [*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 0～65535,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 0～65535. 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 0 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 一 ICMP packet. icmp-type means ICMP packey type which is in the form of characters and numbers. The number is in the range of 0～255；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 0～255；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 0 ~ 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 0 ~ 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 0 ~ 15. This parameter can be used in extended ACL.

[**cos** *vlan-pri*] : 802.1p priority which is in the range of 0 ~ 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 0:0:0:0:ff:ff，user is interested in the first 32 bit of source MAC address (that is the bit position corresponded to the number 0 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 0:0:0:0:ff:ff，user is interested in the first 32 bit of source MAC address (that is the bit position corresponded to the number 0 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* }&<1-20>：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. &<1-20> means at most 20 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 0～127. 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.

```
QTECH(config)#access-list standard example match-order auto
Create ACL item successfully!
QTECH(config-std-nacl-example)#permit 192.168.3.1 0
Config ACL subitem successfully!
QTECH(config-std-nacl-example)#
```

12.1.9 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:

0～6（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 8:00 to 18:00 in every weekday is:

```
QTECH(config-timerange-test)#periodic weekdays 8:00 to 18:00
```

Or:

```
QTECH(config-timerange-test)#periodic Monday Tuesday Wednesday
Thursday Friday 8:00 to 18:00
```

The configuration of 8:00 to 18:00 from Monday to Friday is:

```
QTECH(config-timerange-test)#periodic Monday 8:00 to Friday 18:00
```

【Example】

```
！The time range is effective in 8:00 to 18:00 from Monday to Friday
QTECH(config)#time-range 1to5
QTECH(config-timerange-1to5)#periodic weekdays 8:00 to 18:00
QTECH(config-timerange-1to5)#exit
！The time range is effective in 8:00 to 18:00 every day
QTECH(config)#time-range all_day
QTECH(config-timerange-all_day)#periodic daily 8:00 to 18:00
QTECH(config-timerange-all_day)#exit
！The time range is effective in 8:00 to 18:00 from every Monday to Friday
QTECH(config)#time-range 1to5
QTECH(config-timerange-1to5)#periodic monday 8:00 to friday 18:00
QTECH(config-timerange-1to5)#exit
```

```
！The time range is effective in every weekend
QTECH(config)#time-range wend2
QTECH(config-timerange-wend2)#periodic weekend 0:0 to 23:59
QTECH(config-timerange-wend2)#exit
！The time range is effective in every weekend afternoon
QTECH(config)#time-range wendafternoon
QTECH(config-timerange-wendafternoon)#periodic weekend 14:00 to 18:00
QTECH(config-timerange-wendafternoon)#exit
```

12.1.10 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 0 to 7, slot-num is in the range of 0 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 0/0/1 ethernet 0/0/3 to ethernet 0/0/5 ethernet 0/0/8 to be port isolation downlink port

```
QTECH(config)#port-isolation ethernet 0/0/1 ethernet 0/0/3 to ethernet 0/0/5
ethernet 0/0/8
```

！Delete ethernet 0/0/3 to ethernet 0/0/5 ethernet 0/0/8 from port isolation downlink port

```
QTECH(config)#no port-isolation ethernet 0/0/3 to ethernet 0/0/5 ethernet
0/0/8
```

12.1.11 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 *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 0 to 7, slot-num is in the range of 0 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

【Command configuration mode】

Global configuration mode

【Example】

！Add e0/0/1 and e0/0/3 to port isolation 1

```
QTECH(config)#port-isolation group 1 ethernet 0/0/1 ethernet 0/0/3
```

！Delete port isolation 1

```
QTECH(config)#no port-isolation group 1
```

12.1.12 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

```
QTECH#show access-list config all
```

12.1.13 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.

```
QTECH(config)#show access-list config statistic
```

12.1.14 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.

```
QTECH#show access-list runtime all
```

12.1.15 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.

```
QTECH(config)#show access-list runtime statistic
```

12.1.16 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

```
QTECH(config)#show port-isolation
```

12.1.17 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

```
QTECH(config-timerange-tm2)#show time-range all
```

！Display time range with the name of tm1

```
QTECH(config)#show time-range name tm1
```

! Display statistic information of all time range:

```
QTECH(config)#show time-range statistic
```

12.1.18 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.

```
QTECH(config)#time-range tm1

QTECH(config-timerange-tm1)#
```

Chapter 13 QOS Configuration Command

13.1 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**

13.1.1 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 0～127. 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 200～299；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 0～127. 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

```
QTECH#clear traffic-statistic ip-group 1
```

13.1.2 line-rate

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.

line-rate *target-rate*

no line-rate

【Parameter】

target-rate :the total speed of sending packet which is in the range of 1 ~ 100 , 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 0/01 to be 10

```
QTECH(config-if-fastEthernet-1)#line-rate 10
```

13.1.3 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 0 ~ 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 200～299；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 0～127. 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

QTECH(config)#mirrored-to ip-group 1 interface ethernet 0/0/1

13.1.4 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: 20、30、50. 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 100.

【Example】

！Configure queue-scheduler to be weighted round robin, and 4 weights to be 20、20、30、30

```
QTECH(config)#queue-scheduler wrr 20 20 30 30
```

13.1.5 queue-scheduler cos-map

Use **queue-scheduler cos-map** command to configure 4 queue numbers and cos-map to 8 packed-priority of IEEE802.1p.

queue-scheduler cos-map [*queue-number*] [*packed-priority*]

【Parameter】

queue-number：Range from 0 to 3

packed-priority：The priority defined by IEEE 802.1p ranges from 0 to 7

【Default】

The default mapping is the mapping defined by 802.1p：

802.1p:	0	1	2	3	4	5	6	7
packed-priority：	0	0	1	1	2	2	3	3

【Command configuration mode】

Global configuration mode

【Usage】

There are 4 default packed-priorities from 0 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 802.1p

```
QTECH(config)#queue-scheduler cos-map 1 6
```

13.1.6 queue-scheduler dscp-map

Use this command to configure the mapping relationship between DSCP and 8 priority in IEEE 802.1p.

queue-scheduler dscp-map [*dscp-value*] [*packed-priority*]

【Parameter】

dscp-value：DSCP in ToS which is in the range of 0～63

packed-priority：The priority defined by IEEE 802.1p ranges from 0 to 7

【Default】

The default mapping relationship is that all DSCP map to priority 0.

【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

```
QTECH(config)#queue-scheduler dscp-map 2 5
```

13.1.7 **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 300～399；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 0～

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 0 ~ 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 200 ~ 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 0 ~ 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.

QTECH(config)#rate-limit input ip-group 1 64 exceed-action drop

13.1.8 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

QTECH#show qos-info all

13.1.9 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

```
QTECH#show qos-info mirrored-to
```

13.1.10 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

```
QTECH(config)#show qos-info statistic
```

13.1.11 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

```
QTECH#show qos-info traffic-copy-to-cpu
```

13.1.12 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

```
QTECH#show qos-interface traffic-priority
```

13.1.13 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

```
QTECH#show qos-info traffic-redirect
```

13.1.14 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

```
QTECH#show qos-info traffic-statistic
```

13.1.15 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

QTECH#show qos-info all

13.1.16 **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

```
QTECH(config-if-ethernet-0/04)#show qos-interface line-rate
```

13.1.17 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

```
QTECH#show qos-interface rate-limit
```

13.1.18 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

```
QTECH(config)#show qos-interface statistic
```

13.1.19 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

```
QTECH#show queue-scheduler
Queue scheduling mode: strict-priority
```

13.1.20 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

```
QTECH(config)#show queue-scheduler cos-map
```

13.1.21 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 0/5 to be 1Kpps

QTECH(config-if-ethernet-0/0/5)#storm-control broadcast 1024

13.1.22 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 0 ~ 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 200 ~ 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 0 ~ 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

QTECH(config)#traffic-copy-to-cpu ip-group 1

13.1.23 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 0 ~ 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 200 ~ 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 0 ~ 127. If it is not specified, all subitems will be clear.

dscp *dscp-value*：configure DSCP priority which is in the range of 0 ~ 63.

precedence { *pre-value* | from-cos }：configure IP priority. pre-value is IP priority which is in the range of 0 ~ 7；from-cos means configure IP priority to be the same as 802.1p priority.

cos { *pre-value* | from-ipprec }：configure 802.1p priority. *pre-value* is 802.1p priority which is in the range of 0～7 ; from-ipprec means the priority of 802.1p and IP is the same.

local-precedence *pre-value*：configure local priority which is in the range of 0～7.

【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 802.1p priority) and also can locate packet to corresponding outputting queue according to the specified local priority. If both 802.1p priority and local priority are configured, 802.1p priority will be precedent to use.

【Example】

！Configure the priority of data packet which matches the permit rules of accessing list 1 to be 0

```
QTECH(config)#traffic-priority ip-group 1 local-precedence 0
```

13.1.24 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 0～127. 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 200～299；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 0～127. 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

QTECH(config)#traffic-redirect ip-group 1 interface ethernet 0/0/1

13.1.25 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 0～127. 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 200～299；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 0～127. 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

```
QTECH(config)#traffic-statistic ip-group 1
```

Chapter 14 STP Configuration Command

14.1 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**

14.1.1 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 0 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

```
QTECH#show spanning-tree interface ethernet 0/0/7
```

14.1.2 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 0 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

```
QTECH(config)#show spanning-tree remote-loop-detect interface e 0/1
```

14.1.3 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

```
QTECH(config)#spanning-tree
```

！Disable STP on Ethernet 0/0/8

```
QTECH(config-if-ethernet-0/0/8)#no spanning-tree
```

14.1.4 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 802.1D protocol, the default cost is determined by the speed of the port. The port with the speed 10M have the cost of 100，100M, 19.

【Command configuration mode】

Interface configuration mode

【Usage】

Default cost is suggested to use.

【Example】

！Configure path cost of Ethernet 0/0/8 to 20

QTECH(config-if-ethernet-0/0/8)#spanning-tree cost 20

14.1.5 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 30 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 20 seconds

```
QTECH(config)#spanning-tree forward-time 20
```

14.1.6 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 10 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

```
QTECH(config)#spanning-tree hello-time 8
```

14.1.7 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 40 seconds

【Default】

The default Max Age is 20 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 20 seconds is suggested.

⚠ Caution：2*(Hello Time + 1) ≤ Max Age ≤ 2*(ForwardDelay – 1)

【Example】

！Configure the Max Age to 10 seconds

```
QTECH(config)#spanning-tree max-age 10
```

14.1.8 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 0 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 0/0/1 in STP to 64

```
QTECH(config-if-ethernet-0/0/1)#spanning-tree port-priority 64
```

14.1.9 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 0/0/7 to send RSTP message

```
QTECH(config-if-ethernet-0/0/7)#spanning-tree mcheck
```

14.1.10 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 0/0/7 as a point-to-point link

```
QTECH(config-if-ethernet-0/0/7)#spanning-tree point-to-point forcetrue
```

14.1.11 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 0/0/7 as a non-edge port.

```
QTECH(config-if-ethernet-0/0/7)#spanning-tree portfast
```

14.1.12 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 0/0/7 in each Hello time to 5

```
QTECH(config-if-ethernet-0/0/7)#spanning-tree transit-limit 5
```

14.1.13 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 0 to 61440，and must be a multiple of 4096.

【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 4096

```
QTECH(config)#spanning-tree priority 4096
```

14.1.14 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

```
QTECH(config)#spanning-tree mode stp
```

14.1.15 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 0/0/1, and ethernet 0/0/3

```
QTECH(config)#spanning-tree remote-loop-detect interface ethernet 0/0/1
```

```
ethernet 0/0/3
```

```
！Disable remote-loop-detect of Ethernet 0/0/1
```

```
QTECH(config-if-ethernet-0/0/1)#no spanning-tree remote-loop-detect
```

14.1.16 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 0 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

```
QTECH(config)#clear spanning-tree
```

14.2 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.

14.2.1 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 0-255

【Default】

The default hops is 20

【Command configuration mode】

Global configuration mode

【Example】

！Configure the max-hops of MSTP packet to be 10

```
QTECH(config)#spanning-tree mst max-hops 10
```

14.2.2 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 nicnet

```
QTECH(config)#spanning-tree mst name nicnet
```

14.2.3 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 0 to 65535.

【Default】

The default value is 0.

【Command configuration mode】

Global configuration mode

【Example】

！Configure revision level of MSTP to be 10

QTECH(config)#spanning-tree mst revision 10

14.2.4 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, 10-20

【Default】

All vlan mapped to MSTP instance 0

【Command configuration mode】

Global configuration mode

【Example】

！Configure vlan 2-7 mapping to MSTP instance 2

```
QTECH(config)#spanning-tree mst instance 2 vlan 2-7
```

14.2.5 **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 0-15

priority：the priority of network bridge which is the integer times of 4096 in the range of 0-61440

【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 4096

```
QTECH(config)#spanning-tree mst instance 2 priority 4096
```

14.2.6 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 1-200000000.

【Default】

The external cost of port is 200000.

【Command configuration mode】

Interface configuration mode

【Example】

！Configure the external cost of port 2 to be 200

```
QTECH(config-if-ethernet-0/0/2)#spanning-tree mst external cost 200
```

14.2.7 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 0-15

cost：port cost which is in the range of 1-200000000

【Default】

The cost for port in each instance is 200000

【Command configuration mode】

Interface configuration mode

【Example】

！Configure the cost for port 2 in instance 1 to be 200

```
QTECH(config-if-ethernet-0/0/2)#spanning-tree mst instance 1 cost 200
```

14.2.8 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 0-15

priority：port priority which is the integer times of 16 and is in the range of 1-240

【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

```
QTECH(config-if-ethernet-0/0/2)#spanning-tree mst instance 1 port-priority
16
```

14.2.9 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

```
QTECH(config)#show spanning-tree mst config-id
```

14.2.10 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 0 to 7, slot-num is in the range of 0 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 0

```
QTECH(config)#show spanning-tree mst instance 0 interface ethernet 0/0/1
```

Chapter 15 802.1X Configuration Command

15.1 Domain Configuration Command

Domainn configuration command includes:

- aaa
- access-limit
- default domain-name enable
- domain
- show domain
- radius host binding
- state

15.1.1 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

```
QTECH(config)#aaa

QTECH(config-aaa)#
```

15.1.2 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 640

【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 nic.com to 500

```
QTECH(config-aaa-nic.com)#access-limit enable 500
```

15.1.3 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 nic.com and enable the default domain

```
QTECH(config-aaa)#default domain-name enable nic.com
```

! Disable default domain name

```
QTECH(config-aaa)#default domain-name disable
```

【Related command】

domain

15.1.4 **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 nic.com

QTECH(config-aaa)#domain nic.com

QTECH(config-aaa-nic.com)#

！Remove domain with the name of nic.com

QTECH(config-aaa)#no domain nic.com
```

【Related command】

radius host, state

15.1.5 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 nic.com

```
QTECH(config-aaa-nic.com)#show domain
```

15.1.6 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 “nic”

```
QTECH(config-aaa-nic.com)#radius host binding nic
```

【Related command】

radius host（RADIUS configuration mode）

15.1.7 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 nic.com

```
QTECH(config-aaa-nic.com)#state active
```

【Related command】

domain

15.2 RADIUS Server Configuration Command

RADIUS server configuration command includes:

- **primary-ip**
- **radius host**

- realtime-account

- second-ip

- secret-key

- show radius host

- username-format

15.2.1 primary-ip

Use **primary-ip** command to configure primary IP address, authentication port and accounting port of RADIUS server. Use **no primary-ip** command to delete primary IP address of current RADIUS server.

primary-ip *server-ip authentication-port accounting-port*
no primary-ip

【Parameter】

server-ip：IP address of primary server

authentication-port：Authentication port ranges from 1 to 65535

accounting-port：Accounting port ranges from 1 to 65535

【Default】

Default authentication port is 1812, and accounting port by default is 1813

【Command configuration mode】

RADIUS configuration mode

【Example】

！ Configure ip address of primary authentication server to be 192.168.0.100 ， and authentication port to be 1812, accounting port to be 1813

```
QTECH(config-aaa-radius-nic)#primary-ip 192.168.0.100 1812 1813
```

！Remove ip address of primary accounting server

```
QTECH(config-aaa-radius-nic)#no primary-ip
```

【Related command】

radius host，second-ip

15.2.2 radius host

Use **radius host** command to create RADIUS server and enter it. If RADIUS server exists, enter it. Use **no radius** command to remove specified RADIUS server from radius-scheme.

radius host radius-scheme

no radius radius-scheme

【Parameter】

radius-scheme：The name of RADIUS server ranges from 1 to 32 charaters with no difference in upper-case type and lower case letters and without space.

【Command configuration mode】

AAA configuration mode

【Example】

！Create RADIUS server with the name of myScheme and enter it

```
QTECH(config-aaa)#radius host myScheme

QTECH(config-aaa-radius-myScheme)#
```

【Related command】

radius host (domain configuration mode)

15.2.3 realtime-account

Use **realtime-account** command to configure the real-time account, and the accounting interval. Use **no realtime-account** command to disable the real-time account.

realtime-account interval *minute*
no realtime-account

【Parameter】

minute：Real-time accounting interval ranges from 1 to 255 minutes.

【Default】

Enable real-time accounting with the interval of 12 minutes

【Command configuration mode】

RADIUS configuration mode

【Example】

！Configure the real-time accounting interval of the RADIUS server to be 30 minutes

```
QTECH(config-aaa-radius-nic)#realtime-account interval 30
```

！Disable the real-time accounting

```
QTECH(config-aaa-radius-nic)#no realtime-account
```

15.2.4 second-ip

Use **second-ip** command to configure second IP address, authentication port and accounting port of RADIUS server. Use **no second-ip** command to delete second IP address of current RADIUS server.

second-ip *server-ip authentication-port accounting-port*

no second-ip

【Parameter】

server-ip：IP address of second server

authentication-port：Authentication port ranges from 1 to 65535

accounting-port：Accounting port ranges from 1 to 65535

【Default】

Default authentication port is 1812, and accounting port by default is 1813

【Command configuration mode】

RADIUS configuration mode

【Example】

！ Configure ip address of second authentication server to be 192.168.0.200， and authentication port to be 1812, accounting port to be 1813

```
QTECH(config-aaa-radius-nic)#second-ip 192.168.0.200 1812 1813
```

！Remove ip address of second accounting server

```
QTECH(config-aaa-radius-nic)#no second-ip
```

【Related command】

radius host，primary-ip

15.2.5 **secret-key**

Use **secret-key** command to configure a shared key for the RADIUS server.

Use **no secret-key** command to restore the default shared key.

secret-key key-string

no secret-key

【Parameter】

key-string：Shared key of 1 to 16 characters of strings

【Default】

The default key is Switch

【Command configuration mode】

RADIUS configuration mode

【Usage】

There are such configuration as system ip address and verified key in RADIUS server. Only when the system key is the same as the RADIUS server key, the authentication requirement is accepted by RADIUS server.

【Example】

！Configure the shared key for the RADIUS server with the name of nic to be

```
12345
QTECH(config-aaa-radius-nic)#secret-key 12345
```

【Related command】

radius host

15.2.6 show radius host

Use **show radius host** command to display RADIUS server information, such as: primary ip address, second ip address, authentication port, accounting port, authentication key, etc.

show radius host [*radius-scheme*]

【Parameter】

radius-scheme：The name of RADIUS server

【Command configuration mode】

Any configuration mode

【Example】

！Display RADIUS server information

```
QTECH(config-aaa-radius-default)#show radius host
```

15.2.7 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 nic not to carry domain name.

```
QTECH(config-aaa-radius-nic)#username-format without-domain
```

【Related command】

radius host

15.3 802.1X Related Configuration Command

802.1X 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

15.3.1 **dot1x**

Use **dot1x** command to enable 802.1x. Use **no dot1x** command to disable 802.1x.

dot1x

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 802.1x enables.

【Example】

！Enable 802.1X

```
QTECH(config)#dot1x
```

！Disable 802.1X

```
QTECH(config)#no dot1x
```

15.3.2 dot1x daemon

When 802.1x enables, configure whether a port send 802.1x daemon and sending period.

dot1x daemon [time *time-value*] [interface *interface-list*]
no dot1x daemon

【Parameter】

time-value：the intervals of 802.1x daemon sending ranges from 10 to 600 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 0 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】

802.1x daemon is not sent by default. When 802.1x enables, default interval to send daemon is 60seconds.

【Command configuration mode】

Interface configuration mode, global configuration mode

【Usage】

This command is effective after 802.1x enables.

After 802.1x enables, configure according to the real situation.

【Example】

！Enable dot1x daemon on ethernet 0/5 with the period time of 20 seconds

```
QTECH(config-if-ethernet-0/5)#dot1x daemon time 20
```

！Configure dot1x daemon of ethernet 0/5 globally with the period time of 20 seconds

```
QTECH(config)# dot1x daemon time 20 interface ethernet 0/5
```

！Restore the default dot1x daemon configuration on ethernet 0/5

```
QTECH(config-if-fastethernet-5)#no dot1x daemon
```

！Restore the default dot1x daemon configuration of ethernet 0/5 globally

```
QTECH(config)#no dot1x daemon interface ethernet 0/5
```

15.3.3 dot1x eap-finish

After using dot1x eap-transfer command, 802.1 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

QTECH(config)#dot1x eap-finish

【Related command】

dot1x eap-transfer

15.3.4 **dot1x eap-transfer**

After using **dot1x eap-transfer** command, 802.1 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

```
QTECH(config)#dot1x eap-transfer
```

【Related command】

dot1x eap-finish

15.3.5 **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 100M ethernet port is 16

【Command configuration mode】

Interface configuration mode or global configuration mode

【Usage】

This command is effective after 802.1X authentication.

After 802.1X enables, max-user of a port is determined by the real situation.

The max-user of 100M ethernet port is 16

【Example】

！Configure the max-user of ethernet 0/5 is 10 in interface configuration mode

```
QTECH(config-if-ethernet-0/5)#dot1x max-user 100
```

！Configure the max-user of ethernet 0/5 is 10 globally

```
QTECH(config)#dot1x max-user 100 interface ethernet 0/5
```

！Restore the default max-user of ethernet 0/5 in interface configuration mode

```
QTECH(config-if-fastethernet-5)#no dot1x max-user
```

！Restore the default max-user of ethernet 0/5 globally

```
QTECH(config)#no dot1x max-user interface ethernet 0/5
```

15.3.6 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 802.1X authentication.

After 802.1X 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 0/5 is RADIUS server port. Configure port-control mode of ethernet 0/5 to be forceauthorized in interface configuration mode

```
QTECH(config-if-ethernet-0/5)#dot1x port-control forceauthorized
```

！Configure port-control mode of ethernet 0/5 to be forceauthorized globally.

```
QTECH(config)#dot1x port-control forceauthorized interface ethernet 0/5
```

【Related command】

dot1x

15.3.7 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 802.1X authentication.

802.1X re-authenticate only supports the message transmitting way of dot1x eap-transfer.

【Example】

！Re-authenticate ethernet 0/5 in interface configuration mode

```
QTECH(config-if-ethernet-0/5)#dot1x re-authenticate
```

！Re-authenticate ethernet 0/5 globally

```
QTECH(config)#dot1x re-authenticate interface ethernet 0/5
```

15.3.8 dot1x re-authentication

Use **dot1x re-authentication** command to enable 802.1x re-authentication.

Use **no dot1x re-authentication** command to disable 802.1x re-authentication.

dot1x re-authentication

no dot1x re-authentication

【Default】

802.1X re-authentication disable

【Command configuration mode】

Interface configuration mode, global configuration mode

【Usage】

This command is effective after 802.1x authentication enables.

802.1X authentication only supports the message sending of dot1x eap-transfer.

【Example】

！Enable re-authentication of ethernet 0/5

```
QTECH(config-if-ethernet-0/5)#dot1x re-authentication
QTECH(config)#dot1x re-authentication interface ethernet 0/5
```

【Related command】

dot1x、dot1x eap-finish、dot1x eap-transfer

15.3.9 dot1x timeout re-authperiod

Use **dot1x timeout re-authperiod** command to configure 802.1x re-authperiod.

Use **no dot1x timeout re-authperiod** command to restore the default 802.1x re-authperiod.

dot1x timeout re-authperiod *seconds* [interface *interface-num*]

no dot1x timeout re-authperiod [interface *interface-num*]

【Parameter】

seconds: 802.1X re-authperiod ranges from 1 to 65535 seconds

interface-num：Optional interface number

【Default】

The default 802.1X re-authperiod is 3600 seconds

【Command configuration mode】

Global configuration mode

【Usage】

This command is effective after 802.1X authentication enables.

When no port is specified, use dot1x timeout re-authperiod command to modify 802.1x re-authperiod of all ports，or specified port is modified.

【Example】

！Configure 802.1x re-authperiod of ethernet 0/3 to be 1800

```
QTECH(config)#dot1x timeout re-authperiod 1800 interface ethernet 0/3
```

！Restore all the re-authperiod to the default of 802.1x re-authperiod

```
QTECH(config)#no dot1x timeout re-authperiod
```

15.3.10 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@qtech.ru

QTECH(config)#dot1x user cut username aaa@qtech.ru

15.3.11 show dot1x

Use **show dot1x** command to display 802.1x authentication information, such as: 802.1x 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 802.1x authentication information

```
QTECH(config)#show dot1x
```

15.3.12 show dot1x daemon

Use **show dot1x daemon** command to display 802.1x daemon configuration.

show dot1x daemon [interface *interface-num*]

【Parameter】

interface-num：Optioned interface number

【Command configuration mode】

Any configuration mode

【Example】

！Display the 802.1x daemon of all the ports

```
QTECH(config)#show dot1x daemon
```

15.3.13 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 0/5

```
QTECH(config)#show dot1x interface ethernet 0/5
```

15.3.14 show dot1x session

Use **show dot1x session** command to display 802.1x 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

```
QTECH(config)#show dot1x session
```

Chapter 16 SNTP Client Configuration Command

16.1 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**

16.1.1 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

QTECH(config)#show sntp client

16.1.2 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

```
QTECH(config)#sntp client
```

16.1.3 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

```
QTECH(config)#sntp client authenticate
```

16.1.4 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

```
QTECH(config)#sntp client authentication-key 12 md5 abc
```

16.1.5 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

```
QTECH(config)#sntp client broadcastdelay 1000
```

16.1.6 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 0 to 4294967295，0 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

```
QTECH(config)#sntp client mode anycast
```

16.1.7 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

```
QTECH(config)#sntp client multicast ttl 5
```

16.1.8 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 1024 seconds

【Default】

1000 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 100 seconds

```
QTECH(config)#sntp client poll-interval 100
```

16.1.9 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 10

【Default】

non-retransmit（0）

【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

```
QTECH(config)#sntp client retransmit 2
```

16.1.10 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 30 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 10 seconds.

```
QTECH(config)#sntp client retransmit-interval 10
```

16.1.11 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 0

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

```
QTECH(config)#sntp client valid-server 10.1.0.2 0.0.255.255
```

16.1.12 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 0 to 4294967295. 0 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 192.168.0.100

```
QTECH(config)#sntp server 192.168.0.100
```

16.1.13 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

```
QTECH(config)#sntp trusted-key 12
```

Chapter 17 Syslog Configiration Command

17.1 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**

17.1.1 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.

QTECH(config)#show logging

17.1.2 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 0 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

```
QTECH(config)#show logging buffered level-list 7
```

17.1.3 **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 0 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

```
QTECH(config)#show logging flash module vlan
```

17.1.4 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. 0 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

```
QTECH(config)#show logging filter buffered
```

17.1.5 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

```
QTECH(config)#show debug
```

17.1.6 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

```
QTECH(config)#logging
```

17.1.7 **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.

```
QTECH(config)#logging sequence-numbers
```

17.1.8 **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

```
QTECH(config)#logging timestamps datetime
```

17.1.9 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

```
QTECH(config)#logging language chinese
```

17.1.10 **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. 0 means console, and 1 to 5 means Telnet terminal.

level：Level of information ranges from 0 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

```
QTECH(config)#logging monitor 0
```

！Configure filter regulations of all terminals to allow all module of levels 0 to 6 to output information

```
QTECH(config)#logging monitor 0 6
```

17.1.11 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

```
QTECH(config)#terminal monitor
```

17.1.12 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 0 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 0 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

QTECH(config)#no logging buffered

！Configure filter regulations of all terminals to allow all module of level 0,1,2 and 6 to output information

```
QTECH(config)#logging buffered level-list 0 to 2 6
```

17.1.13 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

```
QTECH(config)#clear logging buffered
```

17.1.14 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 0 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 0 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

```
QTECH(config)#no logging flash
```

！Configure filter regulations of all terminals to allow all vlan module to output information

```
QTECH(config)#logging flash none
QTECH(config)#logging flash 7 module vlan
```

17.1.15 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

QTECH(config)#clear logging flash

17.1.16 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 0 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 0 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

```
QTECH(config)#logging 1.1.1.1
```

！Enable logging host 1.1.1.1

```
QTECH(config)#logging host 1.1.1.1
```

！Configure filter regulations of logging host 1.1.1.1 to allow all module of level 0 to 6 to output information

```
QTECH(config)#logging host 1.1.1.1 6
```

17.1.17 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 localuse0

```
QTECH(config)#logging facility localuse0
```

17.1.18 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

```
QTECH(config)#logging source 1.1.1.2
```

17.1.19 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：Level of information ranges from 0 to 7

none：Any level is not allowed.

xxx：Means the name of the module. … means other modules are omitted.

【Default】

All SNMP Agent logging enable.

Filter regulations of all terminals are to allow all modules of levels 0 to 5 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.

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

```
QTECH(config)#logging snmp-agent
```

！Configure SNMP Agent outputting filtration rule to be permitting 0 to 3 levels of information

```
QTECH(config)#logging snmp-agent 3
```

【Related command】

snmp-server host

17.1.20 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

```
QTECH(config)#debug vlan
```

17.1.21 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

```
QTECH(config)#upload logging tftp 1.1.1.1 aaa.txt
```

Chapter 18 SSH Configuration Command

18.1 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**

18.1.1 **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

```
QTECH#show ssh
```

18.1.2 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

```
QTECH#show keyfile public
```

18.1.3 ssh

Use this command to enable/disable SSH.

ssh

no ssh

【Default】

Disable

【Command configuration mode】

Global configuration mode

【Example】

！Enable SSH

```
QTECH(config)#ssh
```

18.1.4 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.

```
QTECH#crypto key generate rsa
```

18.1.5 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

```
QTECH#crypto key zeroize rsa
```

18.1.6 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.

QTECH#crypto key refresh

18.1.7 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

```
QTECH#load keyfile public tftp 1.1.1.1 pub.txt
```

18.1.8 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

```
QTECH#upload keyfile public tftp 1.1.1.1 pub.txt
```

Chapter 19 VRRP Configuration Command

19.1 VRRP configuration command list

VRRP configuration command includes:

- **ip vrrp**
- **show vrrp**
- **vrrp ping-enable**
- **vrrp preempt**
- **vrrp priority**
- **vrrp timer**

19.1.1 **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

```
QTECH(config-if-vlanInterface-1)#ip vrrp 1 192.168.1.1
```

19.1.2 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

```
QTECH#show vrrp
```

19.1.3 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.

```
QTECH(config)#vrrp ping-enable
```

19.1.4 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 0

【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 0.

【Example】

！Configure preemption and delay time of backup group.

```
QTECH(config-if-vlanInterface-1)#vrrp preempt 1 delay 3
```

19.1.5 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 100.

【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 0 to 255 (the larger the value is, the superior the priority is). The configured priority is from 1 to 254. Priority 0 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 200

```
QTECH(config-if-vlanInterface-1)#vrrp priority 1 200
```

19.1.6 **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.

```
QTECH(config-if-vlanInterface-1)#vrrp timer 1 1
```

Chapter 20 Switch Manage and Maintenance Command

20.1 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**

20.1.1 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

```
QTECH#buildrun mode continue
```

20.1.2 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.

```
QTECH#buildrun mode stop
```

20.1.3 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

```
QTECH#clear startup-config
```

20.1.4 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

```
QTECH#copy nm-interface-config startup-config
```

！Save configuration of VLAN interface 2

```
QTECH#copy nm-interface-config startup-config 2
```

！Save configuration of user-defined interface

```
QTECH#copy nm-interface-config startup-config 2 192.168.0.100
255.255.255.0 192.168.0.1
```

20.1.5 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

```
QTECH#copy running-config startup-config
```

20.1.6 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

```
QTECH#copy startup-config running-config
```

20.1.7 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

```
QTECH#show running-config
```

！Display configuration of GARP and OAM module

```
QTECH#show running-config garp oam
```

20.1.8 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

```
QTECH#show running-config
```

！Display saved configuration of GARP and OAM module

```
QTECH#show running-config garp oam
```

20.2 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

20.2.1 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 192.168.0.100 by FTP

```
QTECH#load application ftp 192.168.0.100 app.arj username password
```

20.2.2 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 192.168.0.100 by TFTP

```
QTECH#load application tftp 192.168.0.100 app.arj
```

20.2.3 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

QTECH#load application xmodem
```

20.2.4 **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 192.168.0.100 by FTP

```
QTECH#load configuration ftp 192.168.0.100 abc username password
```

20.2.5 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 192.168.0.100 by TFTP

```
QTECH#load configuration ftp 192.168.0.100 abc
```

20.2.6 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

QTECH#load configuration xmodem

20.2.7 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 192.168.0.100 by FTP

```
QTECH#load whole-bootrom ftp 192.168.0.100 abc username password
```

20.2.8 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 192.168.0.100 by TFTP

```
QTECH#load whole-bootrom tftp 192.168.0.100 abc username password
```

20.2.9 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

```
QTECH#load whole-bootrom xmodem
```

20.2.10 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 192.168.0.100 by FTP and saved as abc

```
QTECH#upload alarm ftp 192.168.0.100 abc username password
```

20.2.11 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 192.168.0.100 by TFTP and saved as abc

20.2.12 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 192.168.0.100 by FTP and saved as abc

```
QTECH#upload configuration ftp 192.168.0.100 abc username password
```

20.2.13 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 192.168.0.100 by TFTP and saved as abc

QTECH#upload configuration tftp 192.168.0.100 abc

20.2.14 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 192.168.0.100 by FTP and saved as abc

```
QTECH#upload logging ftp 192.168.0.100 abc username password
```

20.2.15 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 192.168.0.100 by TFTP and saved as abc

```
QTECH#upload logging tftp 192.168.0.100 abc
```

20.3 Reboot Switch

Reboot switch command includes:

- reboot

20.3.1 **reboot**

Use **reboot** command to reboot switch.

reboot

【Command configuration mode】

Privileged mode

【Example】

！Reboot switch

```
QTECH#reboot
```

20.4 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**

20.4.1 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 200000 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 5000 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 300 messages per second.

QTECH(config)#broadcast-suppression 300

！Non broadcast suppression

QTECH(config)#no broadcast-suppression

20.4.2 clock set

Use **clock set** command to configure system clock.

clock set

【Parameter】

HH:MM:SS：current time，HH ranges from 0 to 23，MM and SS range from 0 to 59

YYYY/MM/DD：Means current year, month, and date. YYYY ranges from 2000 to 2099，MM ranges from 1 to 12，and DD ranges from 1 to 31

【Default】

The default time is 2004/01/01 0:0:0

【Command configuration mode】

Privileged mode

【Usage】

Use this command to set current date and time when needing it.

【Example】

！Configure system clock to be 2001/01/01 0:0:0

```
QTECH#clock set 0:0:0 2001/01/01
```

【Related command】

show clock

20.4.3 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 0 to 59

【Default】

Beijing time（MCT），offset 3 hours

【Command configuration mode】

Global configuration mode

【Example】

！Configure the clock timezone to be Moscow time.

```
QTECH#clock timezone MCT 3 0
```

【Related command】

show clock

20.4.4 **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

```
QTECH(config)#discard-bpdu
```

20.4.5 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

```
QTECH(config)#no dlf-forward unicast
```

20.4.6 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

QTECH(config)#loopback external

20.4.7 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 500 totally.

【Command configuration mode】

Global configuration mode

【Example】

！Add mac address 00:01:02:03:04:05 to be permanent address table.

QTECH(config)#mac-address-table permanent 00:01:02:03:04:05 interface ethernet 0/1 vlan 1

20.4.8 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 1048575 seconds

disable：Means MAC address not aging.

【Default】

Default MAC address aging time is 300 seconds

【Command configuration mode】

Global configuration mode

【Example】

！Configure MAC address aging time to be 600 seconds

```
QTECH(config)#mac-address-table age-time 600
```

20.4.9 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.

```
QTECH(config)#mac-address-table learning
```

20.4.10 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 0 – 4095.

【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

```
QTECH(config-if-ethernet-0/0/3)#mac-address-table max-mac-count 8
```

20.4.11 **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 192.168.0.100. Test the connection of switch with the ip address of 192.168.0.200

```
QTECH#ping 192.168.0.200
```

20.4.12 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.

```
QTECH(config)#show broadcast-suppression
```

20.4.13 show clock

Use **show clock** command to display system clock.

show clock

【Command configuration mode】

Any configuration mode

【Example】

！Display system clock

```
QTECH#show clock
2001/01/01 00:00:00 MCT 3:00
```

【Related command】

clock set

20.4.14 show cpu

Use **show cpu** command to display cpu use rate. The smaller the rate is, the busier the CPU is.

show cpu

【Command configuration mode】

Any configuration mode

【Example】

！Display CPU busy rate

```
QTECH(config)#show cpu
```

20.4.15 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

```
QTECH(config)#show dhcp-server clients
```

20.4.16 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

```
QTECH(config)#show discard-bpdu
```

20.4.17 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.

QTECH(config)#show dlf-forward

20.4.18 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

QTECH(config)#show ip fdb

20.4.19 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

```
QTECH(config)#show mac-address-table
```

20.4.20 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.

```
QTECH(config)#show mac-address-table aging-time
```

20.4.21 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.

```
QTECH(config)#show mac-address-table learning
```

20.4.22 show memory

Use **show memory** command to display memory usage.

show memory

【Command configuration mode】

Any configuration mode

【Example】

！Display memory usage

```
QTECH(config)#show memory
```

20.4.23 show system

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

show system

【Command configuration mode】

Any configuration mode

【Example】

！Display system information

```
QTECH(config)#show system
```

20.4.24 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.

QTECH (config)#show users

20.4.25 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

```
QTECH# show version
```

20.4.26 login-access-list telnet-limit

Use this command to restrict the number of Telnet user (0-5) 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 (0～5)

【Default】

The max number is defaulted to be 5.

【Example】

！Configure only 1 Telnet user can enter privileged mode

```
QTECH(config)# login-access-list telnet-limit 1
```

【Related command】

show users

20.4.27 **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 30；

time_out：the overtime of waiting for the response which is in the range of 10 to 60 with the unit of second and default to be 10 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 192.168.0.200
QTECH#tracert 192.168.0.200
```

20.5 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**

20.5.1 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

```
QTECH(config)#show snmp community
```

20.5.2 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

```
QTECH(config)#show snmp contact
```

20.5.3 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

```
QTECH(config)#show snmp host
```

20.5.4 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

```
QTECH(config)#show snmp notify
```

20.5.5 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

```
QTECH(config)#show snmp location
```

20.5.6 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

```
QTECH(config)# show snmp engine id local
```

20.5.7 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

```
QTECH(config)# show snmp group
```

20.5.8 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

QTECH(config)# show snmp user

20.5.9 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

QTECH(config)# show snmp view

20.5.10 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 20 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 nic，and configure privilege to be ro，and permit

```
QTECH(config)#snmp-server community nic ro permit
```

！Remove community nic

```
QTECH(config)#no snmp-server community nic
```

20.5.11 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】

“QTECH” (http://www.qtech.ru)”

【Command configuration mode】

Global configuration mode

【Usage】

Use quotation mark to quote space in charater string.

【Example】

！Configure administrator contact way to be support@qtech.ru。

QTECH(config)#snmp-server contact support@qtech.ru

20.5.12 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 192.168.0.100，and SNMP version to be 2c，and community name to be user

```
QTECH(config)#snmp-server host 192.168.0.100 version 2c user
```

20.5.13 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。

```
QTECH(config)#snmp-server location “sample sysLocation factory”
```

20.5.14 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“QTECH S2926V-O”

【Command configuration mode】

Global configuration mode

【Usage】

Use quotation mark to quote space in charater string.

【Example】

！Configure system name to be QTECH S2926V-O

```
QTECH(config)#snmp-server name "QTECH S2926V-O"
```

20.5.15 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

```
QTECH(config)# snmp-server enable traps gbn
```

20.5.16 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 4094。

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

```
QTECH(config)# snmp-server trap-source vlan-interface 1
```

20.5.17 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 1346400000000000000000

【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

```
QTECH(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

```
QTECH(config)# snmp-server engineid remote 1.1.1.1 udp-port 888 1234
```

！Display local engine configuration

```
QTECH(config)# show snmp engineid local
```

20.5.18 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 0 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”

```
QTECH(config)# snmp-server view view1 1.3.6.1 include
```

！Add a subtree “1.3.6.2” for existed view “view1”

```
QTECH(config)# snmp-server view view1 1.3.6.2 include
```

！Remove existed view “view1”

```
QTECH(config)# no snmp-server view view1
```

20.5.19 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

```
QTECH(config)# snmp-server group group1 1 read internet write internet notify Internet
```

！Remove group “group1” from local facility

```
QTECH(config)# no snmp-server group group1 1
```

！Display current group configuration.

```
QTECH(config)# show snmp group
```

20.5.20 **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 "a20102b32123c45508f91232a4d47a5c"

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 "a20102b32123c45508f91232a4d47a5c"

Authkey is authentication key. Unauthenticated key is in the range of 16 byte (using md5 key folding) or 20 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.

```
QTECH(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

```
QTECH(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

```
QTECH(config)# snmp-server user user3 grp3 auth md5 auth-password 1234
priv des priv-password 4321
```

20.6 Manage IP Restriction Configuration

Manage IP restriction configuration includes:

- **login-access-list**
- **show login-access-list**

20.6.1 **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，0.0.0.0 means any ip address is allowed to manage system except 127.*.*.*

wildcard means mask wildcard which is in the form of mask in reverse. 0 means mask this bit, and 1 ,eams does not mask this bit. When mask in reserve is 0.0.0.0, it means host address, and 255.255.255.255 means all host.

【Command configuration mode】

Global cofiguration mode

【Usage】

Remove ip address 0.0.0.0 so that the configuration can be successful.

【Example】

！Configure ip address allowed by telnet management system to be

```
192.168.0.100

QTECH(config)#login-access-list telnet 192.168.0.100 0.0.0.0

QTECH(config)#no login-access-list telnet 0.0.0.0 255.255.255.255
```

20.6.2 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

```
QTECH(config)#show login-access-list
```

20.7 Telnet Client

Telnet client command includes:

- **telnet**
- **show telnet client**
- **stop telnet client**

20.7.1 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 10.9.2.34 from telnet client

```
QTECH#telnet 10.9.2.34
```

20.7.2 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.

```
QTECH#show telnet client
```

20.7.3 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 0-5，0 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

```
QTECH#stop telnet client 2
```

20.8 CPU Alarm Configuration Command

CPU alarm configuration command includes:

- **alarm cpu**
- **alarm cpu threshold**
- **show alarm cpu**

20.8.1 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

```
QTECH(config)#alarm cpu
```

20.8.2 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 0 to 100

unbusy: CPU unbusy threshold ranges from 0 to 100

【Default】

Default CPU busy threshold is 90，and CPU unbusy threshold is 60

【Command configuration mode】

Global configuration mode

【Usage】

busy > unbusy

【Example】

!Configure CPU busy threshold to be 50 ,and CPU unbusy threshold to be 30

```
QTECH(config)#alarm cpu threshold busy 50 unbusy 30
```

20.8.3 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

```
QTECH(config)#show alarm cpu
```

20.9 Mail Alarm Configuration

Mail alarm configuration includes:

- **mailalarm**
- **mailalarm server**
- **mailalarm receiver**
- **mailalarm ccaddr**

- **mailalarm smtp authentication**
- **mailalarm logging level**
- **show mailalarm**

20.9.1 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

QTECH(config)#mailalarm

20.9.2 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 0.

mailalarm server *server-addr*

no mailalarm server

【Parameter】

server-addr：IP address of smtp server

【Default】

Default server address is 0

【Command configuration mode】

Global configuration mode

【Example】

！Configure smtp server address to be 10.11.0.252

```
QTECH#mailalarm server 10.11.0.252
```

20.9.3 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

```
QTECH#mailalarm receiver system@switch.net
```

20.9.4 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

```
QTECH#mailalarm ccaddr system2@switch.net
```

20.9.5 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

```
QTECH#mailalarm smtp authentication username system passwd 123
```

20.9.6 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 0.

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 0

【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

```
QTECH#mailalarm logging level 4
```

20.9.7 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.

QTECH#show mailalarm

20.10　Anti-DOS Attack

- **anti-dos ip fragment**
- **show anti-dos**

20.10.1　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】

800

【Command configuration mode】

Global configuration mode

【Example】

！Configure maximum ip fragment message to be 30

QTECH(config)#anti-dos ip fragment 30

20.10.2 anti-dos ip ttl

Use this command to enable system to receive packey with TTL=0. Use **no** command to disable it.

【Default】

Disable

【Command configuration mode】

Global configuration mode

【Example】

！Enable system to receive packey with TTL=0.

```
QTECH(config)#anti-dos ip ttl
```

20.10.3 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

```
QTECH(config)#show anti-dos
```

Chapter 21　LLDP Configuration Command

21.1　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>]

21.1.1　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

QTECH(config)#lldp

21.1.2 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 30 seconds

【Command configuration mode】

Global configuration mode

【Example】

！Configure LLDP hello-time to be 20 seconds

```
QTECH(config)#lldp hello-time 20
```

21.1.3 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 <*2-10*>
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

```
QTECH(config)#lldp hold-time 2
```

21.1.4 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 0/0/1 only to send LLDP message

```
QTECH(config-if-ethernet-0/0/1)#lldp tx
```

21.1.5 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 0/0/1

```
QTECH(config)#show lldp interface ethernet 0/0/1
```