QTECH QSW-2900 Ethernet 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**
- **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-2900，the hostname in global configuration mode is QSW-2900(config)#.

【Example】

！Configure hostname to be SWITCH-A

QTECH(config)#hostname SWITCH-A

SWITCH-A (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 **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

1.1.10 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

1.1.11 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

1.1.12 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 “red”

QTECH(config)#show username red

1.1.13 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 “red” to disconnect with telnet

QTECH#stop red

1.1.14 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
```

1.1.15 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 "red"， configure privilege to be 15，and password to be 123456

QTECH(config)#username red privilege 15 password 0 123456

！Modify the privilege of administrator "red" to be 1，and password to be 1234

QTECH(config)#username red privilege 1 password 0 1234

1.1.16 **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 “red” to be 123456

QTECH(config)#username change-password

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

please input username :red

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

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

chang user red password success.

Chapter 2 Port Configuration Command

2.1 Ethernet Interface Configuration Command

Ethernet interface configuration command includes:

- **clear interface**
- **description**
- **duplex**
- **flow-control**
- **ingress acceptable-frame**
- **link-aggregation**
- **priority**
- **show description**
- **show interface**
- **show statistics interface**
- **shutdown**
- **speed**
- **switchport access**
- **switchport mode**
- **switchport trunk allowed vlan**
- **switchport trunk native vlan**
- **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 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 “red” for the Ethernet 0/0/3

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

！Clear description of Ethernet 0/0/3

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

【Related command】

show description

2.1.3 **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

2.1.4 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

2.1.5 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
```

2.1.6 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
```

2.1.7 **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

2.1.8 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

2.1.9 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

2.1.10 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

2.1.11 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

2.1.12 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

2.1.13 bandwidth-control

Use **bandwidth-control** command to control the egress and ingress bandwidth and limit the total rate of receiving and sending messages. Use **no bandwidth-control** command to cancel ingress and egress bandwidth-control configuration.

bandwidth-control { ingress | egress } *target-rate*
no bandwidth-control { ingress | egress }

【Parameter】

target-rate：The total rate of bandwidth-control ranges from 64 to 1024000 Kbps

【Command configuration mode】

Interface configuration mode

【Usage】

Use this command to restrict the ingress and egress bandwidth-control.

【Example】

！Configure the bandwidth-control of ethernet to be 10Mbps

QTECH(config-if-fastEthernet-1)# bandwidth-control ingress 10240

2.1.14 **show bandwidth-control**

Use this command to display bandwidth control of all interfaces.

show bandwidth-control

【Command configuration mode】

Any mode

【Usage】

Use this command to restrict the ingress and egress bandwidth-control.

【Example】

QTECH(config)#show bandwidth-control

2.1.15 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

2.1.16 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
```

2.1.17 **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

2.1.18 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

2.1.19 **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

2.1.20 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

2.1.21 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

2.2 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

Information about mirror port(s)

The monitor port : e0/1

The mirrored egress ports : e0/2

The mirrored ingress ports : e0/2

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

Port CAR global status : : enable

Port recover time(second): : 480

Port CAR rate(packet/second): : 300

Port CAR enable port :

e0/1,e0/2,e0/3,e0/4,e0/5,e0/6,e0/7,e0/8,e1/1.

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

e0/1 port alarm information

Port alarm status : enable

Port alarm exceed threshold(Mbps) : 85

Port alarm normal threshold(Mbps) : 60

Total entries: 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 mode**
- **dtag insert**
- **dtag passth-rough**
- **vlan-swap**
- **show dtag**
- **show vlan-swap**

3.3.1 **dtag**

Use this command to configure global QinQ.

dtag { *[flexible-qinq]* | outer-tpid *tpid* }

no dtag

【Parameter】

dtag：This is defaulted static qinq mode and it cannot be configured to ignore tag head of ingress packet. If vlan protocol number is not the same as the port configuration value or the port is configured to ignore tag head， there will be a new tag head between the 12th and 13th bit

flexible-qinq：Configure port vlan protocol number not the ignorance attribution of the ingress port. Only when vlan protocol number of ingress packet is not the same as the port configuration value and not the default value 8100, a new tag head will be added. If egress is TAG，TPID of TAG head is configured TPID.

outer-tpid tpid: vlan protocol number， the default value is 8100.

【Command configuration mode】

Global configuration mode

【Example】

Configure TPID of QinQ globally to be 9100

QTECH(config)dtag outer-tpid 9100

3.3.2 dtag mode

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

dtag mode { *customer* | *uplink* }

no dtag mode

【Parameter】

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

uplink: In this mode, when the vlan protocol number of ingress packet is different from the configured parameter of the interface and not the default value 8100, a new tag head will be added.

【Command configuration mode】

Interface configuration mode

【Example】

Configure interface to be customer interface.

QTECH(config-if-ethernet-0/1)#dtag mode customer

3.3.3 dtag insert

Use this command to configure the vlan tag head added in global QinQ.

dtag insert [start vlan of the series vlan] [end vlan of the series vlan] [destination vlan]

no dtag insert [start vlan of the series vlan] [end vlan of the series vlan]

【Parameter】

start vlan of the series vlan: all vlan tag packets between start vlan will add a destination vlan tag head.

destination vlan: tag vlan needed to insert a new tag head. After inserting it,transmit with the new tag vlan.

【Command configuration mode】

Global configuration mode

【Example】

Configure vlan from vlan1 to vlan2 are adding new tag with tag vlan being vlan3

QTECH(config)dtag insert vlan1 vlan2 vlan3

3.3.4 dtag pass-through

Use this command to configure transparent transmission of dynamic QinQ.

dtag pass-through [start vlan of the series vlan] [end vlan of the series vlan]

no dtag pass-through [start vlan of the series vlan] [end vlan of the series vlan]

【Parameter】

start vlan of the series vlan: dynamic QinQ enabling, the tag packet which can be transparent transmission without adding new tag head. The vlan is all vlans between the start vlan.

【Command configuration mode】

Global configuration mode

【Example】

Configure all vlans to be transparent transmission from vlan1 to vlan2

QTECH(config)dtag pass-through vlan1 vlan2

3.3.5 **rewrite-outer-vlan**

Use this command to configure interface outer vlan rewrite.

rewrite-outer-vlan *start-inner-vid end-inner-vid* [**outer-vlan** *outer-vid*]

new-outer-vlan *new-outer-vid*

no rewrite-outer-vlan *start-inner-vid end-inner-vid* [**outer-vlan** *outer-vid*]

【Parameter】

start-inner-vid : start inner vlan ID

end-inner-vid : end inner vlan ID.

outer-vid : outer vlan ID.

new-outer-vid : new outer vlan ID.

【Command configuration mode】

Interface configuration mode

【Example】

Configure interface outer vlan rewrite of e0/1 with inner vlan ID being the range of

1~50，outer vlan ID being 3 and new outer vlan ID being 100

QTECH(config-if-ethernet-0/1)#rewrite-outer-vlan 1 50 outer-vlan 3

new-outer-vlan 100

3.3.6 **vlan-swap**

Configure global vlan swap.

vlan-swap

no vlan-swap

vlan-swap [source vlanID] [switching vlan ID]

【Parameter】

source vlanID：the vlan ID to be replaces in tag.

switching vlan ID: the vlan used for replacing original vlan ID.

【Command configuration mode】

Global configuration mode

【Example】

Replace vlan2 to vlan1 in tag

QTECH(config)#vlan-swap vlan1 vlan2

3.3.7 **show dtag**

Display the QinQ configurationof the switch.

show dtag

show dtag insert

show dtag pass-through

【Command configuration mode】

Global configuration mode

【Example】

!Display the QinQ configuration

QTECH(config)#show dtag

Display insert vlan of current QinQ

QTECH(config)#show dtag insert

Display transparent transmission vlan of current QinQ

QTECH(config)#show dtag pass-through

3.3.8 show rewrite-outer-vlan

Use this command to display rewrite-outer-vlan

show rewrite-outer-vlan

【Command configuration mode】

Global configuration mode

【Example】

Display rewrite-outer-vlan

QTECH(config)#show rewrite-outer-vlan

3.3.9 show vlan-swap

Display vlan-swap of current switch.

show vlan-swap

【Command configuration mode】

Global configuration mode

【Example】

!Display vlan-swap of current switch

```
QTECH(config)#show vlan-swap
```

Chapter 4 Multicast Protocol Configuration Command

4.1 Static Multicast Configuration Command

Static multicast configuration command includes:

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

4.1.1 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

4.1.2 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

4.1.3 **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

show multicast table information

MAC Address : 01:00:5e:01:02:03

VLAN ID : 3

Static port list : e0/2,e0/3.

IGMP port list

Dynamic port list

Total entries: 1.

4.2 IGMP snooping and GMRP Configuration Command

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**
- **show gmrp**
- **show gmrp interface**
- **show igmp-snooping**

4.2.1 **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

4.2.2 **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

4.2.3 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

4.2.4 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

4.2.5 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

4.2.6 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

4.2.7 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

4.2.8 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

4.2.9 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

4.2.10 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 2/1

port GMRP status

e0/1 enable

e0/2 enable

e0/3 enable

e2/1 enable

Total entries: 4

4.2.11 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

4.2.12 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

4.2.13 **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

4.2.14 **igmp-snooping route-port vlan** *vlanID* **interface** interface-list

Added route port demonstrates the transferred port of leave or report packet of the host in the same multicast.

igmp-snooping route-port vlan *vlanID* interface *port-number*

no igmp-snooping route-port vlan *vlanID* interface *port-number*

【Parameter】

vlanID：ID of existed vlan （between 1～4094）

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. Not all port can be configured to be descendent isolation port.

all：Means all port. Choose “all” to remove descendent isolation port.

【Command configuration mode】

Any configuration mode

【Example】

Configure e0/0/1 of vlan 2 to be route port of current group（determined by source IP of querier）

igmp-snooping route-port vlan *2* interface ethernet 0/1

4.2.15 **no igmp-snooping router-port-age**

Configure the aging of route port. It is defaulted to be aging.

no igmp-snooping router-port-age

igmp-snooping router-port-age

【Command configuration mode】

Any configuration mode

【Usage】

It is defaulted to be aging, so uses no igmp-snooping router-port-age command to disable it.

【Example】

Configure the route port aging

no igmp-snooping router-port-age

4.2.16 **igmp-snooping general-query source-ip** *ipaddress*

Configure IGMP query source IP to demonstrate the destination IP to response to. It is defaulted to be 0.0.0.0

igmp-snooping general-query source-ip *ipaddress*

no igmp-snooping general-query source-ip *ipaddress*

【Command configuration mode】

Any configuration mode

【Parameter】

ipaddress : ip address of ipv4

【Example】

! Configure IGMP query source IP to be 1.1.1.111

QTECH(config)# igmp-snooping general-query source-ip 1.1.1.111

4.2.17 **igmp-snooping query-max-respon** *seconds*

Configure the max response after receiving query, that is the response value in IGMP query. It is defaulted to be 10s.

igmp-snooping query-max-respon *second*

no igmp-snooping query-max-respon

【Command configuration mode】

Any configuration mode

【Parameter】

Seconds : 1 - 255 which is used for max response time of IGMP query packet.

【Example】

! Configure the max response after receiving query to be 150

QTECH(config)# igmp-snooping query-max-respon 150

4.2.18 **igmp-snooping querier-vlan** *vlanID*

Configure vlan which IGMP query sent by querier to be sent to. It is defaulted to be vlan 1.

igmp-snooping querier-vlan *vlanID*

no igmp-snooping querier-vlan

【Parameter】

vlanID：ID of existed vlan （between 1～4094）

【Command configuration mode】

Any configuration mode

【Example】

！Configure querier sending query to vlan 10

QTECH(config)# igmp-snooping querier-vlan 10

4.2.19 **igmp-snooping query-interval** *seconds*

Configure interval of sending IGMP query. It is defaulted to be 60s.

igmp-snooping query-interval *seconds*

no igmp-snooping query-interval

【Command configuration mode】

Any configuration mode

【Parameter】

Seconds：1 - 30000s

【Example】

！Configure interval of sending IGMP query to be 90s

QTECH(config)# igmp-snooping querier 90

4.2.20 igmp-snooping querier

Enable or disable querier sending IGMP query packet. It is defaulted not to send.

igmp-snooping querier

no igmp-snooping querier

【Command configuration mode】

Any configuration mode

【Example】

！Enable igmp-snooping querier

QTECH(config)# igmp-snooping querier

4.3 Cross-VLAN Multicast Configuration

Cross-VLAN Multicast Configuration includes:

- **cross-vlan multicast**
- **cross-vlan multicast** [tag vlan *vlanid*| untag]
- **cross-vlan multicast**

!Caution：only in MAC address learning mode of SVL for layer 3 packet, the multicast can be correct.

4.3.1 **cross-vlan multicast**

Use this command to enable Cross-VLAN multicast.

cross-vlan multicast

no cross-vlan multicast

【Parameter】

Non

【Command configuration mode】

Globally configuration mode

【Usage】

Non

【Example】

! enable Cross-VLAN multicast

QTECH(config)#cross-vlan multicast

4.3.2 cross-vlan multicast

Use this command to configure tag/untag attribution of interface transmitting multicast and vlan id of tagged interface.

cross-vlan multicast [tag vlan *vlanid*| untag]

【Parameter】

tag/untag：configure tag/untag attribution of interface transmitting multicast which has nothing to do with 802.1Q configuration

vlan-id：configure vlan id of tagged interface which has nothing to do with 802.1Q configuration

【Command configuration mode】

Interface configuration mode

【Example】

! Configure interface 3 to add tag head when transmitting multicast packet and vlanid to be 5

QTECH(config-if-ethernet-0/5)#cross-vlan multicast tag vlan 5

4.3.3 show cross-vlan multicast

Use this command to display cross vlan configuration and specified interface configuration.

show cross-vlan multicast [interface]

【Parameter】

interface：specified interface

【Command configuration mode】

Any configuration mode

【Usage】

If interface is not specified, display cross vlan globally.

【Example】

！Display configuration of cross vlan multicast of e0/1

QTECH(config)#show cross-vlan multicast interface ethernet 0/1

cross-vlan multicast : enabled.

port tag vlanid

0/1 false 0

Total [1] item(s), printed [1] item(s).

Chapter 5 ACL Configuration Command

5.1 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**
- **show access-list config**
- **show access-list config statistic**
- **show access-list runtime all**
- **show access-list runtime statistic**
- **show time-range**
- **time-range**

5.1.1 **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

5.1.2 access-group

Use **access-group** command to activate accessing control list. Use **no access-group** command to cancel activate.

access-group { **user-group** { *access-list-number* | *access-list-name* } [**subitem** *subitem*] | { [**ip-group** { *access-list-number* | *access-list-name* } [**subitem** *subitem*]] [**link-group** { *access-list-number* | *access-list-name* } [**subitem** *subitem*]] } }

no access-group { **all** | **user-group** { *access-list-number* | *access-list-name* }
[**subitem** *subitem*] | { [**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.

【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

5.1.3 access-list

Use **access-list** command to configure a ACL with number ID, which can be: standard ACL, extended ACL, Layer 2 ACL and user-defined ACL. Use **no access-list** command to delete all the subitems or one subitem in one ACL with number ID or name ID or all ACLs.

1. Define standard ACL with number ID.

access-list *access-list-number1* { permit | deny } { *source-addr source-wildcard* | any } [**fragments**] [**time-range** *time-range-name*]

2. Define extended ACL with number ID.

access-list *access-list-number2* { permit | deny } [*protocol*] [established]

{ *source-addr source-wildcard* | any } [*port* [*portmask*]] { *dest-addr dest-wildcard* | any } [*port* [*portmask*]] [*icmp-type* [*icmp-code*] | *icmp-packet*] [fragments] { [**precedence** *precedence*] [**tos** tos] | [**dscp** *dscp*] } [**time-range** *time-range-name*]

3. Define Layer 2 ACL with number ID.

access-list *access-list-number3* { permit | deny } [*protocol*] [**cos** *vlan-pri*] **ingress** { { [*source-vlan-id*] [*source-mac-addr source-mac-wildcard*] [**interface** *interface-num*] } | any } **egress** { { [*dest-mac-addr dest-mac-wildcard*] [**interface** *interface-num* | **cpu**] } | any } [**time-range** *time-range-name*]

4. Define user-defined ACL with number ID.

access-list *access-list-number4* { permit | deny } { *rule-string rule-mask offset* }&<1-20> [**ingress interface** *interface-num*] [**egress interface** *interface-num* | **cpu**] [**time-range** *time-range-name*]

5. 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

access-list-number4：user-defined ACL rules in the range of 300～399

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

5.1.4 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

5.1.5 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

5.1.6 **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

5.1.7 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

5.1.8 access-list user

Use **access-list user** command to create a user-defined ACL with a name ID and enter user-defined ACL configuration mode. Use **no access-list user** command to delete one or all subitems of ACL with number ID or name ID or delete all ACL.

access-list user *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 user-defined ACL with the name of “name”. After entering the user-defined 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 user-defined ACL with the name to be example and specify the order to be deep precedency.

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

5.1.9 { **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*]

4. Add a subitem to user-defined ACL with the name ID.

{ **permit** | **deny** } { *rule-string rule-mask offset* }&<1-20> [**ingress interface** *interface-num*] [**egress interface** *interface-num* | **cpu**] [**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 5 configuration modes as: standard, extended, layer 2, interface, user-defined)

【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)#

5.1.10 **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

5.1.11 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
Standard IP Access List 10, 1 rule,
0 : permit 10.0.0.1 0 (0 times matched)
Standard IP Access List 20, 1 rule,
0 : permit 20.0.0.1 0 (0 times matched)
Standard IP Access List std1, 2 rules,
0 : permit 20.0.0.1 0 (0 times matched)
1 : permit 30.0.0.1 0 (0 times matched)
```

5.1.12 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
 access-list 1        : 1 rules
 access-list 2        : 2 rules
 access-list 10       : 1 rules
 access-list 11       : 1 rules
 access-list 12       : 1 rules
```

access-list 200 : 1 rules

access-list 202 : 2 rules

access-list 210 : 1 rules

total config rules : 10 rules

5.1.13 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. If ACL subitem has been delivered to hardware, the priority of ACL subitem will be diaplayed. Priority value is from 2 to 13, and there are 5 blocks, interface 1-8 of which belong to block 0, interface 9-16 of which belong to block 1, interface 17-24 of which belong to block 2, interface 25 belongs to block 3 and interface 26 belongs to block 4. This command will display the priorities of flow statistics in 5 blocks. Such as the priority of the first 2 blocks is 3, and the priority of the latter 10 is 5, which will be displayed as 3,3,5,5,5,5,5,5,5,5,5. If flow statistics has only be issued to some block, the priority of the flow statistics in the current block is displayed, and priority in other block is shown as "/", such as if flow statistics is only be issued to block0, and its priority is 8，it will be

displayed as 8,/,/,/,/,/,/,/,/,/,/,/

【Example】

! Display runtime application of ACL of all interfaces.

QTECH#show access-list runtime all

access-list std1 subitem 0 running (2,2,2,2,2,2,2,2,2,2,2,2)

access-list std1 subitem 1 running (3,3,3,3,3,3,3,3,3,3,3,3)

5.1.14 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

access-list 1 access-list 200 : 1 rules

access-list 2 : 2 rules

access-list 202 : 2 rules

access-list 10 access-list 210 : 1 rules

access-list 11 access-list 210 : 1 rules

access-list 12 access-list 210 : 1 rules

total runtime rules : 8 rules

5.1.15 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

5.1.16 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 6 QOS Configuration Command

6.1 QoS Configuration Command

QoS configuration command includes:

- **queue-scheduler**
- **queue-scheduler cos-map**
- **show queue-scheduler**
- **show queue-scheduler cos-map**

6.1.1 **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 1，3，6，9

QTECH(config)#queue-scheduler wrr 1 3 6 9

6.1.2 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

6.1.3 **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

6.1.4 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

6.1.5 **port-isolation**

Use **port-isolation** command to add a or a group of descendent isolation port. Use **no port-isolation** command to remove a or a group of descendent isolation port.

port-isolation { *interface-list* }

no port-isolation { *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(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. Not all port can be configured to be descendent isolation port.

all：Means all port. Choose “all” to remove descendent isolation port.

【Command configuration mode】

Global configuration mode

【Example】

！Add Ethernet 0/1, Ethernet 0/3, Ethernet 0/4, Ethernet 0/5, Ethernet 0/8 to be descendentisolation port.

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

！Remove ethernet 0/3, Ethernet 0/4, Ethernet 0/5, ethernet 0/8 from downlink isolation port.

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

6.1.6 **show port-isolation**

Use show port-isolation command to display port-isolation information.

show port-isolation

【Command configuration mode】

Any configuration mode

【Example】

！Display port-isolation information

QTECH(config)#show port-isolation

6.1.7 **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 1Mbps，and enable broadcast strom-control

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

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

Chapter 7 STP Configuration Command

7.1 STP Configuration Command

STP (Spanning Tree protocol) configuration command includes:

- **show spanning-tree 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**

7.1.1 **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 0/7

7.1.2 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 0/8

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

7.1.3 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 0/8 to 20

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

7.1.4 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

7.1.5 **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

7.1.6 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

7.1.7 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 0/1 in STP to 64

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

7.1.8 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 0/7 to send RSTP message

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

7.1.9 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 0/7 as a point-to-point link

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

7.1.10 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 0/7 as a non-edge port.

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

7.1.11 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 0/7 in each Hello time to 5

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

7.1.12 **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.

【举例】

！Configure the priority of the switch in spanning tree to 4096

QTECH(config)#spanning-tree priority 4096

7.1.13 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

7.1.14 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 0/1, and ethernet 0/3

QTECH(config)#spanning-tree remote-loop-detect interface ethernet 0/1 ethernet 0/3

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

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

7.1.15 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

7.2 MSTP Configuration command

MSTP（Multiple spanning Tree protocol）Configuration command include：

- 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

Refer to corresponded commands of SST：

spanning-tree forward-time；

spanning-tree hello-time；

spanning-tree max-age；

spanning-tree portfast；

spanning-tree point-to-point

7.2.1 spanning-tree mst max-hops

Use this command to configure max hop of MSTP packet.

spanning-tree mst max-hops *max-hops*

no spanning-tree mst max-hops

【Parameter】

max-hops：hops of MSTP packet which is in the range of 0-255.

【Default】

It is defaulted to be 20

【Command configuration mode】

Global configuration mode

【Example】

！Configure the max hop of MSTP packet to be 10

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

7.2.2 spanning-tree mst name

Use this command to configure name of MSTP configuring mark.

spanning-tree mst name *name*

no spanning-tree mst name

【Parameter】

name：region name of MSTP which is a part of MSTP configuring mark is acharacter string of 32 bits.

【Default】

It is defaulted to be none.

【Command configuration mode】

Global configuration mode

【Example】

！Configure MSTP name to be QTECH

QTECH(config)#spanning-tree mst name QTECH

7.2.3 **spanning-tree mst revision**

Use this command to configure 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

7.2.4 **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

7.2.5 **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

7.2.6 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

7.2.7 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

7.2.8 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

7.2.9 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

7.2.10 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

7.2.11 spanning-tree mst config-digest-snooping

Use this command to enable digest snooping to realize the interconnection with Cisco private MSTP protocol. Use the no command to disable this function.

spanning-tree mst config-digest-snooping

no spanning-tree mst config-digest-snooping

【Default】

Disable

【Command configuration mode】

Interface configuration mode

【Example】

! Enable digest snooping of e0/0/1

QTECH(config-if-ethernet-0/1)#spanning-tree mst config-digest-snooping

Chapter 8 802.1X Configuration Command

8.1 Domain Configuration Command

Domainn configuration command includes:

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

8.1.1 **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)#

8.1.2 **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 red.com to 500

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

8.1.3 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 red.com and enable the default domain

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

！Disable default domain name

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

【Related command】

domain

8.1.4 **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 red.com

QTECH(config-aaa)#domain red.com

QTECH(config-aaa-red.com)#

！Remove domain with the name of red.com

QTECH(config-aaa)#no domain red.com

【Related command】

radius host, state

8.1.5 **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 red.com

QTECH(config-aaa-red.com)#show domain

8.1.6 **radius host**

Use **radius host** command to configure RADIUS authtication and accounting.

radius host 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 “red”

QTECH(config-aaa-red.com)#radius host red

【Related command】

radius host（RADIUS configuration mode）

8.1.7 **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 red.com

QTECH(config-aaa-red.com)#state active

【Related command】

domain

8.2 RADIUS Server Configuration Command

RADIUS server configuration command includes:

- client-ip
- primary-ip
- radius host

- realtime-account
- second-ip
- secret-key
- show radius host
- username-format

8.2.1 client-ip

Use this command to configure client ip of current RADIUS server. Use the no command to remove the client ip.

client-ip *client-ip*

no client-ip

【Parameter】

client-ip：client IP address

【Default】

It is defaulted to be 0.

【Command configuration mode】

RADIUS configuration mode

【Example】

! Configure RADIUS client IP address to be 192.168.0.100

QTECH(config-aaa-radius-red)#client-ip 192.168.0.100

! Remove RADIUS client IP address

QTECH(config-aaa-radius-red)#no client-ip

【Related command】

radius host

8.2.2 **primary-ip**

Use this command to configure primary IP address, authentication port and accounting port of current RADIUS server. Use the **no** command to remove the primary IP address.

primary-ip server-ip authentication-port accounting-port

no primary-ip

【Parameter】

server-ip：primary IP address of RADIUS server

authentication-port：authentication port which is in the range of 1～65535

accounting-port：accounting port which is in the range of 1～65535

【Default】

The default authentication port is 1812 and accounting port is 1813.

【Command configuration mode】

RADIUS configuration mode

【Example】

！Configure primary IP address of RADIUS server to be 192.168.0.100，

authentication port to be 1812 and accounting port to be 1813

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

！Remove primary IP address of RADIUS server

QTECH(config-aaa-radius-red)#no primary-ip

【Related command】

radius host，second-ip

8.2.3 radius host

Use radius host command to create or choose a RADIUS server for current domain. If RADIUS server exists, enter it. Use the **no** command to remove RADIUS server specified by radius-scheme.

radius host radius-scheme

no radius radius-scheme

【Parameter】

radius-scheme :RADIUS server name which is in the range of 1 ~ 32 characters of any form excluding space.

【Command configuration mode】

AAA mode

【Example】

！Create and enter new RADIUS server myScheme

QTECH(config-aaa)#radius host myScheme

QTECH(config-aaa-radius-myScheme)#

【Related command】

radius host

8.2.4 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-red)#realtime-account interval 30

！Disable the real-time accounting

QTECH(config-aaa-radius-red)#no realtime-account

8.2.5 **second-ip**

Use this command to configure second IP address, authentication port and accounting port of RADIUS server. Use the **no** command to remove the seconf IP address.

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

no second-ip

【Parameter】

server-ip：second IP address of RADIUS server

authentication-port：authentication port which is in the range of 1～65535

accounting-port：accounting port which is in the range of 1～65535

【Default】

By default, the authentication port is 1812 and accounting port is 1813.

【Command configuration mode】

RADIUS configuration mode

【Example】

！Configure the second IP address of RADIUS server red to be 192.168.0.200，

authentication port to be 1812 and accounting port to be 1813

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

！Remove the seconf IP address of RADIUS server red

QTECH(config-aaa-radius-red)#no second-ip

【Related command】

radius host，primary-ip

8.2.6 **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 red to be 12345

QTECH(config-aaa-radius-red)#secret-key 12345

【Related command】

radius host

8.2.7 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

8.2.8 **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 red not to carry domain name.

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

【Related command】

radius host

8.3 802.1X Configuration Command

802.1X 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

8.3.1 **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

8.3.2 **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

8.3.3 **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

8.3.4 **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

8.3.5 **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 10

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

QTECH(config)#dot1x max-user 10 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

8.3.6 **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

8.3.7 **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

8.3.8 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

8.3.9 **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

8.3.10 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.com

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

8.3.11 **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

8.3.12 **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

8.3.13 **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

8.3.14 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 9 SNTP Client Configuration Command

9.1 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**

9.1.1 **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

9.1.2 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

9.1.3 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

9.1.4 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

9.1.5 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

9.1.6 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

9.1.7 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

9.1.8 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

9.1.9 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

9.1.10 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

9.1.11 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

9.1.12 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

9.1.13 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 10 Syslog Configiration Command

10.1 Syslog Configuration Command

Syslog configuration command includes:

- **show logging**
- **show logging buffered**
- **show logging flash**
- **show logging filter**
- **show debug**
- **logging on**
- **logging sequence-numbers**
- **logging timestamps**
- **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**

10.1.1 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

10.1.2 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

10.1.3 **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

10.1.4 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

10.1.5 **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

10.1.6 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

10.1.7 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

10.1.8 logging timestamps

se **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

10.1.9 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

【Paramter】

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

10.1.10 terminal monitor

Use **terminal monitor** command to enable current terminal information displaying.

Use **no terminal monitor** command to disable current terminal information displaying.

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

10.1.11 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

10.1.12 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

10.1.13 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

10.1.14 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

10.1.15 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

10.1.16 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

10.1.17 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

10.1.18 **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 filtrate rule to be permitting the information outputting of 0 to 3 levels of all modules of SNMP Agent

QTECH(config)#logging snmp-agent 3

【Related command】

snmp-server host

10.1.19 **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

10.1.20 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 11 SSH Configuration Command

11.1 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**

11.1.1 **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

11.1.2 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

11.1.3 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

11.1.4 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

11.1.5 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

11.1.6 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

11.1.7 **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

11.1.8 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 12 Switch Manage and Maintenance Command

12.1 Configuration Files Management

Configuration files management includes:

- **buildrun mode continue**
- **buildrun mode stop**
- **clear startup-config**
- **copy running-config startup-config**
- **copy startup-config running-config**
- **show running-config**
- **show startup-config**

12.1.1 buildrun mode continue

Use **buildrun mode continue** command to configure buildrun mode to be continune.

buildrun mode continue

【acaommand configuration mode】

Privileged mode

【Example】

！Configure buildrun mode to be continune

QTECH#buildrun mode continue

12.1.2 **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

12.1.3 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

12.1.4 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

12.1.5 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

12.1.6 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

12.1.7 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

12.2 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

12.2.1 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

12.2.2 **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

12.2.3 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

12.2.4 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

12.2.5 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

12.2.6 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

12.2.7 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

12.2.8 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

12.2.9 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

12.2.10 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

12.2.11 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

12.2.12 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

12.2.13 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

12.2.14 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

12.2.15 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

12.3 Reboot Switch

Reboot switch command includes:

- reboot

12.3.1 **reboot**

Use **reboot** command to reboot switch.

reboot

【Command configuration mode】

Privileged mode

【Example】

！Reboot switch

QTECH#reboot

12.4 Basic Configuration and Maintenance

Basic configuration and mainenance includes:

- **bootp**
- **broadcast-suppression**
- **clock set**
- **dhcp**

- **discard-bpdu**
- **dlf-forward**
- **ipaddress**
- **ipaddress vlan**
- **loopback**
- **mac-address-table**
- **mac-address-table aging-time**
- **mac-address-table learning**
- **ping**
- **show broadcast-suppression**
- **show clock**
- **show cpu**
- **show discard-bpdu**
- show dlf-forward
- show ip
- **show mac-address-table**
- **show mac-address-table aging-time**
- **show mac-address-table learning**
- **show memory**
- **show system**
- **show users**
- **show version**

12.4.1 **bootp**

Use **bootp** command to enable bootp way to obtaining ip address. Use **no bootp** command to disable bootp.

bootp

no bootp

【Default】

BOOTP disables

【Usage】

The way to obtain IP address are by BOOTP、DHCP、and manual operation. If BOOTP enables, the switch will obtainn the ip address by bootp, and DHCP or manual operation will be error. If DHCP is wanted, input no bootp first，then input dhcp。

【Command configuration mode】

Global configuration mode

【Example】

！Enable BOOTP to obtainn IP address

QTECH(config)#bootp

12.4.2 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

12.4.3 dhcp

Use **dhcp** command to configure to enable DHCP to obtain IP address. Use **no dhcp** command to disable DHCP to obtain IP address.

dhcp

no dhcp

【Default】

Not to obtain ip address by DHCP

【Command configuration mode】

Global configuration mode

【Usage】

The way to obtain IP address are by BOOTP、DHCP、and manual operation. If dhcp enables, the switch will obtainn the ip address by dhcp, and bootp or manual operation will be error. If bootp is wanted, input no dhcp first，then input bootp.

【Example】

！Enable DHCP to obtainn IP address

QTECH(config)#dhcp

12.4.4 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

12.4.5 **ipaddress**

Use **ipaddress** command to configuration ip address, netmask, and gateway by manual operation.

ipaddress ip-address mask [gateway]

【Parameter】

ip-address：System ip address

mask：Netmask

gateway：If only IP address and netmask are configured, and gateway is not, the gateway will be default to be 0

【Default】

Not to obtain ip address by DHCP、BOOTP.

【Command configuration mode】

Global configuration mode

【Usage】

The way to obtain IP address are by BOOTP、DHCP、and manual operation. If dhcp or bootp enables, the switch will obtainn the ip address by dhcp or bootp, and manual operation will be error. If manual operation is wanted, input **no dhcp** or **no bootp** first.

【Example】

！Original way to obtain IP address is by DHCP. Change IP address by manual operation to be 192.168.0.100

QTECH(config)#no dhcp

QTECH(config)#ipaddress 192.168.0.100 255.255.0.0

12.4.6 ipaddress vlan

Use **ipaddress vlan** command to configure and manage VLAN.

ipaddress vlan *vlan-id*

no ipaddress vlan *vlan-id*

【Parameter】

vlan-id，ranges from 1to 4094. It must be existed VLAN.

【Default】

VLAN 1 is default to be included in manage VLAN

【Command configuration mode】

Global configuration mode

【Usage】

At most 26 manage VLANs can be configured.

【Example】

QTECH(config)#ipaddress vlan 2

12.4.7 **loopback**

Use **loopback** command to loopback. External and internal can be chosed in global confuration or interface configurationmode.

loopback { external | internal }

【Parameter】

external：External loopback

internal：Internal loopback

【Command configuration mode】

Global configuration mode, interface configuration mode

【Example】

！Loopback on all interfaces

QTECH(config)#loopback external

12.4.8 **vct run**

Use **vct run** command to port vct test. Vct test for all the ports in global configuration mode. Vct test for current port in interface configuration mode.

vct run

【Command configuration mode】

Global configuration mode, interface configuration mode

【Example】

! Vct run for all ports

QTECH(config)#vct run

12.4.9 vct auto-run

Use **vct auto-run** command to enable vct auto-run globally or on a port. Use **no vct auto-run** command to disable vct auto-run globally or on a port.

vct auto-run

no vct auto-run

【Default】

vct auto-run disables globally or on a port

【Command configuration mode】

Global configuration mode，Interface configuration mode

【Example】

！Enable VCT auto-run globally

QTECH(config)#vct auto-run

！Enable VCT auto-run on Ethernet 0/8

QTECH(config-if-ethernet-0/8)#vct auto-run

12.4.10 **show vct auto-run**

Use **show vct auto-run** command to display vct auto-run.

show vct auto-run

【Command configuration mode】

Any configuration mode

【Example】

! Display vct auto-run.

QTECH(config)#show vct auto-run

12.4.11 mac-address-table

Use **mac-address-table** command to add mac address table. Use **no**

mac-address-table command to remove mac address table.

mac-address-table { dynamic | permanent | static } *mac* **interface** *interface-num* **vlan** *vlan-id*

mac-address-table blackhole *mac* vlan *vlan-id*

no mac-address-table [blackhole | dynamic | permanent | static] *mac* **vlan** *vlan-id*

no mac-address-table [dynamic | permanent | static] *mac* **interface** *interface-num* **vlan** *vlan-id*

no mac-address-table [dynamic | permanent | static] **interface** *interface-num*

no mac-address-table [blackhole | dynamic | permanent | static] **vlan** *vlan-id*

no mac-address-table

【Parameter】

mac：Unicast mac address

vlan-id：VLAN id

interface-num：Number of interface for message outputting

backhole：Blackhole address table which is not aging, and will not be lost after switch rebooting. Message whose source or destination mac address is the same as this mac address will be dropped.

dynamic：Dynamic address table which can be aging.

permanent：Permanent address table which cannot be aging and will not be lost after switch rebooting.

static：Static address table which is not aging and will be lost after switch reboot.

All blackhole/static/dynamic/permanent address can add 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

12.4.12 mac-address-table age-time

Use **mac-address-table age-time** command to configure MAC address aging time.

Use **no mac-address age-time** command to restore it to default time.

mac-address-table age-time [*agetime* | disable]

no mac-address age-time

【Parameter】

agetime：Means MAC address aging time which ranges from 1 to 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

12.4.13 mac-address-table learning

Use **mac-address-table learning** command to enable MAC address learning. Use **no mac-address-table learning** command to disable MAC address learning. When disabling, the message from a port whose source address is not in this port, will not be transmitted.

mac-address-table learning

no mac-address-table learning

【Command configuration mode】

Global configuration mode

【Example】

！Enable MAC address learning.

QTECH(config)#mac-address-table learning

12.4.14 mac-address-table learning mode

Use **mac-address-table learning mode** command to modify ways of MAC address learning. Ways of MAC address learning includes: SVL and IVL. SVL is shared VLAN learning; and IVL is independent VLAN learning. The default one is SVL.

This command cannot add to configuration files.

mac-address-table learning mode { svl | ivl }

show mac-address-table learning mode

【Command configuration mode】

Global configuration mode

【Example】

！Modify MAC address to be IVL

QTECH(config)#mac-address-table learning mode ivl

12.4.15 ping

Use **ping** command to check the network connection.

ping [**-c** count] [**-s** packetsize] [**-t** timeout] host

【Parameter】

count：The number of message sending.

packetsize：The length of message sending, with the unit of second

timeout：the time of waiting for replying after message is sent，with the unit of second

host：Host ip address

【Command configuration mode】

Any configuration mode

【Usage】

Use this command to test whether the facility in the same net is connected or not.

【Example】

！The ip address of current switch is 192.168.0.100. Test the connection of switch with the ip address of 192.168.0.200

QTECH#ping 192.168.0.200

12.4.16 **show broadcast-suppression**

Use **show broadcast-suppression** command to display the number of the broadcast

flow allowed by switch.

show broadcast-suppression

【Command configuration mode】

Any configuration mode

【Example】

！Display the max number of the broadcast flow allowed by switch per second.

QTECH(config)#show broadcast-suppression

12.4.17 **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 CCT 8:00

【Related command】

clock set

12.4.18 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

12.4.19 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

Status about dlf packets forwarding

Forwarding unknown multicast packets : enable

Forwarding unknown unicast packets : enable

12.4.20 **show ip**

Use **show ip** command to display ip address and its obtaining mode, netmask, and gateway.

show ip

【Command configuration mode】

Any configuration mode

【Example】

！Display ip address information

QTECH(config)#show ip

12.4.21 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 { 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

12.4.22 **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

12.4.23 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

12.4.24 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

12.4.25 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

12.4.26 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

12.4.27 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

12.4.28 **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 users can enter privileged mode

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

【Related command】

show users

12.4.29 **tracert**

Use this command 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】

Use this command to tracert the router and the time that switch reaches the destination.

【Example】

! The current IP address is 192.168.0.100 and tracert 192.168.0.200

QTECH#tracert 192.168.0.200

12.5 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**

12.5.1 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

12.5.2 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

12.5.3 **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

12.5.4 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

12.5.5 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

12.5.6 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

12.5.7 **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

12.5.8 **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

12.5.9 **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

12.5.10 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 red，and configure privilege to be ro，and permit

QTECH(config)#snmp-server community red ro permit

！Remove community red

QTECH(config)#no snmp-server community red

12.5.11 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 MOSCOW RUSSIA (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

12.5.12 **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

12.5.13 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”

12.5.14 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”

【Command configuration mode】

Global configuration mode

【Usage】

Use quotation mark to quote space in charater string.

【Example】

！Configure system name to be QTECH QSW-2900

QTECH(config)#snmp-server name "QTECH QSW-2900"

12.5.15 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

12.5.16 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

12.5.17 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 13464000000000000000000

【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

12.5.18 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
```

12.5.19 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

12.5.20 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

12.6 Manage IP Restriction Configuration

Manage IP restriction configuration includes:

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

12.6.1 **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

12.6.2 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

12.7 CPU Alarm Configuration Command

CPU alarm configuration command includes:

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

- **show alarm cpu**

12.7.1 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

12.7.2 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

12.7.3 **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

CPU status alarm : enable

CPU busy threshold(%) : 90

CPU unbusy threshold(%) : 60

CPU status : unbusy

12.8 Anti-DOS Attack

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

12.8.1 **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

12.8.2 **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 13 LLDP Configuration Command

13.1 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>]

13.1.1 **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

13.1.2 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*

13.1.3 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*

13.1.4 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 0/1 only to send LLDP message

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

13.1.5 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 0/1

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