QTECH
МИР ДОСТУПНЕЕ

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Security Configuration Commands

Оглавление

1.1. aaa accounting commands

Use this command to configure NAS command accounting. Use the **no** form of this command to restore the default setting.

aaa accounting commands *level* **{ default |** *list-name* **} start-stop** *method1* [*method2*…]

no aaa accounting commands *level* { **default |** *list-name* }

Parameter Description

Parameter	Description
level	The accounting command level, 0-15. The message shall be recorded before which command level is executed is determined.
default	When this parameter is used, the following defined method list is used as the default method for command accounting.
list-name	Name of the command accounting method list, which could be any character strings.
method	It must be one of the keywords listed in the following table. One method list can contain up to four methods.
none	Does not perform accounting.
group	Uses the server group for accounting, the TACACS+ server group is supported.

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

RGOS enables the accounting command function after enabling the login authentication. After enabling the accounting function, it sends the command information to the security service.

The configured accounting command method must be applied to the terminal line that needs accounting command; otherwise it is ineffective.

Configuration Examples

Command	Description
aaa new-model	Enables the AAA security service.
aaa authentication	Defines AAA authentication.
accounting commands	Applies the accounting commands to the terminal line.

Related Commands

The following example enables NAS command accounting.

```
QTECH(config)# aaa accounting commands 15 default start-stop group tacacs+
```

Platform Description

N/A

1.2. aaa accounting exec

Use this command to enable NAS access accounting.

Use the **no** form of this command to restore the default setting.

aaa accounting exec { **default |** *list-name* } **start-stop** *method1* [*method2...*]

no aaa accounting exec { **default** | *list-name* }

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined method list is used as the default method for Exec accounting.
list-name	Name of the Exec accounting method list, which could be any

	character strings
method	It must be one of the keywords: **none** and **group**. One method list can contain up to four methods.
none	Does not perform accounting.
group	Uses the server group for accounting, the RADIUS and TACACS+ server group is supported.

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

RGOS enables the exec accounting function after enabling the login authentication. After enabling the accounting function, it sends the account start information to the security server when the users log in the NAS CLI, and sends the account stop information to the security server when the users log out. If it does not send the account start information to the security server when a user logs in, it does not send the account stop information to the security server when a user logs out, either.

The configured exec accounting method must be applied to the terminal line that needs accounting command; otherwise it is ineffective.

Configuration Examples

The following example enables NAS access accounting.

```
QTECH(config)# aaa accounting network start-stop groupradius
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa authentication	Defines AAA authentication.

accounting commands	Applies the Exec accounting to the terminal line.

Platform Description

N/A

1.3. aaa accounting network

Use this command to enable network access accounting.

Use the **no** form of this command to restore the default setting.

aaa accounting network { default | *list-name* **} start-stop** *method1* [*method2*..]

no aaa accounting network { **default** | *list-name* }

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined method list is used as the default method for Network accounting.
list-name	Name of the accounting method list
method	Sends accounting messages at both the start time and the end time of access. Users are allowed to access the network, no matter whether the start accounting message enables the accounting successfully.
none	Does not perform accounting.
group	Uses the server group for accounting, the RADIUS and TACACS+ server group is supported.

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

RGOS performs accounting of user activities by sending record attributes to the security server. Use the **start-stop** keyword to set the user accounting option.

Configuration Examples

The following example enables network access accounting.

```
QTECH(config)# aaa accounting network start-stop groupradius
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa authorization network	Defines a network authorization method list.
aaa authentication	Defines AAA authentication.
username	Defines a local user database.

Platform Description

N/A

1.4. aaa accounting update

Use this command to enable the accounting update function. Use the **no** form of this command to restore the default setting. **aaa accounting update**

no aaa accounting update

Parameter Description

N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

If the AAA security service is not enabled, the accounting update function cannot be used. This command is used to set the accounting interval if the AAA security service has been enabled.

Configuration Examples

The following example enables the accounting update function.

```
QTECH(config)# aaa new-model
QTECH(config)# aaa accounting update
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa accounting network	Defines a network accounting method list.

Platform Description

N/A

1.5. aaa accounting update periodic

Use this command to set the interval of sending the accounting update message. Use the **no** form of this command to restore the default setting.

aaa accounting update periodic *interval*

no aaa accounting update periodic

Parameter Description

Parameter	Description
interval	Interval of sending the accounting update message, in the unit of minutes. The shortest interval is 1 minute.

Defaults

The default is 5 minutes.

Command

Global configuration mode

Mode

Usage Guide

If the AAA security service is not enabled, the accounting update function cannot be used. This command is used to set the accounting interval if the AAA security service has been enabled.

Configuration Examples

The following example sets the interval of accounting update to 1 minute.

```
QTECH(config)# aaa new-model QTECH(config)# aaa
accounting update
QTECH(config)# aaa accounting update periodic 1
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa accounting network	Defines a network accounting method list.

Platform Description

N/A

1.6. aaa authentication dot1x

Use this command to enable AAA authentication 802.1x and configure the 802.1x user authentication method list.

Use the **no** form of this command to delete the 802.1x user authentication method list.

aaa authentication dot1x { **default** | *list-name* } *method1* [*method2*...]

no aaa authentication dot1x { **default** | *list-name* }

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined 802.1x user authentication method list is used as the default method for user authentication.

list-name	Name of the 802.1x user authentication method list, which could be any character string
method	It must be one of the keywords: **local**, **none** and **group**. One method list can contain up to four methods.
local	Uses the local user name database for authentication.
none	Does not perform authentication.
group	Uses the server group for authentication. At present, the RADIUS server group is supported.

Defaults
N/A

Command Mode

Global configuration mode

Usage Guide

If the AAA 802.1x security service is enabled on the device, users must use AAA for 802.1x user authentication negotiation. You must use the **aaa authentication dot1x** command to configure a default or optional method list for 802.1x user authentication.

The next method can be used for authentication only when the current method does not work.

Configuration Examples

Related Commands

Platform Description

The following example defines an AAA authentication method list named **RDS_D1X**. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
QTECH(config)# aaa authentication dot1x rds_d1x group radiuslocal
```

Command	Description
aaa new-model	Enables the AAA security service.
dot1x authentication	Associates a specific method list with the 802.1x user.
username	Defines a local user database.

N/A

1.7. aaa authentication enable

Use this command to enable AAA Enable authentication and configure the Enable authentication method list.

Use the **no** form of this command to delete the user authentication method list.

aaa authentication enable default *method1* [*method2*...]

no aaa authentication enable default

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined authentication method list is used as the default method for Enable authentication.
method	It must be one of the keywords: **local, none** and **group**. One method list can contain up to four methods.
local	Uses the local user name database for authentication.
none	Does not perform authentication.
group	Uses the server group for authentication. At present, the RADIUS and TACACS+ server groups are supported.
enable	Enables AAA Enable authentication.

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

If the AAA Enable authentication service is enabled on the device, users must use AAA for Enable

authentication negotiation. You must use the **aaa authentication enable** command to configure a default or optional method list for Enable authentication.

The next method can be used for authentication only when the current method does not work. The Enable authentication function automatically takes effect after configuring the Enable authentication method list.

Configuration Examples

Related Commands

Platform Description

The following example defines an AAA Enable authentication method list. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
QTECH(config)# aaa authentication enable default group radiuslocal
```

Command	Description
aaa new-model	Enables the AAA security service.
enable	Switchover the user level.
username	Defines a local user database.

N/A

1.8. aaa authentication iportal

Use this command to enable AAA Portal Web user authentication.
Use the **no** form of this command to delete the authentication

method list. **aaa authentication iportal** { **default** | *list-name* }

method1 [*method2...*] **no aaa authentication iportal** {

default | *list-name* }

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined authentication method list is used as the default method for Login authentication.
list-name	Name of the user authentication method list, which could be any character strings
method	It must be one of the keywords: local, none, subs and group. One method list can contain up to four methods.
local	Uses the local user name database for authentication.
none	Does not perform authentication.
group	Uses the server group for authentication. At present, the RADIUS server group is supported.
subs	Uses the subs database for authentication.

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

If the AAA Portal Web security service is enabled on the device, users must use AAA for Portal Web authentication negotiation. You must use the **aaa authentication iportal** command to configure a default or optional method list for Portal Web authentication.

Configuration Examples

The following example defines an AAA Portal Web authentication method list named **rds_web**. First the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
QTECH(config)# aaa authentication iportal rds_web group radiuslocal
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
login authentication	Applies the Login authentication method to the terminal lines.
username	Defines a local user database.

Platform Description

N/A

1.9. aaa authentication login

Use this command to enable AAA Login authentication and configure the Login authentication method list.

Use the **no** form of this command to delete the authentication method list.

aaa authentication login { **default** | *list-name* } *method1* [*method2*..]

no aaa authentication login { **default** | *list-name* }

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined authentication
	method list is used as the default method for Login authentication.

list-name	Name of the user authentication method list, which could be any character strings
method	It must be one of the keywords: **local**, **none**, **group** and **subs**. One method list can contain up to four methods.
local	Uses the local user name database for authentication.
none	Does not perform authentication.
group	Uses the server group for authentication. At present, the RADIUS and TACACS+ server groups are supported.
subs	Uses the subs database for authentication.

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

If the AAA Login authentication security service is enabled on the device, users must use AAA for Login authentication negotiation. You must use the **aaa authentication login** command to configure a default or optional method list for Login authentication.

The next method can be used for authentication only when the current method does not work.

You need to apply the configured Login authentication method to the terminal line which needs Login authentication. Otherwise, the configured Login authentication method is invalid.

Configuration Examples

Related Commands

Platform Description

The following example defines an AAA Login authentication method list named list-1. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
QTECH(config)# aaa authentication login list-1 group radiuslocal
```

Command	Description
aaa new-model	Enables the AAA security service.
login authentication	Applies the Login authentication method to the terminal lines.
username	Defines a local user database.

N/A

1.10. aaa authentication ppp

Use this command to enable the AAA authentication for PPP user and configure the PPP user authentication method list.

Use the **no** form of this command to delete the authentication method list.

aaa authentication ppp { **default** | *list-name* } *method1* [*method2*...]

no aaa authentication ppp { **default** | *list-name* }

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined authentication method list is used as the default method for PPP user authentication.
list-name	Name of the user authentication method list, which could be any character strings
method	It must be one of the keywords: **local**, **none** **group** and **subs**. One method list can contain up to four methods.

local	Uses the local user name database for authentication.
none	Does not perform authentication.
group	Uses the server group for authentication. At present, the RADIUS server group is supported.
subs	Uses the subs database for authentication.

Defaults
N/A

Command Mode

Global configuration mode

Usage Guide

If the AAA PPP security service is enabled on the device, users must use AAA authentication for PPP negotiation. You must use the **aaa authentication ppp** command to configure a default or optional method list for PPP user authentication.

The next method can be used for authentication only when the current method does not work.

Configuration Examples

The following example defines an AAA authentication method list named rds_ppp for PPP session. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
QTECH(config)# aaa authentication ppp rds_ppp group radiuslocal
```

Related Commands

Command	Description
aaa new-model	**Enables the AAA security service.**

ppp authentication	**Associates a specific method list with the PPP user.**
username	**Defines a local user database.**

Platform Description

N/A

1.11. aaa authentication sslvpn

Use this command to enable AAA authentication for the SSL VPN user and configure the SSL VPN user authentication method list.

Use the **no** form of this command to delete the authentication

method list. **aaa authentication sslvpn** { **default** | *list-name* }

method1 [*method2...*] **no aaa authentication sslvpn** {

default | *list-name* }

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined authentication method list is used as the default method for SSL VPN user authentication.
list-name	Name of SSL VPN user authentication method list, which could be any character strings
method	It must be one of the keywords: **local**, **none**, **subs** and **group**. One method list can contain up to four methods.
local	Use the local user name database for authentication.

none	Does not perform authentication.
group	Uses the server group for authentication. At present, the RADIUS server group is supported.
subs	Uses the subs database for authentication.

Defaults
N/A

Command Mode

Global configuration mode

Usage Guide

If the SSL VPN security service is enabled on the device, users must use the AAA authentication for SSL VPN negotiation. You must use the **aaa authentication sslvpn** command to configure a default or optional method list for user authentication.

The next method can be used for authentication only when the current method does not work.

Configuration Examples

The following example defines an AAA authentication method list named **rds_sslvpn** for SSL VPN session. In the authentication method list, the RADIUS security server is first used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
QTECH(config)# aaa authentication sslvpn rds_sslvpn group radiuslocal
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.12. aaa authentication web-auth

Use this command to enable AAA second-generation Web authentication and configure the second-generation Web authentication method list in global configuration mode.

Use the **no** form of this command to delete the authentication method list. **aaa authentication web-auth** { **default** | *list-name* } *method1* [*method2*...] **no aaa authentication web-auth** { **default** | *list-name* }

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined authentication method list is used as the default method for the second-generation Web authentication.
list-name	Name of second-generation Web authentication method list, which could be any character strings
method	It must be one of the keywords: local, none, subs and group. One method list can contain up to four methods.
local	Uses the local user name database for authentication.
none	Does not perform authentication.
group	Uses the server group for authentication. At present, the RADIUS server group is supported.
subs	Uses the subs database for authentication.

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

If the AAA second-generation Web security service is enabled on the device, users must use AAA for the second-generation Web authentication negotiation. You must use the **aaa authentication web-auth** command to configure a default or optional method list for user authentication. The next method can be used for authentication only when the current method does not work.

Configuration Examples

Related Commands

Platform Description

The following example defines an AAA authentication method list named **rds_web**. In the authentication method list, the RADIUS security server is first used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
QTECH(config)# aaa authentication web-auth rds_web group radiusnone
```

Command	Description
N/A	N/A

N/A

1.13. aaa authorization commands

Use this command to authorize the command executed by the user who has logged in the NAS CLI. Use the **no** form of this command to restore the default setting.

aaa authorization commands *level* { **default** | *list-name* } *method1* [*method2...*]

no aaa authorization commands *level* { **default** | *list-name* }

Parameter Description

Parameter	Description
level	Command level to be authorized in the range from 0 to 15

default	When this parameter is used, the following defined method list is used as the default method for command authorization.
list-name	Name of the user authorization method list, which could be any character strings
method	It must be one of the keywords: **none** and **group**. One method list can contain up to four methods.
none	Do not perform authorization.
group	Uses the server group for authorization. At present, the TACACS+ server group is supported.

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

RGOS supports authorization of the commands executed by the users. When the users input and attempt to execute a command, AAA sends this command to the security server. This command is to be executed if the security server allows to. Otherwise, it will prompt command deny.

It is necessary to specify the command level when configuring the command authorization, and this specified command level is the default command level.

The configured command authorization method must be applied to terminal line which requires the command authorization. Otherwise, the configured command authorization method is ineffective.

Configuration Examples

Related Commands

Platform Description

The following example uses the TACACS+ server to authorize the level 15 command.

```
QTECH(config)# aaa authorization commands 15 default grouptacacs+
```

Command	Description
aaa new-model	Enables the AAA security service.
authorization commands	Applies the command authorization for the terminal line.

N/A

1.14. aaa authorization config-commands

Use this command to authorize the configuration commands (including in the global configuration mode and its sub-mode).

Use the **no** form of this command to restore the default setting.

aaa authorization config-commands

no aaa authorization config-commands

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

If you only authorize the commands in the non-configuration mode (for example, privileged EXEC mode), you can use the **no** form of this command to disable the authorization function in the configuration mode, and execute the commands in the configuration mode and its sub-mode without command authorization.

Configuration Examples

Related Commands

Platform Description

The following example enables the configuration command authorization function.

```
QTECH(config)# aaa authorization config-commands
```

Command	Description
aaa new-model	Enables the AAA security service.
aaa authorization commands	Defines the AAA command authorization.

N/A

1.15. aaa authorization console

Use this command to authorize the commands of the users who have logged in the console. Use the **no** form of this command to restore the default setting.

aaa authorization console no aaa authorization console

Parameter Description

Parameter	Description
N/A	N/A

Defaults
This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

RGOS supports to identify the users logged in from the console and from other terminals, configure whether to authorize the users logged in from the console or not. If the command authorization function is disabled on the console, the authorization method list applied to the console line is ineffective.

Configuration Examples

Related Commands

Platform Description

The following example enables the aaa authorization console function.

```
QTECH(config)# aaa authorization console
```

Command	Description
aaa new-model	Enables the AAA security service.
aaa authorization commands	Defines the AAA command authorization.
authorization commands	Applies the command authorization to the terminal line.

N/A

1.16. aaa authorization exec

Use this command to authorize the users logged in the NAS CLI and assign the authority level. Use the **no** form of this command to restore the default setting.

aaa authorization exec { **default** | *list-name* } *method1* [*method2*...]

no aaa authorization exec { **default** | *list-name* }

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined method list is used as the default method for Exec authorization.
list-name	Name of the user authorization method list, which could be any character strings
method	It must be one of the keywords listed in the following table. One method list can contain up to four methods.
local	Uses the local user name database for authorization.
none	Does not perform authorization.

group	Uses the server group for authorization. At present, the RADIUS server group is supported.

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

RGOS supports authorization of users logged in the NAS CLI and assignment of CLI authority level (0-15). The **aaa authorization exec** function is effective on condition that Login authentication function has been enabled. It cannot enter the CLI if it fails to enable the **aaa authorization exec**. You must apply the exec authorization method to the terminal line; otherwise the configured method is ineffective.

Configuration Examples

Related Commands

Platform Description

The following example uses the RADIUS server to authorize Exec.

```
QTECH(config)# aaa authorization exec default group radius
```

Command	Description
aaa new-model	Enables the AAA security service.
authorization exec	Applies the command authorization to the terminal line.
username	Defines a local user database.

N/A

1.17. aaa authorization network

Use this command to authorize the service requests (including such protocols as PPP and SLIP) from the users that access the network.

Use the **no** form of this command to restore the default setting.

aaa authorization network { **default** | *list-name* } *method1* [*method2*...]

no aaa authorization network { **default** | *list-name* }

Parameter Description

Parameter	Description
default	When this parameter is used, the following defined method list is used as the default method for Network authorization.
method	It must be one of the keywords: none and group. One method list can contain up to four methods.
none	Does not perform authorization.
group	Uses the server group for authorization. At present, the RADIUS server group is supported.

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

RGOS supports authorization of all the service requests related to the network, such as PPP and SLIP. If authorization is configured, all the authenticated users or interfaces will be authorized automatically.

Three different authorization methods can be specified. Like authorization, the next method can be used for authorization only when the current authorization method does not work. If the current authorization method fails, other subsequent authorization method is not used.

The RADIUS server authorizes authenticated users by returning a series of attributes. Therefore, RADIUS authorization is based on RADIUS authorization. RADIUS authorization is performed only when the user passes the RADIUS authorization.

Configuration Examples

Related Commands

Platform Description

The following example uses the RADIUS server to authorize network services.

```
QTECH(config)# aaa authorization network default groupradius
```

Command	Description
aaa new-model	Enables the AAA security service.
aaa accounting	Defines AAA accounting.
aaa authentication	Defines AAA authentication.
username	Defines a local user database.

N/A

1.18. aaa domain

Use this command to configure the domain attributes.

Use the **no** form of this command to restore the default setting.

aaa domain { **default** | *domain-name* }

no aaa domain { **default |** *domain-name* }

Parameter Description

Parameter	Description
default	Uses this parameter to configure the default domain.
domain-name	The name of the specified domain

Defaults

No domain is configured by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to configure the domain-name–based AAA service. The **default** is to configure the default domain. That is the method list used by the network device if the users are without domain information. The *domain-name* is the specified domain name, if the users are with this *domain name*, the method lists associated with this domain are used. At present, the system can configure up to 32 domains.

Configuration Examples

The following example configures the domain name.

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

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa domain enable	Enables the domain-name-based AAA service.
show aaa domain	Displays the domain configuration.

Platform Description

N/A

1.19. aaa domain enable

Use this command to enable domain-name-based AAA service. Use the **no** form of this command to restore the default setting. **aaa domain enable**

no aaa domain enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

To perform the domain-name-based AAA service configuration, enable this service.

Configuration Examples

Related Commands

Platform Description

The following example enables the domain-name-based AAA service.

```
QTECH(config)# aaa domain enable
```

Command	Description
aaa new-model	Enables the AAA security service.
show aaa doamain	Displays the domain configuration.

N/A

1.20. aaa local authentication attempts

Use this command to set login attempt times.

aaa local authentication attempts *max-attempts*

Parameter Description

Parameter	Description
max-attempts	In the range from 1 to 2,147,483,647

Defaults

The default is 3.

Command Mode

Global configuration mode

Usage Guide

Use this command to configure login attempt times.

Configuration Examples

The following example sets login attempt times to 6.

```
QTECH #configure terminal
QTECH(config)#aaa local authentication attempts 6
```

Related Commands

Command	Description
show running-config	Displays the current configuration of the switch.
show aaa lockout	Displays the lockout configuration parameter of current login.

Platform Description

N/A

1.21. aaa local authentication lockout-time

Use this command to configure the lockout-time period when the login user has attempted for more than the limited times.

aaa local authentication lockout-time *lockout-time*

Parameter Description

Parameter	Description
lockout-time	In the range from 1 to 3200 in the unit of minutes

Defaults

The default is 15 minutes.

Command Mode

Global configuration mode

Usage Guide

Use this command to configure the length of lockout-time when the login user has attempted for more than the limited times.

Configuration Examples

The following example sets the lockout-time period to 5 minutes.

```
QTECH#configure terminal
QTECH(config)#aaa local authentication lockout-time 5
```

Related Commands

Command	Description
show running-config	Displays the current configuration of the switch.
show aaa lockout	Displays the lockout configuration parameter of current login.

Platform Description

N/A

1.22. aaa log enable

Use this command to enable the system to print the syslog informing AAA authentication success. Use the **no** form of this command to restore the default setting.

aaa log enable no aaa log enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults T
his function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to enable the system to print the syslog informing aaa authentication success.

Configuration Examples

Related Commands

Platform Description

The following example disables the system to print the syslog informing aaa authentication success.

```
QTECH(config)# no aaa log enable
```

Command	Description
N/A	N/A

N/A

1.23. aaa log rate-limit

Use this command to set the rate of printing the syslog informing AAA authentication success. Use the **no** form of this command to restore the default printing rate.

aaa log rate-limit *num*

no aaa log rate-limit

Parameter Description

Parameter	Description
num	The number of syslog entries printed per second. The range is from 0 to 65,535. 0 indicates the printing rate is not limited.

Defaults

The default is 5.

Command Mode

Global configuration mode

Usage Guide

Too much printing may flood the screen or even reduce device performance. In this case, use this command to adjust the printing rate.

Configuration Examples

Related Commands

Platform Description

The following example sets the rate of printing the syslog informing AAA authentication success to 10.

```
QTECH(config)# aaa log rate-limit 10
```

Command	Description
N/A	N/A

N/A

1.24. aaa new-model

Use this command to enable the RGOS AAA security service. Use the **no** form of this command to restore the default setting. **aaa new-model**

no aaa new-model

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to enable AAA. If AAA is not enabled, none of the AAA commands can be configured.

Configuration Examples

Related Commands

Platform Description

The following example enables the AAA security service.

```
QTECH(config)# aaa new-model
```

Command	Description
aaa authentication	Defines a user authentication method list.
aaa authorization	Defines a user authorization method list.
aaa accounting	Defines a user accounting method list.

N/A

1.25. access-limit

Use this command to configure the number of users limit for the domain, which is only valid for the IEEE802.1 users.

Use the **no** form of this command to restore the default setting.

access-limit *num*

no access-limit

Parameter Description

Parameter	Description
num	The number used for the user limitation is only valid for the IEEE802.1 users.

Defaults

By default, no number of users is limited.

Command

Domain configuration mode

Mode

Usage Guide

This command limits the number of users for the domain.

Configuration Examples

The following example sets the number of users to 20 for the domain named QTECH.com.

```
QTECH(config)# aaa domain QTECH.com
QTECH(config-aaa-domain)# access-limit 2
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa domain enable	Switchover the user level.
show aaa domain	Defines a local user database.

Platform Description

N/A

1.26. accounting network

Use this command to configure the Network accounting list. Use the **no** form of this command to restore the default setting. **accounting network** { **default** | *list-name* }

no accounting network

Parameter Description

Parameter	Description
default	Uses this parameter to specify the default method list.
list-name	The name of the network accounting list

Defaults

With no method list specified, if the user sends the request, the device will attempt to specify the default method list for the user.

Command Mode

Domain configuration mode

Usage Guide

Use this command to configure the Network accounting method list for the specified domain.

Configuration Examples

The following example sets the Network accounting method list for the specified domain.

```
QTECH(config)# aaa domain QTECH.com
QTECH(config-aaa-domain)# accounting network default
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa domain enable	Enables the domain-name-based AAA service.
show aaa domain	Displays the domain configuration.

Platform Description

N/A

1.27. authentication dot1x

Use this command to configure the IEEE802.1x authentication list. Use the **no** form of this command to restore the default setting. **authentication dot1x** { **default** | *list-name* }

no authentication dot1x

Parameter Description

Parameter	Description
default	Uses this parameter to specify the default method list
list-name	The name of the specified method list

Defaults

With no method list specified, if users send the request, the device will attempt to specify the default method list for users.

Command Mode

Domain configuration mode

Usage Guide

Specify an IEEE802.1x authentication method list for the domain.

Configuration Examples

The following example sets an IEEE802.1x authentication method list for the specified domain.

```
QTECH(config)# aaa domain QTECH.com
QTECH(config-aaa-domain)# authentication dot1x default
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa domain enable	Enables the domain-name-based AAA service.
show aaa domain	Displays the domain configuration.

Platform Description

N/A

1.28. authorization network

Use this command to configure the Network authorization list. Use the **no** form of this command to restore the default setting. **authorization network** { **default** | *list-name* }

no authorization network

Parameter Description

Parameter	Description
default	**Uses this parameter to specify the default method list.**
list-name	**The name of the specified method list**

Defaults

With no method list specified, if users send the request, the device will attempt to

specify the default method list for users.

Command Mode

Domain configuration mode

Usage Guide

Specify an authorization method list for the domain.

Configuration Examples

The following example sets an authorization method list for the specified domain.

```
QTECH(config)# aaa domain QTECH.com
QTECH(config-aaa-domain)# authorization network default
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa domain enable	Enables the domain-name-based AAA service.
show aaa domain	Displays the domain configuration.

Platform Description

N/A

1.29. clear aaa local user lockout

Use this command to clear the lockout user list.

clear aaa local user lockout { **all | user-name** *word* }

Parameter Description

Parameter	Description
all	Indicates all locked users.
user-name *word*	Indicates the ID of the locked User.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to clear all the user lists or a specified user list.

Configuration Examples

Related

The following example clears the lockout user list.

```
QTECH(config)# clear aaa local user lockout all
```

Commands

Command	Description
show running-config	Displays the current configuration of the switch.
show aaa lockout	Displays the lockout configuration parameter of current login.

Platform Description

N/A

1.30. show aaa accounting update

Use this command to display the accounting update information.

show aaa accounting update

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

Use this command to display the accounting update interval and whether the accounting update is enabled.

Configuration Examples

Related Commands

Platform Description

The following example displays the accounting update information.

```
QTECH# show aaa accounting update
```

Command	Description
aaa new-model	Enables the AAA security service.
aaa domain enable	Enables the domain-name-based AAA service.

N/A

1.31. show aaa domain

Use this command to display all current domain information.

show aaa domain [**default** | *domain-name*]

Parameter Description

Parameter	Description
default	Displays the default domain.
domain-name	Displays the specified domain.

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

If no domain-name is specified, all domain information will be displayed.

Configuration Examples

The following example displays the domain named domain.com.

```
QTECH(config)# show aaa domain domain.com
=============Domain domain.com============= State: Active
Username format: Without-domain Access limit: No limit
802.1X Access statistic: 0

Selected method list: authentication dot1x default
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa domain enable	Enables the domain-name-based AAA service.

Platform Description

N/A

1.32. show aaa lockout

Use this command to display the lockout configuration.

show aaa lockout

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

Use this command to display the lockout configuration.

Configuration Examples

The following example displays the lockout configuration.

```
QTECH# show aaa lockout Lock tries:     3
Lock timeout: 15 minutes
```

Related

Commands

Command	Description
N/A	**N/A**

Platform Description

N/A

1.33. show aaa group

Use this command to display all the server groups configured for AAA.

show aaa group

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following command displays all the server groups.

```
QTECH# show aaa group Type      Reference  Name

--------------------
radius          1         radius
```

```
tacacs+         1       tacacs+
radius          1       dot1x_group
radius          1       login_group
radius          1       enable_group
```

Command	Description
aaa group server	Configures the AAA server group.

N/A

1.34. show aaa method-list

Use this command to display all AAA method lists.

show aaa method-list

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

Use this command to display all AAA method lists.

Configuration Examples

The following example displays the AAA method list.

```
QTECH# show aaa method-list Authentication method-list
aaa authentication login default group radius aaa authentication ppp default group radius
aaa authentication dot1x default group radius
aaa authentication dot1x san-f local group angel group rain none aaa authentication enable
default group radius
Accounting method-list
aaa accounting network default start-stop group radius Authorization method-list
aaa authorization network default group radius
```

Related Commands

Command	Description

aaa authentication	Defines a user authentication method list
aaa authorization	Defines a user authorization method list
aaa accounting	Defines a user accounting method list

Platform Description

N/A

1.35. show aaa user

Use this command to display AAA user information.

show aaa user { all | lockout | by-id *session-id* **| by-name** *user-name* **}**

Parameter Description

Parameter	Description
all	Displays all AAA user information.
lockout	Displays the locked AAA user information.
by-id *session-id*	Displays the information of the AAA user that with a specified session ID.
by-name *user-name*	Displays the information of the AAA user with a specified user name.

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide
Use this command to display AAA user information.

Configuration Examples

Related Commands

Platform Description

The following example displays AAA user information.

```
QTECH#show aaa user all

Id     Name

2345687901    wwxy

QTECH# show aaa user by-id 2345687901

Id     Name

2345687901    wwxy

QTECH# show aaa user by-name wwxy

Id     Name

2345687901    wwxy

QTECH# show aaa user lockout

Name   Tries  Lock   Timeout(min)

QTECH#
```

Command	Description
N/A	N/A

N/A

1.36. state

Use this command to set whether the configured domain is valid. Use the **no** form of this command to restore the default setting.

Parameter Description

state { **block | active** }

no state

Parameter	Description
block	The configured domain is invalid.
active	The configured domain is valid.

Defaults

The default is active.

Command Mode

Domain configuration mode

Usage Guide

Use this command to set whether the specified configured domain is valid.

Configuration Examples

The following example sets the configured domain to be invalid.

```
QTECH(config)# aaa domain QTECH.com
QTECH(config-aaa-domain)# state block
```

Related Commands

Command	Description
aaa new-model	Enables the AAA security service.
aaa domain enable	Enables the domain-name-based AAA service.
show aaa domain enable	Displays the domain configuration.

Platform Description

N/A

COMMANDS

2.1. aaa group server radius

Use this command to enter AAA server group configuration mode. Use the **no** form of this command to restore the default setting. **aaa group server radius** *name*

no aaa group server radius *name*

Parameter Description

Parameter	Description
name	Server group name. Keywords “radius” and “tacacs +” are excluded as they are the default RADIUS and TACACS+ server group names.

Defaults
N/A

Command Mode

Global configuration mode

Usage Guide
This command is used to configure a RADIUS AAA server group.

Configuration Examples

Related Commands

Platform Description

The following example configures a RADIUS AAA server group named ss.

```
QTECH(config)#    aaa    group   radi   ss
server        QTECH(config-gs-   us
radius)#  end  QTECH#  show  aaa
group
Type   Reference  Name
```

```
radius     1     radius

tacacs+    1     tacacs+

radius     1     ss
```

Command	Description
N/A	N/A

N/A

2.2. ip radius source-interface

Use this command to specify the source IP address for the RADIUS packet.

Use the **no** form of this command to delete the source IP address for the RADIUS packet.

ip radius source-interface *interface-name*

no radius source-interface *interface-name*

Parameter Description

Parameter	Description
interface-name	Interface that the source IP address of the RADIUS packet belongs to.

Defaults

The source IP address of the RADIUS packet is set by the network layer.

Command mode

Global configuration mode

Usage Guide

In order to reduce the NAS information to be maintained on the RADIUS server, use this command to set the source IP address of the RADIUS packet. This command uses the first IP address of the specified interface as the source IP address of the RADIUS packet. This command is used in the layer 3 devices.

Configuration Examples

Related Commands

Platform Description

The following example specifies that the RADIUS packet obtains an IP address from the fastEthernet 0/0 interface and uses it as the source IP address of the RADIUS packet.

```
QTECH(config)# ip radius source-interface fastEthernet0/0
```

Command	Description
radius-server host	Defines the RADIUS server.
ip address	Configures the IP address of the interface.

N/A

2.3. ip oob

Use this command to specify the MGMT port used in the TACACS+ server group. Use the **no** form of this command to restore the default setting.

ip oob [**via** *mgmt_name*]

no ip oob

Parameter Description

Parameter	Description
mgmt_name	MGMT port name

Defaults

N/A

Command Mode

TACACS+ server group configuration mode

Usage Guide

Use the **aaa group server tacacs+** command to enter TACACS+ server group configuration mode. If no port is specified as the MGMT port. MGMT Port 0 is

default.

Configuration Examples

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.4. ip vrf forwarding

Use this command to select a VRF for the AAA server group. Use the **no** form of this command to restore the default setting. **ip vrf forwarding** *vrf_name*

no ip vrf forwarding

Parameter Description

Parameter	Description
vrf_name	VRF name

Defaults
N/A

Command Mode

Server group configuration mode

Usage Guide
This command is used to select a VRF for the specified server.

Configuration Examples

The following example selects the VRF named vrf_name for AAA server group ss.

```
QTECH(config)# aaa group server radius ss QTECH(config-gs-radius)# server 192.168.4.12
QTECH(config-gs-radius)#  server  192.168.4.13  QTECH(config-gs-radius)#  ip  vrf  forwarding
```

```
vrf_name
QTECH(config-gs-radius)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.5. radius vendor-specific extend

Use this command to extend RADIUS not to differentiate the IDs of private vendors. Use the **no** form of this command to restore the default setting.

radius vendor-specific extend

no radius vendor-specific extend

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Only the private vendor IDs of QTECH are recognized.

Command Mode

Global configuration mode

Usage Guide

This command is used to identify the attributes of all vendor IDs by type.

Configuration Examples

Related Commands

Platform Description

The following example extends RADIUS so as not to differentiate the IDs of private vendors:

```
QTECH(config)# radius vendor-specific extend
```

Command	Description
radius attribute	Configures vendor type.
radius set qos cos	Sets the QoS value sent by the RADIUS server as the cos value of the interface.

N/A

2.6. radius vendor-specific attribute support

Use this command to configure whether RADIUS accounting request packets carry the private attribute of a specified vendor.

Use the **no** form of this command to configure that RADIUS accounting request packets do not carry the private attribute of a specified vendor.

radius vendor-specific attribute support { cisco | huawei | ms} no radius vendor-specific attribute support { cisco | huawei | ms}

Parameter Description

Parameter	Description
cisco	Indicates the private attribute of Cisco.
huawei	Indicates the private attribute of Huawei.
ms	Indicates the private attribute of Microsoft.

Defaults

By default, RADIUS accounting request packets carry the private attribute of a specified vendor.

Command Mode

Global configuration mode

Usage Guide

This command is used to configure whether RADIUS accounting request packets carry the private attribute of a specified vendor as required.

Configuration Examples

- The following example configures that RADIUS accounting request packets carry the private attribute of Huawei.

```
QTECH(config)# radius vendor-specific attribute support huawei
```

Related Commands

Platform Description

- The following example configures that RADIUS accounting request packets do not carry the private attribute of Huawei.

QTECH(config)# no radius vendor-specific attribute supporthuawei

Command	Description
N/A	N/A

N/A

2.7. radius-server account update retransmit

Use this command to configure accounting update packet retransmission for the second generation Web authentication user.

Use the **no** form of this command to restore the default setting,

radius-server account update retransmit

no radius-server account update retransmit

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command Mode Global configuration mode

Usage Guide

This command is used to configure accounting update packet retransmission for the second generation Web authentication user exclusively.

Configuration Examples

Related Commands

The following example configures accounting update packet retransmission for the second generation Web authentication user.

```
QTECH(config)#radius-server account update retransmit
```

Command	Description
N/A	N/A

Platform Description N/A

2.8. radius-server attribute 31

Use this command to specify the MAC-based format of RADIUS Calling-Station-ID attribute. Use the **no** form of this command to restore the default setting.

radius-server attribute 31 mac format { **ietf** | **normal** | **unformatted** }

no radius-server attribute 31 mac format

Parameter Description

Parameter	Description
ietf	The standard format specified by the IETF RFC3580. '-'is used as the separator, for example: 00-D0-F8-33-22-AC.
normal	Normal format representing the MAC address. ;.'is used as the separator. For example: 00d0.f833.22ac.
unformatted	No format and separator. By default, unformatted is used. For example: 00d0f83322ac.

Defaults

The default format is unformatted.

Command Mode

Global configuration mode

Usage Guide

Some RADIUS security servers (mainly used to 802.1x authentication) may identify the IETF format only. In this case, the RADIUS Calling-Station-ID attribute shall be set as the IETF format type.

Configuration Examples

Related Commands

Platform Description

The following example defines the RADIUS Calling-Station-ID attribute as IETF format.

```
QTECH(config)# radius-server attribute 31 mac formatietf
```

Command	Description
radius-server host	Defines the RADIUS server.

N/A

2.9. radius-server attribute class

Use this command to analyze the flow control value of the RADIUS CLASS attributes. Use the **no** form of this command to restore the default setting.

radius-server attribute class user-flow-control { **format-16bytes** | **format-32bytes** }

no radius-server attribute class user-flow-control

Parameter Description

Parameter	**Description**
user-flow-control	Analyzes flow control value in the CLASS attribute.

format-16bytes	Sets the format of flow control value to 16 bytes.
format-32bytes	Sets the format of flow control value to 32 bytes.

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

This command is required if the server pushes the flow control value through the CLASS attribute.

Configuration Examples

The following example analyzes the flow control value of the CLASS attribute and sets the format to 32 bytes.

```
QTECH(config)#radius-server attribute class user-flow-control
format-32bytes
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.10. radius-server dead-criteria

Use this command to configure criteria on a device to determine that the Radius server is unreachable.

Use the **no** form of this command to restore the default setting.

radius-server dead-criteria { **time** *seconds* [**tries** *number*] **| tries** *number* }

no radius-server dead-criteria { **time** [**tries**] **| tries** }

Parameter Description

Parameter	Description
time *seconds*	Configures the timeout value. If the device does not receive a correct response packet from the Radius server within the specified time, the Radius server is considered to be unreachable. The value is in the range from 1 to 120 in the unit of seconds.
tries *number*	Configures the successive timeout times. When sending a request from the device to the Radius server times out for the specified times, the device considers that the Radius server is unreachable. The value is in the range from 1 to 100 in the unit of seconds.

Defaults

The default **time** *seconds* is 60 and **tries** *number* is 10.

Command Mode

Global configuration mode

Usage Guide

If a Radius server meets the timeout and timeout times at the same time, it is considered to be unreachable. This command is used to adjust the parameter conditions of timeout and timeout times.

Configuration Examples

Related Commands

Platform Description

The following example sets the timeout to 120 seconds and timeout times to 20.

```
QTECH(config)# radius-server dead-criteria time 120 tries 20
```

Command	Description
radius-server host	Defines the RADIUS security server.
radius-server deadtime	Defines the duration when a device stops sending any requests to an unreachable Radius server.
radius-server timeout	Defines the timeout for the packet re-transmission.

N/A

2.11. radius-server deadtime

Use this command to configure the duration when a device stops sending any requests to an unreachable Radius server.

Use the **no** form of this command to restore the default setting.

radius-server deadtime *minutes*

no radius-server deadtime

Parameter Description

Parameter	Description
minutes	Defines the duration in minutes when the device stops sending any requests to the unreachable Radius server. The value is in the range from 1 to 1,440 in the unit of minutes.

Defaults

The default value of *minutes* is 0, that is, the device keeps sending requests to the unreachable Radius server.

Command Mode

Global configuration mode

Usage Guide

If active Radius server detection is enabled on the device, the time parameter of this command does not take effect on the Radius server. Otherwise, the Radius server becomes reachable when the duration set by this command is shorter than the unreachable time.

Configuration Examples

Related Commands

Platform Description

The following example sets the duration when the device stops sending requests to 1 minute.

```
QTECH(config)# radius-server deadtime 1
```

Command	Description
radius-server host	Defines the RADIUS security server.
radius-server dead-criteria	Defines the criteria to determine that a Radius server is unreachable.

N/A

2.12. radius-server host

Use this command to specify a RADIUS security server host. Use the **no** form of this command to restore the default setting.

radius-server host [**oob** [**via** *mgmt-name*]] { *ipv4-address* | *ipv6-address* } [**auth-port** *port-number*] [**acct-port** *port-number*] [**test username** *name* [**idle-time** *time*] [**ignore-auth-port**] [**ignore-acct-port**]] [**key** [**0** | **7**] *text-string*]

no radius-server host { *ipv4-address* | *ipv6-address* }

Parameter Description

Parameter	Description
oob [via mgmt-name]	Specifies an MGMT port as the source port for TACACS+ communication. The default is MGMT Port 0.
ipv4-address	IPv6 address of the RADIUS security server host.
ipv6-address	IPv4 address of the RADIUS security server host.
auth-port	UDP port used for RADIUS authentication.
port-number	Number of the UDP port used for RADIUS authentication. If it is set to 0, this host does not perform authentication.
acct-port	UDP port used for RADIUS accounting.
port-number	Number of the UDP port used for RADIUS accounting. If it is set to 0, this host does not perform accounting.
test username name	(Optional) Enables the active detection to the RADIUS security server and specify the username used by the active detection.
idle-time time	(Optional) Sets the interval of sending the test packets to the reachable RADIUS security server, which is 60 minutes by default and in the range of 1 to 1440 minutes (namely 24 hours).
ignore-auth-port	(Optional) Disables the detection to the authentication port on the RADIUS security server. It is enabled by default.

ignore-acct-port	(Optional) Disables the detection to the authentication port on the RADIUS security server. It is enabled by default.
key [**0** | **7**] *text-string*	Configure a shared key for the server. The type of encryption can be specified. 0 is no encryption and 7 is simple encryption. The default is 0.

Defaults

No RADIUS host is specified by default.

Command Mode

Global configuration mode

Usage Guide

In order to implement the AAA security service using RADIUS, you must define a RADIUS security server. You can define one or more RADIUS security servers using the **radius-server host** command.

Configuration Examples

The following example defines a RADIUS security server host:

```
QTECH(config)# radius-server host 192.168.12.1
```

The following example defines a RADIUS security server host in the IPv4 environment, enable the active detection with the detection interval 60 minutes and disable the accounting UDP port detection:

```
QTECH(config)# radius-server host 192.168.100.1 test username viven idle-time
60 ignore-acct-port
```

Related Commands

Platform Description

The following example defines a RADIUS security server host in the IPv6 environment

```
QTECH(config)# radius-server host 3000::100
```

Command	Description

aaa authentication	Defines the AAA authentication method list
radius-server key	Defines a shared password for the RADIUS security server.
radius-server retransmit	Defines the number of RADIUS packet retransmissions.

N/A

2.13. radius-server key

Use this command to define a shared password for the network access server (device) to communicate with the RADIUS security server.

Use the **no** form of this command to restore the default setting.

radius-server key [**0 | 7**] *text-string*

no radius-server key

Parameter Description

Parameter	Description
text-string	**Text of the shared password**
0 | 7	**Password encryption type. 0: no encryption; 7: Simply-encrypted.**

Defaults

No shared password is specified by default.

Command

Mode

Global configuration mode.

Usage Guide

A shared password is the basis for communications between the device and the RADIUS security server. In order to allow the device to communicate with the RADIUS security server, you must define the same shared password on the device and the RADIUS security server.

Configuration Examples

Related Commands

Platform Description

The following example defines the shared password **aaa** for the RADIUS security server:

```
QTECH(config)# radius-server key aaa
```

Command	Description
radius-server host	Defines the RADIUS security server.
radius-server retransmit	Defines the number of RADIUS packet retransmissions.
radius-server timeout	Defines the timeout for the RADIUS packet.

N/A

2.14. radius-server retransmit

Use this command to configure the number of packet retransmissions before the device considers that the RADIUS security server does not respond.

Use the **no** form of this command to restore the default setting.

radius-server retransmit *retries*

no radius-server retransmit

Parameter Description

Parameter	Description

retries	Number of retransmissions in the range from 0 to 100. The value of 0 indicates no retransmission.

Defaults
The default is 3.

Command Mode
Global configuration mode.

Usage Guide

AAA uses the next method to authenticate users only when the current security server for authentication does not respond. When the device retransmits the RADIUS packet for the specified times and the interval between every two retries is timeout, the device considers that the security sever does not respond.

Configuration Examples

Related Commands

Platform Description

The following example sets the number of retransmissions to 4.

```
QTECH(config)# radius-server retransmit 4
```

Command	Description
radius-server host	Defines the RADIUS security server.
radius-server key	Defines a shared password for the RADIUS server.
radius-server timeout	Defines the timeout for the RADIUS packet.

N/A

2.15. radius-server source-port

Use this command to configure the source port to send RADIUS packets. Use the **no** form of this command to restore the default setting.

radius-server source-port ***port***

no radius-server source-port

Parameter Description

Parameter	Description
port	The port ID, in the range from 0 to 65535.

Defaults

The default is a random number.

Command Mode

Global configuration mode

Usage Guide

The source port is random by default. This command is used to specify a source port.

Configuration Example

Related Commands

The following example configures source port 10000 to send RADIUS packets.

```
QTECH(config)# radius-server source-port 10000
```

Command	Description
N/A	N/A

Platform Description

N/A

2.16. radius-server timeout

Use this command to set the time for the device to wait for a response from the security server after retransmitting the RADIUS packet.

Use the **no** form of this command to restore the default setting.

radius-server timeout *seconds*

no radius-server timeout

Parameter Description

Parameter	Description
seconds	Timeout in the range from 1 to 1,000 in the unit of seconds.

Defaults

The default is 5 seconds.

Command

Mode

Global configuration mode

Usage Guide

This command is used to change the timeout of packet retransmission.

Configuration Examples

Related Commands

Platform Description

The following example sets the timeout to 10 seconds.

```
QTECH(config)# radius-server timeout 10
```

Command	Description
radius-server host	Defines the RADIUS security server.
radius-server retransmit	Defines the number of the RADIUS packet retransmissions.

radius-server key	Defines a shared password for the RADIUS server.

N/A

2.17. radius-server authentication attribute

Use this command to enable access-request packets to contain a specified RADIUS attribute. Use the **no** or **default** form of this command to restore the default setting.

```
radius-server authentication attribute type package
```

Parameter Description

no radius-server authentication attribute *type*
package default radius-server authentication
attribute *type* **package**

Use this command to disable access-request packets to contain a specified RADIUS attribute. Use the **no** or **default** form of this command to restore the default setting.

```
radius-server authentication attribute type unpackage
```

no radius-server authentication attribute *type*
unpackage default radius-server authentication
attribute *type* **unpackage**

Parameter	Description
type	RADIUS attribute in the range from 1 to 255

Defaults

RFC-compliant

Command Mode

Global configuration mode

Usage Guide Use this command to enable access-request packets to contain a specified RADIUS attribute.

Configuration Examples

The following example disables access-request packets to contain attribute NAS-PORT-ID.

```
QTECH(config)# radius-server authentication attribute 87unpackage
```

Platform Description

N/A

2.18. radius-server account attribute

Use this command to enable account-request packets to contain a specified RADIUS attribute. Use the **no** or **default** form of this command to restore the default setting.

```
radius-server account attribute type package
```

no radius-server account attribute *type*

package default radius-server account

attribute *type* **package**

Use this command to disable account-request packets to contain a specified RADIUS attribute. Use the **no** or **default** form of this command to restore the default setting.

```
radius-server account attribute type unpackage
```

no radius-server account attribute *type*

unpackage default radius-server account

attribute *type* **unpackage**

Parameter Description

Parameter	Description
type	RADIUS attribute in the range from 1 to 255

Defaults

RFC-compliant

Command Mode

Global configuration mode

Usage Guide

Use this command to enable or disable account-request packets to contain a specified RADIUS attribute.

Configuration Examples

The following example disables account-request packets to contain attribute NAS-PORT-ID.

```
QTECH(config)# radius-server account attribute 87unpackage
```

Platform Description

N/A

2.19. radius-server authentication vendor

Use this command to enable access-request packets to contain vendor-specific RADIUS attributes. Use the **no** or **default** form of this command to restore the default setting.

```
radius-server authentication vendor [cmcc | microsoft | cisco] package no
radius-server authentication vendor vendor_name package
```

default radius-server authentication vendor *vendor_name* **package**

Parameter Description

Parameter	Description
cmcc | microsoft | cisco	Vendor name

Defaults

Access-request packets do not contain vendor- specific RADIUS attributes by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to enable access-request packets to contain vendor- specific RADIUS attributes.

Configuration Examples

The following example enables access-request packets to contain “cmcc”.

```
QTECH(config)# radius-server authentication vendor cmccpackage
```

Platform Description

N/A

2.20. radius-server account vendor

Use this command to enable account-request packets to contain vendor-specific RADIUS attributes. Use the **no** or **default** form of this command to restore the default setting.

Parameter Description

radius-server account vendor [cmcc | microsoft | cisco]

package no radius-server account vendor *vendor_name*

package

default radius-server account vendor *vendor_name* **package**

Parameter	Description
cmcc | microsoft | cisco	**Vender name**

Defaults

Account-request packets do not contain vendor- specific RADIUS attributes by default.

Command Mode

Global configuration mode

Usage Guide Use this command to enable account-request packets to contain vendor-specific RADIUS attributes.

Configuration Examples

The following example enables account-request packets to contain “cmcc”.

```
QTECH(config)# radius-server account vendor cmcc package
```

Platform Description

N/A

2.21. radius set qos cos

Use this command to set the QoS value sent by the RADIUS server as the CoS value of the interface. Use the **no** form of this command to restore the default setting.

```
radius set qos  cos no radius set qos cos
```

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Set the QoS value sent by the RADIUS server as the DSCP value.

Command Mode

Global configuration mode.

Usage Guide

This command is used to set the QoS value sent by the RADIUS server as the CoS value, and the DSCP value by default.

Configuration Examples

The following example sets the QoS value sent by the RADIUS server as the CoS value of the interface:

```
QTECH(config)# radius set qos cos
```

Related Commands

Command	Description

radius vendor-specific extend	Extends RADIUS as not to differentiate the IDs of private vendors.

Platform Description

N/A

2.22. radius support cui

Use this command to enable RADIUS to support the cui function. Use the **no** form of this command to restore the default setting. **radius support cui**

no radius support cui

Parameter Description

Parameter	Description
N/A	N/A

Defaults
This function is disabled by default.

Command Mode
Global configuration mode

Usage Guide
This command is used to enable RADIUS to support the cui function.

Configuration Examples

Related Commands

Platform Description

The following example enables RADIUS to support the cui function.

```
QTECH(config)# radius support cui
```

Command	Description
N/A	N/A

N/A

2.23. server auth-port acct-port

Use this command to add the server of the AAA server group. Use the **no** form of this command to restore the default setting.

server { *ipv4-addr* | *ipv6-addr*} [**auth-port** *port1*] [**acct-port** *port2*]

no server { *ipv4-addr* | *ipv6-addr*} [**auth-port** *port1*] [**acct-port** *port2*]

Parameter Description

Parameter	Description
ip-addr	Server IP address
Ipv6-addr	Server IPv6 address
port1	Server authentication port
port2	Server accounting port

Defaults

No server is configured by default.

Command Mode

Server group configuration mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example adds server 192.168.4.12 to server group ss and sets the accounting port and authentication port to 5 and 6 respectively.

```
QTECH(config)# aaa group server   radius ss
QTECH(config-gs-radius)# server   192.168.4.12   acct-port   5   auth-port   6
QTECH(config-gs-radius)# end
QTECH# show aaa group
Type   Reference  Name
                                  radius
radius
tacacs+                           tacacs
radius                            ss
```

Command	Description
N/A	N/A

N/A

2.24. show radius acct statistics

Use this command to display RADIUS accounting statistics.
show radius acct statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Global configuration mode/Privileged EXEC mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays RADIUS accounting statistics.

```
QTECH#show radius acct statistics Accounting Servers:
Server Index.1
Server Address.     192.168.1.1
Server Port. 1813
Msg Round Trip Time.............................. 0 (msec)
First Requests.     1
Retry Requests.     1
Accounting Responses.      0
Malformed Msgs.     0
Bad Authenticator Msgs.    0
Pending Requests........
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.25. show radius auth statistics

Use this command to display RADIUS authentication statistics.
show radius auth statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Global configuration mode/Privileged EXEC mode/Interface configuration mode

N/A

Configuration

The following example displays RADIUS authentication statistics.

```
Examples    QTECH#show radius auth statistics Authentication Servers:
            Server Index.1
            Server Address.     192.168.1.1
            Server Port. 1812



              Msg                   Round                  Trip   0  (msec)
              Time..............................

              First                                               0
              Requests.....................................

              Retry                                               0
              Requests.....................................

              Accept                                              0
              Responses....................................

              Reject                                              0
              Responses....................................

              Challenge                                           0
              Responses.............................

              Malformed                                           0
              Msgs.................................

              Bad                               Authenticator     0
              Msgs.........................

              Pending                                             0
              Requests.....................................

              Timeout                                             0
              Requests.....................................

              Unknowntype                                         0
              Msgs.................................

              Other                                               0
              Drops.....................................
```

Related Commands

Platform Description

Parameter	Description

N/A	N/A

2.26. show radius group

Use this command to display RADIUS server group configuration.
show radius group

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Global configuration mode/Privileged EXEC mode/Interface configuration mode

Usage Guide
N/A

Configuration
The following example displays RADIUS server group configuration.

Examples

```
QTECH#show radius group
==========Radius group radius========== Vrf:not-set
Server:192.168.1.1
Server key:QTECH Authentication port:1812 Accounting port:1813 State:Active
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.27. show radius parameter

Use this command to display global RADIUS server parameters.

show radius parameter

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Global configuration mode/Privileged EXEC mode/Interface configuration mode

```
Usage Guide
N/A
```

Configuration Examples

The following example displays global RADIUS server parameters.

```
QTECH# show radius parameter Server Timout:   5 Seconds Server Deadtime: 0 Minutes Server
Retries: 3
Server Dead Critera: Time:10 Seconds
Tries: 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.28. show radius server

Use this command to display the configuration of the RADIUS server.

show radius server

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Global configuration mode/Privileged EXEC mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays the configuration of the RADIUS server.

```
QTECH# show radius server Server IP:    192.168.4.12
Accounting Port: 23
Authen  Port: 77
Test Username:      viven
Test Idle Time:            10 Minutes Test Ports:           Authen Server State:      Active
Current duration 765s, previous duration 0s Dead: total time 0s, count 0
Statistics:
Authen: request 15, timeouts 1
Author: request 0, timeouts 0
Account: request 0, timeouts 0
Server IP:    192.168.4.13
Accounting Port:  45
Authen  Port: 74
Test Username:      <Not Configured> Test Idle Time: 60 Minutes
Test Ports:         Authen and Accounting Server State:     Active
Current duration 765s, previous duration 0s


Dead: total time 0s, count 0 Statistics:
Authen: request 0, timeouts 0
Author: request 0, timeouts 0
```

```
Account: request 20, timeouts 0
```

Related Commands

Command	Description
radius-server host	Defines the RADIUS security server.
radius-server retransmit	Defines the number of RADIUS packet retransmissions.
radius-server key	Defines a shared password for the RADIUS server.
radius-server timeout	Defines the packet transmission timeout.

Platform Description

N/A

2.29. show radius vendor-specific

Use this command to display the configuration of the private vendors.

show radius vendor-specific

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide **N/A**

Configuration Examples

The following example displays the configuration of the private vendors.

```
QTECH#show radius vendor-specific id    vendor-specific     type-value

max-down-rate1

port-priority2

user-ip       3

vlan-id       4

last-supplicant-vers 5

ion
```

```
6   net-ip             6

7   user-name          7

8   password           8

9   file-directory     9

1   file-count         10
0

1   file-name-0        11
1

1   file-name-1        12
2

1   file-name-2        13
3

1   file-name-3        14
4

1   file-name-4        15
5

1   max-up-rate        16
6

current-supplicant-version 17

flux-max-high32     18

flux-max-low32      19

proxy-avoid  20

dialup-avoid 21

ip-privilege 22

login-privilege     42

ipv6-multicast-addre 79 ss

ipv4-multicast-addre 87

ss
```

Related Commands

Command	Description
radius-server host	Defines the RADIUS security server.
radius-server retransmit	Defines the number of RADIUS packet retransmissions.
radius-server key	Defines a shared password for the RADIUS server.
radius-server timeout	Defines the packet transmission timeout.

Platform Description

N/A

2.30. show radius attribute

Use this command to display standard Radius attributes.
show radius attribute

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Global configuration mode/Privileged EXEC mode/Interface configuration mode

Usage Guide **N/A**

Configuration Examples

The following example displays standard RADIUS attributes.

```
QTECH#sh radius attribute type   implicate
```

```
----   ---------
User-Name
User-Password
Chap-Password
NAS-Ip-Addr
Nas-Ip-Port
Service-Type
Framed-Protocol
Frame-Ip-Address
Framed-Ip-Mask
Framed-Routing
Filter-Id
Framed-Mtu
Framed-Compress
Login-Ip-Host
Login-Service
Login-Tcp-Port
Reply-Message
Callback-Num
Callback-Id
Framed-Route
Framed-IPX-Network
State
Class
Vendor-Specific
Session-Timeout
Idle-Timeout
Termination-Action
Called-Station-Id
Calling-Station-Id
Nas-Id
Proxy-State
Login-LAT-Service
Login-LAT-Node
Login-LAT-Group
Framed-AppleTalk-Link
Framed-AppleTalk-Net
Framed-AppleTalk-Zone
Acct-Status-Type
Acct-Delay-Time
Acct-Input-Octets
Acct-Output-Octets
Acct-Session-Id
Acct-Authentic
Acct-Session-Time
```

```
Acct-Input-Packet
Acct-Output-Packet
Acct-Terminate-Cause
Acct-Multi-Session-ID
Acct-Link-Count
Acct-Input-Gigawords
Acct-Output-Gigawords
Chap-Challenge
Nas-Port-Type
Port-Limit
Login-Lat-Port
Tunnel-Type
Tunnel-Medium-Type
Tunnel-Client-EndPoint
Tunnel-Service-EndPoint
79.........eap msg
80.    Message-Authenticator
81.........group id
85.    Acct-Interim-Interval
87.    Nas-Port-Id
89.    cui
Nas-Ipv6-Addr
Framed-Interface-Id
Framed-Ipv6-Prefix
Login-Ipv6-Host
Framed-Ipv6-Route
Framed-Ipv6-Pool
168.   Framed-Ipv6-Addr
```

Platform Description

N/A

3.1. aaa group server tacacs+

Use this command to configure different groups of TACACS+ server hosts.
Use the **no** form of this command to remove a specified TACACS server group.
aaa group server tacacs+ *group_name*
no aaa group server tacacs+ *group_name*

Parameter Description

Parameter	Description
group_name	TACACS+ server group name, which cannot be **radius** or **tacacs+** The two names are the built-in group name.

Defaults
No TACACS+ server group is configured.

Command Mode
Global configuration mode

Usage Guide

After you group different TACACS+ servers, the tasks of authentication, authorization and accounting can be implemented by different server groups.

Configuration Examples
The following example configures a TACACS+ server group named tac1, and configures a TACACS+ server with IP address 1.1.1.1 in this group:

```
QTECH(config)#aaa group server tacacs+ tac1
QTECH(config-gs-tacacs+)# server 1.1.1.1
```

Related Commands

Command	Description

server	Configures server list of TACACS+ server group.
ip vrf forwarding	Configures VRF name supported by TACACS+ server group.

Platform Description

N/A

3.2. ip tacacs source-interface

Use this command to use the IP address of a specified interface for all outgoing TACACS+ packets.

Parameter Description

Use the **no** form of this command to disable use of the specified interface IP address.

ip tacacs source-interface *interface-name*

no ip tacacs source-interface *interface-name*

Parameter	Description
interface-name	Interface for the outgoing TACACS+ packets

Defaults

The source IP address of TACACS+ packets is set on the network layer.

Command Mode

Global configuration mode

Usage Guide

To decrease the work of maintaining massive NAS messages in TACACS+ server, use this command to use the IP address of a specified interface for all outgoing TACACS+ packets.

This command specifies the primary IP address of the specified interface as the source address of TACACS+ packets on Layer 3 devices. If the specified interface is in a VRF instance, the route of this VRF instance is used for packet transmission.

Configuration Examples

Related Commands

Platform Description

The following example specifies the IP address of GigabitEthernet 0/0 for the outgoing TACACS+ packets.

```
QTECH(config)# ip tacacs source-interface gigabitEthernet0/0
```

Command	Description
tacacs-server host	Defines a TACACS+ server.
ip address	Configures the IP address of an interface.

N/A

3.3. ip oob

Use this command to specify the MGMT port used in the TACACS+ server group. Use the **no** form of this command to restore the default setting.

ip oob [**via** *mgmt_name*]

no ip oob

Parameter Description

Parameter	Description
mgmt_name	MGMT port name

Defaults

N/A

Command Mode

TACACS+ server group configuration mode

Usage Guide

Use the **aaa group server tacacs+** command to enter TACACS+ server group configuration mode.

No MGMT port is specified by default.

Configuration Examples

N/A

Platform Description

N/A

3.4. ip vrf forwarding

Use this command to configure the VRF used in the TACACS+ server group.

Use the **no** form of this command to remove the VRF configuration from the TACACS+ server group.

ip vrf forwarding *vrf-name*

no ip vrf forwarding

Parameter Description

Parameter	Description
vrf-name	VRF name

Defaults

N/A

Command Mode

TACACS+ server group configuration mode

Usage Guide

Before you configure this command, you need to use the **aaa group server tacacs+** command to enter TACACS+ server group configuration mode.

The VRF instance must exist and be configured with a correct VRF name through the **vrf definition** command.

Configuration Examples

The following example specifies the VRF instance named vpn1 for the TACACS+ server group:

```
QTECH(config)# aaa group server tacacs+ tac1 QTECH(config-gs-tacacs+)# server 1.1.1.1
QTECH(config-gs-tacacs+)# ip vrf forwarding vpn1
```

Related Commands

Command	Description
aaa group server tacacs+	Configures the TACACS+ server group.
server	Configures a server list of TACACS+ server group.

Platform Description

N/A

3.5. server

Use this command to configure the IP address of the TACACS+ server for the group server. Use the **no** form of this command to remove the TACACS+ server.

server { *ipv4-address* | *ipv6-address* }

no server { *ipv4-address* | *ipv6-address* }

Parameter Description

Parameter	Description
ipv4-address	IPv4 address of the TACACS+ server
ipv6-address	IPv6 address of the TACACS+ server

Defaults

No TACACS+ server is configured by default.

Command Mode

TACACS+ server group configuration mode

Usage Guide

You must configure the **aaa group server tacacs+** command before configuring this command. To configure server address in TACACS+ group server, you must use the **tacacs-server host** command in global configuration mode. If there is no response from the first host entry, the next host entry is tried.

Configuration Examples

The following example configures a TACACS+ server group named tac1 and TACACS+ server address 1.1.1.1 in this group.

```
QTECH(config)#aaa group server tacacs+ tac1
QTECH(config-gs-tacacs+)# server 1.1.1.1
```

Related Commands

Command	Description
aaa group server tacacs+	Configures a TACACS+ server group.

Platform Description

N/A

3.6. show tacacs

Use this command to display the TACACS+ server configuration.

show tacacs

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode/Global configuration/Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays the TACACS+ server configuration.

```
QTECH# show tacacs
Tacacs+ Server : 172.19.192.80/49 Socket Opens: 0
Socket Closes: 0 Total Packets Sent: 0 Total Packets Recv: 0
Reference Count: 0
```

Related Commands

Command	Description
tacacs-server host	Defines a TACACS+ secure server host.

Platform Description

N/A

3.7. tacacs-server host

Use this command to configure a TACACS+ host.

Use the **no** form of this command to remove the TACACS+ host.

tacacs-server host [**oob** [**via** *mgmt-name*]] {*ipv4-address* | *ipv6-address*} [**port** *integer*] [**timeout**

integer] [**key** [**0** | **7**] *text-string*]

no tacacs-server host { *ip-address* | *ipv6-address* }

Parameter Description

Parameter	**Description**
ip-address	IPv4 address of the TACACS+ host
ipv6-address	IPv6 address of the TACACS+ host
oob [via mgmt-name]	Specifies an MGMT port as the source port for TACACS+ communication.

port integer	Port number of the server. The range is from 1 to 65,535. The default is 49.
timeout *integer*	Timeout time of TACACS+ host. The range is from 1 to 1,000.
key *string*	Configures an authentication and encryption key. The value can be 0 or 7. 0 indicates no encryption, while 7 indicates simple encryption. The default is 0.

Defaults

No TACACS+ host is specified by default.

Command Mode

Global configuration mode

Usage Guide

The TACACS+ host must be configured to implement AAA security service You can use this command to configure one or multiple TACACS+ hosts.

Configuration Examples

Related Commands

Platform Description

The following example configures a TACACS+ host.

```
QTECH(config)# tacacs-server host 192.168.12.1
```

Command	Description
N/A	N/A

N/A

3.8. tacacs-server key

Use this command to configure the authentication encryption key used for TACACS+ communications between the access server and the TACACS+ server.

Use the **no** form of this command to remove the authentication encryption key.

tacacs-server key [**0** | **7**] *string*

no tacacs-server key

Parameter Description

Parameter	Description
string	Key string
0 | 7	Encryption type of key 0 indicates no encryption; 7 indicate simple encryption.

Defaults

No authentication encryption key is configured by default.

Command Mode

Global configuration mode

Usage Guide

Use command to configure a global authentication and encryption key for TACACS+ communication.

Use the **key** parameter in the **tacacs-server host** command to configure a server-based key.

Configuration Examples

Related Commands

Platform Description

The following example defines the authentication encryption key of TACACS+ server as aaa:

```
QTECH(config)# tacacs-server key aaa
```

Command	Description
tacacs-server host	Defines a TACACS+ host.

N/A

3.9. tacacs-server timeout

Use this command to set the interval for which the server waits for a server host to reply. Use the **no**

form of this command to restore the default timeout interval.

tacacs-server timeout *seconds*

no tacacs-server timeout

Parameter Description

Parameter	Description
seconds	Timeout interval in the range from 1 to 1,000 in the unit of seconds

Defaults

The default is 5 seconds.

Command Mode

Global configuration mode

Usage Guide

Use command to configure a global timeout interval. Use the **timeout** parameter in the **tacacs-server host** command to configure a server-based interval.

Configuration Examples

Related Commands

Platform Description

The following example configures the timeout interval to 10 seconds.

```
QTECH(config)# tacacs-server timeout 10
```

Command	Description
tacacs-server host	Defines a TACACS+ secure server host.

N/A

4.1. aaa authorization ip-auth-mode

Use this command to set the IP authorization mode.
aaa authorization ip-auth-mode { disable | supplicant | radius-server | dhcp-server | mixed }

Parameter Description

Parameter	Description
disable	Disables IP authorization mode.
supplicant	Enables suppliant authorization mode.
radius-server	Enables Radius server authorization mode.
dhcp-server	Enables DHCP server authorization mode.
mixed	Enables mixed authorization mode.

Defaults
IP authorization mode is disabled by default.

Command mode
Global configuration mode

Usage Guide
Supplicant authorization mode supports only QTECH supplicant.
Radius-server authorization mode requires the server to allocate IP addresses by framed-ip. DHCP-server authorization mode requires the server to enable DHCP snooping or DHCP relay. Mixed authorization mode supports multiple authorization methods.

Configuration Examples

Related Commands

Platform Description

The following example enables suppliant authentication mode.

```
QTECH(config)# aaa authorization ip-auth-mode supplicant
```

Command	Description
show running-config	Displays the IP authentication mode.

N/A

4.2. clear dot1x user all

Use this command to clear all the 802.1X authentication users.
clear dot1x user all

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode

Privileged EXEC mode

Usage Guide Use this command to clear all the 802.1X authentication users.

Configuration Examples

Related Commands

Platform Description

The following example clears all the 802.1X authentication users.

```
QTECH#clear dot1x user all
```

Command	Description
N/A	N/A

N/A

4.3. clear dot1x user mac

Use this command to clear 802.1X authentication users according to MAC addresses.

clear dot1x user mac *mac-addr*

Parameter Description

Parameter	Description
mac-addr	MAC address

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to clear 802.1X authentication users according to MAC addresses.

Configuration Examples

Related Commands

Platform Description

The following example clears an 802.1X authentication user whose MAC address is 0012.3456.789A.

```
QTECH#clear dot1x user mac 0012.3456.789A
```

Command	**Description**
N/A	N/A

N/A

4.4. clear dot1x user name

Use this command to clear the 802.1 X authentication users according to the username.

clear dot1x user name *name-str*

Parameter Description

Parameter	Description
name-str	The username of the 802.1X authentication user

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to clear the 802.1 X authentication users according to the username.

Configuration Examples

Related Commands

Platform Description

The following example clears the 802.1X authentication user named 802.1X-user.

```
QTECH#clear dot1x user name dot1x-user
```

Command	Description
N/A	N/A

N/A

4.5. clear dot1x user ip

Use this command to clear 802.1X authentication users according to IP addresses.

clear dot1x user ip *ip-addr*

Parameter Description

Parameter	Description
ip-addr	IP address

Defaults
N/A

Command Mode
Privileged EXEC mode

Usage Guide
Use this command to clear 802.1X authentication users according to IP addresses.

Configuration Examples

The following example clears an 802.1X authentication user whose IP address is 11.1.1.1.

```
QTECH#clear dot1x user ip 11.1.1.1
```

Platform Description

N/A

4.6. dot1x accounting

Use this command to configure the accounting list.

dot1x accounting *list-name*

Parameter Description

Parameter	Description
list-name	The name of the accounting list

Defaults
N/A

Command Mode

Global configuration mode/WLAN security configuration mode

Usage Guide If

AAA does not adopts 802.1X accounting as the default accounting method.

Use this command to configure the 802.1X accounting method.

Configuration in WLAN security configuration mode is prior to that in global configuration mode.

Configuration Examples

Related Commands

Platform Description

The following example configures the accounting list.

```
QTECH(config)# dot1x accounting dot1x-acct
```

Command	Description
N/A	N/A

N/A

4.7. dot1x acct-update base-on first-time server

Use this command to assign the accounting update interval for the first authentication. Use the **no** form of this command to restore the default settings.

dot1x acct-update base-on first-time server

no dot1x acct-update base-on first-time server

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The assignment is disabled by default.

Command Mode

Global configuration mode

Usage Guide

Some portal servers do not support the assignment of accounting update interval during re-authentication.

Use this command if such servers demand users to issue accounting update packets according to the interval in the first authentication.

Configuration Examples

The following example assigns the accounting update interval for the first authentication.

```
QTECH(config)# dot1x acct-update base-on first-time server
```

Platform Description

N/A

4.8. dot1x auth-fail max-attempt

Use this command to set the maximum auth-attempts.

Use the **no** form of this command to restore the default setting.

`dot1x auth-fail max-attempt` ***value***

no dot1x auth-fail max-attempt

Parameter Description

Parameter	Description
value	The maximum auth-attempts

Defaults

The default is 3.

Command Mode

Global configuration mode

Usage Guide

Use the **show dot1x** command to adjust the maximum authentication attempts for those failed users.

Configuration Examples

Related Commands

Platform Description

The following example sets the maximum auth-attempts to 2.

```
QTECH(config)# dot1x auth-fail max-attempt 2
```

Command	Description

show dot1x	Displays the 802.1x configuration.

N/A

4.9. dot1x auth-mode

Use this command to specify the 802.1X authentication mode.

```
dot1x auth-mode { eap | chap | pap }
```

Parameter Description

Parameter	Description
eap	Enables EAP-MD5 authentication mode.
chap	Enables CHAP authentication mode.
pap	Enables PAP authentication mode.

Defaults

The default is EAP-MD5 authentication mode.

Command Mode

Global configuration mode

Usage Guide

The selection of authentication mode depends on the suppliant and portal server.

Configuration Examples

Related Commands

Platform Description

The following example enables CHAP authentication mode.

```
QTECH(config)# dot1x auth-mode chap
```

Command	Description

show dot1x	Displays the 802.1X information.

N/A

4.10. dot1x auth-address-table address

Use this command to configure the authentication address table.

dot1x auth-address-table address *mac-addr* **interface** *interface*

Parameter Description

Parameter	Description
mac-addr	The MAC address of the authentication host
interface	The interface of the authentication host

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

Only the specified interface with the specified MAC address is able to pass the 802.1x authentication.

Configuration Examples

The following example configures the authentication address table.

```
QTECH(config)# dot1x auth-address-table 00d0.f800.0cb2 interface
fastethernet 0/1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.11. dot1x authentication

Use this command to configure the authentication method list.

dot1x authentication *list-name*

Parameter Description

Parameter	Description
list-name	Authentication method list

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

If AAA does not adopt the default 802.1X authentication, use this command to configure the 802.1X authentication method.

Configuration Examples

Related Commands

Platform Description

The following example configures the authentication method list

```
QTECH(config)# dot1x authentication dot1x-authen
```

Command	Description
N/A	N/A

N/A

4.12. dot1x auto-req

Use this command to configure auto-request 802.1X authentication. Use the **no** form of this command to restore the default setting. **dot1x auto-req**

no dot1x auto-req

Parameter Description

Parameter	Description
N/A	N/A

Defaults
This function is disabled by default.

Command Mode
Global configuration mode

Usage Guide

Enable this function for MAB. If the authentication agent is already in the terminal system, enable it by clicking.

Configuration Examples

Related Commands

Platform Description

The following example enables auto-request 802.1X authentication.

```
QTECH(config)# dot1x auto-req
```

Command	Description
show dot1x auto-req	Displays the automatic authentication request information.

N/A

4.13. dot1x auto-req packet-num

Use this command to set the number of auto-request authentication packets.

```
dot1x auto-req packet-num num
```

Parameter Description

Parameter	Description
num	The number of auto-request authentication packets in the range from 0 to 1,000,000

Defaults
The default is 0.

Command Mode

N/A

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example sets the number of auto-request authentication packets to 100.

```
QTECH(config)# dot1x auto-req packet-num 100
```

Command	Description
show dot1x auto-req	Displays the authentication request information.

N/A

4.14. dot1x auto-req req-interval

Use this command to set the auto-request authentication interval.

```
dot1x auto-req req-interval time
```

Parameter Description

Parameter	Description

time	The auto-request authentication interval, in the range from 10 to 3,600 in the unit of seconds

Defaults
The default is 30 seconds.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example sets the auto-request authentication interval to 50 seconds.

```
QTECH(config)# dot1x auto-req req-interval 50
```

Command	Description
show dot1x auto-req	Displays the authentication request information.

N/A

4.15. dot1x auto-req user-detect

Use this command to enable online user detection for auto-request authentication. Use the **no** form of this command to disable this function.

```
dot1x auto-req  user-detect no dot1x auto-req user-detect
```

Parameter Description

Parameter	Description
N/A	N/A

Defaults
This function is enabled by default.

Command Mode
Global configuration mode

`Usage Guide` **`N/A`**

Configuration Examples

Related Commands

Platform Description

The following example enables online user detection for auto-request authentication.

```
QTECH(config)# dot1x auto-req user-detect
```

Command	Description
show dot1x auto-req	Displays the authentication request information.

N/A

4.16. dot1x client-probe enable

Use this command to enable online user probe function.

Use the **no** form of this command to restore the default setting.

dot1x client-probe enable no do1x client-probe enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults
This function is disabled by default.

Command Mode
Global configuration mode

Usage Guide

Use this command to enable online user probe function.

Configuration Examples

Related Commands

Platform Description

The following example enables online user probe function.

```
QTECH(config)# dot1x client-probe enable
```

Command	Description
show dot1x	Displays 802.1X configuration.

N/A

4.17. dot1x critical

Use this command to enable the server IAB (Inaccessible Authentication Bypass) on the port. Use the **no** form of this command to restore the default setting.

dot1x critical no dot1x critical

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This functions is disabled by default.

Command Mode

Interface configuration mode/VXLAN mode

Usage Guide

With the IAB function enabled on the port, if there is only RADIUS

authentication method in the 802.1X authentication method list and all RADIUS servers in this method list take no effect, the switch will set the network accessing authority for users by the IAB method, and send the EAPOL-SUCCESS packets to the users.

Except for the RADIUS authentication method, if there are other authentication methods in the 802.1X authentication method list, the IAB function will take no effect. (Such as the **aaa authentication dot1x default group radius none,** there exists none authentication method after the RADIUS authentication method.

For the users of IAB authorized, as the user identity legality cannot be checked, no matter whether the accounting function is configured, they will not send the accounting request.

With the AAA multi-domain authentication enabled globally, the 802.1X user authentication will not use the globally configured method list. After all RADIUS servers in the 802.1X globally configured method list are checked to be invalid, the IAB will directly send the successful authentication to the user with no need to enter the username, the AAA multi-domain authentication on this port is useless.

Configuration Examples

Related Commands

Platform Description

The following example enables the server IAB (Inaccessible Authentication Bypass) function on the port.

```
QTECH(config-if-GigabitEthernet 0/5)#dot1x critical
```

Command	Description
N/A	N/A

N/A

4.18. dot1x critical recovery action reinitialize

Use this command to allow IAB users under the port to reinitialize authentication when the server has recovered.

Use the **no** form of this command to restore the default setting.

dot1x critical recovery action reinitialize

no dot1x critical recovery action reinitialize

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode/VXLAN mode

Usage Guide

After the port entering the inaccessible authentication bypass status, if the RADIUS server returns to normal, you need to reinitialize the authentication for all users that have accomplished the network access authorization through the inaccessible authentication bypass on ports in order to ensure the user legality.

Configuration Examples

The following example allows IAB users under the port to reinitialize authentication when the server has recovered.

```
QTECH(config-if-GigabitEthernet 0/5)#dot1x critical recovery action
reinitialize
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.19. dot1x critical vlan

Use this command to configure the port in IAB status to jump to a specified auth-fail VLAN. Use the **no** form of this command to disable this function.

```
dot1x critical  vlan no dot1x critical vlan
```

Parameter Description

Parameter	Description
vlan-id	The VLAN where the port will jump

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode/VXLAN mode

Usage Guide

With this function enabled, if no user authentication is performed on the ports initially, after all RADIUS servers are invalidated, the user will initiate the authentication and the port will enter the IAB status and to be added to the VLAN configured. If this function is disabled, the VLAN of the port is not changed when the port is in the IAB status.

Configuration Examples

Related Commands

Platform Description

The following example configures the port in IAB status to jump to a specified auth-fail VLAN.

```
QTECH(config-if-GigabitEthernet 0/5)#dot1x critical vlan10
```

Command	Description

N/A	N/A

N/A

4.20. dot1x dbg-filter

Use this command to enable debug information print for a user with a specified MAC address. Use the **no** form of this command to clear the debug information.

dot1x dbg-filter *H.H.H*

```
no dot1x dbg-filter H.H.H
```

Parameter Description

Parameter	Description
H.H.H	The MAC address of a user

Defaults

Debug information of all authentication users is printed by default.

Command mode

Global configuration mode

Usage Guide

Use this command to print the debug information of a specific user If you want to locate the fault on the network where there are multiple users.

Configuration Examples

Related Commands

Platform Description

The following example prints the debug information of the device with the specified MAC address.

```
QTECH(config)# dot1x dbg-filter 00d0.f800.0001
```

Command	Description
N/A	N/A

N/A

4.21. dot1x default-user-limit

Use this command to set the maximum auth-user number on controlled interfaces. Use the **no** form of this command to restore the default setting.

`dot1x default-user-limit` ***num***

no dot1x default-user-limit

Parameter Description

Parameter	Description
num	**The maximum auth-user number allowed by a controlled interface, in the range from 1 to 1,000,000**

Defaults

The default is 1,000,000.

Command mode

Interface configuration mode/ VXLAN mode

Usage Guide

This command is used to limit the number of users to be authenticated on a specific port.

Configuration Examples

Related Commands

Platform Description

The following example sets the maximum auth-user number on a controlled interface.

```
QTECH(config-if)# dot1x default-user-limit 10
```

Command	Description

show dot1x port-control interface fastEthernet 0/10	**Displays the number of users allowed by a specific 802.1X interface.**
show dot1x port-control interface fastEthernet 0/10	**Displays the number of users allowed by a specific 802.1X interface.**

N/A

4.22. dot1x default

Use this command to restore 802.1X configuration to the default setting.

dot1x default

Parameter Description

Parameter	Description
N/A	**N/A**

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

This command is used to restore 802.1X configuration for quick re-configuration.

Configuration Examples

Related Commands

Platform Description

The following example restores 802.1X configuration to the default setting.

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

Command	Description
show dot1x	**Displays the 802.1X information.**

N/A

4.23. dot1x get-static-ip enable

Use this command to obtain static IP addresses.
dot1x get-static-ip enable

Use this command to restore the default setting.
no dot1x get-static-ip enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults
This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide
Enable this function when wireless terminals use static IP addresses and need to upload the static IP addresses to the server.
Note that the IP addresses are uploaded to the server via accounting packets. In addition, when static IP addresses are used, terminal identification information is not provided.

Configuration Examples
The following example obtains static IP addresses.

```
QTECH(config)# dot1x get-static-ip enable
```

Platform Description

This command is supported only on wireless products.

4.24. dot1x mab-username upper

Use this command to enable uppercase letters in MAB user names.

dot1x mab-username upper

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode.

Usage Guide

By default, lowercase letters are used in the user name of MAB. After this function is enabled, uppercase letters are used in new user names of MAB to meet server requirements.

Configuration Examples

Related

The following example enables uppercase letters in MAB user names.

```
QTECH(config)# dot1x mab-username upper
```

Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.25. dot1x mac-auth-bypass

Use this command to configure single MAB authentication. Use the **no** form of this command to restore the default setting. **dot1x mac-auth-bypass**

no dot1x mac-auth-bypass

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

Use this command on a single dumb terminal.

Configuration Examples

Related Commands

Platform Description

The following example configures single MAB authentication.

```
QTECH(config-if-GigabitEthernet 0/0)# dot1xmac-auth-bypass
```

Command	Description
show dot1x port-control interface	**Displays the information about 802.1X on the interface.**

N/A

4.26. dot1x mac-auth-bypass multi-user

Use this command to configure multiple MAB authentications. Use the **no** form of this command to restore the default setting. **dot1x mac-auth-bypass multi-user**

no dot1x mac-auth-bypass multi-user

Parameter Description

Parameter	Description
N/A	N/A

Defaults
This function is disabled by default.

Command Mode

Interface configuration mode/VXLAN mode

Usage Guide

Use this command when the interface is connected with multiple dumb terminals.

Configuration Examples

Related Commands

Platform Description

The following example configures multiple MAB authentications.

```
QTECH(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypassmulti-user
```

Command	Description
N/A	N/A

N/A

4.27. dot1x mac-auth-bypass timeout-activity

Use this command to set the MAB authentication timeout interval.

`dot1x mac-auth-bypass timeout-activity` ***time***

no dot1x mac-auth-bypass timeout-activity

Parameter Description

Parameter	Description

time	**The online time, in the range from 1 to 65,535 in the unit of seconds**

Defaults

The default is 0 second.

Command Mode

Interface configuration mode/VXLAN mode

Usage Guide

Use this command to set the MAB authentication timeout interval for dumb terminals.

Configuration Examples

The following example sets the MAB authentication timeout interval.

```
QTECH(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass
timeout-activity 3600
```

Related Commands

Command	Description
show dot1x port-control interface	**Displays the 802.1X information.**
show dot1x port-control interface	**Displays the 802.1X information.**

Platform Description

N/A

4.28. dot1x mac-auth-bypass violation

Use this command to configure the MAB violation.

Use the **no** form of this command to restore the default setting.

dot1x mac-auth-bypass violation

no dot1x mac-auth-bypass violation

Parameter Description

Parameter	Description

N/A	**N/A**

Defaults
This function is disabled by default.

Command Mode
Interface configuration mode

Usage Guide

This command is used to configure the MAB violation on the port with only one dumb terminal in single MAB environment.

Configuration Examples

Related Commands

Platform Description

The following example configures the MAB violation.

```
QTECH(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypassviolation
```

Command	Description
show dot1x port-control interface	**Displays the 802.1X information.**

N/A

4.29. dot1x mac-auth-bypass vlan

Use this command to configure the MAB VLAN function.
Use the **no** form of this command to restore the default setting.
dot1x mac-auth-bypass vlan *vlan-list*
no dot1x mac-auth-bypass vlan *vlan-list*

Parameter Description

Parameter	Description

vlan-list	**Configures the MAB VLANs.**

Defaults
This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

Use this command to allow users within specified VLANs on the port to perform MAB authentication.

Configuration Examples

The following example configures MAB VLANs.

```
QTECH(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass vlan5，8-20
```

Related Commands

Command	Description
N/A	**N/A**

Platform Description

N/A

4.30. dot1x max-req

Use this command to set the maximum attempts of authentication requests.

```
dot1x max-req num
```

Parameter Description

Parameter	Description
num	**Maximum attempts**

Defaults
The default is 3.

Command Mode

Global configuration mode

Usage Guide

Use the **show dot1x** command to display the 802.1X configuration.

Configuration Examples

Related Commands

Platform Description

The following example sets the maximum attempts of authentication requests to 2.

```
QTECH(config)# dot1x max-req 2
```

Command	Description
show dot1x	**Displays the information about 802.1X.**

N/A

4.31. dot1x multi-account enable

Use this command to enable the user with one single MAC address to perform authentication with multiple accounts.

Use the **no** form of this command to restore the default setting.

```
dot1x multi-account  enable no dot1x multi-account enable
```

Parameter Description

Parameter	Description
N/A	**N/A**

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

Use the command to enable the multiple-account authentication if you want to

switch the username in the authentication or re-authentication, especially in the windows domain authentication.

Configuration Examples

Related Commands

Platform Description

The following example enables the multiple-account authentication.

```
QTECH(config)# dot1x multi-account enable
```

Command	Description
N/A	N/A

N/A

4.32. dot1x multi-mab quiet-period

Use this command to set the quiet time after the multiple MAB authentication failure.

```
dot1x multi-mab quiet-period time
```

Parameter Description

Parameter	Description
time	Sets the quiet period after the multiple MAB authentication failure, in the range from 0 to 65,535 in the unit of seconds.

Defaults

The default is 0 second, indicating no quiet period.

Command Mode

Global configuration mode

Usage Guide

The default setting is recommended.

Configuration Examples

Related Commands

The following example sets the quiet period after the multiple MAB authentication failure to 2 seconds.

```
QTECH(config)# dot1x multi-mab quiet-period 2
```

Command	Description
N/A	N/A

Platform Description

N/A

4.33. dot1x mab-username format

Use this command to configure the MAB authentication user name format. Use the **no** form of this command to restore the default setting.

dot1x mab-username format [with-dot | with-colon | with-hyphen] no dot1x mab-username format

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, this function is disabled.

Command Mode

Global configuration mode

Usage Guide

dot1x mab-username format with-dot is used to configure the MAB authentication user name format xxxx.xxxx.xxxx.

dot1x mab-username format with-colon is used to configure the MAB authentication user name format xx:xx:xx:xx:xx:xx.

dot1x mab-username format with-hyphen is used to configure the MAB authentication user name format xx-xx-xx-xx-xx-xx.

Configuration Examples

The following example configures the MAB authentication user name format.

```
QTECH(config)# dot1x mab-username formatwith-hyphen
```

Platform Description

N/A

4.34. dot1x port-control auto

Use this command to configure the 802.1X authentication on the port. Use the **no** form of this command to restore the default setting.

dot1x port-control auto no dot1x port-control

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode/VXLAN mode

Usage Guide

Use the **show dot1x** command to display the 802.1X configuration.

Configuration Examples

Related Commands

Platform Description

The following example configures the 802.1X authentication on the port.

```
QTECH(config-if-GigabitEthernet 0/0)# dot1x port-controlauto
```

Command	Description

show dot1x	**Displays the 802.1X information.**

N/A

4.35. dot1x port-control-mode

By default, 802.1x adopts MAC address-based control mode. In this mode, only authenticated users have access to the network, while other users that connect to the same port cannot access the network. In the port-based control mode, however, if one user that connects to the port passes the authentication, this port becomes an authenticated port and all the users that connect to this port have access to the network. In the port-based single-user control mode, the port is authenticated when it allows only one authenticated user who is enable to use the network normally. If you find other users on the port, you should clear all the users on the port and re-authenticate. The authentication mode can be configured using the following commands

dot1x port-control-mode { mac-based | port-based | port-based single-host} no dot1x port-control-mode

Parameter Description

Parameter	Description
mac-based	**Enable the MAC address-based control.**
port-based	**Enable port-based control.**
port-based single-host	**Enable single host-based control.**

Defaults

MAC address-based access control is used by default.

Command Mode

Interface configuration mode.

Usage Guide

Use the **show dot1x port-control** command to show the 802.1X configuration for the port. Single-host is port-based single-user 802.1x access control. Use **show dot1x port-control** to display port-based and use **show running-config** to display dot1x

port-control-mode port-based single-host. Since single-host only supports the single-user form, setting default-user-limit on the port manually does not take effect in single-host mode. If you set default-user-limit on the port after setting single-host, only one user can be permitted to use the network still.

Configuration Examples

Related Commands

Platform Description

The following example sets the port to participate in authentication and enable port-based authentication.

QTECH(config-if-GigabitEthernet 0/0)# dot1x port-control-mode port-based

Command	Description
show dot1x port-control	**Displays the port control mode.**
Show running-config	**Displays the configuration.**

N/A

4.36. dot1x probe-timer interval

Use this command to set the QTECH terminal detection interval.

`dot1x probe-timer interval` ***time***

Parameter Description

Parameter	Description
time	**Terminal detection interval in the range from 1 to 65,535 in the unit of seconds**

Defaults

The default is 20 seconds.

Command Mode

Global configuration mode

Usage Guide

The default setting is recommended.

Configuration Examples

Related Commands

Platform Description

The following example sets QTECH terminal detection interval to 30 seconds.

```
QTECH(config)# dot1x probe-timer interval 30
```

Command	Description
N/A	N/A

N/A

4.37. dot1x probe-timer alive

Use this command to set the QTECH terminal alive interval.

```
dot1x probe-timer alive time
```

Parameter Description

Parameter	Description
time	Terminal alive interval, in the range from 1 to 65,535 in the unit of seconds

Defaults

The default is 250 seconds.

Command Mode

Global configuration mode

Usage Guide

If the device does not receive the probe packet from the terminal when the terminal alive interval expires, the device is considered offline. The default setting is recommended.

Configuration Examples

Related Commands

Platform Description

The following example sets QTECH terminal alive interval to 120 seconds.

```
QTECH(config)# dot1x probe-timer alive 120
```

Command	Description
N/A	N/A

N/A

4.38. dot1x private-supplicant-only

Use this command to filter non-QTECH clients.

Use the **no** form of this command to restore the default setting.

```
dot1x private-supplicant-only
```

no dot1x private-supplicant-only

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function disabled by default.

Command Mode

Global configuration mode

Usage Guide

This command is used for authentication supporting only QTECH clients.

Configuration Examples

Related Commands

The following example filters non-QTECH clients.

```
QTECH(config)# dot1x private-supplicant-only
```

Command	Description

show dot1x private-supplicant-only	Displays the information about the private supplicant.

Platform

N/A

Description

4.39. dot1x pseudo source-mac

Use this command to use a virtual MAC address as the source MAC address of the 802.1X packets sent by the device.

Use the **no** form of this command to restore the default setting.

```
dot1x pseudo  source-mac no dot1x pseudo source-mac
```

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command Mode

Global configuration mode

Usage Guide

By default, the device uses its own MAC address as the source MAC address of the EAP packets for the 802.1X authentication. Some versions of the QTECH supplicant judge whether the access device is a QTECH device based on the source MAC address of the EAP packets. If the access device is a QTECH device, the supplicant device performs some private features. Configure this command if you want to enable these features.

Configuration Examples

Related Commands

Platform Description

The following example uses the virtual MAC address as the source MAC address of the 802.1X packets sent by the device:

```
QTECH(config)# dot1x pseudo source-mac
```

Command	Description
N/A	N/A

N/A

4.40. dot1x redirect

Use this command to enable the second generation SU upgrade function. Use the **no** form of this command to restore the default setting.

```
dot1x redirect
```

no dot1x redirect

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

Redirect to the supplicant software download website through the browser. See *Web Authentication Configuration Guide* for details about parameters.

Configuration Examples

Related Commands

Platform Description

The following example enables the second generation SU upgrade function,

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

Command	Description
N/A	N/A

N/A

4.41. dot1x reauth-max

Use this command to set the maximum re-auth attempts.

`dot1x reauth-max num`

no dot1x reauth-max

Parameter Description

Parameter	Description
num,	Maximum re-auth attempts. The range is from 1 to 10.

Defaults
The default is 3.

Command Mode

Global configuration mode

Usage Guide

Use this command to specify the maximum number of supplicant re-authentications. Use the **show dot1x** command to display 802.1X configuration.

Configuration Examples

Related Commands

Platform Description

The following example sets the maximum re-auth attempts to 2.

```
QTECH(config)# dot1x reauth-max 2
```

Command	Description
show dot1x	Displays the 802.1X information.

N/A

4.42. dot1x re-authentication

Use this command to enable timed re-authentication function. Use the **no** form of the command to restore the default setting. **dot1x re-authentication**

```
no dot1x re-authentication
```

Parameter Description

Parameter	Description
N/A	N/A

Defaults
This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

This command will re-authenticate the supplicant periodically after he passes the authentication. Use the **show dot1x** command to display 802.1X configuration. The default setting is recommended.

Configuration Examples

Related Commands

Platform Description

The following example enables timed re-authentication function.

```
QTECH(config)# dot1x re-authentication
```

Command	Description
show dot1x	Displays the 802.1X information.

N/A

4.43. dot1x stationarity enable

In the port-based 802.1X control mode, dynamic users can transit freely among the ports by default. Use this command to prevent users from transition.

Use the **no** form of this command to restore the default setting.

```
dot1x stationarity  enable no dot1x stationarity enable
```

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

This command must be configured before user authentication. Otherwise, you need re-authenticate all the users.

Configuration Examples

Related Commands

Platform Description

The following example prevents the user from transiting from 802.1X port to other port.

```
QTECH(config)# dot1x stationarity enable
```

Command	Description
N/A	N/A

N/A

4.44. dot1x timeout re-authperiod

Use this command to set the re-authentication interval when re-authentication is enabled.

```
dot1x timeout re-authperiod time
```

Parameter Description

Parameter	Description
time	Authentication interval, in the range from 1 to 65,535 in the unit of seconds.

Defaults

The default is 3,600 seconds.

Command Mode

Global configuration mode

Usage Guide

Use the **show dot1x** command to display the 802.1X configuration.

Configuration Examples

Related Commands

Platform Description

The following example sets the re-authentication interval to 2,400 seconds.

```
QTECH(config)# dot1x timeout re-authperiod 2400
```

Command	Description
show dot1x	Displays the information about 802.1X.

N/A

4.45. dot1x timeout quiet-period

Use this command to set the quiet period when authentication fails.

`dot1x timeout quiet-period` ***time***

Parameter Description

Parameter	Description
time	Quiet period, in the range from 1 to 65,535 in the unit of seconds.

Defaults

The default is 10 seconds.

Command Mode

Global configuration mode

Usage Guide

The default value is recommended.

Configuration Examples

Related Commands

Platform Description

The following example sets the quiet period after failed authentication.

```
QTECH(config)# dot1x timeout quiet-period 60
```

Command	Description
N/A	N/A

N/A

4.46. dot1x timeout supp-timeout

Use this command to set the authentication timeout between the device and the supplicant.

```
dot1x timeout supp-timeout time
```

Parameter Description

Parameter	Description
time	Authentication timeout between the device and the supplicant The range is from 1 to 65,535 seconds.

Defaults

The default is 3 seconds.

Command Mode

Global configuration mode

Usage Guide

Use the **show dot1x** command to show display 802.1X configuration.

Configuration Examples

The following example sets the authentication timeout between the device and the supplicant to 10s:

```
QTECH(config)# dot1x timeout supp-timeout 10
```

Related Commands

Command	Description
show dot1x	Displays the information about 802.1x.

Platform Description

N/A

4.47. dot1x timeout server-timeout

Use this command to set the server timeout interval.

```
dot1x timeout server-timeout time
```

Parameter Description

Parameter	Description
time	The server timeout interval, in the range from 1 to 65,535 in the unit of seconds

Defaults
The default is 5 seconds.

Command Mode

Global configuration mode

Usage Guide

By default, the timeout of the 802.1X server is less than that of the Radius server. Use this command to raise the 802.1X timeout so as to exceed the Radius value. For details, see *Configuration Guide*.

Configuration Examples

Related Commands

Platform Description

The following example set the server timeout interval to 10 seconds.

```
QTECH(config)# dot1x timeout server-timeout 10
```

Command	Description
show dot1x	Displays the 802.1X information.

N/A

4.48. dot1x timeout tx-period

Use this command to set the request/id packet re-transmission interval.

```
dot1x timeout tx-period time
```

Parameter Description

Parameter	Description
time	The request/id packet re-transmission interval, in range from 1 to 65,535 in the unit of seconds

Defaults

The default is 3 seconds for switches, and 4 seconds for wireless devices.

Command Mode

Global configuration mode

Usage Guide

Use the **show dot1x** command to display 802.1X configuration.

Configuration Examples

Related Commands

Platform Description

The following example sets the request/id packet re-transmission interval to 5 seconds.

```
QTECH(config)# dot1x timeout tx-period 5
```

Command	Description
show dot1x	Displays the information about 802.1X.

N/A

4.49. dot1x valid-ip-acct enable

Use this command to enable IP address-triggered accounting. Use the **no** form of this command to restore the default setting. **dot1x valid-ip-acct enable**

no dot1x valid-ip-acct enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults
This function is disabled by default.

Command Mode
Global configuration mode

Usage Guide
Use this command to enable accounting only when users obtain valid IP addresses.

Configuration Examples
The following example enables IP address-triggered accounting.

```
QTECH(config)#dot1x valid-ip-acct enable
```

Platform Description
N/A

4.50. dot1x valid-ip-acct timeout

Use this command to configure IP address-triggered accounting timeout. Use the **no** form of this command to restore the default setting.

`dot1x valid-ip-acct timeout` ***time***

no dot1x valid-ip-acct timeout

Parameter Description

Parameter	Description
time	IP address-triggered accounting timeout in the unit of minutes

Defaults
The default is 5 minutes.

Command Mode

Global configuration mode

Usage Guide

The SNMP server will not start accounting until users obtain IP addresses. In this case, use this command to configure the IP address-triggered accounting timeout.

Configuration Examples

The following example configures IP address-triggered accounting timeout.

```
QTECH(config)# dot1x valid-ip-acct timeout 10
```

Platform Description

N/A

4.51. dot1x system disable

Use this command to disable global 802.1x. Use the **no** form of this command to restore the default settings.

```
dot1x system  disable no dot1x system disable
```

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, global 802.1x is enabled.

Command Mode

Global configuration mode

Usage Guide

(Optional) When the server is unreachable, disable global 802.1x, so users can access the Internet without authentication. After the server resumes reachability, enable global 802.1x, and users have to pass authentication before accessing the Internet.

Configuration Examples

Related Commands

The following example disables global 802.1x.

```
QTECH(config)# dot1x system disable
```

Command	Description
N/A	N/A

Platform Description

N/A

4.52. show dot1x

Use this command to display the 802.1X setting.

show dot1x

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays the 802.1X setting.

```
QTECH#show dot1x



802.1X basic information:
802.1X Statusenable
Authentication Mode eap
Authorization mode  disable
Total User Number ..................... 0 (exclude dynamic user) Authenticated User Number
..... 0 (exclude dynamic user) Dynamic User Number 0
Re-authentication   disable
Re-authentication Period ..... 3600 seconds
Re-authentication max ..... 3 times Quiet Period ..... 10
seconds
Tx Period ..... 30 seconds
Supplicant Timeout ..... 3 seconds
Server Timeout ..... 5 seconds
Maximum Request ..... 3 times
Client Online Probe disable
Eapol Tag    enable
802.1x redirect     disable
Private supplicant only    disable
```

Related Commands

Command	Description
dot1x auth-mode	Sets the 802.1X authentication mode.
dot1x max-req	Sets the maximum number of authentication request
	re-transmissions.
dot1x port-control auto	Sets the port to participate in authentication.

dot1x reauth-max	Sets the maximum number of the supplicant re-authentications.
dot1x re-authentication	Sets the re-authentication attribute.
dot1x timeout quiet-period	Sets the time the device waits before re-authentication.
dot1x timeout re-authperiod	Sets the re-authentication period for the supplicant.
dot1x timeout server-timeout	Sets the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Sets the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Sets the re-transmission interval.

Platform Description

N/A

4.53. show dot1x auth-address-table

Use this command to display 802.1X authentication address table.

show dot1x auth-address-table [**address** *addr* | **interface** *interface*]

Parameter Description

Parameter	Description
addr	Physical IP address that can be authenticated
interface	Interface number

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays the 802.1X authentication address table.

```
QTECH #show Interface   dot1x auth-address-
                        table Address

Fa0/1 Fa0/2             00d0.f800.0c0e
                        001a.c800.0102
QTECH #show Interface

                        dot1x auth-address    interface   fastEthernet   0/1
                        -table Address

Fa0/1                   00d0.f800.0c0e
```

```
QTECH       dot1x    auth-address-   addre   00d0.f8.00.0c0e
#show       table Address            ss
Interface


Fa0/1       00d0.f800.0c0e
```

Related Commands

Command	Description
dot1x auth-mode	Sets the 802.1x authentication mode.
dot1x max-req	Sets the maximum number of authentication request re-transmissions.
dot1x port-control auto	Sets the port to participate in authentication.
dot1x reauth-max	Sets the maximum number of the supplicant re-authentications.
dot1x re-authentication	Sets the re-authentication attribute.
dot1x timeout quiet-period	Sets the time the device waits before re-authentication.

dot1x timeout re-authperiod	Sets the re-authentication period for the supplicant.
dot1x timeout server-timeout	Sets the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Sets the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Sets the re-transmission interval.

Platform Description

N/A

4.54. show dot1x auto-req

Use this command to display the auto-request authentication information.
show dot1x auto-req

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide **N/A**

Configuration Examples

The following example displays the auto-request authentication information.

```
QTECH# show dot1x auto-req Auto-Req: Enabled
User-Detect : Enabled
Packet-Num : 0
```

Related Commands

Platform Description

Req-Interval: 30 Seconds

Command	Description
dot1x auth-mode	Sets the 802.1X authentication mode.
dot1x max-req	Sets the maximum number of authentication request re-transmissions.
dot1x port-control auto	Sets the port to participate in authentication.
dot1x reauth-max	Sets the maximum number of the supplicant re-authentications.
dot1x re-authentication	Sets the re-authentication attribute.
dot1x timeout quiet-period	Sets the time the device waits before re-authentication.
dot1x timeout re-authperiod	Sets the re-authentication period for the supplicant.
dot1x timeout server-timeout	Sets the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Sets the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Sets the re-transmission interval.

N/A

4.55. show dot1x max-req

Use this command to display the maximum number of request/challenge packet transmission.

show dot1x max-req

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide **N/A**

Configuration Examples

The following example displays the maximum number of request/challenge packet transmission.

```
QTECH#show dot1x max-req


Max-Req: 3 Times
```

Related

Command	Description
dot1x auth-mode	Sets the 802.1X authentication mode.
dot1x max-req	Sets the maximum number of authentication request re-transmissions.
dot1x port-control auto	Sets the port to participate in authentication.
dot1x reauth-max	Sets the maximum number of the supplicant re-authentications.
dot1x re-authentication	Sets the re-authentication attribute.
dot1x timeout quiet-	Sets the time the device waits before re-

period	authentication.
dot1x timeout re-authperiod	Sets the re-authentication period for the supplicant.
dot1x timeout server-timeout	Sets the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Sets the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Sets the re-transmission interval.

Commands

Platform Description

N/A

4.56. show dot1x port-control

Use this command to display the port-control information.

show dot1x port-control [**interface** *interface-type interface-number*]

Parameter Description

Parameter	Description
interface-type	Interface type
interface-number	Interface ID

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

`Usage Guide` **`N/A`**

Configuration Examples

Related Commands

The following example displays the port-control information.

Command	Description
dot1x auth-mode	Sets the 802.1X authentication mode.
dot1x max-req	Sets the maximum number of authentication request

```
QTECH#show dot1x port-control
Interface Mode        Dynamic-User Static-User Max-User Authened MAB
----------
Gi0/5     mac-based   0            0           unlimited  no     disable
```

	re-transmissions.
dot1x port-control auto	Sets the port to participate in authentication.
dot1x reauth-max	Sets the maximum number of the supplicant re-authentications.
dot1x re-authentication	Sets the re-authentication attribute.
dot1x timeout quiet-period	Sets the time the device waits before re-authentication.
dot1x timeout re-authperiod	Sets the re-authentication period for the supplicant.
dot1x timeout server-timeout	Sets the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Sets the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Sets the re-transmission interval.

Platform Description

N/A

4.57. show dot1x private-supplicant-only

Use this command to display the information about the private supplicant.
show dot1x private-supplicant-only

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays the information about the private supplicant:

```
QTECH#show dot1x private-supplicant-only


private-supplicant-only: Disabled
```

Related Commands

Command	Description
dot1x auth-mode	Sets the 802.1X authentication mode.
dot1x max-req	Sets the maximum number of authentication request re-transmissions.
dot1x port-control auto	Sets the port to participate in authentication.
dot1x reauth-max	Sets the maximum number of the supplicant

	re-authentications.
dot1x re-authentication	Sets the re-authentication attribute.
dot1x timeout quiet-period	Sets the time the device waits before re-authentication.
dot1x timeout re-authperiod	Sets the re-authentication period for the supplicant.
dot1x timeout server-timeout	Sets the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Sets the authentication timeout between the device and the supplicant.
dot1x timeout tx-period	Sets the re-transmission interval.

Platform Description

N/A

4.58. show dot1x probe-timer

Use this command to display the configuration of online user probe.
show dot1x probe-timer

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide **N/A**

Configuration Examples

The following example displays the configuration of online user probe.

```
QTECH#show dot1x probe-timer Hello Interval   : 20
Hello Alive   : 60
```

Related Commands

Platform Description

Field Description

Command	Description
Hello Interval	Sets the probe period.
Hello Alive	Sets the probe alive interval.

Command	Description
N/A	N/A.

N/A

4.59. show dot1x re-authentication

Use this command to display re-authentication status.
show dot1x re-authentication

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

```
Usage Guide
N/A
```

Configuration Examples

Related Commands

Platform Description

The following example displays re-authentication status.

```
QTECH#show dot1x re-authentication


Reauth-Enabled: Disabled
```

Command	Description
Reauth-Enabled	Whether to enable re-authentication.

Command	Description
N/A	N/A

N/A

4.60. show dot1x reauth-max

Use this command to display the maximum re-auth attempts.
show dot1x reauth-max

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example displays the maximum re-authentication attempts.

```
QTECH#show dot1x reauth-max

Reauth-Max: 3 Times
```

Command	Description
Reauth-Enabled	Sets the maximum re-authentication attempts.

Command	Description
N/A	N/A

N/A

4.61. show dot1x summary

Use this command to display the 802.1X authentication summary.

show dot1x summary

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

It is convenient to display the 802.1X authentication summary according to the MAC address or username.

Configuration Examples

The following example displays the summary of 802.1X authentication.

```
QTECH#show dot1x summary
ID     User   MAC          Interface VLAN INNER-VLAN Auth-State
Backend-State Port-Status User-Type Time
```

Related Commands

Command	Description
dot1x auth-mode	Sets the 802.1X authentication mode.
dot1x max-req	Sets the maximum number of authentication request re-transmissions.
dot1x port-control auto	Sets the port to participate in authentication.
dot1x reauth-max	Sets the maximum number of the supplicant re-authentications.
dot1x re-authentication	Sets the re-authentication attribute.
dot1x timeout quiet-period	Sets the time the device waits before re-authentication.
dot1x timeout re-authperiod	Sets the re-authentication period for the supplicant.
dot1x timeout server-timeout	Sets the authentication timeout between the device and authentication server.
dot1x timeout supp-timeout	Sets the authentication timeout between the device and

	the supplicant.
dot1x timeout tx-period	Sets the re-transmission interval.

Platform Description

N/A

4.62. show dot1x timeout quiet-period

Use this command to display the time for the device to wait before re-authentication quiet period after the authentication failure.

show dot1x timeout quiet-period

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

Use this command to display the time for the device to wait before re-authentication quiet period after the authentication failure.

Configuration Examples

The following example shows how to displays the quiet period the time for the device to wait before re-authentication after the authentication failure.

```
QTECH#show dot1x timeout quiet-period


Quiet-Period: 10 Seconds
```

Related Commands

Command	Description
N/A	N/A

Parameter Description:

Parameter	Description
Quiet-Period	The time for the device to wait before re-authentication after the authentication failure.

Platform N/A

Description

4.63. show dot1x timeout re-authperiod

Use this command to display the re-authentication interval.
show dot1x timeout re-authperiod

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

Use this command to display the re-authentication interval.

Configuration Examples

The following example displays the re-authentication interval.:

```
QTECH#show dot1x timeout re-authperiod
```

```
Reauth-Period: 3600 Seconds
```

Related Commands

Platform Description

Parameter Description:

Parameter	Description
Reauth-Period	Re-authentication interval.

Command	Description
N/A	N/A

N/A

4.64. show dot1x timeout server-timeout

Use this command to display the authentication timeout period.
show dot1x timeout server-timeout

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

Use this command to display the authentication timeout period.

Configuration Examples

Use this command to display the authentication timeout period:

```
QTECH#show dot1x timeout server-timeout
```

```
Server-Timeout: 5 Seconds
```

Related Commands

Platform Description

Parameter Description:

Parameter	Description
Server-Period	AuthenticationServer timeout periodinterval.

Command	Description
N/A	N/A

N/A

4.65. show dot1x timeout supp-timeout

Use this command to display the request/challenge packets re-transmission interval.
show dot1x timeout supp-timeout

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide Use this command to display the request/challenge packets re-transmission interval.

Configuration Examples

Use this command to display the request/challenge packets re-transmission interval:

```
QTECH#show dot1x timeout supp-timeout

Supp-Timeout: 3 Seconds
```

Related Commands

Command	Description
N/A	N/A

Field Description:

Field	Description
Server-Period	The request/challenge packets re-transmission interval.

Platform Description

N/A

4.66. show dot1x timeout tx-period

Use this command to display the request/id packets re-transmission interval.
show dot1x timeout tx-period

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide Use this command to display the request/id packets re-transmission interval.

Configuration Examples

Use this command to display the request/ id packets re-transmission interval:

```
QTECH#show dot1x timeout tx-period


Tx-Period: 30 Seconds
```

Related Commands

Platform Description

Parameter Description:

Parameter	Description
Tx-Period	Request/id packets re-transmission interval.

Command	Description
N/A	N/A

N/A

4.67. show dot1x user mac

Use this command to display the information about 802.1X authentication users based on MAC addresses.

show dot1x user mac *mac-addr*

Parameter Description

Parameter	Description
mac-addr	MAC address

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

Use the **show dot1x summary** command to display 802.1X authentication summaries. And use this command to display detailed information of a specific user based on its MAC address.

Configuration Examples

The following example displays the information about the 802.1X authentication user according to the user's MAC address.

```
QTECH#show dot1x user mac 0023.aeaa.4286

User name: ts-user User id:
16777225 Type: static
Mac address is 0023.aeaa.4286 Vlan id is 2
Access from port Gi0/5
Time online: 0days 0h 0m17s User ip address is
192.168.3.21
Max user number on this port is 0 Authorization session
time is 1000 seconds Supplicant is private
Start accounting Permit proxy user
Permit dial user IP privilege is 0
 user acl-name ts-user_6_0_0 :
```

Parameter Description:

Parameter	Description
User name	User name
User id	User ID
Type	User type
Mac address	User's MAC address
Vlan id	User VLAN ID
Access from port	The port that user access from
Time online	User online time
User ip address	User IP address
Max user number on this port	The maximum number of users on the port
Authorization session time	The authorized session time

Supplicant is private	Whether the terminal is a QTECH device
Start accounting	The accounting is enabled.
Permit proxy user	The user is allowed to use the proxy.
Permit dial user	The user is allowed to dial.
IP privilege	The IP privilege level
user acl-name	The ACL information

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.68. show dot1x user name

Use this command to display information about 802.1X authentication users based on usernames.

```
show dot1x user name name
```

Parameter Description

Parameter	Description
name	User name

Defaults
N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

Use the **show dot1x summary** command to display 802.1X authentication summaries. And use this command to display detailed information of a specific user based on its username.

Configuration Examples

The following example displays the information about the 802.1X authentication user according to the user name.

```
QTECH#show dot1x user name ts-user

User name: ts-user User id:
16777225 Type: static
Mac address is 0023.aeaa.4286 Vlan id is 2
Access from port Gi0/5
Time online: 0days 0h 0m17s User ip address is
192.168.3.21
Max user number on this port is 0 Authorization session
time is 1000 seconds Supplicant is private
Start accounting Permit proxy user
Permit dial user IP privilege is 0
 user acl-name ts-user_6_0_0 :
```

Related Commands

Platform Description

Parameter Description:

Parameter	Description
User name	User name
User id	User ID
Type	User type
Mac address	User’s MAC address
Vlan id	User VLAN ID
Access from port	The port that user access from
Time online	User online time
User ip address	User IP address

Max user number on this port	The maximum number of users on the port
Authorization session time	The authorized session time
Supplicant is private	Whether the terminal is a QTECH device.
Start accounting	The accounting is enabled.
Permit proxy user	The user is allowed to use the proxy.
Permit dial user	The user is allowed to dial.
IP privilege	The IP privilege level.
user acl-name	The ACL information.

Command	Description
N/A	N/A

N/A

5.1. accounting

Use this command to set an accounting method for the template. Use the **no** form of this command to restore the default setting. **accounting** { *method-list* }

no accounting

Parameter Description

Parameter	Description
method-list	Name of the method list

Defaults

N/A

Command Mode

Template configuration mode

Usage Guide

The *method-list* parameter in this command should be consistent with network accounting list name configured in AAA.

Configuration Examples

Related Commands

Platform Description

The following example sets the **mlist1** accounting method for the **eportalv2** template.

```
QTECH(config.tmplt.eportalv2)# accounting mlist1
```

Command	Description

N/A	N/A

N/A

5.2. authentication

Use this command to set an authentication method for the template. Use the **no** form of this command to restore the default setting. **authentication** { *method-list* }

no authentication

Parameter Description

Parameter	Description
method-list	Name of the method list

Defaults

N/A

Command Mode

Template configuration mode

Usage Guide

The *method-list* parameter in this command should be consistent with the Web authentication method list configured in AAA.

The first generation authentication does not support the authentication method list configuration.

Configuration Examples

Related Commands

Platform Description

The following example sets the **mlist1** authentication method for the **eportalv2** template.

```
QTECH(config.tmplt.eportalv2)#authentication mlist1
```

Command	Description
N/A	N/A

N/A

5.3. bindmode

Use this command to set a binding mode for the template.

Use the **no** form of this command to restore the default setting.

bindmode { **ip-mac-mode** | **ip-only-mode** }

no bindmode

Parameter Description

Parameter	Description
ip-mac-mode	IP+MAC mode. The device will write both the IP address information and the MAC address information into the forwarding entry.
ip-only-mode	IP only mode. The device writes only the IP address information into the forwarding entry. On the L3 network, it is recommended to adopt this mode in case that the MAC address is inaccurate.

Defaults

The default is **ip-mac-mode**.

Command Mode

Template configuration mode

Usage Guide

N/A

Configuration Examples

The following example adopts the IP only mode for the **eportalv2** template.

```
QTECH(config.tmplt.eportalv2)# bindmode ip-only-mode
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.4. clear web-auth direct-arp

Use this command to clear all ARP resources exempt from authentication.

clear web-auth direct-arp

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example clears all ARP resources exempt from authentication.

```
QTECH# clear web-auth direct-arp
```

Command	Description
N/A	N/A

N/A

5.5. clear web-auth direct host

Use this command to clear all authentication-exempted users.clear web-auth direct-host [range]

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example clears all authentication-exempted users.

```
QTECH# clear web-auth direct-host
```

Command	Description
N/A	N/A

N/A

5.6. clear web-auth direct-site

Use this command to clear all authentication-exempted network resources.

clear web-auth direct-site [range]

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example clears all authentication-exempted network resources.

```
QTECH# clear web-auth direct-site
```

Command	Description
N/A	N/A

N/A

5.7. clear web-auth user

Use this command to force the user to go offline.

clear web-auth user { **all** | **ip {** *ip-address* | *ipv6-address }* | **mac** *mac-address* **| name** *name-string* }

Parameter Description

Parameter	Description
ip-address	Specifies the user's IPv4 address.
ipv6-address	Specifies the user's IPv6 address.
mac-address	Specifies the user's MAC address.
name-string	Specifies the user name.

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide
N/A

Configuration Examples

Related Commands

Platform Description

The following example forces all users to go offline.

```
QTECH(config) clear web-auth user all
```

Command	Description
N/A	N/A

N/A

5.8. fmt

Use this command to set the URL redirection format in the second template configuration mode.

fmt { cmcc-ext1 | cmcc-ext2 | cmcc-normal }

Use this command to set the URL redirection format in the first template configuration mode.

fmt { ace | QTECH| custom }

Parameter Description

Parameter	Description
cmcc-ext1	Extended CMCC format
cmcc-ext2	Liaoning CMCC format
cmcc-normal	Standard CMCC format

Defaults

The default URL redirection format is QTECH format.

Command Mode

Template configuration mode

Usage Guide

Use this command to set the URL redirection format based on the corresponding portal standard.

Configuration Examples

The following example sets the URL redirection format to extended CMCC format.

```
QTECH(config.tmplt.eportalv2)#fmt cmcc-ext1
```

Platform Description

N/A

5.9. http redirect direct-arp

Use this command to set the address range of the authentication-exempted ARP. Use the **no** form of this command to restore the default setting.

http redirect direct-arp { *ip-address* [*ip-mask*] }

no http redirect direct- arp { *ip-address* [*ip-mask*] }

Parameter Description

Parameter	Description
ip-address	IPv4 address
ip-mask	(Optional) IPv4 mask

Defaults

No authentication-exempted ARP resource is configured by default.

Command Mode

Global configuration mode

Usage Guide

The user cannot learn the ARPs of devices such as the gateway with the ARP CHECK function enabled. Use this command to enable the device to learn the ARP within a specified IP address range without authentication.

Configuration Examples

Related Commands

Platform Description

The following example sets the IP address 172.16.0.1 as the authentication-exempted ARP resource.

```
QTECH(config)# http redirect direct-arp172.16.0.1
```

Command	Description
N/A	N/A

N/A

5.10. http redirect direct-site

Use this command to set the range of authentication-exempted network resources. Use the **no** form of this command to restore the default setting.

http redirect direct-site { *ipv6-address* | *ipv4-address* [*ip-mask*] [**arp**]| *mac-address* | range *starip-address endip-address*} [description *description-str*] [group *group-name*]

no http redirect direct-site { *ipv6-address* | *ipv4-address* [*ip-mask*] | *mac-address* | range *startip-address endip-address* }

Parameter Description

Parameter	Description
ipv6-address	IPv6 address of the authentication-exempted network resources
ip-address	IPv4 address of the authentication-exempted network resources
ip-mask	IPv4 address mask of the authentication-exempted network resources (optional)
arp	If the ARP Check is enabled on the access device, the keyword arp is needed for ARP binding of the authentication-exempted network resources (optional). It is necessary for IPv4 network resources only.

mac-address	MAC address of the authentication- exempted user
startip-address	Start IP address of the authentication-exempted user
endip-address	End IP address of the authentication-exempted user
group-name	Group name of the authentication-exempted user
description-str	Description of the authentication-exempted user

Defaults
No authentication-exempted network resource is set.

Command Mode

Global configuration mode

Usage Guide

When Web/802.1x authentication is enabled, all users must pass Web/client authentication to access network resources. This command is used to make certain network resources available to unauthenticated users. All users can access the authentication-exempted Web sites.

Up to 50 authentication-exempted users are supported.

Configuration Examples

The following example sets the Web site with IP address 172.16.0.1 as the authentication-exempted resource.

```
QTECH(config)# http redirect direct-site 172.16.0.1
```

The following example sets the Web site with MAC address 0000:5e00:0101 as the authentication-exempted resource.

```
QTECH(config)# http redirect direct-site 0000:5e00:0101
```

The following example sets the range from 10.0.0.1 to 12.0.0.1 as authentication-exempted network resources.

Related Commands

Platform Description

QTECH(config)# http redirect direct-site range 10.0.0.112.0.0.1

Command	Description
show http redirect	Displays the HTTP redirection configuration.

N/A

5.11. http redirect port

Use this command to redirect users' HTTP redirection request to a certain destination port. Use the **no** form of this command to restore the default setting.

http redirect port *port-num*

no http redirect port *port-num*

Parameter Description

Parameter	Description
port-num	Destination port of the HTTP request

Defaults

The default is port 80.

Command Mode

Global configuration mode

Usage Guide

When you access the network resource, you send HTTP packets. The access device can intercept such HTTP packets to detect your access. If the access

device detects that an unauthenticated user is accessing the network resource, it stops the users with an authentication page/client download page.

By default, the access device intercepts users' HTTP packets with port 80 to check whether they are accessing network resources.

This command is used to change the destination port of HTTP packets that are intercepted by the access device.

Up to 10 ports can be configured, excluding port 80 and port 443.

Configuration Examples

Related Commands

The following example redirects users' HTTP requests with port 8080.

```
QTECH(config)# http redirect port 8080
```

The following example does not redirect users' HTTP requests with port 80.

```
QTECH(config)# no http redirect port 80
```

Command	Description
show http redirect	Displays the HTTP redirection configuration.

Platform Description

N/A

5.12. http redirect session-limit

Use this command to set the total number of HTTP sessions that can be originated by an unauthenticated user, or the maximum number of HTTP sessions that can be originated by an unauthenticated user connected to each port.

Use the **no** form of this command to restore the default setting. **http redirect session-limit** *session-num* [**port** *port-session-num*] **no http redirect session-limit**

Parameter Description

Parameter	Description
session-num	Total number of HTTP sessions that can be originated by an unauthenticated user, in the range from 1 to 255.
port-session-num	The maximum number of HTTP sessions that can be originated by an unauthenticated user connected to each port, in the range from 1 to 65535.

Defaults

Totally 255 HTTP sessions can be originated by an unauthenticated user, and 300 HTTP sessions that can be originated by an unauthenticated user connected to each port.

Command Mode

Global configuration mode

Usage Guide

To prevent HTTP attacks caused by unauthenticated users from using up the TCP connections of the access device, the maximum number of HTTP sessions by unauthenticated users must be limited on the access device.

In addition to authentication, other programs may also occupy HTTP sessions. Therefore, it is not recommended that the maximum number of HTTP sessions by unauthenticated users be 1

Configuration Examples

Related Commands

Platform Description

The following example sets the maximum number of HTTP sessions

originated by an unauthenticated user to 4.

```
QTECH(config)# http redirect session-limit 4
```

Command	Description
show http redirect	Displays the HTTP redirection configuration.

N/A

5.13. http redirect timeout

Use this command to set the timeout for the redirection connection maintenance. Use the **no** form of this command to restore the default setting.

http redirect timeout *seconds*

no http redirect timeout

Parameter Description

Parameter	Description
seconds	Set the timeout for the redirection connection maintenance, in the range from 1 to 10 in the unit of seconds.

Defaults

The default is 3 seconds.

Command Mode

Global configuration mode

Usage Guide

This command is used to set the timeout for the redirection connection maintenance. After the three-way handshake succeeds, the redirection

connection is maintained until the user sends an HTTP GET/HEAD packet and the system returns an HTTP redirection packet. This timeout is set to prevent users from occupying TCP connections for long without sending any GET/HEAD packets.

Configuration Examples

Related Commands

Platform Description

The following example sets the timeout for the redirection connection maintenance to 4 seconds.

```
QTECH(config)# http redirect timeout 4
```

Command	Description
show http redirect	Displays the HTTP redirection configuration.

N/A

5.14. ip

Parameter Description

Use this command to set an IP address for the portal server. Use the **no** form of this command to restore the default setting. **port** { *ip-address* }

no port

Parameter	Description
ip-address	The IPv4 address of the portal server

Defaults

No IP address is set for the portal server by default.

Command Mode

Template configuration mode

Usage Guide

This command takes place of the **http redirect** [*ip-address*] command, which is now hidden as a compatible command.

Configuration Examples

The following example sets the IP address of the eportalv1 template to 172.16.0.1.

```
QTECH(config.tmplt.eportalv1)#ip 172.16.0.1
QTECH(config.tmplt.eportalv1)#
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.15. ip portal source-interface

Use this command to specify a communication port for the portal server. Use the **no** form of this command to restore the default setting.

ip portal source-interface *interface-type interface-num*

no ip portal source-interface

Parameter Description

Parameter	Description

interface-type	Port type
interface-num	Port No.

Defaults
No communication interface is specified by default.

Command Mode

Global configuration mode

Usage Guide N/A

Configuration Examples

The following example specifies an aggregate port as the communication port.

```
QTECH (config)# ip portal source-interface Aggregateport1
```

Platform Description

N/A

5.16. port

Parameter Description

Use this command to set a surveillance port for the portal server. Use the **no** form of this command to restore the default setting. **port** { *port-num* }

no port

Parameter	Description
port	The surveillance port of the portal server, which is on only the 2nd generation portal server,

Defaults
The default is 50100 based on the UDP protocol.

Command Mode

Template configuration mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example sets the surveillance port number of the eportalv2 server to 10000.

```
QTECH(config.tmplt.eportalv2)#port 10000
```

Command	Description
N/A	N/A

N/A

5.17. redirect

Use this command to specify the encapsulation format of the Web-auth URL.

redirect { ***http*** **|** ***js*** }

no redirect

Parameter Description

Parameter	Description
http	HTTP encapsulation format
js	Java Script encapsulation format

Defaults

The default encapsulation format is Java Script.

Command Mode

Template configuration mode

Usage Guide N/A

Configuration Examples

The following example specifies HTTP as the encapsulation format of the Web-auth URL.

```
QTECH(config.tmplt.eportalv2)#redirect http
```

Platform Description

N/A

5.18. show web-auth acl

Use this command to display whitelist configuration.

show web-auth acl [white-url]

Parameter Description

Parameter	Description
N/A	N/A

Command Mode

Privileged EXEC mode

Usage Guide The command is used to check the whitelist configuration of web authentication.

Configuration Examples

The following example displays whitelist configuration.

```
QTECH# show web-auth acl


White URL List:0
```

Platform Description

N/A

5.19. show web-auth authmng

Use this command to display authentication experience data.

show web-auth authmng [statistic | abnormal]

Parameter Description

Parameter	Description
N/A	**N/A**

Command Mode

Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays authentication experience data.

```
QTECH# show web-auth authmng statistic
```

The following example displays abnormal authentication experience data.

```
QTECH# show web-auth authmng abnormal
record num:0, value:3000, max-num:1000, clock:1
```

Field	Description
record num	Number of records.
value	Timeout period in the unit of ms. By default, one abnormal

	record is generated when the timeout exceeds 3s.
max-num	Maximum number of records.
clock	The time when the record is written into flash in the range from 0 o’clock to 23 o’clock. The default time is 1 o’clock.

Abnormal records are stored in the directory: /data/security/authmanage/webauth/.

Platform Description

N/A

5.20. show web-auth control

Use this command to display the authentication configuration.

show web-auth control

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide
N/A

Configuration Examples

The following example displays the authentication configuration and statistics information on the interface.

```
QTECH(config)#show web-auth control
Port  Control  Server Name    Online User Count

GigabitEthernet 0/1     On    <not configured>  0
QTECH(config)#
```

Field	Description
Port	Name of the authentication port.
Control	Displays whether the Web authentication is enabled on the port or not.
Server Name	The customized server name on the port. **<not configured>** indicates the server name has not been configured.
Online User Count	The number of online users on this port.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.21. show web-auth direct-arp

Use this command to display the address range of the authentication-exempted ARP.

show web-auth direct-arp

Parameter Description

Parameter	Description

N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide I N/A

Configuration Examples

The following example displays the address range of the authentication-exempted ARP.

```
QTECH(config)#show web-auth direct-arp Direct arps:
  Address         Mask
1.1.1.    255.255.255.255
2.2.2.    255.255.255.255
```

Related Commands

Platform Description

QTECH(config)#

Field	Description
Address	IPv4 address.
Mask	IPv4 mask.

Command	Description
N/A	N/A

N/A

5.22. show web-auth direct-host

This command is used to display the Web authentication-exempted users.

show web-auth direct-host

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode

Privileged EXEC mode

Usage Guide N/A

Configuration Examples

The following example displays the Web authentication-exempted users.

```
QTECH# show web-auth direct-host
Direct hosts:
  Address            Mask           Port    ARP Binding  Group  Description
                                                                 ---------------------------
  192.168.0.1      255.255.255.255  Gi0/2      On          N/A       N/A
  192.168.4.11     255.255.255.255  Gi0/10     On          N/A       N/A
  192.168.5.0      255.255.255.0    Gi0/16     Off         N/A       N/A
```

Field	Description
Address	IP address of the user free of authentication
Mask	IP address mask of the user free of authentication

Port	**Access device port that is bound with the user's IP address**

ARP Binding	Enable/Disable ARP binding

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.23. show web-auth direct site

Use this command to display the range of the Web authentication-exempted network resources.

show web-auth direct-site

Parameter Description

Parameter	Description
N/A	N/A

Defaults

No network resource without authentication is set.

Command Mode

Privileged EXEC mode

`Usage Guide` **`N/A`**

Configuration Examples

The following example displays the range of the Web authentication-exempted network resources without authentication.

```
QTECH(config)#show web-auth direct-site
Direct sites:
  Address         Mask           ARP Binding

  1.1.1.1         255.255.255.255 Off
  2.2.2.2         255.255.255.255 On
QTECH(config)#
```

Field	Description
Address	IP address.
Mask	IP mask.
ARP Binding	Displays whether the ARP binding function is enabled.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.24. show web-auth parameter

Use this command to display the HTTP redirect configuration.
show web-auth parameter

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode
Privileged EXEC mode

Usage Guide
N/A

Configuration Examples

Related Commands

Platform Description

The following example displays the HTTP redirect configuration

```
QTECH# show web-auth
  parameter session-limit: 10
  timeout:          5
```

Field	Description
session-limit	Total number of HTTP sessions that are created by an unauthenticated user.
timeout	Timeout interval of the redirection connection.

Command	Description
N/A	N/A

N/A

5.25. show web-auth portal-check

Use this command to display the portal-check configuration.

show web-auth portal-check

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the portal-check configuration.

```
QTECH#sh web portal-check Check: Enable
  Interval:    3s
  Timeout:     5s Retransmit:  3
Escape:        Enable
Nokick:        Disable
```

Platform Description

N/A

5.26. show web-auth rdport

Use this command to display the TCP interception port.
show web-auth rdport

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode
Privileged EXEC mode

Usage Guide
N/A

Configuration Examples

The following example displays the TCP interception port.

```
QTECH#show web-auth rdport
Rd-Port:
80 443
QTECH#
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.27. show web-auth syslog ip

Use this command to display online and offline records about users.

show web-auth syslog ip *ip-address*

Parameter Description

Parameter	Description
Ip-address	A user's IP address.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command cannot be used to save original data after hot backup.

Configuration Examples

The following example displays online and offline records of users.

```
QTECH#show web-auth syslog ip 192.168.197.35 Address: 192.168.197.35
Core-index 0 Current index 2
Index: 0
Time: 2015-10-16 20:37:34

 Behavior:        ONLINE
 Mac:            00d0.f822.33e7
 Vid:            101
 Port:           Gi3/1
 Timeused:        0d 00:00:00
 Flow_up:         0
 Flow_down:       0

 Index:          1
 Time:           2015-10-16 20:42:08
 Behavior:        OFFLINE
 Mac:            00d0.f822.33e7
 Vid:            101
 Port: Gi3/1
 Timeused:   0d 00:04:27
 Flow_up:    2107872
 Flow_down:  2108224
```

Field	Description
Index	The number of the record.
Time	Time when the record is made.
Behavior	Online or offline behavior.
MAC	The Mac address of a user.
Vid	The VLAN ID of a user.
Port	The user port.
Timeused	The time when a user gets online.
Flow UP	The uplink traffic of a user.
Flow down	The downlink traffic of a user.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.28. show web-auth template

Use this command to display the portal server configuration.

show web-auth template

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to display the portal server configuration.

Configuration

The following example displays the port server configuration.

Examples

```
QTECH#show web-auth template
Webauth Template Settings:
-------------------------------------------------------------------------------------------------
  Name:      eportalv1
  Url:       http://17.17.1.21:8080/eportal/index.jsp
  Ip:        17.17.1.21
  BindMode:  ip-mac-mode
  Type:      v1
-------------------------------------------------------------------------------------------------
  Name:      eportalv2
  Url:       http://17.17.1.21:8080/eportal/index.jsp
  Ip:        17.17.1.21
  BindMode:  ip-only-mode
  Type:      v2
  Port:      50100
  Acctmlist:
  Authmlist:
QTECH#
```

Field	Description
Name	Template name.
Url	Server homepage address.

Ip	Server IP address.
Type	Server type, including the first generation portal server v1, the second generation portal server v2, and internal is intra.
Port	The protocol packet communication port of the server, which is on only the second generation portal server.
Acctmlist	Accounting method list name, which is on the second generation portal and internal servers.
Authmlist	Authentication method list name. which is on only the second generation portal and internal servers.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.29. show web-auth user

Use this comma to display the online information, including IP address, interface, and online duration, of all users or the specified users.

show web-auth user { **all** | **ip** *ip-address* | **mac** *mac-address* | **name** *name-string* }

Parameter Description

Parameter	Description
ip-address	IPv4 address of the user.
mac-address	MAC address of the user.
name-string	User name.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide **N/A**

Configuration Examples

The following example displays the global Web authentication configuration and statistics.

```
QTECH# show web-auth user all
Current user num : 4, online 2

Address          Online   Time Limit     Time Used    Status  Name

192.168.0.11    On       0d 01:00:00   0d 00:15:10    Active
192.168.0.13    On       0d 01:00:00   0d 00:00:59    Active   111
192.168.0.25    Off      0d 01:00:00   0d 00:00:59    Create
192.168.0.46    Off      0d 01:00:00   0d 01:00:00    Destroy  222

QTECH# show web-auth user ip 192.168.0.11
Address      :   192.168.0.11
 Mac          :   00d0.f800.2233
 Port         :   Gi0/2
 Online       :   On
 Time Limit   :   0d 01:00:00
 Time Used    :   0d 00:15:10
 Time Start   :   2009-02-22 20:05:10
 Status       :   Active
```

Field	Description
Address	IP address of the user
Mac	MAC address of the user
Port	Access device port connected to the user
Online	Whether the user is online
Time Limit	Available duration of the user. 0 means unlimited.
Time Used	Online duration of the user

Time Start	Time when the user passes authentication and gets online
Status	User status. Active means the user is normally online, Create means the user is created without any settings, Destroy means the user is deleted with its settings not cleared.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.30. url

Parameter Description

Use this command to set the portal server URL.

Use the **no** form of this command to restore the default setting.

url *url-string*

no url

Parameter	Description
url-string	Portal server URL, starting with **http://** or **https://**. The maximum length of this address is 255 bytes.

Defaults

On the first/second/inner/wifidog auth, no portal server URL is set by default.

On WeChat auth, the URL when MCP/WMC server adopts WeChat and MSG auth by default.

Command Mode

Template configuration mode

Usage Guide

This command takes place of the **http redirect homepage** [*url-string*] command, which is now hidden as a compatible command.,

If no URL is specified, the default URL in the **http://[ip-address]** format will be adopted, among which **ip-address** is the IP address of the server.

Configuration Examples

Related Commands

The following example sets the eportalv1 template URL to **http://www.web-auth.net/login**.

```
QTECH(config.tmplt.eportalv1)#urlhttp://www.web-auth.net/login
```

Command	Description
N/A	N/A

Platform

N/A

Description

5.31. web-auth acl

The whitelist users can access partial network resources before auth, and the blacklist users can not access partial network resources after auth. Use **no** form of this command to restore the default setting. **web-auth acl** {**white-url** *name* }

no web-auth acl { **white-url** *name* }

Parameter Description

Parameter	Description
name	Whitelist URL

Command Mode

Global configuration mode

Usage Guide

The command is used to check the whitelist configuration of web authentication.

Configuration Examples

The following example configures whitelist.

```
QTECH (config)# web-auth acl white-urlwww.QTECH.com.cn
```

Platform Description

N/A

5.32. web-auth dhcp-check

Use this command to enable DHCP IP address check.

Use **no** form of this command to restore the default setting.

web-auth dhcp-check

no web-auth dhcp-check

Parameter Description

Parameter	Description
N/A	N/A

Defaults

DHCP IP address check is disabled by default.

Command Mode

Global configuration mode

Usage Guide

Only users whose IP addresses are allocated by DHCP are allowed to take authentication.

Configuration

The following example enables DHCP IP address check.

Examples

```
QTECH (config)# web-auth dhcp-check
```

Platform Description

N/A

5.33. web-auth dhcp-check vlan

Use this command to check whether the IP address of a client is assigned by the DHCP server. Use the **no** form of this command to restore the default setting.

```
web-auth dhcp-check {vlan [vlan-list]} no web-auth dhcp-check
```

Parameter Description

Parameter	Description
vlan-list	Indicates the VLAN range in which DHCP address check needs to be enabled in interface.

Defaults

By default, this function is disabled.

Command Mode

Interface configuration mode

```
Usage Guide      N/A
```

Configuration Examples

Related Commands

Platform Description

The following example checks whether the IP address of a client is assigned by the DHCP server.

```
QTECH(config-if-TenGigabitEthernet 3/1)# web-auth dhcp-check vlan1,3-4
```

Command	Description
N/A	N/A

N/A

5.34. web-auth dhcp-server check

Use this command to disable DHCP server detection.

no web-auth dhcp-server check

Use this form of this command to restore the default setting.

web-auth dhcp-server check

Parameter

Parameter	Description
N/A	**N/A**

Description

Defaults

By default, this function is enabled.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example disables DHCP server detection.

```
QTECH (config)# no web-auth dhcp-server check
```

Command	Description
N/A	N/A

N/A

5.35. web-auth direct-host

Use this command to set the authentication-exempted IP/MAC address range. Use the **no** form of this command to restore the default setting.

web-auth direct-host { *ipv4-address* [i*p-mask*] [**arp**] | *ipv6-address* } [**port** *interface-name*]

no web-auth direct-host { *ipv4-address* [i*p-mask*] | *ipv6-address* }

Parameter Description

Parameter	Description
ip-address	IPv4 address of authentication-exempted user
ip-mask	Mask of the IPv4 address free of authentication (optional).
port *interface-name*	Binds user's IP address with a port of the access device (optional).
arp	If ARP CHECK is enabled on the access device, keyword arp is needed for ARP binding of the IP address used by users free of authentication (optional). It is necessary for IPv4 addresses only.

Defaults

No user is exempted from authentication. All users must pass the Web authentication to access the restricted network resources.

Command Mode

Global configuration mode

Usage Guide

When a user is set to be exempted from authentication, it can access all reachable network resources without Web authentication.

Up to 50 users can be set to be exempted from authentication.

Configuration Examples

Related Commands

Platform Description

The following example sets the user with the IP address 172.16.0.1 to be exempted from authentication.

```
QTECH(config)# web-auth direct-host 172.16.0.1
```

The following example sets the user with the IP address FF02::/64 to be exempted from authentication.

```
QTECH(config)# web-auth direct-host FF02::/64
```

Command	Description
show web-auth direct-host	Displays the users free of Web authentication.

N/A

5.36. web-auth enable

Use this command to enable the Web authentication function on a port. This command is compatible with the **web-auth port-control** command.

Use the **no** form of this command to restore the default setting. **web-auth enable** [**eportalv1 | eportalv2 |** *template-name*] **no web-auth enable**

Parameter Description

Parameter	Description
eportalv1	Applies the first generation authentication template.
eportalv2	Applies the second generation authentication template.
template-name	Customized template.

Defaults

The Web authentication function is disabled on the port by default.

The **default** template is eportalv1.

Command Mode

Interface configuration mode

Usage Guide

To ensure the Web authentication function, the authentication page URL should be configured.

Because template applications are integrated into the controlled switch, the template or the server applications of the interface where the Web authentication function is disabled will be automatically cleared. This command is compatible with the original command that used to apply the template or server application in the global configuration mode.

Configuration Examples

The following example enables the Web authentication function on gigabitEthernet 0/14.

```
QTECH(config)# interface GigabitEthernet 0/14
QTECH(config-if-GigabitEthernet 0/14)# web-auth enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

5.37. web-auth linkdown-timeout

Use this command to set the link-down timeout.

Use the **no** form of this command to restore the default setting.

web-auth linkdown-timeout { *timeout* }

no web-auth linkdown-timeout

Parameter Description

Parameter	Description
timeout	Link-down timeout

Defaults

By default, the timeout is 60 seconds.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example sets the link-down timeout to 30 seconds.

```
QTECH (config)# web-auth linkdown-timeout 30
```

Command	Description
N/A	N/A

N/A

5.38. web-auth logging enable

Use this command to enable the Web authentication syslog function. Use the **no** form of this command to restore the default setting.

Parameter Description

web-auth logging enable { *num* }

no web-auth logging enable

Parameter	Description
num	The syslog printing rate, indicating how many syslog entries can be printed in a second. The value is in the range from 0 to 65535. 0 indicates no limit.

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

This command is used to limit the syslog printing rate for only the functional module.

Configuration Examples

Related Commands

Platform Description

The following example enables the syslog printing with no rate limit.

```
QTECH(config)# web-auth logging enable 0
```

Command	Description
N/A	N/A

N/A

5.39. web-auth portal

Use this command to map different portal servers with users in different subnets. Use the **no** form of this command to restore the default setting.

```
web-auth portal { eportalv1 | eportalv2| name }  no web-auth portal { eportalv1 | eportalv2| name }
```

Parameter Description

Parameter	Description
name	Portal server name

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

```
Usage Guide
N/A
```

Configuration Examples

N/A

Platform Description

N/A

5.40. web-auth portal extension

Use this command to enable portal extension to support CMCC portal server. Use the **no** form of this command to restore the default setting.

```
web-auth portal  extension no web-auth portal extension
default web-auth portal extension
```

Parameter Description

Parameter	Description
N/A	N/A

Defaults

By default, QTECH portal server is supported.

Command Mode

Global configuration mode

```
Usage Guide
N/A
```

Configuration Examples

The following example disables portal extension.

```
QTECH (config)# no web-auth portal extension
```

Platform Description

N/A

5.41. web-auth portal key

Use this command to set the communication key between the access device and the authentication server.

Use the **no** form of this command to clear the communication key between the redirected Web request of a user and the authentication server.

web-auth portal key *key-string*

no web-auth portal key

Parameter Description

Parameter	Description
key-string	Communication key between the access device and the
	authentication server. The maximum length of the key is 255 bytes.

Defaults

No key is set by default.

Command Mode

Global configuration mode

Usage Guide

To use the Web authentication function, the communication key between the access device and the authentication server must be set.

Configuration Examples

Related Commands

Platform Description

The following example sets the communication key between the access device and the authentication server to web-auth.

```
QTECH(config)# web-auth portal key web-auth
```

Command	Description
http redirect	Sets the IP address of the authentication server.

http redirect homepage	Sets the address of the authentication homepage.
web-auth port-control	Enables the Web authentication on the port.

N/A

5.42. web-auth portal-check

Use this command to enable portal server check.

Use the **no** form of this command to restore the default setting.

web-auth portal-check [**interval** *intsec*] [**timeout** *tosec*] [**retransmit** *retires*]
no web-auth porta-check

Parameter Description

Parameter	Description
Intsec	Check interval in the range from 1 to 1,000 in the unit of seconds. The default is 10 seconds.
tosec	Timeout interval in the range from 1 to 1,000 in the unit of seconds. The default is 5 seconds.
retries	Retry count in the range from 1 to 100. The default is 3.

Defaults

Portal server check is disabled by default.

Command Mode

Global configuration mode

Usage Guide

It is recommended to use this command when there are multiple servers.

Configuration Examples

The following example enables portal server check.

```
QTECH (config)# web-auth portal-check interval 20 timeout 2 retransmit2
```

Platform Description

N/A

5.43. web-auth portal-escape

Use this command to enable portal-escape function.

Use the **no** form of this command to restore the default setting.

```
web-auth  portal-escape no web-auth portal-escape
```

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

Use this command together with **web-auth portal-check** command to sustain key services when the portal server is abnormal.

Configuration Examples

The following example enables portal-escape function.

```
QTECH (config)# web-auth portal-escape
```

Platform Description

N/A

5.44. web-auth template

Use this command to create the first generation authentication template and enter its configuration mode.

web-auth template eportalv1

Use this command to create the customized first generation authentication template and enter its configuration mode.

Parameter Description

web-auth template { template-name } **v1**

Parameter	Description
eportalv1	Applies the first generation authentication template.
eportalv2	Applies the second generation authentication template.
template-name	Sets the name of the customized authentication template.

Use this command to create the second generation authentication template and enter its configuration mode.

web-auth template eportalv2

Use this command to create the customized second generation authentication template and enter its configuration mode.

web-auth template { *template-name* } **v2**

Use this command to remove the template.

no web-auth template { *template-name* }

Defaults

No template is configured by default.

Command Mode

Global configuration mode

Usage Guide

You can enter the **eportalv1** template mode to configure the IP address and URL instead of executing the **http redirect** and **http redirect homepage** commands**.** The **http redirect** and **http redirect homepage** commands are compatible on the device, which will be converted to this command.

The original command **portal-server** is compatible on the device, which will be converted to this command.

To ensure the Web authentication function, configure and apply a functional portal server. The **eportalv1** template is applied by default. The IP address, the URL and the communication secret key of the **eportalv1** template should be configured. If no URL format is specified, the default **http://[ip-address]** format will be adopted. The IP address of the portal server is the network resource exempted from authentication, so the unauthenticated user can access it. The device limits the uplink traffic that accesses the IP address to prevent attacks. The upper limit is proportionate to the number of the physical ports.

Configuration Examples

The following example configures the **eportalv1** template.

```
QTECH(config)# web-auth template eportalv1
QTECH(config.tmplt.eportalv1)#
```

Related

Commands

Command	Description
N/A	**N/A**

Platform Description

N/A

5.45. web-auth update-interval

Use this command to set the interval at which the online user information is updated. Use the **no** form of this command to restore the default setting.

web-auth update-interval {*seconds*}

no web-auth update-interval

Parameter Description

Parameter	Description
seconds	Update interval in seconds, in the range from 30 to 3,600 in the unit of seconds.

Defaults

The default is 180 seconds.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example sets the interval at which the online user information is updated to 60 seconds.

```
QTECH(config)# web-auth update-interval 60
```

Command	Description
N/A	N/A

N/A

5.46. web-auth vlan-control

Use this command to configure the authenticable VLAN list. Use the **no** form of this command to restore the default setting. **web-auth vlan-control** *vlan-list*

no web-auth vlan-control

Parameter

Parameter	Description
vlan-list	**Authenticable VLAN list**

Description

Defaults
The default is port-control authentication.

Command Mode

Interface configuration mode

Usage Guide

N/A

Configuration Examples

Use this command to configure the authenticable VLAN list.

```
QTECH (config-if-GigabitEthernet 0/1)# web-auth vlan-control1
```

Platform Description

N/A

6.1. Identifier Description

The following is a list of command identifiers used in commands for reference:

Identifier	Description
vlanlist	Authentication-exemption VLAN list
interval	Authenticated-user online-status detection interval
thredshold	The traffic threshold of authenticated-user online-status detection

6.2. authmanage user-escape

Use this command to enable user escape.

authmanage user-escape { **enable** | **time** *time-value1* | **when authentication-time** *time-value2* | **when timeout-ratio** *ratio-number* | **life** *life-value* }

Use this command to disable user escape.

```
no authmanage user-escape { enable | time | when authentication-time | when timeout-ratio | life }
```

Parameter Description

Parameter	Description
time-value1	Indicates the escape duration, in the unit of minutes.
time-value2	Indicates the authentication duration, in the unit of ms. When the value exceeds that of *time-value2*, part of users is allowed to escape for *time-value1* minutes.

ratio-number	When the ratio of authenticated users exceeds the value of ratio-number, part of users is allowed to escape for time-value1 minutes.
life-value	Indicates the escape lifetime, in the unit of minute.

Defaults *time-value1*:
The value is 30 minutes by default and can be set to 10 minutes to 240 minutes.
time-value2: The default value is 5,000, which indicates that part of users are allowed to escape when the average handling duration exceeds 5s. The value ranges from 1,000 to 10,000.
ratio-number: The default value is 10, which indicates that the part of users are allowed to escape when the ratio of timeout authentication users exceed 10%. The value ranges from 1 to 100.
life-value: The value is 30 minutes by default and can be set to 10 minutes to 240 minutes.

Command Mode
Global configuration mode

`Default Level` **14**

Usage Guide
User escape needs to be enabled only when the system is detected to fail timely authentication.

Configuration Examples
The following example enables user escape in global configuration mode.

```
QTECH(config)# authmanage user-escape enable
```

Verification Run **show authmanage user-escape** to display user escape configuration.

Prompt Messages

N/A

Common Errors

N/A

Platforms

This command is supported only on switches.

6.3. direct-vlan

Use this command to configure authentication-exemption VLANs.

direct-vlan *vlanlist*

Use this command to delete the authentication-exemption VLAN configuration.

no direct-vlan *vlanlist*

Parameter Description

Parameter	Description
vlanlist	VLAN list, which can be a VLAN or a group of VLANs.

Defaults

By default, no authentication-exemption VLANs are configured.

Command Mode

Global/Interface configuration mode

```
Default Level    14
```

Usage Guide

You can use this command to configure authentication-exemption VLANs, so that users in specified VLANs can access the Internet without experiencing dot1x or Web authentication. In interface configuration mode, the command

takes effect on users from authentication-exempted VLANs of the interface.

Configuration Examples

The following example configures the VLAN2 as an authentication-exemption VLAN.

```
QTECH(config)# direct-vlan 2
```

Verification Use the **show direct-vlan** command to display the authentication-exemption VLAN configuration.

Prompt Messages

N/A

Common Errors

N/A

Platforms N/A

6.4. nac-author-user maxinum

Use this command to configure the limit on IPv4 user capacity on a port.

nac-author-user maxinum *max-user-num*

Use this command to remove the limit on the IPv4 user capacity on a port.

no nac-author-user maxinum

Parameter Description

Parameter	Description
max-user-num	Defines the maximum number of IPv4 access users. The range is from 1 to 1,024.

Defaults

By default, the number of IPv4 access users is not limited.

Command Mode

Interface configuration mode

Default Level **14**

Usage Guide

Use this command to configure the maximum number of IPv4 access users on a port.

Configuration Examples

The following example restricts the maximum number of IPv4 users to 100 on interface Gi 0/1.

```
QTECH(config)#int gigabitEthernet 0/1
QTECH(config-if-GigabitEthernet 0/1)#nac-author-user maxinum 100
```

Verification 1.

Use the **show nac-author-user** command to display the current and the maximum numbers of IPv4 access users on all ports.

2. Use the **show nac-author-user interface** *interface-name* command to display the current and the maximum numbers of IPv4 access users on the specified port.

Prompt Messages

N/A

Common Errors

N/A

Platforms N/A

6.5. offline-detect interval threshold

Use this command to configure user online-status detection, so that a user is disconnected when its traffic is lower than a specified threshold or is zero in a specified interval.

offline-detect interval *interval* **threshold** *thredshold*

Use this command to restore the default user online-status detection configuration.

default offline-detect

Use this command to disable user online-status detection.

no offline-detect

Parameter Description

Parameter	Description
interval	Indicates the interval of traffic detection (in minutes). The range is from 1 to 65,535 in minutes on a non-switch device or from 6 to 65,535 in minutes on a switch.
threshold	Indicates the traffic threshold (in bytes). The range is from 0 to 4,294,967,294 in bytes. The value of 0 indicates that the user is disconnected when no traffic of the user is detected.

Defaults

By default, the detection interval is 8 hours and the traffic threshold is 0.

Command Mode

Global configuration mode

Default Level

14

Usage Guide

You can use this command to configure user online-status detection to enable the device to disconnect the authenticated user whose traffic is lower than a specified value and end accounting process.

Configuration Examples

The following example directly disconnects a user for the user's traffic is lower than 5 Kbytes within 5 minutes.

```
QTECH(config)#offline-detect interval 5 threshold5120
```

Verification Use the **show running** command to display the configuration of online-status detection for authenticated users.

Prompt Messages

N/A

Common Errors

N/A

Platforms N/A

6.6. show direct-vlan

Use this command to display the authentication-exemption VLAN configuration.
show direct-vlan

Parameter Description

Parameter	Description
interface-name	Interface name

Command Mode

Privileged EXEC mode

Level

14

Usage Guide

N/A

Configuration Examples

The following example displays the authentication-exemption VLAN configuration.

```
QTECH #show direct-vlan
```

```
direct-vlan 5,7,100
```

Prompt N/A

Messages

Platforms
N/A

6.7. show nac-author-user interface

Use this command to display the capacity limit and current number of IPv4 users on all interfaces or a specified interface.

show nac-author-user [**interface** *interface-name*]

Parameter Description

Parameter	Description
interface-name	Interface name

Command Mode

Privileged EXEC mode

Level

14

Usage Guide

N/A

Configuration Examples

The following example displays the current number and capacity limit of IPv4 users on interface Gi 0/1.

```
QTECH#show nac-author-user interface gi 0/1
Port   Cur_num  Max_num
Gi0/    0        100
```

Prompt Messages

N/A

Platforms

N/A

6.8. station-move permit

Use this command to enable authenticated-user migration.
station-move permit

Use this command to disable authenticated-user migration.
no station-move permit

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Authenticated-user migration is not permitted by default.

Command Mode

Global configuration mode

Level

14

Usage Guide

You can enable the authenticated-user migration function to allow the online users to be authenticated again and get online from different physical locations (different ports or VLANs).

Configuration Examples

The following examples enables authenticated-user migration.

```
QTECH(config)#station-move permit
```

Verification Use the **show running** command to check whether the authenticated-user migration function is enabled.

Prompt Messages

N/A

Common Errors

N/A

Platforms N/A

7. GLOBAL IP-MAC BINDING COMMANDS

7.1. address-bind

Use this command to configure global IP-MAC address binding. Use the **no** form of this command to restore the default setting.

address-bind { *ip-address* | *ipv6-address* } *mac-address*

no address-bind { *ip-address* | *ipv6-address* } *mac-address*

Parameter Description

Parameter	Description
ip-address	IPv4 address to be bound
ipv6-address	IPv6 address to be bound
mac-address	MAC address to be bound

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide **N/A**

Configuration Examples

The following example configures global IP-MAC address binding.

```
QTECH# configure terminal
Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)# address-bind 192.168.5.1 00d0.f800.0001
```

Related Commands

Command	Description
show address-bind	Displays the IP address-MAC address binding table.

Platform Description

N/A

7.2. address-bind install

Use this command to enable a binding policy globally. Use the **no** form of this command to restore the default setting.

```
address-bind  install no address-bind install
```

Parameter
Description

Parameter	Description
N/A	**N/A**

Defaults
N/A

Command Mode
Global configuration mode

Usage Guide

If you bind an IP address to a MAC address, run this command to make the installation policy take effect.

Configuration Examples
The following example enables a binding policy.

```
QTECH# configure terminal
Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)# address-bind
192.168.5.1 00d0.f800.0001 QTECH(config)# address-bind install
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

7.3. address-bind ipv6-mode

This command is used to set the IPv6 address binding mode. Use the **no** form of this command to restore the default setting.

This command is also used to set the compatible mode. **address-bind ipv6-mode** { **compatible** | **loose** | **strict** } **no address-bind ipv6-mode**

Parameter Description

Parameter	Description
compatible	Compatible mode
loose	Loose mode
strict	Strict mode

Defaults

The default is strict mode.

Command Mode

Global configuration mode.

Usage Guide

N/A

Configuration Examples

The following example configures the IPv6 address binding mode.

```
QTECH# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
QTECH(config)# address-bind ipv6-mode compatible
```

Related Commands

Command	Description
show address-bind uplink	Displays the exceptional port of the address binding.

Platform Description

N/A

7.4. address-bind uplink

This command is used to configure the exception port. Use the **no** form of this command to restore the default setting.

address-bind uplink *interface-id*

no address-bind uplink *interface-id*

Parameter Description

Parameter	Description
interface-id	Switching port or layer 2 aggregate port.

Defaults

All ports are non-exception ports by default.

Command Mode

Global configuration mode.

Usage Guide

If you have bound an IP address and a MAC address, the switch will discard the packets that have the same source IP address but different source MAC address.

If the port is an exceptional port and is installed (see address-bind install), this binding policy does not take effect.

Configuration Examples

The following example configures the exception port.

```
QTECH# configure terminal
Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)# address-bind
```

```
uplink GigabitEthernet 0/1
```

Related Commands

Command	Description
show address-bind uplink	Displays the exceptional port of address binding.

Platform Description

N/A

7.5. show address-bind

Use this command to display global IP address-MAC address binding.

show address-bind

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode.

```
Usage Guide
N/A
```

Configuration Examples

Related Commands

Platform Description

The following example displays global IPv4 address-MAC address binding.

```
QTECH#show address-bind
Total Bind Addresses in System : 1 IP Address  Binding MAC Addr



192.168.5.1    00d0.f800.0001
```

Field	Description
Total Bind Addresses in System	IPv4 address-MAC address binding count
IP Address	Bound IP address
Binding MAC Addr	Bound MAC address

Command	Description
address-bind	Enables IP address-MAC address binding.

N/A

7.6. show address-bind uplink

Use this command to display the exception port.

show address-bind uplink

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command mode

N/A

```
Usage Guide
```

N/A

Configuration Examples

Related Commands

Platform Description

The following example displays the exception port.

```
QTECH#show address-bind uplink Port     State


Gi0/1      Enabled Disabled
Default
```

Field	Description
Port	Short for exception ports. All ports are non-exception ports by default.
State	Indicates whether the port is exception port. State Enabled indicates that it is an exception port while state Disabled indicates that it it not.

Command	Description
address-bind uplink	Sets the exception port.

N/A

8.1. password policy life-cycle

Use this command to set the password lifecycle. Use the **no** form of this command to restore the default setting.

`password policy life-cycle` ***days***

no password policy life-cycle

Parameter Description

Parameter	Description
days	Sets the password lifecycle, in the range from 1 to 65,535 in the unit of days.

Defaults

No password lifecycle is set by default.

Command Mode

Global configuration mode

Usage Guide

This command is used to set the password lifecycle. After the password lifecycle expires, the system reminds you to change the password when you login next time.

This function is valid for the global password (the enable password and the enable secret commands) and the local user password (the username *name* password *password* command) while not valid for the password in line mode.

Configuration Examples

Related Commands

Platform Description

The following example sets the password lifecycle to 90 days.

```
QTECH(config)# password policy life-cycle 90
```

Command	Description
N/A	N/A

N/A

8.2. password policy min-size

Use this command to set the minimum length of the password. Use the **no** form of this command to restore the default setting.

```
password policy min-size length
```

no password policy min-size

Parameter Description

Parameter	Description
length	Sets the minimum length of the password, in the range from 1 to 31.

Defaults

No minimum length of the password is set by default.

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to set the minimum length of the password,

This function is valid for the global password (the enable password and the enable secret commands) and the local user password (the username *name* password *password* command)

while not valid for the password in line mode.

Configuration Examples

Related Commands

Platform Description

The following example sets the minimum length of the password to 8.

```
QTECH(config)# password policy min-size 8
```

Command	Description
N/A	N/A

N/A

8.3. password policy no-repeat-times

Use this command to ban the use of passwords used in the past several times.

Use the no form of this command to restore the default setting.

`password policy no-repeat-times` ***times***

no password policy no-repeat-times

Parameter Description

Parameter	Description
times	The past several times when passwords are configured, in the range from 1 to 31.

Defaults
This function is disabled by default.

Command Mode
Global configuration mode

Usage Guide
After this function is enabled, passwords used in the past several times are recorded. If the new password has been used, the alarm message is displayed and password configuration fails.

This command is used to set the maximum number of password entries. When the actual number of password entries exceeds the configured number, the new password overwrites the oldest password.

This function is valid for the global password (the enable password and the enable secret commands) and the local user password (the username *name* password *password* command) while not valid for the password in line mode.

Configuration Examples

Command	Description
N/A	N/A

Related Commands
The following example bans the use of passwords used in the past five times.
QTECH(config)# password policy no-repeat-times 5

Platform Description **N/A**

8.4. password policy strong

Use this command to enable strong password check.
password policy strong no password policy strong

Parameter Description

Parameter	Description

N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

If the following two kinds of passwords are set not matching the strength policy, the alarm message is displayed.

1. The password the same as the username.
2. The simple password containing only characters or numbers.

This function is valid for the global password (the enable password and the enable secret commands) and the local user password (the username *name* password *password* command)

while not valid for the password in line mode.

Configuration

The following example configures the strong password check.

Examples

```
QTECH(config)# password policy strong
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

8.5. service password-encryption

Use this command to encrypt a password. Use the **no** form of this command to restore default setting.

service password-encryption

no service password-encryption

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

This command is disabled by default. Various passwords are displayed in plain text, unless they are encrypted. After you run the **service password-encryption** and **show running** or **write** command to save your configuration, the password changes into cipher text. If you disable the command, the password in cipher text cannot be restored to plain text.

Configuration Examples

Related Commands

Platform Description

The following example encrypts the password:

```
QTECH(config)# service password-encryption
```

Command	Description

enable password	Sets passwords of different privileges.

N/A

8.6. show password policy

Use this command to display the password security policy set by the user.

show password policy

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide This command is used to display the password security policy set by the user.

Configuration Examples

Related Commands

Platform Description

The following example displays the password security policy set by the user.

```
QTECH#show password policy
Global password policy configurations:
Password encryption:       Enabled
Password strong-check:     Enabled
Password min-size:  Enabled (6 characters)
Password life-cycle:       Enabled (90 days)
Password no-repeat-times:  Enabled (max history record: 5)
```

Field	Description
Password encryption	Whether to encrypt the password.
Password strong-check	Whether to enable password strong-check.
Password min-size	Whether to set the minimum length of the password.
Password life-cycle	Whether to set the password lifecycle.
Password no-repeat-times	

Command	Description
N/A	N/A

N/A

9.1. switchport port-security

Use this command to configure port security and the way to deal with violation. Use the **no** form of this command to restore the default setting.

switchport port-security [**violation** { **protect | restrict | shutdown** }]

no switchport port-security [**violation**]

Parameter Description

Parameter	Description
protect	Discards the packets breaching security.
restrict	Discards the packets breaching security and sends the Trap message.
shutdown	Discards the packets breaching the security, sends the Trap message and disables the interface.

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

With port security, you can strictly control the input on a specific port by restricting access to the MAC address and IP address (optional) of the port on the switch. After you configure some secure addresses for the port security-enabled port, only the packets from these addresses can be forwarded. In addition, you can also restrict the maximum number of secure addresses on a port. If you set the maximum value to 1 and configure one secure address for

this port, the workstation (whose address is the configured secure Mac address) connected to this port will occupy all the bandwidth of this port exclusively.

If the violation handling mode is changed after violation occurs, the new mode takes effect only after the violation mode is restarted.

Configuration Examples

The following example enables port security on interface gigabitethernet 1/1, and the way to deal with violation is **shutdown**:

```
QTECH(config)#interface gigabitethernet 1/1 QTECH(config-if)# switchport port-security
QTECH(config-if)# switchport port-security violation shutdown
```

Related Commands

Command	Description
show port-security	Displays port security settings.

Platform Description

N/A

9.2. switchport port-security aging

Use this command to set the aging time for all secure addresses on an interface. Use the **no** form of this command to restore the default setting.

`switchport port-security aging {static | time time }`

no switchport port-security aging {**static** | **time** }

Parameter Description

Parameter	Description

static	Applies the aging time to both manually configured secure addresses and automatically learned addresses. Otherwise, apply it to only the automatically learned secure addresses.
time *time*	Specifies the aging time for the secure address on this port. Its range is 0-1,440 in minutes. If you set it to 0, the aging function is disabled actually.

Defaults

No secure address is aged by default.

Command Mode

Interface configuration mode

Usage Guide

In interface configuration mode, use the **no switchport port-security aging time** command to disable the aging for security addresses on the port. Use the **no switchport port-security aging static** command to apply the aging time to only the dynamically learned security address.
Use the **show port-security** command to display configuration.
When both port security and 802.1X authentication functions are enabled, 802.1X clients must get re-authenticated for network access once the secure addresses are aged.

To enable this function, you need to set the maximum number of secure addresses. In this way, you can make the switch automatically add or delete the secure addresses on the interface.

Configuration Examples

The following example sets the aging time for all secure addresses on interface gigabitethernet 1/1 to eight minutes.

```
QTECH# configure terminal
QTECH(config)# interface gigabitethernet 1/1 QTECH(config-if)# switchport port-security aging time 8 QTECH(config-if)# switchport port-security aging static QTECH(config-if)# end
```

Related

Commands

Command	Description
show port-security	**Displays port security settings.**

Platform Description

N/A

9.3. switchport port-security binding

Use these commands to configure secure address binding manually in the interface configuration mode through performing the source IP address plus source MAC address binding or only the source IP address binding. With this binding configured, only the packets match the binding secure address could enter the switch, others will be discarded.

Use the **no** form of these commands to remove the binding addresses.

switchport port-security binding [*mac-address* **vlan** *vlan_id*] { *ipv4-address* | *ipv6-address* }

switchport port-security binding { *ipv4-address* | *ipv6-address* }

no switchport port-security binding [*mac-address* **vlan** *vlan_id*] { *ipv4-address* | *ipv6-address* }

no switchport port-security binding { *ipv4-address* | *ipv6-address* }

Parameter Description

Parameter	Description
mac-address	The source MAC addresses to be bound
vlan_id	VLAN ID of the binding source MAC address
ipv4-address	Binds IPv4 addresses.

ipv6-address	Binds IPv6 addresses.

Defaults
N/A

Command Mode

Interface configuration mode

Usage Guide

- For packets complying with IP/IP-MAC binding, they can be forwarded only if MAC addresses are secure addresses.
- For dynamic secure addresses, packets cannot be forwarded before bound even if their addresses comply with the binding list.

Network is often accessible to static users with secure addresses without authorization. If authorization is configured, these users must comply with it.

Configuration Examples

The following example binds the IP address 192.168.1.100 on interface g 0/10:

```
QTECH# configure terminal QTECH(config)#interface gigabitethernet 0/10
QTECH(config-if)# switchport port-security binding 192.168.1.100
QTECH(config-if)# end
```

The following example binds the IP address 192.168.1.100 and MAC address 00d0.f800.5555 with VLAN ID 1 on interface g 0/10.

```
QTECH# configure terminal QTECH(config)#interface gigabitethernet 0/10
QTECH(config-if)# switchport port-security binding 00d0.f800.5555 vlan 1 192.168.1.100
QTECH(config-if)# end
```

Related Commands

Command	Description
show port-security	Displays port security settings.
switchport port-security	Enables the port-security.
switchport port-security binding interface	Configures the secure address binding in privileged EXEC mode.

switchport port-security mac-address	Sets the static secure address.
switchport port-security aging	Sets the aging time for secure address.

Platform Description

N/A

9.4. switchport port-security binding-filter logging

Use this command to enable binding filter logging.
Use the **no** form of these commands to restore

the default setting. **switchport port-security binding-filter logging** [**rate-limit** *rate*] **no switchport port-security binding-filter logging**

Parameter Description

Parameter	Description
rate-limit *rate*	Indicates the printing rate of binding filter logging. The default rate is 10logs/minute. The configurable range is from 1 to 120 logs per minute.

Defaults

By default, binding filter logging is disabled.

Command Mode

Global configuration mode

Usage Guide

- If you run the **switchport port-security binding-filter logging** command without configuring the *rate* parameter, binding filter logging is enabled and the default printing rate, 10logs/minute, is adopted.
- After binding filter logging is enabled, for packets that do not comply with IP/IP-MAC binding, warmings are printed.

- After binding filter logging is enabled, if the printing rate exceeds the configured rate, the number of suppressed packets is displayed.

Configuration Examples

The following example enables binding filter logging.

```
QTECH# configure terminal
QTECH(config)# switchport port-security binding-filter logging QTECH(config)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

9.5. switchport port-security interface binding

Use these commands to configure secure address binding manually in the privileged EXEC mode through performing the source IP address plus source MAC address binding or only the source IP address binding. With this binding configured, only the packets match the binding secure address could enter the switch, others will be discarded.

Use the **no** form of these commands to remove the binding addresses.

switchport port-security interface i*nterface-id* **binding** [*mac-address* **vlan** *vlan_id*] {*ipv4-address* | *ipv6-address* }

switchport port-security interface *interface-id* **binding** { *ipv4-address* | *ipv6-address* }

no switchport port-security interface i*nterface-id* **binding** [*mac-address* **vlan** *vlan_id*] { *ipv4-address* | *ipv6-address* }

no switchport port-security interface *interface-id* **binding** { *ipv4-address* | *ipv6-address* }

Parameter Description

Parameter	Description

interface-id	Binds interface ID.
mac-address	Binds source MAC address.
vlan_id	VLAN ID of the binding source MAC address
ipv4-address	Binds IPv4 address.
ipv6-address	Binds IPv6 address .

Defaults
N/A

Command Mode
Global configuration mode

Usage Guide

- For packets complying with IP/IP-MAC binding, they can be forwarded only if MAC addresses are secure addresses.
- For dynamic secure addresses, packets cannot be forwarded before bound even if their addresses

comply with the binding list.

Configuration Examples
The following example binds the IP address 192.168.1.100 on the interface g 0/10.

```
QTECH# configure terminal
QTECH(config)# switchport port-security binding interface g0/10 binding 192.168.1.100
QTECH(config)# end
```

The following example binds the IP address 192.168.1.100 and MAC address 00d0.f800.5555 with VLAN ID 1 on the interface g 0/10.

```
QTECH# configure terminal
QTECH(config)# switchport port-security binding interface g0/10 binding 00d0.f800.5555 vlan
1 192.168.1.100
QTECH(config)# end
```

Related Commands

Command	Description
show port-security	Displays port security settings.

switchport port-security	Enables the port-security.
switchport port-security binding	Configures the secure address binding in interface configuration mode.
switchport port-security mac-address	Sets the static secure address.
switchport port-security aging	Sets the aging time for secure address.

Platform Description

N/A

9.6. switchport port-security mac-address

Use this command to configure the static secure address.

Use the **no** form of this command to remove the configuration.

switchport port-security mac-address *mac-address* [vlan *vlan-id*] no switchport port-security mac-address *mac-address* [vlan *vlan-id*]

Parameter Description

Parameter	Description
mac-address	Static secure MAC address
vlan-id	VLAN ID of the MAC address The configuration of vlan-id is only supported on the TRUNK port.

Defaults
N/A

Command Mode

Interface configuration mode

Configuration Examples

The following example sets the static secure address and VLAN ID of TRUNK port 10 to 00d0.f800.5555 and 2 respectively.

```
QTECH# configure terminal QTECH(config)#interface gigabitethernet 0/10
QTECH(config-if)# switchport port-security mac-address 00d0.f800.5555 vlan 2
QTECH(config-if)# end
```

Related Commands

Command	Description
show port-security	Displays port security settings.
switchport port-security	Enables the port-security.
switchport port-security binding	Configures the secure address binding.
switchport port-security mac-address interface	Sets the static secure address in privileged EXEC mode.
switchport port-security aging	Sets the aging time for the secure address.

Platform Description

N/A

9.7. switchport port-security interface mac-address

Use this command to configure the static secure address.
Use the **no** form of this command to remove the configuration.
switchport port-security interface *interface-id* **mac-address** *mac-address* [**vlan** *vlan-id*]
no switchport port-security interface *interface-id* **mac-address** *mac-address* [**vlan** *vlan-i*]

Parameter Description

Parameter	Description
interface-id	Interface ID
mac-address	Static secure address
vlan-id	VLAN ID of the MAC address The configuration of vlan-id is only supported on the TRUNK port.

Defaults
N/A

Command Mode
Glocal configuration mode

Usage Guide
N/A

Configuration Examples

The following example sets the static secure address and VLAN ID of TRUNK port 10 to 00d0.f800.5555 and 2 respectively.

```
QTECH# configure terminal
QTECH(config)# switchport port-security interface g0/10 mac-address 00d0.f800.5555 vlan 2
QTECH(config)# end
```

Related Commands

Command	Description
show port-security	Displays port security settings.
switchport port-security	Enables the port-security.
switchport port-security binding	Configures the secure address binding.

switchport port-security mac-address	Sets the static secure address in interface configuration mode.
switchport port-security aging	Sets the aging time for the secure address.

Platform Description

N/A

9.8. switchport port-security maximum

Use this command to set the maximum number of port secure addresses. Use the **no** form of this command to restore the default setting. **switchport port-security maximum** *value*

no switchport port-security maximum

Parameter Description

Parameter	Description
value	Maximum number of the secure address, in the range from 1 to 128.

Defaults
The default is 128.

Command Mode

Interface configuration mode

Usage Guide

The number of the secure address contains the sum of static secure address and dynamically learnt secure address, 128 by default.

If the number of the secure address you set is less than current number, it will prompt this setting failure.

Configuration Examples

The following example sets the maximum number of the secure address to 2 for interface g 0/10.

```
QTECH# configure terminal QTECH(config)#interface gigabitethernet 0/10
QTECH(config-if)# switchport port-security maximum 2
QTECH(config-if)# end
```

Related Commands

Command	Description
show port-security	Displays port security settings.
switchport port-security	Enables the port-security.
switchport port-security binding	Configures the secure address binding.
Switchport port-security mac-address	Sets the static secure address in the interface configuration mode.
switchport port-security aging	Sets the aging time for the port secure address.

Platform Description

N/A

9.9. switchport port-security mac-address sticky

Use this command to configure the Sticky MAC secure address. Use the **no** form of this command to restore the default setting.

switchport port-security mac-address sticky *mac-address* [**vlan** *vlan-id*]

no switchport port-security mac-address sticky *mac-address* [**vlan** *vlan-id*] Use the command without parameters to enable the Sticky MAC address learning. Use the **no** form of this command to disable the Sticky MAC address learning. **switchport port-security mac-address sticky**

no switchport port-security mac-address sticky

Parameter Description

Parameter	Description
mac-address	Static secure address
vlan-id	Vlan ID of the MAC address The configuration of vlan-id is only supported on the TRUNK port.

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

Sticky MAC addresses, either static or dynamic, are special addresses free from aging.

Configuration Examples

The following example sets the MAC address and VLAN ID of TRUNK port 10 to 00d0.f800.5555 to 2 respectively.

```
QTECH# configure terminal QTECH(config)#interface gigabitethernet 0/10
QTECH(config-if)# switchport port-security mac-address 00d0.f800.5555 vlan 2
QTECH(config-if)# end
```

```
QTECH# configure terminal QTECH(config)#interface gigabitethernet 0/10
QTECH(config-if)# switchport port-security sticky mac-address
QTECH(config-if)# end
```

The following example enables the Sticky MAC address learning on interface g0/10.

Related Commands

Command	Description
show port-security	Displays port security settings.

switchport port-security	Enables the port-security.
switchport port-security binding	Configures the secure address binding.
switchport port-security mac-address interface	Sets the static secure address in privileged EXEC mode.
switchport port-security mac-address	Sets the static secure address in interface configuration mode.
switchport port-security aging	Sets the aging time for the secure address.

Platform Description

N/A

9.10. show port-security

Use this command to display the port security configuration and the secure address.

show port-security [**address** [**interface** *interface-id*] | **binding** [**interface** *interface-id*] | **interface**
interface-id | **all**]

Parameter Description

Parameter	Description
address	Displays all secure addresses, or the secure address of the specified port.
binding	Displays all port security bindings, or the port security bindings of the specified port.
interface *interface-id*	Displays the port security configuration of the specified port.
all	Displays all valid secure addresses and valid port security bindings.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

To display all port security configuration and violation management, execute the command without any parameter. To display the security configuration, the secure address, or the port security binding of the specified interface, execute the command with the corresponding parameter.

Configurati on Examples

The following example displays the port security statistics.

```
QTECH#show port-security
NO.  SecurePort  MaxSecureAddr  CurrentAddr  CurrentIpBind  CurrentIpMacBind
SecurityAction
(Count)       (Count)       (Count)       (Count)




1    Gi0        128     2          2          1             protect
     /1


Total secure addresses in System : 2 Total secure bindings in System : 3
```

Field	Description
NO.	Serial number.
Secure Port	Port name
MaxSecureAddr(count)	The maximum number of secure addresses on the port.
CurrentAddr(count)	The current number of secure addresses on the

	port.
CurrentIpBind (count)	The current number of IP addresses bindings on the port.
CurrentIpMacBind (count)	The current number of IP-MAC address bindings on the port.
Security Action	Violation management.
Total secure addresses in System	The total number of secure addresses on the device.
Total secure bindings in System	The total number of port security bindings on the device,

The following example displays the port security configuration on interface Gigabitethernet 0/1.

```
QTECH#show port-security interface gigabitEthernet 0/1 Interface  : GigabitEthernet 0/1
Port status   : down
Port Security: enabled
SecureStatic address aging             : disabled Sticky dynamic address             :
disabled Violation mode    : protect
Maximum MAC Addresses      : 128
Total MAC Addresses : 2 Configured MAC Addresses                  : 2 Dynamic MAC Addresses
             : 0
Sticky MAC Addresses       : 0 Total security binding       : 3 IPv4-ONLY Binding Addresses
: 1 IPv6-ONLY Binding Addresses : 1 IPv4-MAC Binding Addresses                 : 1 IPv6-MAC
Binding Addresses                : 0
Aging time(min)     : 0
```

Field	Description
Interface	Port name.
Port status	Port status.
Port Security	Displays whether the port security is enabled.

SecureStatic address aging	Displays whether the static secure address aging is enabled.
Sticky dynamic address	Displays whether the dynamic secure address is converted to the sticky secure address,
Violation mode	Port violation management.
Maximum MAC Addresses	The maximum number of secure addresses on the port.
Total MAC Addresses	The number of valid secure addresses on the port.
Configured MAC Addresses	The number of static secure addresses.
Dynamic MAC Addresses	The number of dynamic secure addresses.
Sticky MAC Addresses	The number of sticky secure addresses,
Total security binding	The number of valid port security bindings.
IPv4-ONLY Binding Addresses	The number of IPv4 addresses bindings.
IPv6-ONLY Binding Addresses	The number of IPv6 addresses bindings.
IPv4-MAC Binding Addresses	The number of IPv4-MAC address bindings.
IPv6-MAC Binding Addresses	The number of IPv6-MAC address bindings.
Aging time(min)	The aging time of the secure address.

```
QTECH#show port-security address
NO. VLAN MacAddress    TYPE   RemainingAge(mins) mins
STATUS
```

```
1               00d0.f800.073c GigabitEthernet 0/1      Configured  -
2      1      00d0.f800.073d  GigabitEthernet 0/1     Configured    -- active
```

The following example displays all secure addresses on the device.

Field	Description
NO.	Serial number.
Vlan	VLAN ID.
Mac Address	MAC address.
Port	Port name.
Type	Secure address type.
Remaining Age(mins)	The aging time of the secure address.
STATUS	The secure address status.

Related Commands

Platform Description

The following example displays all port security bindings on the device.

```
QTECH#show port-security binding
NO.  VLAN MacAddress PORT   IpAddress FilterType FilterStatus




1      1      00d0.f800.073c Gi0/1 192.168.12.202      ipv4-mac
active
2      --     --     Gi0/1  192.168.0.1  ipv4-only active
3      --     --     Gi0/1  ffaa:ddcc::1 ipv6-only
activ
```

Field	Description
NO.	Serial number.

Vlan	VLAN ID.
Mac Address	MAC address.
Port	Port name.
IpAddress	IP address.
FilterType	The filtering type of the port security binding.
FilterStatus	The status of the port security binding.

Command	Description
N/A	N/A

N/A

10.1. show storm-control

Use this command to display storm suppression information.

show storm-control [*interface-type interface-number*]

Parameter Description

Parameter	Description
interface-type interface-number	Specifies an interface.

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example displays storm control configuration on FastEthernet 0/1.

```
QTECH# show storm-control fastEthernet 0/1
Interface    Broadcast Control Multicast Control Unicast Control Action


FastEthernet 0/1          1%       50%             1%        none
```

Command	Description
storm-control	Enables storm suppression.

N/A

10.2. storm-control

Use this command to enable the storm suppression for unknown unicast packets. Use the **no** or **default** form of this command to restore the default setting.

storm-control unicast [{ **level** *percent* | **pps** *packets* | *rate-bps* }]

no storm-control unicast default storm-control unicast

Parameter Description

Use this command to enable the storm suppression for multicast packets. Use the **no** or **default** form of this command to restore the default setting. **storm-control multicast** [{ **level** *percent* | **pps** *packets* | *rate-bps* }]

no storm-control multicast default storm-control multicast

Use this command to enable the storm suppression for broadcast packets. Use the **no** or **default** form of this command to restore the default setting. **storm-control broadcast** [{ **level** *percent* | **pps** *packets* | *rate-bps* }]

no storm-control broadcast default storm-control broadcast

Parameter	Description
level *percent*	Sets the bandwidth percentage, for example, 20 means 20%.
pps *packets*	Sets the pps, which means packets per second.
rate-bps	Rate allowed

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

Too many broadcast, multicast or unicast packets received on a port may cause storm and thus slow network and increase timeout. Protocol stack implementation errors or wrong network configuration may also lead to such storms.

A device can implement the storm suppression to a broadcast, a multicast, or a unicast storm respectively. When excessive broadcast, multicast or unknown unicast packets are received, the switch temporarily prohibits forwarding of relevant types of packets till data streams are recovered to the normal state (then packets will be forwarded normally).

Configuration Examples

The following example enables the multicast storm suppression on FastEthernet 0/1 and sets the allowed rate to 4M.

```
QTECH(config)# int fastEthernet 0/1
QTECH(config-if-FastEthernet 0/1)# storm-control multicast 4096
```

Related Commands

Command	Description
show storm-control	Displays storm suppression information.

Platform Description

N/A

11.1. crypto key generate

Use this command to generate a public key to the SSH server.
crypto key generate { **rsa | dsa** }

Parameter Description

Parameter	Description
rsa	Generates an RSA key.
dsa	Generates a DSA key.

Defaults
By default, the SSH server does not generate a public key.

Command Mode

Global configuration mode

Usage Guide

When you need to enable the SSH SERVER service, use this command to generate a public key on the SSH server and enable the SSH SERVER service by command **enable service ssh-server** at the same time. SSH 1 uses the RSA key; SSH 2 uses the RSA or DSA key. Therefore, if a RSA key has been generated, both SSH1 and SSH2 can use it. If only a DSA key is generated, only SSH2 can use it.

Only DSA/RSA authentication is available for one connection. Also, the key algorithm may differ in different client. Thus, it is recommended to generate both RSA and DSA keys so as to ensure connection with the portal server.

RSA has a minimum modulus of 512 bits and a maximum modulus of 2,048 bits; DSA has a minimum modulus of 360 bits and a maximum modulus of 2,048 bits. For

some clients like SCP

clients, a 768-bit or more key is required. Thus, it is recommended to generate

the key of 768 bits or more.

A key can be deleted by using the **no crypto key generate** command. The **no crypto key zeroize** command is not available.

Configuration Examples

The following example generates an RSA key to the SSH server.

```
QTECH# configure terminal
QTECH(con fig)# crypto key generate rsa
```

Related Commands

Command	Description
show ip ssh	Displays the current status of the SSH server.
crypto key zeroize { **rsa** | **dsa** }	Deletes DSA and RSA keys and disables the SSH server function.

Platform Description

N/A

11.2. crypto key zeroize

Use this command to delete a public key to the SSH server.

```
crypto key zeroize { rsa | dsa }
```

Parameter Description

Parameter	Description
rsa	Deletes the RSA key.
dsa	Deletes the DSA key.

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

This command deletes the public key to the SSH server. After the key is deleted, the SSH server state becomes DISABLE. If you want to disable the SSH server, run the **no enable service ssh-server** command.

Configuration Examples

The following example deletes a RSA key to the SSH server.

```
QTECH# configure terminal
QTECH(config)# crypto key zeroize rsa
```

Related Commands

Command	Description
show ip ssh	Displays the current status of the SSH server.
crypto key generate { **rsa | dsa** }	Generates DSA and RSA keys.

Platform Description

N/A

11.3. disconnect ssh

Use this command to disconnect the established SSH connection.

disconnect ssh [**vty**] *session-id*

Parameter Description

Parameter	Description
vty	Established VTY connection
session-id	ID of the established SSH connection, in the range

	from 0 to 35

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide

You can disconnect a SSH connection by entering the ID of the SSH connectionor disconnect a SSH connection by entering the specified VTY connection ID. Only connections of the SSH type can be disconnected.

Configuration Examples

Related Commands

Platform Description

The following example disconnects the established SSH connection by specifying the SSH session ID.

```
QTECH# disconnect ssh 1
```

The following example disconnects the established SSH connection by specifying the VTY session ID.

```
QTECH# disconnect ssh vty 1
```

Command	Description
show ssh	Displays the information about the established SSH connection.
clear line vty *line_number*	Disconnects the current VTY connection.

N/A

11.4. ip scp server enable

Use this command to enable the SCP server function on a network device. Use the **no** form of this command to restore the default setting.

ip scp server enable

no ip scp server enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

Secure Copy (SCP) enables an authenticated user to transfer files to/from a remote device in an encrypted way, with high security and guarantee.

Configuration Examples

The following example enables the SCP server function.

```
QTECH# configure terminal
QTECH(config)# ip scp server enable
```

Related Commands

Command	Description

show ip ssh	Displays the current status of the SSH server.

Platform Description

N/A

11.5. ip scp server topdir

Use this command to set the path for uploading/downloading files to/from the SCP server. Use the **no** form of this command to restore the default settings.

ip scp server topdir {flash:*/path* **| flash2:***/path* **| usb0:***/path* **| usb1:***/path* **| sd0:***/path* **| sata0:***/path* **| tmp:***/path* **}**

no ip scp server topdir

Parameter Description

Parameter	Description
flash	Selects the file transfer path from the extended flash memory. The file transfer path is **flash:/** by default.
flash2	Selects the file transfer path from Extended Flash Memory 2. This option is supported only when the device has the data2 partition.
usb0	Selects the file transfer path from USB Disk 0. This option is supported only when the device has one USB interface and is connected with an extended USB device.
usb1	Selects the file transfer path from USB Disk 1. This option is supported only when the device has two USB interfaces and is connected with extended USB devices.
sd0	Selects the file transfer path from the SD card. This option is supported only when the device has an SD card interface and is connected with an extended SD card.

sata0	Selects the file transfer path from the hard disk. This option is supported only when the device has the SATA partition.
tmp	Sets the file transfer path to **tmp/vsd/**.

Defaults
The file transfer path is **flash:/** by default.

Command Mode

Global configuration mode

Default Level14

Usage Guide This command is used to change the file transfer path for uploading and downloading files.

Configuration Examples

```
QTECH# configure terminal
```

The following example changes the file transfer path to **tmp/vsd**.

```
QTECH(config)# ip scp server topdir tmp:/
```

11.6. ip ssh access-class

Use this command to set the ACL filtering of the SSH server.
ip ssh access-class { *access-list-number* | *access-list-name* }

Use the **no** form of this command to delete the ACL filtering of the SSH server.
no ip ssh access-class

Parameter Description

Parameter	Description
access-list-number	The ACL number and the number range is configurable. The standard ACL number ranges are 1 to 99 and 1,300 to 1,999. The extended ACL number ranges are 100 to 199 and 2,000 to 2,699.

access-list-name	An ACL name.

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

Run this command to perform ACL filtering for all connections to the SSH server.

In line mode, ACL filtering is performed only for specific lines. However, ACL filtering rules of the SSH are effective to all SSH connections.

Configuration Examples

The following example performs the ACL filtering named testv4 for all connections to the SSH server.

```
QTECH# configure terminal

QTECH(config)# ip ssh access-class testv4
```

Platform Description

N/A

11.7. ip ssh authentication-retries

Use this command to set the authentication retry times of the SSH server. Use the **no** form of this command to restore the default setting.

ip ssh authentication-retries *retry times*

no ip ssh authentication-retries

Parameter Description

Parameter	Description
retry times	Authentication retry times, ranging from 0 to 5

Defaults
The default is 3.

Command Mode
Global configuration mode

Usage Guide

User authentication is considered failed if authentication is not successful when the configured authentication retry times on the SSH server is exceeded. Use the **show ip ssh** command to display the configuration of the SSH server

Configuration Examples
The following example sets the authentication retry times to 2.

```
QTECH# configure terminal
QTECH(config)# ip ssh authentication-retries 2
```

Related Commands

Command	Description
show ip ssh	Displays the current status of the SSH server.

Platform Description

N/A

11.8. ip ssh cipher-mode

Parameter Description
Use this command to set the SSH server encryption mode. Use the **no** form of this command to restore the default setting. **ip ssh cipher-mode** { **cbc** | **ctr** | **others** }

no ip ssh cipher-mode

Parameter	Description
cbc	Encryption mode: CBC (Cipher Block Chaining) Encryption algorithm: DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-

	256-CBC, Blow fish-CBC
ctr	Encryption mode: CTR (Counter) Encryption algorithm: AES128-CTR, AES192-CTR, AES256-CTR
others	Encryption mode: Others Encryption algorithm: RC4

Defaults

All encryption modes are supported by default.

Command Mode

Global configuration mode

Usage Guide

This command is used to set the SSH server encryption mode.

For QTECH Networks, the SSHv1 server supports DES-CBC, 3DES-CBC, and Blowfish-CBC; the SSHv2 server supports AES128-CTR, AES192-CTR, AES256-CTR, DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC, Blowfish-CBC, and RC4. All these algorithms can be grouped into CBC, CTR and Other as shown above.

With the advancement of cryptography study, CBC and Others encryption modes are proved to easily decipher. It is recommended to enable the CTR mode to raise assurance for organizations and enterprises demanding high security.

Configuration Examples

The following example enables CTR encryption mode.

```
QTECH# configure terminal
QTECH(config)# ip ssh cipher-mode ctr
```

Platform Description

N/A

11.9. ip ssh hmac-algorithm

Parameter Description

Use this command to set the algorithm for message authentication. Use the **no** form of this command to restore the default setting.

```
ip ssh hmac-algorithm { md5 | md5-96 | sha1 | sha1-96 }
```

no ip ssh hmac-algorithm

Parameter	Description
md5	MD5 algorithm
md5-96	MD5-96 algorithm
sha1	SHA1 algorithm
sha1-96	SHA1-96 algorithm

Defaults

SSHv1: all the algorithms are not supported.

SSHv2: all the algorithms are supported.

Command Mode

Global configuration mode

Usage Guide

QTECH SSHv1 servers do not support algorithms for message authentication. For QTECH Networks, the SSHv1 server does not support message authentication algorithms; the SSHv2 server supports MD5, MD5-96, SHA1, and SHA1-96 algorithms. Set the algorithm on your demand.

Configuration Examples

The following example sets the algorithm for message authentication to SHA1.

```
QTECH# configure terminal
QTECH(config)# ip ssh hmac-algorithm sha1
```

Platform Description

N/A

11.10. ip ssh key-exchange

Use this command to configure support for DH key exchange method on the SSH server

Parameter Description

Use the **no** form of this command to restore the default setting.

ip ssh key-exchange { dh_group_exchange_sha1 | dh_group14_sha1 | dh_group1_sha1 } no ip ssh key-exchange

Parameter	Description
dh_group_exchange_sha1	Indicates configuration of diffie-hellman-group-exchange-sha1 for keyexchange. The key has 2,048 bytes, which cannot be edited.
dh_group14_sha1	Indicates configuration of diffie-hellman-group14-sha1 for keyexchange. The key has 2,048 bytes.
dh_group1_sha1	Indicates configuration of diffie-hellman-group1-sha1 for keyexchange. The key has 1,024 bytes.

Defaults

By default, the SSHv1 server does not support DH key exchange method, while the SSHv2 server supports diffie-hellman-group-exchange-sha1 and diffie-hellman-group14-sha1 for key exchange.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

The following example configures the support for diffie-hellman-group14-sha1.

```
QTECH# configure terminal

QTECH(config)# ip ssh key-exchange dh_group14_sha1
```

Related Commands

Command	Description
show ip ssh	Displays the current status of the SSH server.

Platform Description

N/A

11.11. ip ssh peer

Parameter Description

Use this command to associate the public key file and the user name on the client. During client login authentication, you can specify a public key file based on the user name.

Use the **no** form of this command to restore the default setting.

ip ssh peer *username* **public-key** { **rsa** | **dsa** } *filename*

no ip ssh peer *username* **public-key** { **rsa** | **dsa** } *filename*

Parameter	Description
username	User name
filename	Name of a public key file
rsa	The public key is a RSA key
dsa	The public key is a DSA key

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide **N/A**

Configuration Examples

The following example sets RSA and DSA key files associated with user **test**.

```
QTECH# configure terminal
QTECH(config)# ip ssh peer test public-key rsa flash:rsa.pub QTECH(config)# ip ssh peer test public-key dsa flash:dsa.pub
```

Related Commands

Command	Description
show ip ssh	Displays the current status of the SSH server.

Platform Description

N/A

11.12. ip ssh port

Use this command to set a monitoring port ID for the SSH server.

ip ssh port *port*

Use either of the following commands to restore the monitoring port ID of the SSH server to the default value.

no ip ssh port ip ssh port 22

Parameter Description

Parameter	Description
port	Monitoring port ID of the SSH server. The value ranges from 1025 to 65535.

Defaults

N/A

Command Mode

Global configuration mode

```
Default Level
14
```

Usage Guide

N/A

Configuratio n Examples

The following example sets the monitoring port ID of the SSH server to 10000.

```
QTECH# configure terminal
QTECH(config)# ip ssh port 10000
```

Verification Run the **show ip ssh** command to display the configured monitoring port ID of the SSH server.

Prompts

1. If the required port ID is the same as the current value, a prompt is displayed, indicating that the current port ID is the required value.

```
QTECH(config)# ip ssh port 22
% SSH tcp-port has been 22
```

If a port in the monitoring state is configured as the monitoring port of the SSH server, a prompt is displayed, indicating that the port is already in the monitoring state and you are required to set another port ID, and the SSH server still uses the previous port ID.

```
QTECH(config)# ip ssh port 10000
% SSH open tcp-port(10000) failed, please use another tcp-port, otherwise the system will use the old tcp-port(22)!
```

If a monitoring error occurs after a monitoring port ID is configured for the SSH server, a port ID configuration failure prompt is displayed.

```
QTECH(config)# ip ssh port 10000
% SSH change to tcp-port(10000) fail!
```

If a port ID is configured successfully, a port ID configuration success prompt is displayed.

```
QTECH(config)# ip ssh port 10000
% SSH change to tcp-port(10000) success!
```

11.13. ip ssh time-out

Use this command to set the authentication timeout for the SSH server. Use the **no** form of this command to restore the default setting.

```
ip ssh time-out time
```

no ip ssh time-out

Parameter Description

Parameter	Description
time	Authentication timeout, in the range from 1 to 120 in the unit of seconds

Defaults
The default is 120 seconds.

Command Mode

Global configuration mode

Usage Guide

The authentication is considered timeout and failed if the authentication is not successful within 120 seconds starting from receiving a connection request. Use the **show ip ssh** command to display the configuration of the SSH server.

Configuration Examples

The following example sets the timeout value to 100 seconds.

```
QTECH# configure terminal
```

Related Commands

Platform Description

```
QTECH(config)# ip ssh time-out 100
```

Command	Description
show ip ssh	Displays the current status of the SSH server.

N/A

11.14. ip ssh version

Use this command to set the version of the SSH server.

Use the **no** form of this command to restore the default setting.

ip ssh version { **1** | **2** }

no ip ssh version

Parameter Description

Parameter	Description
1	Supports the SSH1 client connection request.
2	Supports the SSH2 client connection request.

Defaults

SSH1 and SSH2 are compatible by default.

Command Mode

Global configuration mode

Usage Guide

This command is used to configure the SSH connection protocol version supported by SSH server. By default, the SSH server supports SSH1 and SSH2. If Version 1 or 2 is set, only the SSH client of this version can connect to the SSH server. Use the **show ip ssh** command to display the current status of SSH server.

Configuration Examples

The following example sets the version of the SSH server.

```
QTECH# configure terminal
QTECH(config)# ip ssh version 2
```

Related Commands

Command	Description
show ip ssh	Displays the current status of the SSH server.

Platform Description

N/A

11.15. ipv6 ssh access-class

Use this command to set the IPv6 ACL filtering of the SSH server.

ipv6 ssh access-class *accessv6-list-name*

Parameter Description

Use the **no** form of this command to delete the IPv6 ACL filtering of the SSH server.

no ipv6 ssh access-class

Parameter	Description
accessv6-list-name	An IPv6 ACL name.

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

Run this command to perform IPv6 ACL filtering for all connections to the SSH server. In line mode, IPv6 ACL filtering is performed only for specific lines. However, IPv6 ACL filtering rules of the SSH are effective to all SSH connections.

Configuration Examples

The following example performs the IPv6 ACL filtering named testv6 for all connections to the SSH server.

```
QTECH# configure terminal

QTECH(config)# ipv6 ssh access-class testv6
```

Platform Description

N/A

11.16. show crypto key mypubkey

Use this command to display the information about the public key part of the public key to the SSH server.

```
show crypto key mypubkey { rsa | dsa }
```

Parameter Description

Parameter	Description
rsa	Displays the RSA key.
dsa	Displays the DSA key.

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode

Usage Guide

This command is used to show the information about the public key part of the generated public key on the SSH server, including key generation time, key name, contents in the public key part, etc.

Configuration

The following example displays the information about the public key part of the public key to the SSH

```
QTECH(config)#show crypto key mypubkey rsa
% Key pair was generated at: 7:1:25 UTC Jan 16 2013 Key name: RSA1 private
Usage: SSH Purpose Key Key is not exportable. Key Data:
AAAAAwEA AQAAAEEA 2m6H/J+2 xOMLW5MR 8tOmpW1I XU1QItVN mLdR+G7O
Q10kz+4/
/IgYR0ge 1sZNg32u dFEifZ6D zfLySPqC MTWLfw==


% Key pair was generated at: 7:1:25 UTC Jan 16 2013 Key name: RSA private
```

```
Usage: SSH Purpose Key Key is not exportable. Key Data:
AAAAAwEA AQAAAEEA 0E5w2H0k v744uTIR yZBd/7AM 8pLItnW3 XH3LhEEi
BbZGZvn3
LEYYfQ9s pgYL0ZQf S0s/GY0X gJOMsc6z i8OAkQ==
```

Examples server.

Related Commands

Command	Description
crypto key generate { **rsa** | **dsa** }	Generates DSA and RSA keys.

Platform Description

N/A

11.17. show ip ssh

Use this command to display the information of the SSH server.
show ip ssh

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode
Privileged EXEC mode/Global configuration mode

Usage Guide

This command is used to display the information of the SSH server, including version, enablement state, port ID, encryption, message authentication algorithm, authentication timeout, and authentication retry times.
Note: If no key is generated for the SSH server, the SSH version is still unavailable even if this SSH version has been configured.

Configuration Examples

The following example displays the information of the SSH server.

```
QTECH(config)#show ip ssh SSH Disable - version 1.99
please generate rsa and dsa key to enable SSH SSH Port:  22
SSH Cipher Mode:  cbc,ctr,others
SSH  HMAC  Algorithm:  md5-96,md5,sha1-96,sha1  Authentication  timeout:  120  secs
Authentication retries: 3
SSH SCP Server:  disabled

// 显示SSH Server 功能和SCP 功能均已打开的配置信息QTECH(config)#show ip ssh
SSH Enable - version 1.99 SSH Port:  22
SSH Cipher Mode:  cbc,ctr,others
SSH  HMAC  Algorithm:  md5-96,md5,sha1-96,sha1  Authentication  timeout:  120  secs
Authentication retries: 3
SSH SCP Server:  enabled
```

Related Commands

Command	Description
ip ssh version {**1** | **2**}	Configures the version for the SSH server.
ip ssh time-out time	Sets the authentication timeout for the SSH server.
ip ssh authentication-retries	Sets the authentication retry times for the SSH server.

Platform Description

N/A

11.18. show ssh

Use this command to display the information about the established SSH connection.
show ssh

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode

Privileged EXEC mode/Global configuration mode

Usage Guide

This command is used to display the information about the established SSH connection, including VTY number of connection, SSH version, encryption algorithm, message authentication algorithm, connection status, and user name.

Configuration Examples

The following example displays the information about the established SSH connection:

```
QTECH#show ssh
Connection Version Encryption    Hmac     Compress    State
Username
1.5 blowfish zlib   Session started test
2.0 aes256-cbc      hmac-sha1     zlib   Session started test
```

Related Commands

Platform Description

Field Description

Field	Description
Connection	VTY number
Version	SSH version
Encryption	Encryption algorithm
Hmac	Message authentication algorithm
Compress	Compress algorithm
State	Connection state
Username	Username

Command	Description

N/A	N/A

N/A

12.1. clear ip urpf

Use this command to clear IPv4 URPF packet drop statistics.

clear ip urpf [**interface** *interface-name*]

Parameter Description

Parameter	Description
interface *interface-name*	Clears statistics on the specified interface.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

If no interface is specified, IPv4 URPF packet drop statistics on all interfaces are cleared by default.

Configuration Examples

Related Commands

Platform Description

The following example clears IPv4 URPF packet drop statistics on port GigabitEthernet 0/1.

```
QTECH# clear ip urpf interface gigabitEthernet0/1
```

The following example clears IPv4 URPF packet drop statistics on all interfaces.

```
QTECH# clear ip urpf
```

Command	Description
showip urpf	Displays the URPF configuration

	and statistics.

N/A

12.2. ip verify unicast source reachable-via (Interface Configuration Mode)

Use this command to enable the IPv4 URPF feature in the interface configuration mode. Use the **no** form of this command to restore the default setting.

```
ip verify unicast source reachable-via { rx | any } [ allow-default ]
```

no ip verify unicast

Parameter Description

Parameter	Description
rx	URPF check in the strict mode. In the strict mode, the egress port for the forwarding entry in the forwarding list found through the source address for the IP packet shall be matched with the ingress port.
any	URPF check in the loose mode. In the loose mode, the forwarding entry for the source address for the IP packet can be found in the forwarding list.
allow-default	(Optional) Allows using the default route to check URPF.

Defaults
This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

To determine whether the route for the source address is in the forwarding list or

not and the packet validity, enable the URPF feature to check the source address for the received IP packets. If no forwarding entry is matched, the packets are illegal.

Enabling URPF feature in the interface configuration mode enables URPF check for the received packets on the interface.

By default, the default route is not used for URPF check. Use the keyword allow-default to enable the

URPF check.

By default, the packets that failed to pass the URPF check are dropped. With ACL (acl-name) configured, the ACL matching continues when the routing fails. The packets will be dropped if the ACL is inexistent or the deny ACE is matched; otherwise, if the permit ACE is matched, the packets will be forwarded.

After this command is used, URPF check on IPv4 packets will be enabled.

This function is supported only on routed and Layer 3 interfaces, and have the following restrictions:

- Not support the ACL association;

Not support to use the IPv6 route with prefix in 65 to 127 bits for the URPF check;

- After enabling the URPF feature, the range of packets received on the interface will be expanded, that is, the URPF feature is enabled for all packets received on the physical ports.
- After enabling the URPF feature, it halves the route forwarding capacity.
- After enabling the URPF feature in the strict mode, the user can match the equivalent route when URPF check is enabled for the packets received on the interface.

URPF feature cannot be configured in the global configuration mode and in the interface configuration mode at the same time.

URPF feature cannot be configured on range interface.

Configuration Examples

The following example checks the URPF feature of the received packets in the strict mode on the interface GigabitEthernet 0/1.

```
QTECH(config)# interface gigabitEthernet0/1
QTECH(config-if-GigabitEthernet 0/1)# ip verify unicast source reachable-via rx
```

Related Commands

Command	Description
show ip urpf	Displays the URPF information.

Platform Description

N/A

12.3. ip verify urpf drop-rate compute interval

Use this command to set the URPF drop-rate compute interval. Use the **no** form of this command to restore the default setting. **ip verify urpf drop-rate compute interval** *seconds*

no ip verify urpf drop-rate compute interval

Parameter Description

Parameter	Description
seconds	Sets the URPF drop-rate compute interval, in the range from 30 to
	300 in the unit of seconds.

Defaults

The default is 30 seconds.

Command Mode

Global configuration mode

Usage Guide

The URPF drop-rate is computed globally for both IPv4 and IPv6 packets on interfaces enabled with URPF.

Configuration Examples

Related Commands

Platform Description

The following example sets the URPF drop-rate compute interval as 60 seconds.

```
QTECH(config)# ip verify urpf drop-rate compute interval60
```

Command	Description
ip verify urpf drop-rate notify	Sets the URPF drop-rate information monitoring.
ip verify urpf drop-rate notify hold-down	Sets the URPF drop-rate warning interval.
ip verify urpf notification threshold	Sets the URPF drop-rate threshold.

N/A

12.4. ip verify urpf drop-rate notify

Use this command to enable the URPF drop-rate monitoring.

Use the **no** or **default** form of this command to restore the default setting.

ip verify urpf drop-rate notify

no ip verify urpf drop-rate notify

default ip verify urpf drop-rate notify

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

This command is used to enable the URPF drop-rate monitoring, notifying the user of the URPF packet drop information by means of Syslog or Trap for the convenience of the user network monitoring.

URPF feature cannot be configured on range interface.

Configuration Examples

The following example enables the URPF drop-rate monitoring on port GigabitEthernet 0/1.

```
QTECH(config)# interface gigabitEthernet0/1
QTECH(config-if-GigabitEthernet 0/1)# ip verify urpf drop-rate notify
```

Related Commands

Command	Description
ip verify urpf drop-rate compute interval	Sets the URPF drop-rate compute interval.
ip verify urpf drop-rate notify hold-down	Sets the URPF drop-rate warning interval.
ip verify urpf notification threshold	Sets the URPF drop-rate threshold.

Platform Description

N/A

12.5. ip verify urpf drop-rate notify hold-down

Use this command to set the URPF drop-rate notification interval. Use the **no** form of this command to restore to the default setting. **ip verify urpf drop-**

rate notify hold-down *seconds*

no ip verify urpf drop-rate notify hold-down

Parameter Description

Parameter	Description
seconds	Sets the URPF drop-rate notification interval, in the range from 30 to 300 in the unit of seconds.

Defaults

The default is 300 seconds.

Command Mode

Global configuration mode

Usage Guide N/A

Configuration Examples

Related Commands

The following example sets the URPF drop-rate notification interval as 60 seconds.

```
QTECH(config)# ip verify urpf drop-rate notify hold-down60
```

Command	Description
ip verify urpf drop-rate compute interval	Sets the URPF drop-rate computing interval.
ip verify urpf drop-rate notify	Sets the URPF drop-rate monitoring.
ip verify urpf notification threshold	Sets the URPF drop-rate threshold.

Platform

N/A

Description

12.6. ip verify urpf notification threshold

Use this command to set the URPF drop-rate threshold.

Use the **no** form of this command to restore the default setting.

ip verify urpf notification threshold *rate-value*

no ip verify urpf notification threshold

Parameter Description

Parameter	Description
threshold *rate-value*	Sets the URPF drop-rate threshold, in the range from 0 to 4,294,967,295 in the unit of packets per second (pps).

Defaults

The default is 1,000 pps.

Command Mode

Interface configuration mode

Usage Guide

The threshold 0 indicates that once the device detects a dropped packet due to the IPv4 URPF check, the notification is sent.

The user can adjust the drop-rate threshold value according to the actual network performance. URPF feature cannot be configured on range interface.

Configuration Examples

The following example sets the URPF drop-rate threshold 10pps on the interface GigabitEthernet 0/1.

```
QTECH(config)# interface gigabitEthernet0/1
QTECH(config-if-GigabitEthernet 0/1)# ipv6 verify urpf drop-rate notify QTECH(config-if-GigabitEthernet 0/1)# ipv6 verify urpf notification threshold 10
```

Related Commands

Command	Description
ip verify urpf drop-rate compute interval	Sets the URPF drop-rate computing interval.
ip verify urpf drop-rate notify	Sets the URPF drop-rate information monitoring.
ip verify urpf drop-rate notify hold-down	Sets the URPF drop-rate notification interval.

Platform Description

N/A

12.7. show ip urpf

Use this command to display the IPv4 URPF configuration and statistics.

show ip urpf [**interface** *interface-name*]

Parameter Description

Parameter	Description
interface *interface-name*	Displays the configuration and statistics on the specified interface.

Defaults

N/A

Command Mode

Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide

The global configuration and statistics of all interfaces are displayed by default.

Configuration Examples

The following example displays IPv4 URPF configuration and statistics on port GigabitEthernet 0/1.

```
QTECH# show ip urpf interface
gigabitEthernet0/21 IP verify source reachable-via
RX
IP verify URPF drop-rate notify disabled
IP verify URPF notification threshold is 1000pps
Number of drop packets in this interface is 124
Number of drop-rate notification counts in this interface is 0
```

Field	Description
IP verify source reachable-via xx	xx in strict mode is displayed as RX and in loose mode as ANY.
IP verify URPF drop-rate notify xx	If drop rate notification is enabled, xx is displayed as enabled. Otherwise, it is displayed as disabled.
IP verify URPF notification threshold is xxpps	The threshold of URPF drop rate, in the range from 0 to 4294967295 in the unit of packets per second (pps). The default is 1000.
Number of drop packets in this interface is x	The number of drop packets
Number of drop-rate notification counts in this interface is x	The URPF drop-rate notification counts

The following example displays IPv4 URPF configuration and statistics.

```
QTECH# show ip urpf
IP verify URPF drop-rate compute interval is 30s IP verify URPF drop-rate notify hold-down is 300s
```

```
Interface GigabitEthernet 0/1
IP verify source reachable-via RX
IP verify URPF drop-rate notify disabled
IP verify URPF notification threshold is 1000pps
```

Number of drop packets in this interface is 124 **Number of drop-rate notification counts in this interface is 2**	
Field	**Description**
IP verify URPF drop-rate compute interval is x	Drop-rate computing interval
IP verify URPF drop-rate notify hold-down is x	Drop-rate notification interval
Interface interface-name	interface-name is the name of the interface on which URPF is applied. Configuration and statistics on this interface are displayed.

Related Commands

Command	Description
ip verify unicast source reachable-via	Enables the URPF features.
ip verify urpf drop-rate compute interval	Sets the URPF drop-rate compute interval.
ip verify urpf drop-rate notify hold-down	Sets the URPF drop-rate warning interval.
ip verify urpf notification threshold	Sets the URPF drop-rate threshold.
clear ip urpf	Clears the URPF statistical information.

Platform Description

N/A

13.1. clear cpu-protect-counters

Use this command to clear the CPP statistics.

clear cpu-protect counters [**device** *device_num*]

Parameter Description

Parameter	Description
device_num	As a single physical device, there is no device parameter; As a VSU, the device parameter indicates the chassis or the box-type device. If no device parameter is specified, that indicates this command takes effect to the master chassis or the master box-type device.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example clears the CPP statistics.

```
QTECH(config)#show cpu-protect type bpdu
Packet Type   Traffic-class   Bandwidth(pps)   Rate(pps)   Drop(pps)   Total
      Total Drop
```

```
bpdu   6      200    0       0      600    50
QTECH#clear  cpu-protect  counters  QTECH(config)#show  cpu-protect  type
bpdu
Packet Type  Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)  Total
       Total Drop

         ----------------
bpdu                      200           0          0         0        0
         6
```

Command	Description
N/A	N/A

N/A

13.2. clear cpu-protect-counters mboard

Use this command to clear the CPP statistics on the supervisor module.
clear cpu-protect counters mboard

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide
N/A

Configuration Examples

Related Commands

Platform Description

The following example clears the CPP statistics on the supervisor module.

```
QTECH(config)#show cpu-protect type bpdu
Packet Type   Traffic-class   Bandwidth(pps)   Rate(pps)   Drop(pps)   Total
       Total Drop



bpdu   6      200    0      0      600    50
QTECH#clear  cpu-protect  counters  mboard  QTECH(config)#show  cpu-protect
type bpdu
Packet Type   Traffic-class   Bandwidth(pps)   Rate(pps)   Drop(pps)   Total
       Total Drop




         --------------
bpdu                     200            0          0         0         0
         6
```

Command	Description
N/A	N/A

N/A

13.3. cpu-protect cpu bandwidth

Use this command to configure the bandwidth for the CPU port. Use the **no** form of this command to restore the default setting.

cpu-protect cpu bandwidth *bandwidth_value*

no cpu-protect cpu bandwidth

Parameter Description

Parameter	Description

bandwidth_value	An integer number ranges from 0 to 100000 (PPS). Indicates the bandwidth value of the CPU port.

Defaults

The default CPU port bandwidth varies with products.

Command Mode

Global configuration mode

Usage Guide N/A

Configuration Examples

The following example sets the CPU port bandwidth to 32000pps.

```
QTECH# configure terminal
QTECH(config)# cpu-protect cpu bandwidth 32000 QTECH#show cpu-protect cpu
%cpu port bandwidth: 32000(pps)
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

13.4. cpu-protect traffic-class bandwidth

Use this command to configure the bandwidth for each priority queue. Use the **no** form of this command to restore the default setting.

cpu-protect traffic-class *traffic-class-num* **bandwidth** *bandwidth_value*

no cpu-protect traffic-class *traffic-class-num* **bandwidth**

Parameter Description

Parameter	Description
traffic-class-num	A default integer that varies with products, indicating the queue priority
bandwidth_value	An integer number ranges from 0 to 100000 (pps). Indicates the bandwidth value of the CPU port.

Defaults

The default bandwidth of each priority queue varies with products.

Command

Global configuration mode

Mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example s sets the priority queue 5 to 3500 pps.

```
QTECH#         configure         terminal
QTECH(config)#    cpu-protect    traffic-
class  QTECH#show  cpu-protect  traffic-
class           5           Traffic-class
       Bandwidth(pps)  Rate(pps)
                                                 5 bandwidth 3500
                                                   Drop(pps)


5             3500      0           0
```

Command	Description
N/A	N/A

N/A

13.5. cpu-protect type bandwidth

Use this command to configure the bandwidth of a specific packet. Use the **no** form of this command to restore the default setting. **cpu-protect type** *packet-type* **bandwidth** *bandwidth_value*

no cpu-protect type *packet-type* **bandwidth**

Parameter Description

Parameter	Description
packet-type	Packet type, which varies with products
bandwidth_value	An integer number ranges from 0 to 32000 (pps). Indicates the bandwidth value of the CPU port.

Defaults

The default CPU port bandwidth varies with products.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the BPDU bandwidth to 200 pps.

```
QTECH# configure terminal
QTECH(config)# cpu-protect type bpdu bandwitdth 200 QTECH(config)#show cpu-protect type bpdu
Packet Type  Traffic-class Bandwidth(pps) Rate(pps) Drop(pps)

Total  Total Drop
```

```
                    ------------------------
bpdu                200          0          0          0          0
        6
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

13.6. cpu-protect type traffic-class

Use this command to set the priority queue (PQ) of the packet. Use the **no** form of this command to restore the default setting. **cpu-protect type** *packet-type* **traffic-class** *traffic-class-num* **no cpu-protect type** *packet-type* **traffic-class**

Parameter Description

Parameter	Description
packet-type	Packet type, which varies with products
traffic-class-num	An integer number varying with products. Indicates the bandwidth value of the CPU port.

Defaults

The default PQ varies with products.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

Related Commands

The following example sets the PQ of BPDU packets to 5.

```
QTECH# configure terminal
QTECH(config)# cpu-protect type bpdu traffic-class 5
QTECH(config)#show cpu-protect type bpdu
Packet Type          Traffic-class Bandwidth(pps) Rate(pps) Drop(pps)
Total       Total Drop
-------------------------------------------------
----------------  ---------------
bpdu                 5             20
0                    0             0             0
```

Command	Description
N/A	N/A

Platform Description

N/A

13.7. show cpu-protect

Use this command to display all CPP configuration and statistics.

show cpu-protect [**device** *device_num*]

Parameter Description

Parameter	Description

device_num	As a single physical device, there is no device parameter; As a VSU, the device parameter indicates the chassis or the box-type device. If no device parameter is specified, that indicates this command takes effect to the master chassis or the master box-type device.

Defaults
N/A

Command Mode

All configuraiton mode

Usage Guide
N/A

Configuration Examples

Related Commands

Platform Description

N/A

Command	Description
N/A	N/A

N/A

13.8. show cpu-protect cpu

Use this command to display the configurations of the CPU port.

show cpu-protect cpu

Parameter Description

Parameter	Description

N/A	N/A

Defaults

N/A

Command Mode

All configuration modes

Usage Guide

N/A

Configuration Examples

The following example displays the configuration of the CPU port.

```
QTECH#show cpu-protect cpu
%cpu port bandwidth: 32000(pps)
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

13.9. show cpu-protect mboard

Use this command to display the statistics of various packets of CPU protection on the management board.

show cpu-protect mboard

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

All configuration modes

Usage Guide

This command displays the statistics of the packets received by CPU on the management board.

Configuration Examples

The following example displays the CPP configuration and statistics of the master device.

```
QTECH#show cpu-protect mboard
%cpu port bandwidth: 80000(pps)
Traffic-classBandwidth(pps)  Rate(pps)
                                          Drop(pps)


0             8000      0                 0

1             8000      0                 0

2             8000      0                 0

3             8000      0                 0

4
       800
0      0
       0

5
       800
0      0
       0

6
       800
0      0
       0

7
       800
0      0
       0

Packet        Rate(p    Drop(pps)
Type          ps)
       Tra
ffic-class
Bandwidth(
pps)

Total
       Tot
al Drop
```

```
bpdu   6      128    0                    0          0          0
arp    3      10000  0                    0          0          0
arp-dai       3      10000  0             0          0          0
arp-proxy     3      10000  0             0          0          0
tpp    7      128    0                    0          0          0
dot1x  4      128    0                    0          0          0
gvrp   5      128    0                    0          0          0
rldp   6      128    0                    0          0          0
lacp   6      128    0                    0          0          0
rerp   6      128    0                    0          0          0
reup   6      128    0                    0          0          0
lldp   5      128    0                    0          0          0
cdp    5      128    0                    0          0          0
dhcps  4      128    0                    0          0          0
dhcps6 4      128    0                    0          0          0
dhcp6-client  4      128    0             0          0          0
dhcp6-server  4      128    0             0          0          0
dhcp-relay-c  4      128    0             0          0          0
dhcp-relay-s  4      128    0             0          0          0
option82      4      128    0             0          0          0
tunnel-bpdu   5      128    0             0          0          0
tunnel-gvrp   5      128    0             0          0          0
unknown-v6mc  3      128    0             0          0          0
known-v6mc    3      128    0             0          0          0
xgv6-ipmc     3      128    0             0          0          0
stargv6-ipmc  3      128    0             0          0          0
unknown-v4mc  3      128    0             0          0          0
known-v4mc    3      128    0             0          0          0
xgv-ipmc      3      128    0             0          0          0
sgv-ipmc      3      128    0             0          0          0
udp-helper    4      128    0             0          0          0
dvmrp  5      128    0                    0          0          0
igmp   4      128    0                    0          0          0
icmp   4      128    0                    0          0          0
ospf   5      128    0                    0          0          0
ospf3  5      128    0                    0          0          0
```

```
pim                          6     128                0         0         0         0
pimv6                        6     128                0         0         0         0
rip                          6     128                0         0         0         0
ripng                        6     128                0         0         0         0
vrrp                         6     128                0         0         0         0
vrrp6                        6     128                0         0         0         0
ttl0                         6     128                0         0         0         0
ttl1                         6     128                0         0         0         0
err_hop_limit                1     800                0         0         0         0
local-ipv4                   6     128                0         0         0         0
local-ipv6                   6     128                0         0         0         0
route-host-v4                0     4096               0         0         0         0
route-host-v6                0     4096               0         0         0         0
mld                          0     1000               0         0         0         0
nd-snp-ns-na                 6     128                0         0         0         0
nd-snp-rs                    6     128                0         0         0         0
nd-snp-ra-redirect 0              6     128          0         0         0
nd-non-snp
                                 6                                                   0
                                       128          0         0         0
            erps             4     128                0         0         0         0
            mpls-ttl0        6     128                0         0         0         0
            mpls-ttl1        6     128                0         0         0         0
            mpls-ctrl        6     128                0         0         0         0
            isis             5     2000               0         0         0         0
            bgp              1     128                0         0         0         0
            cfm              0     128                0         0         0         0
            fcoe-fip         6     128                0         0         0         0
            fcoe-local       6     128                0         0         0         0
            bfd-echo         6     5120               0         0         0         0
            bfd-ctrl         6     5120               0         0         0         0
            madp             7     1000               0         0         0         0
            ip4-other        6     128                0         0         0         0
            ip6-other        6     128                0         0         0         0
            non-ip-other     6     20000              0         0         0         0
            trill            2     1000               0         0         0         0
```

```
            trill-oam       2     1000                0        0        0        0
            efm             2     1000                0        0        0        0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

13.10. show cpu-protect summary

Use this command to display the CPP configuration and statistics of the master device.

show cpu-protect summary

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

All configuration modes

Usage Guide

N/A

Configuration Examples

```
QTECH#show cpu-protect summary
%cpu port bandwidth: 100000(pps)
Traffic-classBandwidth(pps) Rate(pps)  Drop(pps)


0           60    0       0
```

```
            00

1           60    0      0
            00

2           60    0      0
            00

3           60    0      0
            00

4           60    0      0
            00

5           60    0      0
            00

6           60    0      0
            00

7           60    0      0
            00

Packet              Traffic-class              Rate(p    Drop(p    Total
Type                Bandwidth(pps)             ps)       ps)
Total
Drop

bpdu        6    128    0                      0         0         0

arp         1    3000   0                      0         0         0

tpp         6    128    0                      0         0         0

dot1x       2    1500   0                      0         0         0

gvrp        5    128    0                      0         0         0

rldp        5    128    0                      0         0         0

lacp        5    256    0                      0         0         0

rerp        5    128    0                      0         0         0

reup        5    128    0                      0         0         0

lldp        5    768    0                      0         0         0

cdp         5    768    0                      0         0         0

dhcps       2    1500   0                      0         0         0
```

```
dhcps6        2          1500          0     0        0        0

dhcp6-        2          1500          0     0        0        0
client

dhcp6-        2          1500          0     0        0        0
server

dhcp-         2          1500          0     0        0        0
relay-c

dhcp-         2          1500          0     0        0        0
relay-s
```

option82	2	1500	0	0	0	0
tunnel-bpdu	2	128	0	0	0	0
tunnel-gvrp	2	128	0	0	0	0
unknown-v6mc	1	128	0	0	0	0
xgv6-ipmc	1	128	0	0	0	0
stargv6-ipmc	1	128	0	0	0	0
unknown-v4mc	1	128	0	0	0	0
xgv-ipmc	2	128	0	0	0	0
stargv-ipmc	2	128	0	0	0	0
udp-helper	1	128	0	0	0	0
dvmrp	4	128	0	0	0	0
igmp	2	1000	0	0	0	0
icmp	3	1600	0	0	0	0
ospf	4	2000	0	0	0	0
ospf3	4	2000	0	0	0	0
pim	4	1000	0	0	0	0
pimv6	4	1000	0	0	0	0
rip	4	128	0	0	0	0
ripng	4	128	0	0	0	0
vrrp	6	256	0	0	0	0
vrrpv6	6	256	0	0	0	0
ttl0	0	128	0	0	0	0
ttl1	0	2000	0	0	0	0
hop-limit	0	800	0	0	0	0
local-ipv4	3	4000	0	0	0	0
local-ipv6	3	4000	0	0	0	0
v4uc-route	1	800	0	0	0	0
v6uc-route	1	800	0	0	0	0
rt-host	4	3000	0	0	0	0
mld	2	1000	0	0	0	0
nd-snp-ns-na	1	3000	0	0	0	0
nd-snp-rs	1	1000	0	0	0	0
nd-snp-ra-redirect	1	1000		0	0	0	0

```
erps   5              128          0          0          0          0
mpls-ttl0    4        128          0          0          0          0
mpls-ttl1    4        128          0          0          0          0
mpls-ctrl    4        128          0          0          0          0
isis   4              2000         0          0          0          0
bgp    4              2000         0          0          0          0
```

```
cfm                    5        512          0     0          0          0
web-auth               2        2000         0          0     0          0
fcoe-fip               4        1000         0          0     0          0
fcoe-local             4        1000         0          0     0          0
bfd                    6        5120         0     0          0          0
micro-bfd              6        5120         0          0     0          0
micro-bfd-v6           6        5120         0          0     0          0
            dldp       6        3200         0     0          0          0
            other      0        4096         0     0          0          0
            trill      4        1000         0     0          0          0
            efm        5        1000         0     0          0          0
            ipv6-all   0        2000         0     0          0          0
            ip-option  0        800          0     0          0          0
            mgmt       -        4000         4     0          4639       0
            dns        2        200          0     0          0          0
            sdn        0        5000         0     0          0          0
            sdn_of_fetc 0       5000         0     0          0          0
            h
            sdn_of_copy 0       5000         0     0          0          0
            sdn_of_trap 0       5000         0     0          0          0
            vxlan-non- 1        512          0     0          0          0
            uc
            local-     3        1000         0     0          0          0
            telnet
            local-snmp 3        1000         0     0          0          0
            local-ssh  3        1000         0     0          0          0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

13.11. show cpu-protect traffic-class

Use this command to display the summarized configuration and statistics of priority queues.

show cpu-protect traffic-class {*traffic-class-num* **| all} [device** *device_num***]**

Parameter Description

Parameter	Description
traffic-class-num	A default integer that varies with products, indicating the queue priority.
all	Displays configurations and statistics of all priority queues.
device_num	As a single physical device, there is no device parameter; As a VSU, the device parameter indicates the chassis or the box-type device. If no device parameter is specified, that indicates this command takes
	effect to the master chassis or the master box-type device.

Defaults

N/A

Command Mode

All configuration modes

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example displays the summarized configuration and statistics of priority queues.

```
QTECH#show cpu-protect traffic-class all
Traffic-classBandwidth(pps)  Rate(pps)  Drop(pps)


0             8000            0            0
1             8000            0            0
2             8000            0            0
3             8000            0            0
4             8000            0            0
5             3200            0            0
6             8000            0            0
7             8000            0            0
```

Command	Description
N/A	N/A

N/A

13.12. show cpu-protect type

Use this command to display the statistics of the specified type of packets

show cpu-protect type *packet-type* [**device** *device_num*]

Parameter Description

Parameter	Description
packt-type	Packet type, which varies with products
all	Displays the configurations and statistics of all packet types.

device_num	As a single physical device, there is no device parameter; As a VSU, the device parameter indicates the chassis or the box-type device. If no device parameter is specified, that indicates this command takes effect to the master chassis or the master box-type device.

Defaults

N/A

Command Mode

All configuration modes

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example displays the statistics of the ICMP packets.

```
QTECH(config)#show cpu-protect type icmp
Packet Type   Traffic-class   Bandwidth(pps)   Rate(pps)   Drop(pps)   Total
       Total Drop


icmp     --------------
100                     1500            50          0         10000
         5
```

Command	Description
N/A	N/A

N/A

14.1. clear ip dhcp snooping binding

Use this command to delete the dynamic user information from the DHCP Snooping binding database.

clear ip dhcp snooping binding [*ip*] [*mac*] [**vlan** *vlan-id*] [**interface** *interface-id*]

Parameter Description

Parameter	Description
mac	Specifies the user MAC address to be cleared.
vlan-id	Specifies the ID of the VLAN to be cleared.
ip	Specifies the IP address to be cleared.
interface-id	Specifies the ID of the interface to be cleared.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to clear the current dynamic user information from the DHCP Snooping binding database.

After this command is used, all the DHCP clients connecting interfaces with IP Source Guard function enabled should request IP addresses again, or they cannot access network.

Configuration Examples

The following example clears the dynamic database information from the DHCP Snooping binding database.

```
QTECH# clear ip dhcp snooping binding QTECH# show ip dhcp snooping binding Total number of
```

```
bindings: 0
MacAddress IpAddress Lease(sec) Type VLAN Interface
```

Related Commands

Command	Description
show ip dhcp snooping binding	Displays the information of the DHCP Snooping binding database.

Platform Description

N/A

14.2. ip dhcp snooping

Use this command to enable the DHCP Snooping function globally. Use the **no** form of this command to restore the default setting.

ip dhcp snooping no

ip dhcp snooping

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

The **show ip dhcp snooping** command is used to display whether the DHCP Snooping function is enabled.

Configuration Examples

The following example enables the DHCP Snooping function.

```
QTECH# configure terminal
QTECH(config)# ip dhcp snooping QTECH(config)# end
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the configuration information of DHCP Snooping.
ip dhcp snooping vlan	Configures DHCP Snooping enabled VLAN.

Platform Description

N/A

14.3. ip dhcp snooping bootp-bind

Use this command to enable DHCP Snooping BOOTP-bind function. Use the **no** form of this command to restore the default setting.

ip dhcp snooping bootp-bind

no ip dhcp snooping bootp-bind

Platform Description

in

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

By default, the DHCP Snooping only forwards BOOTP packets. With this function enabled, it can Snoop BOOTP packets. After the BOOTP client requests an address successfully, the DHCP Snooping adds the BOOTP user to the static binding database.

Configuration Examples

The following example enables the DHCP Snooping BOOTP-bind function.

```
QTECH# configure terminal
QTECH(config)# ip dhcp snooping bootp-bind QTECH(config)# end
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP Snooping configuration.

Platform Description

N/A

14.4. ip dhcp snooping check-giaddr

Use this command to enable DHCP Snooping to support the function of processing Relay requests. Use the **no** form of this command to restore the default setting.

ip dhcp snooping check-giaddr

no ip dhcp snooping check-giaddr

Parameter Description

Parameter	Description
N/A	N/A

Defaults
This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

After the feature is enabled, services using DHCP Snooping binding entries generated based on Relay requests, such as IP Source Guard/802.1x authentication, cannot be deployed. Otherwise, users fail to access the Internet.
After the feature is enabled, the **ip dhcp snooping verify mac-address** command cannot be used. Otherwise, DHCP Relay requests will be discarded and as a result, users fail to obtain addresses.

Configuration Examples

The following example enables DHCP Snooping to support the function of processing Relay requests.

```
QTECH# configure terminal
QTECH(config)# ip dhcp snooping check-giaddr QTECH(config)# end
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the configuration information of the DHCP Snooping.

Platform Description

N/A

14.5. ip dhcp snooping database

Use this command to configure file backup of the DHCP Snooping binding database. Use the **no** form of this command to restore the

default setting.

ip dhcp snooping database sata0 [interval *time*]

no ip dhcp snooping database sata0

Parameter Description

Parameter	Description
time	Indicates the interval of storing the database in the unit of second. The range is from 10s to 86,400s. The default value is 300s.

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

After this feature is enabled, the DHCP Snooping database can be written to the backup file of a specified type. In this way, users are able to resume communication immediately after restart of the device.

Configuration Examples

The following example sets configures file backup of the DHCP Snooping binding database with the default interval.

```
QTECH# configure terminal
QTECH(config)# ip dhcp snooping database sata0 QTECH(config)# end
```

Related Commands

Command	Description
show ip dhcp snooping	**Displays the configuration information of the DHCP Snooping.**

show run	**Displays the current backup mode.**

Platform Description

N/A

14.6. ip dhcp snooping database write-delay

Use this command to configure the switch to write the dynamic user information of the DHCP Snooping binding database into the flash periodically.
Use the **no** form of this command to restore the default setting.
ip dhcp snooping database write-delay *time*
no ip dhcp snooping database write-delay

Parameter Description

Parameter	Description
time	The interval at which the system writes the dynamic user information of the DHCP Snooping database into the flash, in the range from 600 to 86,400 in the unit of seconds

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

Too fast writing will reduce flash durability

This function writes user information into flash in case of loss after restart. In that case, users need to obtain IP addresses again for normal communication.

Configuration Examples

The following example sets the interval at which the switch writes the user information into the flash to 3,600 seconds.

```
QTECH# configure terminal
QTECH(config)# ip dhcp snooping database write-delay 3600 QTECH(config)# end
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the configuration information of the DHCP Snooping.

Platform Description

N/A

14.7. ip dhcp snooping database write-to-flash

Use this command to write the dynamic user information of the DHCP binding database into flash in real time.

ip dhcp snooping database write-to-flash

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

This command is used to write the dynamic user information of the DHCP binding database into flash in real time.

Configuration Examples

The following example writes the dynamic user information of the DHCP binding database into flash.

```
QTECH# configure terminal
QTECH(config)# ip dhcp snooping database write-to-flash QTECH(config)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

14.8. ip dhcp snooping information option

Use this command to add option82 to the DHCP request message. Use the **no** form of this command to restore the default setting.

ip dhcp snooping information option [**standard-format**]

no ip dhcp snooping information option [**standard-format**]

Parameter Description

Parameter	Description
standard-format	The option82 uses the standard format.

Defaults

This function is disabled by default,

Command Mode

Global configuration mode

Usage Guide

This command adds option82 to the DHCP request messages based on which

the DHCP server assigns IP addresses.

By default, this function is in extended mode.

DHCP Relay function adds option82 by default. Therefore, it is unnecessary to enable functions of DHCP Snooping option82 and DHCP Relay at the same time.

Configuration Examples

The following example adds option82 to the DHCP request message.

```
QTECH# configure terminal
QTECH(config)# ip dhcp snooping information option QTECH(config)# end
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP Snooping configuration.

Platform Description

N/A

14.9. ip dhcp snooping information option format remote-id

Use this command to set the option82 sub-option remote-id as the customized character string. Use the **no** form of this command to restore the default setting.

ip dhcp snooping information option format remote-id { **string** *ascii-string* **| hostname** }

no ip dhcp snooping information option format remote-id { **string** *ascii-string* **| hostname** }

Parameter Description

Parameter	Description
string *ascii-string*	The content of the option82 remote-id extension format is customized

	character string.
hostname	The content of the option82 remote-id extension format hostname

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

This command sets the remote-id in the option82 to be added to the DHCP request message as the

customized character string. The DHCP server will assign the IP address

according to the option82 information.

Configuration Examples

The following example adds the option82 into the DHCP request packets

with the content of remote-id as hostname.

```
QTECH# configure terminal
QTECH(config)# ip dhcp snooping information option format remote-id hostname
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

14.10. ip dhcp snooping monitor

Use this command to enable DHCP Snooping monitoring.

Use the **no** form of this command to restore the default setting.

```
ip dhcp snooping  monitor no ip dhcp snooping monitor
```

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

After the feature is enabled, DHCP Snooping generates binding entries according to the interaction process by copying DHCP packets. It, however, does not check the validity of packets.

Configuration Examples

The following example enables DHCP Snooping monitoring.

```
QTECH# configure terminal
QTECH(config)# ip dhcp snooping monitor QTECH(config)# end
```

Related Commands

Command	Description
N/A	N/A

Platform

N/A

Description

14.11. ip dhcp snooping suppression

Use this command to set the port to be the

suppression status. Use the **no** form of this command to restore the default setting. **ip dhcp snooping suppression**

no ip dhcp snooping suppression

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode/WLAN security configuration mode

Usage Guide

This command denies all DHCP request messages under the port, that is, all the users under the port are prohibited to request IP addresses through DHCP.

This command is only supported on Layer 2 switch interfaces and aggregate ports (APs).

Configuration Examples

The following example sets **fastethernet** 0/2 and WLAN 1 to be in the suppression status.

```
QTECH# configure  terminal QTECH(config)# interface fastEthernet 0/2
QTECH(config-if)# ip dhcp snooping suppression QTECH(config-if)# end
QTECH# configure terminal
QTECH(config)# wlansec 1
QTECH(config-wlansec)# ip dhcp snooping suppression
QTECH(config-if-wlansec)# end
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP Snooping configuration.

Platform Description

N/A

14.12. ip dhcp snooping trust

Use this command to set the trusted ports for DHCP Snooping. Use the **no** form of this command to restore the default setting.

Parameter Description

ip dhcp snooping trust

no ip dhcp snooping trust

Parameter	Description
N/A	N/A

Defaults

All ports are untrusted by default.

Command Mode

Interface configuration mode

Usage Guide

Use this command to set a port as a trusted port. The DHCP response messages received under the trust port are forwarded normally, but the response messages received under the untrusted port will be discarded. This command is only supported on Layer 2 switch interfaces and aggregate ports (APs).

Configuration Examples

The following example sets fastEthernet 0/1 as a trusted port:

```
QTECH# configure  terminal QTECH(config)# interface fastEthernet 0/1 QTECH(config-if)# ip dhcp snooping trust
QTECH(config-if)# end
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP Snooping configuration.

Platform Description

N/A

14.13. ip dhcp snooping verify mac-address

Use this command to check whether the source MAC address of the DHCP request message matches against the **client addr** field of the DHCP message.
Use the **no** form of this command to restore the default setting.

```
ip dhcp snooping verify mac-address  no ip dhcp snooping verify mac-address
```

Parameter Description

Parameter	Description
N/A	N/A

Defaults
This function is disabled by default.

Command Mode
Global configuration mode

Usage Guide

Use this command to check the source MAC address of the DHCP request message. If the MAC address in the link-layer header is different from the CHADDR (Client MAC Address), the check fails ,and the packets will be discarded.

Configuration Examples

The following example enables the check of the source MAC address of the DHCP request message.

```
QTECH# configure terminal
QTECH(config)# ip dhcp snooping verify mac-address QTECH(config)# end
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP Snooping configuration.

Platform Description

N/A

14.14. ip dhcp snooping vlan

Use this command to enable DHCP Snooping for the specific VLAN. Use the **no** form of this command to restore the default setting.

ip dhcp snooping vlan {*vlan-rng* | { *vlan-min* [*vlan-max*] } }

no ip dhcp snooping vlan {*vlan-rng* | { *vlan-min* [*vlan-max*] } }

Parameter Description

Parameter	Description
vlan-rng	VLAN range of effective DHCP Snooping
vlan-min	Minimum VLAN of effective DHCP Snooping
vlan-max	Maximum VLAN of effective DHCP Snooping

Defaults

By default, once the DHCP Snooping is enabled globally, it takes effect for all VLANs.

Command Mode

Global configuration mode

Usage Guide

Use this command to enable DHCP Snooping for specified VLANs globally.

Configuration Examples

The following example enables the DHCP Snooping function in VLAN 1000.

```
QTECH# configure  terminal QTECH(config)# ip dhcp snooping vlan 1000
QTECH(config)# end
```

```
QTECH# configure terminal
QTECH(config)# ip dhcp snooping vlan 1-10 QTECH(config)# end
```

The following example enables the DHCP Snooping function from VLAN1 to VLAN10.

Related Commands

Command	Description
ip dhcp snooping	Enables DHCP Snooping globally.

Platform Description

N/A

14.15. renew ip dhcp snooping database

Use this command to import the information in current flash to the DHCP Snooping binding database manually as needed.

renew ip dhcp snooping database

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to import the flash file information to the DHCP

Snooping database in real time.

Records out of lease time and repeated will be neglected.

Configuration Examples

Related Commands

Platform Description

The following example imports the flash file information to the DHCP Snooping database.

```
QTECH# renew ip dhcp snooping database
```

Command	Description
N/A	N/A

N/A

14.16. show ip dhcp snooping

Use this command to display the DHCP Snooping configuration.

show ip dhcp snooping

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

```
The following example displays the DHCP Snooping configuration.
QTECH# show ip dhcp snooping
Switch DHCP snooping status :ENABLE
Verification of hwaddr field status :DISABLE
DHCP snooping database write-delay time: 0 seconds
DHCP snooping option 82 status: ENABLE
DHCP snooping Support Bootp bind status: ENABLE
Interface                                    Trusted           Rate
limit(pps)
-----------------------------------------
------------------------------
GigabitEthernet 0/4                            YES              unlimited
Default                                      No
```

Related Commands

Command	Description
ip dhcp snooping	Enables the DHCP Snooping globally.
ip dhcp snooping verify mac-address	Enables the check of source MAC address of DHCP Snooping packets.
ip dhcp snooping write-delay	Sets the interval of writing user information to FLASH periodically.
ip dhcp snooping information option	Adds option82 to the DHCP request message.
ip dhcp snooping bootp-bind	Enables the DHCP Snooping bootp bind function.
ip dhcp snooping trust	Sets the port as a trust port.

Platform Description

N/A

14.17. show ip dhcp snooping binding

Use this command to display the information of the DHCP Snooping binding database.
show ip dhcp snooping binding

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode
Privileged EXEC mode

Usage Guide
This command is used to display all the information of the DHCP Snooping binding database.

Configuration Examples
1: The following example displays the information of the DHCP Snooping binding database.

```
QTECH# show ip dhcp snooping
binding Total number of bindings: 1
NO.  MACADDRESS                    LEASE(SEC)              VLA
       IPADDRESS INTERFACE                                 TYPE        N
----------
-------------------------------------
1                        1.1.1.1       78128       DHCP-        1
       0000.0000.000                                 Snooping
1
GigabitEthernet 0/1
2                        2.2.2.2       78111       DHCP-        1      WL  1
       0000.0000.000                                 Snooping            AN
2
```

2: For products supporting QINQ termination, the following example displays the information of the inner VLAN.

```
QTECH# show ip dhcp snooping binding
Total number of bindings: 1
NO.   MACADDRESS        IPADDRESS      LEASE(SEC)   TYPE         VLAN
INNER-VLAN INTERFACE
```

```
----------
1     0000.0000.0001     1.1.1.1         78128        DHCP-Snooping 1     10
GigabitEthernet 0/1
```

3: For products supporting VXLAN, the following example displays the information of the VXLAN.

```
QTECH# show ip dhcp snooping binding
Total number of bindings: 1
NO.    MACADDRESS    IPADDRESS    LEASE(SEC)     TYPE    VLAN
INNER-VLAN VXLAN     INTERFACE
1      0000.0000.0001    1.1.1.    78128    DHCP-Snooping
1      GigabitEthernet 0/1
```

Parameter	Description
Total number of bindings	The total number of bindings in the DHCP Snooping database.
NO.	The record order.
MacAddress	The MAC address of the user.
IpAddress	The IP address of the user.
Lease(sec)	The lease time of the record.
Type	The record type.
VLAN	The VLAN where the user belongs.
INNER-VLAN	The inner VLAN of the user. It is applicable to all QINQ-termination products.
VXLAN	The VXLAN where the user belongs.
Interface	The user's connection interface. It can be a either a wired access interface or wireless

	access WLAN.

Related Commands

Command	Description
ip dhcp snooping binding	Adds the static user information to the DHCP Snooping database.
clear ip dhcp snooping binding	Clears the dynamic user information from the DHCP Snooping binding database.

Platform Description

N/A

15.1. clear ipv6 dhcp snooping binding

Use this command to clear all the user information in the DHCPv6 Snooping binding database.

clear ipv6 dhcp snooping binding [*mac* **| vlan** *vlan-id* **|** *ipv6-address* **| interface** *interface-id*]

Parameter Description

Parameter	Description
mac	Specifies the MAC address to be deleted.
vlan-id	Specifies the ID of the VLAN to be cleared.
ipv6-address	Specifies the IPv6 address to be cleared.
interface-id	Specifies the interface to be cleared.

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to clear the generated user information in the DHCPv6 Snooping binding database.

Configuration Examples

Related Commands

Platform Description

The following example clears all the user information in the DHCPv6 Snooping binding database.

```
QTECH# clear ipv6 dhcp snooping
binding QTECH# show ipv6 dhcp
snooping binding
NO.  MacAddress    IPv6 Address Lease(sec) VLAN
Interface FilterType  FilterStatus
------
------

Total number of bindings: 0
```

Command	Description
N/A	N/A

N/A

15.2. clear ipv6 dhcp snooping prefix

Use this command to clear all the user information in the DHCPv6 Snooping prefix list.

clear ipv6 dhcp snooping prefix [*mac* **| vlan** *vlan-id* **|** *ipv6-prefix* **| interface** *interface-id*]

Parameter Description

Parameter	Description
mac	Specifies the MAC address to be deleted.
vlan-id	Specifies the ID of the VLAN to be cleared.
ipv6-address	Specifies the IPv6 address to be cleared.
interface-id	Specifies the interface to be cleared.

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to clear the generated user information in the DHCPv6 Snooping prefix list.

Configuration Examples

Related Commands

Platform Description

The following example clears all the user information in the DHCPv6 Snooping binding database

```
QTECH# clear ipv6 dhcp snooping
prefix QTECH# show ipv6 dhcp
snooping prefix
NO.  MacAddress    IPv6 Prefix Lease(sec) VLAN
Interface FilterType  FilterStatus
------
------

Total number of prefixes: 0
```

Command	Description
N/A	N/A

N/A

15.3. clear ipv6 dhcp snooping statistics

Use this command to clear the statistical information of the DHCPv6 packets.
clear ipv6 dhcp snooping statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to clear the statistical information of the DHCPv6 packets.

Configuration Examples

The following example clears the statistical information of the DHCPv6 packets.

```
QTECH# clear ipv6 dhcp snooping statistics QTECH# show ipv6 dhcp snooping statistics
Packets Processed by DHCPv6 Snooping = 0 Packets Dropped Because
Received on untrusted ports             = 0 Relay forward    = 0
No binding entry    = 0
Binding fail = 0
Unknown packet      = 0
Unknown output interface   = 0
No enough memory    = 0
Admin filter-dhcpv6-pkt    = 0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

15.4. ipv6 dhcp snooping

Use this command to enable the DHCPv6 Snooping function globally. Use the **no** form of this command to restore the default setting.

```
ipv6 dhcp  snooping no ipv6 dhcp snooping
```

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

The **show ip dhcpv6 snooping** command is used to display whether the DHCPv6 Snooping function is enabled.

Configuration Examples

The following example enables the DHCPv6 Snooping function globally.

```
QTECH# configure terminal
QTECH(config)# ipv6 dhcp snooping QTECH(config)# end
```

Related Commands

Command	Description
show ipv6 dhcp snooping	Displays the DHCPv6 Snooping .

Platform Description

N/A

15.5. ipv6 dhcp snooping binding-delay

Use this command to add the dynamic binding entry to the hardware filtering list after the delay. Use the **no** form of this command to restore the default setting.

`ipv6 dhcp snooping binding-delay` ***seconds***

no ipv6 dhcp snooping binding-delay

Parameter Descripti

on

Parameter	Description
seconds	Sets the binding delay time.

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

By default, the dynamic binding entries are added to the hardware filtering list in real time. With this command configured, if no IPv6 address conflict is detected within the specified time, the dynamic binding entries are added to the hardware filtering list.

Configuration Examples

Related Commands

Platform Description

The following example sets the delay to 10 seconds.

```
QTECH(config)# ipv6 dhcp snooping binding-delay 10
```

Command	Description
N/A	N/A

N/A

15.6. ipv6 dhcp snooping database write-delay

Use this command to write the dynamic user information of the DHCPv6 Snooping binding database into the flash periodically.

Use the **no** form of this command to restore the default setting.

ipv6 dhcp snooping database write-delay ***time***

no ipv6 dhcp snooping database write-delay

Parameter Description

Parameter	Description
time	The interval ranging from 600 to 86,400 in the unit of seconds, at which the system writes the dynamic user information of the DHCP Snooping database into the flash.

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

Too fast writing will reduce flash durability.

This function writes user information into flash and can avoid loss after restart. In that case, users need to obtain IP addresses again for normal communication.

Configuration Examples

The following example sets the interval at which the switch writes the user information into the flash to 3,600 seconds.

```
QTECH# configure terminal
QTECH(config)# ip dhcp snooping database write-delay 3600 QTECH(config)# end
```

Related Commands

Command	Description
show ipv6 dhcp snooping	Displays the DHCPv6 Snooping configuration.

Platform Description

N/A

15.7. ipv6 dhcp snooping database write-to-flash

Use this command to write the dynamic user information of the DHCPv6 binding database into flash in real time.

ipv6 dhcp snooping database write-to-flash

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

Use this command to write the dynamic user information of the DHCPv6 binding database into flash in real time.

Configuration Examples

The following example writes the dynamic user information of the DHCPv6 binding database into flash.

```
QTECH# configure terminal
QTECH(config)# ipv6 dhcp snooping database write-to-flash QTECH(config)#
end
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

15.8. ipv6 dhcp snooping information option

Use this command to add option18/37 to the DHCPv6 request packets. Use the **no** form of this command to restore the default setting.

`ipv6 dhcp snooping information option [ standard-format ]`

no ipv6 dhcp snooping information option [**standard-format**]

Parameter Description

Parameter	Description
standard-format	The Option18/37 uses the standard format.

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

With this command configured, the option18/37 will be added to the DHCPv6 request packets and the DHCPv6 server will assign the addresses according to the option18/37 information. Use this command without parameter **standard-format** to enable the standard format.

DHCPv6 Relay function adds option18/37 by default. Therefore, it is unnecessary to enable functions of DHCP Snooping option18/37 and DHCPv6 Relay at the same time.

Configuration Examples

The following example adds the option18/37 into the DHCPv6 packets.

```
QTECH# configure terminal
QTECH(config)# ipv6 dhcp snooping information option QTECH(config)# end
QTECH# show ipv6 dhcp snooping Switch
DHCPv6 snooping status :ENABLE DHCPv6 snooping vlan: 1-4094
DHCPv6 snooping database write-delay time: 0 seconds
DHCPv6 snooping option 18/37 status: ENABLE
DHCPv6 snooping link detection :DISABLE
Interface    Trusted      Filter DHCP
```

```
FastEthernet0/10        yes       DISABLE
```

Related Commands

Command	Description
show ipv6 dhcp snooping	Displays the configuration information of the DHCPv6 Snooping.

Platform Description

N/A

15.9. ipv6 dhcp snooping information option format remote-id

Use this command to add option37 remote-id customized character string into the DHCPv6 request packets.

Use the no form of this command to restore the default setting.

ipv6 dhcp snooping information option format remote-id [string *ascii-string* | hostname]

no ipv6 dhcp snooping information option format remote-id [string *ascii-string* | hostname]

Parameter Description

Parameter	Description
string *ascii-string*	The content of Option37 remote-id extension format is customized character string.
hostname	The content of Option37 remote-id extension format is hostname.

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

With this command configured, the option37 remote-id will be added to the DHCPv6 request packets with the content as the customized and the DHCPv6 server will assign the addresses according to the option37 information.

Configuration Examples

The following example adds the option37 remote-id to the DHCPv6 request packets with the content being hostname.

```
QTECH# configure terminal
QTECH(config)# ipv6 dhcp snooping information option format remote-id hostname
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

15.10. ipv6 dhcp snooping filter-dhcp-pkt

Use this command to filter all received DHCPv6 request packets. Use the no form of this command to restore the default setting. ipv6 dhcp snooping filter-dhcp-pkt

no ipv6 dhcp snooping filter-dhcp-pkt

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

Use this command to filter all received DHCPv6 request packets, that is, to avoid all the DHCPv6 users on this interface to apply for the addresses.

This command is valid only on 2-layer wired switch ports, aggregate ports and sub interfaces as well as in air interfaces.

Configuration Examples

The following example filters all DHCPv6 request packets on interface FastEthernet 0/1 and WLAN 1.

```
QTECH# configure terminal
QTECH(config)# interface GigabitEthernet 0/2
QTECH(config-if-GigabitEthernet 0/2)# ipv6 dhcp snooping filter-dhcp-pkt QTECH(config-if-GigabitEthernet 0/2)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

15.11. ipv6 dhcp snooping link-detection

Use this command to clear the dynamic binding entry on an interface when the interface links down. Use the **no** form of this command to restore the default setting.

```
ipv6 dhcp snooping  link-detection no ipv6 dhcp snooping link-detection
```

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

By default, the dynamic binding entries are not cleared on a wired interface when the interface links down. With this function enabled, the dynamic binding entries are auto-cleared on an interface when the interface is in the LINK DOWN status.

Configuration Examples

The following example clears the dynamic binding entry on a wired interface when the interface is in the LINK DOWN status.

```
QTECH# configure terminal
QTECH(config)# ipv6 dhcp snooping link-detection
```

Related Commands

Command	Description
show ipv6 dhcp snooping	Displays the configuration information of the DHCPv6 Snooping.

Platform Description

N/A

15.12. ipv6 dhcp snooping trust

Use this command to set the specified DHCPv6 Snooping ports as the trusted ports. Use the **no** form of this command to restore the default setting.

```
ipv6 dhcp snooping  trust no ipv6 dhcp snooping trust
```

Parameter Description

Parameter	Description
N/A	N/A

Defaults
All ports are untrusted ports by default.

Command Mode
Interface configuration mode

Usage Guide

1. Use this command to set a port as a trusted port. The DHCPv6 Server response messages received under the trust port are forwarded normally, but the response messages received under the untrusted port will be discarded.
2. This command is valid only on Layer 2 wired switch ports and aggregate ports.

Configuration Examples
The following example sets **FastEthernet** *0/1* as a trust port:

```
QTECH# configure terminal
QTECH(config)# interface GigabitEthernet 0/1 QTECH(config-if)# ipv6 dhcp snooping trust
QTECH(config-if)# end
```

Related Commands

Command	Description
show ipv6 dhcp snooping	Displays the DHCPv6 Snooping configuration.

Platform Description

N/A

15.13. ipv6 dhcp snooping vlan

Use this command to enable DHCPv6 Snooping for the specific VLAN. Use the **no** form of this command to disable this function.

ipv6 dhcp snooping vlan { *vlan-rng* **|** { *vlan-min* [*vlan-max*] } }

no ipv6 dhcp snooping vlan { *vlan-rn* **|** { *vlan-min* [*vlan-max*] } }

Parameter Description

Parameter	Description
vlan-rng	Sets the valid VLAN range.
vlan-min	Minimum VLAN ID
vlan-max	Maximum VLAN ID

Defaults

By default, once the DHCPv6 Snooping is enabled globally, it takes effect for all VLANs.

Command Mode

Global configuration mode

Usage Guide

With the global DHCPv6 snooping enabled, this function is enabled in all VLANs by default.

Configuration Examples

The following example enables the DHCPv6 Snooping function in VLAN 1000.

```
QTECH# configure terminal
QTECH(config)# ipv6 dhcp snooping vlan 1000 QTECH(config)# end
```

The following example enables the DHCPv6 Snooping function in VLAN 1 to VLAN 10.

```
QTECH# configure terminal
QTECH(config)# ipv6 dhcp snooping vlan 1-10 QTECH(config)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

15.14. ipv6 dhcp snooping vlan information option change-vlan-to vlan

Use this command to enable the function of adding the option18 interface-is into the DHCP request packets and change the VLAN to the specified VLAN for the forwarding.

Use the **no** form of this command to restore the default setting.

ipv6 dhcp snooping vlan *vlan-id* **information option change-vlan-to vlan** *vlan-id*

no ipv6 dhcp snooping vlan *vlan-id* **information option change-vlan-to vlan** *vlan-id*

Parameter Description

Parameter	Description
vlan-id	Specifies the ID of the VLAN to be replaced.

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

With this command enabled, the option18 interface-id will be added into the DHCPv6 request packets and the VLAN will be changed to the specified one and the DHCP server will assign the addresses according to the optionq8 information.

Configuration Examples

The following example adds the option18 interface-id into the DHCPv6 request packets and changes the VLAN4094 in the option to VLAN 4093.

```
QTECH# configure terminal
QTECH(config)# interface fastEthernet 0/1
QTECH(config-if)# ipv6 dhcp snooping vlan 4094 information option change-vlan-to vlan 4093
QTECH(config-if)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

15.15. ipv6 dhcp snooping vlan information option format-type interface-id string

Use this command to enable the function of adding the option18 into the DHCP request packets and filling the option18 interface-id with the content being the user-defined (the storage format is ASCII) and performing the packet forwarding.

Use the **no** form of this command to restore the default setting.

ipv6 dhcp snooping vlan *vlan-id* **information option format-type interface-id string** *ascii-string*

```
no ipv6 dhcp snooping vlan vlan-id information option format-type interface-id string
```

ascii-string

Parameter Description

Parameter	Description
vlan-id	The VLAN where the DHCPv6 request packets are
ascii-string	User-defined content for filling the interface-id

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

With this command configured, the option18 interface-id will be added into the DHCPv6 request packets with the content being user-defined and the DHCPv6 server will assign the addresses according to the option18 information.

Configuration Examples

The following example adds the option18 interface-id to the DHCPv6 request packets with the content being *port-name*.

```
QTECH# configure terminal
QTECH(config)# interface fastEthernet 0/1
QTECH(config-if)# ipv6 dhcp snooping vlan 4094 information option format-type  interface-id string port-name
QTECH(config-if)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

15.16. renew ipv6 dhcp snooping database

Use this command to import the information in current flash to the DHCPv6 Snooping binding database manually as needed.

renew ipv6 dhcp snooping database

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to import the flash file information to the DHCPv6 Snooping database in real time.

Records out of lease time and repeated will be neglected

Configuration Examples

Related Commands

The following example imports the flash file information to the DHCPv6 Snooping database.

```
QTECH# renew ipv6 dhcp snooping database
```

Command	Description
N/A	N/A

Platform

N/A

Description

15.17. show ipv6 dhcp snooping

Use this command to display the setting of the DHCPv6 Snooping.

show ipv6 dhcp snooping

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the setting of the DHCPv6 Snooping.

```
QTECH# show ipv6 dhcp snooping Switch DHCPv6 snooping status :ENABLE DHCPv6 snooping vlan: 1-4094
DHCPv6 snooping database write-delay time: 0 seconds DHCPv6 snooping option 18/37 status: DISABLE
DHCPv6 snooping link detection :DISABLE
Interface    Trusted      Filter DHCP

FastEthernet0/10    yes    DISABLE
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

15.18. show ipv6 dhcp snooping vlan

Use this command to display the VLAN with DHCPv6 Snooping function disabled.

show ipv6 dhcp snooping vlan

Parameter Description

Parameter	Description
N/A	**N/A**

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command is used to display the VLAN with DHCPv6 Snooping function disabled.

Configuration Examples

Related Commands

Platform Description

The following example displays the VLAN with DHCPv6 Snooping function disabled.

```
QTECH#s          ipv6 snoopin vlan
how VLAN         dhcp g
Name             Closed
--------
2    VLA 2       YES
     N
```

Field	Description
VLAN	VLAN ID
NAME	VLAN name
Close	Indicates whether DHCPv6 Snooping is disabled.

Command	Description
N/A	N/A

N/A

15.19. show ipv6 dhcp snooping binding

Use this command to display the information of the DHCPv6 Snooping binding database.

show ipv6 dhcp snooping binding [*mac*] [**vlan** *vlan-id*] [*ipv6-address*] [**interface** *interface-id*]

Parameter Description

Parameter	Description

mac	Displays the MAC address binding entry.
vlan_id	Displays the VLAN binding entry.
ipv6-address	Displays the IPv6 address binding entry.
interface-id	Displays the interface binding entry.

Defaults
N/A

Command Mode
Privileged EXEC mode

Usage Guide
N/A

Configuration Examples

Related Commands

Platform Description

The following example displays the information of the DHCP Snooping binding database.

```
QTECH# show ipv6 dhcp snooping
binding Total number of bindings: 1
NO.   MacAddress        IPv6                                    Lease(sec
)
Address VLAN  Interface
----------
----------
1      00d0.f801.0101     2001::10                                42368        2
GigabitEthernet 0/1
```

Command	Description
N/A	N/A

N/A

15.20. show ipv6 dhcp snooping prefix

Use this command to display all user information in the DHCPv6 Snooping prefix list.

show ipv6 dhcp snooping prefix [*mac* | **vlan** *vlan-id* **|** *ipv6-prefix* | **interface** *interface-id*]

Parameter Description

Parameter	Description
mac	Displays the MAC address prefix entry.
vlan_id	Displays the VLAN prefix entry.
ipv6-prefix	Displays the IPv6 address prefix entry.
interface-id	Displays the interface prefix entry.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example displays all user information in the DHCPv6 Snooping prefix list.

```
QTECH# show ipv6 dhcp snooping
prefix Total number of prefix: 1

NO.  MacAddress      IPv6 Prefix      Lease(sec)  VLAN      Interface

1    00d0.f801.0101  2001:2002::      42368       2         GigabitEthernet 0/1
```

Command	Description
N/A	N/A

N/A

15.21. show ipv6 dhcp snooping statistics

Use this command to display the statistical information of the DHCPv6 packets.
show ipv6 dhcp snooping statistics

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode
Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the statistical information of the DHCPv6 packets.

```
QTECH# show ipv6 dhcp snooping statistics
Packets Processed by DHCPv6 Snooping = 0 Packets Dropped Because
Received on untrusted ports             = 0
Relay forward= 0
No binding entry    = 0
Binding fail = 0
Unknown packet      = 0
Unknown output interface    = 0
No enough memory          = 0
Admin filter-dhcpv6-pkt = 0
```

Field	Description
Received on untrusted ports	The discarded server response packets on the untrust port.
Relay forward	The packets that have been relayed once are discarded.
No binding entry	The binding entries of the release/decline packets are in-existent or error and the packets are discarded.
Binding fail	The entry binding fails and the packets are discarded due to a lack of the hardware resources.
Unknown packet	The unknown DHCP packets.
Unknown output interface	The packets on the unknown output interface. The MAC address for the interface is not found or the trust port is not configured.
No enough memory	There is no enough memory.
Admin filter-dhcpv6-pkt	The filtered DHCPv6 packets configured by the administrator. Use the **ipv6 dhcp snooping filter-dhcp-pkt** command to filter the packets.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

16.1. arp-check

Use this command to enable the ARP check function on the Layer 2 interface. Use the **no** form of this command to restore the default setting.

arp-check

no arp-check

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command mode

Interface configuration mode

Usage Guide

The ARP check function generates the ARP filtering information according to legal user information, implementing the illegal ARP packet filtering on the network.

Configuration Examples

This following example enables the APR check function on interface GigabitEthernet 0/1.

```
QTECH# configure terminal
QTECH(config)# interface GigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)# arp-check QTECH(config-if-GigabitEthernet 0/1)# end
```

Related Commands

Command	Description

show interfaces arp-check list	Displays the ARP check entries.

Platform Description

N/A

16.2. show interfaces arp-check list

Use this command to display the ARP check entries on the Layer 2 interface.

show { **interfaces** [*interface-type interface-number*]] } **arp-check list**

Parameter Description

Parameter	Description
interface-type	Wired interface type
interface-number	Wired interface number

Command mode

Privileged EXEC mode

Usage Guide

Use this command to display the ARP check entries.

Configuration Examples

Related Commands

Platform Description

The following example displays the ARP check entries.

```
QTECH(config)#show interfaces arp-check list
INTERFACE                    SENDER MAC  SENDER IP
                             POLIC Y SOURCE
-------------------------------------------------
-------------------------------------

GigabitEthernet 0/1        00D0.F800.000    192.168.1.3
                                        3
```

```
address-bind
GigabitEthernet 0/1      00D0.F800.0001   192.168.1.1
port-security
GigabitEthernet 0/4                       192.168.1.3
port-security
GigabitEthernet 0/5      00D0.F800.0003   192.168.1.3
address-bind
GigabitEthernet 0/7      00D0.F800.0006   192.168.1.6      AAA
ip-auth-mode
GigabitEthernet 0/8      00D0.F800.0007   192.168.1.7      GSN
```

Field	Description
INTERFACE	Interface name
SENDER MAC	Source MAC address
SENDER IP	Source IP address
POLICY SOURCE	Source of the entry

Command	Description
N/A	N/A

N/A

17.1. ip arp inspection trust

Use this command to configure the L2 port to a trusted port.

Use the **no** form of this command to restore the L2 port to an untrusted port.

ip arp inspection trust

no ip arp inspection

trust

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The L2 port is untrusted.

Command Mode

Interface configuration mode

Usage Guide

If it is necessary to make the ARP message received by some interface pass the DAI inspection unconditionally, you can set the interface to a trusted port, indicating that you do not need to check whether the ARP message received by this interface is legal.

Configuration Examples

The following example sets the gigabitEthernet 0/19 interface as the trusted port.

```
QTECH# configure terminal
QTECH(config)# interface gigabitEthernet 0/19
QTECH(config-if-GigabitEthernet 0/19)# ip arp inspection trust QTECH(config-if-GigabitEthernet 0/19)# end
```

Related Commands

Command	Description
show ip arp inspection interface	Displays related DAI information on the interface, including the trust state and rate limit of the interface.

Platform Description

N/A

17.2. ip arp inspection vlan

Use this command to configure the DAI function on the VLAN. Use the **no** form of this command to disable this function.

Parameter Description

ip arp inspection vlan { *vlan-id* | *word* }
no ip arp inspection vlan { *vlan-id* | *word* }

Parameter	Description
vlan-id	VLAN ID, ranging from 1 to 4094
word	String of the VLAN range, such as 1,3-5,7,9-11

Defaults
The DAI function on all VLANs is disabled by default.

Command Mode

Global configuration mode

Usage Guide
To make this command take effect, you need to enable the ARP Check function first, Not all ports of the VLAN support the ARP packet detection function. For example, the DHCP Snooping Trust port does not support any security detection, including this function.

Configuration Examples

The following example detects the received ARP packets on the VLAN1 interfaces:

```
QTECH# configure terminal QTECH(config)# ip arp inspection QTECH(config)# ip arp inspection vlan 1
QTECH(config)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

17.3. show ip arp inspection vlan

Use this command to verify whether the DAI function on the VLAN is enabled.

show ip arp inspection vlan [*vlan-id* | *word*]

Parameter Description

Parameter	Description
vlan-id	VLAN ID, ranging from 1 to 4094
word	String of the VLAN range, such as 1,3-5,7,9-11

Defaults
N/A

Command
Privileged EXEC mode

Mode

Usage Guide
Use this command to verify whether the DAI function on the VLAN is enabled.

Configuration Examples

The following example verifies whether the DAI function on the VLAN is enabled:

Related Commands

```
QTECH# show ip arp inspection vlan
Vlan   Configuration
1                              Active
```

Platform Description

Parameter Description:

Parameter	Description
Vlan	VLAN number.
Configuration	DAI status (active / inactive)

Command	Description
N/A	N/A

N/A

17.4. show ip arp inspection interface

Use this command to verify whether the interface is a DAI trust interface.

show ip arp inspection interface

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command to verify whether the interface is a DAI trust interface.

Configuration Examples

The following example verifies the DAI trust state of all :

```
QTECH#show ip arp inspection interface
Interface    Trust State

GigabitEthernet 0/1      Untrusted
Default                  Untrusted
```

Parameter Description:

Parameter	Description
Interface	Interface name.
Trust State	DAI trust state.

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

18.1. ip source binding

Use this command to add static user information to IP source address binding database. Use the **no** form of this command to delete static user information from IP source address binding database.

ip source binding *mac-address* **{ vlan** *vlan-id* **}** *ip-address* { **interface** *interface-id* **| ip-mac | ip-only** }

no ip source binding *mac-address* **{ vlan** *vlan-id* **}** *ip-address* { **interface** *interface-id* **| ip-mac | ip-only** }

Parameter Description

Parameter	Description
mac-address	Adds user MAC address statically.
vlan-id	Adds user VLAN ID statically.
ip-address	Adds user IP address statically.
interface-id	Adds user interface ID statically.
ip-mac	The global binding type is IP+MAC
ip-only	The global binding type is IP only.

Defaults

No static address is added by default.

Command Mode

Global configuration mode

Usage Guide

This command allows specific clients to go through IP source guard detection instead of DHCP. This command is supported on the wired L2 switching port, AP port, and sub interface.

This command enables global binding for IP source guard so that specific clients will get detected on all interfaces.

A static IPv6 source binding is valid either on wired interfaces or in global configuration mode. A new binding will overwrite the old one sharing the same configuration.

Configuration Examples

The following example adds the interface ID of static users.

```
QTECH# configure terminal
QTECH(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 interface GigabitEthernet 0/1
QTECH(config)# end
```

The following example adds static user information based on IP-MAC binding.

```
QTECH# configure terminal
QTECH(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 ip-mac QTECH(config)# end
```

The following example adds static user information based on IP binding.

```
QTECH# configure terminal
QTECH(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 ip-only QTECH(config)# end
```

Related Commands

Command	Description
show ip source binding	Displays the binding information of IP source address and database.

Platform Description

N/A

18.2. ip verify source

Use this command to enable IP Source Guard function on the interface. Use the **no** form of this command to restore the default setting.

ip verify source [**port-security**]

no ip verify source

Parameter Description

Parameter	Description
port-security	Configures IP Source Guard to do IP+MAC-based detection.

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

This command enables IP Source Guard function on the interface to do IP-based or IP+MAC-based

detection.

This command is supported on the wired L2 switching port, AP port, and sub interface

IP Source Guard takes effect only on DHCP Snooping untrusted port. In other words, IP Source Guard does not take effect when configuring it on Trust port or the port which is not controlled by DHCP Snooping.

Configuration Examples

The following example enables IP-based IP Source Guard function.

```
QTECH# configure terminal
QTECH(config)# interface GigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)# ip verify source
QTECH(config-if)# end
```

The following example enables IP+MAC-based IP Source Guard function.

```
QTECH# configure terminal
QTECH(config)# interface GigabitEthernet 0/2
QTECH(config-if-GigabitEthernet 0/2)# ip verify source port-security QTECH(config-if)# end
```

Related Commands

Command	Description
show ip verify source	Displays user filtering entry of IP

	Source Guard.

Platform Description

N/A

18.3. ip verify source exclude-vlan

Use this command to exclude a VLAN from the IP source guard configuration on the port. Use the **no** form of this command to restore the function.

ip verify source exclude-vlan *vlan-id*

no ip verify source exclude-vlan *vlan-id*

Parameter Description

Parameter	Description
vlan-id	The ID of VLAN excluded from the IP source guard configuration.

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

This command is used to exclude a VLAN from the IP source guard configuration. IP packets in this VLAN are forwarded without being checked and filtered.

- Once the IP source guard function is disabled, the excluded VLAN is cleared automatically.
- This command is supported on the wired L2 switching port, AP port, and sub interface.

Only when the IP source guard configuration is enabled on the port can a VLAN be excluded.

Configuration Examples

The following example configuration configures the IP source guard configuration for the port and excludes a VLAN.

```
QTECH# configure terminal
QTECH(config)# interface GigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)# ip verify source
QTECH(config-if-GigabitEthernet 0/1)# ip verify exclude-vlan 1
QTECH(config-if)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

18.4. show ip source binding

Use this command to display the binding information of IP source addresses and database.

show ip source binding [*ip-address*] [*mac-address*] [**dhcp-snooping**] [**static**] [**vlan** *vlan-id*] [**interface** *interface-id*]

Parameter Description

Parameter	Description
ip-address	Displays user binding information of corresponding IP.
mac-address	Displays user binding information of corresponding MAC.
dhcp-snooping	Displays binding information of dynamic user.
static	Displays binding information of static user.
vlan-id	Displays user binding information of corresponding VLAN.
interface-id	Displays user binding information of corresponding interface.

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the binding information of IP source guard addresses and database.

```
QTECH# show ip source binding static QTECH#show ip source
binding static Total number of bindings: 5
NO. MACADDRESS IPADDRESS LEASE(SEC) TYPE VLAN  INTERFACE
                                                                    1
0001.0002.0001     1.2.3.2      Infinite    Static      1       Global
2    0001.0002.0002.... 1.2.3.3 Infinite Static 1 GigabitEthernet 0/5
3    0001.0002.0003     1.2.3.4      Infinite    Static      1       Global
4    0001.0002.0004     1.2.3.5      Infinite    Static      1       Global
```

Related Commands

Command	Description
ip source binding	Sets the binding static user.

Platform Description

N/A

18.5. show ip verify source

Use this command to display user filtering entry of IP Source Guard.

show ip verify source [**interface** *interface-id*]

Parameter Description

Parameter	Description
interface-id	Displays user filtering entry of corresponding interface.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

If IP Source Guard is not enabled on the corresponding interface, the printing information will be shown on the terminal as: “IP source guard is not configured on the interface FastEthernet 0/10” Now, IP Source Guard supports the following filtering modes:

inactive-restrict-off: the IP Source Guard is disabled on bound interfaces.

inactive--not-apply: the IP Source Guard cannot adds bound entries into filtering entries for system errors.

active: the IP Source Guard is active.

Configuration Examples

The following example displays user filtering entry of IP Source Guard.

```
QTECH # show ip verify source
Total number of bindings: 7
```

```
NO.             FILTERTYPE  FILTERSTATUS   IPADDRESS VLAN TYPE
       INTERF
ACE
MACADDRESS


Global IP+MAC Inactive-not-apply  192.168.0.127
0001.0002.0003 1 Static
GigabitEthernet 0/5  IP-ONLY      Active 1.2.3.4
0001.0002.0004 1 DHCP-Snooping
Global IP-ONLY       Active 1.2.3.7
0001.0002.0007 1 Static
Global IP+MAC Active 1.2.3.6
0001.0002.0006 1 Static
GigabitEthernet 0/1  UNSET Inactive-restrict-off  1.2.3.9
0001.0002.0009 1 DHCP-Snooping
GigabitEthernet 0/5  IP-ONLY      Active Deny-All
```

Related Commands

Command	Description

ip verify source	Sets IP Source Guard on the interface.

Platform Description

N/A

19.1. ipv6 source binding

Use this command to configure a static IPv6 source binding.

Use the **no** form of this command to delete a static IPv6 source binding.

ipv6 source binding *mac-address* **vlan** *vlan-id ipv6-address* { **interface** *interface-id* **| | ip-mac | ip-only** }

no ipv6 source binding *mac-address* **vlan** *vlan-id ipv6-address* { **interface** *interface-id* **| | ip-mac | ip-only** }

Parameter Description

Parameter	Description
mac-address	MAC address
vlan-id	VLAN ID
ipv6-address	IPv6 address
interface-id	Wired interface ID
ip-mac	IPv6-MAC binding
ip-only	IPv6-only binding

Defaults

No static IPv6 source binding is configured by default.

Command Mode

Global configuration mode

Usage Guide

Use this command to exempt trusted hosts from IPv6 source guard.

This command is supported only on Layer 2 ports, aggregate ports and encapsulated sub interfaces.

A static IPv6 source binding is valid either on wired interfaces or in global configuration mode.

A new binding will overwrite the old one sharing the same configuration.

Configuration Examples

The following example configures static IPv6 source bindings on GigabitEthernet 0/1.

```
QTECH# configure terminal
QTECH(config)# ipv6 source binding 0000.0000.0001 vlan 1 1::1 interface GigabitEthernet 0/1
QTECH(config)# end
```

The following example configures a static IPv6-MAC binding.

```
QTECH# configure terminal
QTECH(config)# ipv6 source binding 0000.0000.0001 vlan 1 1::1 ip-mac QTECH(config)# end
```

The following example configures a static IPv6-only binding.

```
QTECH# configure terminal
QTECH(config)# ipv6 source binding 0000.0000.0001 vlan 1 1::1 ip-only QTECH(config)# end
```

Platform Description

N/A

19.2. ipv6 verify source

Use this command to enable IPv6 source guard.

Use the **no** form of this command to restore the default setting.

ipv6 verify source [**port-security**]
no ipv6 verify source

Parameter Description

Parameter	Description
port-security	Enables source IPv6-MAC filtering.

Defaults
IPv6 source guard is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

Use this command to enable IPv6 source guard with source IPv6 filtering or source IPv6-MAC filtering.

This command is supported only on Layer 2 ports, aggregate ports and encapsulated sub interface.

Currently, the IPv6 source guard feature of QTECH devices filters traffic based on the DHCPv6 Snooping database or on manually configured IPv6 source bindings. A port with only IPv6 source guard enabled cannot realize normal network access for connected hosts.

Configuration Examples

The following example enables IPv6 source guard based on source IPv6 filtering.

```
QTECH# configure terminal
QTECH(config)# interface GigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)# ipv6 verify source QTECH(config-if)# end
```

```
QTECH# configure terminal
QTECH(config)# interface GigabitEthernet 0/2
QTECH(config-if-GigabitEthernet 0/2)# ipv6 verify source port-security QTECH(config-if)# end
```

The following example enables IPv6 source guard based on source IPv6-MAC filtering.

Platform

N/A

Description

19.3. show ipv6 source binding

Use this command to display the IPv6 source binding database.

show ipv6 source binding [*ipv6-address*] [*mac-address*] [**dhcp-snooping**] [**static**] [**vlan** *vlan-id*] [**interface** *interface-id*]

Parameter Description

Parameter	Description

ipv6-address	Displays the source IPv6 address bindings.
mac-address	Displays the source MAC address bindings.
dhcp-snooping	Displays the DHCP snooping bindings.
static	Displays the static IPv6 source bindings.
vlan-id	Displays the VLAN bindings.
interface-id	Displays the interface bindings.

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the IPv6 source binding database.

```
QTECH# show ipv6 source binding
Total number of bindings: 7
NO.     Filter Type  Filter Status          IPv6 Address
MACAddress      VLAN Type  Interface
-----------
----------------------------------------------------------------------------------------------------------------------------------------------------
----------------------------
1       IPv6+MAC     Inactive-system-error   2000::127
0001.0002.0003   1     Static          Global
2       IPv6-ONLY    Active                2008::4
0001.0002.0004  1     DHCPv6-Snooping    GigabitEthernet 0/5
3       IPv6-ONLY    Active                2008::7
0001.0002.0007   1     Static          Global
4       IPv6+MAC     Active                2008::1
0001.0002.0006   1     Static          Global
5       UNSET       Inactive-restrict-off   2008::9
0001.0002.0009   1     DHCPv6-Snooping    GigabitEthernet 0/1
6       IPv6-ONLY    Active                Deny-All
                                    GigabitEthernet 0/5
```

Platform

N/A

Description

20.1. anti-arp-spoofing ip

Use this command to enable anti-ARP spoofing.

Use the **no** form of this command to disable this function.

anti-arp-spoofing ip *ip-address*

no anti-arp-spoofing ip *ip-address*

Parameter Description

Parameter	Description
ip-address	Gateway IP address

Defaults

The anti-ARP spoofing function is disabled by default.

Command Mode

Interface configuration mode/Wireless security configuration mode

Usage Guide

This command is used to enable anti-ARP spoofing on only L2 interfaces.

This command is used on AC/AP only in wireless security configuration mode. Use the **show anti-arp-spoofing** command to display the configuration.

Configuration Examples

The following example enables anti-ARP spoofing.

```
QTECH(config)#interface fastEthernet 0/1
QTECH(config-if)#anti-arp-spoofing ip 192.168.1.1
```

Related Commands

Command	Description
show anti-arp-spoofing	Displays the anti-ARP spoofing

	configuration.

Platform Description

N/A

20.2. show anti-arp-spoofing

Use this command to display the anti-ARP spoofing configuration on all interfaces.

show anti-arp-spoofing

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

This command is used to display the anti-ARP spoofing configuration on all interfaces.

Configuration Examples

Related Commands

Platform Description

The following example displays the anti-ARP-spoofing configuration on all interfaces.

```
QTECH#s   anti-arp-spoofing
how NO          IP                STATUS
        POR
T
----------
```

```
1       Gi0/1       192.168.1.1       active
```

Field Description

Field	Description
NO	Order number
PORT	Port number
IP	Gateway IP
STATUS	Anti-ARP spoofing status

Command	Description
anti-arp-spoofing ip	Configures anti-ARP spoofing.

N/A

21.1. arp-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.

Use the **no** or **default** form of this command to restore the default setting. **arp-guard attack-threshold** { **per-src-ip** | **per-src-mac** | **per-port** } *pps* **no arp-guard attack-threshold** { **per-src-ip** | **per-src-mac** | **per-port** }
default arp-guard attack-threshold { **per-src-ip** | **per-src-mac** | **per-port** }

Parameter Description

Parameter	Description
per-src-ip	Sets the attack threshold for each source IP address.
per-src-mac	Sets the attack threshold for each source MAC address.
per-port	Sets the attack threshold for each port.
pps	Sets the attack threshold, in the range from 1 to 19,999 in unit of pps.

Defaults

The default value varies with products. For details, see the *Configuration Guide*.

Command Mode

NFPP configuration mode.

Usage Guide

The attack threshold shall be equal to or greater than the rate-limit threshold.

Configuration Examples

The following example sets the global attack threshold.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# arp-guard attack-threshold per-src-ip 2 QTECH(config-nfpp)# arp-guard attack-threshold per-src-mac 3
```

```
QTECH(config-nfpp)# arp-guard attack-threshold per-port 50
```

Related Commands

Command	Description
nfpp arp-guard policy	Displays the rate-limit threshold and attack threshold.
show nfpp arp-guard summary	Displays the configuration.
show nfpp arp-guard hosts	Displays the monitored host.
clear nfpp arp-guard hosts	Clears the isolated host.

Platform Description

N/A

21.2. arp-guard enable

Use this command to enable the anti-ARP guard function globally.

Use the **no** or **default** form of this command to restore the default setting.

arp-guard enable no

arp-guard enable

default arp-guard enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command Mode

NFPP configuration mode.

Usage Guide

N/A

Configuration Examples

The following example enables the anti-ARP guard function globally.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# arp-guard enable
```

Related Commands

Command	Description
nfpp arp-guard enable	Enables the anti-ARP attack on the interface.
show nfpp arp-guard summary	Displays the configuration.

Platform Description

N/A

21.3. arp-guard isolate-period

Use this command to set the arp-guard isolate time globally.

Use the **no** or **default** form of this command to restore the default setting.

arp-guard isolate-period { *seconds* | **permanent** }

no arp-guard isolate-period

default arp-guard isolate-

period

Parameter Description

Parameter	Description
seconds	Sets the isolate time. The value is 0, or in the range from 30 to 86400 in the unit of seconds.
permanent	Permanent isolation.

Defaults

The default isolate time is 0, which means no isolation.

Command Mode

NFPP configuration mode.

Usage Guide

N/A

Configuration Examples

The following example sets the arp-guard isolate time globally to 180 seconds.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# arp-guard isolate-period 180
```

Related Commands

Command	Description
nfpp arp-guard isolate-period	Sets the isolate time on the interface.
show nfpp arp-guard summary	Displays the configuration.

Platform Description

N/A

21.4. arp-guard isolate-forwarding enable

Use this command to enable packet forwarding through NFPP isolation. Use the **no** form of this command to disable this function.
Use the **default** form of this command to restore the default setting.

arp-guard isolate-forwarding enable

no arp-guard isolate-forwarding

enable default arp-guard isolate-forwarding enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults
This function is enabled by default.

Command Mode

NFPP configuration mode

Usage Guide N/A

Configuration Examples

The following example enables packet forwarding through NFPP isolation.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# arp-guard isolate-forwarding enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

21.5. arp-guard monitored-host-limit

Use this command to set the maximum monitored host number.
Use the **no** or **default** form of this command to restore the default setting.
arp-guard monitored-host-limit *number* **no arp-guard monitored-host-limit default arp-guard monitored-host-limit**

Parameter Description

Parameter	Description
number	The maximum monitored host number, in the range from 1 to 4,294,967,295.

Defaults

The default is 20000.

Command Mode

NFPP configuration mode

Usage Guide

If the monitored host number has reached the default 20,000, the administrator shall set the max-number smaller than 20,000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20,000, please clear a part of monitored hosts to remind the administrator of the invalid configuration and removing the monitored hosts.

When the maximum monitored host number has been exceeded, it prompts the message that % NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts to remind the administrator.

Configuration Examples

The following example sets the maximum monitored host number to 200.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# arp-guard monitored-host-limit 200
```

Related Commands

Command	Description
show nfpp arp-guard summary	Displays the configuration.

Platform Description

N/A

21.6. arp-guard monitor-period

Use this command to configure the arp guard monitor time.
Use the **no** or **default** form of this command to restore the default setting.
arp guard monitor-period *seconds* **no arp-guard monitor-period default arp-guard monitor-period**

Parameter Description

Parameter	Description
seconds	Sets the monitor time, in the range from 180 to 86,400 in the unit of seconds.

Defaults
The default is 600.

Command Mode

NFPP configuration mode

Usage Guide

When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.
If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

Configuration Examples

The following example sets the arp guard monitor time to 180 seconds.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# arp-guard monitor-period 180
```

Related Commands

Command	Description
show nfpp arp-guard summary	Displays the configuration.
show nfpp arp-guard hosts	Displays the monitored host list.
clear nfpp arp-guard hosts	Clears the isolated host.

Platform Description

N/A

21.7. arp-guard rate-limit

Use this command to set the arp guard rate limit.

Use the **no** or **default** form of this command to restore the default setting.

arp-guard rate-limit { **per-src-ip** | **per-src-mac** | **per-port** } *pps*

Parameter Description

no arp-guard rate-limit { **per-src-ip | per-src-mac | per-port** }

default arp-guard rate-limit { **per-src-ip | per-src-mac | per-port** }

Parameter	Description
per-src-ip	Sets the rate limit for each source IP address.
per-src-mac	Sets the rate limit for each source MAC address.
per-port	Sets the rate limit for each port.
pps	Sets the rate limit, in the range of 1 to 19,999.

Defaults

The default value varies with products. For details, see the *Configuration Guide*.

Command Mode

NFPP configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the arp guard rate limit.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# arp-guard rate-limit per-src-ip 2 QTECH(config-nfpp)# arp-guard rate-limit per-src-mac 3 QTECH(config-nfpp)# arp-guard rate-limit per-port 50
```

Related Commands

Command	Description
nfpp arp-guard policy	Sets the rate limit and the attack threshold.
show nfpp arp-guard summary	Displays the configuration.

Platform Description

N/A

21.8. arp-guard ratelimit-forwarding enable

Use this command to set the port based arp guard rate limit. Use the **no** form of this command to disable this function.
Use the **default** form of this command to restore the default setting.

arp-guard ratelimit-forwarding enable
no arp-guard ratelimit-forwarding enable
default arp-guard ratelimit-forwarding enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command Mode

NFPP configuration mode

Usage Guide N/A

Configuration Examples

The following example sets the port based arp guard rate limit.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# arp-guard ratelimit-forwarding enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

21.9. arp-guard scan-threshold

Use this command to set the global scan threshold.

Use the **no** or **default** form of this command to restore the default setting.

arp-guard scan-threshold ***pkt-cnt*** no arp-guard scan-threshold default arp-guard scan-threshold

Parameter Description

Parameter	Description
pkt-cnt	Sets the scan threshold, in the range from 1 to 19,999 in the unit of

	seconds.

Defaults

The default value varies with products. For details, see the *Configuration Guide*.

Command Mode

NFPP configuration mode

Usage Guide

The scanning may occur on the condition that:

- More than 15 packets are received within 10 seconds;
- The source MAC address for the link layer is constant while the source IP address is uncertain;
- The source MAC and IP address for the link layer is constant while the destination IP address is uncertain.

Configuration Examples

The following example sets the global scan threshold to 20pps.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# arp-guard scan-threshold 20
```

Related Commands

Command	Description
nfpp arp-guard scan-threshold	Sets the scan threshold on the port.
show nfpp arp-guard summary	Displays the configuration.
show nfpp arp-guard scan	Displays the ARP guard scan table.
clear nfpp arp-guard scan	Clears the ARP guard scan table.

Platform Description

N/A

21.10. clear nfpp arp-guard hosts

Use this command to clear the monitored host isolation.

clear nfpp arp-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*ip-address* | *mac-address*]

Parameter Description

Parameter	Description
vid	Sets the VLAN ID.
interface-id	Sets the interface name and number.
ip-address	Sets the IP address.
mac-address	Sets the MAC address.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

Related Commands

The following example clears the monitored host isolation.

```
QTECH# clear nfpp arp-guard hosts vlan 1 interface g0/1
```

Command	Description
arp-guard attack-threshold	Sets the global attack threshold.
nfpp arp-guard policy	Sets the limit threshold and attack threshold.
show nfpp arp-guard hosts	Displays the monitored host.

Platform

N/A

Description

21.11. clear nfpp arp-guard scan

Use this command to clear ARP scanning table.

clear nfpp arp-guard scan

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example clears ARP scanning table.

```
QTECH# clear nfpp arp-guard scan
```

Command	Description
arp-guard attack-threshold	Sets the global attack threshold.
nfpp arp-guard policy	Sets the attack threshold.

show nfpp arp-guard scan	Displays the ARP scanning table.

N/A

21.12. clear nfpp define *name* hosts

Use this command to clear the monitored hosts. If the host is isolated, you need to release it. **clear nfpp define** *name* **hosts** [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*] [*mac-address*] [*ipv6-address*]

Parameter Description

Parameter	Description
name	Defines guard name
vid	VLAN ID
interface-id	Interface name
ip-address	IP address
mac	MAC address
ipv6-address	IPv6 address

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command without the parameter to clear all monitored hosts in the self-defined range.

Configuration Examples

Related Commands

Platform Description

The following example clears the monitored hosts.

```
QTECH# clear nfpp define tcp hosts vlan 1 interface g0/1
```

Command	Description
show nfpp define hosts	Displays the isolated hosts.

N/A

21.13. clear nfpp dhcp-guard hosts

Use this command to clear the DHCP monitored hosts, that it, release them from isolation.

clear nfpp dhcp-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]

Parameter Description

Parameter	Description
vid	Sets the VLAN ID.
interface-id	Sets the interface name and number.
mac-address	Sets the MAC address.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command without the parameter to clear all monitored hosts.

Configuration Examples

Related Commands

The following example clears the DHCP monitored hosts.

```
QTECH# clear nfpp dhcp-guard hosts vlan 1 interface g0/1
```

Command	Description

dhcp-guard attack-threshold	Sets the global attack threshold.
nfpp dhcp-guard policy	Sets the limit threshold and attack threshold.
show nfpp dhcp-guard hosts	Displays the monitored host.

Platform Description

N/A

21.14. clear nfpp dhcpv6-guard hosts

Use this command to clear the DHCPv6 monitored host isolation.

clear nfpp dhcpv6-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]

Parameter Description

Parameter	Description
vid	Sets the VLAN ID.
interface-id	Sets the interface name and number.
mac-address	Sets the MAC address.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command without the parameter to clear all monitored hosts

Configuration Examples

Related Commands

Platform Description

The following example clears the DHCPv6 monitored hosts.

```
QTECH# clear nfpp dhcpv6-guard hosts vlan 1 interface g0/1
```

Command	Description
dhcpv6-guard attack-threshold	Sets the global attack threshold.
nfpp dhcpv6-guard policy	Sets the limit threshold and attack threshold.
show nfpp dhcpv6-guard hosts	Displays the monitored host.

N/A

21.15. clear nfpp icmp-guard hosts

Use this command to clear the ICMP monitored hosts.

clear nfpp icmp-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]

Parameter Description

Parameter	Description
vid	Sets the VLAN ID.
interface-id	Sets the interface name and number.
ip-address	Sets the IP address.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

Use this command without the parameter to clear all monitored hosts.

Configuration Examples

Related Commands

Platform Description

The following example clears the ICMP monitored hosts.

```
QTECH# clear nfpp icmp-guard hosts vlan 1 interface g0/1
```

Command	Description
icmp-guard attack-threshold	Sets the global attack threshold.
nfpp icmp-guard policy	Sets the limit threshold and attack threshold.
show nfpp icmp-guard hosts	Displays the monitored host.

N/A

21.16. clear nfpp ip-guard hosts

Use this command to clear the monitored host isolation.

clear nfpp ip-guard hosts [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]

Parameter Description

Parameter	Description
vid	Sets the VLAN ID.
interface-id	Sets the interface name and number.
ip-address	Sets the IP address.

Defaults

N/A.

Command Mode

Privileged EXEC mode

Usage Guide

Use this command without the parameter to clear all monitored hosts.

Configuration Examples

The following example clears the monitored host isolation.

```
QTECH# clear nfpp ip-guard hosts vlan 1 interface g0/1
```

Related Commands

Command	Description
ip-guard attack-threshold	Sets the global attack threshold.
nfpp ip-guard policy	Sets the limit threshold and attack threshold.
show nfpp ip-guard hosts	Displays the monitored host.

Platform Description

N/A

21.17. clear nfpp nd-guard hosts

Use this command to remove the speed limit on the monitored host.

clear nfpp nd-guard hosts [**vlan** *vid*] [**interface** *interface-id*]

Parameter Description

Parameter	Description
vid	Sets the VLAN ID.
interface-id	Sets the interface name and number.

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command without any parameter is used to remove speed limit on all monitored hosts.

Configuration Examples

The following example removes speed limit on interface g0/1 in VLAN 1.

```
QTECH# clear nfpp nd-guard hosts vlan 1 interface g0/1
```

Prompt Messages

N/A

Platform Description

N/A

21.18. clear nfpp log

Use this command to clear the NFPP log buffer area.

clear nfpp log

Parameter

Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example clears the NFPP log buffer area.

```
QTECH# clear nfpp log
```

Command	Description

show nfpp log	Displays the NFPP log configuration or the log buffer area.

N/A

21.19. define

Use this command to define the anti-attack type.

Use the **no** or **default** form of this command to restore the default setting.

define *name*

no define *name*

default define *name*

Parameter Description

Parameter	Description
name	Name of the user-defined anti-attack type

Defaults

N/A

Command Mode

NFPP configuration mode

Usage Guide

Use this command to define the anti-attack type.

Configuration Examples

The following example creates the user-defined anti-attack type.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# define tcp QTECH(config-nfpp-define)#
```

Related Commands

Command	Description
show nfpp define summary	Displays the defined anti-attack

	configuration.

Platform Description

N/A

21.20. define *name* enable

Use this command to enable the user-defined anti-attack globally.

Use the **no** or **default** form of this command to restore the default setting.

define *name* **enable**

no define *name* **enable**

default define *name* **enable**

Parameter Description

Parameter	Description
name	Defines guard name.

Defaults

This function is disabled by default.

Command Mode

NFPP configuration mode

Usage Guide

This command takes effect only after the match, rate-limit and attack-threshold have been configured.

Configuration Examples

The following example enabled the user-defined anti-attack globally.

```
QTECH(config)# nfpp
QTECH(config-nfpp)#define tcp enable
```

Related Commands

Command	Description

show nfpp define summary	Displays the user-defined anti-attack configuration

Platform Description

N/A

21.21. dhcp-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.

Parameter Description

Use the **no** or **default** form of this command to restore the default setting.
dhcp-guard attack-threshold { **per-src-mac** | **per-port** } *pps*
no dhcp-guard attack-threshold { **per-src-mac** | **per-port** }
default dhcp-guard attack-threshold { **per-src-mac** | **per-port** }

Parameter	Description
per-src-mac	Sets the attack threshold for each source MAC address.
per-port	Sets the attack threshold for each port.
pps	Sets the attack threshold, in pps. The valid range is 1 to 19,999.

Defaults

The default value varies with products. For details, see the *Configuration Guide*

Command Mode

NFPP configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the global attack threshold.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# dhcp-guard attack-threshold per-src-mac 15 QTECH(config-nfpp)# dhcp-guard attack-threshold per-port 200
```

Related Commands

Command	Description
nfpp dhcp-guard policy	Displays the rate-limit threshold and attack threshold.
show nfpp dhcp-guard summary	Displays the configuration.
show nfpp dhcp-guard hosts	Displays the monitored host list.
clear nfpp dhcp-guard hosts	Clears the monitored host.

Platform Description

N/A

21.22. dhcp-guard enable

Use this command to enable the DHCP anti-attack function.

Use the **no** or **default** form of this command to restore the default setting.

dhcp-guard enable no

dhcp-guard enable

default dhcp-guard enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

NFPP configuration mode

Usage Guide

N/A

Configuration Examples

The following example enables the DHCP anti-attack function.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# dhcp-guard enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

21.23. dhcp-guard isolate-period

Use this command to set the isolate time globally.

Use the **no** or **default** form of this command to restore the default setting.

dhcp-guard isolate-period { *seconds* | **permanent** }

no dhcp-guard isolate-period

default dhcp-guard isolate-

period

Parameter Description

Parameter	Description
seconds	Sets the isolate time. The value is 0 or in the range from 30 to 86,400 in the unit of seconds.
permanent	Permanent isolation.

Defaults

The default isolate time is 0, which means no isolation.

Command Mode

NFPP configuration mode

Usage Guide

The isolate period can be configured globally or based on the interface. For one interface, if the isolate period is not set based on the interface, the global value shall be adopted; or the interface-based isolate period shall be adopted.

Configuration Examples

The following example sets the isolate time globally to 180 seconds.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# dhcp-guard isolate-period 180
```

Related Commands

Command	Description
nfpp dhcp-guard isolate-period	Sets the isolate time on the interface.
show nfpp dhcp-guard summary	Displays the configuration.

Platform Description

N/A

21.24. dhcp-guard monitored-host-limit

Use this command to set the maximum monitored host number.

Use the **no** or **default** form of this command to restore the default setting.

dhcp-guard monitored-host-limit *number* **no dhcp-guard monitored-host-limit default dhcp-guard monitored-host-limit**

Parameter Description

Parameter	Description
number	The maximum monitored host number, in the range from 1 to 4,294,967,295.

Defaults
The default is 20,000.

Command Mode

NFPP configuration mode

Usage Guide

If the monitored host number has reached the default 20,000, the administrator shall set the max-number smaller than 20,000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20,000, please clear a part of monitored hosts to remind the administrator of the invalid configuration and removing the monitored hosts.
When the maximum monitored host number has been exceeded, it prompts the message that % NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts to remind the administrator.

Configuration Examples

The following example sets the maximum monitored host number to 200.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# dhcp-guard monitored-host-limit 200
```

Related Commands

Command	Description
show nfpp dhcp-guard summary	**Displays the configuration.**

Platform Description

N/A

21.25. dhcp-guard monitor-period

Use this command to configure the monitor time.

Use the **no** or **default** form of this command to restore the default setting.

dhcp-guard monitor-period *seconds* **no dhcp-guard monitor-period default dhcp-guard monitor-period**

Parameter Description

Parameter	Description
seconds	Sets the monitor time, in the range from 180 to 86,400 in the unit of seconds.

Defaults

The default is 600 seconds.

Command Mode

NFPP configuration mode

Usage Guide

When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.

If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

Configuration Examples

The following example sets the monitor time to 180 seconds.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# dhcp-guard monitor-period 180
```

Related Commands

Command	Description
show nfpp dhcp-guard summary	Displays the configuration.
show nfpp dhcp-guard hosts	Displays the monitored host list.
clear nfpp dhcp-guard hosts	Clears the isolated host.

Platform Description

N/A

21.26. dhcp-guard rate-limit

Use this command to set the rate-limit threshold globally.

Use the **no** or **default** form of this command to restore the default setting.

dhcp-guard rate-limit { **per-src-mac | per-port** } *pps*

no dhcp-guard rate-limit { **per-src-mac | per-port** }

default dhcp-guard rate-limit { **per-src-mac | per-port** }

Parameter Description

Parameter	Description
per-src-mac	Sets the rate limit for each source MAC address.
per-port	Sets the rate limit for each port.
pps	Sets the rate limit, in the range of 1 to 19,999.

Defaults

The default value varies with products. For details, see the *Configuration Guide*.

Command Mode

NFPP configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the rate-limit threshold globally.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# dhcp-guard rate-limit per-src-mac 8 QTECH(config-nfpp)# dhcp-guard rate-limit per-port 100
```

Related Commands

Command	Description
nfpp dhcp-guard policy	Sets the rate limit and the attack threshold.
show nfpp dhcp-guard summary	Displays the configuration.

Platform Description

N/A

21.27. dhcpv6-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.

Use the **no** or **default** form of this command to restore the default setting.

dhcpv6-guard attack-threshold { **per-src-mac** | **per-port** } *pps* **no dhcpv6-guard attack-threshold** {**per-src-mac** | **per-port**} **default dhcpv6-guard attack-threshold** { **per-src-mac** | **per-port**}

Parameter Description

Parameter	Description
per-src-mac	Sets the attack threshold for each source MAC address.
per-port	Sets the attack threshold for each port.
pps	Sets the attack threshold, in the range is from 1 to 19,999 pps.

Defaults

The default value varies with products. For details, see the *Configuration Guide*.

Command Mode

NFPP configuration mode

Usage Guide

N/A.

Configuration Examples

The following example sets the global attack threshold.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# dhcpv6-guard attack-threshold per-src-mac 15 QTECH(config-nfpp)# dhcpv6-guard attack-threshold per-port 200
```

Related Commands

Command	Description
nfpp dhcpv6-guard policy	Displays the rate-limit threshold and attack threshold.
show nfpp dhcpv6-guard summary	Displays the configuration.
show nfpp dhcpv6-guard hosts	Displays the monitored host list.
clear nfpp dhcpv6-guard hosts	Clears the monitored host.

Platform Description

N/A

21.28. dhcpv6-guard enable

Use this command to enable the DHCPv6 anti-attack function.

Use the **no** or **default** form of this command to restore the default setting.

dhcpv6-guard enable

no dhcpv6-guard enable

default dhcpv6-guard

enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

NFPP configuration mode

Usage Guide

N/A

Configuration Examples

The following example enables the DHCPv6 anti-attack function globally.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# dhcpv6-guard enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

21.29. dhcpv6-guard monitored-host-limit

Use this command to set the maximum monitored host number.

Use the **no** or **default** form of this command to restore the default setting.

dhcpv6-guard monitored-host-limit *number* **no dhcpv6-guard monitored-host-limit default dhcpv6-guard monitored-host-limit**

Parameter Description

Parameter	Description
number	The maximum monitored host number, in the range from 1 to 4,294,967,295.

Defaults
The default is 20,000.

Command Mode

NFPP configuration mode

Usage Guide

If the monitored host number has reached the default 20,000, the administrator shall set the max-number smaller than 20,000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20,000, please clear a part of monitored hosts to remind the administrator of the invalid configuration and removing the monitored hosts.
When the maximum monitored host number has been exceeded, it prompts the message that % NFPP_DHCPV6_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts to remind the administrator.

Configuration Examples

The following example sets the maximum monitored host number to 200.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# dhcpv6-guard monitored-host-limit 200
```

Related Commands

Command	Description
show nfpp dhcpv6-guard summary	Displays the configuration.

Platform Description

N/A

21.30. dhcpv6-guard monitor-period

Use this command to configure the monitor time.

Use the **no** or **default** form of this command to restore the default setting.

dhcpv6-guard monitor-period *seconds* **no dhcpv6-guard monitor-period default dhcpv6-guard monitor-period**

Parameter Description

Parameter	Description
seconds	Sets the monitor time, in the range from 180 to 86,400 in the unit of seconds.

Defaults

The default is 600 seconds.

Command Mode

NFPP configuration mode

Usage Guide

When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.

If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

Configuration Examples

The following example sets the monitor time to 180 seconds.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# dhcpv6-guard monitor-period 180
```

Related Commands

Command	Description
show nfpp dhcpv6-guard summary	Displays the configuration.
show nfpp dhcpv6-guard hosts	Displays the monitored host list.
`clear nfpp dhcpv6-guard hosts`	`Clears the isolated host.`

Platform Description

N/A

21.31. dhcpv6-guard rate-limit

Use this command to set the rate-limit threshold globally.

Use the **no** or **default** form of this command to restore the default setting.

dhcpv6-guard rate-limit { **per-src-mac** | **per-port** } *pps*

no dhcpv6-guard rate-limit { **per-src-mac** | **per-port** }

default dhcpv6-guard rate-limit { **per-src-mac** | **per-port** }

Parameter Description

Parameter	Description
per-src-mac	Sets the rate limit for each source MAC address.
per-port	Sets the rate limit for each port.
pps	Sets the rate limit, in the range from 1 to 19,999.

Defaults

The default value varies with products. For details, see the *Configuration Guide*.

Command Mode

NFPP configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the rate-limit threshold globally.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# dhcpv6-guard rate-limit per-src-mac 8 QTECH(config-nfpp)# dhcpv6-guard rate-limit per-port 100
```

Related Commands

Command	Description
nfpp dhcpv6-guard policy	Sets the rate limit and the attack threshold.
show nfpp dhcpv6-guard summary	Displays the configuration.

Platform Description

N/A

21.32. global-policy

Use this command to set the rate-limit threshold and attack threshold based on the host or port.

Parameter Description

Use the **no** or **default** form of this command to restore the default setting.

global-policy { **per-src-mac** | **per-src-ip** | **per-port** } *rate-limit-pps attack-threshold-pps*

no global-policy { **per-src-mac** | **per-src-ip** | **per-port** }

default global-policy **{** per-src-mac **|** per-src-ip **|** per-port **}**

Parameter	Description
per-src-ip	Performs the rate statistics based on the source IP / VID and port.
per-src-mac	Performs the rate statistics based on the source MAC / VID and port.
per-port	Performs the rate statistics based on each physical port of receiving the packets.
rate-limit-pps	Sets the rate-limit threshold.
attack-threshold-pps	Sets the attack threshold.

Defaults

By default, no rate-limit threshold and attack threshold is configured. To enable self-defined anti-attack, these two parameters must be set.

Command Mode

NFPP define configuration mode

Usage Guide

To create a user-defined anti-attack type, the classification rule for the rate statistics must be specified, that is, recognize the host based on the source IP address/ source MAC address for the user-defined packets rate statistics based on the user / port and specify the rate-limit threshold and attack threshold for each classification. The rate-limit threshold shall be equal to or greater than the attack threshold. If the rate is greater than the rate-limit threshold, the packets that meet this classification rule will be discarded. If the rate exceeds the attack threshold, the user will be regarded as an attacker. The log will be printed and the trap will be sent.

Configuration Examples

The following example sets the rate-limit threshold and attack threshold based on the host or port.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# nfpp define tcp
QTECH(config-nfpp-define)# global-policy per-src-ip 10 20
QTECH(config-nfpp-define)# global-policy per-port 100 200
```

Related Commands

Command	Description
nfpp define *name* **policy**	Sets the rate-limit threshold and attack threshold.
show nfpp define summary	Displays the user-defined anti-attack

	configuration

Platform Description

N/A

21.33. icmp-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.

Use the **no** or **default** form of this command to restore the default setting.

icmp-guard attack-threshold { **per-src-ip** | **per-port** } *pps*

no icmp-guard attack-threshold { **per-src-ip** | **per-port** }

default icmp-guard attack-threshold { **per-src-ip** | **per-port** }

Parameter Description

Parameter	Description
per-src-ip	Sets the attack threshold for each source IP address.
per-port	Sets the attack threshold for each port.
pps	Sets the attack threshold, in the range from 1 to 19,999 in the unit of pps.

Defaults

The default value varies with products. For details, see the *Configuration Guide*.

Command Mode

NFPP configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the global attack threshold.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# icmp-guard attack-threshold per-src-ip 600 QTECH(config-nfpp)# icmp-guard attack-threshold per-port 1200
```

Related Commands

Command	Description
nfpp icmp-guard policy	Displays the rate-limit threshold and attack threshold.
show nfpp icmp-guard summary	Displays the configuration.
show nfpp icmp-guard hosts	Displays the monitored host list.
clear nfpp icmp-guard hosts	Clears the monitored host.

Platform Description

N/A

21.34. icmp-guard enable

Use this command to enable the ICMP anti-attack function.

Parameter Description

Use the **no** or **default** form of this command to restore the default setting.

icmp-guard enable no

icmp-guard enable

default icmp-guard enable

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command Mode

NFPP configuration mode

Usage Guide

N/A

Configuration Examples

The following example enables the ICMP anti-attack function globally.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# icmp-guard enable
```

Related Commands

Command	Description
nfpp icmp-guard enable	Enables the ICMP anti-attack function on the interface.
show nfpp icmp-guard summary	Displays the configuration.

Platform Description

N/A

21.35. icmp-guard isolate-period

Use this command to set the isolate time globally.

Use the **no** or **default** form of this command to restore the default setting.

icmp-guard isolate-period { *seconds* | **permanent** }

no icmp-guard isolate-period

default icmp-guard isolate-

period

Parameter Description

Parameter	Description
seconds	Sets the isolate time. The value is in the range is 0 or from 30 to 86,400 in the unit of seconds.
permanent	Permanent isolation.

Defaults

The default isolate time is 0, which means no isolation.

Command Mode

NFPP configuration mode

Usage Guide

The isolate period can be configured globally or based on the interface. For one interface, if the isolate period is not set based on the interface, the global value shall be adopted; or the interface-based isolate period shall be adopted.

Configuration Examples

The following example sets the isolate time globally to 180 seconds.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# icmp-guard isolate-period 180
```

Related Commands

Command	Description
nfpp icmp-guard isolate-period	Sets the isolate time on the interface.
show nfpp icmp-guard summary	Displays the configuration.

Platform Description

N/A

21.36. icmp-guard monitored-host-limit

Use this command to set the maximum monitored host number.
Use the **no** or **default** form of this command to restore the default setting.

icmp-guard monitored-host-limit *number* **no icmp-guard monitored-host-limit default icmp-guard monitored-host-limit**

Parameter Description

Parameter	Description
number	The maximum monitored host number, in the range from 1 to 4,294,967,295.

Defaults

The default is 20,000.

Command Mode

NFPP configuration mode

Usage Guide

If the monitored host number has reached the default 20,000, the administrator shall set the max-number smaller than 20,000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20,000, please clear a part of monitored hosts to remind the administrator of the invalid configuration and removing the monitored hosts.

When the maximum monitored host number has been exceeded, it prompts the message that % NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20,000 monitored hosts to remind the administrator.

Configuration Examples

The following example sets the maximum monitored host number to 200.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# icmp-guard monitored-host-limit 200
```

Related Commands

Command	Description
show nfpp icmp-guard summary	Displays the configuration.

Platform Description

N/A

21.37. icmp-guard monitor-period

Use this command to configure the monitor time.

Use the **no** or **default** form of this command to restore the default setting.

icmp-guard monitor-period *seconds* **no icmp-guard monitor-period default icmp-guard monitor-period**

Parameter Description

Parameter	Description
seconds	Sets the monitor time, in the range from180 to 86,400 seconds.

Defaults

The default is 600.

Command Mode

NFPP configuration mode

Usage Guide

When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.

If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

Configuration Examples

The following example sets the monitor time to 180 seconds.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# icmp-guard monitor-period 180
```

Related Commands

Command	Description
show nfpp icmp-guard summary	Displays the configuration.
show nfpp icmp-guard hosts	Displays the monitored host list.
clear nfpp icmp-guard hosts	Clears the isolated host.

Platform Description

N/A

21.38. icmp-guard rate-limit

Use this command to set the rate-limit threshold globally.

Use the **no** or **default** form of this command to restore the default setting.

icmp-guard rate-limit { **per-src-ip** | **per-port** } *pps*

no icmp-guard rate-limit { **per-src-ip | per-port** }

default icmp-guard rate-limit { **per-src-ip | per-port** }

Parameter Description

Parameter	Description
per-src-ip	Sets the rate limit for each source IP address.
per-port	Sets the rate limit for each port.
pps	Sets the rate limit, in the range from1 to19,999.

Defaults

The default value varies with products. For details, see the *Configuration Guide*.

Command Mode

NFPP configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the rate-limit threshold globally.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# icmp-guard rate-limit per-src-ip 500 QTECH(config-nfpp)# icmp-guard rate-limit per-port 800
```

Related Commands

Command	Description
nfpp icmp-guard policy	Sets the rate limit and the attack threshold.
show nfpp icmp-guard summary	Displays the configuration.

Platform Description

N/A

21.39. icmp-guard trusted-host

Use this command to set the trusted hosts free form monitoring.

Use the **no** or **default** form of this command to restore the default setting.

icmp-guard trusted-host *ip mask*

no icmp-guard trusted-host { **all** | *ip mask* }

default icmp-guard trusted-host

Parameter Description

Parameter	Description
ip	Sets the IP address.
mask	Sets the IP mask.
all	Deletes the configuration of all trusted hosts.

Defaults

No trusted host is configured by default.

Command Mode

NFPP configuration mode

Usage Guide

The administrator can use this command to set the trusted host free from monitoring. The ICMP packets are allowed to send to the trusted host CPU without any rate-limit and warning configuration. Configure the mask to set all hosts in one network segment free from monitoring.

UP to 500 trusted hosts are supported.

Configuration Examples

The following example sets the trusted hosts free form monitoring.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# icmp-guard trusted-host 1.1.1.0 255.255.255.0
```

Related Commands

Command	Description
show nfpp icmp-guard trusted-host	Displays the configuration.

Platform Description

N/A

21.40. ip-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.

Use the **no** or **default** form of this command to restore the default setting.

ip-guard attack-threshold { **per-src-ip** | **per-port** } *pps*

no ip-guard attack-threshold { **per-src-ip** | **per-port** }

default ip-guard attack-threshold { **per-src-ip** | **per-port** }

Parameter Description

Parameter	Description
per-src-ip	Sets the attack threshold for each source IP address.
per-port	Sets the attack threshold for each port.
pps	Sets the attack threshold, in pps. The valid range is 1 to 19,999.

Defaults

The default value varies with products. For details, see the *Configuration Guide*.

Command Mode

NFPP configuration mode

Usage Guide

The attack threshold shall be equal to or larger than the rate-limit threshold.

Configuration Examples

The following example sets the global attack threshold.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# ip-guard attack-threshold per-src-ip 2 QTECH(config-nfpp)# ip-guard attack-threshold per-port 50
```

Related Commands

Command	Description
nfpp ip-guard policy	Displays the rate-limit threshold and attack threshold.
show nfpp ip-guard summary	Displays the configuration.
show nfpp ip-guard hosts	Displays the monitored host list.
clear nfpp ip-guard hosts	Clears the monitored host.

Platform Description

N/A

21.41. ip-guard enable

Use this command to enable IP guard.

Use the **no** or **default** form of this command to restore the default setting.

ip-guard enable

no ip-guard enable

default ip-guard enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command Mode

NFPP configuration mode.

Usage Guide

This configuration aims at attacks whose destination IP address is not the local one. For those with the local address as the destination, CPP (CPU Protect Policy) will limit their rates.

Configuration Examples

The following example enables the IP guard globally.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# ip-guard enable
```

Related Commands

Command	Description
nffp ip-guard enable	Enables the IP guard on the

	interface.

Platform Description

N/A

21.42. ip-guard isolate-period

Use this command to set the isolate time globally.

Use the **no** or **default** form of this command to restore the default setting.

ip-guard isolate-period { *seconds* | **permanent** }

no ip-guard isolate-period

default ip-guard isolate-

period

Parameter Description

Parameter	Description
seconds	Sets the isolate time. The value is 0 or in the range from 30 to 86，400 in the unit of seconds.
permanent	Permanent isolation

Defaults

The default isolate time is 0 second, which means no isolation.

Command Mode

NFPP configuration mode

Usage Guide

N/A.

Configuration Examples

The following example sets the isolate time globally to 180 seconds.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# ip-guard isolate-period 180
```

Related Commands

Command	Description
nfpp ip-guard isolate-period	Sets the isolate time on the interface.
show nfpp ip-guard summary	Displays the configuration.

Platform Description

N/A

21.43. ip-guard monitor-period

Use this command to configure the monitor time.

Use the **no** or **default** form of this command to restore the default setting.

ip-guard monitor-period *seconds* **no ip-guard monitor-period** **default ip-guard monitor-period**

Parameter Description

Parameter	Description
seconds	Sets the monitor time, in the range from 180 to 86,400 in the unit of seconds.

Defaults

The default is 600 seconds.

Command Mode

NFPP configuration mode

Usage Guide

When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored

attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.

If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software

Configuration Examples

The following example sets the monitor time to 180 seconds.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# ip-guard monitor-period 180
```

Related Commands

Command	Description
show nfpp ip-guard summary	Displays the configuration.
show nfpp ip-guard hosts	Displays the monitored host list.
clear nfpp ip-guard hosts	Clears the isolated host.

Platform Description

N/A

21.44. ip-guard monitored-host-limit

Use this command to set the maximum monitored host number.

Use the **no** or **default** form of this command to restore the default setting.

ip-guard monitored-host-limit *number* **no ip-guard monitored-host-limit default ip-guard monitored-host-limit**

Parameter Description

Parameter	Description

number	The maximum monitored host number, in the range from 1 to 4,294,967,295.

Defaults

The default is 20,000 seconds.

Command Mode

NFPP configuration mode

Usage Guide

If the monitored host number has reached the default 20,000, the administrator shall set the max-number smaller than 20,000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20,000, please clear a part of monitored hosts to remind the administrator of the invalid configuration and removing the monitored hosts.

When the maximum monitored host number has been exceeded, it prompts the message that % NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20,000 monitored hosts to remind the administrator.

Configuration Examples

The following example sets the maximum monitored host number to 200.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# ip-guard monitored-host-limit 200
```

Related Commands

Command	Description
show nfpp ip-guard summary	Displays the configuration.

Platform Description

N/A

21.45. ip-guard rate-limit

Use this command to set the rate-limit threshold globally.

Parameter Description

Use the **no** or **default** form of this command to restore the default setting.

ip-guard rate-limit { **per-src-ip** | **per-port** }

pps **no ip-guard rate-limit** { **per-src-ip |**

per-port } **default ip-guard rate-limit** {**per-**

src-ip | per-port }

Parameter	Description
per-src-ip	Sets the rate limit for each source IP address.
per-port	Sets the rate limit for each port.
pps	Sets the rate limit, in the range of 1 to 19,999.

Defaults

The default value varies with products. For details, see the *Configuration Guide*.

Command Mode

NFPP configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the rate-limit threshold globally.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# ip-guard rate-limit per-src-ip 2 QTECH(config-nfpp)# ip-guard rate-limit per-port 50
```

Related Commands

Command	Description
nfpp ip-guard policy	Sets the rate limit and the attack threshold.
show nfpp ip-guard summary	Displays the configuration.

Platform Description

N/A

21.46. ip-guard scan-threshold

Use this command to set the global scan threshold.

Use the **no** or **default** form of this command to restore the default setting.

ip-guard scan-threshold *pkt-cnt* **no ip-guard scan-threshold default ip-guard scan-threshold**

Parameter Description

Parameter	Description
pkt-cnt	Sets the scan threshold, in the range from 1 to 19,999.

Defaults

The default value varies with products. For details, see the *Configuration Guide*.

Command Mode

NFPP configuration mode.

Usage Guide

N/A

Configuration Examples

The following example sets the global scan threshold to 20 pps.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# ip-guard scan-threshold 20
```

Related Commands

Command	Description
nfpp ip-guard scan-threshold	Sets the scan threshold on the port.

show nfpp ip-guard summary	Displays the configuration.

Platform Description

N/A

21.47. ip-guard trusted-host

Use this command to set the trusted hosts free form monitoring.
Use the **no** or **default** form of this command to restore the default setting.

ip-guard trusted-host *ip mask*

no ip-guard trusted-host { **all** | *ip mask* }

default ip-guard trusted-host

Parameter Description

Parameter	Description
ip	Sets the IP address.
mask	Sets the IP mask.
all	Deletes the configuration of all trusted hosts.

Defaults

N/A

Command Mode

NFPP configuration mode

Usage Guide

The administrator can use this command to set the trusted host free f

rom monitoring. The ICMP packets are allowed to sent to the trusted host CPU without any rate-limit and warning configuration. Configure the mask to set all hosts in one network segment free from monitoring.

UP to 500 trusted hosts are supported.

Configuration Examples

The following example sets the trusted hosts free form monitoring.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# ip-guard trusted-host 1.1.1.0 255.255.255.0
```

Related Commands

Command	Description
show nfpp ip-guard trusted-host	Displays the configuration.

Platform Description

N/A

21.48. log-buffer enable

Use this command to display logs on the screen.

Use the **no** or the **default** form of this command to restore the default setting.

log-buffer enable

no log-buffer enable

default log-buffer enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

Logs are stored in the cache by default.

Command Mode

NFPP configuration mode

Usage Guide

N/A

Configuration Examples

The following example displays logs on the screen.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# log-buffer enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

21.49. log-buffer entries

Use this command to set the NFPP log buffer area size.

Use the **no** or **default** form of this command to restore the default setting.

log-buffer entries

number **no log-buffer**

entries default log-buffer

entries

Parameter Description

Parameter	Description
number	The buffer area size, in the range from 0 to 1,024.

Defaults

The default is 256.

Command Mode

NFPP configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the NFPP log buffer area size.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# log-buffer entries 50
```

Related Commands

Command	Description
log-buffer logs *number_of_message* **interval** *length_in_seconds*	Displays the rate of the syslog generated from the NFPP buffer area.
show nfpp log	Displays the NFPP log configuration or the log buffer area.

Platform Description

N/A

21.50. log-buffer logs

Use this command to set the rate of syslog generated from the NFPP log buffer area. Use the **no** or **default** form of this command to restore the default setting.

log-buffer logs *number_of_message* **interval** *length_in_seconds*

no log-buffer logs

default log-buffer logs

Parameter Description

Parameter	**Description**
number_of_message	The valid range is from 0 to1024. 0 indicates that all logs are recorded in the specific buffer area and no syslogs are generated.

length_in_seconds	The valid range is from 0 to 86400(one day). 0 indicates not to write the log to the buffer area but generate the syslog immediately. With both the *number_of_message* and *length_in_seconds* values are 0, it indicates not to write the log to the buffer area but generate the syslog immediately. The parameter *number_of_message /length_in_second* indicates the rate of syslog generated from the NFPP log buffer area.

Defaults

By default, *number_of_message* is 0 and *length_in_seconds* is 0.

Command Mode

NFPP configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the rate of syslog generated from the NFPP log buffer area.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# log-buffer logs 2 interval 12
```

Related Commands

Command	Description
log-buffer entries *number*	Sets the NFPP log buffer area size.
show nfpp log summary	Displays the NFPP log configuration or the log buffer area.

Platform Description

N/A

21.51. logging

Use this command to set the VLAN or the interface log for NFPP.

Use the **no** or **default** form of this command to restore the default setting.

logging vlan *vlan-range*

logging interface *interface-id* **no logging vlan** *vlan-range*

no logging interface *interface-id*

default logging

Parameter Description

Parameter	Description
vlan-range	Sets the specified VLAN range, in the format such as “1-3, 5”.
interface-id	Sets the interface ID.

Defaults

All logs are recorded by default.

Command Mode

NFPP configuration mode

Usage Guide

Use this command to filter the logs and records the logs within the specified VLAN range or the specified port

Configuration Examples

The following example records the logs in VLAN 1, VLAN 2,VLAN 3 and VLAN 5 only.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# logging vlan 1-3,5
```

```
QTECH(config)# nfpp
QTECH(config-nfpp)# logging interface G 0/1
```

The following example records the logs on the interface GigabitEthernet 0/1 only.

Related Commands

Command	Description
show nfpp log summary	Displays the NFPP log configuration or the log buffer area.

Platform Description

N/A

21.52. match

Use this command to specify the message matching filed for the user-defined anti-attack.

match [**etype** *type*] [**src-mac** *smac* [**src-mac-mask** *smac_mask*]] [**dst-mac** *dmac* [**dst-mac-mask** *dst_mask*]] [**protocol** *protocol*] [**src-ip** *sip* [**src-ip-mask** *sip-mask*]] [**src-ipv6** *sipv6* [**src-ipv6-masklen** *sipv6-masklen*]] [**dst-ip** *dip* [**dst-ip-mask** *dip-mask*]] [**dst-ipv6** *dipv6* [**dst-ipv6-masklen** *dipv6-masklen*]] [**src-port** *sport*] [**dst-port** *dport*]

Parameter Description

Parameter	**Description**
type	Ethernet link layer packet type
smac	Source MAC address
smac_mask	Source MAC address mask
dmac	Destination MAC address
dmac_mask	Destination MAC address mask
protocol	IPv4/v6 message protocol
sip	Source IPv4 address
sip_mask	Source IPv4 address mask

sipv6	Source IPv6 address
sipv6_masklen	Source IPv6 address mask
dip	Destination IPv4 address
dip_mask	Destination IPv4 address mask
dipv6	Destination IPv6 address
dipv6_masklen	Length of the destination IPv6 address mask.
sport	Source port
dport	Destination port

Defaults

N/A

Command Mode

NFPP configuration mode

Usage Guide

Use this command to create a new user-defined anti-attack type and specify the message fields to be matched.

Configuration Examples

The following example specifies the message matching filed for the user-defined anti-attack.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# nfpp define tcp
QTECH(config-nfpp-define)#match etype 0x0800 protocol 0x06
```

Related Commands

Command	Description
show nfpp define summary	Displays the user-defined anti-attack configuration

Platform Description

N/A

21.53. monitored-host-limit

Use this command to set the maximum monitored host number.

Use the **no** or **default** form of this command to restore the default setting.

monitored-host-limit

number **no monitored-host-**

limit default monitored-

host-limit

Parameter Description

Parameter	Description
number	The maximum monitored host number, in the range from 1 to
	4,294,967,295.

Defaults

The default is 20,000.

Command Mode

NFPP define configuration mode

Usage Guide

If the monitored host number has reached the default 20,000, the administrator shall set the max-number smaller than 20,000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20,000, please clear a part of monitored hosts to remind the administrator of the invalid configuration and removing the monitored hosts.

When the maximum monitored host number has been exceeded, it prompts the message that % % NFPP_DEFINE-4-SESSION_LIMIT: Attempt to exceed limit of name's 20,000 monitored hosts. to remind the administrator

Configuration Examples

The following example sets the maximum monitored host number.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# nfpp define tcp
QTECH(config-nfpp-define)#monitored-host-limit 500
```

Related Commands

Command	Description
show nfpp define summary	Displays the user-defined anti-attack configuration

Platform Description

N/A

21.54. monitor period

Use this command to set the monitoring time.

Use the **no** or **default** form of this command to restore the default setting.

monitor-period *seconds*

no monitor-period

default monitor-period

Parameter Description

Parameter	Description
seconds	Sets the monitor time, in the range from180 to 86,400 in the unit of seconds.

Defaults

The default is 600 seconds.

Command

NFPP define configuration mode

Mode

Usage Guide

When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.

If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

Configuration Examples

The following example sets the monitoring time to 1,000 seconds.

```
QTECH(config)# nfpp QTECH(config-nfpp)# define tcp
QTECH(config-nfpp-define)#monitor-period 1000
```

Related Commands

Command	Description
show nfpp define summary	Displays the user-defined anti-attack configuration.

Platform Description

N/A

21.55. nd-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.

Use the **no** or **default** form of this command to restore the default setting.

nd-guard attack-threshold per-port { **ns-na** | **rs** | **ra-redirect** } *pps*

no nd-guard attack-threshold per-port { **ns-na** | **rs** | **ra-redirect** }

default nd-guard attack-threshold per-port { **ns-na** | **rs** | **ra-redirect** }

Parameter Description

Parameter	Description
ns-na	Sets the neighbor request and neighbor

	advertisement.
rs	Sets the router request.
ra-redirect	Sets the router advertisement and the redirect packets.
pps	Sets the attack threshold, in the range from1 to 19999 in the unit of seconds.

Defaults

The default value varies with products. For details, see the *Configuration Guide*.

Command Mode

NFPP configuration mode.

Usage Guide

The attack threshold shall be equal to or larger than the rate-limit threshold.

Configuration Examples

The following example sets the global attack threshold.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# nd-guard attack-threshold per-port ns-na 20 QTECH(config-nfpp)# nd-guard attack-threshold per-port rs 10 QTECH(config-nfpp)# nd-guard attack-threshold per-port ra-redirect 10
```

Related Commands

Command	Description
nfpp ip-guard policy	Displays the rate-limit threshold and attack threshold.
show nfpp ip-guard summary	Displays the configuration.

Platform Description

N/A

21.56. nd-guard enable

Use this command to enable the ND anti-attack function.

Use the **no** or **default** form of this command to restore the default setting.

nd-guard enable

no nd-guard enable

default nd-guard enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is enabled by default.

Command Mode

NFPP configuration mode

Usage Guide

N/A

Configuration Examples

The following example enables the ND anti-attack function.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# nd-guard enable
```

Related Commands

Command	Description
nffp nd-guard enable	Enables the ND anti-attack function on the interface.

show nfpp nd-guard summary	Displays the configuration.

Platform Description

N/A

21.57. nd-guard rate-limit

Use this command to set the rate-limit threshold globally.

Use the **no** or **default** form of this command to restore the default setting.

nd-guard rate-limit per-port { **ns-na** | **rs** | **ra-redirect** } *pps*

no nd-guard rate-limit per-port { **ns-na** | **rs** | **ra-redirect** }

default nd-guard rate-limit per-port { **ns-na** | **rs** | **ra-redirect** }

Parameter Description

Parameter	Description
ns-na	Sets the neighbor request and neighbor advertisement.
rs	Sets the router request.
ra-redirect	Sets the router advertisement and the redirect packets.
pps	Sets the attack threshold, in the range is from 1 to 19,999 in the unit of pps.

Defaults

The default value varies with products. For details, see the *Configuration Guide*.

Command Mode

NFPP configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the rate-limit threshold globally.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# nd-guard rate-limit per-port ns-na 10
```

```
QTECH(config-nfpp)# nd-guard rate-limit per-port rs 5 QTECH(config-nfpp)# nd-guard rate-limit per-port ra-redirect 5
```

Related Commands

Command	Description
nfpp nd-guard policy	Sets the rate limit and the attack threshold.
show nfpp nd-guard summary	Displays the configuration.

Platform Description

N/A

21.58. nd-guard ratelimit-forwarding enable

Use this command to enable the ND-guard ratelimit-forwarding on the interface.

nd-guard ratelimit-forwarding enable

Use this command to disable the ND-guard ratelimit-forwarding on the interface.

no nd-guard ratelimit-forwarding enable

Use this command to restore the default setting.

default nd-guard ratelimit-forwarding enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The function is enabled by default.

Command Mode

NFPP configuration mode

Usage Guide

N/A

Configuration Examples

The following example enables the ND-guard ratelimit-forwarding on the interface.

```
QTECH(config)# nfpp
QTECH(config-nfpp)# nd-guard ratelimit-forwarding enable
```

Platform Description

N/A

21.59. nfpp

Parameter Description

Use this command to enter NFPP configuration mode.

nfpp

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Global configuration mode

Usage Guide

Use this command to enter NFPP configuration mode and make further configuration.

Configuration Examples

The following example enters NFPP configuration mode.

```
QTECH(config)# nfpp
```

Platform Description

N/A

21.60. nfpp arp-guard enable

Use this command to enable the anti-ARP attack function on

the interface. Use the **no** or **default** form of this command to restore the default setting. **nfpp arp-guard enable**

no nfpp arp-guard enable

default nfpp arp-guard enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The anti-ARP attack function is not enabled on the interface.

Command Mode

Interface configuration mode

Usage Guide

The interface anti-ARP attack configuration is prior to the global configuration.

Configuration Examples

The following example enables the anti-ARP attack function on the interface.

```
QTECH(config)# interface G0/1
QTECH(config-if)# nfpp arp-guard enable
```

Related Commands

Command	Description
arp-guard enable	Enables the anti-ARP attack function.
show nfpp arp-guard summary	Displays the configuration.

Platform Description

N/A

21.61. nfpp arp-guard isolate-period

Use this command to set the isolate period in the interface configuration mode. Use the **no** or **default** form of this command to restore the default setting.

Parameter Description

nfpp arp-guard isolate-period { *seconds* | **permanent** }
no nfpp arp-guard isolate-period
default nfpp arp-guard isolate-period

Parameter	Description
seconds	Sets the isolate period. The value is 0, or in the range from 30 to 86,400 in the unit of seconds.
permanent	Permanent isolation

Defaults

By default, the isolate period is not configured.

Command Mode

Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the isolate period in the interface configuration mode.

```
QTECH(config)# interface G0/1
QTECH(config-if)# nfpp arp-guard isolate-period 180
```

Related Commands

Command	Description

arp-guard isolate-period	Sets the global isolate period.
show nfpp arp-guard summary	Displays the configuration.

Platform Description

N/A

21.62. nfpp arp-guard policy

Use this command to set the rate-limit threshold and the attack threshold. Use the **no** or **default** form of this command to restore the default setting.

nfpp arp-guard policy { **per-src-ip** | **per-src-mac** | **per-port** } *rate-limit-pps attack-threshold-pps*

no nfpp arp-guard policy { **per-src-ip** | **per-src-mac** | **per-port** }

default nfpp arp-guard policy { **per-src-ip** | **per-src-mac** | **per-port** }

Parameter Description

Parameter	Description
per-src-ip	Sets the rate-limit threshold and the attack threshold for each source IP address.
per-src-mac	Sets the rate-limit threshold and the attack threshold for each source MAC address.
per-port	Sets the rate-limit threshold and the attack threshold for each port.
rate-limit-pps	Sets the rate-limit threshold, in the range from 1 to 19999.
attack-threshold-pps	Sets the attack threshold, in the range from1 to 19999.

Defaults

By default, the rate-limit threshold and the attack threshold are not configured.

Command Mode

Interface configuration mode

Usage Guide

The attack threshold value shall be equal to or greater than the rate-limit threshold.

Configuration Examples

The following example sets the rate-limit threshold and the attack threshold.

```
QTECH(config)# interface G 0/1
QTECH(config-if)# nfpp arp-guard policy per-src-ip 2 10 QTECH(config-if)# nfpp arp-guard policy per-src-mac 3 10 QTECH(config-if)# nfpp arp-guard policy per-port 50 100
```

Related Commands

Command	Description
arp-guard attack-threshold	Sets the global attack threshold.
arp-guard rate-limit	Sets the global rate-limit threshold.
show nfpp arp-guard summary	Displays the configuration.
show nfpp arp-guard hosts	Displays the monitored host.
clear nfpp arp-guard hosts	Clears the isolated host.

Platform Description

N/A

21.63. nfpp arp-guard scan-threshold

Use this command to set the scan threshold.

Use the **no** or **default** form of this command to restore the default setting.

nfpp arp-guard scan-threshold *pkt-cnt* **no nfpp arp-guard scan-threshold default nfpp arp-guard scan-threshold**

Parameter Description

Parameter	Description

pkt-cnt	Sets the scan threshold, in the range from1 to 19,999.

Defaults
By default, the sport-based scan threshold is not configured.

Command I
nterface configuration mode

Mode

Usage Guide
N/A

Configuration Examples

The following example sets the scan threshold to 20 pps.

```
QTECH(config)# interface G 0/1
QTECH(config-if)# nfpp arp-guard scan-threshold 20
```

Related Commands

Command	Description
arp-guard attack-threshold	Sets the global attack threshold.
show nfpp arp-guard summary	Displays the configuration.
show nfpp arp-guard scan	Displays the ARP scan table.
clear nfpp arp-guard scan	Clears the ARP scan table.

Platform Description

N/A

21.64. nfpp define *name* enable

Use this command to enable the user-defined anti-attack function on the interface. Use the **no** or **default** form of this command to restore the default setting.
nfpp define *name* **enable**

no nfpp define *name* **enable**

default nfpp define *name*

enable

Parameter Description

Parameter	Description
name	Name of the user-defined anti-attack type

Defaults

N/A

Command Mode

Interface configuration mode.

Usage Guide

This command takes effect only after the name of the user-defined anti-attack and the match, rate-count, rate-limit and the attack-threshold have been configured.

Configuration Examples

The following example enables the user-defined anti-attack function on the interface.

```
QTECH(config)# interface G0/1
QTECH(config-if)# nfpp define tcp enable
```

Related Commands

Command	Description
show nfpp define summary	Displays the user-defined anti-attack configuration.

Platform Description

N/A

21.65. nfpp define policy

Use this command to set the local rate-limit threshold and the attack threshold. Use the **no** or **default** form of this command to restore the default setting.

nfpp define *name* **policy** { **per-src-ip** | **per-src-mac** | **per-port** } *rate-limit-pps attack-threshold-pps*

no nfpp define *name* **policy** {**per-src-ip | per-src-mac** | **per-port**} **default nfpp define** *name* **policy** { **per-src-ip** | **per-src-mac** | **per-port** }

Parameter Description

Parameter	Description
per-src-ip	Sets the attack threshold for each source IP address.
per-src-mac	Sets the attack threshold for each source MAC address.
per-port	Sets the attack threshold for each port.
rate-limit-pps	Sets the rate-limit threshold, in the range from 1 to 19,999.
attack-threshold-pps	Sets the attack threshold, in the range of from1 to 19,999.

Defaults

By default, the rate-limit threshold and the attack threshold are not configured.

Command Mode

Interface configuration mode

Usage Guide

The attack threshold value shall be equal to or greater than the rate-limit threshold.

Configuration Examples

The following example sets the local rate-limit threshold and the attack threshold.

```
QTECH(config)# interface G 0/1
QTECH(config-if)# nfpp define tcp policy per-src-ip 2 10 QTECH(config-if)# nfpp define tcp
```

```
policy per-port 50 100
```

Related Commands

Command	Description
define-policy	Sets the global rate-limit threshold and attack threshold.
show nfpp define summary	Displays the user-defined anti-attack configuration.

Platform Description

N/A

21.66. nfpp dhcp-guard enable

Use this command to enable the DHCP anti-attack function on the interface. Use the **no** or **default** form of this command to restore the default setting. **nfpp dhcp-guard enable**
no nfpp dhcp-guard enable
default nfpp dhcp-guard
enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults
The DHCP anti-attack function is not enabled on the interface.

Command Mode

Interface configuration mode

Usage Guide

The interface DHCP anti- attack configuration is prior to the global configuratio

Configuration Examples

The following example enables the DHCP anti-attack function on the interface.

```
QTECH(config)# interface G0/1
QTECH(config-if)# nfpp dhcp-guard enable
```

Related Commands

Command	Description
dhcp-guard enable	Enables the anti-ARP attack function.
show nfpp dhcp-guard summary	Displays the configuration.

Platform Description

N/A

21.67. nfpp dhcp-guard policy

Use this command to set the rate-limit threshold and the attack threshold on the port. Use the **no** or **default** form of this command to restore the default setting.

nfpp dhcp-guard policy { **per-src-mac** | **per-port** } *rate-limit-pps attack-threshold-pps*

no nfpp dhcp-guard policy { **per-src-mac** | **per-port** }

default nfpp dhcp-guard policy { **per-src-mac** | **per-port** }

Parameter Description

Parameter	Description
per-src-mac	Sets the rate-limit threshold and the attack threshold for the designated source MAC address.
per-port	Sets the rate-limit threshold and the attack threshold for the designated port.

rate-limit-pps	Sets the rate-limit threshold, in the range from1 to 19,999.
attack-threshold-pps	Sets the attack threshold, in the range from1 to 19,999.

Defaults

The rate-limit threshold and the attack threshold are not configured by default. So the device adopts the rate-limit threshold and the attack threshold that are set in the global configuration mode.

Command Mode

Interface configuration mode

Usage Guide

The attack threshold value shall be equal to or greater than the rate-limit threshold.

Configuration Examples

The following example sets the rate-limit threshold and the attack threshold on interface G0/1.

```
QTECH(config)#interface G 0/1
QTECH(config-if)# nfpp dhcpv6-guard policy per-src-mac 3 10 QTECH(config-if)# nfpp dhcpv6-guard policy per-port 50 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

21.68. nfpp dhcpv6-guard enable

Use this command to enable the DHCPv6 anti-attack function on the interface. Use the **no** or **default** form of this command to restore the default setting. **nfpp dhcpv6-guard enable**

no nfpp dhcpv6-guard enable

default nfpp dhcpv6-guard

enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The DHCPv6 anti-attack function is not enabled on the interface.

Command Mode

Interface configuration mode

Usage Guide

The interface DHCPv6 anti- attack configuration is prior to the global configuration.

Configuration Examples

The following example enables the DHCPv6 anti-attack function on interface G0/1.

```
QTECH(config)# interface G0/1
QTECH(config-if)# nfpp dhcpv6-guard enable
```

Related Commands

Command	Description
dhcpv6-guard enable	Enables the anti-ARP attack function.
show nfpp dhcpv6-guard summary	Displays the configuration.

Platform Description

N/A

21.69. nfpp dhcpv6-guard policy

Use this command to set the rate-limit threshold and the

attack threshold. Use the **no** or **default** form of this command

to restore the default setting.

nfpp dhcpv6-guard policy { **per-src-mac** | **per-port** } *rate-limit-pps attack-threshold-pps*

no nfpp dhcpv6-guard policy { **per-src-mac** | **per-port**} **default nfpp dhcpv6-guard policy** { **per-src-mac** | **per-port**}

Parameter Description

Parameter	Description
per-src-mac	Sets the rate-limit threshold and the attack threshold for each source MAC address.
per-port	Sets the rate-limit threshold and the attack threshold for each port.
rate-limit-pps	Sets the rate-limit threshold, in the range of from1 to 19,999.
attack-threshold-pps	Sets the attack threshold, in the range from1 to19,999.

Defaults

By default, the rate-limit threshold and the attack threshold are not configured.

Command Mode

Interface configuration mode

Usage Guide

The attack threshold value shall be equal to or greater than the rate-limit threshold.

Configuration Examples

The following example sets the rate-limit threshold and the attack threshold.

```
QTECH(config)# interface G 0/1
QTECH(config-if)# nfpp dhcpv6-guard policy per-src-mac 3 10 QTECH(config-if)# nfpp dhcpv6-guard policy per-port 50 100
```

Related Commands

Command	Description

dhcpv6-guard attack-threshold	Sets the global attack threshold.
dhcpv6-guard rate-limit	Sets the global rate-limit threshold.
show nfpp dhcpv6-guard summary	Displays the configuration.
show nfpp dhcpv6-guard hosts	Displays the monitored host.
clear nfpp dhcpv6-guard hosts	Clears the isolated host.

Platform Description

N/A

21.70. nfpp icmp-guard enable

Use this command to enable the ICMP anti-attack function on the interface. Use the **no** or **default** form of this command to restore the default setting. **nfpp icmp-guard enable**

no nfpp icmp-guard enable

default nfpp icmp-guard enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The ICMP anti-attack function is not enabled on the interface.

Command Mode

Interface configuration mode

Usage Guide

The interface ICMP anti- attack configuration is prior to the global configuration.

Configuration Examples

The following example enables the ICMP anti-attack function on the interface.

```
QTECH(config)# interface G0/1
```

```
QTECH(config-if)# nfpp icmp-guard enable
```

Related Commands

Command	Description
icmp-guard enable	Enables the anti-ARP attack function.
show nfpp icmp-guard summary	Displays the configuration.

Platform Description

N/A

21.71. nfpp icmp-guard isolate-period

Use this command to set the isolate period in the interface configuration mode. Use the **no** or **default** form of this command to restore the default setting.

Parameter Description

nfpp icmp-guard isolate-period { *seconds* | **permanent** }
no nfpp icmp-guard isolate-period
default nfpp icmp-guard isolate-period

Parameter	Description
seconds	Sets the isolate period. The value is 0 or in the range from 30 to 86,400 in the unit of seconds.
permanent	Permanent isolation

Defaults

By default, the isolate period is not configured.

Command Mode

Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the isolate period in the interface configuration mode.

```
QTECH(config)# interface G0/1
QTECH(config-if)# nfpp icmp-guard isolate-period 180
```

Related Commands

Command	Description
icmp-guard isolate-period	Sets the global isolate period.
show nfpp icmp-guard summary	Displays the configuration.

Platform Description

N/A

21.72. nfpp icmp-guard policy

Use this command to set the rate-limit threshold and the attack threshold. Use the **no** or **default** form of this command to restore the default setting.

nfpp icmp-guard policy { p**er-src-ip** | **per-port** } *rate-limit-pps attack-threshold-pps*

no nfpp icmp-guard policy { **per-src-ip** | **per-port** }

default nfpp icmp-guard policy { **per-src-ip** | **per-port** }

Parameter Description

Parameter	Description
per-src-ip	Sets the rate-limit threshold and the attack threshold for each source IP address.
per-port	Sets the rate-limit threshold and the attack

	threshold for each port.
rate-limit-pps	Sets the rate-limit threshold, in the range from1 to 19,999.
attack-threshold-pps	Sets the attack threshold, in range from1 to 19,999.

Defaults

By default, the rate-limit threshold and the attack threshold are not configured.

Command Mode

Interface configuration mode

Usage Guide

The attack threshold value shall be equal to or greater than the rate-limit threshold.

Configuration Examples

The following example sets the rate-limit threshold and the attack threshold.

```
QTECH(config)# interface G 0/1
QTECH(config-if)# nfpp icmp-guard policy per-src-ip 5 10 QTECH(config-if)# nfpp icmp-guard policy per-port 100 200
```

Related Commands

Command	Description
icmp-guard attack-threshold	Sets the global attack threshold.
icmp-guard rate-limit	Sets the global rate-limit threshold.
show nfpp icmp-guard summary	Displays the configuration.
show nfpp icmp-guard hosts	Displays the monitored host.
clear nfpp icmp-guard hosts	Clears the isolated host.

Platform Description

N/A

21.73. nfpp ip-guard enable

Use this command to enable the IP anti-attack function on the interface. Use the **no** or **default** form of this command to restore the default setting. **nfpp ip-guard enable**

no nfpp ip-guard enable

default nfpp ip-guard

enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The IP anti-attack function is disabled on the interface.

Command Mode

Interface configuration mode

Usage Guide

The interface IP anti-attack configuration is prior to the global configuration.

```
QTECH(config)# interface G0/1
QTECH(config-if)# nfpp ip-guard enable
```

Configuration Examples

The following example enables the IP anti-attack function on the interface.

Related Commands

Command	Description
ip-guard enable	Enables the anti-ARP attack function.
show nfpp ip-guard summary	Displays the configuration.

Platform Description

N/A

21.74. nfpp ip-guard isolate-period

Use this command to set the isolate period in the interface configuration mode. Use the **no** or **default** form of this command to restore the default setting. **nfpp ip-guard isolate-period** { *seconds* | **permanent** }

no nfpp ip-guard isolate-period

default nfpp ip-guard isolate-period

Parameter Description

Parameter	Description
seconds	Sets the isolate period, in the range from 30 to 86,400 in the unit of seconds.
permanent	Permanent isolation

Defaults

By default, the isolate period is not configured.

Command Mode

Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the isolate period in the interface configuration mode.

```
QTECH(config)# interface G0/1
QTECH(config-if)# nfpp ip-guard isolate-period 180
```

Related Commands

Command	Description
ip-guard isolate-period	Sets the global isolate period.
show nfpp ip-guard summary	Displays the configuration.

Platform Description

N/A

21.75. nfpp ip-guard policy

Use this command to set the rate-limit threshold and the attack threshold. Use the **no** or **default** form of this command to restore the default setting.

nfpp ip-guard policy { **per-src-ip** | **per-port** } *rate-limit-pps attack-threshold-pps*

no nfpp ip-guard policy { **per-src-ip** | **per-port** }

default nfpp ip-guard policy { **per-src-ip** | **per-port** }

Parameter Description

Parameter	Description
per-src-ip	Sets the rate-limit threshold and the attack threshold for each source IP address.
per-port	Sets the rate-limit threshold and the attack threshold for each port.
rate-limit-pps	Sets the rate-limit threshold, in the range from 1 to 19,999.
attack-threshold-pps	Sets the attack threshold, in the range from 1 to 19,999.

Defaults

By default, the rate-limit threshold and the attack threshold are not configured.

Command Mode

Interface configuration mode

Usage Guide

The attack threshold value shall be equal to or greater than the rate-limit threshold.

Configuration Examples

The following example sets the rate-limit threshold and the attack threshold.

```
QTECH(config)# interface G 0/1
QTECH(config-if)# nfpp ip-guard policy per-src-ip 2 10 QTECH(config-if)# nfpp ip-guard policy per-port 50 100
```

Related Commands

Command	Description
ip-guard attack-threshold	Sets the global attack threshold.
ip-guard rate-limit	Sets the global rate-limit threshold.
show nfpp ip-guard summary	Displays the configuration.
show nfpp ip-guard hosts	Displays the monitored host.
clear nfpp ip-guard hosts	Clears the isolated host.

Platform Description

N/A

21.76. nfpp ip-guard scan-threshold

Use this command to set the scan threshold.

Use the **no** or **default** form of this command to restore the default setting.

nfpp ip-guard scan-threshold *pkt-cnt* **no nfpp ip-guard scan-threshold default nfpp ip-guard scan-threshold**

Parameter Description

Parameter	Description
pkt-cnt	Sets the scan threshold, in the range from 1 to

	19,999.

Defaults

By default, the sport-based scan threshold is not configured.

Command Mode

Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the scan threshold to 20pps.

```
QTECH(config)# interface G 0/1
QTECH(config-if)# nfpp ip-guard scan-threshold 20
```

Related Commands

Command	Description
ip-guard attack-threshold	Sets the global attack threshold.
show nfpp ip-guard summary	Displays the configuration.

Platform Description

N/A

21.77. nfpp nd-guard enable

Use this command to enable the ND anti-attack function on the interface. Use the **no** or **default** form of this command to restore the default setting. **nfpp nd-guard enable**

no nfpp nd-guard enable

default nfpp nd-guard

enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The ND anti-attack function is disabled on the interface.

Command Mode

Interface configuration mode

Usage Guide

The interface ND anti-attack configuration is prior to the global configuration.

```
QTECH(config)# interface G0/1
QTECH(config-if)# nfpp nd-guard enable
```

Configuration Examples

The following example enables the ND anti-attack function on the interface.

Related Commands

Command	Description
nd-guard enable	Enables the ND anti-attack function.
show nfpp nd-guard summary	Displays the configuration.

Platform Description

N/A

21.78. nfpp nd-guard policy

Use this command to set the rate-limit threshold and the attack threshold. Use the **no** or **default** form of this command to restore the default setting.

nfpp nd-guard policy per-port { **ns-na** | **rs** | **ra-redirect** } *rate-limit-pps attack-threshold-pps*

no nfpp nd-guard policy per-port { **ns-na** | **rs** | **ra-redirect** }

default nfpp nd-guard policy per-port { **ns-na** | **rs** | **ra-redirect** }

Parameter Description

Parameter	Description
ns-na	Sets the neighbor request and neighbor advertisement.
rs	Sets the router request.
ra-redirect	Sets the router advertisement and the redirect packets.
rate-limit-pps	Sets the rate-limit threshold, in the range from 1 to 19,999.
attack-threshold-pps	Sets the attack threshold, in the range from 1 to 19,999.

Defaults

By default, the rate-limit threshold and the attack threshold are not configured.

Command Mode

Interface configuration mode

Usage Guide

The attack threshold value shall be equal to or greater than the rate-limit threshold.

Configuration

The following example sets the rate-limit threshold and the attack threshold.

Examples

```
QTECH(config)# interface G 0/1
QTECH(config-if)# nfpp nd-guard policy per-port ns-na 50 100 QTECH(config-if)# nfpp nd-guard policy per-port rs 10 20 QTECH(config-if)# nfpp nd-guard policy per-port ra-redirect 10 20
```

Related Commands

Command	Description
nd-guard attack-threshold	Sets the global attack threshold.
nd-guard rate-limit	Sets the global rate-limit threshold.

show nfpp nd-guard summary	Displays the configuration.

Platform Description

N/A

21.79. show nfpp arp-guard hosts

Use this command to display the monitored host.

show nfpp arp-guard hosts [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*] [*ip-address* | *mac-address*]]]

Parameter Description

Parameter	Description
statistics	Displays the statistical information of the monitored host.
vid	The VLAN ID
interface-id	The interface name
ip-address	The IP address
mac-address	The MAC address

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the statistical information of the monitored host.

```
QTECH# success   show nfpp fail   arp-guard total   hosts   statistics


100             20              120
```

The following example shows the monitored host.

```
QTECH# show nfpp arp-guard hosts
If column 1 shows '*', it means "hardware do not isolate user" .

VLAN   interface   IP          MAC address   remain-time(s)
                   address

1      Gi0/1       1.1.1.1     -               110
2      Gi0/2       1.1.2.1     -               61
*3     Gi0/3       -           0000.0000.1111  110
4      Gi0/4       -           0000.0000.2222  61
Total:4 hosts
```

Related Commands

Command	Description
clear nfpp arp-guard hosts	Clears the monitored hosts.

Platform Description

N/A

21.80. show nfpp arp-guard scan

Use this command to display the ARP scan list.

show nfpp arp-guard scan [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*] [*ip-address*] [*mac-address*]]]

Parameter Description

Parameter	Description
statistics	Displays the statistical information of the ARP scan list.
vid	The VLAN ID
interface-id	The interface name
ip-address	The IP address
mac-address	The MAC address

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the ARP scan list.

```
QTECH# show nfpp arp-guard scan statistics
arp-guard table has 4 record(s).
QTECH# show nfpp arp-guard scan
VLAN   interface    IP address    MAC address   timestamp
```

The following example displays the ARP scan list.

```
1    Gi0/1       -           0000.0000.0001    2008-01-23 16:23:10
2    Gi0/2       1.1.1.1     0000.0000.0002    2008-01-23 16:24:10
3    Gi0/3       -           0000.0000.0003    2008-01-    16:25:10
                                               23
4    Gi0/4       -           0000.0000.0004    2008-01-    16:26:10
                                               23
Total:4 record(s)
```

Related Commands

Platform Description

The following example displays the ARP scan list.

```
QTECH# show nfpp arp-guard scan vlan 1 interface G 0/1 0000.0000.0001
VLAN   interface    IP address    MAC address   timestamp



1      Gi0/1       -      0000.0000.0001       2008-01-23 16:23:10
Total:1
record(s)
```

Command	Description

arp-guard scan-threshold	Sets the global scan threshold.
nfpp arp-guard scan-threshold	Sets the scan threshold.
clear nfpp arp-guard scan	Clears the ARP scan list.

N/A

21.81. show nfpp arp-guard summary

Use this command to display the configuration.

show nfpp arp-guard summary

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the configuration.

```
QTECH# show nfpp arp-guard summary
(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface Status Isolate-period Rate-limit Attack-threshold Scan-threshold
Global Enable  300   4/5/60 8/10/100     15

Gi 0/1    Enable  180               5/-/-    8/-/-         -
Gi 0/2    Disable 200               4/5/60   8/10/100      20

Maximum   count        of
Monitor   monitored          hosts:   1000
          period:300s
```

Field	Description

Interface(Global)	Global configuration
Status	Enables/Disables the anti-attack function.
Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port
Attack-threshold	In the same format as the rate-limit.
Scan-threshold	Scan threshold

Related Commands

Command	Description
arp-guard attack-threshold	Sets the global attack threshold.
arp-guard enable	Enables the anti-ARP attack function.
arp-guard isolate-period	Sets the global isolate time.
arp-guard monitor-period	Sets the monitor period.
arp-guard monitored-host-limit	Sets the maximum number of the monitored hosts.
arp-guard rate-limit	Sets the global rate-limit threshold.
arp-guard scan-threshold	Sets the global scan threshold.
nfpp arp-guard enable	Enables the anti-ARP attack function on the interface.
nfpp arp-guard isolate-period	Sets the isolate time.
nfpp arp-guard policy	Sets the rate-limit threshold and attack threshold.
nfpp arp-guard scan-threshold	Sets the scan threshold.

Platform Description

N/A

21.82. show nfpp define hosts

Use this command to display the monitored hosts.

show nfpp define hosts *name* [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*] [*ip-address*] [*mac-address*] [*ipv6-address*]]]

Parameter Description

Parameter	Description
name	**Name of the user-defined anti-attack type**
statistics	**Displays the statistics of monitored hosts.**
vid	**VLAN ID**
interface-id	**Interface name**
ip-address	**IP address**
mac-address	**MAC address**
ipv6-address	**IPv6 address**

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

This command allows filtering the hosts with parameters specified

Configuration Examples

The following example displays the monitored hosts.

```
QTECH#show nfpp define hosts abc
If col_filter 1 shows '*', it means "hardware do not isolate host". VLAN interface    MAC address      remain-time(s)
1   Gi4/2       00d0.f822.33e5  592
Total: 1 host
```

Related Commands

Command	Description
clear nfpp define hosts	Clears the monitored hosts of user-defined anti-attack type.

Platform Description

N/A

21.83. show nfpp define summary

Use this command to display the configuration.

show nfpp define summary [*name*]

Parameter Description

Parameter	Description
name	Name of the user-defined anti-attack type

Defaults
N/A

Command
Privileged EXEC mode

Mode

Usage Guide

This command can be used to display the configuration. Without the name specified, all user-defined anti-attack types will be displayed.

Configuration Examples

Related Commands

Platform Description

The following example displays the configuration.

```
QTECH#show nfpp define summary abc Define abc summary:
match etype 0x800 src-ip 1.1.1.1 src-ip-mask 255.255.255.255 Maximum count of monitored hosts: 20000
Monitor period:600s
(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface Status Rate-limit Attack-threshold Global Disable
-/10/- -/20/-
Gi4/1 Enable -/-/- -/-/-
```

Field	Description
Interface	If the interface field is displayed as Global, it means that is configured in the global configuration mode.
Status	Enables/ Disables the anti-attack function.
Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port
Attack-threshold	In the same format as the rate-limit.

Command	Description
match	Clears the monitored hosts of user-defined anti-attack type.
policy	Attack threshold and rate-limit threshold.
isolate-period	Isolates time

monitored-period	Monitored time
monitored-host-limit	Maximum monitored host number

N/A

21.84. show nfpp define trusted-host

Use this command to display the trusted host free from monitoring.

show nfpp define trusted-host *name*

Parameter

Description

Parameter	Description
name	**Name of the user-defined anti-attack type**

Defaults

N/A.

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the trusted host configuration.

```
QTECH# show nfpp define trusted-host tcp
Define tcp:
IP address    mask

1.1.1.0.    255.255.255.0
1.1.2.0.    255.255.255.0
```

Related Commands

Command	Description

trusted-host	Configures the trusted hosts.

Platform Description

N/A

21.85. show nfpp dhcp-guard hosts

Use this command to display the monitored host.

show nfpp dhcp-guard hosts [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]]]

Parameter Description

Parameter	Description
statistics	Displays the statistical information of the monitored host.
vid	VLAN ID
interface-id	Interface name
mac	MAC address

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide
N/A

Configuration Examples

Related Commands

Platform Description

The following example displays the monitored host.

```
QTEC  show      dhcp-       hosts statistics
H#          nfpp    guard total
succes      fail
s
-------------

100         2           120
            0
```

The following example displays the monitored host.

```
QTECH# show nfpp dhcp-guard hosts
If column 1 shows '*', it means "hardware failed to     isolate   host".
VLAN  interface   MAC address  remain-
time(seconds)
------------------------------

 1      gi0/2       0000.0000.000   10
                    1
 *2     gi0/1       0000.0000.000   20
                    2
Total:2 host(s)
```

Command	Description
clear nfpp dhcp-guard hosts	Clears the monitored host.

N/A

21.86. show nfpp dhcp-guard summary

Use this command to display the configuration.

show nfpp dhcp-guard summary

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide
N/A

Configuration Examples

The following example displays the configuration.

```
QTECH# show nfpp dhcp-guard summary
(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)
```

Interface	Status Isolate-period	Rate-limit	Attack-threshold
Global	Enable 300	-/5/150	-/10/300
Gi 0/1	Enable 180	-/6/-	-/8/-
Gi 0/2	Disable 200	-/5/30	-/10/50
Maximum count of monitored hosts: 1000 Monitor period:300s			

Field	Description
Interface(Global)	Global configuration
Status	Enables/Disables the anti-attack function.

Isolate-period	Isolate period
Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port
Attack-threshold	In the same format as the rate-limit.

Related Commands

Command	Description
dhcp-guard attack-threshold	Sets the global attack threshold.
dhcp-guard enable	Enables the DHCP anti-attack function.
dhcp-guard isolate-period	Sets the global isolate time.
dhcp-guard monitor-period	Sets the monitor period.
dhcp-guard monitored-host-limit	Sets the maximum number of the monitored hosts.
dhcp-guard rate-limit	Sets the global rate-limit threshold.
nfpp dhcp-guard enable	Enables the DHCP anti-attack function on the interface.
nfpp dhcp-guard isolate-period	Sets the isolate time.
nfpp dhcp-guard policy	Sets the rate-limit threshold and attack threshold.

Platform Description

N/A

21.87. show nfpp dhcpv6-guard hosts

Use this command to display the monitored host.

show nfpp dhcpv6-guard hosts [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]]]

Parameter Description

Parameter	Description
statistics	Displays the statistical information of the monitored host.
vid	The VLAN ID
interface-id	The interface name
mac-address	The MAC address

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example displays the monitored host.

```
QTECH# show nfpp dhcpv6-    hosts
guard If column 1 shows '*', it    "hardware failed to  isolate  host".
means VLAN  interface    MAC remain-
address                          time(seconds)
------------------------------

 *1      gi0/2       0000.0000.00    10
                     01
```

```
 *2     gi0/1       0000.0000.000   20
                    2
Total:2 host(s)
```

Command	Description
clear nfpp dhcpv6-guard hosts	Clears the monitored host.

N/A

21.88. show nfpp dhcpv6-guard summary

Use this command to display the configuration.

show nfpp dhcpv6-guard summary

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration

The following example displays the configuration.

Examples

```
QTECH#show nfpp dhcpv6-guard summary

(Format of column Rate-limit and Attack-threshold is
per-src-ip/per-src-mac/per-port.)
Interface Status  Rate-limit     Attack-threshold
Global    Enable  -/5/1200       -/10/1500

Maximum count of monitored hosts: 20000
Monitor period: 600s
```

Field	Description
Interface(Global)	Global configuration
Status	Enables/Disables the anti-attack function.
Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port
Attack-threshold	In the same format as the rate-limit.

Related Commands

Command	Description
dhcpv6-guard attack-threshold	Sets the global attack threshold.
dhcpv6-guard enable	Enables the DHCPv6 anti-attack function.
dhcpv6-guard monitor-period	Sets the monitor period.
dhcpv6-guard monitored-host-limit	Sets the maximum number of the monitored hosts.
dhcpv6-guard rate-limit	Sets the global rate-limit threshold.
nfpp dhcpv6-guard enable	Enables the DHCPv6 anti-attack function on

	the interface.
nfpp dhcpv6-guard policy	Sets the rate-limit threshold and attack threshold.

Platform Description

N/A

21.89. show nfpp icmp-guard hosts

Use this command to display the monitored host.

show nfpp icmp-guard hosts [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]]]

Parameter Description

Parameter	Description
statistics	Displays the statistical information of the monitored host.
vid	The VLAN ID
interface-id	The interface name
ip-address	The IP address

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example displays the monitored host.

```
QTEC    show       icmp-       hos    statistics
H#      nfpp       guard       ts
succ    fail       total
ess


100     20         120
```

The following example displays the monitored host.

```
QTECH# show nfpp icmp-guard hosts
If  column  1  shows  '*',  it  means  "hardware   t  isola   host".
failed VLAN  interface IP address remain-         o  te
time(s)


1       Gi0/1      1.1.1.1     110

2       Gi0/2      1.1.2.1     61

Total:2
host(s)
```

Command	Description
clear nfpp icmp-guard hosts	Clears the monitored host.

N/A

21.90. show nfpp icmp-guard summary

Use this command to display the configuration.

show nfpp icmp-guard summary

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command
Privileged EXEC mode

Mode

Usage Guide
N/A

Configuration Examples

The following example displays the configuration.

```
QTECH# show nfpp icmp-guard summary
(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface Status Isolate-period Rate-limit Attack-threshold


Global    Enable  300          4/-/60         8/-/100
Gi 0/1    Enable  180          5/-/-          8/-/-
Gi 0/2    Disable 200          4/-/60         8/-/100

Maximum count of monitored hosts: 1000 Monitor
period:300s
```

Field	Description
Interface(Global)	Global configuration
Status	Enables/Disables the anti-attack function.
Isolate-period	Isolate period
Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port
Attack-threshold	In the same format as the rate-limit.

Related Commands

Command	Description

icmp-guard attack-threshold	Sets the global attack threshold.
icmp-guard enable	Enables the ICMP anti-attack function.
icmp-guard isolate-period	Sets the global isolate time.
icmp-guard monitor-period	Sets the monitor period.
icmp-guard monitored-host-limit	Sets the maximum number of the monitored hosts.
icmp-guard rate-limit	Sets the global rate-limit threshold.
nfpp icmp-guard enable	Enables the ICMP anti-attack function on the interface.
nfpp icmp-guard isolate-period	Sets the isolate time.
nfpp icmp-guard policy	Sets the rate-limit threshold and attack threshold.

Platform Description

N/A

21.91. show nfpp icmp-guard trusted-host

Use this command to display the trusted host free from being monitored.

show nfpp icmp-guard trusted-host

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the trusted host free from being monitored.

```
QTECH# show nfpp icmp-guard trusted-host
IP address    mask
1.1.1.0.    255.255.255.0
1.1.2.0     255.255.255.0
```

Related Commands

Command	Description
icmp-guard trusted-host	Sets the trusted host.

Platform Description

N/A

21.92. show nfpp ip-guard hosts

Use this command to display the monitored host.

show nfpp ip-guard hosts [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]]]

Parameter Description

Parameter	Description
statistics	Displays the statistical information of the monitored host.
vid	The VLAN ID.
interface-id	The interface name.
mac-address	The MAC address.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example displays the monitored host.

```
QTEC    show       ip-       hos    statistics
H#      nfpp       guard     ts
succ    fail       total
ess


100     20         120
```

The following example displays the monitored host.

```
QTECH#show    nfpp    ip-   hosts
guard If column 1 shows
'*', it VLAN interface
IP address                  means    "hardware    do    not    hos    .
                            isolate Reason       remain-     t"
                            time(s)


1       Gi0/1     1.1.1.1   ATTACK       110

2       Gi0/2     1.1.2.1   SCAN         61

Total:2
host(s)
```

Command	Description
clear nfpp ip-guard hosts	Clears the monitored host.

N/A

21.93. show nfpp ip-guard summary

Use this command to display the configuration.

show nfpp ip-guard summary

Parameter Description

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide
N/A

Configuration Examples

The following example displays the configuration.

```
QTECH# show nfpp ip-guard summary
(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface Status Isolate-period Rate-limit Attack-threshold Scan-threshold

Global    Enable  300          4/-/60         8/-/100       15
Gi 0/1    Enable  180          5/-/-          8/-/-         -
Gi 0/2    Disable 200          4/-/60         8/-/100       20

Maximum count of monitored hosts: 1000 Monitor period..300s
```

Field	Description
Interface(Global)	Global configuration
Status	Enables/Disables the anti-attack function.
Isolate-period	Isolate period
Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port
Attack-threshold	In the same format as the rate-limit.

Scan-threshold	Scan threshold

Related Commands

Command	Description
ip-guard attack-threshold	Sets the global attack threshold.
ip-guard enable	Enables the IP anti-attack function.
ip-guard isolate-period	Sets the global isolate time.
ip-guard monitor-period	Sets the monitor period.
ip-guard monitored-host-limit	Sets the maximum number of the monitored hosts.
ip-guard rate-limit	Sets the global rate-limit threshold.
nfpp ip-guard enable	Enables the IP anti-attack function on the interface.
nfpp ip-guard isolate-period	Sets the isolate time.
nfpp ip-guard policy	Sets the rate-limit threshold and attack threshold.

Platform Description

N/A

21.94. show nfpp ip-guard trusted-host

Use this command to display the trusted host free from being monitored.

show nfpp ip-guard trusted-host

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the trusted host free from being monitored.

```
QTECH# show nfpp ip-guard trusted-host
IP address    mask
1.1.1.0.    255.255.255.0
1.1.2.0.255.255.255.0
Total.2 record(s)
```

Related Commands

Command	Description
ip-guard trusted-host	Sets the trusted host.

Platform Description

N/A

21.95. show nfpp log

Use this command to display the NFPP log configuration.

show nfpp log summary

Use this command to display the NFPP log buffer area content.

show nfpp log buffer [**statistics**]

Parameter Description

Parameter	Description
statistics	Displays the statistical information of the NFPP log buffer area.

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

When the log buffer area is full, the subsequent logs are to be dropped, and an entry with all attributes ”-” is displayed in the log buffer area. The administrator shall increase the capacity of the log buffer area or improve the rate of generating the syslog.

The generated syslog in the log buffer area carries with the timestamp, for example: %NFPP_ARP_GUARD-4-DOS_DETECTED: Host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was detected.(2009-07-01 13:00:00)

Configuration Examples

The following example displays the NFPP log configuration.

```
QTECH#show nfpp log summary Total log buffer size : 10
Syslog rate : 1 entry per 2 seconds Logging:
VLAN 1-3, 5
interface Gi 0/1 interface Gi 0/2
```

The following example displays the log number in the buffer area.

```
QTECH#show nfpp log buffer statistics
There are 6 logs in buffer.
```

The following example shows the NFPP log buffer area:

```
QTECH#show nfpp log buffer
Protocol VLAN  Interface IP address MAC address      Reason Timestamp
       -
ARP    1                           -      DoS    2009-05-30
           Gi0/1      1.1.1.1
16:23:10
ARP    1   Gi0/1      1.1.1.1     -      ISOLATED     2009-05-30
16:23:10
ARP    1   Gi0/1      1.1.1.2     -      DoS    2009-05-30
16:23:15
ARP    1   Gi0/1      1.1.1.2     -      ISOLATE_FAILED 2009-05-30
```

```
16:23:15
ARP    1    Gi0/1      -          0000.0000.0001  SCAN2009-05-30
16:30:10
ARP    -    Gi0/2      -          -      PORT_ATTACKED2009-05-30
16:30:10
```

Field	Description
Protocol	ARP, IP, ICMP, DHCP,DHCPv6, NS-NA, RS, RA-REDIRECT
Reason	DoS, ISOLATED, ISOLATE_FAILE, SCAN, PORT_ATTACKED

Related Commands

Command	Description
clear nfpp log	Clears the NFPP log buffer area.

Platform Description

N/A

21.96. show nfpp nd-guard summary

Use this command to display the configuration.

show nfpp nd-guard summary

Parameter Descript ion

Parameter	Description
N/A	N/A

Defaults
N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

Related Commands

The following example displays the configuration.

```
QTECH# show nfpp nd-guard summary
(Format of column Rate-limit and Attack-threshold is NS-NA/RS/RA-REDIRECT.)
Interface Status Rate-limit Attack-threshold

Global   Enable  20/5/10      40/10/20

Gi 0/1   Enable  15/15/15     30/30/30

Gi 0/2   Disable -/5/30       -/10/50
```

Command	Description
nd-guard attack-threshold	Sets the global attack threshold.
nd-guard enable	Enables the ND anti-attack function.
nd-guard rate-limit	Sets the global rate-limit threshold.
nfpp nd-guard enable	Enables the ND anti-attack function on the interface.
nfpp nd-guard policy	Sets the rate-limit threshold and attack

Field	Description
Interface(Global)	Global configuration
Status	Enables/Disables the anti-attack function.
Rate-limit	In the format of the rate-limit threshold for the NS-NA/RS/RA-REDIRECT.
Attack-threshold	In the same format as the rate-limit.

	threshold.

Platform Description

N/A

21.97. show nfpp nd-guard hosts

Use this command to display the monitored host.

show nfpp nd-guard hosts [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*]]]

Parameter Description

Parameter	Description
statistics	Displays the statistics of the monitored host.
vid	Sets the VLAN ID.
interface-id	Sets the interface name and number.

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the statistics of the host monitored by ND-guard.

```
QTECH#show nd- hosts statistics
nfpp success guard
fail total
----------

10 2 12
```

The following example displays the host monitored by ND-guard. The “remain-time(s)” refers to the remaining time of isolation.

```
QTECH#show nfpp nd-guard hosts
If col_filter 1 shows '*', it means "hardware do not isolate host". VLAN interface ND-guard remain-time(s)
- C14/2 ns-na-guard 174
- C14/2 rs-guard 98
```

```
-  C14/2   ra-redirect-guard 127
Total: 3 hosts
```

Platform Description

N/A

21.98. trusted-host

Use this command to set the trusted hosts free form monitoring.

Parameter Description

Use the **no** or **default** form of this command to restore the default setting,

trusted-host { *mac mac_mask* | *ip mask* | *IPv6/prefixlen* }

no trusted-host {**all |** *mac mac_mask* **|** *ip mask* | *IPv6/prefixlen* }

default trusted-host

Parameter	Description
ip	Sets the IP address
mac	MAC address
mac_mask	MAC address mask
IPv6/prefixlen	IPv6 address and mask length
mask	IP mask
all	Deletes the configuration of all trusted hosts with the no form of this command.

Defaults

N/A

Command Mode

NFPP define configuration mode

Usage Guide

The administrator can use this command to set the trusted host free from monitoring. The ICMP packets are allowed to be sent to the trusted host CPU without any rate-limit and warning configuration. Configure the mask to set all hosts in one network segment free from monitoring. UP to 500 trusted hosts are supported.

Before configuring the trusted-host, the match type must be configured. If the message type configured by the match is Ipv4, the Ipv6 trusted addresses are not allowed. In the same way, if the message type is IPv6, the IPv4 trusted addresses are not allowed.

Configuration Examples

The following example sets the trusted hosts free form monitoring.

```
QTECH(config)# nfpp QTECH(config-nfpp)# define tcp
QTECH(config-nfpp-define)#trusted-host 1.1.1.1 255.255.255.255
```

Related Commands

Command	Description
show nfpp define trusted-host	Displays the trusted host configuration.

Platform Description

N/A

21.99. no all-guard enable

Use this command to disable all NFPP guards (except guards self-defined and enabled in interface configuration mode).

Parameter Description

Command Mode

no all-guard enable

Use this command to enable all NFPP guards.

all-guard enable

Parameter	Description
N/A	N/A

NFPP configuration mode

Usage Guide

By default, all basic NFPP guards are enabled.

- This global command supports basic NFPP guards including ARP-GUARD, IP-GUARD, ICMP-GUARD, DHCP-GUARD, DHCPv6-

GUARD and ND-GUARD.

- The **no** form command will disable all guards, which is displayed guard-by-guard by using the **show running-config** command. The exception is guards self-defined and configured in interface configuration mode.

Configuration Examples

```
QTECH(config)#show running-config | begin nfpp nfpp
log-buffer enable
arp-guard rate-limit per-port 201
arp-guard attack-threshold per-port 210
!
QTECH(config)# nfpp
QTECH(config-nfpp)#no all-guard enable QTECH(config-nfpp)#show running-config | begin nfpp
nfpp
log-buffer enable no arp-guard enable
arp-guard rate-limit per-port 201
arp-guard attack-threshold per-port 210
```

```
no service password-encryption
!
```

Platform Description

N/A

22.1. ip deny invalid-l4port

Use this command to enable the anti-attack of the self-consumption. Use the **no** form of this command to restore the default setting.

ip deny invalid-l4port

no ip deny invalid-l4port

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example enables the anti-attack of the self-consumption.

```
QTECH(config)# ip deny invalid-l4port
```

The following example disables the anti-attack of the self-consumption.

```
QTECH(config)# no ip deny invalid-l4port
```

Command	Description

show ip deny invalid-l4port	Displays the state of anti-attack of the self-consumption.

N/A

22.2. ip deny invalid-tcp

Use this command to enable the anti-attack of the invalid TCP packets. Use the **no** form of this command to restore the default setting.

ip deny invalid-tcp no

ip deny invalid-tcp

Parameter Description

Parameter	Description
N/A	N/A

Defaults

The function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

Related Commands

Platform Description

The following example enables the anti-attack of the invalid TCP packets:

```
QTECH(config)# ip deny invalid-tcp
```

The following example disables the anti-attack of the invalid TCP packets:

```
QTECH(config)# no ip deny invalid-tcp
```

Command	Description
show ip deny invalid-tcp	Displays the state of anti-attack of the invalid TCP packets.

N/A

22.3. ip deny land

Use this command to enable the anti-land-attack.

Use the **no** form of this command to restore the default setting.

ip deny land

no ip deny land

Parameter Description

Parameter	Description
N/A	N/A

Defaults
This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration
The following example enables the anti-land-attack:

Examples

```
QTECH(config)# ip deny land
```

The following example disables the anti-land-attack:

```
QTECH(config)# no ip deny land
```

Related Commands

Command	Description
show ip deny land	Displays the anti-land-attack state.

Platform Description

N/A

22.4. show ip deny

Use this command to display the state of the anti-DOS-attack.

show ip deny

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the state of the anti-DOS-attack.

```
QTECH#show ip deny
Protect against Land attack      On
Protect against invalid L4port attack         Off Protect against invalid TCP attack  Off
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

22.5. show ip deny invalid-l4port

Use this command to display the state of the anti-consumption-attack.

show ip deny invalid-l4port

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the state of the anti-consumption-attack.

```
QTECH# show ip deny invalid-l4port
DoS Protection Mode    State

protect against invalid l4port attack  Off
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

22.6. show ip deny invalid-tcp

Use this command to display the state of the anti-attack of the invalid TCP packets.

show ip deny invalid-tcp

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the state of the anti-attack of the invalid TCP packets.

```
QTECH# show ip deny invalid-l4port
DoS Protection Mode    State

protect against invalid l4port attack  Off
```

```
QTECH# show ip deny invalid-l4port
```

Related Commands

Command	Description
ip deny invalid-tcp	Enables the anti-attack of the invalid TCP packets.

Platform Description

N/A

22.7. show ip deny land

Use this command to display the anti-land-attack state.

show ip deny land

Parameter Description

Parameter	Description
N/A	N/A

Defaults

N/A

Command Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example displays the anti-land-attack state.

```
QTECH# show ip deny invalid-l4port
DoS Protection Mode    State

protect against invalid l4port attack  Off
```

Related Commands

Command	Description
no ip deny land	Enables the anti-land-attack function.

Platform Description

N