Security Configuration Commands

1 AAA Commands

1.1 aaa accounting commands

Use this command to account users in order to enable 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 determing which command level is executed.
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 NOS 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 The following example enables NAS command accounting.

```
Orion_B54Q(config)# aaa accounting commands 15 default start-stop group tacacs+
```

Related Commands

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.

Platform N/A

Description

1.2 aaa accounting exec

Use this command to enable NAS access accournting. 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

NOS 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.

```
Orion_B54Q(config)# aaa accounting network start-stop group radius
```

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

NOS 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.

```
Orion_B54Q(config)# aaa accounting network start-stop group radius
```

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.

```
Orion_B54Q(config)# aaa new-model
Orion_B54Q(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

If the accounting update function has been enabled, use this command to set the interval of sednign 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 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 sets the interval of accounting update to 1 minute.

```
Orion_B54Q(config)# aaa new-model
Orion_B54Q(config)# aaa accounting update
Orion_B54Q(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

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.

```
Orion_B54Q(config)# aaa authentication dot1x rds_d1x group radius local
```

Related Commands

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.

Platform Description

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** | *list-name* } *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.

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

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.

```
Orion_B54Q(config)# aaa authentication enable default group radius local
```

Related Commands

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

Platform Description

N/A

1.8 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

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.

```
Orion_B54Q(config)# aaa authentication login list-1 group radius local
```

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 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 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.

```
Orion_B54Q(config)# aaa authentication web-auth rds_web group radius none
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.10 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	Dose 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

NOS 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

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

```
Orion_B54Q(config)# aaa authorization commands 15 default group tacacs+
```

Related Commands

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

Platform Description

N/A

1.11 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 resotre 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 The following example enables the configuration command authorization function.

```
Orion_B54Q(config)# aaa authorization config-commands
```

Related Commands

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

Platform Description N/A

1.12 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 NOS 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

The following example enables the aaa authorization console function.

```
Orion_B54Q(config)# aaa authorization console
```

Related Commands

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.

Platform Description

N/A

1.13 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

NOS 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 can not 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

The following example uses the RADIUS server to authorize Exec.

```
Orion_B54Q(config)# aaa authorization exec default group radius
```

Related

Command	Description

Commands

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

Platform Description

N/A

1.14 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

NOS 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

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

```
Orion_B54Q(config)# aaa authorization network default group radius
```

Related Commands

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.

Platform Description

N/A

1.15 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.

```
Orion_B54Q(config)# aaa domain Orion_B54Q.com
Orion_B54Q(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

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

```
Orion_B54Q(config)# aaa domain enable
```

Related Commands

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

Platform Description N/A

1.17 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 2147483647

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.

```
Orion_B54Q #configure terminal
Orion_B54Q (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

1.18 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 2147483647 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.

```
Orion_B54Q#configure terminal
Orion_B54Q(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

1.19 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 disable the system to print the system informing AAA authentication success.

aaa log enable

no aaa log enable

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled 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

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

```
Orion_B54Q(config)# no aaa log enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.20 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. The default is 5.

Defaults

The default is 5.

Command Mode

Global configuration mode

Usage Guide

N/A

Configuration Examples

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

```
Orion_B54Q(config)# aaa log rate-limit 10
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

1.21 aaa new-model

Use this command to enable the NOS 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 The following example enables the AAA security service.

```
Orion_B54Q(config)# aaa new-model
```

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

1.22 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 Mode Domain configuration 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 Orion_B54Q.com.

```
Orion_B54Q(config)# aaa domain Orion_B54Q.com
Orion_B54Q(config-aaa-domain)# access-limit 2
```

Related

Command	Description

Commands

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

1.23 accounting network

Use this command to configure the Network accounting list. Usethe **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.

```
Orion_B54Q(config)# aaa domain Orion_B54Q.com
Orion_B54Q(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

1.24 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.

```
Orion_B54Q(config)# aaa domain Orion_B54Q.com
Orion_B54Q(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

1.25 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.

```
Orion_B54Q(config)# aaa domain Orion_B54Q.com
Orion_B54Q(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

1.26 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 The following example clears the lockout user list.

```
Orion_B54Q(config)# clear aaa local user lockout all
```

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

1.27 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

The following example displays the accounting update information.

```
Orion_B54Q# show aaa accounting update
```

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

1.28 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.

```
Orion_B54Q(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

1.29 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.

```
Orion_B54Q# show aaa lockout
Lock tries:    3
Lock timeout:  15 minutes
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.30 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 The following command displays all the server groups.

```
Orion_B54Q# show aaa group
```

```
Type       Reference  Name
---------- ---------- ----------
radius     1          radius
tacacs+    1          tacacs+
radius     1          dot1x_group
radius     1          login_group
radius     1          enable_group
```

Related Commands

Command	Description
aaa group server	Configures the AAA server group.

Platform Description

N/A

1.31 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.

```
Orion_B54Q# 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 authorizating 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

1.32 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 The following example displays AAA user information.

```
Orion_B54Q#show aaa user all
-----------------------------
        Id ----- Name
 2345687901      wwxy
-----------------------------
Orion_B54Q# show aaa user by-id 2345687901
-----------------------------
        Id ----- Name
 2345687901      wwxy
Orion_B54Q# show aaa user by-name wwxy
-----------------------------
        Id ----- Name
 2345687901      wwxy
-----------------------------

Orion_B54Q# show aaa user lockout

Name                             Tries      Lock       Timeout(min)
-------------------------------- ---------- ---------- ------------
```

```
Orion_B54Q#
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.33 state

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

state { **block | active** }

no state

Parameter Description

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.

```
Orion_B54Q(config)# aaa domain Orion_B54Q.com
Orion_B54Q(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

1.34 username-format

Use this command to configure the user name whether to be with the domain information when the NAS interacts with the servers. Use the **no** form of this command to restore the default setting.

username-format { **without-domain** | **with-domain** }

no username-format

Parameter

Parameter	Description

Description

without-domain	Sets the user name without the domain information.
with-domain	Sets the user name with the domain information.

Defaults

The default is without-domain.

Command Mode

Domain configuration mode

Usage Guide

Use this command to configure the user name whether to be with the domain information when the NAS interacts with the servers.

Configuration Examples

The following example sets the user name without the domain information.

```
Orion_B54Q(config)# aaa domain Orion_B54Q.com
Orion_B54Q(config-aaa-domain)# username-domain without-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

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

```
Orion_B54Q(config)# aaa group server radius ss
Orion_B54Q(config-gs-radius)# end
Orion_B54Q# show aaa group
Type       Reference  Name
---------- ---------- ----------
radius     1          radius
tacacs+    1          tacacs+
radius     1          ss
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.2 ip radius source-interface

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

ip radius source-interface *interface*

no radius source-interface

Parameter Description

Parameter	Description
interface	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 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.

```
Orion_B54Q(config)# ip radius source-interface fastEthernet 0/0
```

Related Commands

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

Platform Description N/A

2.3 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.

```
Orion_B54Q(config)# aaa group server radius ss
Orion_B54Q(config-gs-radius)# server 192.168.4.12
Orion_B54Q(config-gs-radius)# server 192.168.4.13
Orion_B54Q(config-gs-radius)# ip vrf forwarding vrf_name
Orion_B54Q(config-gs-radius)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.4 radius attribute

Use this command to set the private attribute type value. Use the **no** form of this command to restore the default setting.

radius attribute { *id* **| down-rate-limit | dscp | mac-limit | up-rate-limit** } **vendor-type** *type*

no radius attribute { *id* | **down-rate-limit** | **dscp** | **mac-limit | up-rate-limit** } **vendor-type**

Parameter Description

Parameter	Description
id	Function ID, in the range from 1 to 255
type	Private attribute type, in the range from 1 to 255.

Defaults

Only the default configuration of private attributes in Orion_B54Q is recognized.

id	Function	type
1	max down-rate	1
2	q	s 2
3	user ip	3
4	vlan id	4
5		ersion to client 5
6	net ip	6
7	user name	7
8	password	8
9	file-directory	9
10	file-count	10
11	file-name-0	11

	2 file-name-1	12
13	file-name-2	13
14	file-name-3	14
15	file-name-4	15
16	max up-rate	16
17	version to server	17
18	flux-max-high32	18
19	flux-max-low32	19
20	proxy-avoid	20
21	dailup-avoid	21
22	ip privilege	22
23	login privilege	42

Extended attributes:

id	Function	type
1	max down-rate	76
2	qos	77
3	user ip	3
4	vlan id	4
5	version to client	5
6	net ip	6
7	user name	7
8	password	8
9	file-directory	9
10	file-count	10
11	file-name-0	11
12	file-name-1	12
13	file-name-2	13
14	file-name-3	14
15	file-name-4	15
16	max up-rate	75
17	version to server	17
18	flux-max-high32	18

19	flux-max-low32	19
20	proxy-avoid	20
21	dailup-avoid	21
22	ip privilege	22
23	login privilege	42
24	limit to user number	50

Command Mode Global configuration mode.

Usage Guide This command is used to configure the private attribute type value.

Configuration Examples The following example sets the type of max up-rate to 211.

```
Orion_B54Q(config)# radius attribute 16 vendor-type 211
```

Related Commands

Command	Description
radius set qos cos	Sets the qos value sent by the RADIUS server as the cos value of the interface.

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 Orion_B54Q are recognized.

Command Mode Global configuration mode

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

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

n Examples

```
Orion_B54Q(config)# radius vendor-specific extend
```

Related Commands

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.

Platform Description N/A

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

```
Orion_B54Q(config)#radius-server account update retransmit
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.7 radius-server attribute 31

Use this command to specify the MAC-based format of RADIUS Calling-Station-ID attribute in global configuration mode. 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

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

```
Orion_B54Q(config)# radius-server attribute 31 mac format ietf
```

Related Commands

Command	Description
radius-server host	Defines the RADIUS server.

Platform Description

N/A

2.8 radius-server dead-ctriteria

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** ***seconds*** [**tries** ***number***] **|** **tries** *number* }

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

```
Orion_B54Q(config)# radius-server dead-criteria time 120 tries 20
```

Related Commands

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.

Platform Description N/A

2.9 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 *minnutes*

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 1440 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

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

```
Orion_B54Q(config)# radius-server deadtime 1
```

Related Commands

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.

Platform Description

N/A

2.10 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.
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:

```
Orion_B54Q(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:

```
Orion_B54Q(config)# radius-server host 192.168.100.1 test username viven
idle-time 60 ignore-acct-port
```

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

```
Orion_B54Q(config)# radius-server host 3000::100
```

Related Commands

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.

Platform Description N/A

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

```
Orion_B54Q(config)# radius-server key aaa
```

Related Commands

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.

Platform Description N/A

2.12 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

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

The following example sets the number of retransmissions to 4:

```
Orion_B54Q(config)# radius-server retransmit 4
```

Related Commands

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.

Platform Description

N/A

2.13 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 number, 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 Examples

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

```
Orion_B54Q(config)# radius-server source-port 10000
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.14 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 1000 in the unit of seconds.

Defaults The default is five.

Command Mode Global configuration mode

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

Configuration Examples The following example sets the timeout to 10 seconds.

```
Orion_B54Q(config)# radius-server timeout  10
```

Related Commands

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.

Platform Description N/A

2.15 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 Global configuration mode.

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:

```
Orion_B54Q(config)# radius set qos cos
```

Related Commands

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

Platform Description N/A

2.16 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 The following example enables RADIUS to support the cui function.

```
Orion_B54Q(config)# radius support cui
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.17 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 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.

```
Orion_B54Q(config)# aaa group server radius ss
Orion_B54Q(config-gs-radius)# server 192.168.4.12 acct-port 5 auth-port 6
Orion_B54Q(config-gs-radius)# end
Orion_B54Q# show aaa group
Type       Reference  Name
---------- ---------- ----------
radius     1          radius
tacacs+    1          tacacs+
radius     1          ss
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.18 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.

```
Orion_B54Q#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

2.19 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

Usage Guide N/A

Configuration Examples The following example displays RADIUS authentication statistics.

```
Orion_B54Q#show radius auth statistics
Authentication Servers:

Server Index...................................... 1
Server Address.................................... 192.168.1.1
Server Port....................................... 1812
Msg Round Trip Time............................... 0 (msec)
First Requests.................................... 0
Retry Requests.................................... 0
Accept Responses.................................. 0
Reject Responses.................................. 0
Challenge Responses............................... 0
Malformed Msgs.................................... 0
Bad Authenticator Msgs............................ 0
Pending Requests.................................. 0
Timeout Requests.................................. 0
Unknowntype Msgs.................................. 0
Other Drops....................................... 0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.20 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 Examples

The following example displays RADIUS server group configuration.

```
Orion_B54Q#show radius group
==========Radius group radius==========
Vrf:not-set
Server:192.168.1.1
  Server key:Orion_B54Q
  Authentication port:1812
  Accounting port:1813
   State:Active
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.21 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.

```
Orion_B54Q# 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

2.22 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 Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the configuration of the RADIUS server.

```
Orion_B54Q# show radius server
erver 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

2.23 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.

```
Orion_B54Q#show radius vendor-specific
id    vendor-specific      type-value
----- -------------------- ----------
1     max-down-rate        1
2     port-priority        2
3     user-ip              3
4     vlan-id              4
5     last-supplicant-vers 5
      ion
6     net-ip               6
7     user-name            7
8     password             8
```

```
9     file-directory       9
10    file-count           10
11    file-name-0          11
12    file-name-1          12
13    file-name-2          13
14    file-name-3          14
15    file-name-4          15
16    max-up-rate          16
17    current-supplicant-v 17
      ersion
18    flux-max-high32      18
19    flux-max-low32       19
20    proxy-avoid          20
21    dialup-avoid         21
22    ip-privilege         22
23    login-privilege      42
26    ipv6-multicast-addre 79
      ss
27    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

3 TACACS+ Commands

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:

```
Orion_B54Q(config)#aaa group server tacacs+ tac1
Orion_B54Q(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. Use the **no** form of this command to disable use of the specified interface IP address.

ip tacacs source-interface *interface*

no ip tacacs source-interface

Parameter Description

Parameter	Description
interface	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

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

```
Orion_B54Q(config)# ip tacacs source-interface gigabitEthernet 0/0
```

Related Commands

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

Platform Description

N/A

3.3 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:

```
Orion_B54Q(config)# aaa group server tacacs+ tac1
Orion_B54Q(config-gs-tacacs+)# server 1.1.1.1
Orion_B54Q(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

3.4 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 a TACACS+ server address 1.1.1.1 in this group.

```
Orion_B54Q(config)#aaa group server tacacs+ tac1
Orion_B54Q(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

3.5 show tacacs

Use this command to display the TACACS+ server configuration.

show tacacs

Parameter Description

Parameter	Description
N/A	N/A

Defaults

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.

```
Orion_B54Q# 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

3.6 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* [**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 The following example configures a TACACS+ host.

```
Orion_B54Q(config)# tacacs-server host 192.168.12.1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

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

```
Orion_B54Q(config)# tacacs-server key aaa
```

Related Commands

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

Platform Description N/A

3.8 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 The following example configures the timeout interval to 10 seconds.

```
Orion_B54Q(config)# tacacs-server timeout 10
```

Related Commands

Command	Description

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

Platform Description N/A

4 802.1X Commands

4.1 aaa authorization ip-auth-mode

Use this command to set the IP authentication mode.

aaa authorization ip-auth-mode {**disabled** | **dhcp-server** | **radius-server** | **supplicant** | **mixed** }

Parameter Description

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

Defaults

IP authentication mode is disabled by default.

Command mode

Global configuration mode

Usage Guide

Use the **show running-config** command to check the IP authentication mode.

Configuration Examples

The following example enables Radius server authentication mode.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# aaa new-model
Orion_B54Q(config)# aaa authorization ip-auth-mode radius-server
Orion_B54Q(config)# end
Orion_B54Q# show running-config
!
aaa new-model
!
aaa authorization ip-auth-mode radius-server
!
Orion_B54Q# write memory
```

Related Commands

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

Platform Description

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 The following example clears all the 802.1X authentication users.

```
Orion_B54Q#clear dot1x user all
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.3 clear dot1x user id

Use this command to clear 802.1X authentication users according to session IDs.

clear dot1x user id *session-id*

Parameter Description

Parameter	Description
session-id	Session ID

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to clear 802.1X authentication users according to session IDs.

Configuration Examples The following example clears an 802.1X authentication user whose session ID is 12345678.

```
Orion_B54Q#clear dot1x user id 12345678
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.4 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

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

```
Orion_B54Q#clear dot1x user mac 0012.3456.789A
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.5 clear dot1x user name

Use this command to clear the 802.1X authentication user 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

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

```
Orion_B54Q#clear dot1x user name dot1x-user
```

Related Commands

Command	Description
N/A	N/A

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

Privileged EXEC 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 Examples

The following example configures the the accounting list.

```
Orion_B54Q(config)# dot1x accounting dot1x-acct
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.7 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

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

Configuration Examples

The following example enables EAP-MD5 authentication mode.

```
Orion_B54Q(config)# dot1x auth-mode eap
```

Related Commands

Command	Description
show dot1x	Displays the 802.1X information.

Platform Description

N/A

4.8 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.

```
Orion_B54Q(config)# dot1x auth-address-table 00d0.f800.0cb2 interface
fastethernet 0/1
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.9 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

The following example configures the authentication method list

```
Orion_B54Q(config)# dot1x authentication dot1x-authen
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.10 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

This command is used to actively initiate 802.1X authentication on the device. Use the **show dot1x auto-req** command to display the setting.

Configuration Examples

The following example enables auto-request 802.1X authentication.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# dot1x auto-req
Orion_B54Q(config)# end
Orion_B54Q(config)# show dot1x auto-req
Auto-Req: Enabled
User-Detect : Enabled
Packet-Num : 0
Req-Interval: 30 Second
```

Related Commands

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

Platform Description

N/A

4.11 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

Defaults The default is 0.

Command Mode N/A

Usage Guide Use the **show dot1x auto-req** command to display the setting.

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

```
Orion_B54Q(config)# dot1x auto-req packet-num 100
```

Related Commands

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

Platform Description N/A

4.12 dot1x auto-req req-interval

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

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

dot1x auto-req req-interval *interval*

no dot1x auto-req req-interval

Parameter Description

Parameter	Description
interval	The auto-request authentication interval, in the range from 10 to 3600 in the unit of seconds

Defaults The default is 30 seconds.

Command Mode Global configuration mode

Usage Guide Use the **show dot1x auto-req** command to display the configuration.

Configuration Examples The following example sets the auto-request authentication interval to 60 seconds.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# dot1x auto-req req-interval 60
Orion_B54Q(config)# end
```

```
Orion_B54Q# show dot1x auto-req
Auto-Req: Enabled
User-Detect : Enabled
Packet-Num : 0
Req-Interval: 60 Second
```

Related Commands

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

Platform Description N/A

4.13 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 restore the default setting.

dot1x auto-req user-detect

no dot1x auto-req user-detect

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide Use the **show dot1x auto-req** command to display the configuration.

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

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# dot1x auto-req user-detect
Orion_B54Q(config)# end
Orion_B54Q# show dot1x auto-req
Auto-Req: Enabled
User-Detect : Enabled
Packet-Num : 0
Req-Interval: 60 Second
```

Related Commands

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

Platform Description N/A

4.14 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 The following example enables online user probe function.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# dot1x client-probe enable
Orion_B54Q(config)# end
Orion_B54Q# show dot1x
802.1X Status:  Enabled
Authentication mode:    EAP-MD5
Authed User Number:     0
Re-authen Enabled:  Enabled
Re-authen Period:   1000 sec
Quiet Timer Period:     1000 sec
Tx Timer Period:    10 sec
Supplicant Timeout:     10 sec
Server Timeout:     10 sec
Re-authen Max:  5 times
Maximum Request:    3 times
Filter Non-RG Supp:     Disabled
Client Online Probe:    Enabled
Eapol Tag Enable:   Disabled
Authorization Mode:     Group Server
```

Related Commands

Command	Description
show dot1x	Displays 802.1X configuration.

Platform Description N/A

4.15 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

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

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

```
Orion_B54Q# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Orion_B54Q(config)# interface fa 0/10
Orion_B54Q(config-if)# dot1x port-control auto
Orion_B54Q(config-if)# dot1x critical
Orion_B54Q(config-if)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.16 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

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.

```
Orion_B54Q# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Orion_B54Q(config)# interface fa 0/10
Orion_B54Q(config-if)# dot1x port-control auto
Orion_B54Q(config-if)# dot1x critical recovery action reinitialize
Orion_B54Q(config-if)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

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

```
Orion_B54Q(config)# dot1x dbg-filter 00d0.f800.0001
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.18 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 1000000

Defaults The default is 1000000.

Command mode Interface configuration mode

Usage Guide Use the **show dot1x dynamic-vlan** command to display the 802.1X setting.

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

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# interface fa 0/10
Orion_B54Q(config-if)# dot1x default-user-limit 1000
Orion_B54Q(config)# end
Orion_B54Q#
```

Related Commands

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	Displays the number of users allowed by a specific 802.1X

interface fastEthernet 0/10	interface.

Platform Description N/A

4.19 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 the **show dot1x port-control interface** command to display the configuration.

Configuration Examples The following example configures single MAB authentication.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# interface fa 0/1
Orion_B54Q(config)# dot1x mac-auth-bypass
Orion_B54Q(config)# end
Orion_B54Q#
```

Related Commands

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

Platform Description N/A

4.20 dot1x mac-auth-bypass multi-user

Use this command to configure multiple MAB authentication.

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

Usage Guide

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

Configuration Examples

The following example configures multiple MAB authentications.

```
Orion_B54Q(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass multi-
user
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.21 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 65535 in the unit of seconds

Defaults

The default is 0 second.

Command Mode

Interface configuration mode

Usage Guide

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

Configuration Examples

The following example sets the MAB authentication timeout interval.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# interface fa0/1
Orion_B54Q(config)# dot1x mac-auth-bypass timeout-activity
Orion_B54Q(config)# end
Orion_B54Q#write
```

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

4.22 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 Use the **show run** command to display the 802.1X configuration.

Configuration Examples The following example configures the MAB violation.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# interface fa0/1
Orion_B54Q(config)# dot1x mac-auth-bypass violation
Orion_B54Q(config)# end
Orion_B54Q#write
```

Related Commands

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

Platform Description N/A

4.23 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.

```
Orion_B54Q(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass vlan 5，8-20
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.24 dot1x max-req

During interaction between the 802.1X and the server, the 802.1X will send a request to the server again if it does not receive a response from the server within a certain period of time. Use this command to set the maximum number of authentication requests sent to the server. Use the **no** form of this command to restore the default setting.

dot1x max-req *count*

no dot1x max-req

Parameter Description

Parameter	Description
count	Maximum auth-request number

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

The following example sets the maximum auth-request number to 7.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# dot1x max-req 7
Orion_B54Q(config)# end
Orion_B54Q#
```

Related Commands

Command	Description
show dot1x	Displays the information about 802.1X.

Platform Description

N/A

4.25 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 The following example enables the multiple-account authentication.

```
Orion_B54Q(config)# dot1x multi-account enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.26 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 65535 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 The following example sets the quiet period after the multiple MAB authentication failure to 2 seconds.

```
Orion_B54Q(config)# dot1x multi-mab quiet-period 2
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.27 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

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

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

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# interface g0/1
Orion_B54Q(config-if)# dot1x port-control auto
Orion_B54Q(config-if)# end
Orion_B54Q#
```

Related Commands

Command	Description
show dot1x	Displays the 802.1X information.

Platform Description N/A

4.28 dot1x probe-timer interval

Use this command to set the Orion_B54Q terminal detection interval.

dot1x probe-timer interval *time*

Parameter Description

Parameter	Description
time	Terminal detection interval in the range from 1 to 65535 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

The following example sets Orion_B54Q terminal detection interval to 30 seconds.

```
Orion_B54Q(config)# dot1x probe-timer interval 30
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.29 dot1x probe-timer alive

Use this command to set the Orion_B54Q terminal alive interval.

dot1x probe-timer alive *time*

Parameter Description

Parameter	Description
time	Terminal alive interval, in the range from 1 to 65535 in the unit of seconds

Defaults

The default is 60 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

The following example sets Orion_B54Q terminal alive interval to 120 seconds.

```
Orion_B54Q(config)# dot1x probe-timer alive 120
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.30 dot1x private-supplicant-only

Use this command to filter non-Orion_B54Q client.

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 You can use the **show dot1x private-supplicant-only** command to check the 802.1X setting.

Configuration Examples The following example filters non-Orion_B54Q client.

```
Orion_B54Q# configure t
Orion_B54Q(config)# dot1x private-supplicant-only
Orion_B54Q(config)# end
Orion_B54Q#
```

Related Commands

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

Platform Description N/A

4.31 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 disabled 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 Orion_B54Q supplicant judge whether the access device is a Orion_B54Q device based on the source MAC address of the EAP packets. If the access device is a Orion_B54Q device, the supplicant device performs some private features. Configure this command if you want to enable these features.

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

```
Orion_B54Q(config)# dot1x pseudo source-mac
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

4.32 dot1x redirect

Use this command to enable the 2nd 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 The following example enables the 2nd generation SU upgrade function,

```
Orion_B54Q(config)# dot1x redirect
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.33 dot1x reauth-max

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

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

dot1x reauth-max *count*

no dot1x reauth-max

Parameter Description

Parameter	Description
count	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

The following example sets the maximum re-auth attempts to 5.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# dot1x reauth-max 5
Orion_B54Q(config)# end
Orion_B54Q# show dot1x
802.1X Status:  Enabled
Authentication mode:   EAP-MD5
Authed User Number:    0
Re-authen Enabled:  Enable
Re-authen Period:   1000 sec
Quiet Timer Period:    1000 sec
Tx Timer Period:   10 sec
Supplicant Timeout:    10 sec
Server Timeout:    10 sec
Re-authen Max:  5 times
Maximum Request:   3 times
Filter Non-RG Supp:    Disabled
Client Online Probe:   Disabled
Eapol Tag Enable:  Disabled
Authorization Mode:    Group Server
```

Related Commands

Command	Description
show dot1x	Displays the 802.1X information .

Platform Description

N/A

4.34 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

The following example enables timed re-authentication function.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# dot1x re-authentication
Orion_B54Q(config)# end
Orion_B54Q# show dot1x
802.1X Status:  Enabled
Authentication mode:   EAP-MD5
Authed User Number:     0
Re-authen Enabled: Enabled
Re-authen Period:  1000 sec
Quiet Timer Period:    1000 sec
Tx Timer Period:   10 sec
Supplicant Timeout:    10 sec
Server Timeout:    10 sec
Re-authen Max:  3 times
Maximum Request:   3 times
Filter Non-RG Supp:    Disabled
Client Online Probe:   Disabled
Eapol Tag Enable:  Disabled
Authorization Mode:    Group Server
```

Related Commands

Command	Description
show dot1x	Displays the 802.1X information.

Platform Description

N/A

4.35 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 65535 in the unit of seconds.

Defaults

The default is 3600 seconds.

Command Mode

Global configuration mode

Usage Guide

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

Configuration Examples

The following example sets the re-authentication interval to 1000 seconds.

```
Orion_B54Q# configure terminal
```

```
Orion_B54Q(config)# dot1x timeout re-authperiod 1000
Orion_B54Q(config)# end
Orion_B54Q# show dot1x
802.1X Status:  Enabled
Authentication mode    EAP-MD5
Authed User Number:    0
Re-authen Enabled:  Disabled
Re-authen Period:   1000 sec
Quiet Timer Period:    1000 sec
Tx Timer Period:   3 sec
Supplicant Timeout:    3 sec
Server Timeout:    5 sec
Re-authen Max:  3 times
Maximum Request:   3 times
Filter Non-RG Supp:    Disabled
Client Online Probe:   Disabled
Eapol Tag Enable:  Disabled
Authorization Mode:    Group Server
```

Related Commands

Command	Description
show dot1x	Displays the information about 802.1X.

Platform Description

N/A

4.36 dot1x timeout quiet-period

Use this command to set the quiet period after authentication failure. Use the **no** form of this command to restore the default setting.

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

Parameter Description

Parameter	Description
seconds	Sets the quiet period after authentication failure, in the range from 1 to 65535 in the unit of seconds.

Defaults

The default is 10 seconds.

Command Mode

Global configuration mode

Usage Guide

When authentication fails, the supplicant must wait for a period of time before re-authentication.

Configuration Examples

The following example sets the quiet period after authentication failure to 1000 seconds.

```
Orion_B54Q# configure terminal
```

```
Orion_B54Q(config)# dot1x timeout quiet-period 1000
Orion_B54Q(config)# end
Orion_B54Q# show dot1x
802.1X Status:  Enabled
Authentication mode:    EAP-MD5
Authed User Number:     0
Re-authen Enabled:  Disabled
Re-authen Period:   3600 sec
Quiet Timer Period:     1000 sec
Tx Timer Period:    3 sec
Supplicant Timeout:     3 sec
Server Timeout:     5 sec
Re-authen Max:  3 times
Maximum Request:    3 times
Filter Non-RG Supp:     Disabled
Client Online Probe:    Disabled
Eapol Tag Enable:   Disabled
Authorization Mode:     Group Server
```

Related Commands

Command	Description
show dot1x	Displays the 802.1X information.

Platform Description

N/A

4.37 dot1x timeout supp-timeout

Use this command to set the authentication timeout between the device and the supplicant. Use the **no** form of the this command to restore the default setting.

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

Parameter Description

Parameter	Description
seconds	Authentication timeout between the device and the supplicant The range is from 0 to 65535 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:

```
Orion_B54Q# configure terminal
```

```
Orion_B54Q(config)# dot1x timeout supp-timeout 10
Orion_B54Q(config)# end
Orion_B54Q# show dot1x
802.1X Status:  Enabled
Authentication Mode:    EAP-MD5
Authed User Number:     0
Re-authen Enabled:  Disabled
Re-authen Period:   1000 sec
Quiet Timer Period:     1000 sec
Tx Timer Period:    3 sec
Supplicant Timeout:     10 sec
Server Timeout:     10 sec
Re-authen Max:  3 times
Maximum Request:    3 times
Filter Non-RG Supp:     Disabled
Client Oline Probe:     Disabled
Eapol Tag Enable:   Disabled
Authorization Mode:     Group Server
```

Related Commands

Command	Description
show dot1x	Show Displays the information about 802.1x.

Platform Description

N/A

4.38 dot1x timeout server-timeout

Use this command to set the server timeout interval. Use the **no** form of this command to restore the default setting

dot1x timeout server-timeout *time*

no dot1x timeout server-timeout

Parameter Description

Parameter	Description
time	The server timeout interval, in the range from 1 to 65535 in the unit of seconds

Defaults

The default is 5 seconds.

Command Mode

Global configuration mode

Usage Guide

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

Configuration Examples

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

```
Orion_B54Q# configure terminal
```

```
Orion_B54Q(config)# dot1x timeout server-timeout 10
Orion_B54Q(config)# end
Orion_B54Q# show dot1x
802.1X Status:  Enabled
Authentication mode:    EAP-MD5
Authed User Number:     0
Re-authen Enabled:  Disabled
Re-authen Period:   1000 sec
Quiet Timer Period:     1000 sec
Tx Timer Period:    3 sec
Supplicant Timeout:     3 sec
Server Timeout:     10 sec
Re-authen Max:  3 times
Maximum Request:    3 times
Filter Non-RG Supp:     Disabled
Client Online Probe:    Disabled
Eapol Tag Enable:   Disabled
Authorization Mode:     Group Server
```

Related Commands

Command	Description
show dot1x	Displays the 802.1X information.

Platform Description N/A

4.39 dot1x timeout tx-period

Use this command to set the request/id packet re-transmission interval. Use the **no** form of this command to restore the default setting.

dot1x timeout tx-period *time*

no dot1x timeout tx-period

Parameter Description

Parameter	Description
time	The request/id packet re-transmission interval, in range from 1 to 65535 in the unit of seconds

Defaults The default is 3 seconds.

Command Mode Global configuration mode

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

Configuration Examples The following example sets the request/id packet re-transmission interval to 10 seconds.

```
Orion_B54Q# configure terminal
```

```
Orion_B54Q(config)# dot1x timeout tx-period 10
Orion_B54Q(config)# end
Orion_B54Q# show dot1x
802.1X Status:  Enabled
Authentication mode:   EAP-MD5
Authed User Number:    0
Re-authen Enabled:  Disabled
Re-authen Period:   1000 sec
Quiet Timer Period:    1000 sec
Tx Timer Period:   10 sec
Supplicant Timeout:    10 sec
Server Timeout:    10 sec
Re-authen Max:  3 times
Maximum Request:   3 times
Filter Non-RG Supp:    Disabled
Client Online Probe:   Disabled
Eapol Tag Enable:  Disabled
Authorization Mode:    Group Server
```

Related Commands

Command	Description
show dot1x	Displays the information about 802.1X.

Platform Description

N/A

4.40 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.

```
Orion_B54Q(config)#dot1x valid-ip-acct enable
```

Platform

N/A

Description

4.41 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.

```
Orion_B54Q(config)# dot1x valid-ip-acct timeout 10
```

Platform Description N/A

4.42 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.

```
Orion_B54Q# show dot1x
802.1X Status:  Enabled
Authentication Mode:    EAP-MD5
```

```
Authed User Number:     0
Re-authen Enabled:  Disabled
Re-authen Period:   3600 sec
Quiet Timer Period:     10 sec
Tx Timer Period:    3 sec
Supplicant Timeout:     3 sec
Server Timeout:     5 sec
Re-authen Max:  3 times
Maximum Request:    3 times
Filter Non-RG Supp:     Disabled
Client Online Probe:    Disabled
Eapol Tag Enable:   Disabled
Authorization Mode:     Group Server
Orion_B54Q#
```

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

4.43 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.

```
Orion_B54Q# show dot1x auth-address-table
interface:g3/1
-----------------------------------
mac-addr 00D0.F800.0001
Orion_B54Q#
```

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

4.44 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

Configuratio

The following example displays the auto-request authentication information.

n Examples

```
Orion_B54Q# show dot1x auto-req
Auto-Req: Disabled
User-Detect : Enabled
Packet-Num : 0
Req-Interval: 30 Seconds
Orion_B54Q#
```

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

4.45 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.

```
Orion_B54Q# show dot1x max-req
max-req: 2 times
Orion_B54Q#
```

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

4.46 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 The following example displays the port-control information.

```
Orion_B54Q# show dot1x port-control
Interface Mode Dynamic-User Static-User Max-User Authened Mab
--------- ---------- ------------ ----------- -------- -------- ---------
Fa0/5 mac-based 0 1 6000 yes
disable
Orion_B54Q#
```

Related

Command	Description

Commands

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

4.47 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:

```
Orion_B54Q# show dot1x private-supplicant-only
private-supplicant-only:: disabled
Orion_B54Q#
```

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

4.48 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.

```
Orion_B54Q# show dot1x probe-timer
Hello Interval: 20 Seconds
Hello Alive: 250 Seconds
Orion_B54Q#
```

Related Commands

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

Platform Description

N/A

4.49 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

The following example displays re-authentication status.

```
Orion_B54Q# show dot1x re-authentication
eauth-enabled: disabled
Orion_B54Q#
```

Related Commands

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

Platform Description

N/A

4.50 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

The following example displays the maximum re-authentication attempts.

```
Orion_B54Q# show dot1x reauth-max
reauth-max: 2 times
Orion_B54Q#
```

Related Commands

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

Platform Description

N/A

4.51 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 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.

```
Orion_B54Q(config)#sh dot1x summary
ID        Username   MAC              Interface VLAN Auth-State
Backend-State Port-Status User-Type Time
--------- ---------- --------------  --------- ---- ---------------
------------- ----------- --------- ------------------
16777228  6c626dd... 6c62.6dd5.84ac  Gi0/5     2    Authenticated   Idle
Authed      static    0days 0h 0m 2s
16777229  6c626dd... 6c62.6dd5.84b4  Gi0/5     2    Authenticated   Idle
Authed      static    0days 0h 0m 2s
16777217  0023aea... 0023.aeaa.4286  Gi0/5     2    Authenticated   Idle
Authed      static    0days 0h 0m32s
16777227  6c626dd... 6c62.6dd5.84af  Gi0/5     2    Authenticated   Idle
Authed      static    0days 0h 0m 2s
16777218  6c626dd... 6c62.6dd5.84aa  Gi0/5     2    Authenticated   Idle
Authed      static    0days 0h 0m 2s
16777219  6c626dd... 6c62.6dd5.84b2  Gi0/5     2    Authenticated   Idle
Authed      static    0days 0h 0m 2s
16777230  6c626dd... 6c62.6dd5.84ad  Gi0/5     2    Authenticated   Idle
Authed      static    0days 0h 0m 2s
16777223  6c626dd... 6c62.6dd5.84b0  Gi0/5     2    Authenticated   Idle
Authed      static    0days 0h 0m 2s
16777222  6c626dd... 6c62.6dd5.84a8  Gi0/5     2    Authenticated   Idle
Authed      static    0days 0h 0m 2s
16777220  6c626dd... 6c62.6dd5.84ab  Gi0/5     2    Authenticated   Idle
Authed      static    0days 0h 0m 2s
16777221  6c626dd... 6c62.6dd5.84b3  Gi0/5     2    Authenticated   Idle
Authed      static    0days 0h 0m 2s
16777226  6c626dd... 6c62.6dd5.84ae  Gi0/5     2    Authenticated   Idle
```

```
Authed      static    0days 0h 0m 2s
16777225  6c626dd... 6c62.6dd5.84b1  Gi0/5     2    Authenticated   Idle
Authed      static    0days 0h 0m 2s
16777224  6c626dd... 6c62.6dd5.84a9  Gi0/5     2    Authenticated   Idle
Authed      static    0days 0h 0m 2s
Orion_B54Q(config)#show dot1x u
Orion_B54Q(config)#show dot1x user ip
Orion_B54Q(config)#show dot1x user id 16777226

User name: 6c626dd584ae
User id: 16777226
Type: static
Mac address is 6c62.6dd5.84ae
Vlan id is 2
Access from port Gi0/5
Time online: 0days 0h 3m55s
Max user number on this port is 0
No accounting
Permit proxy user
Permit dial user
IP privilege is 0
 user acl-name 6c626dd584ae_6_0_0 :

Orion_B54Q(config)#show dot1x user mac 6c62.6dd5.84a9

User name: 6c626dd584a9
User id: 16777224
Type: static
Mac address is 6c62.6dd5.84a9
Vlan id is 2
Access from port Gi0/5
Time online: 0days 0h 4m 7s
Max user number on this port is 0
No accounting
Permit proxy user
Permit dial user
IP privilege is 0
 user acl-name 6c626dd584a9_6_0_0 :

Orion_B54Q(config)#show dot1x user name 6c626dd584a9

User name: 6c626dd584a9
User id: 16777224
Type: static
```

```
Mac address is 6c62.6dd5.84a9
Vlan id is 2
Access from port Gi0/5
Time online: 0days 0h 4m19s
Max user number on this port is 0
No accounting
Permit proxy user
Permit dial user
IP privilege is 0
 user acl-name 6c626dd584a9_6_0_0 :
```

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

4.52 show dot1x timeout quiet-period

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

show dot1x timeout quiet-period

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Privileged EXEC mode/Global configuration mode/Interface configuration mode

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.

```
Orion_B54Q#show dot1x timeout quiet-period


Quiet-Period: 10 Seconds
```

Parameter Description:

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.53 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.:

```
Orion_B54Q#show dot1x timeout re-authperiod


Reauth-Period: 3600 Seconds
```

Parameter Description:

Parameter	Description
Reauth-Period	Re-authentication interval.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.54 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:

```
Orion_B54Q#show dot1x timeout server-timeout


Server-Timeout: 5 Seconds
```

Parameter Description:

Parameter	Description
Server-Period	AuthenticationServer timeout periodinterval.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

4.55 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:

```
Orion_B54Q#show dot1x timeout supp-timeout

Supp-Timeout: 3 Seconds
```

Parameter Description:

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

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

4.56 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:

```
Orion_B54Q#show dot1x timeout tx-period

Tx-Period: 30 Seconds
Parameter Description:
```

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

Related

Command	Description

Commands

N/A	N/A

Platform Description N/A

4.57 show dot1x user id

Use this command to display the information about 802.1X authentication users based on user IDs.

show dot1x user id *id*

Parameter Description

Parameter	Description
id	User ID

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 ID.

Configuration Examples The following example displays the information about the 802.1X authentication user according to the user ID.

```
Orion_B54Q#show dot1x user id 16777225

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 accesses 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 Orion_B54Q 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

4.58 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.

```
Orion_B54Q#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 Orion_B54Q 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

4.59 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.

```
Orion_B54Q#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 :
```

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 Orion_B54Q 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

5 SCC Commands

5.1 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

5.2 auth-mode gateway

Use this command to change the authentication mode configured on the device from access authentication to gateway authentication.

auth-mode gateway

Use this command to change the authentication mode configured on the device from gateway authentication to access authentication.

no auth-mode gateway

Parameter Description

Parameter	Description
N/A	N/A

Defaults Access authentication mode

Command Mode Global configuration mode

Default Level 14

Usage Guide The core device that performs access control needs to be enabled with the gateway authentication mode.

Configuration Examples The following example changes the authentication mode configured on the device to gateway authentication.

```
Orion_B54Q(config)# auth-mode gateway
Please save config and reload system.
```

Defaults Use the **show running** command to display the authentication mode configured on a device.

Prompt N/A

Messages

Common Errors

Forget to save the authentication mode configuration change before restarting the device. This error causes that the newly configured authentication mode does not take effect.

Platforms

This command is supported only on switches.

5.3 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 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.

Configuration Examples

The following example configures the VLAN2 as an authentication-exemption VLAN.

```
Orion_B54Q(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

This command is supported only on switches.

5.4 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.

```
Orion_B54Q(config)#int gigabitEthernet 0/1
Orion_B54Q(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 This command is supported only on switches.

5.5 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.

```
Orion_B54Q(config)#offline-detect interval 5 threshold 5120
```

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

5.6 show direct-vlan

Use this command to display the authentication-exemption VLAN configuration.

show direct-vlan

Parameter Description

Parameter	Description
N/A	N/A

Command Privileged EXEC mode

Mode

Level 14

Usage Guide N/A

Configuration Examples The following example displays the authentication-exemption VLAN configuration.

```
Orion_B54Q #show direct-vlan
direct-vlan 5,7,100
```

Prompt Messages N/A

Platforms This command is supported only on switches.

5.7 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.

```
Orion_B54Q#show nac-author-user interface gi 0/1
 Port      Cur_num  Max_num
 --------  -------  -------
 Gi0/1     0         100
```

Prompt Messages N/A

Platforms This command is supported only on switches.

5.8 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 example enables authenticated-user migration.

```
Orion_B54Q(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 This command is supported only on switches.

6 Global IP-MAC Binding Commands

6.1 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* }

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.Orion_B54Q# configure terminal

```
Enter configuration commands, one per line. End with CNTL/Z.
Orion_B54Q(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

6.2 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.

```
Orion_B54Q(config)# address-bind 3.3.3.3 00d0.f811.1112
Orion_B54Q(config)# address-bind install
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

6.3 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.

```
Orion_B54Q# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Orion_B54Q(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

6.4 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. Orion_B54Q# configure terminal

```
Enter configuration commands, one per line. End with CNTL/Z.
Orion_B54Q(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

6.5 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

Configuratio The following example displays global IPv4 address-MAC address binding.

n Examples

```
Orion_B54Q#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

Related Commands

Command	Description
address-bind	Enables IP address-MAC address binding.

Platform Description

N/A

6.6 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

The following example displays the exception port.

```
Orion_B54Q#show address-bind uplink
Port       State
---------- ---------
Gi0/1      Enabled
Default    Disabled
```

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.

Related Commands

Command	Description
address-bind uplink	Sets the exception port.

Platform Description N/A

7 Password-Policy Commands

7.1 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 65535 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.

ℹ 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 The following example sets the password lifecycle to 90 days.

```
Orion_B54Q(config)# password policy life-cycle 90
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.2 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 The following example sets the minimum length of the password to 8.

```
Orion_B54Q(config)# password policy min-size 8
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

7.3 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

The following example bans the use of passwords used in the past five times.

```
Orion_B54Q(config)# password policy no-repeat-times 5
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

7.4 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 Examples

The following example configures the strong password check.

```
Orion_B54Q(config)# password policy strong
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

7.5 service password-encryption

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

service password-encryption

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 The following example encrypts the password:

```
Orion_B54Q(config)# service password-encryption
```

Related Commands

Command	**Description**
enable password	Sets passwords of different privileges.

Platform Description N/A

7.6 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

The following example displays the password security policy set by the user.

```
Orion_B54Q#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	

Related Commands

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

Platform Description

N/A

8 Port Security Commands

8.1 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.

Configuration Examples The following example enables port security on interface gigabitethernet 1/1, and the way to deal with violation is **shutdown**:

```
Orion_B54Q(config)#interface gigabitethernet 1/1
Orion_B54Q(config-if)# switchport port-security
Orion_B54Q(config-if)# switchport port-security violation shutdown
```

Related Commands

Command	Description
show port-security	Displays port security settings.

Platform Description N/A

8.2 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 0-1440 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 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.
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.

Configuration Examples The following example sets the aging time for all secure addresses on interface gigabitethernet 1/1 to eight minutes.

```
Orion_B54Q(config)# interface gigabitethernet 1/1
Orion_B54Q(config-if)# switchport port-security aging time 8
Orion_B54Q(config-if)# switchport port-security aging static
```

Related Commands

Command	**Description**
show port-security	Displays port security settings.

Platform Description N/A

8.3 switchport port-security binding

Use this command 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 this command to remove the binding addresses.

switchport port-security binding *mac-address* **vlan** *vlan_id ipv4-address* | *ipv6-address*

no 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 *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	Binding IPv4 addresses
ipv6-address	Binding IPv6 addresses

Defaults N/A

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example binds the IP address 192.168.1.100 on interface g 0/10:

```
Orion_B54Q(config)#inter g0/10
Orion_B54Q(config-if)# switchport port-security binding 192.168.1.100
```

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.

```
Orion_B54Q(config)#inter g0/10
Orion_B54Q(config-if)# switchport port-security binding 00d0.f800.5555
vlan 1 192.168.1.100
```

Related Commands

Command	Description
switchport 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

8.4 switchport port-security binding interface

Use this command 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 this command to remove the binding addresses

switchport port-security binding interface i*nterface-id mac-address* **vlan** *vlan_id ipv4-address* | *ipv6-address*

no switchport port-security binding interface *interface-id mac-address* **vlan** *vlan_id ipv4-address* | *ipv6-address*

switchport port-security binding interface i*nterface-id ipv4-address* | *ipv6-address*

no switchport port-security binding interface i*nterface-id ipv4-address* | *ipv6-address*

Parameter Description

Parameter	**Description**
mac-address	Binding source MAC address
vlan_id	Vlan ID of the binding source MAC address
ipv4-address	Binding IPv4 address
ipv6-address	Binding IPv6 address

Defaults

N/A

Command Mode

Interface configuration mode

Usage Guide

N/A

Configuration Examples

The following example binds the IP address *192.168.1.100* on the interface *g 0/10.*

```
Orion_B54Q(config)# switchport port-security binding interface g 0/10
192.168.1.100
```

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.

```
Orion_B54Q(config)# switchport port-security binding interface g 0/10
00d0.f800.5555 vlan 1 192.168.1.100
```

Related Commands

Command	**Description**
switchport 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

8.5 switchport port-security mac-address

Use this command to configure manually 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. ℹ The configuration of vlan-id is only supported on the TRUNK port.

Defaults N/A

Command Mode Interface 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.

```
Orion_B54Q(config)#inter g0/10
Orion_B54Q(config-if)# switchport port-security mac-address 00d0.f800.5555
vlan 2
```

Related Commands

Command	Description
switchport 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

8.6 switchport port-security interface mac-address

Use this command to configure manually 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-id*]

Parameter Description

Parameter	Description
interface-id	Interface ID
mac-address	Static secure address
vlan-id	VLAN ID of the MAC address ℹ The configuration of vlan-id is only supported on the TRUNK port.

Defaults N/A

Command Mode Privileged EXEC 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.

```
Orion_B54Q(config)# switchport port-security interface g0/10 mac-address
00d0.f800.5555 vlan 2
```

Related Commands

Command	Description
switchport 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

8.7 switchport port-security maximum

Use this command to set the maximum number of the port secure address.

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.

This limit only works for secure addresses. It does not affect the number of secure address binding.

Configuration Examples The following example sets the maximum number of the secure address to 2 for interface g 0/10.

```
Orion_B54Q(config)#inter g0/10
Orion_B54Q(config-if)# switchport port-security maximum 2
```

Related Commands

Command	Description
switchport 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

8.8 switchport port-security mac-address sticky

Use this command to configure manually 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

Parameter	Description

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 N/A

Configuration Examples The following example sets the MAC address and VLAN ID of TRUNK port 10 to 00d0.f800.5555 to 2 respectively.

```
Orion_B54Q(config)#inter g0/10
Orion_B54Q(config-if)# switchport port-security mac-address 00d0.f800.5555
vlan 2
```

The following example enables the Sticky MAC address learning on interface g0/10.

```
Orion_B54Q(config)#inter g0/10
Orion_B54Q(config-if)# switchport port-security sticky mac-address
```

Related Commands

Command	**Description**
switchport 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

8.9 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.

Configuration Examples The following example displays the port security statistics.

```
Orion_B54Q#show port-security
NO.  SecurePort MaxSecureAddr CurrentAddr CurrentIpBind CurrentIpMacBind
SecurityAction
                   (Count)      (Count)      (Count)         (Count)
---- ---------- ------------- ----------- ------------- ----------------
--------------
1    Gi0/1      128           2           2             1
protect
-----------------------------------------------------------------------------
----------
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 addresses 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.

```
Orion_B54Q#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.

The following example displays all secure addresses on the device.

```
Orion_B54Q#show port-security address
NO.  VLAN  MacAddress      PORT                      TYPE
RemainingAge(mins)  STATUS
---- ----- --------------- ------------------------- ----------
------------------  ---------
1    1     00d0.f800.073c  GigabitEthernet 0/1       Configured         --
active
2    1     00d0.f800.073d  GigabitEthernet 0/1       Configured         --
active
```

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.

The following example displays all port security bindings on the device.

```
Orion_B54Q#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.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

9 Storm Control Commands

9.1 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 The following example displays storm control configuration on FastEthernet 0/1.

```
Orion_B54Q# show storm-control gigabitethernet 1/1
Interface Broadcast Control Multicast Control Unicast Control
----------- --------------- ---------------- ---------------
Gi1/1 Disabled Disabled Disabled
```

Related Commands

Command	Description
storm-control	Enables storm suppression.

Platform Description N/A

9.2 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

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

Parameter	Description
Broadcast	Enables the broadcast storm suppression function.
Multicast	Enables the unknown unicast storm suppression function.
Unicast	Enables the unknown unicast storm suppression function.
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).

Use the **show storm-control** command to display configuration.

Configuration Examples

The following example enables the multicast storm suppression on GigabitEthernet 1/1 and sets the allowed rate to 4M.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# interface GigabitEthernet 1/1
Orion_B54Q(config-if)# storm-control multicast 4096
Orion_B54Q(config-if)# end
```

Related Commands

Command	Description
show storm-control	Displays storm suppression information.

Platform Description

N/A

10 SSH Commands

10.1 cryptozoic key generate

Use this command to generate a public key to the SSH server:

cryptozoic key generate { **rsa | ads** }

Parameter Description

Parameter	Description
Rsa	Generates an RSA key.
Ads	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.

⚠ A key can be deleted by using the **cryptozoic key mobilizer** command. The **no cryptozoic key generate** command is not available.

Configuration Examples

The following example generates a RSA key to the SSH server:

```
Orion_B54Q# configure terminal
Orion_B54Q(con fig)# Cryptozoic key generate SARS
```

Related Commands

Command	Description
show ip ssh	Displays the current status of the SSH server.
cryptozoic key mobilizer { **rsa** | **ads** }	Deletes DSA and RSA keys and disables the SSH server function.

Platform Description

N/A

10.2 cryptozoic key zeroize

Use this command to delete a public key to the SSH server.

cryptozoic key zeroize { **rsa | ads** }

Parameter

Parameter	Description

Description

rsa	Deletes the RSA key.
ads	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.

```
Orion_B54Q# configure terminal
Orion_B54Q(con fig)# Cryptozoic key zeroize rsa
```

Related Commands

Command	Description
show ip ssh	Displays the current status of the SSH server.
Cryptozoic key generate {**rsa**| **ads** }	Generates DSA and RSA keys.

Platform Description N/A

10.3 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 connection or disconnect a SSH connection by entering the specified VTY connection ID. Only connections of the SSH type can be disconnected.

Configuration Examples The following example disconnects the established SSH connection by specifying the SSH session ID.

```
Orion_B54Q# disconnect ssh 1
```

The following example disconnects the established SSH connection by specifying the VTY session ID.

```
Orion_B54Q# disconnect ssh vty 1
```

Related Commands

Command	Description
show ssh	Displays the information about the established SSH connection.
clear line vty *line_number*	Disconnects the current VTY connection.

Platform Description

N/A

10.4 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

N/A

Configuration Examples

The following example enables the SCP server function.

```
Orion_B54Q# configure terminal
Orion_B54Q(con fig)# ip scp server enable
```

Related Commands

Command	Description
show ip ssh	Displays the current status of the SSH server.

Platform Description

N/A

10.5 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.

```
Orion_B54Q# configure terminal
Orion_B54Q(con fig)# ip ssh authentication-retries 2
```

Related Commands

Command	Description
show ip ssh	Displays the current status of the SSH server.

Platform Description

N/A

10.6 ip ssh peer

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**| **ads** } *enameler*

no ip ssh peer *username* **public-key** { **rsa**| **ads** } *enameler*

Parameter Description

Parameter	Description
Username	User name
Enameler	Name of a public key file
Rsa	The public key is a RSA key
Ads	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**.

```
Orion_B54Q# configure terminal
Orion_B54Q(con fig)# ip ssh peer test public-key rsa flash:rsa.pub
Orion_B54Q(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

10.7 ip ssh time-out

Use this command to set the authentication timeout interval 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 interval, 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:

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# ip ssh time-out 100
```

Related Commands

Command	Description
show ip ssh	Displays the current status of the SSH server.

Platform Description N/A

10.8 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. When a version is set, the connection sent by the SSH client of this version is accepted only. The **no ip ssh version** command can also be used to restore the default setting.

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:

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# ip ssh version 2
```

Related Commands

Command	Description
show ip ssh	Displays the current status of the SSH server.

Platform Description

N/A

10.9 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 Examples

The following example displays the information about the public key part of the public key to the SSH server.

```
Orion_B54Q# show crypto key mypubkey rsa
```

Related Commands

Command	Description
crypto key generate { **rsa** | **dsa** }	Generates DSA and RSA keys.

Platform

N/A

Description

10.10 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, 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.

```
Orion_B54Q# show ip ssh
```

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

10.11 show ssh

Use this command to displays 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:

```
Orion_B54Q# show ssh
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

11 URPF Commands

11.1 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*	Displays statistics on the specified interface.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide IPv4 URPF packet drop statistics on all interfaces are cleared by default.

Configuration Examples

The following example clears IPv4 URPF packet drop statistics on port GigabitEthernet 0/1.

```
Orion_B54Q# clear ip urpf interface gigabitEthernet0/1
```

The following example clears IPv4 URPF packet drop statistics on all interfaces.

```
Orion_B54Q# clear ip urpf
```

Related Commands

Command	Description
showip urpf	Displays the URPF configuration and statistics.

Platform Description N/A

11.2 ip verify unicast source reachable-via (Interface Configuration Mode)

Use this command to enable the 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**] [*acl-id*]

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.
acl-id	(Optional) Sets the ACL number: 1 to 99 (IP standard access list) 100 to 199 (IP extended access list) 1300 to 1999 (IP standard access list, expanded range) 2000 to 2699 (IP extended access list, expanded range)

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.

✓ Not support the ACL association;
Not support to use the IPv6 route with prefix in 65~127 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.

Configuration Examples The following example checks the URPF feature of the received packets in the strict mode on the interface GigabitEthernet 0/1.

```
Orion_B54Q(config)# interface gigabitEthernet0/1
Orion_B54Q(config-if)# ip verify unicast source reachable-via rx
```

Related Commands

Command	Description
show ip urpf	Displays the URPF information.

Platform Description N/A

11.3 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
interval *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 N/A

Configuration Examples The following example sets the URPF drop-rate compute interval as 60 seconds.

```
Orion_B54Q(config)# ip verify urpf drop-rate compute interval 60
```

Related Commands

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.

Platform Description N/A

11.4 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.

Configuration Examples The following example enables the URPF drop-rate monitoring on port GigabitEthernet 0/1.

```
Orion_B54Q(config)# interface gigabitEthernet0/1
Orion_B54Q(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

11.5 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

The following example sets the URPF drop-rate notification interval as 1 minute.

```
Orion_B54Q(config)# ip verify urpf drop-rate notify hold-down 60
```

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 monitoring.
ip verify urpf notification threshold	Sets the URPF drop-rate threshold.

Platform Description

N/A

11.6 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 4294967295 in the unit of packets per second (pps).

Defaults

The default is 1000 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.

Configuration Examples

The following example sets the URPF drop-rate threshold 10pps on the interface GigabitEthernet 0/1.

```
Orion_B54Q(config)# interface gigabitEthernet0/1
Orion_B54Q(config-if-GigabitEthernet 0/1)# ipv6 verify urpf drop-rate
notify
Orion_B54Q(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

11.7 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.

```
Orion_B54Q# 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.

```
Orion_B54Q# 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

12 CPU Protection Commands

12.1 clear cpu-protect-counters

Use this command to clear the CPP statistics.

clear cpu-protect counters [**device** *device_num*] [**slot** *slot_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.
slot_num	To the box-type device, there is no slot parameter. To the chassis device, the slot parameter indicates the line card of the master chassis. If no slot parameter is specified, that means the command will clear all node statistics in the system. If you want to clear the statistics of a specific node, both the device parameter and the slot parameter will be required.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example clears the CPP statistics.

```
Orion_B54Q(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
Orion_B54Q#clear cpu-protect counters
Orion_B54Q(config)#show cpu-protect type bpdu
Packet Type         Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)
Total     Total Drop
------------------  -------------  --------------  ---------  ---------
--------  ----------
bpdu                6              200             0          0          0
0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.2 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 The following example clears the CPP statistics on the supervisor module.

```
Orion_B54Q(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
Orion_B54Q#clear cpu-protect counters mboard
Orion_B54Q(config)#show cpu-protect type bpdu
Packet Type         Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)
Total     Total Drop
------------------  -------------  --------------  ---------  ---------
--------  ----------
bpdu                6              200             0          0          0
0
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

12.3 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 Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example sets the CPU port bandwidth to 32000pps.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# cpu-protect cpu bandwidth 32000
Orion_B54Q#show cpu-protect cpu
%cpu port bandwidth: 32000(pps)
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.4 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 Mode

Privileged EXEC mode

Usage Guide

N/A

Configuration Examples

The following example s sets the priority queue 5 to 3500 pps.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# cpu-protect traffic-class 5 bandwidth 3500
Orion_B54Q#show cpu-protect traffic-class 5
Traffic-class   Bandwidth(pps)  Rate(pps)       Drop(pps)
-------------   --------------  ---------       ---------
 5              3500            0               0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

12.5 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.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# cpu-protect type bpdu bandwitdth 200
```

```
Orion_B54Q(config)#show cpu-protect type bpdu
Packet Type         Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)
Total     Total Drop
------------------  -------------  --------------  ---------  ---------
--------  ----------
bpdu                6              200             0          0          0
0
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

12.6 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

The following example sets the PQ of BPDU packets to 5.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# cpu-protect type bpdu traffic-class 5
Orion_B54Q(config)#show cpu-protect type bpdu
Packet Type         Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)
Total     Total Drop
------------------  -------------  --------------  ---------  ---------
--------  ----------
bpdu                5              200             0          0          0
0
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

12.7 show cpu-protect

Use this command to display all CPP configuration and statistics.

show cpu-protect [**device** *device_num*] [**slot** *slot_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.
slot_num	To the box-type device, there is no slot parameter. To the chassis device, the slot parameter indicates the line card of the master chassis. If no slot parameter is specified, that means the command will clear all node statistics in the system. If you want to clear the statistics of a specific node, both the device parameter and the slot parameter will be required.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example displays all CPP configuration and statistics of a line card.

```
Orion_B54Q#show cpu-protect slot 3/2
%cpu port bandwidth: 80000(pps)
Traffic-class   Bandwidth(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              8000            0               0
 6              8000            0               0
 7              8000            0               0
```

```
Packet Type          Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)
Total     Total 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  6              128            0          0          0
0
nd-non-snp          6              128            0          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

12.8 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.

```
Orion_B54Q#show cpu-protect cpu
%cpu port bandwidth: 32000(pps)
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

12.9 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.

```
Orion_B54Q#show cpu-protect mboard
%cpu port bandwidth: 80000(pps)
Traffic-class   Bandwidth(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              8000            0               0
 6              8000            0               0
 7              8000            0               0
Packet Type         Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)
Total     Total 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  6              128             0          0          0
0
nd-non-snp          6              128             0          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

12.10 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 The following example displays the CPP configuration and statistics of the master device.

```
Orion_B54Q#show cpu-protect summary
%cpu port bandwidth: 80000(pps)
Traffic-class   Bandwidth(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              8000            0               0
 6              8000            0               0
 7              8000            0               0
Packet Type         Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)
Total      Total 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  6              128              0          0          0
0
nd-non-snp          6              128              0          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

12.11 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***] [slot** *slot_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.
slot_num	To the box-type device, there is no slot parameter. To the chassis device, the slot parameter indicates the line card of the master chassis. If no slot parameter is specified, that means the command will clear all node statistics in the system. If you want to clear the statistics of a specific node, both the device parameter and the slot parameter will be required.

Defaults N/A

Command Mode

All configuration modes

Usage Guide

N/A

Configuration Examples

The following example displays the summarized configuration and statistics of priority queues.

```
R Orion_B54Q#show cpu-protect traffic-class all
Traffic-class   Bandwidth(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
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

12.12 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*] [**slot** *slot_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.
slot_num	To the box-type device, there is no slot parameter. To the chassis device, the slot parameter indicates the line card of the master chassis. If no slot parameter is specified, that means the command will clear all node statistics in the system. If you want to clear the statistics of a specific node, both the device parameter and the slot parameter will be required.

Defaults N/A

Command Mode All configuration modes

Usage Guide N/A

Configuration Examples The following example displays the statistics of the ICMP packets.

```
Orion_B54Q(config)#show cpu-protect type icmp
Packet Type         Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)
Total     Total Drop
------------------  -------------  --------------  ---------  ---------
--------  ----------
icmp                5              1500             50        0
10000     100
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

13 DHCP Snooping Commands

13.1 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.

Configuration Examples The following example clears the dynamic database information from the DHCP Snooping binding database.

```
Orion_B54Q# clear ip dhcp snooping binding
Orion_B54Q# 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

13.2 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.Note that DHCP Snooping cannot coexist with private VLAN.

Configuration Examples The following example enables the DHCP Snooping function.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# ip dhcp snooping
Orion_B54Q(config)# end
Orion_B54Q# show ip dhcp snooping
Switch DHCP snooping status: ENABLE
DHCP snooping 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)
------------------------   -------     ---------------
```

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

13.3 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

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 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.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# ip dhcp snooping bootp-bind
Orion_B54Q(config)# end
Orion_B54Q# 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)
------------------------  -------    ------------
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP Snooping configuration.

Platform Description N/A

13.4 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 *time*

Parameter Description

Parameter	Description
time	The interval 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

This function avoids loss of user information 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 3600 seconds.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# ip dhcp snooping database write-delay 3600
Orion_B54Q(config)# end
Orion_B54Q# show ip dhcp snooping
Switch DHCP snooping status: ENABLE
DHCP snooping Verification of hwaddr field status: ENABLE
DHCP snooping database write-delay time: 3600
DHCP snooping option 82 status: DISABLE
DHCP Snooping Support Bootp bind status: ENABLE
Interface         Trusted           Rate limit (pps)
------------------------   -------      ---------------
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the configuration information of the DHCP Snooping.

Platform Description

N/A

13.5 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.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# ip dhcp snooping database write-to-flash
Orion_B54Q(config)# end
Orion_B54Q#
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

13.6 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 message based on which the DHCP server assigns IP address.

Configuration Examples

The following example adds option82 to the DHCP request message.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# ip dhcp snooping information option
Orion_B54Q(config)# end
Orion_B54Q# show ip dhcp snooping
Switch DHCP snooping  status                       :   ENABLE
DHCP snooping  Verification of hwaddr status    :   ENABLE
DHCP snooping database write-delay time         :   0
DHCP snooping option 82 status                  :   DISABLE
DHCP Snooping Support Bootp bind status: ENABLE
Interface                Trusted       Rate limit (pps)
------------------------ -------       ----------------
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP Snooping configuration.

Platform Description

N/A

13.7 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 being hostname.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# ip dhcp snooping information option format remote-id
hostname
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

13.8 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

Usage Guide This command denies all DHCP request messages under the port, that is, all the users under the port are prohibited to request addresses through DHCP.

Configuration Examples The following example sets **fastethernet** 0/2 to be in the suppression status.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# interface fastEthernet 0/2
Orion_B54Q(config-if)# ip dhcp snooping suppression
Orion_B54Q(config-if)# end
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP Snooping configuration.

Platform Description N/A

13.9 ip dhcp snooping trust

Use this command to set the trusted ports.

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

ip dhcp snooping trust

no ip dhcp snooping trust

Parameter Description

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.

Configuration Examples

The following example sets **fastEthernet** *0/1* as a trusted port:

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# interface fastEthernet 0/1
Orion_B54Q(config-if)# ip dhcp snooping trust
Orion_B54Q(config-if)# end
Orion_B54Q# show ip dhcp snooping
Switch DHCP snooping status: ENABLE
DHCP snooping 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)
-----------------   -------            ----------------
FastEthernet0/1 yes                   unlimited
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP Snooping configuration.

Platform Description

N/A

13.10 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 enable checking the validity of the source MAC address of the DHCP request message. Once the function is enabled, the system will discard the DHCP request message that fails to pass the source MAC address check.

Configuratio

The following example enables the check of the source MAC address of the DHCP request

n Examples

message.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# ip dhcp snooping verify mac-address
Orion_B54Q(config)# end
Orion_B54Q# show ip dhcp snooping
Switch DHCP snooping status: ENABLE
Verification of hwaddr field status: ENABLE
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)
```

Related Commands

Command	Description
show ip dhcp snooping	Displays the DHCP Snooping configuration.

Platform Description

N/A

13.11 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 configure effective DHCP Snooping VLAN by character string.

Configuration Examples

The following example enables the DHCP Snooping function in VLAN1000.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# ip dhcp snooping vlan 1000
Orion_B54Q(config)# end
```

Related Commands

Command	Description

ip dhcp snooping	Enables DHCP Snooping globally.

Platform Description N/A

13.12 ip dhcp snooping vlan information option change-vlan-to vlan

Use this command to enable the option82 sub-option circuit and change the VLAN in the circuit-id into the specified VLAN.

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

ip dhcp snooping vlan *vlan-id* **information option change-vlan-to vlan** *vlan-id*

no ip dhcp snooping vlan *vlan-id* **information option change-vlan-to vlan** *vlan-id*

Parameter Description

Parameter	**Description**
vlan-id	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 configured, the option82 is added to the DHCP request packets, the circuit-id in the option82 information is the specified VLAN and the DHCP server will assign the addresses according to the option82 information.

Configuration Examples The following adds the option82 to the DHCP request packets and changes the VLAN4094 in the option82 sub-option circuit-id to VLAN93:

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# interface fastEthernet 0/1
Orion_B54Q(config-if)# ip dhcp snooping vlan 4094 information option
change-vlan-to vlan 4093
Orion_B54Q(config-if)# end
```

Related Commands

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

Platform Description N/A

13.13 ip dhcp snooping vlan information option format-type circuit-id string

Use this command to configure the option82 sub-option circuit-id as user-defined (the storage format is ASCII) and to perform the packet forwarding. Use the **no** form of this command to restore the default setting.

ip dhcp snooping vlan *vlan-id* **information option format-type circuit-id string** *ascii-string*

no ip dhcp snooping vlan *vlan-id* **information option format-type circuit-id string** *ascii-string*

Parameter Description

Parameter	Description
vlan-id	The VLAN where the DHCP request packets are
ascii-string	The user-defined content to fill to the Circuit ID

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide This command is used to add the option82 to the DHCP request packets. The content of the sub-option circuit-id is customized, and the DHCP server will assign the addresses according the option82 information.

Configuration Examples The following example adds the option82 to the DHCP request packets with the content of the sub-option circuit-id being *port-name*.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# interface fastEthernet 0/1
Orion_B54Q(config-if)# ip dhcp snooping vlan 4094 information option
format-type circuit-id string port-name
Orion_B54Q(config-if)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description This command is supported on all switches.

13.14 ip dhcp snooping vlan max-user

Use this command to set the maximum number of users bound with the VLAN. Use the **no** form of this command to restore the default setting.

ip dhcp snooping vlan *vlan-word* **max-user** *user-number*

no ip dhcp snooping vlan *vlan-word* **max-user** *user-number*

Parameter Description

Parameter	Description
vlan-word	The VLAN range.
user-number	The maximum number of users bound with the VLAN.

Defaults

The limit for the number of users bound with the VLAN is disabled by default.

Command Mode

Interface configuration mode

Usage Guide

Use this command to set the maximum number of users bound with the VLAN. This function combined with the corresponding topology can prevent illegal DHCP packet attacks.

Configuration Examples

The following example sets the maximum number of users bound with VLAN 1-10 and VLAN 20 to 30 respectively.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# interface GigabitEthernet 0/1
Orion_B54Q(config-if-GigabitEthernet 0/1)# ip dhcp snooping vlan 1-10,20 max-user 30
Orion_B54Q(config-if-GigabitEthernet 0/1)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

13.15 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.

Configuration Examples

The following example imports the flash file information to the DHCP Snooping database.

```
Orion_B54Q# renew ip dhcp snooping database
```

Related Commands

Command	Description
N/A	N/A

Platform Description

This command is supported on all switches.

13.16 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.

```
Orion_B54Q# 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)
------------------------ -------    ------------
```

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

13.17 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 N/A

Configuration Examples The following example displays the information of the DHCP Snooping binding database.

```
Orion_B54Q# show ip dhcp snooping binding
Total number of bindings: 1
NO.   MACADDRESS         IPADDRESS       LEASE(SEC)   TYPE          VLAN
INTERFACE
----- ------------------ --------------- ------------ ------------- -----
--------------------
1     0000.0000.0001     1.1.1.1         78128        DHCP-Snooping 1
GigabitEthernet 0/1
```

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

14 ARP-Check Commands

14.1 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 example enables the APR check function on interface GigabitEthernet 0/1.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# interface GigabitEthernet 0/1
Orion_B54Q(config-if-GigabitEthernet 0/1)# arp-check
Orion_B54Q(config-if-GigabitEthernet 0/1)# end
```

Related Commands

Command	Description
show interface arp-check list	Displays the ARP check entries.

Platform Description N/A

14.2 show interface arp-check list

Use this command to display the ARP check entries on the Layer 2 interface.

show { **interface** [*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

The following example displays the ARP check entries.

```
Orion_B54Q(config)#show interface arp-check list
INTERFACE
SENDER MAC      SENDER IP            POLICY SOURCE
------------------------ ---------------- ----------------
--------------------
GigabitEthernet 0/1        00D0.F800.0003   192.168.1.3      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

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

15 DAI Commands

15.1 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 an untrusted port.

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**.**

```
Orion_B54Q(config)# interface gigabitEthernet 0/19
Orion_B54Q(config-if)# ip arp inspection trust
```

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

15.2 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.

ip arp inspection vlan { *vlan-id* | *word* }

no ip arp inspection vlan { *vlan-id* | *word* }

Parameter

Parameter	Description

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:

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# ip arp inspection
Orion_B54Q(config)# ip arp inspection vlan 1
Orion_B54Q(config)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

15.3 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 Mode Privileged EXEC 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:

```
Orion_B54Q# show ip arp inspection vlan
Vlan     Configuration
```

```
----     -------------
1                                                 Enable
```

Parameter Description:

Parameter	Description
Vlan	VLAN number.
Configuration	DAI status (active / inactive)

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

15.4 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 :

```
Orion_B54Q#show ip arp inspection interface
Interface         Trust State
---------------------    -----------
GigabitEthernet 0/1      Trusted
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

16 IP Source Guard Commands

16.1 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 restore the default setting.

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

N/A

Configuration Examples

The following example configures a static user.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1
interface FastEthernet 0/1
Orion_B54Q(config)# end
Orion_B54Q# show ip source binding
MacAddress     IpAddress  Lease(sec)   Type     VLAN  Interface
------------- --------- ----------   ----     ----  ------------
0000.0000.0001 1.1.1.1   infinite    static    1  FastEthernet 0/1
Total number of bindings: 1
```

Related Commands

Command	Description
show ip source binding	Displays the binding information of IP source address and database.

Platform

N/A

Description

16.2 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 [**port-security**]

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.

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 configures IP Source Guard on port fastEthernet 0/1:

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# interface fastEthernet 0/1
Orion_B54Q(config-if)# ip verify source
Orion_B54Q(config-if)# end
```

Related Commands

Command	Description
show ip verify source	Displays user filtering entry of IP Source Guard.

Platform Description

N/A

16.3 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

1. 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.
2. Once the IP source guard function is disabled, the excluded VLAN is cleared automatically.
3. This command is supported on the wired L2 switching port, AP port, and sub interface.

ℹ 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.

```
Orion_B54Q# configure terminal
Orion_B54Q(config)# interface GigabitEthernet 0/1
Orion_B54Q(config-if-GigabitEthernet 0/1)# ip verify source
Orion_B54Q(config-if-GigabitEthernet 0/1)# ip verify exclude-vlan 1
Orion_B54Q(config-if)# end
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

16.4 show ip source binding

Use this command to display the binding information of IP source address and database.

show ip binding [*ip-address*] [*mac-addres s*] [**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

```
Orion_B54Q# show ip source binding static
MacAddress     IpAddress  Lease(sec)   Type     VLAN  Interface
------------- --------- ----------    ----     ----  ------------
0000.0000.0001 1.0.0.1   infinite    static    1  FastEthernet 0/1
Total number of bindings: 1
```

Related Commands

Command	Description
ip source binding	Sets the binding static user.

Platform Description

N/A

16.5 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.

```
Orion_B54Q # show ip verify source
Total number of bindings: 7
NO.   INTERFACE            FILTERTYPE  FILTERSTATUS           IPADDRESS
```

```
MACADDRESS      VLAN TYPE
----- -------------------- ----------- ---------------------
--------------- --------------- -------- -------------
1     Global               IP+MAC      Inactive-not-apply
192.168.0.127   0001.0002.0003  1 Static
2     GigabitEthernet 0/5  IP-ONLY     Active                 1.2.3.4
0001.0002.0004  1 DHCP-Snooping
3     Global               IP-ONLY     Active                 1.2.3.7
0001.0002.0007  1 Static
4     Global               IP+MAC      Active                 1.2.3.6
0001.0002.0006  1 Static
5     GigabitEthernet 0/1  UNSET       Inactive-restrict-off  1.2.3.9
0001.0002.0009  1 DHCP-Snooping
6     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

17 Anti-ARP Spoofing Commands

17.1 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

Usage Guide

This command is used to enable anti-ARP spoofing on only L2 interfaces.

Use the **show anti-arp-spoofing** command to display the configuration.

Configuration Examples

The following example enables anti-ARP spoofing.

```
Orion_B54Q(config)#interface fastEthernet 0/1
Orion_B54Q(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

17.2 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

Global configuration mode

Mode

Usage Guide This command is used to display the anti-ARP spoofing configuration on all interfaces.

Configuration Examples The following example displays the anti-ARP-spoofing configuration on all interfaces.

```
Orion_B54Q#show anti-arp-spoofing
Fa0/NO    PORT       IP                STATUS
----- ---------- ---------------- ----------
1     Gi0/1      192.168.1.1      active
```

Field Description

Field	Description
NO	Port ID
PORT	Port name
IP	Gateway IP
STATUS	Anti-ARP spoofing status

Related Commands

Command	Description
anti-arp-spoofing ip	Configures anti-ARP spoofing.

Platform Description N/A

18 NFPP Commands

18.1 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 19999 in unit of pps.

Defaults

By default, the attack threshold for each source IP address and source MAC address is 3000pps; and the attack threshold for each port is 8000pps.

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.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# arp-guard attack-threshold per-src-ip 2
Orion_B54Q(config-nfpp)# arp-guard attack-threshold per-src-mac 3
Orion_B54Q(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

18.2 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.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(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

18.3 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.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(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

18.4 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.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# arp-guard isolate-forwarding enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

18.5 arp-guard monitored-host-limit

Use this command to set the maxmum 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 4294967295.

Defaults The default is 20000.

Command Mode NFPP configuration mode

Usage Guide If the monitored host number has reached the default 20000, the administrator shall set the max-number smaller than 20000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20000, 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 maxmum monitored host number to 200.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# arp-guard monitored-host-limit 200
```

Related Commands

Command	Description
show nfpp arp-guard summary	Displays the configuration.

Platform Description N/A

18.6 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 86400 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.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(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

18.7 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*

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

Parameter	Description
per-src-ip	Setsthe 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 19999

Defaults The default rate limit for each source IP address and MAC address is 30pps; the default rate limit for each port is 5000pps.

Command Mode NFPP configuration mode.

Usage Guide N/A

Configuration Examples The following example sets the arp guard rate limit.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# arp-guard rate-limit per-src-ip 2
Orion_B54Q(config-nfpp)# arp-guard rate-limit per-src-mac 3
Orion_B54Q(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

18.8 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..

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# arp-guard ratelimit-forwarding enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

18.9 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 19999.

Defaults The default scan threshold is 100.

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.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(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

18.10 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 Use this command without the parameter to clear all monitored hosts.

Configuration Examples The following example clears the monitored host isolation.

```
Orion_B54Q# clear nfpp arp-guard hosts vlan 1 interface g0/1
```

Related Commands

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 Description N/A

18.11 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

The following example clears ARP scanning table.

```
Orion_B54Q# clear nfpp arp-guard scan
```

Related Commands

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.

Platform Description

N/A

18.12 clear nfpp define *name* hosts

Use this command to clear the monitored hosts. If the host is isolated, you need to disisolate 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
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

The following example clears the monitored hosts.

```
Orion_B54Q# clear nfpp define tcp hosts vlan 1 interface g 0/1
```

Related Commands

Command	Description
show nfpp define hosts	Displays the isolated hosts.

Platform Description

N/A

18.13 clear nfpp dhcp-guard hosts

Use this command to clear the monitored host 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 The following example clears the monitored host isolation.

```
Orion_B54Q# clear nfpp dhcp-guard hosts vlan 1 interface g0/1
```

Related Commands

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

18.14 clear nfpp dhcpv6-guard hosts

Use this command to clear the 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 The following example clears the monitored host isolation.

```
Orion_B54Q# clear nfpp dhcpv6-guard hosts vlan 1 interface g0/1
```

Related Commands

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.

Platform Description N/A

18.15 clear nfpp icmp-guard hosts

Use this command to clear the monitored host isolation.

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 The following example clears the monitored host isolation.

```
Orion_B54Q# clear nfpp icmp-guard hosts vlan 1 interface g0/1
```

Related Commands

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.

Platform Description N/A

18.16 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.

```
Orion_B54Q# 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

18.17 clear nfpp nd-guard hosts

Use this command to remove the speed limit on the 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..

```
Orion_B54Q# clear nfpp nd-guard hosts vlan 1 interface g0/1
```

Prompt Messages

N/A

Platform Description

N/A

18.18 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

The following example clears the NFPP log buffer area.

```
Orion_B54Q# clear nfpp log
```

Related Commands

Command	Description
show nfpp log	Displays the NFPP log configuration or the log buffer area.

Platform Description

N/A

18.19 cpu-protect sub-interface { manage | protocol | route } percent

Use this command to configure the percent value of each type of packets occupied in the buffer area. Use the **no** or **default** form of this command to restore the default setting.

cpu-protect sub-interface { **manage** | **protocol** | **route** } **percent** *percent_vaule*

no cpu-protect sub-interface {*manage*|*protocol*|*route*} **percent**

default cpu-protect sub-interface {*manage*|*protocol*|*route*} **percent**

Parameter Description

Parameter	Description
percent_value	The percent value, in the range from 1 to 100.

Defaults

The default percent values of each type of packets occupied in the buffer area are:

Manage packets: 30;

Route packets: 20;

Protocol packets: 45.

Command Mode

Global configuration mode.

Usage Guide

N/A

Configuration Examples

The following example sets the percent value of management packets in the buffer area to 60.

```
Orion_B54Q(config)# cpu-protect sub-interface manage
percent 60
```

Related Commands

Command	Description
cpu-protect sub-interface { **manage** | **protoco**l | **route** } pps	Configures the traffic bandwidth of each type of packets.

Platform Description

N/A

18.20 cpu-protect sub-interface { manage | protocol | route } pps

Use this command to configure the traffic bandwidth of each type of packets. Use the **no** or **default** form of this command to restore the default setting.

cpu-protect sub-interface { **manage** | **protocol** | route} **pps** *pps_vaule*

no cpu-protect sub-interface { *manage* | *protocol* | *route* } **pps**

default cpu-protect sub-interface { *manage* | *protocol* | *route* } **pps**

Parameter Description

Parameter	Description
pps_value	The rate limit threshold, in the range from 1 to 8192

Defaults

The default traffic bandwidths of each type of packets are:

Manage packets: 3000pps;

Route packets: 3000pps;

Protocol packets: 3000pps.

Command Mode

Global configuration mode.

Usage Guide

N/A

Configuration Examples

The following example sets the traffic bandwidth of management packets to 2000 pps.

```
Orion_B54Q(config)# cpu-protect sub-interface manage pps 2000
```

Related Commands

Command	Description
cpu-protect sub-interface { **manage** | **protocol** | **route** } **percent**	Configures the percent value of each type of packets occupied in the buffer area.

Platform Description

N/A

18.21 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.

```
Orion_B54Q(config)# nfppOrion_B54Q(config-nfpp)# define tcp
Orion_B54Q(config-nfpp-define)#
```

Related Commands

Command	Description
show nfpp define summary	Displays the defined anti-attack configuration.

Platform Description

N/A

18.22 define 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.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)#define tcp enable
```

Related Commands

Command	Description
show nfpp define summary	Displays the user-defined anti-attack configuration

Platform Description N/A

18.23 dhcp-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.

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

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 19999.

Defaults The default settings are as follows:

For the 11.X CM supervisor module, the attack thresholds for each source MAC address and each port are 10 pps and 1500 pps respectively.

For the 11.X CMII supervisor module, the attack thresholds for each source MAC address and each port are 10 pps and 10000 pps respectively.

Command Mode

NFPP configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the global attack threshold.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# dhcp-guard attack-threshold per-src-mac 15
Orion_B54Q(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

18.24 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.

```
Orion_B54Q(config)# nfpp
```

```
Orion_B54Q(config-nfpp)# dhcp-guard enable
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

18.25 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 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 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.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(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

18.26 dhcp-guard monitored-host-limit

Use this command to set the maxmum 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 4294967295.

Defaults The default is 20000.

Command Mode NFPP configuration mode

Usage Guide If the monitored host number has reached the default 20000, the administrator shall set the max-number smaller than 20000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20000, 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 maxmum monitored host number to 200.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# dhcp-guard monitored-host-limit 200
```

Related Commands

Command	Description
show nfpp dhcp-guard summary	Displays the configuration.

Platform Description N/A

18.27 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 86400 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 monitor time to 180 seconds.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(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

18.28 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 19999

Defaults The default settings are as follows:

For the 11.X CM supervisor module, the rate-limit thresholds for each source MAC address and each port are 5 pps and 1200 pps respectively.
For the 11.X CMII supervisor module, the rate-limit thresholds for each source MAC address and each port are 5 pps and 8000 pps respectively.

Command Mode NFPP configuration mode.

Usage Guide N/A

Configuration Examples The following example sets the rate-limit threshold globally.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# dhcp-guard rate-limit per-src-mac 8
Orion_B54Q(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

18.29 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 19999 pps.

Defaults The default settings are as follows:
For the 11.X CM supervisor module, the attack thresholds for each source MAC address and each port are 10 pps and 1500 pps respectively.
For the 11.X CMII supervisor module, the attack thresholds for each source MAC address and each port are 10 pps and 10000 pps respectively.

Command Mode NFPP configuration mode.

Usage Guide N/A.

Configuration Examples The following example sets the global attack threshold.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# dhcpv6-guard attack-threshold per-src-mac 15
Orion_B54Q(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

18.30 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.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# dhcpv6-guard enable
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

18.31 dhcpv6-guard monitored-host-limit

Use this command to set the maxmum 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 4294967295.

Defaults The default is 20000

Command Mode NFPP configuration mode

Usage Guide If the monitored host number has reached the default 20000, the administrator shall set the max-number smaller than 20000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20000, 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 maxmum monitored host number to200.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# dhcpv6-guard monitored-host-limit 200
```

Related Commands

Command	**Description**
show nfpp dhcpv6-guard summary	Displays the cconfiguration.

Platform Description N/A

18.32 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 86400 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 monitor time to 180 seconds.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(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

18.33 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 19999.

Defaults

The default settings are as follows:
For the 11.X CM supervisor module, the rate-limit thresholds for each source MAC address and each port are 5 pps and 1200 pps respectively.
For the 11.X CMII supervisor module, the rate-limit thresholds for each source MAC address and each port are 5 pps and 8000 pps respectively.

Command Mode

NFPP configuration mode

Usage Guide

N/A

Configuration Examples

The following example sets the rate-limit threshold globally.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# dhcpv6-guard rate-limit per-src-mac 8
Orion_B54Q(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

18.34 global-policy

Use this command to set the rate-limit threshold and attack threshold based on the host or port. 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

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

N/A

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.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# nfpp define tcp
Orion_B54Q(config-nfpp-define)# global-policy per-src-ip 10  20
Orion_B54Q(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

18.35 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 19999 in the unit of pps.

Defaults

The default settings are as follows:

For the 11.X CM supervisor module, the attack thresholds for each source IP address and each port are 2000 pps and 4000 pps respectively.

For the 11.X CMII supervisor module, the attack thresholds for each IP MAC address and each port are 2500 pps and 4500 pps respectively.

Command Mode

NFPP configuration mode.

Usage Guide

N/A.

Configuration Examples

The following example sets the global attack threshold.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# icmp-guard attack-threshold per-src-ip 600
Orion_B54Q(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

18.36 icmp-guard enable

Use this command to enable the ICMP anti-attack function.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

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.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# icmp-guard enable
```

Related

Command	Description

Commands

nffp icmp-guard enable	Enables the ICMP anti-attack function on the interface.
show nfpp icmp-guard summary	Displays the configuration.

Platform Description

N/A

18.37 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 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

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.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(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

18.38 icmp-guard monitored-host-limit

Use this command to set the maxmum 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 4294967295.

Defaults The default is 20000.

Command Mode NFPP configuration mode

Usage Guide If the monitored host number has reached the default 20000, the administrator shall set the max-number smaller than 20000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20000, 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 maxmum monitored host number to 200.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# icmp-guard monitored-host-limit 200
```

Related Commands

Command	Description
show nfpp icmp-guard summary	Displays the configuration.

Platform Description N/A

18.39 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 86400 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.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(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

18.40 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 to19999.

Defaults The default settings are as follows:

For the 11.X CM supervisor module, the rate-limit thresholds for each source IP address and each port are 2000 pps and 4000 pps respectively.

For the 11.X CMII supervisor module, the rate-limit thresholds for each IP MAC address and each port are 2500 pps and 4500 pps respectively.

Command Mode NFPP configuration mode.

Usage Guide N/A

Configuration Examples The following example sets the rate-limit threshold globally.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# icmp-guard rate-limit per-src-ip 500
Orion_B54Q(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

18.41 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.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(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

18.42 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 19999.

Defaults

By default, the attack threshold for each source IP address and each port are 200pps and 400pps respectively.

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.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# ip-guard attack-threshold per-src-ip 2
Orion_B54Q(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

18.43 ip-guard enable

Use this command to enable the IP anti-scanfunction.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 N/A

Configuration Examples The following example enables the IP anti-scan function globally.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# ip-guard enable
```

Related Commands

Command	Description
nffp ip-guard enable	Enables the IP anti-scan function on the interface.

Platform Description N/A

18.44 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

Parameter	Description

Description

seconds	Sets the isolate time. The value is 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 isolate time globally to 180 seconds.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(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

18.45 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 86400 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 monitor time to 180 seconds.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(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

18.46 ip-guard monitored-host-limit

Use this command to set the maxmum 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 4294967295.

Defaults

The default is 20000.

Command Mode

NFPP configuration mode

Usage Guide

If the monitored host number has reached the default 20000, the administrator shall set the max-number smaller than 20000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20000, 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 maxmum monitored host number to 200.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# ip-guard monitored-host-limit 200
```

Related Commands

Command	Description
show nfpp ip-guard summary	Displays the configuration.

Platform Description

N/A

18.47 ip-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.

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

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 19999

Defaults

By default, the the rate-limit threshold for each source IP address and each port is 20pps and 100pps respectively.

Command Mode

NFPP configuration mode.

Usage Guide

N/A

Configuration Examples

The following example sets the rate-limit threshold globally.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# ip-guard rate-limit per-src-ip 2
Orion_B54Q(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

18.48 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 19999.

Defaults The default scan threshold is 100, in 10 seconds.

Command Mode NFPP configuration mode.

Usage Guide N/A

Configuration Examples The following example sets the global scan threshold to 20pps.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(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

18.49 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 from 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.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(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

18.50 log-buffer enable

Use this command to display logs on the screen. Use the **no** form of this command to store logs in the cache, instead of being displayed 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.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# log-buffer enable
```

Related Commands

Command	Description

N/A	N/A

Platform Description N/A

18.51 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 1024.

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.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(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

18.52 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.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(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

18.53 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

Parameter	Description

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.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# logging vlan 1-3,5
```

The following example records the logs on the interface GigabitEthernet 0/1 only.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# logging interface G 0/1
```

Related Commands

Command	Description
show nfpp log summary	Displays the NFPP log configuration or the log buffer area.

Platform Description N/A

18.54 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 fileds to be matched.

Configuration Examples The following example specifies the message matching filed for the user-defined anti-attack.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# nfpp define tcp
Orion_B54Q(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

18.55 monitored-host-limit

Use this command to set the maxmum 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 4294967295.

Defaults The default is 20000.

Command NFPP define configuration mode

Mode

Usage Guide If the monitored host number has reached the default 20000, the administrator shall set the max-number smaller than 20000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20000, 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 20000 monitored hosts. to remind the administrator

Configuration Examples The following example sets the maxmum monitored host number.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# nfpp define tcp
Orion_B54Q(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

18.56 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 86400 in the unit of seconds.

Defaults The default is 600.

Command Mode NFPP define 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 monitoring time to 1000 seconds.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# define tcp
Orion_B54Q(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

18.57 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

By default, the default attack threshold for the ns-na, rs and ra-redirect on each port is 5000, 1000 and 1000 respectively.

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.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# nd-guard attack-threshold per-port ns-na 20
Orion_B54Q(config-nfpp)# nd-guard attack-threshold per-port rs 10
Orion_B54Q(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

18.58 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.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(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

18.59 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 19999 in the unit of pps.

Defaults By default, the default rate-limit thresholds for the ns-na, rs and ra-redirect on each port are 2000, 500 and 500 respectively.

Command Mode NFPP configuration mode.

Usage Guide N/A

Configuration Examples The following example sets the rate-limit threshold globally.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# nd-guard rate-limit per-port ns-na 10
Orion_B54Q(config-nfpp)# nd-guard rate-limit per-port rs 5
Orion_B54Q(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

18.60 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

Parameter	Description

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.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# nd-guard ratelimit-forwarding enable
```

Platform Description N/A

18.61 nfpp

Use this command to enter NFPP configuration mode.

nfpp

Parameter Description

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

```
Orion_B54Q(config)# nfpp
```

Platform Description N/A

18.62 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.

```
Orion_B54Q(config)# interface G0/1
Orion_B54Q(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

18.63 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.

nfpp arp-guard isolate-period { **seconds** | **permanent** }

no nfpp arp-guard isolate-period

default nfpp arp-guard isolate-period

Parameter Description

Parameter	Description
seconds	Sets the isolate period. The value is 0, or in the range from 30 to 86400 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.

```
Orion_B54Q(config)# interface G0/1
```

```
Orion_B54Q(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

18.64 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.

```
Orion_B54Q(config)# interface G 0/1
Orion_B54Q(config-if)# nfpp arp-guard policy per-src-ip 2 10
Orion_B54Q(config-if)# nfpp arp-guard policy per-src-mac 3 10
Orion_B54Q(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

18.65 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 19999.

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.

```
Orion_B54Q(config)# interface G 0/1
Orion_B54Q(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

18.66 nfpp define 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.

```
Orion_B54Q(config)# interface G0/1
Orion_B54Q(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

18.67 nfpp define isolate-period

Use this command to set the local isolate period in the interface configuration mode.

nfpp define *name* **isolate-period** { *seconds* | **permanent** }

Parameter Description

Parameter	Description
seconds	Sets the isolate period, in second. The valid range is 0, or [30, 86400]. 0 indicates no isolation.
name	Name of the user-defined anti-attack type.
permanent	Permanent isolation.

Defaults By default, the local isolate period is not configured. The global isolate period is used.

Command Mode Interface configuration mode.

Usage Guide N/A

Configuratio The following example shows how to set the local isolate period in the interface configuration mode.

n Examples

```
Orion_B54Q(config)# interface G 0/1
Orion_B54Q(config-if)# nfpp define tcp isolate-period 180
```

Related Commands

Command	Description
isolate-period	Sets the global isolate period.
show nfpp define summary	Displays the configurations.

Platform Description

N/A

18.68 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 19999.
attack-threshold-pps	Sets the attack threshold, in the range of 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 local rate-limit threshold and the attack threshold.

```
Orion_B54Q(config)# interface G 0/1
Orion_B54Q(config-if)# nfpp define tcp policy per-src-ip 2 10
Orion_B54Q(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

18.69 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.

```
Orion_B54Q(config)# interface G0/1
Orion_B54Q(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

18.70 nfpp dhcp-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 dhcp-guard isolate-period { *seconds* | **permanent** }

no nfpp dhcp-guard isolate-period

default nfpp dhcp-guard isolate-period

Parameter Description

Parameter	Description
seconds	Sets the isolate period. The value is 0 or in the range from 30 to

	86400 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 to 180 seconds.

```
Orion_B54Q(config)# interface G0/1
Orion_B54Q(config-if)# nfpp dhcp-guard isolate-period 180
```

Related Commands

Command	Description
dhcp-guard isolate-period	Sets the global isolate period.
show nfpp dhcp-guard summary	Displays the configuration.

Platform Description N/A

18.71 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 19999.
attack-threshold-pps	Sets the attack threshold, in the range from1 to 19999.

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.

```
Orion_B54Q(config)#interface G 0/1
Orion_B54Q(config-if)# nfpp dhcpv6-guard policy per-src-mac 3 10
Orion_B54Q(config-if)# nfpp dhcpv6-guard policy per-port 50 100
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

18.72 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.

```
Orion_B54Q(config)# interface G0/1
Orion_B54Q(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

18.73 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 19999.
attack-threshold-pps	Sets the attack threshold, in the range from1 to19999.

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.

```
Orion_B54Q(config)# interface G 0/1
Orion_B54Q(config-if)# nfpp dhcpv6-guard policy per-src-mac 3 10
Orion_B54Q(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

18.74 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.

```
Orion_B54Q(config)# interface G0/1
Orion_B54Q(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

18.75 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.

nfpp icmp-guard isolate-period { *seconds* | **permanent** }

no nfpp icmp-guard isolate-period

default nfpp icmp-guard isolate-period

Parameter Description

Parameter	Description
seconds	Sets the isolate period. The value is 0 or in the range from 30 to 86400 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

Configuratio The following example sets the isolate period in the interface configuration mode.

n Examples

```
Orion_B54Q(config)# interface G0/1
Orion_B54Q(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

18.76 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 19999.
attack-threshold-pps	Sets the attack threshold, in 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.

```
Orion_B54Q(config)# interface G 0/1
Orion_B54Q(config-if)# nfpp icmp-guard policy per-src-ip 5 10
Orion_B54Q(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

18.77 nfpp ip-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 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-scan function is not enabled on the interface.

Command Mode Interface configuration mode.

Usage Guide The interface IP anti-scan configuration is prior to the global configuration.

Configuration Examples The following example enables the ICMP anti-attack function on the interface.

```
Orion_B54Q(config)# interface G0/1
Orion_B54Q(config-if)# nfpp ip-guard enable
```

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

18.78 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

Parameter	Description

Description

seconds	Sets the isolate period, in the range from 30 to 86400 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.

```
Orion_B54Q(config)# interface G0/1
Orion_B54Q(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

18.79 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 19999.
attack-threshold-pps	Sets the attack threshold, in the range from 1 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.

```
Orion_B54Q(config)# interface G 0/1
Orion_B54Q(config-if)# nfpp ip-guard policy per-src-ip 2 10
Orion_B54Q(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

18.80 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 19999.

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.

```
Orion_B54Q(config)# interface G 0/1
Orion_B54Q(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

N/A

Description

18.81 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 not enabled on the interface.

Command Mode Interface configuration mode.

Usage Guide The interface ND anti-attack configuration is prior to the global configuration.

Configuration Examples The following example enables the ND anti-attack function on the interface.

```
Orion_B54Q(config)# interface G0/1
Orion_B54Q(config-if)# nfpp nd-guard enable
```

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

18.82 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 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.

```
Orion_B54Q(config)# interface G 0/1
Orion_B54Q(config-if)# nfpp nd-guard policy per-port ns-na 50 100
Orion_B54Q(config-if)# nfpp nd-guard policy per-port rs 10 20
Orion_B54Q(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

18.83 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.

```
Orion_B54Q# show nfpp arp-guard hosts statistics
success    fail    total
-------    ----    -----
100         20        120

The following example shows the monitored host:
Orion_B54Q# show nfpp arp-guard hosts
If column 1 shows '*', it means "hardware do not isolate user" .
VLAN  interface IP address   MAC address   remain-time(s)
----  --------   ---------   -----------   -------------
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 host.

Platform Description N/A

18.84 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.

```
Orion_B54Q# show nfpp arp-guard scan statistics
arp-guard table has 4 record(s).

Orion_B54Q# show nfpp arp-guard scan
VLAN    interface   IP address   MAC address    timestamp
----    --------   ----------  -----------     ---------
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   2008-01-23 16:25:10
4        Gi0/4       -           0000.0000.0004   2008-01-23 16:26:10
Total:4 record(s)

Orion_B54Q# 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)
```

Related Commands

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.

Platform Description

N/A

18.85 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

Configuratio

The following example displays the configuration.

n Examples

```
Orion_B54Q# 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 monitored hosts: 1000
Monitor period:300s
```

Field Description:

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.
-	No configuration.

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

18.86 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*]]]

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.

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.

```
Orion_B54Q#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

18.87 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 Mode Privileged EXEC 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 The following example displays the configuration.

```
Orion_B54Q#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.

Related Commands

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

Platform Description N/A

18.88 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.

```
Orion_B54Q# 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
Total:2 record(s)
```

Related Commands

Command	Description
trusted-host	Configures the trusted hosts.

Platform Description N/A

18.89 show nfpp dhcp-guard hosts

Use this command to display the monitored host.

show nfpp dhcp-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.

```
Orion_B54Q# show nfpp dhcp-guard hosts statistics
```

```
success    fail    total
-------    ----    -----
100         20        120

The following example shows the monitored host:
Orion_B54Q# 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      0000.0000.0001   10
 *2    gi0/1      0000.0000.0002   20
Total:2 host(s)
```

Related Commands

Command	Description
clear nfpp dhcp-guard hosts	Clears the monitored host.

Platform Description

N/A

18.90 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.

```
Orion_B54Q# 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

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.
-	No configuration.

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

18.91 show nfpp dhcpv6-guard hosts

Use this command to display the monitored host.

show nfpp dhcpv6-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.

```
Orion_B54Q# show nfpp dhcpv6-guard hosts
If column 1 shows '*', it means "hardware failed to isolate host".
VLAN  interface   MAC address    remain-time(seconds)
----     ---------    -----------         -------------------
 *1     gi0/2      0000.0000.0001   10
 *2    gi0/1      0000.0000.0002   20
Total:2 host(s)
```

Related Commands

Command	Description
clear nfpp dhcpv6-guard hosts	Clears the monitored host.

Platform Description N/A

18.92 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 Examples The following example displays the configuration.

```
Orion_B54Q#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.
-	No configuration.

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

18.93 show nfpp icmp-guard hosts

Use this command to display the monitored host.

show nfpp icmp-guard hosts [**statistics** | [[*vlan vid*] [**interfac**e *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.

```
Orion_B54Q# show nfpp icmp-guard hosts statistics
success    fail    total
-------    ----    -----
100         20        120
```

The following example displays the monitored host.

```
Orion_B54Q# show nfpp icmp-guard hosts
If column 1 shows '*', it means "hardware failed to isolate host".
VLAN  interface IP address      remain-time(s)
----    --------   ---------          -------------
1      Gi0/1       1.1.1.1      110
2      Gi0/2       1.1.2.1      61
Total:2 host(s)
```

Related Commands

Command	Description
clear nfpp icmp-guard hosts	Clears the monitored host.

Platform Description N/A

18.94 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 Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example displays the configuration.

```
Orion_B54Q# 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.
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.
-	No configuration.

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

18.95 show nfpp icmp-guard trusted-host

Use this command to display the trusted host free from being monitored.

show nfpp icmp-guard summary

Parameter

Parameter	**Description**

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.

```
Orion_B54Q# 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
Total:2 record(s)
```

Related Commands

Command	Description
icmp-guard trusted-host	Sets the trusted host.

Platform Description N/A

18.96 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* | 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.

```
Orion_B54Q# show nfpp ip-guard hosts statistics
success    fail    total
-------    ----    -----
100         20        120

Orion_B54Q#show nfpp ip-guard hosts
If column 1 shows '*', it means "hardware do not isolate host" .
VLAN  interface IP address   Reason      remain-time(s)
----  --------   ---------   -------      -------------
1      Gi0/1       1.1.1.1      ATTACK      110
2      Gi0/2       1.1.2.1      SCAN          61
Total:2 host(s)
```

Related Commands

Command	Description
clear nfpp ip-guard hosts	Clears the monitored host.

Platform Description

N/A

18.97 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.

```
Orion_B54Q# 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.
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.
-	No configuration.

Related Commands

Command	**Description**
ip-guard attack-threshold	Sets the global attack threshold.
ip-guard enable	Enables the IP anti-scan 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-scan 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

18.98 show nfpp ip-guard trusted-host

Use this command to display the trusted host free from being monitored.

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 trusted host free from being monitored.

```
Orion_B54Q# 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

18.99 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.

```
Orion_B54Q#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.

```
Orion_B54Q#show nfpp log buffer statistics
There are 6 logs in buffer.

The following example shows the NFPP log buffer area:
Orion_B54Q#show nfpp log buffer
Protocol VLAN  Interface IP address MAC address     Reason
Timestamp
------- ----  --------   ---------  -----------     ------
---------
ARP    1      Gi0/1       1.1.1.1      -       DoS              2009-05-30
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  SCAN
2009-05-30 16:30:10
ARP    -      Gi0/2       -          -           PORT_ATTACKED   2009-05-
30 16:30:10
```

Field	Description
Protocol	ARP, IP, ICMP, DHCP,DHCPv6, NS-NA, RS, RA-REDIRECT
Reason	1. DoS 2. ISOLATED 3. ISOLATE_FAILE 4. SCAN 5. PORT_ATTACKED

Related Commands

Command	Description
clear nfpp log	Clears the NFPP log buffer area.

Platform Description N/A

18.100 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.

```
Orion_B54Q#show nfpp nd-guard hosts statistics
success    fail    total
-------    ----    -----
10         2        12

The following example displays the host monitored by ND-guard. The “remian-
time(s)” refers to the remaining time of isolation.
Orion_B54Q#show nfpp nd-guard hosts
If col_filter 1 shows '*', it means "hardware do not isolate host".
 VLAN    interface   ND-guard            remain-time(s)
 ----    ---------   --------            --------------
 -       Gi4/2       ns-na-guard         174
 -       Gi4/2       rs-guard            98
 -       Gi4/2       ra-redirect-guard   127
Total: 3 hosts
```

Prompt Messages

N/A

Platform Description

N/A

18.101 show nfpp nd-guard summary

Use this command to display the configuration.

show nfpp nd-guard summary

Parameter

Parameter	Description

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.

```
Orion_B54Q# 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
```

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.
-	No configuration.

Related Commands

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 threshold.

Platform Description N/A

18.102 trusted-host

Use this command to set the trusted hosts free form monitoring. Use the no form of this command to restore the default setting,

trusted-host { *mac mac_mask* | *ip mask* | *IPv6/prefixlen* }

no trusted-host { **all** | *ip mask* | *IPv6/prefixlen* }

Parameter Description

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 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.

```
Orion_B54Q(config)# nfpp
Orion_B54Q(config-nfpp)# define tcp
Orion_B54Q(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

19 DoS Protection Commands

19.1 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 The following example enables the anti-attack of the self-consumption:

```
Orion_B54Q(config)# ip deny invalid-l4port
```

The following example disables the anti-attack of the self-consumption:

```
Orion_B54Q(config)# no ip deny invalid-l4port
```

Related Commands

Command	Description
show ip deny invalid-l4port	Displays the state of anti-attack of the self-consumption.

Platform Description N/A

19.2 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 The following example enables the anti-attack of the invalid TCP packets:

```
Orion_B54Q(config)# ip deny invalid-tcp
```

The following example disables the anti-attack of the invalid TCP packets:

```
Orion_B54Q(config)# no ip deny invalid-tcp
```

Related Commands

Command	Description
show ip deny invalid-tcp	Displays the state of anti-attack of the invalid TCP packets.

Platform Description N/A

19.3 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 Examples The following example enables the anti-land-attack:

```
Orion_B54Q(config)# ip deny land
```

The following example disables the anti-land-attack:

```
Orion_B54Q(config)# no ip deny land
```

Related Commands

Command	Description
show ip deny land	Displays the anti-land-attack state.

Platform Description N/A

19.4 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.

```
Orion_B54Q#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

19.5 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.

```
Orion_B54Q# 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

19.6 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.

```
Orion_B54Q# show ip deny invalid-tcp
DoS Protection Mode                            State
-------------------------------------      -----
protect against invalid tcp attack          On
```

Related Commands

Command	Description
ip deny invalid-tcp	Enables the anti-attack of the invalid TCP packets.

Platform Description N/A

19.7 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.

```
Orion_B54Q# show ip deny land
DoS Protection Mode                State
------------------------------  -----
protect against land attack       On
```

Related Commands

Command	Description
no ip deny land	Enables the anti-land-attack function.

Platform Description N/A