1 NFPP Commands

Command	Function
all-guard enable	Enable all the basic types of global guard of Network Foundation Protection Policy (NFPP).
arp-guard attack-threshold	Configure the global attack threshold of ARP guard.
arp-guard enable	Enable the function of global ARP guard.
arp-guard isolate-forwarding enable	Enable the function of global isolation forwarding of ARP guard.
arp-guard isolate-period	Configure the global isolation time of ARP guard.
arp-guard monitored-host-limit	Configure the maximum number of monitored hosts of ARP guard in global configuration mode.
arp-guard monitor-period	Configure the monitoring time of ARP guard.
arp-guard rate-limit	Configure the global rate limiting threshold of ARP guard.
arp-guard ratelimit-forwarding enable	Enable the function of port-based rate limit forwarding of ARP guard.
arp-guard scan-threshold	Configure the global scanning threshold of ARP guard.
clear nfpp arp-guard hosts	Clear the monitored hosts of ARP guard.
clear nfpp arp-guard scan	Clear the scanning table of ARP guard.
clear nfpp define hosts	Clear the monitored hosts of the customized guard type.
clear nfpp dhcp-guard hosts	Clear the monitored hosts of DHCP guard.
clear nfpp dhcpv6-guard hosts	Clear the monitored hosts of DHCPv6 guard.
clear nfpp icmp-guard hosts	Clear the monitored hosts of ICMP guard.
clear nfpp ip-guard hosts	Clear the monitored hosts of IP guard.
clear nfpp log	Clear the log buffer of NFPP.
clear nfpp nd-guard hosts	Clear the monitored hosts of ND guard.
clear nfpp tcp-syn-guard hosts	Clear the monitored hosts of TCP-SYN guard.

define	Customize a guard type and enter the customized guard configuration mode of NFPP.
define enable	Enable the function of global customized guard.
dhcp-guard attack-threshold	Configure the global attack threshold of DHCP guard.
dhcp-guard enable	Enable the function of global DHCP guard.
dhcp-guard isolate-period	Configure the global isolation time of DHCP guard.
dhcp-guard monitored-host-limit	Configure the maximum number of monitored hosts of DHCP guard.
dhcp-guard monitor-period	Configure the monitoring time of DHCP guard.
dhcp-guard rate-limit	Configure the global rate limiting threshold of DHCP guard.
dhcpv6-guard attack-threshold	Configure the global attack threshold of DHCPv6 guard.
dhcpv6-guard enable	Enable the DHCPv6 guard function.
dhcpv6-guard monitored-host-limit	Configure the maximum number of monitored hosts of DHCPv6 guard.
dhcpv6-guard monitor-period	Configure the monitoring time of DHCPv6 guard.
dhcpv6-guard rate-limit	Configure the global rate limiting threshold of DHCPv6 guard.
global-policy	Configure the global rate limiting threshold and global attack threshold of the customized guard type.
icmp-guard attack-threshold	Configure the global attack threshold of ICMP guard.
icmp-guard enable	Enable the function of global ICMP guard.
icmp-guard isolate-period	Configure the global isolation time of ICMP guard.
icmp-guard monitored-host-limit	Configure the maximum number of monitored hosts of ICMP guard.
icmp-guard monitor-period	Configure the monitoring time of ICMP guard.
icmp-guard rate-limit	Configure the global rate limiting threshold of ICMP guard.
icmp-guard trusted-host	Configure the trusted hosts of ICMP guard.
ip-guard attack-threshold	Configure the global attack threshold of IP guard.

nfpp arp-guard scan-threshold	Configure the scanning threshold of ARP guard on an interface.
nfpp define enable	Enable the customized guard function on an interface.
nfpp define policy	Configure a local rate limiting threshold and a local attack threshold of customized guard on an interface.
nfpp dhcp-guard enable	Enable the DHCP guard function on an interface.
nfpp dhcp-guard isolate-period	Configure the local isolation time of DHCP guard on an interface.
nfpp dhcp-guard policy	Configure a local rate limiting threshold and a local attack threshold of DHCP guard on an interface.
nfpp dhcpv6-guard enable	Enable the DHCPv6 guard function on an interface.
nfpp dhcpv6-guard policy	Configure a local rate limiting threshold and a local attack threshold of DHCPv6 guard on an interface.
nfpp icmp-guard enable	Enable the ICMP guard function on an interface.
nfpp icmp-guard isolate-period	Configure the local isolation time of ICMP guard on an interface.
nfpp icmp-guard policy	Configure a local rate limiting threshold and a local attack threshold of ICMP guard on an interface.
nfpp ip-guard enable	Enable the IP guard function on an interface.
nfpp ip-guard isolate-period	Configure the local isolation time of IP guard on an interface.
nfpp ip-guard policy	Configure a local rate limiting threshold and a local attack threshold of IP guard on an interface.
nfpp ip-guard scan-threshold	Configure the local scanning threshold of IP guard on an interface.
nfpp nd-guard enable	Enable the ND guard function on an interface.
nfpp nd-guard policy per-port	Configure a local rate limiting threshold and a local attack threshold of ND guard on an interface.
nfpp tcp-syn-guard enable	Enable the TCP-SYN guard function on an interface.
nfpp tcp-syn-guard isolate-period	Configure the local isolation time of TCP-SYN guard on an interface.

nfpp tcp-syn-guard policy	Configure a local rate limiting threshold and a local attack threshold of TCP-SYN guard on an interface.
show nfpp arp-guard hosts	Display the monitored hosts of ARP guard.
show nfpp arp-guard scan	Display the scanning table of ARP guard.
show nfpp arp-guard summary	Display the configuration information of ARP guard.
show nfpp define hosts	Display the monitored hosts of a customized guard type.
show nfpp define summary	Display the configuration information of a customized summary type.
show nfpp define trusted-host	Display the trusted hosts of a customized guard type.
show nfpp dhcp-guard hosts	Display the monitored hosts of DHCP guard.
show nfpp dhcp-guard summary	Display the configuration information of DHCP guard.
show nfpp dhcpv6-guard hosts	Display the monitored hosts of DHCPv6 guard.
show nfpp dhcpv6-guard summary	Display the configuration information of DHCPv6 guard.
show nfpp icmp-guard hosts	Display the monitored hosts of ICMP guard.
show nfpp icmp-guard summary	Display the configuration information of ICMP guard.
show nfpp icmp-guard trusted-host	Display the trusted hosts of ICMP guard.
show nfpp ip-guard hosts	Display the monitored hosts of IP guard.
show nfpp ip-guard summary	Display the configuration information of IP guard.
show nfpp ip-guard trusted-host	Display the trusted hosts of IP guard.
show nfpp log buffer	Display the information in the log buffer of NFPP.
show nfpp log buffer statistics	Display the statistics about the log buffer of NFPP.
show nfpp log summary	Display the configuration information of NFPP logs.
show nfpp nd-guard hosts	Display the monitored hosts of ND guard.
show nfpp nd-guard summary	Display the configuration information of ND guard.
show nfpp tcp-syn-guard hosts	Display the monitored hosts of TCP-SYN guard.
show nfpp tcp-syn-guard summary	Display the configuration information of TCP-SYN guard.

show nfpp tcp-syn-guard trusted-host	Display the trusted hosts of TCP-SYN guard.
tcp-syn-guard attack-threshold	Configure the global attack threshold of TCP-SYN guard.
tcp-syn-guard enable	Enable the global TCP-SYN guard function.
tcp-syn-guard isolate-period	Configure the global isolation time of TCP-SYN guard.
tcp-syn-guard monitored-host-limit	Configure the maximum number of monitored hosts of TCP-SYN guard.
tcp-syn-guard monitor-period	Configure the monitoring time of TCP-SYN guard.
tcp-syn-guard rate-limit	Configure the global rate limiting threshold of TCP-SYN guard.
tcp-syn-guard trusted-host	Configure the trusted hosts of TCP-SYN guard.
trusted-host	Configure trusted hosts of a customized guard type.

1.1 all-guard enable

Function

Run the **all-guard enable** command to enable all the basic types of global guard of Network Foundation Protection Policy (NFPP).

Run the **no** form of this command to disable this feature.

Syntax

all-guard enable

no all-guard enable

Parameter Description

N/A

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

The preceding two commands cannot be displayed by running the **show running-config** command.

This global disabling/enabling command is supported on the basic types of global guard, including ARP guard, ICMP guard, TCP-SYN guard, DHCP guard, DHCPv6 guard, and ND guard.

This command is not supported on global customized guard types and does not affect the enabling status of the guard type in interface configuration mode.

This command cannot be saved, but its running result can be saved and take effect after device restart.

If you have configured the function of ARP source suppression and the isolation time for the IP guard function in global or interface configuration mode, an error is reported when you enable the IP guard function.

Examples

The following example disables all the basic types of global guard.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# no all-guard enable
```

Notifications

If you have configured the function of ARP source suppression, the following notification will be displayed when you configure isolation time for IP guard:

```
Configuration is prohibited, please disable the arp-guard suppression function
first!
```

Common Errors

N/A

Related Commands

N/A

1.2 arp-guard attack-threshold

Function

Run the **arp-guard attack-threshold** command to configure the global attack threshold of ARP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the global attack threshold of ARP guard for each interface is 200 pps, for each source IP address is 100 pps, and for each source MAC address is 100 pps.

Syntax

arp-guard attack-threshold { **per-port** *attack-threshold* | **per-src-ip** *attack-threshold* | **per-src-mac** *attack-threshold* }

no arp-guard attack-threshold { **per-port** | **per-src-ip** | **per-src-mac** }

default arp-guard attack-threshold { **per-port** | **per-src-ip** | **per-src-mac** }

Parameter Description

per-port *attack-threshold*: Configures an attack threshold for each interface, in pps. The value range is from 1 to 19999.

per-src-ip *attack-threshold*: Configures an attack threshold for each source IP address, in pps. The value range is from 1 to 19999.

per-src-mac *attack-threshold*: Configures an attack threshold for each source MAC address, in pps. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When packets are sent at a rate higher than the attack threshold, an attack occurs. The attack threshold must be equal to or greater than the rate limiting threshold.

Examples

The following example sets the global attack thresholds of ARP guard to **50** pps, **2** pps, and **3** pps for each interface, source IP address, and source MAC address respectively.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard attack-threshold per-port 50
Hostname(config-nfpp)# arp-guard attack-threshold per-src-ip 2
Hostname(config-nfpp)# arp-guard attack-threshold per-src-mac 3
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 arp-guard enable

Function

Run the **arp-guard enable** command to enable the function of global ARP guard.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The function of global ARP guard is enabled by default.

Syntax

arp-guard enable

no arp-guard enable

default arp-guard enable

Parameter Description

N/A

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of global ARP guard.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 arp-guard isolate-forwarding enable

Function

Run the **arp-guard isolate-forwarding enable** command to enable the function of global isolation forwarding of ARP guard.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The function of global isolation forwarding of ARP guard is enabled by default.

Syntax

arp-guard isolate-forwarding enable

no arp-guard isolate-forwarding enable

default arp-guard isolate-forwarding enable

Parameter Description

N/A

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of global isolation forwarding of ARP guard.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard isolate-forwarding enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 arp-guard isolate-period

Function

Run the **arp-guard isolate-period** command to configure the global isolation time of ARP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default global isolation time of ARP guard is **0**.

Syntax

arp-guard isolate-period { *interval* | **permanent** }

no arp-guard isolate-period

default arp-guard isolate-period

Parameter Description

interval: Isolation time, in seconds. The value is **0** or the value range is from 30 to 86400. The value **0** specifies no isolation.

permanent: Configures permanent isolation.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the global isolation time of ARP guard to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard isolate-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 arp-guard monitored-host-limit

Function

Run the **arp-guard monitored-host-limit** command to configure the maximum number of monitored hosts of ARP guard in global configuration mode.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum number of monitored hosts of ARP guard in global configuration mode is **20000** by default.

Syntax

arp-guard monitored-host-limit *limit-number*

no arp-guard monitored-host-limit

default arp-guard monitored-host-limit

Parameter Description

limit-number: Maximum number of monitored hosts. The value range is from 1 to 4294967295.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When the number of monitored hosts reaches the default value **20000**, the monitored hosts are not automatically deleted if the administrator sets the maximum number of monitored hosts to a value smaller than

20000. An alarm message "%ERROR: The value that you configured is smaller than current monitored hosts 20000 (number of monitored hosts), please clear a part of monitored hosts." is printed to remind users of configuration failure and the need to clear some monitored hosts.

When the table of monitored hosts is full, the log "% NFPP_ARP_GUARD-SESSION_LIMIT: Attempt to exceed limit of ARP 20000 (number of monitored hosts) monitored hosts." is printed to remind the administrator.

Examples

The following example sets the maximum number of monitored hosts of ARP guard in global configuration mode to **200**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard monitored-host-limit 200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 arp-guard monitor-period

Function

Run the **arp-guard monitor-period** command to configure the monitoring time of ARP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default monitoring time of ARP guard is **600** seconds.

Syntax

arp-guard monitor-period *interval*

no arp-guard monitor-period

default arp-guard monitor-period

Parameter Description

interval: Monitoring time, in seconds. The value range is from 180 to 86400.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When an attacker is detected, if the isolation time is 0, the attacker is monitored through software and the timeout time is the monitoring time. During software monitoring, when the isolation time is configured as a non-zero value, this function automatically isolates the attacker under software monitoring and the timeout time is configured as the isolation time. The monitoring time takes effect when the isolation time is 0.

If you change the isolation time to 0 from a non-zero value, the isolated attacker is directly deleted without monitoring the attacker through software.

Examples

The following example sets the monitoring time of ARP guard to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard monitor-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 arp-guard rate-limit

Function

Run the **arp-guard rate-limit** command to configure the global rate limiting threshold of ARP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the global rate limiting threshold of ARP guard for each interface is 128 pps, for each source IP address is 30 pps, and for each source MAC address is 30 pps.

Syntax

arp-guard rate-limit { **per-port** *rate-limit* | **per-src-ip** *rate-limit* | **per-src-mac** *rate-limit* }

no arp-guard rate-limit { **per-port** | **per-src-ip** | **per-src-mac** }

default arp-guard rate-limit { **per-port** | **per-src-ip** | **per-src-mac** }

Parameter Description

per-port *rate-limit*: Configures a rate limiting threshold for each interface, in pps. The value range is from 1 to 19999.

per-src-ip *rate-limit*: Configures a rate limiting threshold for each source IP address, in pps. The value range is from 1 to 19999.

per-src-mac *rate-limit*: Configures a rate limiting threshold for each source MAC address, in pps. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the global rate limiting thresholds of ARP guard to **50** pps, **2** pps, and **3** pps for each interface, source IP address, and source MAC address respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard rate-limit per-port 50
Hostname(config-nfpp)# arp-guard rate-limit per-src-ip 2
Hostname(config-nfpp)# arp-guard rate-limit per-src-mac 3
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 arp-guard ratelimit-forwarding enable

Function

Run the **arp-guard ratelimit-forwarding enable** command to enable the function of port-based rate limit forwarding of ARP guard.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The function of port-based rate limit forwarding of ARP guard is disabled by default.

Syntax

arp-guard ratelimit-forwarding enable

no arp-guard ratelimit-forwarding enable

default arp-guard ratelimit-forwarding enable

Parameter Description

N/A

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of port-based rate limiting forwarding of ARP guard.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard ratelimit-forwarding enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 arp-guard scan-threshold

Function

Run the **arp-guard scan-threshold** command to configure the global scanning threshold of ARP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The global scanning threshold of ARP guard is 100 packets per 10 seconds by default.

Syntax

arp-guard scan-threshold *scan-threshold*

no arp-guard scan-threshold

default arp-guard scan-threshold

Parameter Description

scan-threshold: Scanning threshold, in packets per 10 seconds. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

For the ARP packets received within 10 seconds beyond the scanning threshold, if the source MAC address is unchanged and the source IP address is changing on the link layer, or the source MAC address and source IP address on the link layer are unchanged but the destination IP address is changing, a scanning attack is suspected.

Examples

The following example sets the global scanning threshold of ARP guard to 20 packets per 10 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard scan-threshold 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 clear nfpp arp-guard hosts

Function

Run the **clear nfpp arp-guard hosts** command to clear the monitored hosts of ARP guard.

Syntax

clear nfpp arp-guard hosts [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*ipv4-address* | *mac-address*]

Parameter Description

vlan *vlan-id*: Clears the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Clears the monitored hosts of a specified interface.

ipv4-address: Specified IPv4 address of a monitored host to be cleared.

mac-address: Specified MAC address of a monitored host to be cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

The isolated hosts must be released.

Examples

The following example clears the monitored hosts of ARP guard on VLAN 1 interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear nfpp arp-guard hosts vlan 1 interface gigabitethernet 0/1
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.12 clear nfpp arp-guard scan

Function

Run the **clear nfpp arp-guard scan** command to clear the scanning table of ARP guard.

Syntax

clear nfpp arp-guard scan

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears the scanning table of ARP guard.

```
Hostname> enable
Hostname# clear nfpp arp-guard scan
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.13 clear nfpp define hosts

Function

Run the **clear nfpp define hosts** command to clear the monitored hosts of the customized guard type.

Syntax

clear nfpp define *define-name* **hosts** [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*ipv4-address* | *mac-address* | *ipv6-address*] *]

Parameter Description

define-name: Specified customized guard type.

vlan *vlan-id*: Clears the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Clears the monitored hosts of a specified interface.

ipv4-address: Specified IPv4 address of a monitored host to be cleared.

mac-address: Specified MAC address of a monitored host to be cleared.

ipv6-address: Specified IPv6 address of a monitored host to be cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

The isolated hosts must be released.

If this command is run without parameters, all monitored hosts of this customized type are cleared.

Examples

The following example clears the monitored hosts of the customized TCP guard type on VLAN 1 interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear nfpp define tcp hosts vlan 1 interface gigabitethernet 0/1
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.14 clear nfpp dhcp-guard hosts

Function

Run the **clear nfpp dhcp-guard hosts** command to clear the monitored hosts of DHCP guard.

Syntax

clear nfpp dhcp-guard hosts [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*mac-address*]

Parameter Description

vlan *vlan-id*: Clears the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Clears the monitored hosts of a specified interface.

mac-address: Specified MAC address of a monitored host to be cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If this command is run without parameters, all isolated hosts are cleared.

Examples

The following example clears the monitored hosts of DHCP guard on VLAN 1 interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear nfpp dhcp-guard hosts vlan 1 interface gigabitethernet 0/1
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.15 clear nfpp dhcpv6-guard hosts

Function

Run the **clear nfpp dhcpv6-guard hosts** command to clear the monitored hosts of DHCPv6 guard.

Syntax

clear nfpp dhcpv6-guard hosts [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*mac-address*]

Parameter Description

vlan *vlan-id*: Clears the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Clears the monitored hosts of a specified interface.

mac-address: Specified MAC address of a monitored host to be cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If this command is run without parameters, all isolated hosts are cleared.

Examples

The following example clears the monitored hosts of DHCPv6 guard on VLAN 1 interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear nfpp dhcpv6-guard hosts vlan 1 interface gigabitethernet 0/1
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.16 clear nfpp icmp-guard hosts

Function

Run the **clear nfpp icmp-guard hosts** command to clear the monitored hosts of ICMP guard.

Syntax

clear nfpp icmp-guard hosts [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*ipv4-address*]

Parameter Description

vlan *vlan-id*: Clears the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Clears the monitored hosts of a specified interface.

ipv4-address: Specified IPv4 address of a monitored host to be cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If this command is run without parameters, all monitored hosts are cleared.

Examples

The following example clears the monitored hosts of ICMP guard on VLAN 1 interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear nfpp icmp-guard hosts vlan 1 interface gigabitethernet 0/1
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.17 clear nfpp ip-guard hosts

Function

Run the **clear nfpp ip-guard hosts** command to clear the monitored hosts of IP guard.

Syntax

clear nfpp ip-guard hosts [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*ipv4-address*]

Parameter Description

vlan *vlan-id*: Clears the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Clears the monitored hosts of a specified interface.

ipv4-address: Specified IPv4 address of a monitored host to be cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If this command is run without parameters, all monitored hosts are cleared.

Examples

The following example clears the monitored hosts of IP guard on VLAN 1 interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear nfpp ip-guard hosts vlan 1 interface gigabitethernet 0/1
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.18 clear nfpp log

Function

Run the **clear nfpp log** command to clear the log buffer of NFPP.

Syntax

clear nfpp log

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears the log buffer of NFPP.

```
Hostname> enable
Hostname# clear nfpp log
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.19 clear nfpp nd-guard hosts

Function

Run the **clear nfpp nd-guard hosts** command to clear the monitored hosts of ND guard.

Syntax

clear nfpp nd-guard hosts [**vlan** *vlan-id*] [**interface** *interface-type interface-number*]

Parameter Description

vlan *vlan-id*: Clears the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Clears the monitored hosts of a specified interface.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If this command is run without parameters, all monitored hosts are cleared.

If a host is configured with a rate limiting threshold by hardware, this configuration must be cleared.

Examples

The following example clears the monitored hosts of ND guard on VLAN 1 interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear nfpp nd-guard hosts vlan 1 interface gigabitethernet 0/1
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.20 clear nfpp tcp-syn-guard hosts

Function

Run the **clear nfpp tcp-syn-guard hosts** command to clear the monitored hosts of TCP-SYN guard.

Syntax

clear nfpp tcp-syn-guard hosts [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*ipv4-address*]

Parameter Description

vlan *vlan-id*: Clears the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Clears the monitored hosts of a specified interface.

ipv4-address: Specified IPv4 address of a monitored host to be cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

If this command is run without parameters, all monitored hosts are cleared.

Examples

The following example clears the monitored hosts of TCP-SYN guard on VLAN 1 interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear nfpp tcp-syn-guard hosts vlan 1 interface gigabitethernet 0/1
```

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.21 define

Function

Run the **define** command to customize a guard type and enter the customized guard configuration mode of NFPP.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

Syntax

define *define-name*

no define *define-name*

default define *define-name*

Parameter Description

define-name: Name of a customized guard type.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example creates a customized guard type named TCP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# define tcp
Hostname(config-nfpp-define)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.22 define enable

Function

Run the **define enable** command to enable the function of global customized guard.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The function of global customized guard is disabled by default.

Syntax

define *define-name* **enable**

no define *define-name* **enable**

default define *define-name* **enable**

Parameter Description

define-name: Name of an enabled customized guard function.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

To validate the configuration of this command, you must configure the **match**, **rate-limit**, and **attack-threshold** parameters for this command.

Examples

The following example enables the global guard function of the TCP type.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# define tcp enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.23 dhcp-guard attack-threshold

Function

Run the **dhcp-guard attack-threshold** command to configure the global attack threshold of DHCP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the global attack threshold of DHCP guard for each interface is 256 pps, and for each source MAC address is 10 pps.

Syntax

dhcp-guard attack-threshold { **per-port** *attack-threshold* | **per-src-mac** *attack-threshold* }

no dhcp-guard attack-threshold { **per-port** | **per-src-mac** }

default dhcp-guard attack-threshold { **per-port** | **per-src-mac** }

Parameter Description

per-port *attack-threshold*: Configures an attack threshold for each interface, in pps. The value range is from 1 to 19999.

per-src-mac *attack-threshold*: Configures an attack threshold for each source MAC address, in pps. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When packets are sent at a rate higher than the attack threshold, an attack occurs.

Examples

The following example sets the global attack thresholds of DHCP guard to **200** pps and **15** pps for each interface and source MAC address respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcp-guard attack-threshold per-port 200
Hostname(config-nfpp)# dhcp-guard attack-threshold per-src-mac 15
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.24 dhcp-guard enable

Function

Run the **dhcp-guard enable** command to enable the function of global DHCP guard.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The function of global DHCP guard is enabled by default.

Syntax

dhcp-guard enable

no dhcp-guard enable

default dhcp-guard enable

Parameter Description

N/A

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of global DHCP guard.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcp-guard enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.25 dhcp-guard isolate-period

Function

Run the **dhcp-guard isolate-period** command to configure the global isolation time of DHCP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default global isolation time of DHCP guard is **0**.

Syntax

dhcp-guard isolate-period { *interval* | **permanent** }

no dhcp-guard isolate-period

default dhcp-guard isolate-period

Parameter Description

interval: Isolation time, in seconds. The value is **0** or the value range is from 30 to 86400. The value **0** specifies no isolation.

permanent: Configures permanent isolation.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

Isolation time of attackers falls into global isolation time and port-based isolation time (or local isolation time). If no port-based isolation time is configured for an interface, the global isolation time applies.

Examples

The following example sets the global isolation time of DHCP guard to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcp-guard isolate-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.26 dhcp-guard monitored-host-limit

Function

Run the **dhcp-guard monitored-host-limit** command to configure the maximum number of monitored hosts of DHCP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum number of monitored hosts of DHCP guard is **20000** by default.

Syntax

dhcp-guard monitored-host-limit *number*

no dhcp-guard monitored-host-limit

default dhcp-guard monitored-host-limit

Parameter Description

number: Configured maximum number of monitored hosts. The value range is from 1 to 4294967295.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When the number of monitored hosts reaches the default value **20000**, the monitored hosts are not automatically deleted if the administrator sets the maximum number of monitored hosts to a value smaller than 20000. An alarm message "%ERROR: The value that you configured is smaller than current monitored hosts 20000 (number of monitored hosts), please clear a part of monitored hosts." is printed to remind users of configuration failure and the need to clear some monitored hosts.

When the table of monitored hosts is full, the log "% NFPP_DHCP_GUARD-SESSION_LIMIT: Attempt to exceed limit of DHCP 20000 monitored hosts." is printed to remind the administrator.

Examples

The following example sets the maximum number of monitored hosts of DHCP guard to **200**.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcp-guard monitored-host-limit 200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.27 dhcp-guard monitor-period

Function

Run the **dhcp-guard monitor-period** command to configure the monitoring time of DHCP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default monitoring time of DHCP guard is **600** seconds.

Syntax

dhcp-guard monitor-period *interval*

no dhcp-guard monitor-period

default dhcp-guard monitor-period

Parameter Description

interval: Configured monitoring time, in seconds. The value range is from 180 to 86400.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When DHCP guard detects an attacker, if the isolation time is 0, this function monitors the attacker through software and the timeout time is the monitoring time. During software monitoring, when the isolation time is configured as a non-zero value, this function automatically isolates the attacker under software monitoring and the timeout time is configured as the isolation time. The monitoring time takes effect when the isolation time is 0.

If you change the isolation time to 0 from a non-zero value, the isolated attacker is directly deleted without monitoring the attacker through software.

Examples

The following example sets the monitoring time of DHCP guard to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcp-guard monitor-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.28 dhcp-guard rate-limit

Function

Run the **dhcp-guard rate-limit** command to configure the global rate limiting threshold of DHCP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the global rate limiting threshold of DHCP guard for each interface is 150 pps, and for each source MAC address is 5 pps.

Syntax

dhcp-guard rate-limit { **per-port** *rate-limit* | **per-src-mac** *rate-limit* }

no dhcp-guard rate-limit { **per-port** | **per-src-mac** }

default dhcp-guard rate-limit { **per-port** | **per-src-mac** }

Parameter Description

per-port *rate-limit*: Configures a rate limiting threshold for each interface, in pps. The value range is from 1 to 19999.

per-src-mac *rate-limit*: Configures a rate limiting threshold for each source MAC address, in pps. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the global attack thresholds of DHCP guard to **100** pps and **8** pps for each interface and source MAC address respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcp-guard rate-limit per-port 100
Hostname(config-nfpp)# dhcp-guard rate-limit per-src-mac 8
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.29 dhcpv6-guard attack-threshold

Function

Run the **dhcpv6-guard attack-threshold** command to configure the global attack threshold of DHCPv6 guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the global attack threshold of DHCPv6 guard for each interface is 256 pps, and for each source MAC address is 10 pps.

Syntax

dhcpv6-guard attack-threshold { **per-port** *attack-threshold* | **per-src-mac** *attack-threshold* }

no dhcpv6-guard attack-threshold { **per-port** | **per-src-mac** }

default dhcpv6-guard attack-threshold { **per-port** | **per-src-mac** }

Parameter Description

per-port *attack-threshold*: Configures an attack threshold for each interface, in pps. The value range is from 1 to 19999.

per-src-mac *attack-threshold*: Configures an attack threshold for each source MAC address, in pps. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When packets are sent at a rate higher than the attack threshold, an attack occurs.

Examples

The following example sets the global attack thresholds of DHCPv6 guard to **200** pps and **15** pps for each interface and source MAC address respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcpv6-guard attack-threshold per-port 200
Hostname(config-nfpp)# dhcpv6-guard attack-threshold per-src-mac 15
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.30 dhcpv6-guard enable

Function

Run the **dhcpv6-guard enable** command to enable the DHCPv6 guard function.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The DHCPv6 guard function is enabled by default.

Syntax

dhcpv6-guard enable

no dhcpv6-guard enable

default dhcpv6-guard enable

Parameter Description

N/A

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the global DHCPv6 guard function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcpv6-guard enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.31 dhcpv6-guard monitored-host-limit

Function

Run the **dhcpv6-guard monitored-host-limit** command to configure the maximum number of monitored hosts of DHCPv6 guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum number of monitored hosts of DHCPv6 guard is **20000** by default.

Syntax

dhcpv6-guard monitored-host-limit *number*

no dhcpv6-guard monitored-host-limit

default dhcpv6-guard monitored-host-limit

Parameter Description

number: Configured maximum number of monitored hosts. The value range is from 1 to 4294967295.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When the number of monitored hosts reaches the default value **20000**, the monitored hosts are not automatically deleted if the administrator sets the maximum number of monitored hosts to a value smaller than 20000. An alarm message "%ERROR: The value that you configured is smaller than current monitored hosts 20000 (number of monitored hosts), please clear a part of monitored hosts." is printed to remind users of configuration failure and the need to clear some monitored hosts.

When the table of monitored hosts is full, the log "% NFPP_DHCPV6_GUARD -SESSION_LIMIT: Attempt to exceed limit of DHCPv6 20000 monitored hosts." is printed to remind the administrator.

Examples

The following example sets the maximum number of monitored hosts of DHCPv6 guard to **200**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcp-guard monitored-host-limit 200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.32 dhcpv6-guard monitor-period

Function

Run the **dhcpv6-guard monitor-period** command to configure the monitoring time of DHCPv6 guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default monitoring time of DHCPv6 guard is **600** seconds.

Syntax

dhcpv6-guard monitor-period *interval*

no dhcpv6-guard monitor-period

default dhcpv6-guard monitor-period

Parameter Description

interval: Configured monitoring time, in seconds. The value range is from 180 to 86400.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When DHCPv6 guard detects an attacker, if the isolation time is 0, this function monitors the attacker through software and the timeout time is the monitoring time. During software monitoring, when the isolation time is configured as a non-zero value, this function automatically isolates the attacker under software monitoring and the timeout time is configured as the isolation time. The monitoring time takes effect when the isolation time is 0.

If you change the isolation time to 0 from a non-zero value, the isolated attacker is directly deleted without monitoring the attacker through software.

Examples

The following example sets the monitoring time of DHCPv6 guard to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcpv6-guard monitor-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.33 dhcpv6-guard rate-limit

Function

Run the **dhcpv6-guard rate-limit** command to configure the global rate limiting threshold of DHCPv6 guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the global rate limiting threshold of DHCPv6 guard for each interface is 150 pps, and for each source MAC address is 5 pps.

Syntax

dhcpv6-guard rate-limit { **per-port** *rate-limit* | **per-src-mac** *rate-limit* }

no dhcpv6-guard rate-limit { **per-port** | **per-src-mac** }

default dhcpv6-guard rate-limit { **per-port** | **per-src-mac** }

Parameter Description

per-port *rate-limit*: Configures a rate limiting threshold for each interface, in pps. The value range is from 1 to 19999.

per-src-mac *rate-limit*: Configures a rate limiting threshold for each source MAC address, in pps. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the global rate limiting threshold of DHCPv6 guard to **100** pps and **8** pps for each interface and source MAC address respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcpv6-guard rate-limit per-port 100
Hostname(config-nfpp)# dhcpv6-guard rate-limit per-src-mac 8
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.34 global-policy

Function

Run the **global-policy** command to configure the global rate limiting threshold and global attack threshold of the customized guard type.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No global rate limiting threshold and global attack threshold of the customized guard type are configured by default.

Syntax

global-policy { **per-port** *rate-limit attack-threshold* | **per-src-ip** *rate-limit attack-threshold* | **per-src-mac** *rate-limit attack-threshold* }

no global-policy { **per-port** | **per-src-ip** | **per-src-mac** }

default global-policy { **per-port** | **per-src-ip** | **per-src-mac** }

Parameter Description

per-port: Performs rate statistics based on the physical port that receives packets.

per-src-ip: Performs rate statistics based on the source IP address, VLAN ID, and port that are used to identify hosts.

per-src- mac: Performs rate statistics based on the source MAC address, VLAN ID, and port that are used to identify hosts.

rate-limit: Configured rate limiting threshold, in pps. The value range is from 1 to 19999.

attack-threshold: Configured attack threshold, in pps. The value range is from 1 to 19999.

Command Modes

Customized configuration mode of NFPP

Default Level

14

Usage Guidelines

To create a customized guard type, you must specify rules of rate statistics classification for this type. You must identify hosts based on the source IP address and source MAC address, perform customized packet rate statistics based on the users, or perform rate statistics based on ports and specify rate limiting thresholds and attack thresholds for different classes of rate statistics. The attack threshold must be equal to or greater than the rate limiting threshold. When the rate exceeds the rate limiting threshold, packets of the customized type in

this class are discarded. When the rate exceeds the attack threshold, an attack occurs, a log is printed, and a Trap message is sent.

Examples

The following example configures the customized guard type as TCP, sets the global rate limiting threshold and global attack threshold for each interface to **100** pps and **200** pps, and sets the global rate limiting threshold and global attack threshold for each source IP address to **10** pps and **20** pps respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# define tcp
Hostname(config-nfpp-define)# global-policy per-port 100 200
Hostname(config-nfpp-define)# global-policy per-src-ip 10 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.35 icmp-guard attack-threshold

Function

Run the **icmp-guard attack-threshold** command to configure the global attack threshold of ICMP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the global attack threshold of ICMP guard for each interface is 400 pps, and for each source IP address is 300 pps.

Syntax

icmp-guard attack-threshold { **per-port** *attack-threshold* | **per-src-ip** *attack-threshold* }

no icmp-guard attack-threshold { **per-port** | **per-src-ip** }

default icmp-guard attack-threshold { **per-port** | **per-src-ip** }

Parameter Description

per-port *attack-threshold*: Configures an attack threshold for each interface, in pps. The value range is from 1 to 19999.

per-src-ip *attack-threshold*: Configures an attack threshold for each source IP address, in pps. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the global attack thresholds of ICMP guard to **1200** pps and **600** pps for each interface and source IP address respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# icmp-guard attack-threshold per-port 1200
Hostname(config-nfpp)# icmp-guard attack-threshold per-src-ip 600
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.36 icmp-guard enable

Function

Run the **icmp-guard enable** command to enable the function of global ICMP guard.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The function of global ICMP guard is enabled by default.

Syntax

icmp-guard enable

no icmp-guard enable

default icmp-guard enable

Parameter Description

N/A

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of global ICMP guard.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# icmp-guard enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.37 icmp-guard isolate-period

Function

Run the **icmp-guard isolate-period** command to configure the global isolation time of ICMP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form this command to restore the default configuration.

The default global isolation time of ICMP guard is **0**.

Syntax

icmp-guard isolate-period { *interval* | **permanent** }

no icmp-guard isolate-period

default icmp-guard isolate-period

Parameter Description

interval: Isolation time, in seconds. The value is **0** or the value range is from 30 to 86400. The value **0** specifies no isolation.

permanent: Configures permanent isolation.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

Isolation time of attackers falls into global isolation time and port-based isolation time (or local isolation time). If no port-based isolation time is configured for an interface, the global isolation time applies.

Examples

The following example sets the global isolation time of ICMP guard to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# icmp-guard isolate-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.38 icmp-guard monitored-host-limit

Function

Run the **icmp-guard monitored-host-limit** command to configure the maximum number of monitored hosts of ICMP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum number of monitored hosts is **20000** by default.

Syntax

icmp-guard monitored-host-limit *number*

no icmp-guard monitored-host-limit

default icmp-guard monitored-host-limit

Parameter Description

number: Configured maximum number of monitored hosts. The value range is from 1 to 4294967295.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When the number of monitored hosts reaches the default value **20000**, the monitored hosts are not automatically deleted if the administrator sets the maximum number of monitored hosts to a value smaller than 20000. An alarm message "%ERROR: The value that you configured is smaller than current monitored hosts 20000 (number of monitored hosts), please clear a part of monitored hosts." is printed to remind users of configuration failure and the need to clear some monitored hosts.

When the table of monitored hosts is full, the log "% NFPP_ICMP_GUARD-SESSION_LIMIT: Attempt to exceed limit of ICMP 20000 (number of monitored hosts) monitored hosts." is printed to remind the administrator.

Examples

The following example sets the maximum number of monitored hosts of ICMP guard to **200**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# icmp-guard monitored-host-limit 200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.39 icmp-guard monitor-period

Function

Run the **icmp-guard monitor-period** command to configure the monitoring time of ICMP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default monitoring time of ICMP guard is **600** seconds.

Syntax

icmp-guard monitor-period *interval*

no icmp-guard monitor-period

default icmp-guard monitor-period

Parameter Description

interval: Configured monitoring time, in seconds. The value range is from 180 to 86400.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When ICMP guard detects an attacker, if the isolation time is 0, this function monitors the attacker through software and the timeout time is the monitoring time. During software monitoring, when the isolation time is configured as a non-zero value, this function automatically isolates the attacker under software monitoring and the timeout time is configured as the isolation time. The monitoring time takes effect when the isolation time is 0.

If you change the isolation time to 0 from a non-zero value, the isolated attacker is directly deleted without monitoring the attacker through software.

Examples

The following example sets the monitoring time of ICMP guard to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# icmp-guard monitor-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.40 icmp-guard rate-limit

Function

Run the **icmp-guard rate-limit** command to configure the global rate limiting threshold of ICMP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the global rate limiting threshold of ICMP guard for each interface is 250 pps, and for each source IP address is 200 pps.

Syntax

icmp-guard rate-limit { **per-port** *rate-limit* | **per-src-ip** *rate-limit* }

no icmp-guard rate-limit { **per-port** | **per-src-ip** }

default icmp-guard rate-limit { **per-port** | **per-src-ip** }

Parameter Description

per-port *rate-limit*: Configures a rate limiting threshold for each interface, in pps. The value range is from 1 to 19999.

per-src-ip *rate-limit*: Configures a rate limiting threshold for each source IP address, in pps. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the global rate limiting thresholds of ICMP guard to **800** pps and **500** pps for each interface and source IP address respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# icmp-guard rate-limit per-port 800
Hostname(config-nfpp)# icmp-guard rate-limit per-src-ip 500
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.41 icmp-guard trusted-host

Function

Run the **icmp-guard trusted-host** command to configure the trusted hosts of ICMP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No host is configured as a trusted host by default.

Syntax

icmp-guard trusted-host *ipv4-address mask*

no icmp-guard trusted-host { *ipv4-address mask* | **all** }

default icmp-guard trusted-host

Parameter Description

ipv4-address mask: IPv4 address+mask. The mask is entered in dotted decimal mode.

all: Deletes the configuration of all trusted hosts when this parameter is used with the **no** parameter.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

To cancel the monitoring of a host, the administrator can run this command to configure the host as a trusted host. In this case, ICMP packets sent by this host can be forwarded to the CPU without rate limit or alarm. All hosts in a network segment can be configured as trusted hosts by configuring a mask.

A maximum of 500 trusted hosts can be configured.

Examples

The following example configures all hosts in the network segment 1.1.1.0/24 as trusted hosts of ICMP guard.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# icmp-guard trusted-host 1.1.1.0 255.255.255.0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.42 ip-guard attack-threshold

Function

Run the **ip-guard attack-threshold** command to configure the global attack threshold of IP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the global attack threshold of IP guard for each interface is 200 pps, and for each source IP address is 100 pps.

Syntax

ip-guard attack-threshold { **per-port** *attack-threshold* | **per-src-ip** *attack-threshold* }

no ip-guard attack-threshold { **per-port** | **per-src-ip** }

default ip-guard attack-threshold { **per-port** | **per-src-ip** }

Parameter Description

per-port *attack-threshold*: Configures an attack threshold for each interface, in pps. The value range is from 1 to 19999.

per-src-ip *attack-threshold*: Configures an attack threshold for each source IP address, in pps. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

The attack threshold must be equal to or greater than the rate limiting threshold.

IP guard is to solve IP attacks whose destination IP address is not a local IP address. If the destination IP address is a local IP address, the rates of IP packets are limited by the function of CPU protect policy (CPP).

Examples

The following example sets the global attack thresholds of IP guard to **50** pps and **2** pps for each interface and source IP address respectively.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard attack-threshold per-port 50
Hostname(config-nfpp)# ip-guard attack-threshold per-src-ip 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.43 ip-guard enable

Function

Run the **ip-guard enable** command to enable the global IP guard function.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The global IP guard function is enabled by default.

Syntax

ip-guard enable

no ip-guard enable

default ip-guard enable

Parameter Description

N/A

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the global IP guard function.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard enable
```

Notifications

No notification can be configured.

```
Configuration is prohibited, please disable the arp-guard suppression function
first!
```

Common Errors

If you have configured the function of ARP source suppression and the isolation time for IP guard in global or interface configuration mode, an error is reported when you enable the function of global IP guard.

Platform Description

N/A

Related Commands

N/A

1.44 ip-guard isolate-period

Function

Run the **ip-guard isolate-period** command to configure the global isolation time of IP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default global isolation time of IP guard is **0**.

Syntax

ip-guard isolate-period { *interval* | **permanent** }

no ip-guard isolate-period

default ip-guard isolate-period

Parameter Description

interval: Isolation time, in seconds. The value is **0** or the value range is from 30 to 86400.

permanent: Configures permanent isolation.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

If you have configured the function of ARP source suppression, you are not allowed to configure the isolation function unless you disable the function of ARP source suppression.

Examples

The following example sets the global isolation time of IP guard to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard isolate-period 180
```

Notifications

If you have configured the ARP source suppression function, the following notification will be displayed when you configure isolation time for the IP guard function:

```
Configuration is prohibited, please disable the arp-guard suppression function
first!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.45 ip-guard monitored-host-limit

Function

Run the **ip-guard monitored-host-limit** command to configure the maximum number of monitored hosts of IP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum number of monitored hosts of IP guard is **20000** by default.

Syntax

ip-guard monitored-host-limit *number*

no ip-guard monitored-host-limit

default ip-guard monitored-host-limit

Parameter Description

number: Configured maximum number of monitored hosts. The value range is from 1 to 4294967295.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When the number of monitored hosts reaches the default value **20000**, the monitored hosts are not deleted if the administrator sets the maximum number of monitored hosts to a value smaller than 20000. An alarm message "%ERROR: The value that you configured is smaller than current monitored hosts 20000 (number of monitored hosts), please clear a part of monitored hosts." is printed to remind users of configuration failure and the need to delete clear some monitored hosts.

When the table of monitored hosts is full, the log "% NFPP_IP_GUARD-SESSION_LIMIT: Attempt to exceed limit of IP 20000 (number of monitored hosts) monitored hosts." is printed to remind the administrator.

Examples

The following example sets the maximum number of monitored hosts of IP guard to **200**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard monitored-host-limit 200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.46 ip-guard monitor-period

Function

Run the **ip-guard monitor-period** command to configure the monitoring time of IP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default monitoring time of IP guard is **600** seconds.

Syntax

ip-guard monitor-period *interval*

no ip-guard monitor-period

default ip-guard monitor-period

Parameter Description

interval: Configured monitoring time, in seconds. The value range is from 180 to 86400.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When IP guard detects an attacker, if the isolation time is 0, this function monitors the attacker through software and the timeout time is the monitoring time. During software monitoring, when the isolation time is configured as a non-zero value, this function automatically isolates the attacker under software monitoring and the timeout time is configured as the isolation time. The monitoring time takes effect when the isolation time is 0.

If you change the isolation time to 0 from a non-zero value, the isolated attacker is directly deleted without monitoring the attacker through software.

Examples

The following example sets the monitoring time of IP guard to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard monitor-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.47 ip-guard rate-limit

Function

Run the **ip-guard rate-limit** command to configure the global rate limiting threshold of IP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the global rate limiting threshold of IP guard for each interface is 50 pps, and for each source IP address is 20 pps.

Syntax

ip-guard rate-limit { **per-port** *rate-limit* | **per-src-ip** *rate-limit* }

no ip-guard rate-limit { **per-port** | **per-src-ip** }

default ip-guard rate-limit { **per-port** | **per-src-ip** }

Parameter Description

per-port *rate-limit*: Configures a rate limiting threshold for each interface, in pps. The value range is from 1 to 19999.

per-src-ip *rate-limit*: Configures a rate limiting threshold for each source IP address, in pps. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the global rate limiting thresholds of IP guard to **50** pps and **2** pps for each interface and source IP address respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard rate-limit per-port 50
Hostname(config-nfpp)# ip-guard rate-limit per-src-ip 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.48 ip-guard scan-threshold

Function

Run the **ip-guard scan-threshold** command to configure the global scanning threshold of IP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The global scanning threshold of IP guard is 100 packets per 10 seconds by default.

Syntax

ip-guard scan-threshold *scan-threshold*

no ip-guard scan-threshold

default ip-guard scan-threshold

Parameter Description

scan-threshold: Configured scanning threshold, in packets per 10 seconds. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the global scanning threshold of IP guard to 20 packets per 10 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard scan-threshold 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.49 ip-guard trusted-host

Function

Run the **ip-guard trusted-host** command to configure the trusted hosts of IP guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No host is configured as a trusted host of IP guard by default.

Syntax

ip-guard trusted-host *ipv4-address mask*

no ip-guard trusted-host { *ipv4-address mask* | **all** }

default ip-guard trusted-host

Parameter Description

ipv4-address mask: IPv4 address+mask. The mask is entered in dotted decimal mode.

all: Deletes the configuration of all trusted hosts when this parameter is used with the **no** parameter.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

To cancel the monitoring of a host, the administrator can run this command to configure the host as a trusted host. In this case, IP packets sent by this host can be forwarded to the CPU without rate limit or alarm.

A maximum of 500 trusted hosts can be configured.

Examples

The following example configures all hosts in the network segment 1.1.1.0/24 as trusted hosts of IP guard.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)#ip-guard trusted-host 1.1.1.0 255.255.255.0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.50 log-buffer enable

Function

Run the **log-buffer enable** command to enable the function of screen log output.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The function of screen log output is disabled by default and logs are saved in the buffer.

Syntax

log-buffer enable

no log-buffer enable

default log-buffer enable

Parameter Description

N/A

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

Full scanning table of ARP entries and session oversize are directly output on the screen without limit by the following rules.

When you configure the **log-buffer logs** command and set the value of the *message-number* parameter to **0**:

- If the **log-buffer enable** command is also configured, logs are output onto the screen without limit.
- If the **log-buffer enable** command is not configured, the logs related to isolation and port rate limit are output onto the screen without limit by the **log-buffer logs** command and other types of logs are stored in the log buffer without output. In this case, you can run the **show nfpp log buffer** command to display the logs.

When you configure the **log-buffer logs** command and set the value of the *message-number* parameter to **0** and the value of *interval* to a none-zero value: Logs are stored in the log buffer without output. In this case, you can run the **show nfpp log buffer** command to display the logs.

When you configure the **log-buffer logs** command and set the values of the *message-number* and *interval* parameters to none-zero values:

- If the **log-buffer enable** command is configured, logs are first stored in the log buffer and then output onto the screen regularly based on the *interval* configuration.
- If the **log-buffer enable** command is not configured, logs are first stored in the log buffer, and logs related to isolation and port rate limit are output onto the screen regularly based on the *interval* configuration.

When logs are first output onto the screen, the historical logs in the log buffer are output onto the screen. Before starting the configuration, you are advised to run the **clear nfpp log** command to clear the logs in the log buffer.

After active/standby switchover of a device, the device will clear logs in a buffer and record new logs again.

Examples

The following example enables the function of screen log output.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# log-buffer enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.51 log-buffer entries

Function

Run the **log-buffer entries** command to configure the size of the log buffer.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default size of the NFPP log buffer is **256** pieces.

Syntax

log-buffer entries *number*

no log-buffer entries

default log-buffer entries

Parameter Description

number: Configured buffer size, in pieces. The value range is from 0 to 1024.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the size of the NFPP log buffer to 50 pieces.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# log-buffer entries 50
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.52 log-buffer logs

Function

Run the **log-buffer logs** command to configure the rate of generating system messages from logs of the log buffer through NFPP.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No rate of generating system messages from logs of the log buffer is configured through NFPP and NFPP logs are not written into the buffer by default.

Syntax

log-buffer logs *message-number* **interval** *interval*

no log-buffer logs

default log-buffer logs

Parameter Description

message-number: Number of system messages output in the specified *interval*, in pieces. The value range is from 0 to 1024. The value **0** specifies that logs are recorded in the special buffer without generating system messages.

interval: Time configured to generate *message-number* system messages, in seconds. The value range is from 0 to 86400. The value **0** specifies that logs are not written into the log buffer, but are used to immediately generate system messages.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When the values of *message-number* and *interval* are 0, logs are not written into the log buffer, but are used to immediately generate system messages.

The result of *message-number* divided by *interval* specifies the rate of generating system messages from logs of the log buffer.

When you configure the **log-buffer logs** command and set the value of the *message-number* parameter to 0:

- If the **log-buffer enable** command is also configured, logs are output onto the screen without limit.
- If the **log-buffer enable** command is not configured, the logs related to isolation and port rate limit are output onto the screen without limit by the **log-buffer logs** command and other types of logs are stored in the log buffer without output. In this case, you can run the **show nfpp log buffer** command to display the logs.

When you configure the **log-buffer logs** command and set the value of the *message-number* parameter to 0 and the value of *interval* to a none-zero value: Logs are stored in the log buffer without output. In this case, you can run the **show nfpp log buffer** command to display the logs.

When you configure the **log-buffer logs** command and set the values of the *message-number* and *interval* parameters to non-zero values:

- If the log-buffer enable command is configured, logs are first stored in the log buffer and then output onto the screen regularly based on the *interval* configuration.
- If the **log-buffer enable** command is not configured, logs are first stored in the log buffer, and logs related to isolation and port rate limit are output onto the screen regularly based on the *interval* configuration.

When logs are first output onto the screen, the historical logs in the log buffer are output onto the screen. Before starting the configuration, you are advised to run the **clear nfpp log** command to clear the logs in the log buffer.

Examples

The following example sets the system message generation rate to 2 logs per 12 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# log-buffer logs 2 interval 12
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.53 logging

Function

Run the **logging** command to configure NFPP to records the logs of a specified VLAN ID and a specified interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

NFPP records logs of all VLANs and interfaces by default.

Syntax

logging { **interface** *interface-type interface-number* | **vlan** *vlan-range* }

no logging { **interface** *interface-type interface-number* | **vlan** *vlan-range* }

default logging

Parameter Description

interface *interface-type interface-number*: Records only the NFPP logs of a specified interface.

vlan *vlan-range*: Records only the NFPP logs in the specified VLAN range. The value range is from 1 to 4095. The input format is as follows: 1-3, 5.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

This command can be used to filter logs and record the logs of a specified VLAN range or an interface. If the relationship of two log filtering configurations is OR, logs are recorded into the log buffer when one log filtering configuration is met.

Examples

The following example records the logs of VLAN 1, VLAN 2, VLAN 3, and VLAN 5.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# logging vlan 1-3,5
```

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

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# logging interface gigabitethernet 0/1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.54 match

Function

Run the **match** command to configure the matched packet types of a customized guard type.

Syntax

match { **dst-ip** *destination-ipv4-address* [**dst-ip-mask** *mask*] | **dst-ipv6** *destination-ipv6-address* [**dst-ipv6-masklen** *prefix-length*] | **dst-mac** *destination-mac* [**dst-mac-mask** *destination-mac-mask*] | **dst-port** *port-number* | **etype** *type* | **protocol** *protocol* | **src-ip** *source-ip-address* [**src-ip-mask** *mask*] | **src-ipv6** *source-ipv6-address* [**src-ipv6-masklen** *prefix-length*] | **src-mac** *source-mac-address* | **src-port** *port-number* } *

Parameter Description

dst-ip *destination-ipv4-address*: Specifies a destination IPv4 address.

dst-ip-mask *mask*: Specifies a destination IPv4 address mask.

dst-ipv6 *destination-ipv6-address*: Specifies a destination IPv6 address.

dst-ipv6-masklen *prefix-length*: Specifies the length of a destination IPv6 address mask.

dst-mac *destination-mac*: Specifies a destination MAC address.

dst-mac-mask *destination-mac-mask*: Specifies a destination MAC address mask.

dst-port *port-number*: Specifies a destination port number on the transport layer.

etype *type*: Specifies an Ethernet link layer packet type.

protocol *protocol*: Specifies a protocol number.

src-ip *source-ip-address*: Specifies a source IPv4 address.

src-ip-mask *mask*: Specifies a source IPv4 address mask.

src-ipv6 *source-ipv6-address*: Specifies a source IPv6 address.

src-ipv6-masklen *prefix-length*: Specifies the length of a source IPv6 address mask.

src-mac *source-mac-address*: Specifies a source MAC address.

src-port *port-number*: Specifies a source port number on the transport layer.

Command Modes

Customized configuration mode of NFPP

Default Level

14

Usage Guidelines

After you create a customized guard type, you must specify packet fields to match this guard type.

Examples

The following example creates a customized TCP guard type and matches packets with **etype** being **0x0800** and **protocol** being **0x06**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# define tcp
Hostname(config-nfpp-define)# match etype 0x0800 protocol 0x06
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.55 monitored-host-limit

Function

Run the **monitored-host-limit** command to configure the maximum number of monitored hosts of a customized guard type.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum number of monitored hosts is **20000** by default.

Syntax

monitored-host-limit *number*

no monitored-host-limit

default monitored-host-limit

Parameter Description

number: Configured maximum number of monitored hosts. The value range is from 1 to 4294967295.

Command Modes

Customized configuration mode of NFPP

Default Level

14

Usage Guidelines

When the number of monitored hosts reaches the default value **20000**, the monitored hosts are not automatically deleted if the administrator sets the maximum number of monitored hosts to a value smaller than 20000. An alarm message "%ERROR: The value that you configured is smaller than current monitored hosts 20000 (number of monitored hosts), please clear a part of monitored hosts." is printed to remind users of configuration failure and the need to clear some monitored hosts.

When the table of monitored hosts is full, the log "% NFPP_DEFINE_GUARD -SESSION_LIMIT: Attempt to exceed limit of name (name of a customized guard type)'s 20000 (number of monitored hosts) monitored hosts." is printed to remind the administrator.

Examples

The following example sets the maximum number of monitored hosts of the customized TCP guard type to **500**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# define tcp
Hostname(config-nfpp-define)# monitored-host-limit 500
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.56 monitor-period

Function

Run the **monitor-period** command to configure the monitoring time of a customized guard type.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default monitoring time of a customized guard type is **600** seconds.

Syntax

monitor-period *interval*

no monitor-period

default monitor-period

Parameter Description

interval: Configured monitoring time, in seconds. The value range is from 180 to 86400.

Command Modes

Customized configuration mode of NFPP

Default Level

14

Usage Guidelines

When customized guard detects an attacker, if the isolation time is 0, this function monitors the attacker through software and the timeout time is the monitoring time. During software monitoring, when the isolation time is configured as a non-zero value, this function automatically isolates the attacker under software monitoring and the timeout time is configured as the isolation time. The monitoring time takes effect when the isolation time is 0.

If you change the isolation time to 0 from a non-zero value, the isolated attacker is directly deleted without monitoring the attacker through software.

Examples

The following example sets the monitoring time of the customized TCP guard type to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# define tcp
Hostname(config-nfpp-define)# monitor-period 180
```

Platform Description

N/A

Related Commands

N/A

1.57 nd-guard attack-threshold per-port

Function

Run the **nd-guard attack-threshold per-port** command to configure the global attack threshold of ND guard.

Run the **no** form of command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the global attack threshold of ND guard for NDSNP packets is 200 pps, for neighbor requests and advertisements is 100 pps, for route advertisements and redirection packets is 50 pps, and for route requests is 50 pps.

Syntax

nd-guard attack-threshold per-port { **ndsnp** *attack-threshold* | **ns-na** *attack-threshold* | **ra-redirect** *attack-threshold* | **rs** *attack-threshold* }

no nd-guard attack-threshold per-port { **ndsnp** | **ns-na** | **ra-redirect** | **rs** }

default nd-guard attack-threshold per-port { **ndsnp** | **ns-na** | **ra-redirect** | **rs** }

Parameter Description

ndsnp *attack-threshold*: Configures an attack threshold for NDSNP packets, in pps. The value range is from 1 to 19999. After the **ipv6 nd snooping enable** command is run in global configuration mode, all ND packets are NDSNP packets.

ns-na *attack-threshold*: Configures an attack threshold for neighbor requests and advertisements, in pps. The value range is from 1 to 19999.

ra-redirect *attack-threshold*: Configures an attack threshold for route advertisements and redirection packets, in pps. The value range is from 1 to 19999.

rs *attack-threshold*: Configures an attack threshold for route requests, in pps. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

The attack threshold must be equal to or greater than the rate limiting threshold.

Examples

The following example sets the global attack thresholds of ND guard to **10** pps, **20** pps, **10** pps, and **10** pps for NDSNP packets, neighbor requests and advertisements, route advertisements and redirection packets, and route requests respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# nd-guard attack-threshold per-port ndsnp 10
Hostname(config-nfpp)# nd-guard attack-threshold per-port ns-na 20
Hostname(config-nfpp)# nd-guard attack-threshold per-port ra-redirect 10
Hostname(config-nfpp)# nd-guard attack-threshold per-port rs 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.58 nd-guard enable

Function

Run the **nd-guard enable** command to enable the function of global ND guard.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The function of global ND guard is enabled by default.

Syntax

nd-guard enable

no nd-guard enable

default nd-guard enable

Parameter Description

N/A

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of global ND guard.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# nd-guard enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.59 nd-guard rate-limit per-port

Function

Run the **nd-guard rate-limit per-port** command to configure the global rate limiting threshold of ND guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the global rate limiting threshold of ND guard for NDSNP packets is 100 pps, for neighbor requests and advertisements is 50 pps, for route advertisements and redirection packets is 25 pps, and for route requests is 25 pps.

Syntax

nd-guard rate-limit per-port { **ndsnp** *rate-limit* | **ns-na** *rate-limit* | **ra-redirect** *rate-limit* | **rs** *rate-limit* }

no nd-guard rate-limit per-port { **ndsnp** | **ns-na** | **ra-redirect** | **rs** }

default nd-guard rate-limit per-port { **ndsnp** | **ns-na** | **ra-redirect** | **rs** }

Parameter Description

ndsnp *rate-limit*: Configures a rate limiting threshold for NDSNP packets, in pps. The value range is from 1 to 19999. After the **ipv6 nd snooping enable** command is run in global configuration mode, all ND packets are NDSNP packets.

ns-na *rate-limit*: Configures a rate limiting threshold for neighbor requests and advertisements, in pps. The value range is from 1 to 19999.

ra-redirect *rate-limit*: Configures a rate limiting threshold for route advertisements and redirection packets, in pps. The value range is from 1 to 19999.

rs *rate-limit*: Configures a rate limiting threshold for route requests, in pps. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the global rate limiting thresholds of ND guard to **5** pps, **10** pps, **5** pps, and **5** pps for NDSNP packets, neighbor requests and advertisements, route advertisements and redirection packets, and route requests respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# nd-guard rate-limit per-port ndsnp 5
Hostname(config-nfpp)# nd-guard rate-limit per-port ns-na 10
Hostname(config-nfpp)# nd-guard rate-limit per-port ra-redirect 5
Hostname(config-nfpp)# nd-guard rate-limit per-port rs 5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.60 nd-guard ratelimit-forwarding enable

Function

Run the **nd-guard ratelimit-forwarding enable** command to enable the function of port-based rate limit forwarding of ND guard.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The function of port-based rate limit forwarding of ND guard is enabled by default.

Syntax

nd-guard ratelimit-forwarding enable

no nd-guard ratelimit-forwarding enable

default nd-guard ratelimit-forwarding enable

Parameter Description

N/A

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of port-based rate limit forwarding of ND guard.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# nd-guard ratelimit-forwarding enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.61 nfpp

Function

Run the **nfpp** command to enter the NFPP configuration mode.

Syntax

nfpp

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to enter the NFPP configuration mode for NFPP configuration.

Examples

The following example enters the NFPP configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.62 nfpp arp-guard enable

Function

Run the **nfpp arp-guard enable** command to enable the ARP guard function on an interface.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The ARP guard function is not configured on an interface by default. The function of global ARP guard is enabled.

Syntax

nfpp arp-guard enable

no nfpp arp-guard enable

default nfpp arp-guard enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The ARP guard function on an interface takes precedence over the function of global ARP guard.

Examples

The following example enables the ARP guard function on interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp arp-guard enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.63 nfpp arp-guard isolate-period

Function

Run the **nfpp arp-guard isolate-period** command to configure the isolation time of ARP guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No isolation time of ARP guard is configured on an interface by default. The global isolation time of ARP guard is used.

Syntax

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

no nfpp arp-guard isolate-period

default nfpp arp-guard isolate-period

Parameter Description

interval: Isolation time, in seconds. The value is **0** or the value range is from 30 to 86400. The value **0** specifies no isolation.

permanent: Configures permanent isolation.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the isolation time of ARP guard on interface GigabitEthernet 0/1 to **180** seconds.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp arp-guard isolate-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.64 nfpp arp-guard policy

Function

Run the **nfpp arp-guard policy** command to configure the local rate limiting threshold and local attack threshold of ARP guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No local rate limiting threshold or local attack threshold of ARP guard is configured on an interface by default. The global rate limiting threshold and global attack threshold of ARP guard are used.

Syntax

nfpp arp-guard policy { **per-port** *rate-limit attack-threshold* | **per-src-ip** *rate-limit attack-threshold* | **per-src-mac** *rate-limit attack-threshold* }

no nfpp arp-guard policy { **per-port** | **per-src-ip** | **per-src-mac** }

default nfpp arp-guard policy { **per-port** | **per-src-ip** | **per-src-mac** }

Parameter Description

per-port: Configures a rate limiting threshold and an attack threshold for each interface.

per-src-ip: Configures a rate limiting threshold and an attack threshold for each source IP address.

per-src-mac: Configures a rate limiting threshold and an attack threshold for each source MAC address.

rate-limit: Configured rate limiting threshold, in pps. The value range is from 1 to 19999.

attack-threshold: Configured attack threshold, in pps. The value range is from 1 to 19999.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The attack threshold must be equal to or greater than the rate limiting threshold.

Examples

The following example sets the local rate limiting threshold and local attack threshold of ARP guard to **50** pps and **100** pps for each interface on GigabitEthernet 0/1, to **2** pps and **10** pps for each source IP address, and to **3** pps and **10** pps for each source MAC address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp arp-guard policy per-port 50 100
Hostname(config-if-GigabitEthernet 0/1)# nfpp arp-guard policy per-src-ip 2 10
Hostname(config-if-GigabitEthernet 0/1)# nfpp arp-guard policy per-src-mac 3 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.65 nfpp arp-guard scan-threshold

Function

Run the **nfpp arp-guard scan-threshold** command to configure the scanning threshold of ARP guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No scanning threshold of ARP guard is configured on an interface by default. The global scanning threshold of ARP guard is used.

Syntax

nfpp arp-guard scan-threshold *scan-threshold*

no nfpp arp-guard scan-threshold

default nfpp arp-guard scan-threshold

Parameter Description

scan-threshold: Configured scanning threshold, in packets per 10 seconds. The value range is from 1 to 19999.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the scanning threshold of ARP guard on GigabitEthernet 0/1 to 20 packets per 10 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp arp-guard scan-threshold 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.66 nfpp define enable

Function

Run the **nfpp define enable** command to enable the customized guard function on an interface.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The customized guard function is not configured on an interface by default. The global customized guard function is used.

Syntax

nfpp define *define-name* **enable**

no nfpp define *define-name* **enable**

default nfpp define *define-name* **enable**

Parameter Description

define-name: Name of a customized guard type.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

A customized guard type must be configured. To validate this configuration, you must configure the **match** and **global-policy** parameters.

Examples

The following example enables the function of customized TCP guard on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp define tcp enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.67 nfpp define policy

Function

Run the **nfpp define policy** command to configure a local rate limiting threshold and a local attack threshold of customized guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No local rate limiting threshold or local attack threshold of the customized guard type is configured on an interface by default. The global rate limiting threshold and global attack threshold of the customized guard type are used.

Syntax

nfpp define *define-name* **policy** { **per-port** *rate-limit attack-threshold* | **per-src-ip** *rate-limit attack-threshold* | **per-src-mac** *rate-limit attack-threshold* }

no nfpp define *define-name* **policy** { **per-port** | **per-src-ip** | **per-src-mac** }

default nfpp define *define-name* **policy** { **per-port** | **per-src-ip** | **per-src-mac** }

Parameter Description

define *define-name*: Name of a specified customized guard type.

per-port: Configures a rate limiting threshold and an attack threshold for each interface.

per-src-ip: Configures a rate limiting threshold and an attack threshold for each source IP address.

per-src-mac: Configures a rate limiting threshold and an attack threshold for each source MAC address.

rate-limit: Configured rate limiting threshold, in pps. The value range is from 1 to 19999.

attack-threshold: Configured attack threshold, in pps. The value range is from 1 to 19999.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The attack threshold must be equal to or greater than the rate limiting threshold.

Examples

The following example sets the local rate limiting threshold and local attack threshold of the customized TCP guard function to **2** pps and **10** pps on GigabitEthernet 0/1 for an IP address, and to **50** pps and **100** pps for an interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp define tcp policy per-src-ip 2 10
Hostname(config-if-GigabitEthernet 0/1)# nfpp define tcp policy per-port 50 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.68 nfpp dhcp-guard enable

Function

Run the **nfpp dhcp-guard enable** command to enable the DHCP guard function on an interface.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The DHCP guard function is not configured on an interface by default. The function of global DHCP guard is used.

Syntax

nfpp dhcp-guard enable

no nfpp dhcp-guard enable

default nfpp dhcp-guard enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The DHCP guard function on an interface takes precedence over the global DHCP guard function.

Examples

The following example enables the DHCP guard function on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp dhcp-guard enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.69 nfpp dhcp-guard isolate-period

Function

Run the **nfpp dhcp-guard isolate-period** command to configure the local isolation time of DHCP guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No local isolation time of DHCP guard is configured on an interface by default. The global isolation time of DHCP guard is used.

Syntax

nfpp dhcp-guard isolate-period { *interval* | **permanent** }

no nfpp dhcp-guard isolate-period

default nfpp dhcp-guard isolate-period

Parameter Description

interval: Configured isolation time, in seconds. The value is **0** or the value range is from 30 to 86400. The value **0** specifies no isolation.

permanent: Configures permanent isolation.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the local isolation time of DHCP guard on GigabitEthernet 0/1 to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp dhcp-guard isolate-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.70 nfpp dhcp-guard policy

Function

Run the **nfpp dhcp-guard policy** command to configure a local rate limiting threshold and a local attack threshold of DHCP guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No local rate limiting threshold or local attack threshold of DHCP guard is configured on an interface by default. The global rate limiting threshold and global attack threshold of DHCP guard are used.

Syntax

nfpp dhcp-guard policy { **per-port** *rate-limit attack-threshold* | **per-src-mac** *rate-limit attack-threshold* }

no nfpp dhcp-guard policy { **per-port** | **per-src-mac** }

default nfpp dhcp-guard policy { **per-port** | **per-src-mac** }

Parameter Description

per-port: Configures a rate limiting threshold and an attack threshold for each interface.

per-src-mac: Configures a rate limiting threshold and an attack threshold for each source MAC address.

rate-limit: Configured rate limiting threshold, in pps. The value range is from 1 to 19999.

attack-threshold: Configured attack threshold, in pps. The value range is from 1 to 19999.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The attack threshold must be equal to or greater than the rate limiting threshold.

Examples

The following example sets the rate limiting threshold and attack threshold of DHCP guard to **50** pps and **100** pps for each interface on GigabitEthernet 0/1 and to **3** pps and **10** pps for each source MAC address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp dhcp-guard policy per-port 50 100
Hostname(config-if-GigabitEthernet 0/1)# nfpp dhcp-guard policy per-src-mac 3 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.71 nfpp dhcpv6-guard enable

Function

Run the **nfpp dhcpv6-guard enable** command to enable the DHCPv6 guard function on an interface.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The DHCPv6 guard function is disabled on an interface by default. The global DHCPv6 guard function is used.

Syntax

nfpp dhcpv6-guard enable

no nfpp dhcpv6-guard enable

default nfpp dhcpv6-guard enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The DHCPv6 guard function on an interface takes precedence over the global DHCP guard function.

Examples

The following example enables the DHCPv6 guard function on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp dhcpv6-guard enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.72 nfpp dhcpv6-guard policy

Function

Run the **nfpp dhcpv6-guard policy** command to configure a local rate limiting threshold and a local attack threshold of DHCPv6 guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No local rate limiting threshold or local attack threshold of DHCPv6 guard is configured on an interface by default. The global rate limiting threshold and global attack threshold of DHCPv6 guard are used.

Syntax

nfpp dhcpv6-guard policy { **per-port** *rate-limit attack-threshold* | **per-src-mac** *rate-limit attack-threshold* }

no nfpp dhcpv6-guard policy { **per-port** | **per-src-mac** }

default nfpp dhcpv6-guard policy { **per-port** | **per-src-mac** }

Parameter Description

per-port: Configures a rate limiting threshold and an attack threshold for each interface.

per-src-mac: Configures a rate limiting threshold and an attack threshold for each source MAC address.

rate-limit: Configured rate limiting threshold, in pps. The value range is from 1 to 19999.

attack-threshold: Configured attack threshold, in pps. The value range is from 1 to 19999.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The attack threshold must be equal to or greater than the rate limiting threshold.

Examples

The following example sets the local rate limiting threshold and local attack threshold of DHCPv6 guard to **50** pps and **100** pps for each interface on GigabitEthernet 0/1 and to **3** pps and **10** pps for each source MAC address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
```

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

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.73 nfpp icmp-guard enable

Function

Run the **nfpp icmp-guard enable** command to enable the ICMP guard function on an interface.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The ICMP guard function is not configured on an interface by default. The function of global ICMP guard is used.

Syntax

nfpp icmp-guard enable

no nfpp icmp-guard enable

default nfpp icmp-guard enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The ICMP guard function on an interface takes precedence over the function of global ICMP guard.

Examples

The following example enables the ICMP guard function on GigabitEthernet 0/1.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp icmp-guard enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.74 nfpp icmp-guard isolate-period

Function

Run the **nfpp icmp-guard isolate-period** command to configure the local isolation time of ICMP guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No local isolation time of ICMP guard is configured on an interface by default. The global isolation time of ICMP guard is used.

Syntax

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

no nfpp icmp-guard isolate-period

default nfpp icmp-guard isolate-period

Parameter Description

interval: Configured isolation time, in seconds. The value is **0** or the value range is from 30 to 86400. The value **0** specifies no isolation.

permanent: Configures permanent isolation.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the local isolation time of ICMP guard on GigabitEthernet 0/1 to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp icmp-guard isolate-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.75 nfpp icmp-guard policy

Function

Run the **nfpp icmp-guard policy** command to configure a local rate limiting threshold and a local attack threshold of ICMP guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No local rate limiting threshold or local attack threshold of ICMP guard is configured on an interface by default. The global rate limiting threshold and global attack threshold of ICMP guard are used.

Syntax

nfpp icmp-guard policy { **per-port** *rate-limit attack-threshold* | **per-src-ip** *rate-limit attack-threshold* }

no nfpp icmp-guard policy { **per-port** | **per-src-ip** }

default nfpp icmp-guard policy { **per-port** | **per-src-ip** }

Parameter Description

per-port: Configures a rate limiting threshold and an attack threshold for each interface.

per-src-ip: Configures a rate limiting threshold and an attack threshold for each source IP address.

rate-limit: Configured rate limiting threshold, in pps. The value range is from 1 to 19999.

attack-threshold: Configured attack threshold, in pps. The value range is from 1 to 19999.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The attack threshold must be equal to or greater than the rate limiting threshold.

Examples

The following example sets the rate limiting threshold and attack threshold of ICMP guard to **100** pps and **200** pps for each interface on GigabitEthernet 0/1 and to **5** pps and **10** pps for each source IP address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp icmp-guard policy per-port 100 200
Hostname(config-if-GigabitEthernet 0/1)# nfpp icmp-guard policy per-src-ip 5 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.76 nfpp ip-guard enable

Function

Run the **nfpp ip-guard enable** command to enable the IP guard function on an interface.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

No IP guard function is configured on an interface by default. The global IP guard function is enabled.

Syntax

nfpp ip-guard enable

no nfpp ip-guard enable

default nfpp ip-guard enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The IP guard function on an interface takes precedence over the function of global IP guard.

If the function of ARP source suppression is enabled and the isolation time is configured for the IP guard function in global or interface configuration mode, an error is reported when you enable the IP guard function.

Examples

The following example enables the IP guard function on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp ip-guard enable
```

Notifications

No notification can be configured.

```
Configuration is prohibited, please disable the arp-guard suppression function
first!
```

Common Errors

If the function of ARP source suppression is configured on an interface and the isolation time is configured for the IP guard function in global or interface configuration mode, an error is reported when you configure the IP guard function on this interface.

Platform Description

N/A

Related Commands

N/A

1.77 nfpp ip-guard isolate-period

Function

Run the **nfpp ip-guard isolate-period** command to configure the local isolation time of IP guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No isolation time of IP guard is configured by default. The global isolation time of IP guard is used.

Syntax

nfpp ip-guard isolate-period { *interval* | **permanent** }

no nfpp ip-guard isolate-period

default nfpp ip-guard isolate-period

Parameter Description

interval: Configured isolation time, in seconds. The value is **0** or the value range is from 30 to 86400. The value **0** specifies no isolation.

permanent: Configures permanent isolation.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

If you have configured the function of ARP source suppression, you cannot configure the isolation time for the IP guard function.

Examples

The following example sets the local isolation time of IP guard on GigabitEthernet 0/1 to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp ip-guard isolate-period 180
```

Notifications

If you have configured the function of ARP source suppression, the following notification will be displayed when you configure isolation time for IP guard:

```
Configuration is prohibited, please disable the arp-guard suppression function
first!
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.78 nfpp ip-guard policy

Function

Run the **nfpp ip-guard policy** command to configure a local rate limiting threshold and a local attack threshold of IP guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No local rate limiting threshold or local attack threshold of IP guard is configured on an interface by default. The global rate limiting threshold and global attack threshold of IP guard are used.

Syntax

nfpp ip-guard policy { **per-port** *rate-limit attack-threshold* | **per-src-ip** *rate-limit attack-threshold* }

no nfpp ip-guard policy { **per-port** | **per-src-ip** }

default nfpp ip-guard policy { **per-port** | **per-src-ip** }

Parameter Description

per-port: Configures a rate limiting threshold and an attack threshold for each interface.

per-src-ip: Configures a rate limiting threshold and an attack threshold for each source IP address.

rate-limit: Configured rate limiting threshold, in pps. The value range is from 1 to 19999.

attack-threshold: Configured attack threshold, in pps. The value range is from 1 to 19999.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The attack threshold must be equal to or greater than the rate limiting threshold.

Examples

The following example sets the rate limiting threshold and attack threshold of IP guard to **50** pps and **100** pps for each interface on GigabitEthernet 0/1 and to **2** pps and **10** pps for each source IP address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp ip-guard policy per-port 50 100
Hostname(config-if-GigabitEthernet 0/1)# nfpp ip-guard policy per-src-ip 2 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.79 nfpp ip-guard scan-threshold

Function

Run the **nfpp ip-guard scan-threshold** command to configure the local scanning threshold of IP guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No scanning threshold of IP guard is configured on an interface by default. The global scanning threshold of IP guard is used.

Syntax

nfpp ip-guard scan-threshold *scan-threshold*

no nfpp ip-guard scan-threshold

default nfpp ip-guard scan-threshold

Parameter Description

scan-threshold: Configured scanning threshold, in packets per 10 seconds. The value range is from 1 to 19999.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the scanning threshold of IP guard on GigabitEthernet 0/1 to 20 packets per 10 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp ip-guard scan-threshold 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.80 nfpp nd-guard enable

Function

Run the **nfpp nd-guard enable** command to enable the ND guard function on an interface.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The ND guard function is not configured on an interface by default. The function of global ND guard is used.

Syntax

nfpp nd-guard enable

no nfpp nd-guard enable

default nfpp nd-guard enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The ND guard function on an interface takes precedence over the global ND guard function.

Examples

The following example enables the ND guard function on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp nd-guard enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.81 nfpp nd-guard policy per-port

Function

Run the **nfpp nd-guard policy per-port** command to configure a local rate limiting threshold and a local attack threshold of ND guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No local rate limiting threshold or local attack threshold of ND guard is configured on an interface by default. The global rate limiting threshold and global attack threshold of ND guard are used.

Syntax

nfpp nd-guard policy per-port { **ndsnp** *rate-limit attack-threshold* | **ns-na** *rate-limit attack-threshold* | **ra-redirect** *rate-limit attack-threshold* | **rs** *rate-limit attack-threshold* }

no nfpp nd-guard policy per-port { **ndsnp** | **ns-na** | **ra-redirect** | **rs** }

default nfpp nd-guard policy per-port { **ndsnp** | **ns-na** | **ra-redirect** | **rs** }

Parameter Description

ndsnp: Configures a rate limiting threshold and an attack threshold for NDSNP packets. After the **ipv6 nd snooping enable** command is enabled in global configuration mode, all ND packets are NDSNP packets.

ns-na: Configures a rate limiting threshold and an attack threshold for neighbor requests and advertisements.

ra-redirect: Configures a rate limiting threshold and an attack threshold for route advertisements and redirection packets.

rs: Configures a rate limiting threshold and an attack threshold for route requests.

rate-limit: Configured rate limiting threshold, in pps. The value range is from 1 to 19999.

attack-threshold: Configured attack threshold, in pps. The value range is from 1 to 19999.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The attack threshold must be equal to or greater than the rate limiting threshold.

Examples

The following example sets the local rate limiting threshold and local attack threshold of ND guard to **5** pps and **10** pps for NDSNP packets on interface GigabitEthernet 0/1, to **50** pps and **100** pps for neighbor requests and advertisements, to **10** pps and **20** pps for route advertisements and redirection packets, and to **10** pps and **20** pps for route requests.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp nd-guard policy per-port ndsnp 5 10
Hostname(config-if-GigabitEthernet 0/1)# nfpp nd-guard policy per-port ns-na 50
100
Hostname(config-if-GigabitEthernet 0/1)# nfpp nd-guard policy per-port ra-
redirect 10 20
Hostname(config-if-GigabitEthernet 0/1)# nfpp nd-guard policy per-port rs 10 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.82 nfpp tcp-syn-guard enable

Function

Run the **nfpp tcp-syn-guard enable** command to enable the TCP-SYN guard function on an interface.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The TCP-SYN guard function is not configured on an interface by default. The function of global TCP-SYN function is used.

Syntax

nfpp tcp-syn-guard enable

no nfpp tcp-syn-guard enable

default nfpp tcp-syn-guard enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The TCP-SYN guard function on an interface takes precedence over the global TCP-SYN guard function.

Examples

The following example enables the TCP-SYN guard function on interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp tcp-syn-guard enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.83 nfpp tcp-syn-guard isolate-period

Function

Run the **nfpp tcp-syn-guard isolate-period** command to configure the local isolation time of TCP-SYN guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No local isolation time of TCP-SYN guard is configured by default. The global isolation time of TCP-SYN guard is used.

Syntax

nfpp tcp-syn-guard isolate-period { *interval* | **permanent** }

no nfpp tcp-syn-guard isolate-period

default nfpp tcp-syn-guard isolate-period

Parameter Description

interval: Configured isolation time, in seconds. The value is **0** or the value range is from 30 to 86400. The value **0** specifies no isolation.

permanent: Configures permanent isolation.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the local isolation time of TCP-SYN guard on interface GigabitEthernet 0/1 to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp tcp-syn-guard isolate-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.84 nfpp tcp-syn-guard policy

Function

Run the **nfpp tcp-syn-guard policy** command to configure a local rate limiting threshold and a local attack threshold of TCP-SYN guard on an interface.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No local rate limiting threshold or local attack threshold of TCP-SYN guard is configured on an interface by default. The global rate limiting threshold and attack threshold of TCP-SYN guard are used.

Syntax

nfpp tcp-syn-guard policy { **per-port** *rate-limit attack-threshold* | **per-src-ip** *rate-limit attack-threshold* }

no nfpp tcp-syn-guard policy { **per-port** | **per-src-ip** }

default nfpp tcp-syn-guard policy { **per-port** | **per-src-ip** }

Parameter Description

per-port: Configures a rate limiting threshold and an attack threshold for each interface.

per-src-ip: Configures a rate limiting threshold and an attack threshold for each source IP address.

rate-limit: Configured rate limiting threshold, in pps. The value range is from 1 to 19999.

attack-threshold: Configured attack threshold, in pps. The value range is from 1 to 19999.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

The attack threshold must be equal to or greater than the rate limiting threshold.

Examples

The following example sets the rate limiting threshold and attack threshold of TCP-SYN guard to **50** pps and **100** pps for each interface on interface GigabitEthernet 0/1 and to **2** pps and **10** pps for each source IP address.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nfpp tcp-syn-guard policy per-port 50
100
Hostname(config-if-GigabitEthernet 0/1)# nfpp tcp-syn-guard policy per-src-ip 2
10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.85 show nfpp arp-guard hosts

Function

Run the **show nfpp arp-guard hosts** command to display the monitored hosts of ARP guard.

Syntax

show nfpp arp-guard hosts [**statistics** | [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*ipv4-address* | *mac-address*]]

Parameter Description

statistics: Displays the statistics about the monitored hosts.

vlan *vlan-id*: Displays the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Displays the monitored hosts of a specified interface.

ipv4-address: Specified IPv4 address of a monitored host to be displayed. Whether this parameter is supported depends on the actual product version.

mac-address: Specified MAC address of a monitored host.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the statistics about the monitored hosts of ARP guard.

```
Hostname> enable
Hostname# show nfpp arp-guard hosts statistics
success    fail    total
---    --    -------
100       20      120
```

Table 1-1 Output Field of the show nfpp arp-guard hosts statistics Command

Field	Description
Success	Number of isolated hosts
Fail	Number of hosts failed to be isolated
total	Number of monitored hosts

The following example displays the monitored hosts of ARP guard.

```
Hostname# 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
```

Table 1-2Output Field of the show nfpp arp-guard hosts Command

Field	Description
VLAN	VLAN ID of a host
interface	Interface name of a host
IP address	IP address of a host
MAC address	MAC address of a host
remain-time	Remaining isolation time
Total: *number* hosts	Total number of monitored hosts. *number* specifies the specific number of hosts.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.86 show nfpp arp-guard scan

Function

Run the **show nfpp arp-guard scan** command to display the scanning table of ARP guard.

Syntax

show nfpp arp-guard scan [**statistics** | [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*mac-address*]]

Parameter Description

statistics: Displays the statistics about the scanning table.

vlan *vlan-id*: Displays the scanning table of a specified VLAN ID.

interface *interface-type interface-number*: Displays the scanning table of a specified interface.

mac-address: Specified MAC address of a scanning table.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the statistics about the scanning table of ARP guard.

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

Table 1-1Output Field of the show nfpp arp-guard scan statistics Command

Field	Description
arp-guard scan table has *number* record(s).	Displays the number of records in the scanning table. *number* specifies the number of records in the scanning table.

The following example displays the scanning table of ARP guard. "timestamp" specifies the detection time of ARP scanning. For example, "2008-01-23 16:23:10" specifies that ARP scanning time is detected at 16:23:10 on January 23, 2008.

```
Hostname> enable
Hostname# 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)
```

Table 1-2Output Field of the show nfpp arp-guard hosts Command

Field	Description
VLAN	VLAN ID of the ARP scanning information
interface	Interface name of the ARP scanning information
IP address	IP address of the ARP scanning information
MAC address	MAC address of the ARP scanning information
timestamp	Detection time of the ARP scanning
Total: *number* record(s)	Total number of records in the ARP scanning table. *number* specifies the specific number of records in the scanning table.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.87 show nfpp arp-guard summary

Function

Run the **show nfpp arp-guard summary** command to display the configuration information of ARP guard.

Syntax

show nfpp arp-guard summary

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration information of ARP guard.

```
Hostname> enable
Hostname# 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
Suppress-mode: disable
Suppress-threshold: 5pps
Suppress-period: 5s
```

Table 1-1 Output Field of the show nfpp arp-guard summary Command

Field	Description
Interface	Interface. **Global** specifies global configuration.
Status	Whether the guard function is enabled: ● **Enable**: The function is enabled.

Field	Description
	● **Disable**: The function is disabled.
Isolat-period	Isolation period configured in a policy, in seconds
Rate-limit	Rate limiting thresholds for a source IP address, source MAC address, and interface respectively
Attack-threshold	Attack thresholds for a source IP address, source MAC address, and interface respectively
Scan-threshold	Scanning threshold
Maximum count of monitored hosts	Maximum number of monitored hosts
Monitor period	Monitoring period, in seconds
suppress-mode	Whether the suppression mode is enabled: ● **Enable**: The mode is enabled. ● **Disable**: The mode is disabled.
suppress-threshold	Suppression threshold, in pps
suppress-period	Suppression period, in seconds

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.88 show nfpp define hosts

Function

Run the **show nfpp define hosts** command to display the monitored hosts of a customized guard type.

Syntax

show nfpp define hosts *name* [**statistics** | [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*ipv4-address* | *mac-address* | *ipv6-address*]]

Parameter Description

name: Name of a specified customized guard type.

statistics: Displays the statistics about the monitored hosts.

vlan *vlan-id*: Displays the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Displays the monitored hosts of a specified interface.

ipv4-address: Specified IPv4 address of a monitored host to be displayed.

mac-address: Specified MAC address of a monitored host.

ipv6-address: Specified IPv6 address of a monitored host.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

Parameters can be configured in the command to filter unwanted monitored hosts.

Examples

The following example displays the monitored hosts of a customized TCP guard type.

```
Hostname> enable
Hostname# show nfpp define hosts tcp
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
```

Table 1-1Output Field of the show nfpp define hosts Command

Field	Description
VLAN	VLAN ID of a host
interface	Interface name of a host
MAC address	MAC address of a host
remain-time	Remaining isolation time of a host, in seconds
Total: *number* hosts	Total number of monitored hosts. *number* specifies the specific number of hosts.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.89 show nfpp define summary

Function

Run the **show nfpp define summary** command to display the configuration information of a customized summary type.

Syntax

show nfpp define summary [*name*]

Parameter Description

name: Name of a specified customized guard type.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration information of the customized TCP guard type.

```
Hostname> enable
Hostname# 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  -/-           -/-/-
```

Table 1-1Output Field of the show nfpp define summary Command

Field	Description
Define *name* summary	Configuration of a specified customized guard type. *name* specifies the name of a customized guard type.
match etype *etype* src-ip *source-ipv4-address* src-ip-mask *source-mask*	Matched packet types of a customized guard type
Maximum count of monitored hosts	Maximum number of monitored hosts
Monitor period	Monitoring time, in seconds

Field	Description
Interface	Interface. **Global** specifies global configuration.
Status	Whether the guard function is enabled: ● **Enable**: The function is enabled. ● **Disable**: The function is disabled.
Rate-limit	Rate limiting thresholds for a source IP address, source MAC address, and interface respectively
Attack-threshold	Attack thresholds for a source IP address, source MAC address, and interface respectively

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.90 show nfpp define trusted-host

Function

Run the **show nfpp define trusted-host** command to display the trusted hosts of a customized guard type.

Syntax

show nfpp define trusted-host *name*

Parameter Description

name: Name of a customized guard type.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the trusted hosts of the customized TCP guard type.

```
Hostname> enable
```

```
Hostname# 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)
```

Table 1-1Output Field of the show nfpp define trusted-host Command

Field	Description
Define *name*	Information of a specified customized guard type. *name* specifies the name of a customized guard type.
IP address	IP address of a trusted host
mask	Subnet mask of a trusted host
Total: *number* record(s)	Total number of trusted hosts. *number* -specifies the specific number of hosts.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.91 show nfpp dhcp-guard hosts

Function

Run the **show nfpp dhcp-guard hosts** command to display the monitored hosts of DHCP guard.

Syntax

show nfpp dhcp-guard hosts [**statistics** | [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*mac-address*]]

Parameter Description

statistics: Displays the statistics about the monitored hosts.

vlan *vlan-id*: Displays the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Displays the monitored hosts of a specified interface.

mac-address: Specified MAC address of a monitored host.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the statistics about the monitored hosts of DHCP guard.

```
Hostname> enable
Hostname# show nfpp dhcp-guard hosts statistics
success    fail    total
---    --    --
100         20        120
```

Table 1-1Output Field of the show nfpp dhcp-guard hosts statistics Command

Field	Description
success	Number of isolated hosts
Fail	Number of hosts failed to be isolated
total	Number of monitored hosts

The following example displays the monitored hosts of DHCP guard.

```
Hostname> enable
Hostname# 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)
```

Table 1-2Output Field of the show nfpp dhcp-guard hosts Command

Field	Description
VLAN	VLAN ID of a host
interface	Interface name of a host
IP address	IP address of a host
MAC address	MAC address of a host
remain-time	Remaining isolation time

Field	Description
Total: *number* hosts	Total number of monitored hosts. *number* specifies the specific number of hosts.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.92 show nfpp dhcp-guard summary

Function

Run the **show nfpp dhcp-guard summary** command to display the configuration information of DHCP guard.

Syntax

show nfpp dhcp-guard summary

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration information of DHCP guard.

```
Hostname> enable
Hostname# 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
```

Table 1-1Output Field of the show nfpp dhcp-guard summary Command

Field	Description
Interface	Interface. **Global** specifies global configuration.
Status	Whether the guard function is enabled: ● **Enable**: The function is enabled. ● **Disable**: The function is disabled.
Isolate-period	Isolation period configured in a policy
Rate-limit	Rate limiting thresholds for a source IP address, source MAC address, and interface respectively
Attack-threshold	Attack thresholds for a source IP address, source MAC address, and interface respectively
Maximum count of monitored hosts	Maximum number of monitored hosts
Monitor period	Monitoring period, in seconds

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.93 show nfpp dhcpv6-guard hosts

Function

Run the **show nfpp dhcpv6-guard hosts** command to display the monitored hosts of DHCPv6 guard.

Syntax

show nfpp dhcpv6-guard hosts [**statistics** | [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*mac-address*]]

Parameter Description

statistics: Displays the statistics about the monitored hosts.

vlan *vlan-id*: Displays the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Displays the monitored hosts of a specified interface.

mac-address: Specified MAC address of a monitored host.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the monitored hosts of DHCPv6 guard.

```
Hostname> enable
Hostname# 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)
```

Table 1-1Output Field of the show nfpp dhcpv6-guard hosts Command

Field	Description
VLAN	VLAN ID of a host
interface	Interface name of a host
MAC address	MAC address of a host
remain-time(seconds)	Remaining isolation time for a host
Total	Maximum number of monitored hosts

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.94 show nfpp dhcpv6-guard summary

Function

Run the **show nfpp dhcpv6-guard summary** command to display the configuration information of DHCPv6 guard.

Syntax

show nfpp dhcpv6-guard summary

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration information of DHCPv6 guard.

```
Hostname> enable
Hostname# 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
```

Table 1-1Output Field of the show nfpp dhcpv6-guard summary Command

Field	Description
Interface	Interface. **Global** specifies global configuration.
Status	Whether the guard function is enabled: ● **Enable**: The function is enabled. ● **Disable**: The function is disabled.
Rate-limit	Rate limiting thresholds for a source IP address, source MAC address, and interface respectively
Attack-threshold	Attack thresholds for a source IP address, source MAC address, and interface respectively
Maximum count of monitored	Maximum number of monitored hosts

Field	Description
hosts	
Monitor period	Monitoring period, in seconds

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.95 show nfpp icmp-guard hosts

Function

Run the **show nfpp icmp-guard hosts** command to display the monitored hosts of ICMP guard.

Syntax

show nfpp icmp-guard hosts [**statistics** | [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*ipv4-address*]]

Parameter Description

statistics: Displays the statistics about the monitored hosts.

vlan *vlan-id*: Displays the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Displays the monitored hosts of a specified interface.

ipv4-address: Specified IPv4 address of a monitored host to be displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the statistics about the monitored hosts of ICMP guard.

```
Hostname> enable
Hostname# show nfpp icmp-guard hosts statistics
success    fail    total
---    --    ---
```

```
100         20        120
```

Table 1-1Output Field of the show nfpp icmp-guard hosts statistics Command

Field	Description
success	Number of isolated hosts
fail	Number of hosts failed to be isolated
total	Number of monitored hosts

The following example displays the monitored hosts of ICMP guard.

```
Hostname> enable
Hostname# 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)
```

Table 1-2Output Field of the show nfpp icmp-guard hosts Command

Field	Description
VLAN	VLAN ID of a host
interface	Interface name of a host
IP address	IP address of a host
MAC address	MAC address of a host
remain-time	Remaining isolation time
Total: *number* hosts	Total number of monitored hosts. *number* specifies the specific number of hosts.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.96 show nfpp icmp-guard summary

Function

Run the **show nfpp icmp-guard summary** command to display the configuration information of ICMP guard.

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration information of ICMP guard.

```
Hostname> enable
Hostname# 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
```

Table 1-1Output Field of the show nfpp icmp-guard summary Command

Field	Description
Interface	Interface. **Global** specifies global configuration.
Status	Whether the guard function is enabled: ● **Enable**: The function is enabled. ● **Disable**: The function is disabled.
Isolate-period	Isolation period configured in a policy
Rate-limit	Rate limiting thresholds for a source IP address, source MAC address, and interface respectively
Attack-threshold	Attack thresholds for a source IP address, source MAC address, and interface respectively
Maximum count of monitored	Maximum number of monitored hosts

Field	Description
hosts	
Monitor period	Monitoring period, in seconds

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.97 show nfpp icmp-guard trusted-host

Function

Run the **show nfpp icmp-guard trusted-host** command to display the trusted hosts of ICMP guard.

Syntax

show nfpp icmp-guard trusted-host

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the monitored trusted hosts of ICMP guard.

```
Hostname> enable
Hostname# 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)
```

Table 1-1Output Field of the show nfpp icmp-guard trusted-host Command

Field	Description
IP address	IP address of a trusted host
mask	Subnet mask of a trusted host
Total	Total number of trusted hosts

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.98 show nfpp ip-guard hosts

Function

Run the **show nfpp ip-guard hosts** command to display the monitored hosts of IP guard.

Syntax

show nfpp ip-guard hosts [**statistics** | [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*ipv4-address*]]

Parameter Description

statistics: Displays the statistics about the monitored hosts.

vlan *vlan-id*: Displays the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Displays the monitored hosts of a specified interface.

ipv4-address: Specified IPv4 address of a monitored host to be displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the statistics about the monitored hosts of IP guard.

```
Hostname> enable
```

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

Table 1-1Output Field of the show nfpp ip-guard hosts statistics Command

Field	Description
success	Number of isolated hosts
fail	Number of hosts failed to be isolated
total	Number of monitored hosts

The following example displays the monitored hosts of IP guard.

```
Hostname> enable
Hostname# 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)
```

Table 1-2Output Field of the show nfpp ip-guard hosts Command

Field	Description
VLAN	VLAN ID of a host
interface	Interface name of a host
IP address	IP address of a host
Reason	Reason of host monitoring: ● **ATTACK**: Specifies that IP packets are sent at a rate higher than the attack threshold. ● **SCAN**: Specifies that a host is scanning a network segment.
remain-time	Remaining isolation time
Total: *number* hosts	Total number of monitored hosts. *number* specifies the specific number of hosts.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.99 show nfpp ip-guard summary

Function

Run the **show nfpp ip-guard summary** command to display the configuration information of IP guard.

Syntax

show nfpp ip-guard summary

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration information of IP guard.

```
Hostname> enable
Hostname# 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
```

Table 1-1Output Field of the show nfpp ip-guard summary Command

Field	Description
Interface	Interface. **Global** specifies global configuration.
Status	Whether the guard function is enabled: ● **Enable**: The function is enabled. ● **Disable**: The function is disabled.
Isolate-period	Isolation period configured in a policy

Field	Description
Rate-limit	Rate limiting thresholds for a source IP address, source MAC address, and interface respectively
Attack-threshold	Attack thresholds for a source IP address, source MAC address, and interface respectively
Scan-threshold	Scanning threshold
Maximum count of monitored hosts	Maximum number of monitored hosts
Monitor period	Monitoring period, in seconds

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.100 show nfpp ip-guard trusted-host

Function

Run the **show nfpp ip-guard trusted-host** command to display the trusted hosts of IP guard.

Syntax

show nfpp ip-guard trusted-host

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the trusted hosts of IP guard.

```
Hostname> enable
Hostname# 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)
```

Table 1-1Output Field of the show nfpp ip-guard trusted-host Command

Field	Description
IP address	IP address of a trusted host
mask	Subnet mask of a trusted host
Total	Total number of trusted hosts

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.101 show nfpp log buffer

Function

Run the **show nfpp log buffer** command to display the information in the log buffer of NFPP.

Syntax

show nfpp log buffer

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

When the log buffer overflows, subsequent logs are discarded, and the log buffer displays an entry with attributes being "-". In this case, the administrator must increase the log buffer size or improve the generation rate of system messages.

The system message generated from logs of the log buffer carries the event timestamp, as shown below:

```
%NFPP_ARP_GUARD-DOS_DETECTED: Host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1>
was detected.(2009-07-01 13:00:00)
```

Examples

The following example displays the log buffer of NFPP.

```
Hostname> enable
Hostname# 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
ND-SNP 258    Te0/1      -          -                PORT_ATTACKED    2019-28
9:31:39
```

Table 1-1Output Field of the show nfpp log buffer Command

Field	Description
Protocol	Corresponding packet protocol
VLAN	VLAN ID
Interface	Corresponding interface
IP address	Corresponding IP address
MAC address	Corresponding MAC address
Reason	Reason for recording
Timestamp	Timestamp of recording

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.102 show nfpp log buffer statistics

Function

Run the **show nfpp log buffer statistics** command to display the statistics about the log buffer of NFPP.

Syntax

show nfpp log buffer statistics

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the statistics about the log buffer of NFPP.

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

Table 1-1 Output Field of the show nfpp log buffer statistics Command

Field	Description
There are *number* logs in buffer.	Number of logs in the log buffer. *number* specifies the specific number.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.103 show nfpp log summary

Function

Run the **show nfpp log summary** command to display the configuration information of NFPP logs.

Syntax

show nfpp log summary

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration information of NFPP logs.

```
Hostname> enable
Hostname# 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
```

Table 1-1 Output Field of the show nfpp log summary Command

Field	Description
Total log buffer size	Buffer size
Syslog rate	Log print rate
Logging	Recorded VLAN and interface information

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.104 show nfpp nd-guard hosts

Function

Run the **show nfpp nd-guard hosts** command to display the monitored hosts of ND guard.

Syntax

show nfpp nd-guard hosts [**statistics** | [**vlan** *vlan-id*] [**interface** *interface-type interface-number*]]

Parameter Description

statistics: Displays the statistics about the monitored hosts.

vlan *vlan-id*: Displays the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Displays the monitored hosts of a specified interface.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the statistics about the monitored hosts of ND guard.

```
Hostname> enable
Hostname# show nfpp nd-guard hosts statistics
success    fail    total
---    --    --
10         2        12
```

Table 1-1Output Field of the show nfpp nd-guard hosts statistics Command

Field	Description
success	Number of isolated hosts
fail	Number of hosts failed to be isolated
total	Number of monitored hosts

The following example displays the monitored hosts of ND guard.

```
Hostname> enable
Hostname# 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
```

Table 1-2Output Field of the show nfpp nd-guard hosts Command

Field	Description
VLAN	VLAN ID of a host
interface	Interface name of a host
ND-guard	Packet type of ND guard
remain-time	Remaining isolation time
Total: *number* hosts	Total number of monitored hosts. *number* specifies the specific number of hosts.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.105 show nfpp nd-guard summary

Function

Run the **show nfpp nd-guard summary** command to display the configuration information of ND guard.

Syntax

show nfpp nd-guard summary

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration information of ND guard, including global configuration information and configuration information on an interface.

```
Hostname> enable
Hostname# show nfpp nd-guard summary
(Format of column Rate-limit and  Attack-threshold is NS-NA/RS/RA-REDIRECT/ND-
SNP.)
Interface  Status  Rate-limit Attack-threshold
Global      Enable  20/5/10/25     40/10/20/50
Gi 0/1       Enable  15/15/15/25    30/30/30/50
Gi 0/2       Disable -/5/30/25       -/10/50/50
```

Table 1-1Output Field of the show nfpp nd-guard summary Command

Field	Description
Interface	Interface. **Global** specifies global configuration.
Status	Whether the guard function is enabled: ● **Enable**: The function is enabled. ● **Disable**: The function is disabled.
Rate-limit	Rate limiting thresholds for neighbor requests and advertisements, route requests, route advertisement and redirection packets, and NDSNP packets respectively
Attack-threshold	Attack thresholds for neighbor requests and advertisements, route requests, route advertisement and redirection packets, and NDSNP packets respectively

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.106 show nfpp tcp-syn-guard hosts

Function

Run the **show nfpp tcp-syn-guard hosts** command to display the monitored hosts of TCP-SYN guard.

Syntax

show nfpp tcp-syn-guard hosts [**statistics** | [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [*ipv4-address*]]

Parameter Description

statistics: Displays the statistics about the monitored hosts.

vlan *vlan-id*: Displays the monitored hosts of a specified VLAN ID.

interface *interface-type interface-number*: Displays the monitored hosts of a specified interface.

ipv4-address: Specified IPv4 address of a monitored host to be displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the statistics about the monitored hosts of TCP-SYN guard.

```
Hostname> enable
Hostname# show nfpp tcp-syn-guard hosts statistics
success    fail    total
---    --    ---
100         20        120
```

Table 1-1Output Field of the show nfpp tcp-syn-guard hosts statistics Command

Field	Description
success	Number of isolated hosts
fail	Number of hosts failed to be isolated
total	Number of monitored hosts

The following example displays the monitored hosts of TCP-SYN guard.

```
Hostname> enable
Hostname# show nfpp tcp-syn-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)
```

Table 1-2Output Field of the show nfpp tcp-syn-guard hosts Command

Field	Description
VLAN	VLAN ID of a host
interface	Interface name of a host
IP address	IP address of a host
Reason	Reason for host monitoring: ● **ATTACK**: Specifies that TCP-SYN packets are sent at a rate higher than the attack threshold. ● **SCAN**: Specifies that a host is scanning a network segment.
remain-time	Remaining isolation time
Total: *number* hosts	Total number of monitored hosts. *number* specifies the specific number of hosts.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.107 show nfpp tcp-syn-guard summary

Function

Run the **show nfpp tcp-syn-guard summary** command to display the configuration information of TCP-SYN guard.

Syntax

show nfpp tcp-syn-guard summary

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration information of TCP-SYN guard.

```
Hostname> enable
Hostname# show nfpp tcp-syn-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
```

Table 1-1 Output Field of the show nfpp tcp-syn-guard summary Command

Field	Description
Interface	Interface. **Global** specifies global configuration.
Status	Whether the guard function is enabled: ● **Enable**: The function is enabled. ● **Disable**: The function is disabled.
Isolate-period	Isolation period configured in a policy
Rate-limit	Rate limiting thresholds for a source IP address, source MAC address, and interface respectively
Attack-threshold	Attack thresholds for a source IP address, source MAC address, and interface respectively
Maximum count of monitored hosts	Maximum number of monitored hosts
Monitor period	Monitoring period, in seconds

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.108 show nfpp tcp-syn-guard trusted-host

Function

Run the **show nfpp tcp-syn-guard trusted-host** command to display the trusted hosts of TCP-SYN guard.

Syntax

show nfpp tcp-syn-guard trusted-host

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the trusted hosts of TCP-SYN guard.

```
Hostname> enable
Hostname# show nfpp tcp-syn-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)
```

Table 1-1 Output Field of the show nfpp tcp-syn-guard trusted-host Command

Field	Description
IP address	IP address of a trusted host
mask	Subnet mask of a trusted host
Total	Total number of trusted hosts

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.109 tcp-syn-guard attack-threshold

Function

Run the **tcp-syn-guard attack-threshold** command to configure the global attack threshold of TCP-SYN guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The global attack threshold of TCP-SYN guard for each interface is 200 pps and for each source IP address is 100 pps by default.

Syntax

tcp-syn-guard attack-threshold { **per-port** *attack-threshold* | **per-src-ip** *attack-threshold* }

no tcp-syn-guard attack-threshold { **per-port** | **per-src-ip** }

default tcp-syn-guard attack-threshold { **per-port** | **per-src-ip** }

Parameter Description

per-port *attack-threshold*: Configures an attack threshold for each interface, in pps. The value range is from 1 to 19999.

per-src-ip *attack-threshold*: Configures an attack threshold for each source IP address, in pps. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

The attack threshold must be equal to or greater than the rate limiting threshold.
TCP-SYN guard is to solve TCP-SYN attacks on the destination IP address, but not the local IP address. If the destination IP address is a local IP address, the rates of IP packets are limited by the function of CPU protect policy (CPP).

Examples

The following example sets the global attack thresholds of TCP-SYN guard to **50** pps and **2** pps for each interface and source IP address respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# tcp-syn-guard attack-threshold per-port 50
Hostname(config-nfpp)# tcp-syn-guard attack-threshold per-src-ip 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.110 tcp-syn-guard enable

Function

Run the **tcp-syn-guard enable** command to enable the global TCP-SYN guard function.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The global TCP-SYN guard function is enabled by default.

Syntax

tcp-syn-guard enable

no tcp-syn-guard enable

default tcp-syn-guard enable

Parameter Description

N/A

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the global TCP-SYN guard function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# tcp-syn-guard enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.111 tcp-syn-guard isolate-period

Function

Run the **tcp-syn-guard isolate-period** command to configure the global isolation time of TCP-SYN guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default global isolation time of TCP-SYN guard is **0**.

Syntax

tcp-syn-guard isolate-period { *interval* | **permanent** }

no tcp-syn-guard isolate-period

default tcp-syn-guard isolate-period

Parameter Description

interval: Configured isolation time, in seconds. The value is **0** or the value range is from 30 to 86400.

permanent: Configures permanent isolation.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the global isolation time of TCP-SYN guard to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# tcp-syn-guard isolate-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.112 tcp-syn-guard monitored-host-limit

Function

Run the **tcp-syn-guard monitored-host-limit** command to configure the maximum number of monitored hosts of TCP-SYN guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The maximum number of monitored hosts of TCP-SYN guard is **20000** by default.

Syntax

tcp-syn-guard monitored-host-limit *number*

no tcp-syn-guard monitored-host-limit

default tcp-syn-guard monitored-host-limit

Parameter Description

number: Configured maximum number of monitored hosts. The value range is from 1 to 4294967295.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When the number of monitored hosts reaches the default value **20000**, the monitored hosts are not deleted if the administrator sets the maximum number of monitored hosts to a value smaller than 20000. An alarm message "%ERROR: The value that you configured is smaller than current monitored hosts 20000 (number of monitored hosts), please clear a part of monitored hosts." is printed to remind users of configuration failure and the need to delete clear some monitored hosts.

When the table of monitored hosts is full, the log "% NFPP_TCP_SYN_GUARD-SESSION_LIMIT: Attempt to exceed limit of IP 20000 (number of monitored hosts) monitored hosts." is printed to remind the administrator.

Examples

The following example sets the maximum number of monitored hosts of TCP-SYN guard to **200**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# tcp-syn-guard monitored-host-limit 200
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.113 tcp-syn-guard monitor-period

Function

Run the **tcp-syn-guard monitor-period** command to configure the monitoring time of TCP-SYN guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The default monitoring time of TCP-SYN guard is **600** seconds.

Syntax

tcp-syn-guard monitor-period *interval*

no tcp-syn-guard monitor-period

default tcp-syn-guard monitor-perio

Parameter Description

interval: Configured monitoring time, in seconds. The value range is from 180 to 86400.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

When TCP-SYN guard detects an attacker, if the isolation time is 0, this function monitors the attacker through software and the timeout time is the monitoring time. During software monitoring, when the isolation time is configured as a non-zero value, this function automatically isolates the attacker under software monitoring and

the timeout time is configured as the isolation time. The monitoring time takes effect when the isolation time is 0.

If you change the isolation time to 0 from a non-zero value, the isolated attacker is directly deleted without monitoring the attacker through software.

Examples

The following example sets the monitoring time of TCP-SYN guard to **180** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# tcp-syn-guard monitor-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.114 tcp-syn-guard rate-limit

Function

Run the **tcp-syn-guard rate-limit** command to configure the global rate limiting threshold of TCP-SYN guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the global rate limiting threshold of TCP-SYN guard for each interface is 50 pps and for each source IP address is 20 pps.

Syntax

tcp-syn-guard rate-limit { **per-port** *rate-limit* | **per-src-ip** *rate-limit* }

no tcp-syn-guard rate-limit { **per-port** | **per-src-ip** }

default tcp-syn-guard rate-limit { **per-port** | **per-src-ip** }

Parameter Description

per-port *rate-limit*: Configures a rate limiting threshold for each interface, in pps. The value range is from 1 to 19999.

per-src-ip *rate-limit*: Configures a rate limiting threshold for each source IP address, in pps. The value range is from 1 to 19999.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the global rate limiting thresholds of TCP-SYN guard to **40** pps and **2** pps for each interface and source IP address respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# tcp-syn-guard rate-limit per-src-ip 2
Hostname(config-nfpp)# tcp-syn-guard rate-limit per-port 40
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.115 tcp-syn-guard trusted-host

Function

Run the **tcp-syn-guard trusted-host** command to configure the trusted hosts of TCP-SYN guard.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No host is configured as a trusted host of TCP-SYN guard by default.

Syntax

tcp-syn-guard trusted-host *ipv4-address mask*

no tcp-syn-guard trusted-host { *ipv4-address mask* | **all** }

default tcp-syn-guard trusted-host

Parameter Description

ipv4-address mask: IPv4 address+mask. The mask is entered in dotted decimal mode.

all: Deletes the configuration of all trusted hosts when this parameter is used with the **no** parameter.

Command Modes

NFPP configuration mode

Default Level

14

Usage Guidelines

To cancel the monitoring of a host, the administrator can run this command to configure the host as a trusted host. In this case, IP packets sent by this host can be forwarded to the CPU without rate limit or alarm.

A maximum of 500 trusted hosts can be configured.

Examples

The following example configures all hosts in the network segment 1.1.1.0/24 as trusted hosts of TCP-SYN guard.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# tcp-syn-guard trusted-host 1.1.1.0 255.255.255.0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.116 trusted-host

Function

Run the **trusted-host** command to configure trusted hosts of a customized guard type.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No host is configured as a trusted host of the customized guard type by default.

Syntax

trusted-host { *ipv4-address mask* | *ipv6-address*/*prefix-length* | *mac-address mask* }

no trusted-host { *ipv4-address mask* | *ipv6-address*/*prefix-length* | *mac-address mask* | **all** }

default trusted-host

Parameter Description

ipv4-address mask: IPv4 address+mask. The mask is entered in dotted decimal mode.

ipv6-address/*prefix-length*: IPv6 address+prefix. The prefix starts with a slash (/).

Mac-address mask: MAC address and mask.

all: Deletes the configuration of all trusted hosts when this parameter is used with the **no** parameter.

Command Modes

Customized configuration mode of NFPP

Default Level

14

Usage Guidelines

To cancel the monitoring of a host, the administrator can run this command to configure the host as a trusted host. In this case, ICMP packets sent by this host can be forwarded to the CPU without rate limit or alarm. All hosts in a network segment can be configured as trusted hosts by configuring a mask.

A maximum of 500 trusted hosts can be configured.

The match type must be configured prior to the configuration of trusted hosts. If the matched packet type is IPv4, IPv6 addresses cannot be configured as trusted. If the matched packet type is IPv6, IPv4 addresses cannot be configured as trusted.

Examples

The following example configures the host 1.1.1.1 as a trusted host of the customized guard type.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# nfpp
Hostname(config-nfpp)# define tcp
Hostname(config-nfpp-define)# trusted-host 1.1.1.1 255.255.255.255
```

Notifications

N/A

Common Errors

N/A

Related Commands

N/A