Contents

1 Configuring NFPP

1.1 Introduction

Many malicious attacks exist in the network environment. If no protection policies are available, attack packets occupy the CPU resources of a device. As a result, the CPU cannot process normal protocol packets and control packets and the device does not normally run. The network foundation protection policy (NFPP) protects devices from attacks and keeps a low CPU load for the devices under attack to ensure normal operation of services and stable operation of the entire network.

1.1.1 Basic Concepts

1. ARP Guard

In a LAN, the Address Resolution Protocol (ARP) can parse an IP address into a MAC address to ensure smooth communication. The Denial of Service (DoS) is a process of sending many invalid ARP packets to a gateway in a network to cause the gateway not to provide services for normal hosts. To avoid this type of attacks, configure a rate limiting threshold for the ARP packets and isolate the source of the attack.

2. IP Guard

Hacking attack and network virus intrusion start at a host that scans network activities. Many scanned packets occupy network bandwidth and thus affect normal communication of the network. To avoid this type of attacks, we configure the IP guard function for a device. This function also reduces the CPU usage of the device. IP attacks include the following two types:

- Scan changes in the destination IP address. This type of attacks consume network bandwidth and increase device load. This indicates most of upcoming hacking attacks.
- Send IP packets to an unconfigured destination IP address. This attack is designed for the CPU of a device. On an L3 device, if a destination IP address is configured, packets are forwarded by the chip without consuming CPU resources. Otherwise, the packets are sent to the CPU and the latter sends ARP requests to request the MAC address of the destination IP address. If too many packets sent to the CPU, this consumes many CPU resources. To avoid this type of attacks, we configure a rate limiting threshold for the IP packets and isolate the source of the attack.

3. TCP SYN Guard

TCP-SYN-Flood attack is also called half-open connection attack. An attacker sends SYN packets to the target device without responding to the SYN+ACK packets returned by the target device. If it does not receive the SYN+ACK responses, the target device waits and thus a half-open connection is formed. The attacker allows the target device to generate many half-open connections with this method, forcing the target device to waste resources on the half-open connections.

The available TCP connections of a server are limited. If a malicious attacker sends this type of connection requests consecutively in an attack, the available TCP connections of this server become congested. Thus, the available system resources and available bandwidth drop dramatically, affecting normal network services. Consequently, a DoS occurs.

To avoid the TCP-SYN-Flood attack, configure the TCP SYN guard function on the device to limit the sending rates of TCP SYN packets.

4. ICMP Guard

The Internet Control Message Protocol (ICMP) is a common means of network fault diagnosis. According to the principle of ICMP, when a host sends an ICMP Echo Request packet, the receiver returns an ICMP Echo Reply upon receipt of the packet. This process requires CPU coordination. If an attacker sends many ICMP requests to the target device, many CPU resources are consumed, which may interrupt normal device operation in extreme conditions. This is called an ICMP flood attack. To avoid it, configure a rate limiting threshold for the ICMP packets and isolate the source of the attack.

5. DHCP Guard

The Dynamic Host Configuration Protocol (DHCP) is widely used in a LAN to dynamically assign IP addresses. A DHCP starvation attack is the most popular DHCP attack that broadcasts DHCP requests by using a false MAC address. When a network attacker sends enough DHCP requests, it can exhaust the address space of the DHCP server within a period. In this case, the legal host fails to request IP addresses from the DHCP server and thus cannot access a network. To avoid this type of attacks, configure a rate limiting threshold for the DHCP packets and isolate the detected source of the attack.

6. DHCPv6 Guard

DHCPv6 is widely used in a LAN to dynamically assign IPv6 addresses. Like DHCPv4, DHCPv6 has security problems. Therefore, the attack methods of DHCPv4 are applicable to DHCPv6. When a network attacker sends enough DHCPv6 requests, it can exhaust the address space of the DHCPv6 server within a period. In this case, the legal host fails to request IPv6 addresses from the DHCP server and thus cannot access a network. To avoid this type of attacks, configure a rate limiting threshold for DHCPv6 packets and isolate the detected source of the attack.

7. ND Guard

Neighbor discovery (ND) parses addresses, discovers routes and prefixes, and redirects routes in an IPv6 network. A ND process involves five types of packets: Neighbor Solicitation (NS), Neighbor Advertisement (NA), Router Solicitation (RS), Router Advertisement (RA), and Redirect packets. The five types of packets are called ND packets collectively.

ND Snooping listens to ND packets in a network, filters out invalid ND packets, and monitors IPv6 users and binds these users to ports to avoid theft of IPv6 addresses. ND Snooping requires ND packets to be sent to the CPU. If they are sent at a high rate, this initiates an attack on the CPU. Therefore, we must configure ND guard to limit the rates of ND packets.

8. Customized Guard

There are many types of network protocols, including routing protocols such as OSPF, BGP, and RIP. To exchange packets between devices running different protocols, the packets must be sent to the CPU and processed by the protocol. Each protocol running on a device gives attackers a chance to initiate attacks. If an attacker sends many protocol packets to a network device, this consumes many CPU resources of the device, even affecting device operation.

Network protocols are diverse and grow constantly. Different protocols are demanded in different user environments. Therefore, protocol-specific guard functions have some limitations. To avoid this type of attacks, configure the customized guard function for the device to allow users to flexibly define and configure guard types to meet guard requirements in different user environments.

1.1.2 Rate Limiting Threshold and Attack Identification for Hosts

By configuring a rate limiting threshold for attack packets of hosts, a device can identify different attack scenarios such as host attacks, ARP scanning, and IP scanning. Host attacks can be identified in the following ways:

- Identify hosts according to the source IP address, VLAN ID, and port.
- Identify hosts according to the source MAC address, VLAN ID, and port on the link layer.

Each host is configured with a rate limiting threshold and an attack or attack threshold. The rate limiting threshold must be smaller than the attack threshold.

- If a single host sends attack packets at a rate higher than the rate limiting threshold, packets out of the threshold are discarded.
- If a single host sends attack packets at a rate higher than the attack threshold, the host behavior is identified as an attack and recorded into the log. Meanwhile, a Trap message is sent.
- If the received ARP packets exceed the scanning threshold in the configured period, the source MAC address in the packets 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, an ARP scanning attack is suspected.
- If the received IP packets exceed the scanning threshold in the configured period and the source IP address in the packets is unchanged and the destination IP address is changing, an IP scanning attack is suspected.

Instruction

- When NFPP detects attacks of a specific packet type, NFPP can send an alarm message to users. To avoid frequent alarm messages, NFPP does not resend an alarm within 60 seconds running after the message is generated.
- To prevent frequent log printing from consuming CPU resources, NFPP writes attacks related log content into the buffer and prints the log content from the buffer at the specified rate. NFPP does not limit the rates of Trap messages.
- Only ARP guard and IP scanning guard support the scanning prevention function.

1.1.3 Rate Limiting and Attack Identification for Ports

Each port is configured with a rate limiting threshold and an attack threshold. The rate limiting threshold must be smaller than the attack threshold.

- If a single port sends packets at a rate higher than the rate limiting threshold, packets out of the threshold are discarded.
- If a single port sends packets at a rate higher than the attack threshold, the port behavior is recorded into the log. Meanwhile, a Trap message is sent.

1.1.4 Hardware Isolation

Hardware is isolated by the guard policy after an attack is detected. Isolation requires a filter of hardware. Attack packets from an isolated device are not sent to the CPU for processing to ensure normal operation of the device.

Hardware isolation falls into host based isolation and port-based isolation. The port-based isolation configures a rate limit for physical ports. Only ARP guard and ND guard support hardware isolation based on physical ports.

To isolate attackers, you must configure policies for hardware entries. Because hardware resources are limited, a log is printed to remind users when such resources are exhausted.

Instruction

Only ARP guard can be configured with the global isolation and forwarding function and the rate limit function for port-based isolation and forwarding.

1.1.5 Monitoring Time

Monitoring hosts can detect attacks in the system. If the isolation time is 0 (indicating no isolation), the guard module automatically monitors attackers through software based on the configured monitoring time. If the isolation time is not 0, the guard module isolates attackers through hardware.

During software monitoring, when the isolation time is configured as a non-zero value, the guard module automatically isolates the attackers under software monitoring through hardware and configures the timeout time of the software monitoring as the isolation time. The monitoring time takes effect only when the isolation time is 0.

1.1.6 Trust Host

To stop monitoring a host is to trust the host. You can configure the host as a trusted host to allow it to send packets to the CPU.

1.2 Configuration Task Summary

NFPP configuration includes the following tasks:

(1)Configuring ARP Guard

(2)Configuring IP Guard

(3)Configuring TCP-SYN Guard

(4)Configuring ICMP Guard

(5)Configuring DHCP Guard

(6)Configuring DHCPv6 Guard

(7)Configuring ND Guard

(8)Customizing Guard

(9)Disabling Guard

(10)Configuring NFPP Logs

1.3 Configuring ARP Guard

1.3.1 Overview

ARP guard is used to detect, process, and prevent ARP based packet attacks. It includes the following functions:

- Identify ARP attacks based on hosts or physical ports. This function can determine an attack host based on the source IP address/MAC address (link layer), VLAN ID, and physical port. A rate limiting threshold and an attack threshold can be configured for each attack identification method. When the ARP packets are sent at a rate higher than the rate limiting threshold, the packets out of the threshold are discarded. When the ARP packets are sent at a rate higher than the attack threshold, an alarm is printed and a Trap message is sent to remind users of ARP attacks.
- Identify ARP scanning attacks. For the ARP packets received within 10 seconds, if the source MAC address is unchanged and the source IP address is changing on the link layer, or the former and source IP address on the link layer are unchanged but the destination IP address is changing more than the specified scanning threshold of times, an ARP scanning attack is suspected and an alarm is printed to remind users.
- Isolate the source of ARP attacks based on hosts or ports.
  - This function configures hardware entries to isolate the identified attack hosts. Thus, attack packets are not sent to the CPU or forwarded.
  - After isolation takes effect, you can enable the isolation forwarding function to limit the isolation range so that only the management plane of the target CPU is isolated and packets on the data plane are still forwarded.
  - If the port-based isolation entries take effect, the default action is to discard all attack packets. After you enable the function of port-based rate limit forwarding, you can allow some of packets to pass through by changing the isolation action.
- Monitor host attacks through software. After this function guard identifies any attacks, it can monitor the attack host through software in the configured monitoring time.

1.3.2 Restrictions and Guidelines

- ARP guard is to solve the ARP DoS attacks on a device. This function can reduce the impact of this type of attacks on the device, but does not cope with ARP spoofing attacks or ARP attacks in a network.
- If this function is configured in global configuration mode and interface configuration mode, the interface configuration prevails. For example, if the ARP guard function is enabled on an interface and then disabled in global configuration mode, the function remains effective on this interface.
- After the ARP guard function is disabled, the system automatically clears the entries related to the monitored hosts, scanning hosts, and isolated ports.
- The rate limiting threshold configured based on a MAC address has a higher priority than that configured based on an IP address, and the rate limiting threshold configured based on an IP address has a higher priority than that configured based on a port. To optimize the ARP guard effect, users are advised to configure rate limiting thresholds and attack thresholds for hosts based on the following rules:
  Attack threshold based on source MAC address > Rate limiting threshold based on source MAC address > Attack threshold based on IP address > Rate limiting threshold based on IP address
- The configured attack threshold must be greater than the rate limiting threshold. Otherwise, the

configuration fails.

- An ARP scanning table can store only 256 latest records. When the ARP scanning table is full, new records overwrite old ones. ARP scanning attacks may be misjudged. Therefore, when ARP guard does not isolate a detected host that is suspected to initiate an ARP scanning attack, this function only provides some information for the reference of users.
- When host attack packets are sent at a rate higher than the rate limiting threshold of CPP, you can configure isolation time to discard the packets and prevent them from occupying bandwidth. When you configure isolation time, you must note that:
  - If you change the isolation time to a non-zero value from 0, attack hosts under software monitoring are automatically isolated by hardware, and the configured monitoring time becomes invalid.
  - If you change the isolation time to 0 from a non-zero value, entries of the isolated attacker are directly deleted without monitoring the attacker through software.
- After you enable the isolation function, the recorded attack host occupies the security module entry.
- When you configure the maximum number of monitored hosts, you must note that:
  - As monitored hosts increase, processing them occupies more CPU resources.
  - If the configured maximum number of hosts is smaller than that of the actually monitored hosts, the existing monitored hosts are not automatically deleted. An alarm is printed to remind users of configuration failure. In this case, users must manually clear some monitored hosts.
  - When the monitored hosts reach the threshold, a log is printed to remind users. In this case, you must manually clear some monitored hosts.

1.3.3 Procedure (Global Configuration)

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the NFPP configuration mode.

nfpp

(4)Enable the function of global ARP guard.

arp-guard enable

The function of global ARP guard is enabled by default.

(5)(Optional) Configure the global isolation time of ARP guard.

arp-guard isolate-period [*interval* | **permanent**]

The default global isolation time of ARP guard is **0**, and the isolation function is disabled by default.

(6)(Optional) Enable the function of global isolation forwarding of ARP guard.

arp-guard isolate-forwarding enable

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

(7)(Optional) Enable the function of port-based rate limit forwarding of ARP guard.

arp-guard ratelimit-forwarding enable

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

(8)Configure the monitoring time of ARP guard.

arp-guard monitor-period *interval*

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

(9)Configure the maximum number of monitored hosts of ARP guard in global configuration mode.

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

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

(10)Configure a global rate limiting threshold of ARP guard.

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

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

(11)Configure a global attack threshold of ARP guard.

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

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

(12)Configure a global scanning threshold of ARP guard.

arp-guard scan-threshold *scan-threshold*

By default, the global scanning threshold of ARP guard is 100 packets every 10 seconds.

Procedure (Interface Configuration)

(13)Enter the privileged EXEC mode.

enable

(14)Enter the global configuration mode.

configure terminal

(15)Enter the interface configuration mode.

- Enter the configuration mode of the L2 Ethernet interface.

  interface *ethernet-type interface-number*

- Enter the configuration mode of the L3 Ethernet interface.

  interface *ethernet-type interface-number*

(16)Enable the ARP guard function on an interface.

nfpp arp-guard enable

The ARP guard function is disabled on an interface by default.

(17)Configure the isolation time of ARP guard on an interface.

nfpp arp-guard isolate-period [*interval* | **permanent**]

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

(18)Configure a rate limiting threshold and an attack threshold of ARP guard on an interface.

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 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.

(19)Configure a local scanning threshold of ARP guard on an interface.

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

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

1.4 Configuring IP Guard

1.4.1 Overview

After the IP guard function is enabled, a device can detect several common types of IP attacks timely, and ensure its stable operation by rate limit and host isolation. IP guard includes the following functions:

- Identify IP attacks based on hosts or physical ports. This function can determine an attack host based on the source IP address, VLAN ID, and physical port. A rate limiting threshold and an attack threshold can be configured for each attack identification method. When the IP packets are sent at a rate higher than the rate limiting threshold, the packets out of the threshold are discarded. When the IP packets are sent at a rate higher than the attack threshold, an alarm is printed and a Trap message is sent to remind users of IP attacks.
- Identify IP scanning attacks. For the IP packets received within 10 seconds, if the source IP address is unchanged and the destination IP address (not the local address) is changing more than the specified scanning threshold of times, an IP scanning attack is suspected and an alarm is printed to remind users.
- Isolate IP attackers based on hosts. This function configures hardware entries to isolate identified attack hosts. Thus, attack packets are not sent to the CPU or forwarded.
- Monitor attack hosts through software.
    - After this function identifies any attacks, it can monitor the attack host through software in the configured monitoring time.
    - This function can configure a specified host as a trusted host based on its IP address so that the host is free from software monitoring and allowed to send packets to the CPU.

1.4.2 Restrictions and Guidelines

- 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).
- If this function is configured in global configuration mode and interface configuration mode, the interface configuration prevails. For example, if the IP guard function is enabled on an interface and then disabled in global configuration mode, the function is still enabled on this interface.
- After the IP guard function is disabled, the system automatically clears the entries related to the monitored hosts.

- The rate limiting threshold configured based on a source IP address has a higher priority than that configured based on a port.
- The configured attack threshold must be greater than the rate limiting threshold. Otherwise, the configuration fails.
- When host attack packets are sent at a rate higher than the rate limiting threshold of CPP, you can configure isolation time to discard the packets and prevent them from occupying bandwidth. When you configure isolation time, you must note that:
  - If you change the isolation time to a non-zero value from 0, attack hosts under software monitoring are automatically isolated by hardware, and the configured monitoring time becomes invalid.
  - If you change the isolation time to 0 from a non-zero value, entries related to the isolated attacker are directly deleted without monitoring the attacker through software.
- After you enable the isolation function, the recorded attack host occupies the security module entry.
- When you configure the maximum number of monitored hosts, you must note that:
  - As monitored hosts increase, processing them occupies more CPU resources.
  - If the configured maximum number of hosts is smaller than that of the actually monitored hosts, the existing monitored hosts are not automatically deleted. An alarm is printed to remind users of configuration failure. In this case, users must manually clear some monitored hosts.
  - When the monitored hosts reach the threshold, a log is printed to remind users. In this case, you must manually clear some monitored hosts.
- IP guard can be configured with trusted hosts. When entries in the table of monitored hosts match the trusted hosts (their IP addresses are the same), the system automatically deletes the entries of the IP addresses. IP guard can be configured with a maximum of 500 trusted hosts.

1.4.3 Procedure (Global Configuration)

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the NFPP configuration mode.

nfpp

(4)Enable the global IP guard function.

ip-guard enable

The global IP guard function is enabled by default.

(5)(Optional) Configure the global isolation time of IP guard.

ip-guard isolate-period [*interval* | **permanent**]

The default global isolation time of IP guard is **0**, and the isolation function is disabled by default.

If the isolation function is enabled, attack host information occupies a hardware entry of the security module.

(6)Configure the monitoring time of IP guard.

ip-guard monitor-period *interval*

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

(7)Configure the maximum number of monitored hosts of IP guard.

ip-guard monitored-host-limit *number*

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

(8)(Optional) Configure a global rate limiting threshold of IP guard.

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

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

(9)Configure a global attack threshold of IP guard.

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

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

(10)Configure a global scanning threshold of IP guard.

ip-guard scan-threshold *scan-threshold*

By default, the global scanning threshold of IP guard is 100 packets every 10 seconds.

(Optional) Configure the trusted hosts of IP guard.

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

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

1.4.4 Procedure (Interface Configuration)

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the interface configuration mode.

- Enter the configuration mode of the L2 Ethernet interface.

  interface *ethernet-type interface-number*

- Enter the configuration mode of the L3 Ethernet interface.

  interface *ethernet-type interface-number*

(4)Enable the IP guard function on an interface.

nfpp ip-guard enable

The IP guard function is disabled on an interface by default.

(5)Configure the local isolation time of IP guard on an interface.

nfpp ip-guard isolate-period [*interval* | **permanent**]

No isolation time of IP guard is configured by default.

(6)Configure a local rate limiting threshold and a local attack threshold of IP guard on an interface.

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

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.

(7)Configure a scanning threshold of IP guard on an interface.

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

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

1.5 Configuring TCP-SYN Guard

1.5.1 Overview

An attacker can launch an attack against the device connected through TCP connections. To detect and prevent the TCP-SYN flooding attacks, you can enable the TCP-SYN guard function on the devices. TCP-SYN guard includes the following functions:

- Identify TCP-SYN attacks based on hosts or physical ports. This function can determine an attack host based on the source IP address, VLAN ID, and physical port. A rate limiting threshold and an attack threshold can be configured for each attack identification method. When the TCP-SYN packets are sent at a rate higher than the rate limiting threshold, the packets out of the threshold are discarded. When the TCP-SYN packets are sent at a rate higher than the attack threshold, an alarm is printed and a Trap message is sent.
- Isolate TCP-SYN attackers based on hosts. This function configures hardware entries to isolate identified attack hosts. Thus, attack packets are not sent to the CPU or forwarded.
- Monitor attack hosts through software.
    - After this function identifies any attacks, it can monitor the attack host through software in the configured monitoring time.
    - This function can configure a specified host as a trusted host of TCP-SYN guard based on its IP address so that it is free from software monitoring and allowed to send packets to the CPU.

1.5.2 Restrictions and Guidelines

- If this function is configured in global configuration mode and interface configuration mode, the interface configuration prevails.
- The rate limiting threshold configured based on a source IP address has a higher priority than that configured based on a port.
- The configured attack threshold must be greater than the rate limiting threshold. Otherwise, the configuration fails.
- When host attack packets are sent at a rate higher than the rate limiting threshold of CPP, you can configure isolation time to discard the packets and prevent them from occupying bandwidth. When you configure isolation time, you must note that:
    - If you change the isolation time to a non-zero value from 0, attack hosts under software monitoring are automatically isolated by hardware, and the configured monitoring time becomes invalid.
    - If you change the isolation time to 0 from a non-zero value, entries related to the isolated attacker are directly deleted without monitoring the attacker through software.

- After you enable the isolation function, the recorded attack host occupies the security module entry.
- When you configure the maximum number of monitored hosts, you must note that:
  - As monitored hosts increase, processing them occupies more CPU resources.
  - If the configured maximum number of hosts is smaller than that of the actually monitored hosts, the existing monitored hosts are not automatically deleted. An alarm is printed to remind users of configuration failure. In this case, users must manually clear some monitored hosts.
  - When the monitored hosts reach the threshold, a log is printed to remind users. In this case, you must manually clear some monitored hosts.
- TCP-SYN guard can be configured with trusted hosts. When entries in the table of monitored hosts match the trusted hosts (their IP addresses are the same), the system automatically deletes the entries of the IP addresses. TCP-SYN guard can be configured with a maximum of 500 trusted hosts.

1.5.3 Procedure (Global Configuration)

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the NFPP configuration mode.

nfpp

(4)Enable the global TCP-SYN guard function.

tcp-syn-guard enable

The TCP-SYN guard function is disabled on the interface and enabled globally by default.

(5)(Optional) Configure the global isolation time of TCP-SYN guard.

tcp-syn-guard isolate-period [*interval* | **permanent**]

The default global isolation time of TCP-SYN guard is **0**, and the isolation function is disabled by default.

(6)Configure the monitoring time of TCP-SYN guard.

tcp-syn-guard monitor-period *interval*

The default monitoring time of TCP-SYN guard is **600** seconds.

(7)Configure the maximum number of monitored hosts of TCP-SYN guard.

tcp-syn-guard monitored-host-limit *number*

The maximum number of monitored hosts of TCP-SYN guard is **20000** by default.

(8)Configure a global rate limiting threshold of TCP-SYN guard.

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

By default, the global rate limiting threshold of TCP-SYN guard for each interface is 50 packets per second, and for each source IP address is 20 packets per second.

(9)Configure a global attack threshold of TCP-SYN guard.

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

By default, the global attack threshold of TCP-SYN guard for each interface is 200 packets per second, and for each source IP address is 100 packets per second.

(Optional) Configure the trusted hosts of TCP-SYN guard.

tcp-syn-guard trusted-host *ipv4-address mask*

No host is configured as a trusted host of TCP-SYN guard by default.

1.5.4 Procedure (Interface Configuration)

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the interface configuration mode.

- Enter the configuration mode of the L2 Ethernet interface.

  interface *ethernet-type interface-number*

- Enter the configuration mode of the L3 Ethernet interface.

  interface *ethernet-type interface-number*

(4)Enable the TCP-SYN guard function on an interface.

nfpp tcp-syn-guard enable

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

(5)Configure the isolation time of TCP-SYN guard on an interface.

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

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

(6)Configure the local rate limiting threshold and local attack threshold of TCP-SYN guard on an interface.

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

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 global attack threshold of TCP-SYN guard are used.

1.6 Configuring ICMP Guard

1.6.1 Overview

The ICMP guard function configured for a device is used to prevent an attacker from consuming system resources by sending many ICMP requests. ICMP guard includes the following functions:

- Identify ICMP attacks based on hosts or physical ports. This function can determine an attack host based on the source IP address, VLAN ID, and port. A rate limiting threshold and an attack threshold can be configured for each attack identification method. When the ICMP packets are sent at a rate higher than the rate limiting threshold, the packets out of the threshold are discarded. When the ICMP packets are sent at a rate higher than the attack threshold, an alarm is printed and a Trap message is sent.

- Isolate ICMP attackers based on hosts. This function configures hardware entries to isolate identified attack hosts. Thus, attack packets are not sent to the CPU or forwarded.
- Monitor attack hosts through software.
    - After this function identifies any attacks, it can monitor the attack host through software in the configured monitoring time.
    - This function can configure a specified host as a trusted host of ICMP guard based on its IP address so that it is free from software monitoring and allowed to send packets to the CPU.

1.6.2 Restrictions and Guidelines

- If this function is configured in global configuration mode and interface configuration mode, the interface configuration prevails.
- After the ICMP guard function is disabled, the system automatically clears the entries related to the monitored hosts.
- The rate limiting threshold configured based on a source IP address has a higher priority than that configured based on a port.
- The configured attack threshold must be greater than the rate limiting threshold. Otherwise, the configuration fails.
- When host attack packets are sent at a rate higher than the rate limiting threshold of CPP, you can configure isolation time to discard the packets and prevent them from occupying bandwidth. When you configure isolation time, you must note that:
    - If you change the isolation time to a non-zero value from 0, attack hosts under software monitoring are automatically isolated by hardware, and the configured monitoring time becomes invalid.
    - If you change the isolation time to 0 from a non-zero value, entries related to the isolated attacker are directly deleted without monitoring the attacker through software.
- After you enable the isolation function, the recorded attack host occupies the security module entry.
- When you configure the maximum number of monitored hosts, you must note that:
    - As monitored hosts increase, processing them occupies more CPU resources.
    - If the configured maximum number of hosts is smaller than that of the actually monitored hosts, the existing monitored hosts are not automatically deleted. An alarm is printed to remind users of configuration failure. In this case, users must manually clear some monitored hosts.
    - When the monitored hosts reach the threshold, a log is printed to remind users. In this case, you must manually clear some monitored hosts.
- ICMP guard can be configured with trusted hosts. When entries in the table of monitored hosts match the trusted hosts (their IP addresses are the same), the system automatically deletes the entries of the IP addresses. ICMP guard can be configured with a maximum of 500 trusted hosts.

1.6.3 Procedure (Global Configuration)

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the NFPP configuration mode.

nfpp

(4)Enable the function of global ICMP guard.

icmp-guard enable

The function of global ICMP guard is enabled by default.

(5)(Optional) Configure the global isolation time of ICMP guard.

icmp-guard isolate-period [*interval* | **permanent**]

The default global isolation time of ICMP guard is **0**, and the isolation function is disabled by default.

(6)Configure the monitoring time of ICMP guard.

icmp-guard monitor-period *interval*

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

(7)Configure the maximum number of monitored hosts.

icmp-guard monitored-host-limit *number*

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

(8)Configure the global rate limiting threshold of ICMP guard.

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

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

(9)Configure the global attack threshold of ICMP guard.

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

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

(10)(Optional) Configure the trusted hosts of ICMP guard.

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

No host is configured as a trusted host by default.

1.6.4 Procedure (Interface Configuration)

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the interface configuration mode.

- Enter the configuration mode of the L2 Ethernet interface.

  interface *ethernet-type interface-number*

- Enter the configuration mode of the L3 Ethernet interface.

  interface *ethernet-type interface-number*

(4)Enable the ICMP guard function on an interface.

nfpp icmp-guard enable

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

(5)Configure the local isolation time of ICMP guard on an interface.

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

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

(6)Configure the local rate limiting threshold and local attack threshold of ICMP guard on an interface.

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

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.

1.7 Configuring DHCP Guard

1.7.1 Overview

In a DHCP starvation attack, all IP addresses of a DHCP server are exhausted. As a result, the DHCP server fails to provide the address assignment service, thus affecting the network access of legal users. To address this type of attacks, you must deploy the DHCP guard function on a device.

DHCP guard includes the following functions:

- Identify DHCP attacks based on hosts or physical ports. This function can determine an attack host based on the source MAC address, VLAN ID, and port on the link layer. A rate limiting threshold and an attack threshold can be configured for each attack identification method. When the DHCP packets are sent at a rate higher than the rate limiting threshold, the packets out of the threshold are discarded. When the DHCP packets are sent at a rate higher than the attack threshold, an alarm is printed and a Trap message is sent.
- Isolate DHCP attackers based on hosts. This function configures hardware entries to isolate identified attack hosts. Thus, attack packets are not sent to the CPU or forwarded.
- Monitor attack hosts through software. After an attack is identified, this function monitors the attack host through software in the configured monitoring time.

1.7.2 Restrictions and Guidelines

- If this function is configured in global configuration mode and interface configuration mode, the interface configuration prevails.
- After the DHCP guard function is disabled, the system automatically clears the entries related to the monitored hosts.
- The configured attack threshold must be greater than the rate limiting threshold. Otherwise, the configuration fails.
- When host attack packets are sent at a rate higher than the rate limiting threshold of CPP, you can configure isolation time to discard the packets and prevent them from occupying bandwidth. When you configure isolation time, you must note that:
  - If you change the isolation time to a non-zero value from 0, attack hosts under software monitoring are automatically isolated by hardware, and the configured monitoring time becomes invalid.
  - If you change the isolation time to 0 from a non-zero value, entries related to the isolated attacker are

directly deleted without monitoring the attacker through software.

- After you enable the isolation function, the recorded attack host occupies the security module entry.
- When you configure the maximum number of monitored hosts, you must note that:
  - As monitored hosts increase, processing them occupies more CPU resources.
  - If the configured maximum number of hosts is smaller than that of the actually monitored hosts, the existing monitored hosts are not automatically deleted. An alarm is printed to remind users of configuration failure. In this case, users must manually clear some monitored hosts.
  - When the monitored hosts reach the threshold, a log is printed to remind users. In this case, you must manually clear some monitored hosts.
- If a port is configured as trusted by the DHCP Snooping function, the DHCP guard function becomes invalid to avoid misjudging DHCP traffic on the trusted port. For trusted port configuration in DHCP Snooping, see "Configuring DHCP Snooping".

1.7.3 Procedure (Global Configuration)

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the NFPP configuration mode.

nfpp

(4)Enable the function of global DHCP guard.

dhcp-guard enable

The function of global DHCP guard is enabled by default.

(5)(Optional) Configure the global isolation time of DHCP guard.

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

The default global isolation time of DHCP guard is **0**, and the isolation function is disabled by default.

(6)Configure the monitoring time of DHCP guard.

dhcp-guard monitor-period *interval*

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

(7)Configure the maximum number of monitored hosts.

dhcp-guard monitored-host-limit *number*

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

(8)Configure the global rate limiting threshold of DHCP guard.

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

By default, the global rate limiting threshold of DHCP guard for each interface is 150 packets per second, and for each source IP address is 5 packets per second.

(9)Configure the global attack threshold of DHCP guard.

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

By default, the global attack threshold of DHCP guard for each interface is 256 packets per second, and for each source IP address is 10 packets per second.

Procedure (Interface Configuration)

(10)Enter the privileged EXEC mode.

enable

(11)Enter the global configuration mode.

configure terminal

(12)Enter the interface configuration mode.

- Enter the configuration mode of the L2 Ethernet interface.

  interface *ethernet-type interface-number*

- Enter the configuration mode of the L3 Ethernet interface.

  interface *ethernet-type interface-number*

(13)Enable the DHCP guard function on an interface.

nfpp dhcp-guard enable

The DHCP guard function is disabled on an interface by default. The global DHCP guard function is enabled.

(14)Configure isolation time of DHCP guard on an interface.

nfpp dhcp-guard isolate-**period** [*interval* | **permanent**]

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

(15)Configure the local rate limiting threshold and local attack threshold of DHCP guard on an interface.

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

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.

1.8 Configuring DHCPv6 Guard

1.8.1 Overview

Like DHCPv4, DHCPv6 has security problems. Therefore, the attack methods of DHCPv4 are applicable to DHCPv6. To prevent this type of attacks, we must also deploy the DHCPv6 guard policy. DHCPv6 guard includes the following functions:

- Identify DHCPv6 attacks based on hosts or physical ports. This function can determine an attack host based on the source MAC address, VLAN ID, and port on the link layer. A rate limiting threshold and an attack threshold can be configured for each attack identification method.
- Isolate DHCPv6 attackers based on hosts. This function configures hardware entries to isolate identified attack hosts. Thus, attack packets are not sent to the CPU or forwarded.
- Monitor attack hosts through software. After an attack is identified, this function monitors the attack host through software in the configured monitoring time.

1.8.2 Restrictions and Guidelines

- If this function is configured in global configuration mode and interface configuration mode, the interface configuration prevails.
- After the DHCPv6 guard function is disabled, the system automatically clears the entries related to the monitored hosts.
- The configured attack threshold must be greater than the rate limiting threshold. Otherwise, the configuration fails.
- When host attack packets are sent at a rate higher than the rate limiting threshold of CPP, you can configure isolation time to discard the packets and prevent them from occupying bandwidth. When you configure isolation time, you must note that:
  - If you change the isolation time to a non-zero value from 0, attack hosts under software monitoring are automatically isolated by hardware, and the configured monitoring time becomes invalid.
  - If you change the isolation time to 0 from a non-zero value, entries related to the isolated attacker are directly deleted without monitoring the attacker through software.
- After you enable the isolation function, the recorded attack host occupies the security module entry.
- When you configure the maximum number of monitored hosts, you must note that:
  - As monitored hosts increase, processing them occupies more CPU resources.
  - If the configured maximum number of hosts is smaller than that of the actually monitored hosts, the existing monitored hosts are not automatically deleted. An alarm is printed to remind users of configuration failure. In this case, users must manually clear some monitored hosts.
  - When the monitored hosts reach the threshold, a log is printed to remind users. In this case, you must manually clear some monitored hosts.
- If a port is configured as trusted by the DHCPv6 Snooping function, the DHCPv6 guard function becomes invalid to avoid misjudging DHCPv6 traffic on the trusted port. For trusted port configuration in DHCPv6 Snooping, see "Configuring DHCPv6 Snooping".

1.8.3 Procedure (Global Configuration)

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the NFPP configuration mode.

nfpp

(4)Enable the function of global DHCPv6 guard.

dhcpv6-guard enable

The function of global DHCPv6 guard is enabled by default.

(5)Configure the monitoring time of DHCPv6 guard.

dhcpv6-guard monitor-period *interval*

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

(6)Configure the maximum number of monitored hosts.

dhcpv6-guard monitored-host-limit *number*

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

(7)Configure the global rate limiting threshold of DHCPv6 guard.

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

By default, the global rate limiting threshold of DHCPv6 guard for each interface is 150 packets per second, and for each source IP address is 5 packets per second.

(8)Configure the global attack threshold of DHCPv6 guard.

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

By default, the global attack threshold of DHCPv6 guard for each interface is 256 packets per second, and for each source IP address is 10 packets per second.

Procedure (Interface Configuration)

(9)Enter the privileged EXEC mode.

enable

(10)Enter the global configuration mode.

configure terminal

(11)Enter the interface configuration mode.

- Enter the configuration mode of the L2 Ethernet interface.

  interface *ethernet-type interface-number*

- Enter the configuration mode of the L3 Ethernet interface.

  interface *ethernet-type interface-number*

(12)Enable the DHCPv6 guard function on an interface.

nfpp dhcpv6-guard enable

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

(13)Configure the local rate limiting threshold and local attack threshold of DHCPv6 guard on an interface.

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

No local rate limiting threshold is 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.

1.9 Configuring ND Guard

1.9.1 Overview

ND packets of ND guard fall into three types by use:

- Type 1: Neighbor requests and neighbor advertisements, which are used to parse addresses.
- Type 2: Route requests, which are used to discover gateways for hosts.
- Type 3: Route advertisements, which are used to advertise gateways and prefixes; and redirection packets, which are used to advertise better next hops.

ND guard identifies ND packets based on physical ports. This function prevents attacks by configuring rate limiting thresholds for attack ports and isolating the ports.

1.9.2 Restrictions and Guidelines

- If this function is configured in global configuration mode and interface configuration mode, the interface configuration prevails.
- The configured attack threshold must be greater than the rate limiting threshold. Otherwise, the configuration fails.
- After you enable the ND Snooping function by running the **ipv6 nd snooping enable** command, all ND packets are NDSNP packets. In this case, you must configure rate limiting thresholds and attack thresholds for the NDSNP packets to validate the guard.
- After you enable the isolation function, the recorded attack host occupies the security module entry. If the port-based isolation entries take effect, the default action is to discard all attack packets. After you enable the function of port-based rate limit forwarding, you can allow some of packets to pass through by changing the isolation action.
- Rate limit by hardware is ineffective to NDSNP packets.

1.9.3 Procedure (Global Configuration)

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the NFPP configuration mode.

nfpp

(4)Enable the global ND guard function.

nd-guard enable

The function of global ND guard is enabled by default.

(5)Enable the function of port-based rate limit forwarding of ND guard.

nd-guard ratelimit-forwarding enable

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

(6)Configure the global rate limiting threshold of ND guard.

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

By default, the global rate limiting threshold of ND guard for NDSNP packet is 100 packets per second, for neighbor request and neighbor advertisement is 50 packets per second, for route advertisement and redirection is 25 packets per second, and for route request is 25 packets per second.

(7)Configure the global attack threshold of ND guard.

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

By default, the global attack threshold of ND guard for NDSNP packet is 200 packets per second, for neighbor request and neighbor advertisement is 100 packets per second, for route advertisement and redirection is 50 packets per second, and for route request is 50 packets per second.

Procedure (Interface Configuration)

(8)Enter the privileged EXEC mode.

enable

(9)Enter the global configuration mode.

configure terminal

(10)Enter the interface configuration mode.

- Enter the configuration mode of the L2 Ethernet interface.

  interface *ethernet-type interface-number*

- Enter the configuration mode of the L3 Ethernet interface.

  interface *ethernet-type interface-number*

(11)Enable the ND guard function on an interface.

nfpp nd-guard enable

The ND guard function is disabled on an interface by default. The global ND guard function is enabled.

(12)Configure the local rate limiting threshold and local attack threshold of ND guard on an interface.

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 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.

1.10 Customizing Guard

1.10.1 Overview

Users can customize guard types and guard policies to solve network attacks in special application scenarios.

Customized guard includes the following functions:

- Allow users to combine packet type fields and use them as packet types of customized guard to meet requirements of guard scenarios.
- Configure guard policies based on hosts and ports. Host guard policies include those based on the source IP address, VLAN ID and port, or those based on the source MAC address, VLAN ID and port on the link layer. A rate limiting threshold and an attack threshold can be configured for each guard policy. When the packets are sent at a rate higher than the rate limiting threshold, the packets out of the threshold are discarded. When the packets are sent at a rate higher than the attack threshold, an alarm is printed and a Trap message is sent.
- Monitor attack hosts through software.
  - After this function identifies any attacks, it can monitor the attack host through software in the configured monitoring time.
  - This function can configure a specified host as a trusted host based on its IPv4, IPv6, or MAC address so that it is free from software monitoring and allowed to send packets to the CPU without rate limit and

processing.

1.10.2 Restrictions and Guidelines

- Customized guard allows users to combine packet type fields to include most existing protocol types and expand new protocol types. Improper configuration of the packet type fields may cause a network exception. Therefore, users must well understand network protocols before they configure this function.
- Customized guard has a higher packet detection priority than basic guard types. When packets match the customized guard policy and the policy of a basic guard type, they preferentially undergo rate limit and attack identification according to the customized guard policy. To ensure the configuration effect of basic guard types, try to refer to the configuration guide when you configure the packet type fields of customized guard.
- Customized guard policies must be configured with different type names and packet types. Matched packet types must differ from the packet types of existing guard types, including those of basic guard types such as ARP guard, IP guard, ICMP guard, TCP-SYN guard, DHCP guard, DHCPv6 guard, and ND guard.
- You can configure packet types of customized guard by combining the following fields. These fields include Ethernet link layer type (etype), source MAC address (src-mac), destination MAC address (dst-mac), IPv4 or IPv6 protocol number (protocol), source IPv4 or IPv6 address (src-ip/src-ipv6), destination IPv4 or IPv6 address (dst-ip/dst-ipv6), source port on the transport layer (src-port), and destination port on the transport layer (dst-port).

  To configure the matched fields of packet fields, conform with the following limit rules. Otherwise, the configuration fails:

  - The IPv4 or IPv6 protocol number (protocol) is configurable only when the Ethernet link layer type (etype) is IPv4 or IPv6.
  - The source IPv4 address (src-ip) and destination IPv4 address (dst-ip) are configurable only when the Ethernet link layer type (etype) is IPv4.
  - The source IPv6 address (src-ipv6) and destination IPv6 address (dst-ipv6) are configurable only when the Ethernet link layer type (etype) is IPv6.
  - The source port on the transport layer (src-port) and destination port on the transport layer (dst-port) are configurable only when the IPv4 or IPv6 protocol number (protocol) is TCP or UDP.
- For the three types of customized guard policies that are based on the source IP address, source MAC address, and port, you must configure at least one type. That is, you must configure the global rate limiting threshold and global attack threshold of customized guard. Otherwise, the customized guard function does not take effect. You can configure a host policy based on the source IP address, VLAN ID, and port only when the specified Ethernet link layer type (etype) is IPv4 or IPv6.
- The rate limiting threshold based on a source MAC address has a higher priority than that based on a source IP address. The configured attack threshold must be greater than the rate limiting threshold. Otherwise, the configuration fails.
- Only after you configure packet types and guard policies can you enable the customized guard function. If you do not complete any configuration, you are reminded that the current customized guard is not completely configured and the configuration fails.
- The host policy of customized guard on an interface must be consistent with the global host policy configuration. For example, if no global rate limiting threshold and global attack threshold are configured

based on the source IP address, you cannot configure the local rate limiting threshold and local attack threshold on an interface.

- If this function is configured in global configuration mode and interface configuration mode, the interface configuration prevails.
- After the customized guard function is disabled, the system automatically clears the entries related to the monitored hosts.
- When you configure the maximum number of monitored hosts, you must note that:
  - As monitored hosts increase, processing them occupies more CPU resources.
  - If the configured maximum number of hosts is smaller than that of the actually monitored hosts, the existing monitored hosts are not automatically deleted. An alarm is printed to remind users of configuration failure. In this case, users must manually clear some monitored hosts.
  - When the monitored hosts reach the threshold, a log is printed to remind users. In this case, you must manually clear some monitored hosts.
- When you configure trusted hosts, note that:
  - You must configure matched packet types before you configure trusted hosts.
  - The trusted hosts of customized guard must be consistent with the matched packet types. For example, only when the Ethernet link layer type (etype) is IPv4, can you add IPv4 addresses as trusted IP addresses. Similarly, when the matched packet type is IPv4, IPv6 addresses cannot be added as trusted IP addresses.
  - You can configure all hosts in a network segment as trusted hosts by configuring masks.
  - When entries in the table of monitored hosts match the trusted hosts, the system automatically deletes the entries of the IP addresses.
  - ICMP guard can be configured with a maximum of 500 trusted hosts.

1.10.3 Procedure (Global Configuration)

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the NFPP configuration mode.

nfpp

(4)Customize a guard type, and enter the configuration mode of the NFPP customized guard type.

define *define-name*

(5)Configure the matched packet types of the customized guard type.

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-ipv4-address* [**src-ip-mask** *mask*] | **src-ipv6** *source-ipv6-address* [**src-ipv6-masklen** *prefix-length*] | **src-mac** *source-mac-address* | **src-port** *port-number* } *

(6)Configure the global rate limiting threshold and global attack threshold of the customized guard type.

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

No global rate limiting threshold or global attack threshold of the customized guard type is configured by default.

They must be configured. Otherwise, you cannot enable the customized guard function.

(7)Configure the monitoring time of the customized guard type.

monitor-period *interval*

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

(8)Configure the maximum number of monitored hosts of the customized guard type.

monitored-host-limit *number*

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

(9)Configure the trusted hosts of the customized guard type.

trusted-host { *ipv4-address mask* | *ipv6-address*/*prefix-length* | *mac-address mask* }

No host is configured as a trusted host of the customized guard type by default.

(10)Enable the function of global customized guard.

define *define-name* **enable**

The function of global customized guard is disabled by default.

1.10.4 Procedure (Interface Configuration)

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the interface configuration mode.

- Enter the configuration mode of the L2 Ethernet interface.

  interface *ethernet-type interface-number*

- Enter the configuration mode of the L3 Ethernet interface.

  interface *ethernet-type interface-number*

(4)Enable the customized guard function on an interface.

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

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

(5)Configure the local rate limiting threshold and local attack threshold of the customized guard type on an interface.

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 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.

1.11 Disabling Guard

1.11.1 Overview

Users can disable or enable all basic types of global guard function by running one command. Basic guard types supported by this function include ARP guard, IP guard, ICMP guard, TCP-SYN guard, DHCP guard, DHCPv6 guard, and ND guard.

1.11.2 Restrictions and Guidelines

- This function applies to only basic guard types and does not affect the customized guard types.
- This function applies to the guard functions in global configuration mode and does not affect the guard functions in interface configuration mode.
- After you run the one-click enabling/disabling command, the configuration of this command cannot be displayed by running the **show running-config** command.
- The one-click enabling/disabling command is to actually enable or disable basic guard types in global configuration mode. After you run this command to disable basic guard types, the **show running-config** command allows you to display the global disabling command of each basic guard function. After you run this command to enable basic guard types, the **show running-config** command allows you to display the default configuration.
- This command cannot be saved, but its running result can be saved and take effect after device restart.

1.11.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enable all the basic types of global guard of NFPP.

all-guard enable

1.12 Configuring NFPP Logs

1.12.1 Overview

When many attacks are launched to a device, the generated prompts may affect user experience. You can configure the size of a log buffer, system message rate, and filtering conditions to restrictively record and display logs.

- NFPP retrieves logs from a special buffer at a rate, uses them to generate system messages, and clears the logs from the buffer. Therefore, you can configure the rate of generating system messages from logs of the log buffer through NFPP to control the message report frequency and avoid log spamming.
- You can also configure filtering conditions to obtain required log information accurately and filter out logs that do not comply with the filtering rules.
- To monitor whether an attack occurs, you can print logs on a screen in real time.

1.12.2 Restrictions and Guidelines

- After active/standby switchover of a device, the device will clear logs in a buffer and record new logs again.
- Even if a device does not suffer an attack, logs are continuously retrieved from the buffer to generate system messages.
- When the log buffer overflows, new logs overwrite the stale logs, and the log buffer displays an entry with attributes being "-". In this case, you must increase the log buffer size or improve the generation rate of system messages.

1.12.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the NFPP configuration mode.

nfpp

(4)Configure the size of a log buffer.

log-buffer entries *number*

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

(5)Configure the rate of generating system messages from logs of the log buffer through NFPP.

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

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.

If the values of the *message-number* and *interval* parameters are **0**, logs are used by NFPP to immediately generate system messages without being written into the buffer.

(6)Configure NFPP to record the logs of a specified VLAN and a specified interface.

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

NFPP records the logs of all VLANs and interfaces by default.

(7)Enable the function of screen log output.

log-buffer enable

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

1.13 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

Notice

- Running the **clear** command may lose vital information and thus interrupt services.

Table 1-1Monitoring

Command	Purpose
clear nfpp arp-guard scan	Clears the scanning table of ARP guard.
clear nfpp arp-guard hosts	Clears the monitored hosts of ARP guard.
clear nfpp ip-guard hosts	Clears the monitored hosts of IP guard.
clear nfpp tcp-syn-guard hosts	Clears the monitored hosts of TCP-SYN guard.
clear nfpp nd-guard hosts	Clears the monitored hosts of ND guard.
clear nfpp icmp-guard hosts	Clears the monitored hosts of ICMP guard.
clear nfpp dhcp-guard hosts	Clears the monitored hosts of DHCP guard.
clear nfpp dhcpv6-guard hosts	Clears the monitored hosts of DHCPv6 guard.
clear nfpp define *define-name* **hosts**	Clears the monitored hosts of customized guard.
clear nfpp log	Clears logs.
show nfpp arp-guard summary	Displays the configuration parameters of ARP guard.
show nfpp arp-guard hosts	Displays the monitored hosts of ARP guard.
show nfpp arp-guard scan	Displays the scanning table of ARP guard.
show nfpp ip-guard summary	Displays the configuration parameters of IP guard.
show nfpp ip-guard hosts	Displays the monitored hosts of IP guard.
show nfpp ip-guard trusted-host	Displays the scanning table of IP guard.
show nfpp tcp-syn-guard summary	Displays the configuration parameters of TCP-SYN guard.
show nfpp tcp-syn-guard hosts	Displays the monitored hosts of TCP-SYN guard.
show nfpp tcp-syn-guard trusted-host	Displays the scanning table of TCP-SYN guard.
show nfpp icmp-guard summary	Displays the configuration parameters of ICMP guard.
show nfpp icmp-guard hosts	Displays the monitored hosts of ICMP guard.
show nfpp icmp-guard trusted-host	Displays the scanning table of ICMP guard.
show nfpp dhcp-guard summary	Displays the configuration parameters of DHCP guard.
show nfpp dhcp-guard hosts	Displays the monitored hosts of DHCP guard.
show nfpp dhcpv6-guard summary	Displays the configuration parameters of DHCPv6 guard.
show nfpp dhcpv6-guard hosts	Displays the monitored hosts of DHCPv6 guard.
show nfpp nd-guard summary	Displays the configuration parameters of ND guard.

Command	Purpose
show nfpp define summary [*name*]	Displays the configuration parameters of customized guard.
show nfpp define hosts *name*	Displays the monitored hosts.
show nfpp define trusted-host *name*	Displays the trusted hosts.
show nfpp log summary	Displays the configuration of NFPP logs.
show nfpp log buffer [**statistics**]	Displays the log buffer of NFPP.

1.14 Configuration Examples

1.14.1 Configuring CPU Guard

1. Requirements

In a network system, protocols such as ARP, IP, TCP-SYN, ICMP, DHCP, DHCPv6, and ND are popular targets of attacks. This may cause packet forwarding failure and high CPU usage. You can enable guard policies to ensure the stable running of devices.

2. Notes

- Configure the rate limiting threshold, attack threshold and isolation time of ARP guard.
- Configure the scanning threshold and isolation time of IP guard.
- Configure the scanning threshold and isolation time of TCP-SYN guard.
- Configure the scanning threshold and isolation time of ICMP guard.
- Configure the scanning threshold and isolation time of DHCP guard.
- Configure the scanning threshold and isolation time of DHCPv6 guard.
- Configure the scanning threshold and isolation time of ND guard.

3. Procedure

Configure ARP guard on Device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# nfpp
DeviceA(config-nfpp)# arp-guard rate-limit per-src-mac 5
DeviceA(config-nfpp)# arp-guard attack-threshold per-src-mac 10
DeviceA(config-nfpp)# arp-guard isolate-period 180
```

Configure IP guard on Device A.

```
DeviceA(config-nfpp)# ip-guard rate-limit per-src-ip 20
DeviceA(config-nfpp)# ip-guard attack-threshold per-src-ip 30
DeviceA(config-nfpp)# ip-guard isolate-period 180
DeviceA(config-nfpp)# ip-guard trusted-host 192.168.201.46 255.255.255.255
```

Configure TCP-SYN guard on Device A.

```
DeviceA(config-nfpp)# tcp-syn-guard rate-limit per-src-ip 20
DeviceA(config-nfpp)# tcp-syn-guard attack-threshold per-src-ip 30
DeviceA(config-nfpp)# tcp-syn-guard isolate-period 180
DeviceA(config-nfpp)# tcp-syn-guard trusted-host 192.168.201.46 255.255.255.255
```

Configure ICMP guard on Device A.

```
DeviceA(config-nfpp)# icmp-guard rate-limit per-src-ip 20
DeviceA(config-nfpp)# icmp-guard attack-threshold per-src-ip 30
DeviceA(config-nfpp)# icmp-guard isolate-period 180
```

Configure DHCP guard on Device A.

```
DeviceA(config-nfpp)# dhcp-guard rate-limit per-src-ip 20
DeviceA(config-nfpp)# dhcp-guard attack-threshold per-src-ip 30
DeviceA(config-nfpp)# dhcp-guard isolate-period 180
DeviceA(config-nfpp)# dhcp-guard trusted-host 192.168.201.46 255.255.255.255
```

Configure DHCPv6 guard on Device A.

```
DeviceA(config-nfpp)# dhcpv6-guard rate-limit per-src-ip 20
DeviceA(config-nfpp)# dhcpv6-guard attack-threshold per-src-ip 30
DeviceA(config-nfpp)# dhcpv6-guard trusted-host 192.168.201.46 255.255.255.255
```

Configure ND guard on Device A.

```
DeviceA (config-nfpp)# nd-guard rate-limit per-port ns-na 30
DeviceA (config-nfpp)# nd-guard attack-threshold per-port ns-na 50
```

4. Verification

Run the **show nfpp arp-guard summary** command to display the configuration.

```
DeviceA# 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    Disable 180            4/5/100         8/10/200         15

Maximum count of monitored hosts: 1000
Monitor period: 600s
```

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

```
DeviceA# show nfpp arp-guard hosts
If col_filter 1 shows '*', it means "hardware do not isolate host".
 VLAN    interface   IP address        MAC address      remain-time(s)
 ----    ---------   ----------        -----------      --------------
 1       Gi0/43      5.5.5.16          -                175
Total: 1 host
```

Run the **show nfpp arp-guard scan** command to display the scanned hosts.

```
DeviceA# show nfpp arp-guard scan
VLAN  interface       IP address        MAC address     timestamp
----  ---------       ----------        -----------     ---------
1     Gi0/5           -                 001a.a9c2.4609  2013-4-30 23:50:32
```

```
1     Gi0/5          192.168.206.2     001a.a9c2.4609  2013-4-30 23:50:33
1     Gi0/5          -                 001a.a9c2.4609  2013-4-30 23:51:33
1     Gi0/5          192.168.206.2     001a.a9c2.4609  2013-4-30 23:51:34
Total: 4 record(s)
```

Instruction

If attack traffic carries the VLAN ID 0, NFPP may consider the corresponding host as an attack host and configure a rate limiting threshold for the attack traffic. Run the **show nfpp arp-guard host** command to display the attack hosts. The VLAN ID field may be displayed as a port PVID or hidden.

Run the **show nfpp ip-guard summary** command to display the configuration.

```
DeviceA# 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    Disable 180            20/-/100        30/-/200         100

Maximum count of monitored hosts: 1000
Monitor period: 600s
```

Run the **show nfpp ip-guard hosts** command to display the monitored hosts.

```
DeviceA# show nfpp ip-guard hosts
If col_filter 1 shows '*', it means "hardware do not isolate host".
 VLAN    interface   IP address         Reason    remain-time(s)
 ----    ---------   ----------         ------    --------------
  1      Gi0/5       192.168.201.47     ATTACK    160
Total: 1 host
```

Run the **show nfpp ip-guard trusted-host** command to display the trusted hosts.

```
DeviceA# show nfpp ip-guard trusted-host
IP address          mask
----------          ----
192.168.201.46      255.255.255.255
Total: 1 record(s)
```

Instruction

If attack traffic carries the VLAN ID 0, NFPP may consider the corresponding host as an attack host and configure a rate limiting threshold for the attack traffic. Run the **show nfpp ip-guard host** command to display the attack hosts. The VLAN ID field may be displayed as a port PVID or hidden.

Run the **show nfpp tcp-syn-guard summary** command to display the configuration.

```
DeviceA# 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 Scan-threshold
Global    Disable 180            20/-/100        30/-/200         100
```

```

Maximum count of monitored hosts: 1000
Monitor period: 600s
```

Run the **show nfpp tcp-syn-guard hosts** command to display the monitored hosts.

Run the **show nfpp tcp-syn-guard trusted-host** command to display the trusted hosts.

```
DeviceA# show nfpp tcp-syn-guard trusted-host
IP address          mask
----------          ----
192.168.201.46      255.255.255.255
Total: 1 record(s)
```

Instruction

If attack traffic carries the VLAN ID 0, NFPP may consider the corresponding host as an attack host and configure a rate limiting threshold for the attack traffic. Run the **show nfpp tcp-syn-guard host** command to display the attack hosts. The VLAN ID field may be displayed as a port PVID or hidden.

Run the **show nfpp icmp-guard summary** command to display the configuration.

```
DeviceA# 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 Scan-threshold
Global    Disable 180            20/-/100        30/-/200         100

Maximum count of monitored hosts: 1000
Monitor period: 600s
```

Run the **show nfpp icmp-guard hosts** command to display the monitored hosts.

```
DeviceA# show nfpp icmp-guard hosts
If col_filter 1 shows '*', it means "hardware do not isolate host".
 VLAN    interface   IP address         Reason    remain-time(s)
 ----    ---------   ----------         ------    --------------
  1      Gi0/5       192.168.201.47     ATTACK    160
Total: 1 host
```

Run the **show nfpp icmp-guard trusted-host** command to display the trusted hosts.

```
DeviceA# show nfpp icmp-guard trusted-host
IP address          mask
----------          ----
192.168.201.46      255.255.255.255
Total: 1 record(s)
```

Instruction

If attack traffic carries the VLAN ID 0, NFPP may consider the corresponding host as an attack host and configure a rate limiting threshold for the attack traffic. Run the **show nfpp icmp-guard host** command to display the attack hosts. The VLAN ID field may be displayed as a port PVID or hidden.

Run the **show nfpp dhcp-guard summary** command to display the configuration.

```
DeviceA# 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 Scan-threshold
Global    Disable 180            20/-/100        30/-/200         100

Maximum count of monitored hosts: 1000
Monitor period: 600s
```

Run the **show nfpp dhcp-guard hosts** command to display the monitored hosts.

```
DeviceA# show nfpp dhcp-guard hosts
If col_filter 1 shows '*', it means "hardware do not isolate host".
 VLAN    interface   IP address        Reason    remain-time(s)
 ----    ---------   ----------        ------    --------------
  1      Gi0/5       192.168.201.47    ATTACK    160
Total: 1 host
```

Run the **show nfpp dhcp-guard trusted-host** command to display the trusted hosts.

```
DeviceA# show nfpp dhcp-guard trusted-host
IP address          mask
----------          ----
192.168.201.46      255.255.255.255
Total: 1 record(s)
```

Instruction

If attack traffic carries the VLAN ID 0, NFPP may consider the corresponding host as an attack host and configure a rate limiting threshold for the attack traffic. Run the **show nfpp dhcp-guard host** command to display the attack hosts. The VLAN ID field may be displayed as a port PVID or hidden.

Run the **show nfpp dhcpv6-guard summary** command to display the configuration.

```
DeviceA# show nfpp dhcpv6-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    Disable 180            20/-/100        30/-/200         100

Maximum count of monitored hosts: 1000
Monitor period: 600s
```

Run the **show nfpp dhcpv6-guard hosts** command to display the monitored hosts.

```
DeviceA# show nfpp dhcpv6-guard hosts
If col_filter 1 shows '*', it means "hardware do not isolate host".
 VLAN    interface   IP address        Reason    remain-time(s)
 ----    ---------   ----------        ------    --------------
  1      Gi0/5       192.168.201.47    ATTACK    160
Total: 1 host
```

Run the **show nfpp dhcpv6-guard trusted-host** command to display the trusted hosts.

```
DeviceA# show nfpp dhcpv6-guard trusted-host
IP address          mask
----------          ----
192.168.201.46      255.255.255.255
Total: 1 record(s)
```

Instruction

If attack traffic carries the VLAN ID 0, NFPP may consider the corresponding host as an attack host and configure a rate limiting threshold for the attack traffic. Run the **show nfpp dhcpv6-guard host** command to display the attack hosts. The VLAN ID field may be displayed as a port PVID or hidden.

Run the **show nfpp nd-guard summary** command to display the configuration.

```
DeviceA# 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    Disable 30/25/25/25
```