Contents

1 Configuring ND Snooping

1.1 Introduction

1.1.1 Overview

The Neighbor Discovery Protocol (NDP) is susceptible to address spoofing and routing information attacks due to its deficiency in inherent security. However, it is complex to enhance security by deploying an external encryption and authentication system. ND Snooping is used to monitor ND packets in a network to filter out invalid address resolution packets and RA packets, monitor IPv6 users in the network, and bind detected IPv6 users to interfaces to prevent IP address spoofing and build a secure and trusted IPv6 network.

1.1.2 Principles

1. NDP

NDP is a core protocol of the IPv6 suite. It combines and optimizes protocols such as the Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP) Router Discovery, and ICMP Redirect in IPv4. As a basic IPv6 protocol, NDP also provides the prefix discovery, neighbor unreachability detection (NUD), duplicate address detection (DAD), and auto address configuration functions.

- Address resolution: a method to determine the link-layer address (LLA) of a target node. The address resolution function of NDP replaces ARP in IPv4 and uses the NUD method to maintain the reachability status between neighbors.
- Stateless Address Autoconfiguration (SLACC): unique SLACC mechanism in NDP, including a series of related functions, such as router discovery, automatic interface ID generation, and DAD. Through SLACC, nodes on a link can automatically obtain global unicast IPv6 addresses.
- Redirection: When a better router for reaching the destination network is found on the local link, the original router needs to send advertisements to nodes, for the nodes to change related configurations.

2. ND Snooping Entries

- Entry creation mechanism

  When receiving an ND packet from an unknown source address, the device creates an ND Snooping entry in **TENTATIVE** state. Then, the device sends a specified number of DAD neighbor solicitation (NS) packets to ND Snooping trusted ports (ports configured with the **ipv6 nd snooping trust** command) for snooping. The number of packets to be sent and the sending interval are configured by running the **ipv6 nd snooping detect packet** command. If no neighbor advertisement (NA) response is received within the **TENTATIVE** state timeout time (which can be configured by running the **ipv6 nd snooping tentative wait** command) after the last NS packet is sent, no conflicted addresses exist in the local area network (LAN). The ND Snooping entry is changed to the **VALID** state. If an NA packet is received within the **TENTATIVE** state timeout time after an NS packet is sent, conflicted addresses exist in the LAN. In this case, the device deletes the ND Snooping entry.

- Entry migration mechanism

Entry migration includes the following types:

- Intra-device migration

  When the device receives an ND packet with the same source address as an existing ND Snooping entry from an ND Snooping untrusted port in the same VLAN, the entry state is changed to **TESTING_VP**. Then, the device sends a specified number of DAD NS packets to the inbound port that learns the ND Snooping entry for snooping. The number of packets to be sent and the sending interval are configured by running the **ipv6 nd snooping detect packet** command. If no NA packet is received within the **TESTING_VP** state timeout time (which can be configured by running the **ipv6 nd snooping detect wait** command), the original user is disconnected from the inbound port. The device changes the inbound port of the ND Snooping entry to the port receiving the new packet and changes the entry state to **VALID**. If an NA packet is received within the **TESTING_VP** state timeout time after the first NS packet is sent, the inbound port of the ND Snooping entry remains unchanged and the entry state is restored to **VALID**.

- Inter-device migration

  When the device receives an ND packet with the same source address as an existing ND snooping entry from an ND Snooping trusted port, the ND Snooping entry is changed to the **TESTING_TP-LT** state. Then, the device sends a specified number of DAD NS packets to the inbound port that learns the ND Snooping entry for snooping. The number of packets to be sent and the sending interval are configured by running the **ipv6 nd snooping detect packet** command. If no NA packet is received within the **TESTING_TP-LT** state timeout time (which can be configured by running the **ipv6 nd snooping detect wait** command), the original user is disconnected from the inbound port. Then, the device deletes the corresponding ND Snooping entry, and the device connected to the ND trusted port creates an ND Snooping entry. In this case, cross-device entry migration is complete. If an NA packet is received within the **TESTING_TP-LT** state timeout time after the NS packets are sent, the original user is not disconnected from the inbound port. In this case, the device reserves the corresponding ND Snooping entry, changes the entry state to **VALID**, and forwards the NA packet to the trusted port.

- Entry aging mechanism

  If no ND packet is received within the **VALID** state timeout time (which can be configured by running the **ipv6 nd snooping bind lifetime** command) since the last update of an ND Snooping entry, the ND Snooping entry is changed to the **TESTING_TP-LT** state. Then, the device sends a specified number of DAD NS packets to the inbound port that learns the ND Snooping entry for snooping. The number of packets to be sent and the sending interval are configured by running the **ipv6 nd snooping detect packet** command. If no NA packet is received within the **TESTING_TP-LT** state timeout time (which can be configured by running the **ipv6 nd snooping detect wait** command), the original user is disconnected from the inbound port. The device deletes the ND Snooping entry. If an NA packet is received within the **TESTING_TP-LT** state timeout time, the original user is not disconnected from the inbound port. In this case, the device reserves the ND Snooping entry, changes the entry state to **VALID**, and resets the timeout time.

3. ND Snooping

ND Snooping supports the following functions:

- ND guard

When SLACC is used, IPv6 nodes use RA information to configure interface IPv6 addresses and obtain the prefixes of direct-connected network segments, gateway IP addresses, and maximum transmission units (MTUs) of links. In addition, routers can use ND redirect packets to modify the next-hop information of related routes in the routing tables of hosts. In this case, attackers can send invalid RA and redirect packets and modify routing table information (such as the gateway IP address) of the attacked host to initiate denial-of-service (DoS) and man-in-the-middle (MITM) attacks. This type of attacks for spoofing hosts' routing information is called routing information attacks.

During unicast communication between IPv6 nodes, the NDP is used for address resolution to obtain LLAs of neighboring nodes. Then, the parsed LLAs are encapsulated into frames to be sent. Five types of ND packets can carry the LLA, and the receiving nodes regard the packets as trusted. Therefore, attackers can send forged ND packets and modify the mappings between IP addresses and LLAs in the neighbor table of the attacked node to initiate DoS and MITM attacks. This type of attacks for spoofing the mappings between IP addresses and LLAs on nodes is called ARP attacks.

To prevent the preceding two types of attacks, ND Snooping classifies interfaces on network devices into trusted interfaces and untrusted interfaces. Trusted interfaces are used to connect trusted nodes, such as the routers and servers, and untrusted interfaces are used to connect untrusted nodes, such as PCs. The device forwards ND packets received on trusted interfaces and discards redirect and RA packets received on untrusted interfaces to prevent routing information attacks. For router solicitation (RS), NS, and NA packets received on untrusted interfaces, the device checks the packet validity and discards invalid ones to prevent address spoofing attacks.

For NS and NA packets, the device checks mappings of the source IP address, destination IP address, VLAN ID (VID), Media Access Control (MAC) address, and inbound interface. The mappings of the four elements of host nodes are provided by monitoring SLACC users. If an NA packet received on an untrusted interface carries information that can be set only by a router (R bit is set to 1), the packet is regarded as invalid.

Security check on ND packets from all host nodes prevent gateway address spoofing attacks. To guard against only gateway address spoofing attack address spoofing attacks, see "ND guard against gateway address spoofing attacks." ND guard against RA attacks is regardless of the preceding factors. You can enable ND guard against address spoofing attacks by running the corresponding command. ND guard against RA attacks is enabled when ND snooping is enabled.

- ND guard against gateway address spoofing attacks

  Gateway address spoofing is a common attack method and causes severe adverse impact. If gateway address spoofing attacks are eliminated, a network is free from most address spoofing attacks. In addition, when only ND guard against gateway address spoofing attacks is enabled, system resources are saved. To facilitate use, ND Snooping supports not only manual gateway information configuration but also automatic gateway information acquisition.

  A gateway is one of key nodes in a network. ND Snooping supports ND guard against gateway address spoofing attacks. That is, ND packets received on untrusted interfaces are checked only to determine whether they are forged ND packets of key nodes, so as to discard forged packets. This significantly reduces the CPU load of network devices, resource consumption, and dependency on other security features, such as the features mentioned in the description about ND guard. Gateway information can be obtained automatically or manually. Key node information is automatically generated from the obtained gateway information to ensure ND guard against gateway address spoofing attacks.

During automatic gateway information acquisition, ND Snooping allows automatic learning of gateway information by snooping RA packets in the network. If the gateway is changed, ND Snooping supports automatic update of the gateway information. The whole process is transparent to the network administrator and does not require special configuration. During manual IPv6 network configuration, you can manually add gateway information and information about servers (key nodes) to guard against server address spoofing attacks.

- RA guard

  RA guard is used to guard against RA packet attacks on L2 access devices. On the basis of ND guard against gateway address spoofing attacks, RA guard is used to check RA packets from ND Snooping trusted interfaces based on more detailed rules, for example, check the source MAC address and source IPv6 address in the RA packets. Only RA packets that meet the rules are forwarded.

- SLACC user monitoring

  Users who use SLACC are called SLACC users. During SLACC, the network administrator does not know how many IPv6 users exist in the network and therefore cannot deploy related management policies.

  When a network attack occurs, the network administrator can obtain the attacker's IP address. However, the network administrator can only locate the specific network segment based on the IP address but not locate the specific network device port or physical client. To resolve the preceding problem, you can monitor SLACC users in the network to obtain related user information. SLACC user monitoring can be configured only on untrusted interfaces.

- ND Snooping and CPP

  Network devices consume certain CPU resources to check ND packet security. To prevent attackers from initiating DoS attacks by sending a large number of ND packets, network devices can use the CPU Protect Policy (CPP) function to control the rate and priority of ND packets. After the ND Snooping function is enabled, the CPP function is enabled automatically for ND packets.

- ND Snooping and NFPP

  The CPP function is used for overall control on ND packets. Moreover, the Network Foundation Protection Policy (NFPP) function can be used to limit the rate of ND packets on interfaces more accurately. The NFPP function takes effect only to ND packets destined for the CPU.

1.1.3 Protocols and Standards

- RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- RFC 4861 Neighbor Discovery for IP version 6 (IPv6)
- RFC 4862 IPv6 Stateless Address Autoconfiguration
- RFC 6620 FCFS SAVI: First-Come, First-Served Source Address Validation Improvement for Locally Assigned IPv6 Addresses

1.2 Configuration Task Summary

ND Snooping configuration includes the following tasks:

(1) Configuring Basic ND Snooping Functions

(2) (Optional) Configuring ND Guard

(3) (Optional) Configuring ND Logging

1.3 Configuring Basic ND Snooping Functions

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the ND Snooping function to monitor the SLACC process.

ipv6 nd snooping enable

ND Snooping is disabled by default.

(4) (Optional) Disable ND Snooping on a VLAN.

no ipv6 nd snooping enable vlan { *vlan-rng* | *vid* }

After ND Snooping is enabled on a device, it takes effect to all VLANs of the device by default.

(5) (Optional) Configure the lease for an ND Snooping binding entry.

ipv6 nd snooping bind lifetime *time*

The lease time of an ND Snooping binding entry is 300s by default.

(6) (Optional) Configure the capacity for ND Snooping binding entries.

ipv6 nd snooping bind limit *limit*

The capacity configured before delivery is used by default. On interfaces, the capacity for ND snooping binding entries is not limited.

(7) (Optional) Configure the capacity alarm threshold for ND snooping binding entries.

ipv6 nd snooping bind warning-threshold *number*

No capacity alarm threshold is configured for the ND snooping binding entries by default.

(8) (Optional) Configure the waiting time for an address conflict response.

ipv6 nd snooping tentative wait *time*

The default waiting time for an address conflict response is 500 ms.

(9) Enter the interface configuration mode.

interface *interface-type interface-number*

(10) Configure an interface as a ND Snooping trusted interface.

ipv6 nd snooping trust

All interfaces are ND Snooping untrusted interfaces by default.

1.4 Configuring ND Guard

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure the number of detection packets to be sent and the interval for sending detection packets when conflicted packets are received.

ipv6 nd snooping detect packet *number* **interval** *time*

Two detection packets are sent at an interval of 250 ms by default.

(4) (Optional) Configure the waiting time for a detection packet response.

ipv6 nd snooping detect wait *time*

The default waiting time for a detection packet response is 500 ms.

(5) (Optional) Configure ND Snooping to work only in ND packet validity check mode.

ipv6 nd snooping nd-check only

ND Snooping is not configured to work only in ND packet validity check mode by default.

After this function is enabled, no ND Snooping entry is generated.

(6) (Optional) Configure the prefix for static IPv6 addresses.

ipv6 nd snooping prefix vlan *vlan-id ipv6-address/prefix-length*

No prefix is configured for static IPv6 addresses by default.

(7) Enter the interface configuration mode.

interface *interface-type interface-number*

(8) Enable ND guard against address spoofing attacks.

ipv6 nd snooping check address-resolution

ND guard against address spoofing attacks is disabled by default.

1.5 Configuring ND Logging

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of logging ND Snooping key information.

ipv6 nd snooping log enable

The function of logging ND Snooping key information is disabled by default.

(4) (Optional) Configure the capacity of ND Snooping key information logs.

ipv6 nd snooping log limit *number*

A maximum of 1000 ND Snooping key information logs can be recorded by default.

(5) Enable the function of prompting ND Snooping key information.

ipv6 nd snooping syslog enable

The function of prompting ND snooping key information is disabled by default.

(6) (Optional) Configure the frequency of ND Snooping key information prompts.

ipv6 nd snooping syslog frequency *number*

A maximum of 5 prompts for ND snooping key information are provided every second by default.

1.6 Monitoring

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

Run the **clear** command to clear information.

Run the **debug** command to output debugging information.

Caution

- Running the **clear** command may lose vital information and thus interrupt services.
- The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-1 Monitoring

Command	Purpose
show ipv6 nd snooping prefix	Displays snooped prefix information.
show ipv6 nd snooping binding [*ipv6-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*]	Displays snooped users with IPv6 stateless addresses.
show ipv6 nd snooping log	Displays ND Snooping key information logs recorded in the memory.
show ipv6 nd snooping packet	Displays ND Snooping packet statistics on an interface.
clear ipv6 nd snooping prefix [**vlan** *vid*]	Clears all prefixes or prefixes snooped in a VLAN.
clear ipv6 nd snooping binding [**vlan** *vid*]	Clears SLACC users.
clear ipv6 nd snooping packet [**interface** *interface-id*]	Clears all packet statistics or packet statistics on an interface.
debug ipv6 nd snooping	Debugs ND Snooping events.

1.7 Configuration Examples

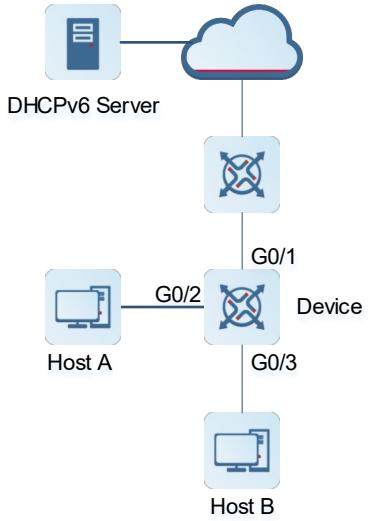
1.7.1 Configuring ND Guard

1. Requirements

Hosts use DHCPv6 to assign IPv6 addresses and enable DHCPv6 Snooping. They also need ND guard against RA attacks and address spoofing attacks.

2. Topology

Figure 1-1 Configuring ND Guard



3. Notes

- Enable ND Snooping.
- Configure trusted interfaces.
- Enable only ND guard against address spoofing attacks.

4. Procedure

```
Device> enable
Device# configure terminal
Device(config)# ipv6 nd snooping enable
Device(config)# interface gigabitethernet 0/1
Device(config-if-GigabitEthernet 0/1)# ipv6 nd snooping trust
Device(config-if-GigabitEthernet 0/1)# exit
Device(config)# interface gigabitethernet 0/2
Device(config-if-GigabitEthernet 0/2)# ipv6 nd snooping check address-resolution
Device(config-if-GigabitEthernet 0/2)# exit
Device(config)# interface gigabitethernet 0/3
Device(config-if-GigabitEthernet 0/3)# ipv6 nd snooping check address-resolution
```

5. Configuration Files

Device configuration file

```
hostname Device
!
ipv6 nd snooping enable
!
interface GigabitEthernet 0/1
 ipv6 nd snooping trust
```

```
!
interface GigabitEthernet 0/2
 ipv6 nd snooping check address-resolution
!
interface GigabitEthernet 0/3
 ipv6 nd snooping check address-resolution
!
end
```