# 1 ND Snooping Commands

| Command | Function |
|---|---|
| clear ipv6 nd snooping prefix | Clear IPv6 prefixes snooped in a virtual local area network (VLAN). |
| clear ipv6 nd snooping binding | Clear snooped Stateless Address Autoconfiguration (SLACC) users. |
| clear ipv6 nd snooping packet | Clear Neighbor Discovery (ND) Snooping packet statistics on an interface. |
| ipv6 nd snooping bind lifetime | Configure the lease of an ND Snooping binding entry. |
| ipv6 nd snooping bind limit | Configure the capacity for ND Snooping binding entries. |
| ipv6 nd snooping bind warning-threshold | Configure a capacity alarm threshold for the ND Snooping binding entries. |
| ipv6 nd snooping check address-resolution | Enable ND guard against address spoofing attacks. |
| ipv6 nd snooping detect packet | 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 wait | Configure the waiting time for a detection packet response. |
| ipv6 nd snooping enable | Enable the ND Snooping function to snoop the SLACC process. |
| ipv6 nd snooping enable vlan | Enable ND Snooping on a VLAN. |
| ipv6 nd snooping log enable | Enable the function of logging ND Snooping key information. |
| ipv6 nd snooping log limit | Configure the capacity for ND Snooping key information logs. |
| ipv6 nd snooping nd-check only | Configure ND Snooping to work only in ND packet validity check mode but not generate binding entries. |
| ipv6 nd snooping prefix vlan | Configure the prefix for static IPv6 addresses. |
| ipv6 nd snooping syslog enable | Enable the function of prompting ND Snooping key |

| | |
|---|---|
| | information. |
| ipv6 nd snooping syslog frequency | Configure the frequency of ND Snooping key information prompts. |
| ipv6 nd snooping tentative wait | Configure the waiting time for an address conflict response. |
| ipv6 nd snooping trust | Configure an interface as an ND Snooping trusted interface. |
| show ipv6 nd snooping prefix | Display snooped prefixes. |
| show ipv6 nd snooping binding | Display snooped ND Snooping binding entries. |
| show ipv6 nd snooping log | Display ND Snooping key information logs recorded in the memory. |
| show ipv6 nd snooping packet | Display ND Snooping packet statistics on an interface. |

## 1.1 clear ipv6 nd snooping prefix

### Function

Run the **clear ipv6 nd snooping prefix** command to clear IPv6 prefixes snooped in a virtual local area network (VLAN).

### Syntax

**clear ipv6 nd snooping prefix** [ **vlan** *vlan-id* ]

### Parameter Description

**vlan** *vlan-id*: Specifies the VLAN in which the snooped IPv6 prefixes are cleared.

### Command Modes

Privileged EXEC mode

### Default Level

14

### Usage Guidelines

N/A

### Examples

The following example clears IPv6 prefixes snooped in all VLANs.

```
Hostname> enable
Hostname# clear ipv6 nd snooping prefix
```

### Notifications

N/A

### Platform Description

N/A

## 1.2 clear ipv6 nd snooping binding

### Function

Run the **clear ipv6 nd snooping binding** command to clear snooped Stateless Address Autoconfiguration (SLACC) users.

### Syntax

**clear ipv6 nd snooping binding** [ **vlan** *vlan-id* ]

### Parameter Description

**vlan** *vlan-id*: Specifies the VLAN in which snooped SLACC users are cleared.

### Command Modes

Privileged EXEC mode

### Default Level

14

### Usage Guidelines

N/A

### Examples

The following example clears SLACC users snooped in all VLANs.

```
Hostname> enable
Hostname# clear ipv6 nd snooping binding
```

### Notifications

N/A

### Platform Description

N/A

## 1.3 clear ipv6 nd snooping packet

### Function

Run the **clear ipv6 nd snooping packet** command to clear Neighbor Discovery (ND) Snooping packet statistics on an interface.

### Syntax

**clear ipv6 nd snooping packet** [ **interface** *interface-type interface-number* ]

### Parameter Description

*interface-type interface-number*: Interface on which the ND Snooping packet statistics are cleared.

### Command Modes

Privileged EXEC mode

### Default Level

14

### Usage Guidelines

This command is used to clear ND Snooping packet statistics on an interface, including the numbers of received, discarded, and forwarded ND packets, the total number of each type of ND packets, and the number of each type of ND packets discarded.

### Examples

The following example clears ND Snooping packet statistics on all interfaces.

```
Hostname> enable
```

```
Hostname# clear ipv6 nd snooping packet
```

### Notifications

N/A

### Platform Description

N/A

## 1.4 ipv6 nd snooping bind lifetime

### Function

Run the **ipv6 nd snooping bind lifetime** command to configure the lease of an ND Snooping binding entry.

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

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

### Syntax

**ipv6 nd snooping bind lifetime** *time*

**no ipv6 nd snooping bind lifetime**

### Parameter Description

*time*: Lease time of an entry, in seconds. The range is from 5 to 604800.

### Command Modes

Global configuration mode

### Default Level

14

### Usage Guidelines

This command is used to configure the lease time for an entry to prevent binding entries from occupying the memory space for a long time.

### Examples

The following example sets the lease time of an ND Snooping binding entry to 3600s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd snooping bind lifetime 3600
```

### Related Commands

N/A

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

## 1.5 ipv6 nd snooping bind limit

### Function

Run the **ipv6 nd snooping bind limit** command to configure the capacity for ND Snooping binding entries.

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

The capacity for binding entries depends on the actual product by default.

### Syntax

**ipv6 nd snooping bind limit** *limit*

**no ipv6 nd snooping bind limit**

### Parameter Description

*limit*: Capacity for binding entry. The value range is from 7 to 1048576.

### Command Modes

Global configuration mode

Interface configuration mode

### Default Level

14

### Usage Guidelines

This command is used to configure the capacity for binding entries. The configured value cannot be less than the current number of binding entries.

### Examples

The following example sets the total capacity for binding entries to **1024** and sets that on GigabitEthernet 0/1 to **128**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd snooping bind limit 1024
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd snooping bind limit 128
Hostname(config-if-GigabitEthernet 0/1)# exit
```

### Notifications

When the configured capacity value is smaller than the current number of binding entries, the following notification will be displayed:

```
% Failed to execute command, because of "current num more than config maximum".
```

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

- **ipv6 nd snooping bind warning-threshold**

## 1.6 ipv6 nd snooping bind warning-threshold

### Function

Run the **ipv6 nd snooping bind warning-threshold** command to configure a capacity alarm threshold for the ND Snooping binding entries.

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

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

### Syntax

**ipv6 nd snooping bind warning-threshold** *number*

**no ipv6 nd snooping bind warning-threshold**

### Parameter Description

*number*: Capacity alarm threshold for the binding entries, in percentage (%). The range is from 15 to 100.

### Command Modes

Global configuration mode

Interface configuration mode

### Default Level

14

### Usage Guidelines

This command is used to configure a capacity alarm threshold for the binding entries. For example, if *num* is set to **60**, an alarm is triggered when the current number of entries exceeds 60% of the configured capacity and a prompt is displayed when the current number of entries is less than 60% of the configured capacity. When the configuration is canceled, *num* is set to **0**. In this case, no capacity alarm is triggered. When this command is configured on an interface and the capacity for binding entries is not limited on the interface (that is, the *limit* parameter in **ipv6 nd snooping bind limit** is set to **0**), no capacity alarm is triggered.

### Examples

The following example sets the capacity alarm threshold for the global binding entries to **60** and sets that on GigabitEthernet 0/1 to **60**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd snooping bind warning-threshold 60
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd snooping bind warning-threshold
60
```

### Notifications

When a capacity alarm threshold (for example, 15) is configured for the binding entries and the percentage of the current number of entries to the configured capacity exceeds the configured threshold, the following notification will be displayed:

```
The binding user has exceeded the 15 percent capacity of count limit.
```

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

- **ipv6 nd snooping bind limit**

## 1.7 ipv6 nd snooping check address-resolution

### Function

Run the **ipv6 nd snooping check address-resolution** command to enable ND guard against address spoofing attacks.

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

ND guard against address spoofing attacks is disabled by default.

### Syntax

**ipv6 nd snooping check address-resolution**

**no ipv6 nd snooping check address-resolution**

### Parameter Description

N/A

### Command Modes

Interface configuration mode

### Default Level

14

### Usage Guidelines

When ND guard against address spoofing attacks is enabled, the IPv6 address and Media Access Control (MAC) address fields in neighbor solicitation (NS), neighbor advertisement (NA), and router solicitation (RS) packets received on an interface are checked whether match the binding entries. ND packets that do not match the binding entries are discarded.

**Note**

The entries for ND guard against address spoofing attacks come from the Source Address Validation Improvements (SAVI) binding table instead of the ND Snooping binding table.

### Examples

The following example enables ND guard against address spoofing attacks.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd snooping check address-resolution
```

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

N/A

## 1.8 ipv6 nd snooping detect packet

### Function

Run the **ipv6 nd snooping detect packet** command to configure the number of detection packets to be sent and the interval for sending detection packets when conflicted packets are received.

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

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

### Syntax

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

**no ipv6 nd snooping detect packet**

### Parameter Description

*number*: Number of detection packets to be sent. The range is from 1 to 10.

*time*: Interval for sending detection packets, in milliseconds. The range is from 50 to 5000.

### Command Modes

Global configuration mode

### Default Level

14

### Usage Guidelines

When the device with ND Snooping enabled receives an NS or NA packet with an address that conflicts with that in a binding entry or the lease of a binding entry expires, the device sends a detection packet to the port recorded in the binding entry. This command is used to set the number of detection packets to be sent and the interval for sending detection packets.

⚠ **Caution**

The interval is only a reference value in ND Snooping for sending packets and may be inaccurate.

### Examples

The following example sets the number of detection packets to be sent to **2** and the interval for sending detection packets to **2000**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd snooping detect packet 2 interval 2000
```

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

- ipv6 nd snooping log limit

## 1.9 ipv6 nd snooping detect wait

### Function

Run the **ipv6 nd snooping detect wait** command to configure the waiting time for a detection packet response.

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

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

### Syntax

**ipv6 nd snooping detect wait** *time*

**no ipv6 nd snooping detect wait**

### Parameter Description

*time*: Waiting time, in milliseconds. The range is from 50 to 5000. The waiting time is only a reference value in ND Snooping and may be inaccurate.

### Command Modes

Global configuration mode

### Default Level

14

### Usage Guidelines

This command is used to configure the waiting time for a detection packet response after the device with ND Snooping enabled sends a detection packet. If no response is received within the waiting time, the device deletes the corresponding entry.

### Examples

The following example sets the waiting time for a detection packet response to 2000 ms.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd snooping detect wait 2000
```

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

- ipv6 nd snooping detect packet

## 1.10 ipv6 nd snooping enable

### Function

Run the **ipv6 nd snooping enable** command to enable the ND Snooping function to snoop the SLACC process.

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

ND Snooping is disabled by default.

### Syntax

**ipv6 nd snooping enable**

**no ipv6 nd snooping enable**

### Parameter Description

N/A

### Command Modes

Global configuration mode

### Default Level

14

### Usage Guidelines

Snooped SLACC user information can be used for ND guard and other security policies.

### Examples

The following example enables ND Snooping.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd snooping enable
```

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

N/A

## 1.11 ipv6 nd snooping enable vlan

### Function

Run the **ipv6 nd snooping enable vlan** command to enable ND Snooping on a VLAN.

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

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

### Syntax

**ipv6 nd snooping enable vlan** { *vlan-range* | *vlan-id* }

**no ipv6 nd snooping enable vlan** { *vlan-range* | *vlan-id* }

### Parameter Description

*vlan-range*: Range of VLANs to which ND Snooping takes effect. The value is a character string, for example 1, 3–5, 7, and 9–11.

*vlan-id*: ID of a VLAN. The range is from 1 to 4096.

### Command Modes

Global configuration mode

### Default Level

14

### Usage Guidelines

If SLACC snooping is not required in a VLAN, you can run this command to disable ND Snooping on the VLAN.

### Examples

The following example disables ND Snooping on VLAN 5 and VLANs 10 to 20.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd snooping enable
Hostname(config)# no ipv6 nd snooping enable vlan 5,10-20
```

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

N/A

## 1.12 ipv6 nd snooping log enable

### Function

Run the **ipv6 nd snooping log enable** command to enable the function of logging ND Snooping key information.

Run the **no** form of this command to disable this feature and clear key information logs in the memory.

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

### Syntax

**ipv6 nd snooping log enable**

**no ipv6 nd snooping log enable**

### Parameter Description

N/A

### Command Modes

Global configuration mode

### Default Level

14

### Usage Guidelines

After enabling ND guard against address spoofing attacks or RA attacks, you can run this command to enable the function of logging ND Snooping key information. When the device receives packets for address spoofing attacks or RA attacks, information about the attacker is recorded to the memory via attack logs.

### Examples

The following example enables the function of logging ND Snooping key information.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd snooping log enable
```

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

- ipv6 nd snooping log limit

## 1.13 ipv6 nd snooping log limit

### Function

Run the **ipv6 nd snooping log limit** command to configure the capacity for ND Snooping key information logs.

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

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

### Syntax

**ipv6 nd snooping log limit** *number*

**no ipv6 nd snooping log limit** *number*

### Parameter Description

*number*: Capacity value. The value range is from 50 to 5000.

### Command Modes

Global configuration mode

### Default Level

14

### Usage Guidelines

When the capacity for address spoofing or RA attack logs reaches the upper limit, new attack logs replace the earliest ones.

### Examples

The following example sets the capacity for ND Snooping key information logs to **500**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd snooping log limit 500
```

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

- ipv6 nd snooping log enable

## 1.14 ipv6 nd snooping nd-check only

### Function

Run the **ipv6 nd snooping nd-check only** command to configure ND Snooping to work only in ND packet validity check mode but not generate binding entries.

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

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

### Syntax

**ipv6 nd snooping nd-check only**

**no ipv6 nd snooping nd-check only**

### Parameter Description

N/A

### Command Modes

Global configuration mode

### Default Level

14

### Usage Guidelines

This command can be configured when ND Snooping entries do not need to be generated but the ND packet validity needs to be checked.

**Note**

This command takes effect only after ND Snooping is enabled.

### Examples

The following example configures ND Snooping to work only in ND packet validity check mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd snooping enable
Hostname(config)# ipv6 nd snooping nd-check only
```

### Related Commands

N/A

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

## 1.15 ipv6 nd snooping prefix vlan

### Function

Run the **ipv6 nd snooping prefix vlan** command to configure the prefix for static IPv6 addresses.

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

No prefix is configured for static IPv6 addresses by default.

### Syntax

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

**no ipv6 nd snooping prefix vlan** *vlan-id ipv6-address/prefix-length*

### Parameter Description

*vlan-id*: Access VLAN.

*ipv6-address/prefix-length-address/prefix-length*: IPv6 address and prefix.

### Command Modes

Global configuration mode

### Default Level

14

### Usage Guidelines

This command can be used to configure IPv6 address prefix entries.

### Examples

The following example sets the prefix for ND Snooping static IPv6 addresses to 2018:7::/64.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd snooping prefix vlan 1 2018:7::/64
```

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

N/A

## 1.16 ipv6 nd snooping syslog enable

### Function

Run the **ipv6 nd snooping syslog enable** command to enable the function of prompting ND Snooping key information.

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

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

### Syntax

**ipv6 nd snooping syslog enable**

**no ipv6 nd snooping syslog enable**

### Parameter Description

N/A

### Command Modes

Global configuration mode

### Default Level

14

### Usage Guidelines

After enabling ND guard against address spoofing attacks or RA attacks, you can run this command to enable the function of prompting ND Snooping key information. When the device receives packets of address spoofing attacks or RA attacks, information about the attacker is displayed via system prompts.

### Examples

The following example enables the function of prompting ND Snooping key information.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd snooping syslog enable
```

### Notifications

```
*Dec 27 20:34:13: %ND_SNP-COLLISION: Receive Address Resolution attack from
host<VLAN=2,port=Gi0/16,MAC=e0db.5594.c026,IPv6=fe80::11da:cb7e:57db:e231> was
detected.
```

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

- ipv6 nd snooping syslog frequency

## 1.17 ipv6 nd snooping syslog frequency

### Function

Run the **ipv6 nd snooping syslog frequency** command to configure the frequency of ND Snooping key information prompts.

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

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

### Syntax

**ipv6 nd snooping syslog frequency** *number*

**no ipv6 nd snooping syslog frequency**

### Parameter Description

*number*: Frequency of system prompts, in pieces per second. The range is from 1 to 65535.

### Command Modes

Global configuration mode

### Default Level

14

### Usage Guidelines

This command is used to configure the frequency of ND Snooping key information prompts, that is, the maximum number of system prompts generated every second. When key information is generated, such as information about address spoofing attacks, RA attacks, capacity threshold alarms, and entry capacity alarms, the system generates corresponding prompt logs. When the number of logs generated every second is greater than the configured frequency, the system displays logs within the frequency range only and discard remaining logs to prevent the screen from frequent refreshing.

⚠ **Caution**

The log limit function is implemented based on the system time, while the log display is implemented based on the user time. Therefore, the number of logs with the same time on the console is [0, 2 x *num*].

### Examples

The following example sets the frequency of ND Snooping key information prompts to 200 pieces per second.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd snooping syslog frequency 200
```

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

- ipv6 nd snooping syslog enable

## 1.18 ipv6 nd snooping tentative wait

### Function

Run the **ipv6 nd snooping tentative wait** command to configure the waiting time for an address conflict response.

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

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

### Syntax

**ipv6 nd snooping tentative wait** *time*

**no ipv6 nd snooping tentative wait**

### Parameter Description

*time*: Waiting time, in milliseconds. The range is from 50 to 5000. The waiting time is only a reference value in ND Snooping and may be inaccurate.

### Command Modes

Global configuration mode

### Default Level

14

### Usage Guidelines

When the device with ND Snooping enabled receives a DAD_NS packet (for duplicate address check) from a client, the device creates an entry in **TENTATIVE** state. The entry is changed to a formal binding entry after a period of time.

### Examples

The following example sets the waiting time for an address conflict response to 2000 ms.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 nd snooping tentative wait 2000
```

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

N/A

## 1.19 ipv6 nd snooping trust

### Function

Run the **ipv6 nd snooping trust** command to configure an interface as an ND Snooping trusted interface.

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

All interfaces are ND Snooping untrusted interfaces by default.

### Syntax

**ipv6 nd snooping trust**

**no ipv6 nd snooping trust**

### Parameter Description

N/A

### Command Modes

Interface configuration mode

### Default Level

14

### Usage Guidelines

After an interface is configured as an ND Snooping trusted interface, RA and RR packets received on this interface are forwarded, and such packets received on untrusted interfaces are discarded.

This command can be configured only on L2 switching ports, aggregation ports (APs), or encapsulation sub-interfaces.

**Note**

Generally, uplink interfaces, that is, interfaces connected to trusted gateways are configured as trusted interfaces.

### Examples

The following example configures GigabitEthernet 0/1 as an ND Snooping trusted interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd snooping trust
```

### Notifications

N/A

### Common Errors

N/A

### Platform Description

N/A

### Related Commands

N/A

## 1.20 show ipv6 nd snooping prefix

### Function

Run the **show ipv6 nd snooping prefix** command to display snooped prefixes.

### Syntax

**show ipv6 nd snooping prefix**

### Parameter Description

N/A

### Command Modes

All modes except the user EXEC mode

### Default Level

14

### Usage Guidelines

N/A

### Examples

The following example displays snooped prefixes.

```
Hostname> enable
Hostname# show ipv6 nd snooping prefix
VLAN  Prefix                                    Lifetime(s)
----  ------                                    -----------
2     1001::/64                                 STATIC
```

**Table 1-1Output Fields of the show ipv6 nd snooping prefix Command**

| Field | Description |
|---|---|
| Prefix | Prefix |
| lifetime | Lease |

### Notifications

N/A

### Platform Description

N/A

## 1.21 show ipv6 nd snooping binding

### Function

Run the **show ipv6 nd snooping binding** command to display snooped ND Snooping binding entries.

### Syntax

**show ipv6 nd snooping binding** [ *ipv6-address* ] [ *mac-address* ] [ **vlan** *vlan-id* ] [ **interface** *interface-type interface-number* ]

### Parameter Description

*ipv6-address*: IPv6 address with its binding entry displayed.

*mac-address*: MAC address with its binding entry displayed.

*vlan-id*: VLAN with learned binding entries displayed.

*interface-type interface-number*: Interface with learned binding entries displayed.

### Command Modes

All modes except the user EXEC mode

### Default Level

14

### Usage Guidelines

N/A

### Examples

The following example displays snooped ND Snooping binding entries.

```
Hostname> enable
Hostname# show ipv6 nd snooping binding
Total number of bindings: 5
VLAN MAC address      Interface    State         IPv6 address
Life time(s)
1024 b8ac.6fc8.8b9a   Gi3/17       VALID         2018:5::1
14376
1024 b8ac.6fc8.8b9a   Gi3/17       TENTATIVE     2018:5::48ed:679a:a862:febd
5
1024 b8ac.6fc8.8b9a   Gi3/17       VALID         2018:5::8880:86f0:ebda:c734
14381
1024 b8ac.6fc8.8b9a   Gi3/17       VALID         2018:5::c58f:91d1:3dab:4e85
14381
1024 b8ac.6fc8.8b9a   Gi3/17       VALID         fe80::c58f:91d1:3dab:4e85
14376
```

**Table 1-1Output Fields of the show ipv6 nd snooping binding Command**

| Field | Description |
|---|---|
| MAC address | MAC address |
| Interface | Interface |
| State | Status |
| IPv6 address | IPv6 address |
| Life time | Lease |

### Notifications

N/A

### Platform Description

N/A

## 1.22 show ipv6 nd snooping log

### Function

Run the **show ipv6 nd snooping log** command to display ND Snooping key information logs recorded in the memory.

### Syntax

**show ipv6 nd snooping log**

### Parameter Description

N/A

### Command Modes

All modes except the user EXEC mode

### Default Level

14

### Usage Guidelines

N/A

### Examples

The following example displays ND Snooping key information logs recorded in the memory.

```
Hostname> enable
Hostname# show ipv6 nd snooping log
Total log num:3
Time                Event         Packet                             IPv6 Address
MAC VLAN    PORT
2017-12-27 20:34:15 ND Error          NA                fe80::11da:cb7e:57db:e231
e0db.5594.c026    2  Gi0/16
2017-12-27 20:34:14 ND Error          NA                fe80::11da:cb7e:57db:e231
e0db.5594.c026    2  Gi0/16
2017-12-27 20:34:13 ND Error          NA                fe80::11da:cb7e:57db:e231
e0db.5594.c026    2  Gi0/16
```

**Table 1-1Output Fields of the show ipv6 nd snooping log Command**

| Field | Description |
|---|---|
| Time | Time when an address spoofing attack packet or RA attack packet is received |
| Event | Type of an attack packet |
| Packet | Content of an attack packet |

| | |
|---|---|
| IPv6 address | IPv6 address used by an attacker |
| MAC | MAC address used by an attacker |
| VLAN | ID of the source VLAN of an attack packet |
| PORT | ID of the source port of an attack packet |

### Notifications

N/A

### Platform Description

N/A

## 1.23 show ipv6 nd snooping packet

### Function

Run the **show ipv6 nd snooping packet** command to display ND Snooping packet statistics on an interface.

### Syntax

**show ipv6 nd snooping packet**

### Parameter Description

N/A

### Command Modes

All modes except the user EXEC mode

### Default Level

14

### Usage Guidelines

N/A

### Examples

The following example displays ND Snooping packet statistics on an interface.

```
Hostname> enable
Hostname# show ipv6 nd snooping packet
Total port num:145 (port which process none packet doesn't display)
Interface     Total Recv  Total Drop   Total Fwd  NS Discard/ NS Process  NA
Discard/ NA Process  RS Discard/ RS Process  RA Discard/ RA Process  RR Discard/
RR Process
Gi7/1              11863       10883         980           0/         70
0/       875           0/         35       10883/      10883           0/
0
```

```
Lc0                 189           0          189             0/          70
0/         70            0/          0            0/          49            0/
0
```

**Table 1-1Output Fields of the show ipv6 nd snooping packet Command**

| Field | Description |
|---|---|
| Interface | Interface name |
| Total Recv | Total number of packets received on the interface |
| Total Drop | Total number of discarded packets from the specified interface |
| Total Fwd | Total number of forwarded packets from the specified interface |
| NS Discard | Total number of discarded NS packets from the interface |
| NS Process | Total number of NS packets from the interface processed by ND Snooping |
| NA Discard | Total number of discarded NA packets from the interface |
| NA Process | Total number of NA packets from the interface processed by ND Snooping |
| RS Discard | Total number of discarded RS packets from the interface |
| RS Process | Total number of RS packets from the interface processed by ND Snooping |
| RA Discard | Total number of discarded RA packets from the interface |
| RA Process | Total number of RA packets from the interface processed by ND Snooping |
| RR Discard | Total number of discarded RR packets from the interface |
| RR Process | Total number of RR packets from the interface processed by ND Snooping |

### Notifications

N/A

### Platform Description

N/A