Contents

1 Configuring DHCPv6 Snooping

1.1 Introduction

1.1.1 Overview

Dynamic Host Configuration Protocol for IPv6 (DHCPv6) snooping snoops DHCPv6 packets are exchanged between clients and servers, including request packets from the clients and response packets from the servers. These packets are used to record and monitor usage of IPv6 addresses and filter out invalid DHCPv6 packets. User data entries generated from DHCPv6 snooping records may serve security applications such as IPv6 Source Guard.

1.1.2 Principles

1. Basic Concepts

- DHCPv6 request packets

  Request packets are sent from a DHCPv6 client to a DHCPv6 server, including DHCPv6 SOLICIT, DHCPv6 REQUEST, DHCPv6 CONFIRM, DHCPv6 REBIND, DHCPv6 RELEASE, DHCPv6 DECLINE, DHCPv6 RENEW, DHCPv6 INFORM_REQ, and DHCPv6 LEASEQUERY packets.

- DHCPv6 response packets

  Response packets are sent from a DHCPv6 server to a DHCPv6 client, including DHCPv6 ADVERTISE, DHCPv6 REPLY, DHCPv6 RECONFIGURE, DHCPv6 RELAY_REPLY, DHCPv6 LEASEQUERY_REPLY, DHCPv6 LEASEQUERY_DONE, and DHCPv6 LEASEQUERY_DATA packets.

- VLAN-based DHCPv6 Snooping

  DHCPv6 Snooping is enabled on a per-VLAN basis. When DHCPv6 Snooping is enabled, it is effective to all virtual local area networks (VLANs) on the current device by default. You can flexibly specify the VLANs to which DHCPv6 Snooping takes effect.

- DHCPv6 Snooping trusted ports

  Packets for obtaining IPv6 addresses or prefixes through DHCPv6 are exchanged via multicast. Rogue DHCPv6 services may affect normal acquisition of IPv6 addresses and lead to spoofing and stealing of user information. To prevent rogue DHCPv6 services, DHCPv6 Snooping ports are classified into two types: trusted and untrusted.

  A device with DHCPv6 Snooping enabled only transmits DHCPv6 response packets received on trusted ports and discards those from untrusted ones. In this way, the ports connected to legitimate DHCP servers are configured as trusted ports and the other ports are configured as untrusted ports to shield rough DHCPv6 servers.

  On switches, all switching ports or L2 aggregation ports (APs) are defaulted as untrusted, and trusted ports can be specified.

- DHCPv6 Snooping binding database

In a DHCPv6 network, clients may set static IPv6 addresses randomly. This increases not only the difficulty of network maintenance but also the possibility that legitimate clients with IPv6 addresses assigned by a DHCPv6 server may fail to use the network due to address conflicts. By snooping packets between the clients and servers, DHCPv6 Snooping summarizes user entries, including IPv6 addresses, Media Access Control (MAC) addresses, VLAN IDs (VIDs), ports, and lease time to build the DHCPv6 Snooping binding database, ensuring proper use of IPv6 addresses.

- DHCPv6 Snooping packet suppression

  To shield all the DHCPv6 packets on a specific client, enable DHCPv6 Snooping packet suppression on untrusted ports.

- Invalid DHCPv6 packets

  The device with DHCPv6 Snooping enabled check validity of received DHCPv6 packets, discards invalid DHCPv6 packets, and records information about legitimate users to form the DHCPv6 Snooping binding database for query by other applications. The following types of packets are considered as invalid DHCPv6 packets:

  - DHCPv6 response packets received on untrusted ports. For details, see description about DHCPv6 response packets in “Basic Concepts”.
  - Relayed DHCPv6 packets received on untrusted ports, that is, the DHCPv6 RELAY_FORW and DHCPv6 RELAY_REPLY packets
  - DHCPv6 RELAY_REPLY packets received on trusted ports with untrusted outbound ports
  - DHCPv6_RELEASE packets with no entries in the DHCPv6 Snooping binding database found based on the source MAC addresses and VIDs in the packets
  - DHCPv6_RELEASE packets that carry IPv6 addresses or prefixes that are not existed in the DHCPv6 Snooping binding database
  - DHCPv6_RELEASE packets that carry IPv6 addresses or prefixes existing in the DHCPv6 Snooping binding database but having untrusted ports unmatched with those saved in the DHCPv6 Snooping binding database
  - DHCPv6 packets in invalid formats or incomplete DHCPv6 packets

2. Building a DHCPv6 Snooping Binding Database

The device with DHCPv6 Snooping enabled detects packets exchanged between DHCPv6 clients and DHCPv6 servers and generates entries in the DHCPv6 Snooping binding database and prefix database based on information of valid DHCPv6 packets. All these entries are used as the information table of legitimate users, and provided to other security modules of the device as the basis for filtering network packets.

The binding database and prefix database are updated during snooping based on the types of DHCPv6 packets.

- Generating binding or prefix entries

  When a DHCPv6 REPLY packet is snooped on a trusted port, the device with DHCPv6 Snooping enabled extracts the client's IPv6 address or prefix, MAC address, and lease time from the packet and generates a binding or prefix entry based on the client's port ID (interface index) and VLAN ID that are recorded on the device.

- Deleting binding or prefix entries

A binding or prefix entry is deleted in the following scenarios:

- The recorded lease time expires.
- A valid DHCPv6 RELEASE or DHCPv6 DECLINE packet from a client is snooped.
- A client user runs the **clear** command to delete a binding or prefix entry.

3. DHCPv6 Option 18 or 37

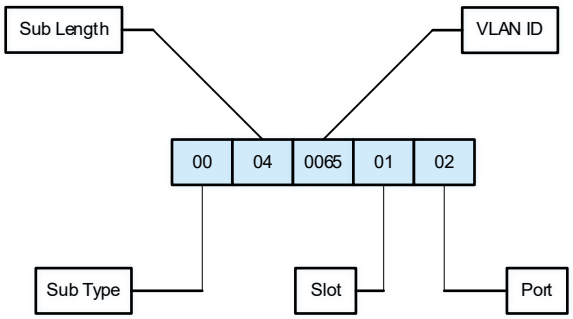
Some network administrators want to assign and manage IP addresses based on information about the network devices connected user clients (that is, client locations). To meet this requirement, a device with DHCPv6 Snooping enabled adds related network device information to DHCPv6 request packets by using a DHCPv6 option, which is Option 18 in RFC 3315 and Option 37 in RFC 4649. After Option 18 or 37 parsing is configured on a DHCPv6 server, the DHCPv6 server can obtain more user information based on the content of Option 18 or 37 and assign IP addresses to users more accurately.

- Option 18: Interface ID

  The default padding content of **Interface ID** is the ID of the VLAN to which the port receiving DHCPv6 request packets from clients resides or the index of the port. The port index value is the corresponding slot ID and port number. The extended padding content is a user-defined string. Extended padding is valid only to wired ports by default. Wired ports include switching ports, L2 APs, and L2 encapsulation sub-interfaces. For wireless ports, the extended padding content is **0**.

  Interface ID supports two padding formats: standard padding and extended padding. In a network, only one padding format can be used. In standard padding format, only the default padding content of is padded, as shown in the following figure.

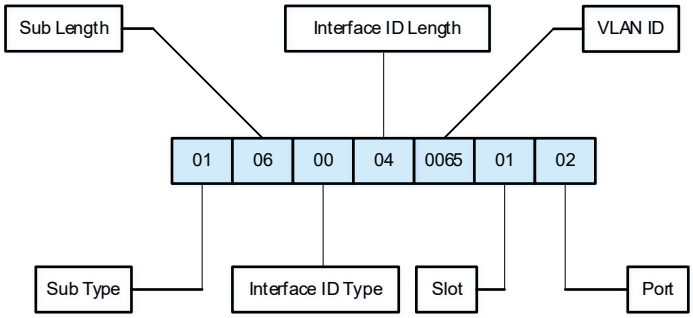
Figure 1-1Standard Padding Format of Interface ID



If user-defined padding content is required, use the extended padding format. In extended padding format, the padding content can be the default padding content or extended padding content. To distinguish between different padding content, a 1-byte content type field and a 1-byte content length field are added after the sub-option length field. For default padding content, the content type is set to **0**. For extended padding content, the content type is set to **1**.

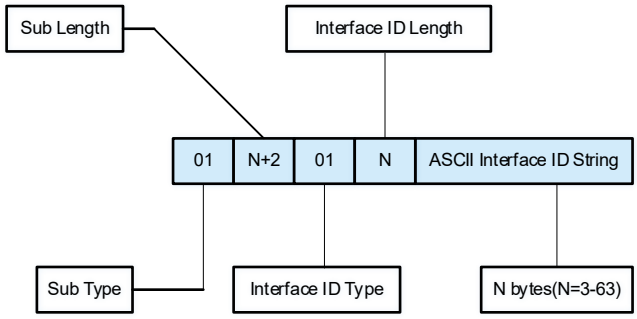
The following figure shows the default padding content in extended padding format.

Figure 1-2Default Padding Content of Interface ID in Extended Padding Format



The following figure shows the extended padding content in extended padding format.

Figure 1-3Extended Padding Content of Interface ID in Extended Padding Format

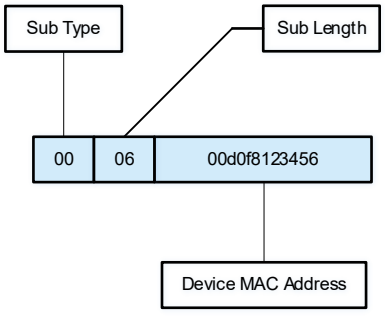


- Option 37: Remote ID

  The default padding content of **Remote ID** is the MAC address of the DHCPv6 relay that receives request packets from DHCPv6 clients, and the extended padding content is a user-defined string.

  Remote ID supports two padding formats: standard padding and extended padding. In a network, only one padding format can be used. In standard padding format, only the default padding content is padded, as shown in the following figure.

Figure 1-4Standard Padding Format of Remote ID

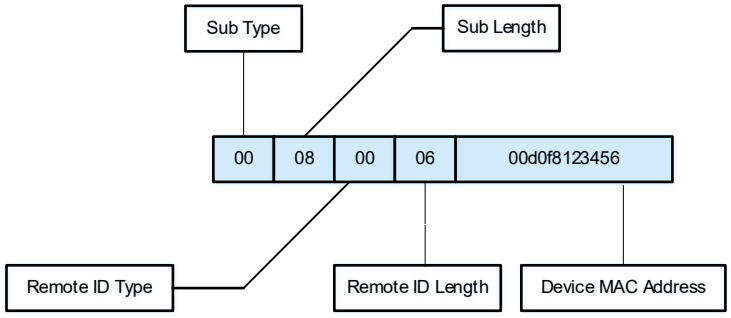


If user-defined padding content is required, use the extended padding format. In extended padding format, the padding content can be the default padding content or extended padding content. To distinguish between different padding content, a 1-byte content type field and a 1-byte content length field are added

after the sub-option length field. For default padding content, the content type is set to **0**. For extended padding content, the content type is set to **1**.

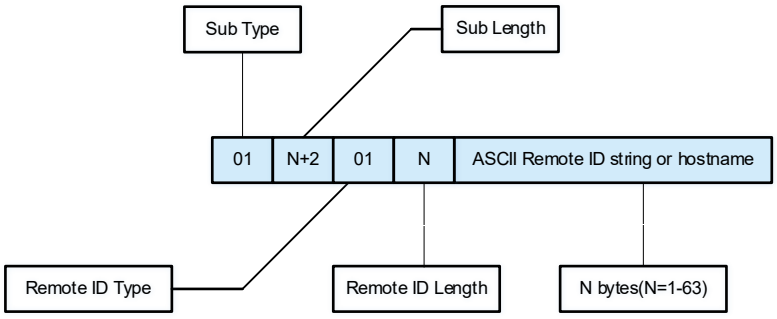
The following figure shows the default padding content in extended padding format.

Figure 1-5Default Padding Content of Remote ID in Extended Padding Format



The following figure shows the extended padding content in extended padding format.

Figure 1-6Extended Padding Content of Remote ID in Extended Padding Format



In **Interface ID** of Option 18, the port index value is the slot ID and port number. The port can be a switching port, L2 AP, or L2 encapsulation sub-interface. The port number indicates the serial number (SN) of a port in a slot. The port number of an L2 AP is the AP number. For example, if the switching port name is Fa0/10, the port number is 10. If the AP name is AP 11, the port number is 11. If the WLAN port name is WLAN 1, the port number is 1.

The slot ID is the SN of a slot on a device (stacked devices are regarded as one). The slot ID of an AP is placed at the end. Slot IDs are numbered starting from 0. You can run the **show slots** command to display slot IDs. For example:

```
Orion_B26Q# show slots
  Dev Slot
  --- ----
  1   0    ------> The slot ID is 0.
  1   1    ------> The slot ID is 1.
  1   2    ------> The slot ID is 2.
```

In this case, the slot ID of the AP is 3.

```
Orion_B26Q# show slots
```

```
Dev Slot
--- ----
1   0    ------> The slot ID is 0.
1   1    ------> The slot ID is 1.
1   2    ------> The slot ID is 2.
2   0    ------> The slot ID is 3.
2   1    ------> The slot ID is 4.
2   2    ------> The slot ID is 5.
```

In this case, the slot ID of the AP is 6.

1.1.3 Applications

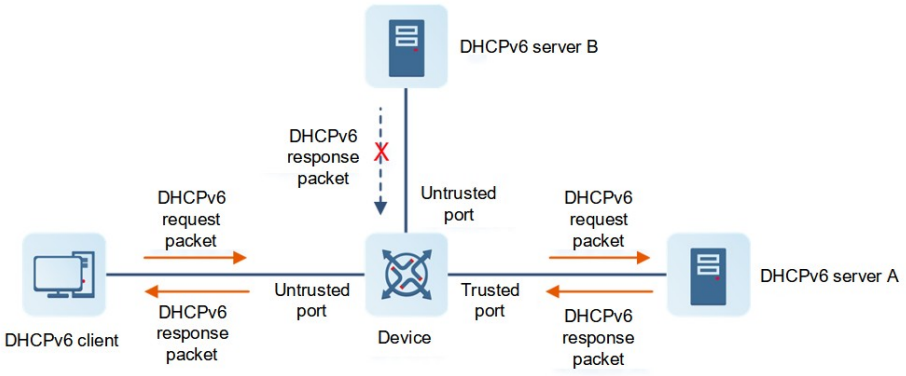
1. Guarding Against DHCPv6 Spoofing

Multiple DHCPv6 servers may exist in a network. It is essential to ensure that user PCs obtain network configurations only from the DHCP servers within a controlled area.

As shown in the following figure, the DHCPv6 client can communicate only with trusted DHCPv6 servers.

- Request packets from the DHCPv6 client are transmitted only to trusted DHCPv6 servers.
- Only response packets from trusted DHCPv6 servers can be transmitted to the DHCPv6 client.

Figure 1-1Guarding Against DHCPv6 Spoofing



Device is an access device, DHCPv6 Server A is in the controlled area, and DHCPv6 Server B is beyond the controlled area.

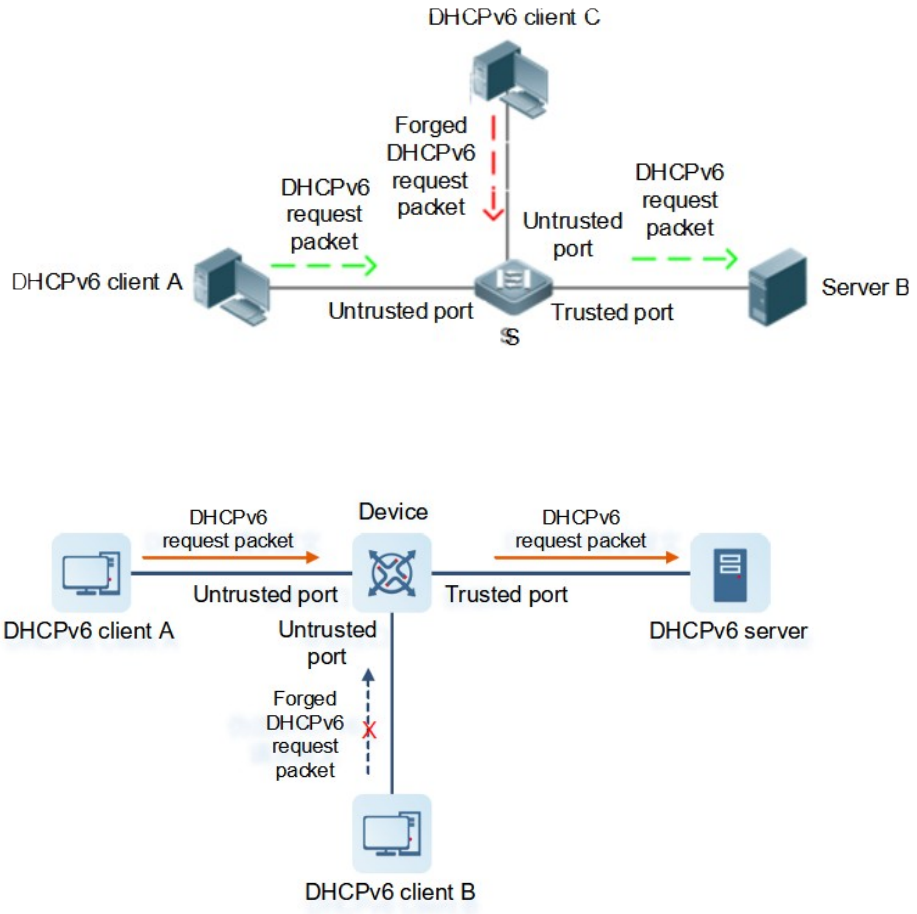
- DHCPv6 Snooping is enabled on Device to monitor DHCPv6 packets.
- The port on Device for connecting to DHCPv6 Server A is configured as a DHCPv6 trusted port to forward response packets.
- The rest ports on Device are configured as DHCPv6 untrusted ports to filter response packets.

2. Guarding Against Forged DHCPv6 Packets

Malicious DHCPv6 clients in a network may forge DHCPv6 request packets, which consumes applicable IPv6 addresses from the servers and probably preempts legitimate users' IPv6 addresses. Therefore, it is necessary to filter out invalid DHCPv6 packets.

As shown in the following figure, request packets sent from a DHCPv6 client are checked. The RELEASE and DECLINE packets from clients must match the entries in the DHCPv6 Snooping binding database.

Figure 1-1Guarding Against Forged DHCPv6 Packets



Device is an access device, and DHCPv6 Server is in the controlled area.

- DHCPv6 Snooping is enabled on Device to monitor DHCPv6 packets.
- The port on Device for connecting to DHCPv6 Server is configured as a DHCPv6 trusted port to forward response packets.
- The rest ports on Device are configured as DHCPv6 untrusted ports to filter DHCPv6 packets.

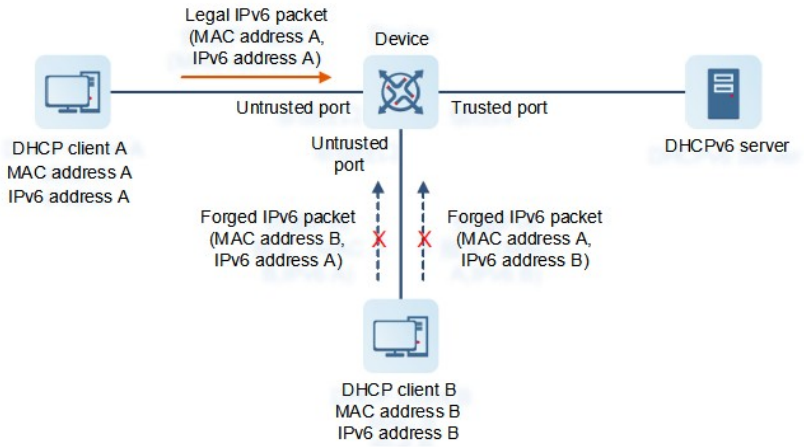
3. Guarding Against IPv6/MAC Address Spoofing

You can check IPv6 packets from untrusted ports based on the IP address field or IP address and MAC address fields to filter out forged IPv6 packets.

As shown in the following figure, IPv6 packets sent from a DHCPv6 client are checked.

- The source address fields in IPv6 packets must match IPv6 addresses assigned by the DHCPv6 server.
- The source MAC address field in L2 packets must match the client MAC address field in DHCPv6 request packets from clients.

Figure 1-1Guarding Against IPv6/MAC Address Spoofing



Device is an access device, and DHCPv6 Server is in the controlled area.

- DHCPv6 Snooping is enabled on Device to monitor DHCPv6 packets.
- The port on Device for connecting to DHCPv6 Server is configured as a DHCPv6 trusted port.
- The rest ports on Device are configured as DHCPv6 untrusted ports.
- IPv6 Source Guard is enabled on Device to filter IPv6 packets.
- The IPv6 Source Guard matching mode is set to IP+MAC on Device to check the MAC address and IPv6 address fields in IPv6 packets.

4. Preventing Private IPv6 Addresses

The device with DHCPv6 Snooping enabled checks whether the source IPv6 addresses in IPv6 packets from untrusted ports are consistent with the addresses assigned by the DHCPv6 server.

If the source IPv6 addresses, connected ports, and L2 source MAC addresses in IPv6 packets do not match the assignments of the DHCPv6 server, such packets are discarded.

The working process of the device in this scenario is the same as that in "Guarding Against IPv6/MAC Address Spoofing."

1.1.4 Protocols and Standards

- RFC 3315: Dynamic Host Configuration Protocol For IPv6
- RFC 5007: DHCPv6 Leasequery
- RFC 5460: DHCPv6 Bulk Leasequery

1.2 Restrictions and Guidelines

- The ports on clients for connecting to trusted DHCPv6 servers must be configured as DHCPv6 trusted ports.
- DHCPv6 Snooping takes effect on switching ports, L2 APs, and L2 encapsulation sub-interfaces.
- The function of clearing entries of linkdown ports takes effect only to wired ports.

1.3 Configuration Task Summary

DHCPv6 Snooping configuration includes the following tasks:

(1) Configuring Basic DHCPv6 Snooping Functions

(2) Configuring Optional DHCPv6 Snooping Functions

(3) (Optional) Configuring Option 18 or 37

1.4 Configuring Basic DHCPv6 Snooping Functions

1.4.1 Overview

Enable basic DHCPv6 Snooping functions to filter out invalid DHCPv6 packets and control the transmission scope of DHCPv6 packets.

1.4.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable DHCPv6 Snooping globally.

ipv6 dhcp snooping

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

(5) Configure an interface as a DHCPv6 Snooping trusted port.

ipv6 dhcp snooping trust

All interfaces are DHCPv6 Snooping untrusted ports by default.

1.5 Configuring Optional DHCPv6 Snooping Functions

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure optional DHCPv6 Snooping functions. Perform at least one of the following configuration steps:

- Disable DHCPv6 Snooping on a VLAN.

  no ipv6 dhcp snooping vlan { *vlan-range* | *vlan-min* [*vlan-max*] }

  After DHCPv6 Snooping is enabled globally, it takes effect to all VLANs by default.

- Write all dynamic user information in the DHCPv6 Snooping binding database to a flash memory at a scheduled time.

  ipv6 dhcp snooping database write-delay *time*

The function of writing all dynamic user information in the DHCPv6 Snooping binding database to a flash memory at a scheduled time is not configured by default.

- Configure an interface to filter all DHCPv6 request packets. Run the following commands in turn.

  interface *interface-type interface-number*

  ipv6 dhcp snooping filter-dhcp-pkt

  No interface is configured to filter all DHCPv6 request packets by default.

1.6 Configuring Option 18 or 37

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Add Option 18 or 37 to DHCPv6 request packets.

ipv6 dhcp snooping information option [**standard-format**]

Option 18 or 37 is not added to DHCPv6 request packets by default.

(4) (Optional) Set **Remote ID** to a user-defined string or the host name when Option 37 is in extended padding mode.

ipv6 dhcp snooping information option format remote-id { **hostname** | **string** *ascii-string* }

When Option 37 is in extended padding mode, **Remote ID** is not set to a user-defined string or host name by default.

(5) Enter the interface configuration mode.

interface *interface-type interface-number*

(6) (Optional) Set **Interface ID** to a user-defined string when Option 18 is in extended padding mode.

ipv6 dhcp snooping vlan *vlan-id* **information option format-type interface-id string** *ascii-string*

Interface ID is not set to a user-defined string by default when Option 18 is in extended padding mode.

(7) (Optional) Change the padded VLAN to a specified VLAN when Option 18 is in extended padding mode.

ipv6 dhcp snooping vlan *vlan-id* **information option change-vlan-to vlan** *vlan-id*

When Option 18 is in extended padding mode, the padded VLAN is not changed to a specified VLAN by default.

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

Table 1-1Monitoring

Command	Purpose
show ipv6 dhcp snooping	Displays DHCPv6 Snooping configurations.
show ipv6 dhcp snooping vlan	Displays VLANs to which DHCPv6 Snooping does not take effect.
show ipv6 dhcp snooping binding [*ipv6-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*]	Displays dynamic user information in the DHCPv6 Snooping binding database.
show ipv6 dhcp snooping prefix [*ipv6-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*]	Displays user information in the DHCPv6 Snooping prefix database.
show ipv6 dhcp snooping statistics	Displays DHCPv6 Snooping packet statistics.
show ipv6 dhcp snooping packet	Displays DHCPv6 Snooping packet statistics on an interface.
clear ipv6 dhcp snooping binding [*ipv6-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*]	Clears dynamic user information in the DHCPv6 Snooping binding database.
clear ipv6 dhcp snooping prefix [*ipv6-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*]	Clears all entries in the DHCPv6 Snooping prefix database.
clear ipv6 dhcp snooping statistics	Clears DHCPv6 Snooping packet statistics.
debug snooping ipv6 event	Debugs DHCPv6 Snooping events.
no debug snooping ipv6 event	Disables debugging of DHCPv6 Snooping events.
debug snooping ipv6 packet	Debugs DHCPv6 Snooping packets.
no debug snooping ipv6 packet	Disables debugging of DHCPv6 Snooping packets.

1.8 Configuration Examples

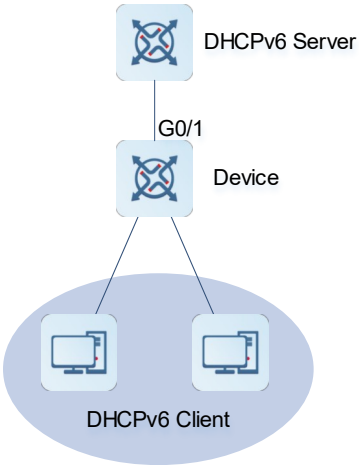
1.8.1 Configuring Basic DHCPv6 Snooping Functions

1. Requirements

DHCPv6 clients can obtain IPv6 addresses from legitimate DHCPv6 servers dynamically.

2. Topology

Figure 1-1Topology of Configuring Basic DHCPv6 Snooping Functions



3. Notes

- Enable DHCPv6 Snooping on Device (an access device).
- Configure the uplink interface GigabitEthernet 0/1 as a trusted port.

4. Procedure

Enable DHCPv6 Snooping on Device.

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

5. Verification

Display DHCPv6 Snooping configurations on Device and check whether the trusted port is correct.

```
Device# show ipv6 dhcp snooping
DHCPv6 snooping status                    : ENABLE
DHCPv6 snooping database write-delay time : 0 seconds
DHCPv6 snooping binding-delay time        : 0 seconds
DHCPv6 snooping option18/37 status        : DISABLE
DHCPv6 snooping link detection            : DISABLE
Interface                  Trusted    Filter DHCPv6
-------------------------  -------    -------------
GigabitEthernet 0/1        YES        DISABLE
```

Display entries generated by Device.

```
Device# show ipv6 dhcp snooping binding
Total number of bindings: 1
```

```
NO.   MAC Address         IPv6 Address                                  Lease(sec)
VLAN  Interface
1     00d0.f801.0101      2001::10                                      42368
2     GigabitEthernet 0/1
```

6. Configuration Files

Device configuration file

```
hostname Device
!
ipv6 dhcp snooping
!
interface GigabitEthernet 0/1
 ipv6 dhcp snooping trust
!
end
```

1.9 Common Misconfigurations

- The uplink interface is not configured as a DHCPv6 Snooping trusted port.
- Another access security option is configured for the uplink interface. As a result, the uplink interface fails to be configured as a DHCPv6 Snooping trusted port.