Contents

1 Configuring DHCP Snooping........1

1.1 Introduction........1

1.1.1 Overview........1

1.1.2 Principles........1

1.1.3 Applications........3

1.1.4 Protocols and Standards........6

1.2 Restrictions and Guidelines........6

1.3 Configuration Task Summary........7

1.4 Configuring Basic DHCP Snooping Functions........7

1.4.1 Overview........7

1.4.2 Procedure........7

1.5 Disabling DHCP Snooping on a VLAN........8

1.6 Enabling Source MAC Address Verification........8

1.6.1 Overview........8

1.6.2 Procedure........8

1.7 Writing Dynamic User Information in the DHCP Snooping Binding Database to the Flash Memory in Real Time........8

1.8 Writing Dynamic User Information in the DHCP Snooping Binding Database to a Flash Memory at a Scheduled Time........9

1.9 Enabling DHCP Snooping to Support BOOTP Binding........9

1.10 Enabling DHCP Snooping to Support Relay Request Packet Processing........9

1.11 Enabling DHCP Snooping to Support Binding Entry Migration........10

1.12 Enabling DHCP Snooping to Fast Age Client Migration Entries..10

1.13 Configuring an Interface in the Suppression State..10

1.14 Configuring the Maximum Number of Users Bound to a VLAN...10

1.15 Configuring Option 82..11

1.15.1 Overview...11

1.15.2 Restrictions and Guidelines...11

1.15.3 Procedure..11

1.16 Enabling DHCP Snooping Monitoring..12

1.16.1 Overview...12

1.16.2 Restrictions and Guidelines...12

1.16.3 Procedure..12

1.17 Monitoring..12

1.18 Configuration Examples..13

1.18.1 Configuring DHCP Snooping...13

1.19 Common Misconfigurations...14

1 Configuring DHCP Snooping

1.1 Introduction

1.1.1 Overview

The Dynamic Host Configuration Protocol (DHCP) snooping function allows a device to snoop DHCP packets exchanged between clients and a server to record and monitor the IP address usage and filter out invalid DHCP packets, including request packets from the clients and response packets from the server. User data entries generated from DHCP Snooping records may serve security applications such as IP Source Guard.

1.1.2 Principles

1. Basic Concepts

- DHCP request packets

  Request packets are sent from a DHCP client to a DHCP server, including DHCP DISCOVER, DHCP REQUEST, DHCP DECLINE, DHCP RELEASE, and DHCP INFORM packets.

- DHCP response packets

  Response packets are sent from a DHCP server to a DHCP client, including DHCP OFFER, DHCP ACK, and DHCP NAK packets.

- VLAN-based DHCP Snooping

  DHCP Snooping is enabled on a per-VLAN basis. When DHCP Snooping is enabled on a device, it is effective to all VLANs of the device by default. You can flexibly configure the VLANs on which DHCP Snooping is enabled.

- DHCP Snooping trusted ports

  Packet for obtaining IP addresses through DHCP are exchanged via broadcast. Rough DHCP services affect clients' normal acquisition of IP addresses and lead to user information spoofing and stealing. DHCP Snooping ports are classified into trusted ports and untrusted ports to prevent rough DHCP services.

  The device only transmits DHCP response packets received on trusted ports and discards those received from untrusted ports. 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 DHCP servers.

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

- DHCP Snooping binding database

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

Combined with Address Resolution Protocol (ARP) detection or ARP check, DHCP Snooping controls the reliable assignment of IP addresses to legitimate clients.

- DHCP Snooping packet suppression

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

- DHCP Snooping rate limit

  DHCP Snooping rate limit can be configured using the rate limit command of Network Foundation Protection Policy (NFPP). For NFPP configuration, see "Configuring NFPP" in the *Security Configuration Guide*.

- DHCP Option 82

  DHCP Option 82, also called the DHCP relay agent information option, is an option in DHCP packets. Option 82 is used to enhance the DHCP server security and optimize the IP address assignment policy. This option is usually configured on the DHCP relay service component, such as DHCP Relay and DHCP Snooping of a network access device. This option is transparent to clients and added or removed by the DHCP relay component.

- Invalid DHCP packets

  The device with DHCP Snooping enabled checks validity of received DHCP packets, discards invalid DHCP packets, and records information about legitimate users to form the DHCP Snooping binding database for query by other applications (for example, ARP detection). The following types of packets are considered as invalid DHCP packets:

  - DHCP response packets received on untrusted ports, including DHCP ACK, DHCP NAK, and DHCP OFFER packets
  - DHCP request packets carrying the **giaddr** field (gateway information) received on untrusted ports
  - Packets with the source MAC addresses different from the value of the **chaddr** field in DHCP packets in a case with MAC address verification enabled
  - DHCP RELEASE packets corresponding to entries in the DHCP Snooping binding database, with the untrusted port on which the packets are received being inconsistent with the untrusted port in the binding table
  - DHCP packets in incorrect formats or incomplete DHCP packets

2. Filtering Invalid DHCP Packets

The device with DHCP Snooping enabled checks validity of DHCP packets from untrusted ports to control the transmission scope of the packets and prevent spoofing.

During snooping, it checks the receiving ports and fields of packets to filter packets, and modifies the destination ports of the packets to control the packet transmission scope.

- Checking ports

  When receiving a DHCP packet, the device first checks whether the port receiving the packet is a DHCP trusted port. If yes, the device directly forwards the packet without checking the validity or generating a binding record. If not, the device checks its validity.

- Checking packet encapsulation and length

The device checks whether received packets are UDP packets, whether the destination port is port 67 or 68, and whether the packet length matches the length field defined in protocols.

- Checking packet fields and types

  According to the invalid DHCP packet types introduced in the “Basic Concepts" section, the device first checks the **giaddr** and **chaddr** fields in packets and then checks whether the restrictive conditions for this packet type are met.

3. Building a DHCP Snooping Binding Database

The device with DHCP Snooping enabled detects packets exchanged between the DHCP clients and the DHCP server and generates entries in the DHCP Snooping binding database based on information about valid DHCP 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 is updated during snooping based on the types of DHCP packets.

- Generating binding entries

  When a DHCP ACK packet is snooped on a trusted port, the device with DHCP Snooping enabled extracts the client's IP address, MAC address, and lease time from the packet and generates a binding entry based on the recorded port ID (interface index) and VLAN ID of the client.

- Deleting binding entries

  A binding entry is deleted in the following scenarios:

  - The recorded lease time expires.
  - A valid DHCP RELEASE or DHCP DECLINE packet sent from the client is snooped.
  - A NAK packet is received from a trusted port.
  - A user runs the **clear** command to delete a binding entry.

1.1.3 Applications

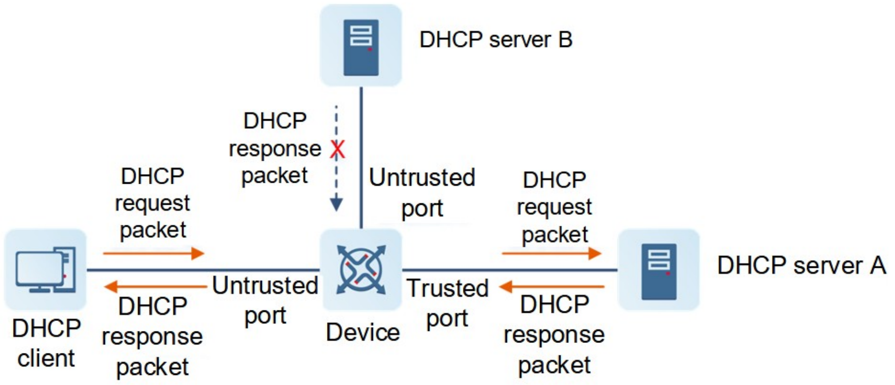
1. Guarding Against DHCP Spoofing

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

As shown in the following figure, the DHCP client can communicate with a trusted DHCP server only.

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

Figure 1-1 Guarding Against DHCP Spoofing



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

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

2. Guarding Against DHCP Packet Flooding

Malicious DHCP clients in a network may send DHCP packets at a high rate. As a result, legitimate users cannot obtain IP addresses, and access devices are heavily loaded or even break down.

- To ensure network stability, the DHCP Snooping rate limit function needs to be enabled for DHCP packets. The request packets from DHCP clients are sent at a rate below the limit. Packets sent at rates beyond the limit are discarded. DHCP Snooping is correlated with the ARP module to delete entries of non-existing users.

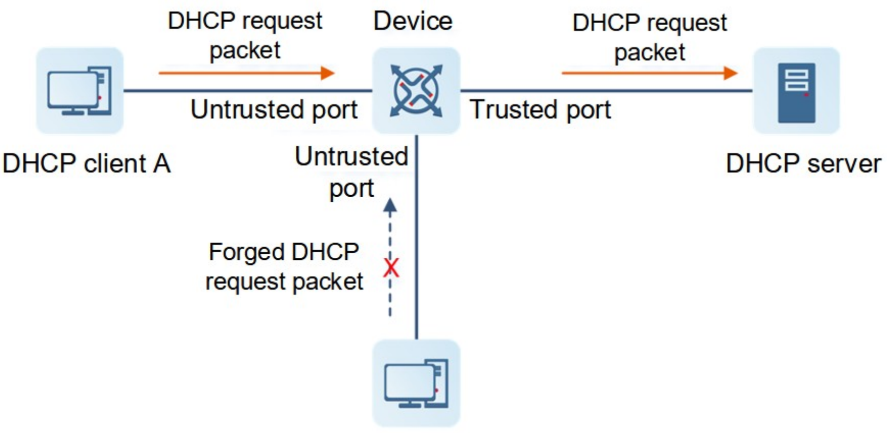
3. Guarding Against Forged DHCP Packets

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

As shown in the following figure, the DHCP request packets sent from DHCP clients are checked.

- The source MAC address field in request packets from DHCP clients must match the client hardware address field of the DHCP packets.
- The RELEASE and DECLINE packets from clients must match the entries in the DHCPv6 Snooping binding database.

Figure 1-1 Guarding Against Forged DHCP Packets



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

- DHCP Snooping is enabled on Device to monitor DHCP packets.
- The port on Device for connecting to DHCP Server is configured as a DHCP trusted port to forward response packets.
- The rest of ports on Device are configured as DHCP untrusted ports to filter response packets.
- DHCP source MAC addresses need to be verified on untrusted ports of Device to filter out invalid DHCP packets.

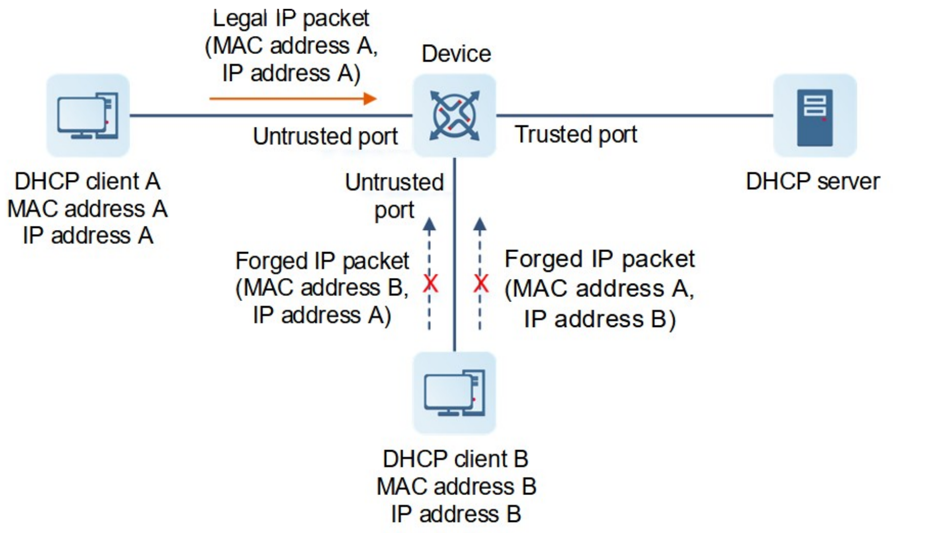
4. Guarding Against IP/MAC Address Spoofing

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

As shown in the following figure, IP packets sent from DHCP clients are checked.

- The source address field in IP packets must match the IP address assigned by the DHCP server.
- The source MAC address field in L2 packets must match the client hardware address field in DHCP request packets from clients.

Figure 1-1 Guarding Against IP/MAC Address Spoofing



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

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

5. Preventing Private IP Addresses

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

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

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

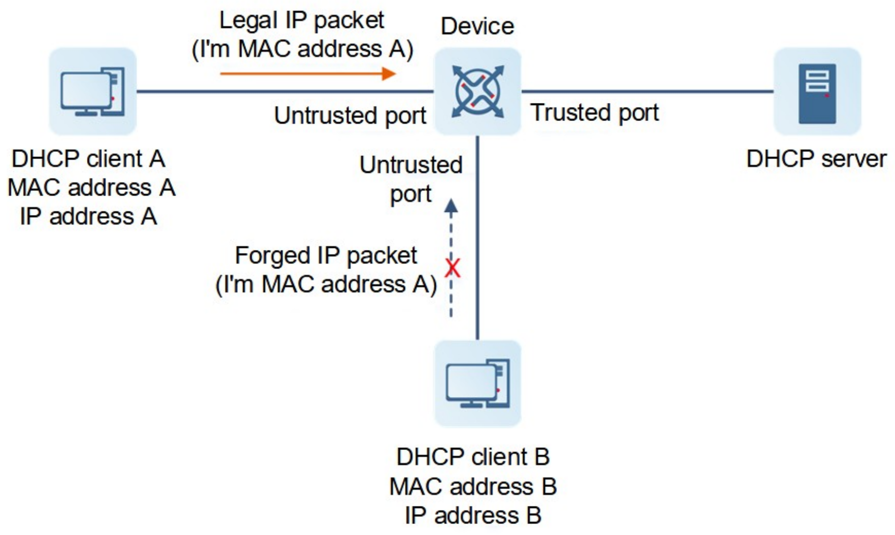
6. Detecting ARP Attacks

The device with DHCP Snooping enabled checks the ARP packets from untrusted ports and filter out the ARP packets unmatched with the assignments of the DHCP server.

As shown in the following figure, ARP packets sent from DHCP clients are checked.

The ports receiving ARP packets, the L2 MAC addresses, and the hardware addresses of ARP packet senders must be consistent with the snooped DHCP packet records.

Figure 1-1 Detecting ARP Attacks



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

- DHCP Snooping is enabled on Device to monitor DHCP packets.
- The port on Device for connecting to DHCP Server is configured as a DHCP trusted port.
- All downlink ports on Device are configured as DHCP untrusted ports.
- IP Source Guard and ARP check are enabled on all untrusted ports on Device to filter ARP packets.

1.1.4 Protocols and Standards

- RFC 2131: Dynamic Host Configuration Protocol
- RFC 2132: DHCP Options and BOOTP Vendor Extensions

1.2 Restrictions and Guidelines

- All security control functions are effective only to DHCP untrusted ports.
- The ports on the device for connecting to trusted DHCP servers must be configured as DHCP trusted ports.
- DHCP Snooping takes effect to switching ports, L2 APs, and L2 encapsulation sub-interfaces.
- DHCP Snooping and DHCP Relay are mutually exclusive in virtual routing and forwarding (VRF) scenarios.

1.3 Configuration Task Summary

DHCP Snooping configuration includes the following tasks:

The following configuration tasks are mutually exclusive. Please configure only one task.

- Configuring DHCP Snooping
  a Configuring Basic DHCP Snooping Functions
  b (Optional) Disabling DHCP Snooping on a VLAN
  c (Optional) Enabling Source MAC Address Verification

d (Optional) Writing Dynamic User Information in the DHCP Snooping Binding Database to the Flash Memory in Real Time

e (Optional) Writing Dynamic User Information in the DHCP Snooping Binding Database to a Flash Memory at a Scheduled Time

f (Optional) Enabling DHCP Snooping to Support BOOTP Binding

g (Optional) Enabling DHCP Snooping to Support Relay Request Packet Processing

h (Optional) Enabling DHCP Snooping to Support Binding Entry Migration

i (Optional) Enabling DHCP Snooping to Fast Age Client Migration Entries

j (Optional) Configuring an Interface in the Suppression State

k (Optional) Configuring the Maximum Number of Users Bound to a VLAN

l (Optional) Configuring Option 82

- Enabling DHCP Snooping Monitoring

1.4 Configuring Basic DHCP Snooping Functions

1.4.1 Overview

This section describes how to enable basic DHCP Snooping functions to filter out invalid DHCP packets and control the transmission scope of DHCP packets.

1.4.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable DHCP Snooping globally.

ip dhcp snooping

DHCP Snooping is disabled globally by default.

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

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

ip dhcp snooping trust

All interfaces are DHCP Snooping untrusted ports by default.

1.5 Disabling DHCP Snooping on a VLAN

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Disable DHCP Snooping on a VLAN.

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

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

1.6 Enabling Source MAC Address Verification

1.6.1 Overview

After source MAC address verification is enabled, the MAC addresses in link layer headers and the **CLIENT MAC** fields in DHCP request packets from untrusted ports are checked for consistence. If the verification fails, packets are discarded.

1.6.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable source MAC address verification.

ip dhcp snooping verify mac-address

Source MAC address verification is disabled by default.

1.7 Writing Dynamic User Information in the DHCP Snooping Binding Database to the Flash Memory in Real Time

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Write dynamic user information in the DHCP Snooping binding database to a flash memory in real time.

ip dhcp snooping database write-to-flash

1.8 Writing Dynamic User Information in the DHCP Snooping Binding Database to a Flash Memory at a Scheduled Time

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Write dynamic user information in the DHCP Snooping binding database to a flash memory at a scheduled time.

ip dhcp snooping database write-delay *time*

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

1.9 Enabling DHCP Snooping to Support BOOTP Binding

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable DHCP Snooping to support Bootstrap Protocol (BOOTP) binding.

ip dhcp snooping bootp-bind

DHCP Snooping does not support BOOTP binding by default.

1.10 Enabling DHCP Snooping to Support Relay Request Packet Processing

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable DHCP Snooping to support relay request packet processing.

ip dhcp snooping check-giaddr

DHCP Snooping does not support relay request packet processing by default.

After this function is enabled, services (IP Source Guard and Dot1x authentication) using DHCP Snooping binding entries generated based on relay requests cannot be deployed. Otherwise, users fail to access the Internet.

After this function is enabled, the **ip dhcp snooping verify mac-address** command cannot be configured. Otherwise, DHCP request packets of the relay are discarded, and users fail to obtain addresses.

1.11 Enabling DHCP Snooping to Support Binding Entry Migration

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable DHCP Snooping to support binding entry migration.

ip dhcp snooping station-move permit

DHCP Snooping does not support binding entry migration by default.

1.12 Enabling DHCP Snooping to Fast Age Client Migration Entries

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable DHCP Snooping to fast age client migration entries.

ip dhcp snooping station-move aging

Fast aging of client migration entries is enabled for DHCP Snooping by default.

1.13 Configuring an Interface in the Suppression State

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure an interface in the suppression state so as to discard all DHCP packets sent to the interface.

ip dhcp snooping suppression

No interface is configured in the suppression state by default.

1.14 Configuring the Maximum Number of Users Bound to a VLAN

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the maximum number of users bound to a VLAN.

ip dhcp snooping vlan *vlan-range* **max-user** *user-number*

The maximum number of users bound to a VLAN is not configured by default.

1.15 Configuring Option 82

1.15.1 Overview

Option 82 includes **Circuit ID** (sub-option 1) and **Remote ID** (sub-option 2). **Circuit ID** identifies the VLAN ID and interface information of a client. **Remote ID** identifies the access device of a client, which is the MAC address of the device generally.

A DHCP server assigns IP addresses based on Option 82 carried in DHCP request packets. Option 82 is transparent to clients.

1.15.2 Restrictions and Guidelines

Option 82 and DHCP Relay are mutually exclusive.

1.15.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Add Option 82 to DHCP request packets.

ip dhcp snooping information option [**standard-format** | **user-defined**]

Option 82 is not added to DHCP request packets by default.

(4) (Optional) Set **Remote ID** to a user-defined string or the host name.

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

Remote ID in Option 82 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) Configure the VLAN in **Circuit ID** as the specified VLAN.

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

When Option 82 is in extended mode, the VLAN in **Circuit ID** is not configured as the specified VLAN by default.

(7) (Optional) Set **the Circuit ID** to user-defined content.

ip dhcp snooping vlan *vlan-id* **information option format-type circuit-id string** *ascii-string*

When Option 82 is in extended mode, **Circuit ID** is not set to user-defined content for forwarding by default.

1.16 Enabling DHCP Snooping Monitoring

1.16.1 Overview

After the DHCP Snooping monitoring function is enabled, DHCP Snooping only copies DHCP packets and generates binding entries based on the interaction status, but does not check the validity of the packets.

1.16.2 Restrictions and Guidelines

The DHCP Snooping monitoring and DHCP Snooping functions are mutually exclusive.

1.16.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable DHCP Snooping monitoring globally.

ip dhcp snooping monitor

DHCP Snooping monitoring is disabled globally by default.

1.17 Monitoring

This section describes the **show** commands used for checking the running status of a configured function to verify the configuration effect,

the **clear** commands used for clearing information,

and the **debug** commands used for outputting 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 1-1 Monitoring

Command	Purpose
show ip dhcp snooping	Displays DHCP Snooping configurations.
show ip dhcp snooping binding	Displays user information in the DHCP Snooping database.
clear ip dhcp snooping binding [*ip-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*]	Clears all dynamic users in the DHCP Snooping database.
debug snooping ipv4 event	Debugs the DHCP Snooping function based on the MAC address.
debug snooping ipv4 mac-address *H.H.H*	Debugs all DHCP Snooping functions.

1.18 Configuration Examples

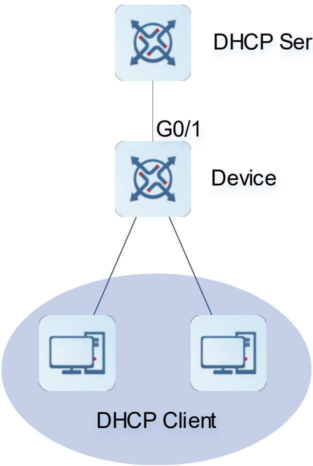
1.18.1 Configuring DHCP Snooping

1. Requirements

DHCP clients can obtain IP addresses from legitimate DHCP servers dynamically.

2. Topology

Figure 1-1 DHCP Snooping Basic Functions



3. Notes

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

4. Procedure

Configure Device (an access device).

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

5. Verification

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

```
Device# show ip dhcp snooping
Switch DHCP snooping status                    :   ENABLE
DHCP snooping verify hardware address status   :   DISABLE
DHCP snooping database write-delay time        :   0 seconds
DHCP snooping option 82 status                 :   DISABLE
DHCP snooping Support bootp bind status        :   DISABLE
Interface                      Trusted       Rate limit (pps)
------------------------       -------       ----------------
GigabitEthernet 0/1            YES           unlimited
```

Display entries generated by Device.

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

```
NO.   MACADDRESS         IPADDRESS       LEASE(SEC)    TYPE           VLAN
INTERFACE
1     0013.2049.9014     172.16.1.2      86207         DHCP-Snooping 1
GigabitEthernet 0/1
```

6. Configuration Files

Device configuration file

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

1.19 Common Misconfigurations

- The uplink interface is not configured as a DHCP 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 DHCP Snooping trusted port.