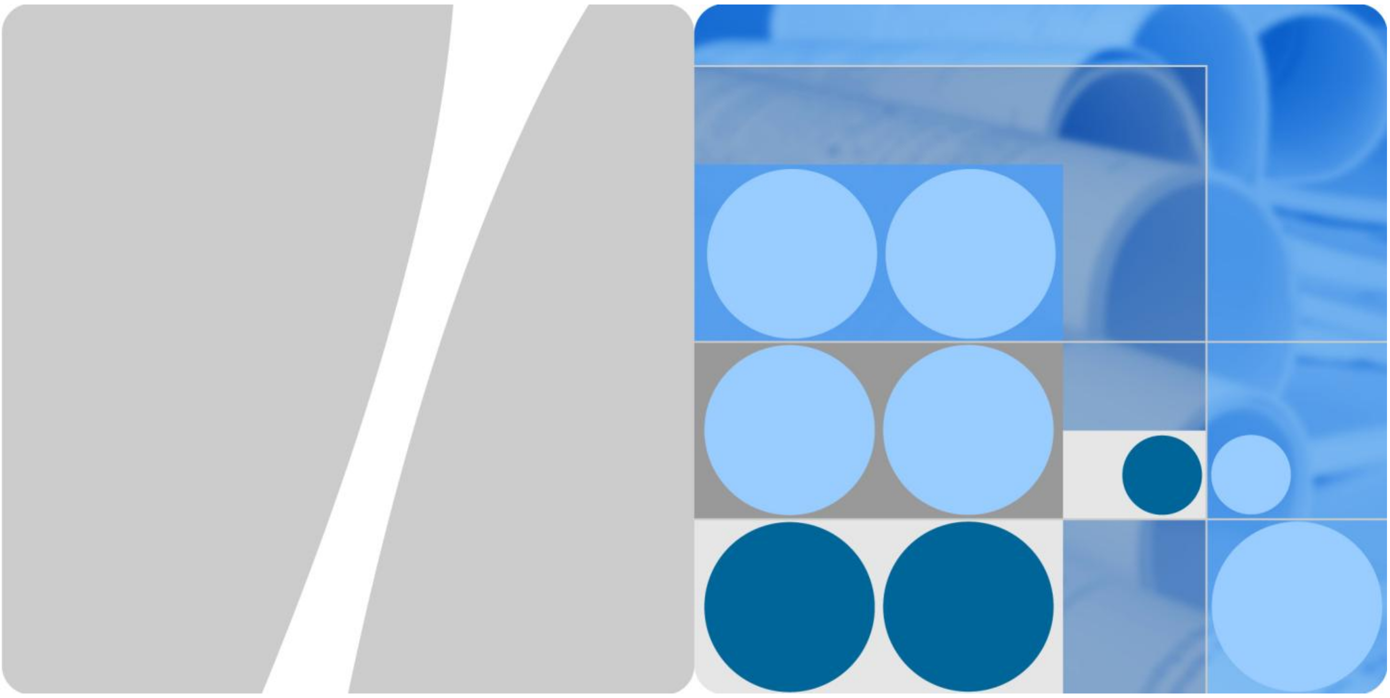


DHCP Snooping Technology White Paper

Issue	**01**
Date	**2012-09-10**

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

1 DHCP Snooping

About This Chapter

1.1 Introduction to DHCP Snooping

Definition

DHCP snooping ensures that DHCP clients obtain IP addresses from authorized DHCP servers and records mappings between IP addresses and MAC addresses of DHCP clients, preventing DHCP attacks on the network.

Purpose

Some attacks are launched on DHCP (RFC2131). These attacks include bogus DHCP server attacks, DHCP server DoS attacks, and bogus DHCP packet attacks.

DHCP snooping acts as a firewall between DHCP clients and a DHCP server to prevent DHCP attacks on the network, ensuring security in communication services.

Benefits

- The device can defend against DHCP attacks on networks. The attack defense capability enhances device reliability and ensures stable network operating.
- Users are provided with more stable services on a more secure network.

1.2 References

For more information about DHCP, see the following documents.

Document No.	Description
RFC 3046	DHCP Relay Agent Information Option
RFC 2132	DHCP Options and BOOTP Vendor Extensions

1.3 Principles

1.3.1 Basic Principles

Trusted Interface

DHCP snooping provides the trusted interface to ensure that the client obtains an IP address from an authorized server.

If a private DHCP server exists on a network, DHCP clients may obtain incorrect IP addresses and network configuration parameters and cannot communicate properly. The trusted interface controls the source of DHCP Reply messages to prevent bogus or unauthorized DHCP servers from assigning IP addresses and other configurations to other hosts.

DHCP snooping supports the trusted interface and untrusted interfaces:

1. Configure the trusted interface.

```
<Quidway> system-view
[Quidway] dhcp snooping enable
[Quidway] interface gigabitethernet 1/0/1
[Quidway-GigabitEthernet1/0/1] dhcp snooping enable
[Quidway-GigabitEthernet1/0/1] dhcp snooping trusted
```

Listening

DHCP snooping also supports the listening function to record mappings between IP addresses and MAC addresses of DHCP clients.

After DHCP snooping is enabled, the device generates a DHCP snooping binding table by listening to DHCP Request messages and Reply messages. A binding entry contains the MAC address, IP address, number of the interface connected to the DHCP client, and VLAN ID.

Enabling Location Transition for a DHCP Snooping User

After the binding table is generated, if the location of an authorized user transits, the corresponding binding entry needs to be updated immediately. After location transition is enabled, the device updates the corresponding binding entry when it detects location transition of a DHCP users, ensuring validity of users.

1. Disable location transition.

```
<Quidway> system-view
[Quidway] dhcp snooping enable
[Quidway] dhcp snooping user-transfer enable
```

Association Between ARP and DHCP Snooping

When a DHCP snooping-enabled device received the DHCP release message sent from a DHCP client, the device deletes the binding entry of the user. However, when a client is abnormally disconnected and cannot send a DHCP Release message, the device cannot immediately delete the binding table of the DHCP client.

After association between ARP and DHCP snooping is enabled, when the ARP entry corresponding to the IP address ages, the DHCP snooping-enabled device detects the IP address by performing ARP probe. If the user is not detected after a specified number of probes, the device deletes the ARP entry. Then, the device detects the IP address by perform ARP probe. If the user still cannot be detected after a specified number of probes, the device deletes the binding entry of the user.

NOTE

The device supports association between ARP and DHCP snooping only when the device functions as a DHCP relay agent.

1. Enable association between ARP and DHCP snooping.

```
<Quidway> system-view
[Quidway] dhcp snooping enable
[Quidway] arp dhcp-snooping-detect enable
```

Clear the MAC Address Entry Immediately When the User Goes Offline

If a user goes offline but its MAC address entry is not aged, the device forwards the message whose destination address is the IP address of the user based on the dynamic MAC address entry. This deteriorates device performance.

The DHCP client sends a DHCP Release message when it goes offline. When the device receives the message, it immediately deletes the DHCP snooping binding entry of the client. You can enable the device to delete the corresponding MAC address entry when the dynamic DHCP snooping binding entry is deleted.

1. Enable the device to delete the MAC address entry of a user when the dynamic binding entry is deleted.

```
<Quidway> system-view
[Quidway] dhcp snooping enable
[Quidway] dhcp snooping user-offline remove mac-address
```

Discard DHCP Request Messages with Non-0 GIADDR Field

The GIADDR field in a DHCP Request message records the IP address of the first DHCP relay agent that the DHCP Request message passes through. If the DHCP server and client are on different network segments, the first DHCP relay agent fills its own IP address in the GIADDR field before forwarding the DHCP Request message from the client to the server. The DHCP server then locates the client and selects an appropriate address pool to assign an IP address to the client.

To ensure that the device obtains parameters such as MAC addresses for generating a binding table, DHCP snooping needs to be applied to Layer 2 access devices or the first DHCP relay agent. Therefore, the GIADDR field in the DHCP Request messages received by the DHCP snooping-enabled device is 0. If the GIADDR field is not 0, the message is unauthorized and then discarded.

1. Enable the device to check whether the GIADDR field in a DHCP Request message is 0 in VLAN 10.

```
<Quidway> system-view
[Quidway] dhcp snooping enable
[Quidway] vlan 10
[Quidway-vlan10] dhcp snooping enable
[Quidway-vlan10] dhcp snooping check dhcp-giaddr enable
```

1.3.2 DHCP Snooping Attack Defense

After basic functions are configured, DHCP clients can obtain IP addresses from authorized DHCP server, preventing bogus DHCP server attacks on the network. However, many other DHCP attacks exist on the network. The administrator can configure DHCP snooping attack defense on the device as required.

Detection Of Bogus DHCP Servers

After DHCP snooping is enabled and the interface is configured as the trusted interface, the device enables DHCP clients to obtain IP addresses from authorized DHCP server, preventing bogus DHCP server attacks. However, the location of the bogus DHCP server cannot be detected, so hidden troubles exist.

After detection of bogus DHCP servers is enabled, the DHCP snooping-enabled device checks and records information about the DHCP server, such as the IP address and port number, in the DHCP Reply messages in the log. The network administrator identifies whether bogus DHCP servers exist on the network based on logs.

1. Enable detection of bogus DHCP servers.

```
<Quidway> system-view
[Quidway] dhcp snooping enable
[Quidway] dhcp server detect
```

Defense Against Attacks from Non-DHCP Users

On a DHCP network, users with static IP addresses may initiate attacks such as bogus DHCP server attacks and bogus DHCP Request message attacks. This brings potential security risks for authorized DHCP users.

Dynamic MAC address entries are learned and generated by the device, and static MAC address entries are configured by command lines. A MAC address entry includes the MAC address, VLAN ID, and number of the interface connected to a DHCP client. The device implements Layer 2 forwarding based on MAC address entries.

After a static MAC address entry is enabled on the interface, the device generates static MAC address entries based on dynamic DHCP snooping binding entries for all DHCP users on the interface, clears all the dynamic MAC address entries on the interface, disables the interface to learn dynamic MAC address entries, and enables the interface to match the source MAC address based on the MAC address entries. Then only the message with the source MAC address matching the static MAC address entry can pass through the interface; otherwise, messages are discarded. Therefore, the administrator needs to manually configure static MAC address entries for non-DHCP users on the interface so that messages sent from non-DHCP users can pass through; otherwise, DHCP messages are discarded. This prevents attacks from non-DHCP users.

1. Enable the device to generate static MAC address entries based on DHCP snooping binding entries on GE1/0/1.

```
<Quidway> system-view
[Quidway] dhcp snooping enable
[Quidway] interface gigabitethernet 1/0/1
[Quidway-GigabitEthernet1/0/1] dhcp snooping enable
[Quidway-GigabitEthernet1/0/1] dhcp snooping sticky-mac
```

Defense Against DHCP Flood Attacks

On a DHCP network, if an attacker sends a large number of DHCP messages to the device within a short time, the performance of the device may be affected and the device may not work normally. To prevent DHCP Flood attacks, you can enable the device to check the rate of sending DHCP messages to the processing unit.

1. In the system view, set the maximum rate of sending DHCP messages to the processing unit to 50 pps.

```
<Quidway> system-view
[Quidway] dhcp snooping enable
[Quidway] dhcp snooping check dhcp-rate enable
[Quidway] dhcp snooping check dhcp-rate 50
```

Defense Against Bogus DHCP Message Attacks

If an attacker sends a bogus DHCP Request message to the DHCP server, the IP address cannot be release after the lease expires and then authorized users cannot use the IP address. If the attacker sends a bogus DHCP Release message to the DHCP server, the user may go offline abnormally.

When a binding table is generated, the device checks whether the DHCP Request message or Release message matches entries in the binding table. Only DHCP messages that match entries can be forwarded. This prevents unauthorized users from sending bogus DHCP Request messages or Release messages to extend or release IP addresses.

1. Enable the device to check DHCP messages against the DHCP snooping binding table.

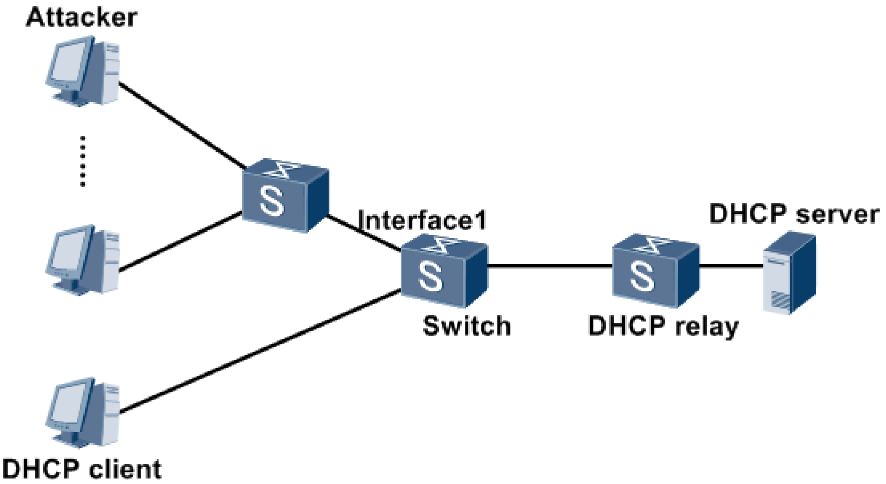
```
<Quidway> system-view
[Quidway] dhcp snooping enable
[Quidway] vlan 10
[Quidway-vlan10] dhcp snooping enable
[Quidway-vlan10] dhcp snooping check dhcp-request enable
```

Defense Against DHCP Server DoS Attacks

As shown in Figure 1-1, if a large number of malicious attackers request IP addresses on interface1, IP addresses in the IP address pool are exhausted so that the DHCP server cannot assign IP addresses to authorized clients.

A DHCP server identifies the MAC address of a client based on the CHADDR field in a DHCP Request message. If an attacker continuously applies for IP addresses by changing the CHADDR field, addresses in the address pool on the DHCP server may be exhausted. As a result, authorized users cannot obtain IP addresses.

Figure 1-1 Networking diagram of defense against DHCP server DoS attacks



To prevent the attack, you can set the maximum number of access users allowed on the device or an interface after DHCP snooping is enabled on the device. When the number of users reaches the maximum value, no user can obtain an IP address through the device or interface.

You can enable the device to check whether the MAC address in the Ethernet frame header matches the CHADDR field in the DHCP message. If the two values match, the message is forwarded; otherwise, the message is discarded.

1. Configure defense against DHCP server DoS attacks.
   - Set the maximum number of DHCP users to 200 on GE1/0/1.

```
<Quidway> system-view
[Quidway] dhcp snooping enable
[Quidway] gigabitethernet 1/0/1
[Quidway-GigabitEthernet1/0/1] dhcp snooping enable
[Quidway-GigabitEthernet1/0/1] dhcp snooping max-user-number 200
```

   - Enable the device to check whether the CHADDR field in the DHCP message matches the source MAC address on GE1/0/1

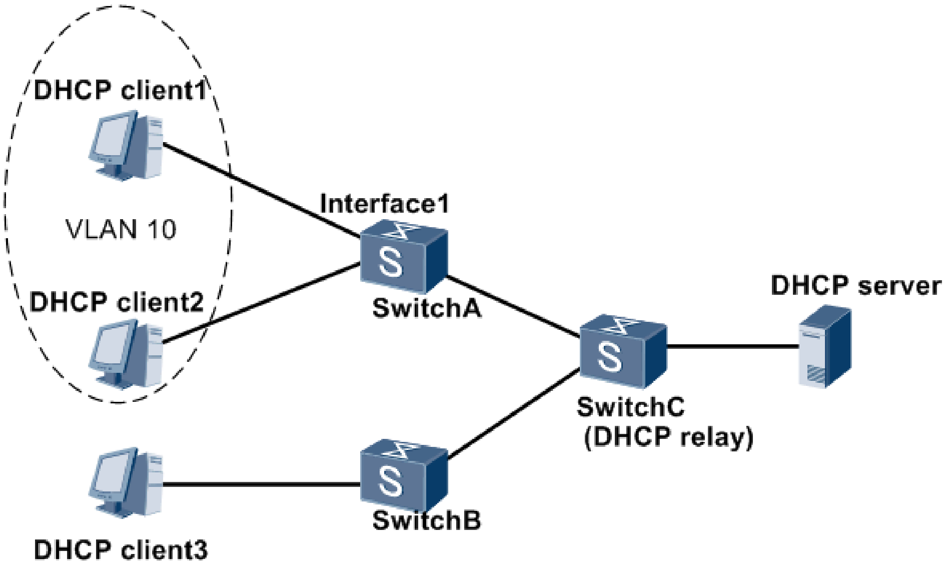
```
<Quidway> system-view
[Quidway] dhcp snooping enable
[Quidway] gigabitethernet 1/0/1
[Quidway-GigabitEthernet1/0/1] dhcp snooping enable
[Quidway-GigabitEthernet1/0/1] dhcp snooping check dhcp-chaddr enable
```

1.3.3 Option 82 Supported by DHCP Snooping

Overview

The DHCP Relay Agent Information Option (Option 82) field records the location of a DHCP client. A DHCP snooping-enabled device or a DHCP relay agent inserts the Option 82 field to a DHCP Request message to notify the DHCP server of the DHCP client location. The DHCP server can assign an IP address and other configurations to the DHCP client, ensuring DHCP client security.

Figure 1-2 Networking diagram of the Option 82 field



As shown in Figure 1-2, the clients obtain IP addresses using DHCP. The administrator configures the device to control clients on **interface1** to access network resources to improve network security.

The DHCP server cannot detect the DHCP client location based on the DHCP Request message. As a result, users in the same VLAN have the same right to access network resources.

To address this problem, the administrator can enable the Option 82 field after DHCP snooping is enabled on SwitchA. Then SwitchA receives DHCP Request messages to request IP addresses and insert the Option 82 field in the messages to notify the server of the client location, including the MAC address, VLAN ID, and number of the interface connected to the client. The DHCP server can assign an IP address and other configurations to the client based on the Option 82 field and the IP address assignment or security policies on the server.

The Option 82 field contains two sub-options: circuit ID and remote ID. The circuit ID identifies VLAN ID and interface number of a client, and the remote ID identifies the MAC address connected to the client. The DHCP server can assign an IP address and other configurations to the client based on the Option 82 field and the IP address assignment or security policies on the server.

Implementation

As a DHCP relay agent or an access device on the Layer 2 network, the device supports the Option 82 field when DHCPv4 snooping is enabled. The device inserts the Option 82 field to a DHCP message in two modes:

- Insert mode: When the device receives a DHCP Request message without the Option 82 field, the device inserts the Option 82 field. When the device receives a DHCP Request message with the Option 82 field, the device checks whether the Option 82 field contains the remote ID. If the remote ID is in the Option 82 field, the device retains the Option 82 field; otherwise, the device inserts the remote ID.
- Rebuild mode: When the device receives a DHCP Request message without the Option 82 field, the device inserts the Option 82 field. When the device receives a DHCP Request message with the Option 82 field, the device deletes the original Option 82 field and inserts the new Option 82 field set by the administrator.

When the device receives a DHCP Reply message from the DHCP server with the Option 82 field, the device deletes the field and forwards the message to a DHCP client; otherwise, the device forwards the message to a DHCP client directly.

1. Enable the device to insert the Option 82 field to DHCP messages on GE1/0/1.

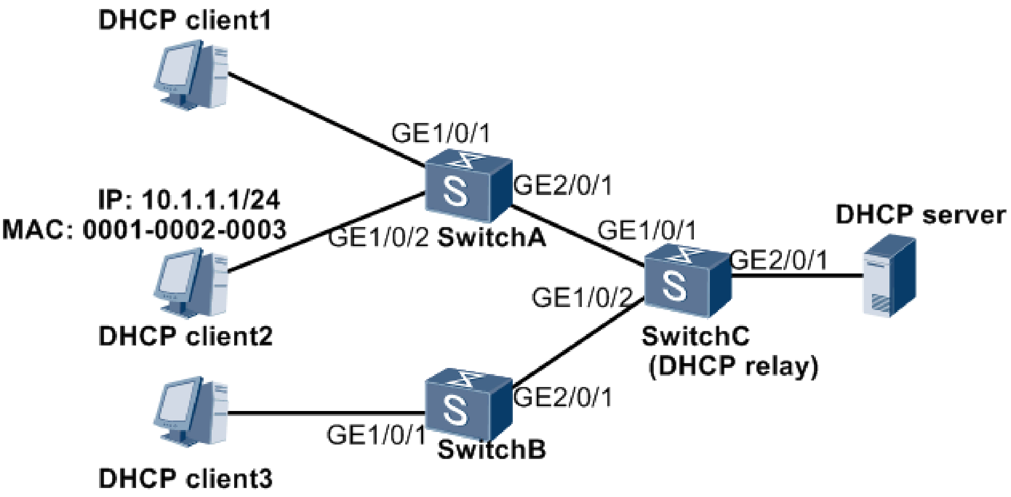
```
<Quidway> system-view
[Quidway] dhcp snooping enable
[Quidway] interface gigabitethernet 1/0/1
[Quidway-GigabitEthernet1/0/1] dhcp snooping enable
[Quidway-GigabitEthernet1/0/1] dhcp option82 insert enable
```

1.4 Application

1.4.1 Example for Configuring DHCP Snooping Attack Defense

As shown in Figure 1-3, SwitchA and SwitchB are access devices, and SwitchC is a DHCP relay agent. Client1 and Client 2 are connected to SwitchA through GE1/0/1 and GE1/0/2 respectively. Client 3 is connected to SwitchB through GE1/0/1. Client1 and Client 3 obtain IPv4 addresses using DHCP, while Client2 uses the static IPv4 address. Attacks from unauthorized users prevent authorized users from obtaining IP address. The administrator expects to enable the device to defend against DHCP attacks on the network and provide better services to DHCP users.

Figure 1-3 Networking diagram of configuring DHCP snooping attack defense



# Configuration files

```
#
sysname SwitchC
#
dhcp enable
#
```

```
dhcp snooping enable ipv4
dhcp snooping check dhcp-rate enable
dhcp snooping check dhcp-rate 90
dhcp snooping alarm dhcp-rate enable
dhcp snooping alarm dhcp-rate threshold 80
arp dhcp-snooping-detect enable
user-bind static ip-address 10.1.1.1 mac-address 0001-0002-0003 interface
gigabitethernet1/0/1
#
interface GigabitEthernet1/0/1
 dhcp snooping sticky-mac
 dhcp snooping enable
 dhcp snooping check dhcp-giaddr enable
 dhcp snooping check dhcp-request enable
 dhcp snooping alarm dhcp-request enable
 dhcp snooping alarm dhcp-request threshold 120
 dhcp snooping check dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr threshold 120
 dhcp snooping alarm dhcp-reply enable
 dhcp snooping alarm dhcp-reply threshold 120
 dhcp snooping max-user-number 20
#
interface GigabitEthernet1/0/2
 dhcp snooping sticky-mac
 dhcp snooping enable
 dhcp snooping check dhcp-request enable
 dhcp snooping alarm dhcp-request enable
 dhcp snooping alarm dhcp-request threshold 120
 dhcp snooping check dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr threshold 120
 dhcp snooping alarm dhcp-reply enable
 dhcp snooping alarm dhcp-reply threshold 120
 dhcp snooping max-user-number 20
#
interface GigabitEthernet2/0/1
 dhcp snooping trusted
#
return
```