Contents

1 Configuring DHCP

1.1 Introduction

1. **Overview**

Dynamic Host Configuration Protocol (DHCP) is a local area network (LAN) protocol that dynamically assigns reusable network addresses and additional configurations to hosts. DHCP uses User Datagram Protocol (UDP) as its transport protocol to send and receive DHCP messages through port 67.

DHCP works in client/server mode. A DHCP client sends a request message to a DHCP server for an IP address and other configurations. When a DHCP client and a DHCP server are not in the same subnet, they need a DHCP relay agent to forward DHCP request and reply messages.

2. **Origin and Development**

DHCP originates from the Bootstrap Protocol (BOOTP), which is used by diskless hosts to obtain their own IP addresses, server IP address, boot image file name, gateway IP address, and other information from a server. BOOTP is designed for static environments. It requires the hardware address of a host be manually added to the BOOTP table and mappings between hardware addresses and IP addresses be static. In other words, BOOTP is less dynamic. In an environment with limited IP addresses, one-to-one mapping of BOOTP wastes IP addresses.

As the network scale expands and network complexity increases, BOOTP designed for static hosts can no longer meet requirements in wireless network scenarios and scenarios in which the number of computers exceeds the number of available IP addresses.

Therefore, the Internet Engineering Task Force (IETF) proposes a new protocol, that is, DHCP. DHCP is an enhanced version of BOOTP and consists of a server and a client. A DHCP server centrally manages all IP network settings and processes DHCP requests from DHCP clients. DHCP clients use the IP environment data assigned by the DHCP server. Compared with BOOTP, DHCP employs the lease concept to allocate clients' TCP/IP settings effectively and dynamically. DHCP also meets compatibility requirements of BOOTP clients.

3. **Benefits**

During network construction, a DHCP server can bring the following benefits:

- Low network access cost: Generally, the network access cost in static address assignment mode is higher than that in dynamic address assignment mode.
- Simplified configuration and low network construction cost: Dynamic address assignment significantly simplifies device configuration and reduces the deployment cost if no professional technical personnel are available to deploy devices.
- Centralized management: You can modify configurations for multiple subnets by simply modifying the DHCP server configuration.

1.2 Principles

1.2.1 Basic Concepts

- DHCP server

  A DHCP server is implemented based on RFC 2131. It assigns IP addresses to hosts and manages these IP addresses.

- DHCP client

  A DHCP client enables a device to automatically obtain an IP address and other configurations from a DHCP server.

- DHCP relay

  When a DHCP client and a DHCP server are not in the same subnet, they need a DHCP relay agent to forward DHCP request and reply messages.

- Lease time

  Lease time is a period of time specified by a DHCP server for a client to use an assigned IP address. An IP address can be leased to a client when a lease time is active. Before a lease expires, a client needs to renew the lease through a server. When a lease expires or is deleted from a server, the lease time becomes inactive.

- Address pool

  An address pool is a collection of IP addresses that a DHCP server can assign to clients.

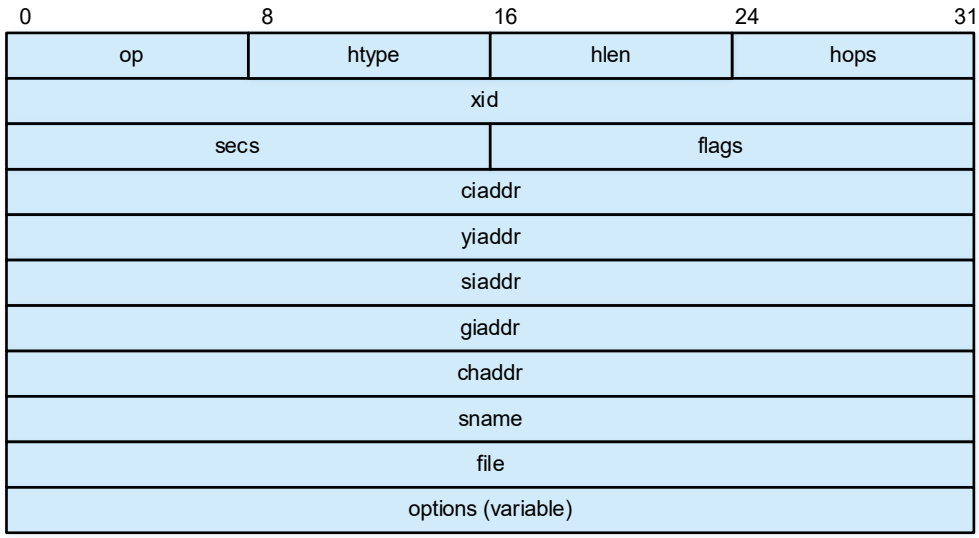
- Option type

  An option type is a parameter specified by a DHCP server when it provides the lease service to a DHCP client. For example, common options include the IP addresses of the default gateway (router), Windows Internet Name Service (WINS) server, and Domain Name System (DNS) server. A DHCP server also allows configuration of other options. Most options are predefined in RFC 2132. You can add user-defined options.

1.2.2 Message Format

1. **DHCP Packet**

Figure 1-1DHCP Packet



The following describes fields contained in a DHCP packet:

- **op**: Packet type, including request packets and reply packets. A packet with **op** set to **1** is a request, and a packet with **op** set to **2** is a reply. The specific packet type is identified by the **options** field.
- **htype** (hardware type): Hardware address type of a DHCP client. For Ethernet clients, the field value is **1**.
- **hlen** (hardware length): Length of the hardware address of a DHCP client. For Ethernet clients, the field value is **6**.
- **hops**: Number of DHCP relay agents that a DHCP packet passes through. The field value increments by 1 each time a DHCP request packet passes through one DHCP relay agent.
- **xid**: Random number selected by a DHCP client when it sends a request. It is used to identify an address requesting process.
- **secs**: Time (in seconds) elapsed since a DHCP client starts a DHCP request.
- **flags**: The first bit is the broadcast reply flag bit and is used to identify whether a DHCP server sends a reply packet in unicast or broadcast mode. **0** indicates unicast, and **1** indicates broadcast. The other 15 bits are set to **0**.
- **ciaddr** (client IP address): IP address of a DHCP client. If a client has a valid and available IP address, add it to this field. During initialization, the client does not have an IP address, and this field is set to **0.0.0.0**. This field is not used to apply for a specific IP address by the client.
- **yiaddr** (your client IP address): IP address assigned by a DHCP server to a DHCP client.
- **siaddr** (server IP address): IP address of the server from which a DHCP client obtains boot configurations.
- **giaddr** (gateway IP address): IP address of the first DHCP relay agent that a request packet of a DHCP client passes through.
- **chaddr** (client hardware address): Hardware address of a DHCP client.

- **sname** (server name): Name of the server from which a DHCP client obtains boot configurations.
- **file**: Boot configuration file name and path specified by a DHCP server for a DHCP client.
- **options**: Optional fields with variable length, including the packet type, valid lease time, IP address of the DNS server, and IP address of the WINS server.

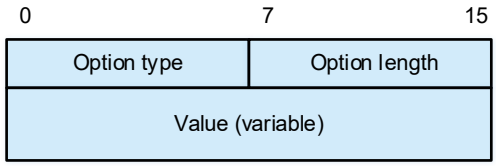
2. Message Types

- DHCP DISCOVER: first message broadcast by a DHCP client for DHCP interaction when it accesses a network for the first time.
- DHCP OFFER: message sent by a DHCP server in response to the DHCP DISCOVER message. The message carries various configuration parameters.
- DHCP REQUEST: This message has the following functions:
  - After a client is initialized, it broadcasts a DHCP REQUEST message to respond to the DHCP OFFER message of a DHCP server.
  - After a client is restarted and initialized, it broadcasts a DHCP REQUEST message to confirm the previously assigned IP address and other configurations.
  - After a client is bound to an IP address, it sends a DHCP REQUEST message to update the IP address lease.
- DHCP ACK: acknowledgment message of a server in response to a client's DHCP REQUEST message. A client obtains an IP address and related configuration parameters only after receiving this message.

3. Option Format

A DHCP server uses the **Options** field to transfer control information and network configuration parameters to dynamically assign IP addresses and provide rich network configurations to clients. The **Options** field consist of the type, length, and value parts. Figure 1-1 shows the format.

Figure 1-1 Option Format



- **Option type**: option number.
- **Option length**: length of the information content.
- **Value**: information content.

4. Common DHCP Options

The type value of the **Options** field ranges from 1 to 255. Common DHCP options include:

- Option 1: subnet mask.
- Option 3: gateway address.
- Option 6: DNS address.
- Option 15: domain name.
- Option 33: static route. This option contains a group of classified static routes (that is, the mask of the

destination network address is a natural mask and cannot be used for subnet division). After a client receives this option, it adds these static routes to the routing table. If Option 33 and Option 121 coexist, Option 33 is ignored.

- Option 51: IP address lease time.
- Option 53: DHCP message type.
- Option 55: parameter request list. A client uses this option to specify the network configurations that need to be obtained from a server. The option content is the values of parameters requested by a client.
- Option 121: classless static route. This option contains a group of classless static routes (that is, the mask of the destination network address is any value and subnets can be divided by mask). After a client receives this option, it adds these static routes to the routing table. If Option 33 and Option 121 coexist, Option 33 is ignored.

For details about more DHCP options, see RFC 2132 and RFC 3442.

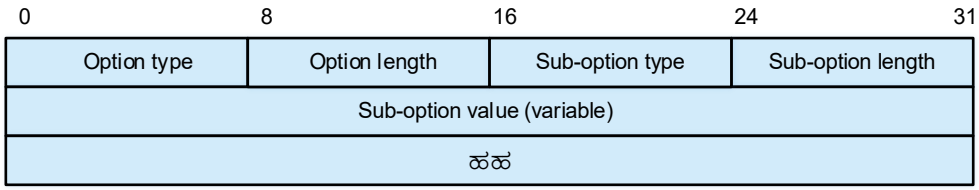
5. User-Defined DHCP Options

- Option 43: specific vendor information

  A DHCP server uses Option 43 to assign specific vendor information to a client. Option 43 uses several sub-options to assign different network configurations to users. The sub-option fields are as follows:

  - **Sub-option type**: type of a sub-option. The value can be **0x01** (ACS parameter), **0x02** (service provider identifier), or **0x80** (PXE boot server address).
  - **Sub-option length**: length of a sub-option.
  - **Sub-option value**: value of a sub-option.

Figure 1-1Option 43

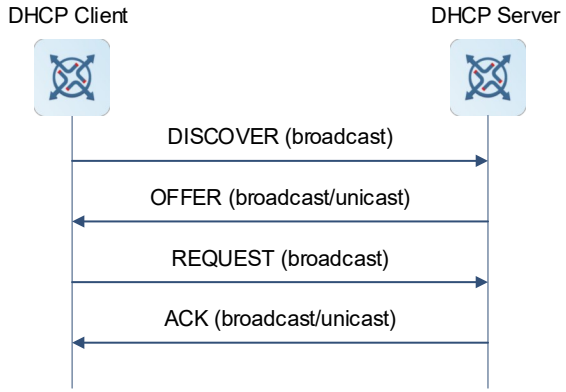


- Option 82: relay agent information

  Option 82 records the location information of a DHCP client. When a DHCP relay agent receives a request packet destined for a DHCP server from a DHCP client, the DHCP relay agent adds Option 82 to the packet and forwards the packet to the DHCP server. An administrator obtains the DHCP client location information from Option 82 to locate the DHCP client, assign an address in a specific range to the client, and control the client security and accounting.

1.2.3 DHCP Lease Process

Figure 1-1DHCP Lease Process



A DHCP client requests an IP address as follows:

(1) The DHCP client broadcasts a DHCP DISCOVER packet to find a DHCP server in the network.

(2) The DHCP server sends a DHCP OFFER packet to the client in unicast/broadcast mode based on the broadcast bit in the **flags** field of the DISCOVER packet, with the packet containing an IP address, a Media Access Control (MAC) address, a domain name, and a lease time.

(3) The DHCP client broadcasts a DHCP REQUEST packet to formally request an IP address from the DHCP server.

(4) The DHCP server searches for the corresponding lease record based on the MAC address carried in the DHCP REQUEST packet.

- If the lease record exists, the DHCP server sends a DHCP ACK packet to the DHCP client. After receiving the DHCP ACK packet, the DHCP client sends a free Address Resolution Protocol (ARP) packet to check whether another host uses the IP address assigned by the DHCP server. If the DHCP client does not receive a response within the specified time, the DHCP client uses the assigned IP address. If the DHCP client finds IP address conflict, it sends a DHCP DECLINE message to notify the server and requests another IP address from the server after 10s.
- If the lease record does not exist or the DHCP server cannot assign an IP address to the client due to some reasons, the DHCP server sends a DHCP NAK packet to inform the DHCP client that no proper IP address can be assigned. The DHCP client needs to send another DHCP DISCOVER packet to apply for a new IP address.

Note

- The DHCP client may receive DHCP OFFER packets from multiple DHCP servers, but usually it accepts only the first DHCP OFFER packet.
- In addition, the address specified in the DHCP OFFER packet is not necessarily assigned to the client. Generally, the DHCP server reserves this address until the client sends a DHCP REQUEST packet.
- A client broadcasts a DHCP REQUEST packet to inform all DHCP servers that respond with DHCP OFFER packets. The servers not selected by the DHCP REQUEST message will release the previously assigned IP address.

1.2.4 DHCP Server

1. **Address Pool**

After a DHCP server receives a client's request, it chooses a valid address pool, determines an available IP address from the pool by using the ping mechanism, and delivers the pool configurations and IP address to the client. In addition, the server saves the lease information locally for validity check upon lease renewal.

Address pool configurations include the IP address range, gateway address, DNS address, and lease time.

2. **Address Management Method and Assignment Policy**

A DHCP server selects an IP address for a client based on the following sequence:

(1) The DHCP server selects an IP address statically bound to the MAC address of the client from its own database.

(2) The DHCP server selects an IP address previously used by the client, that is, the address specified in the IP address option of the DHCP DISCOVER packet sent by the client.

(3) The DHCP server selects an available IP address first found from the DHCP address pool.

(4) If no available IP address is found from the DHCP address pool, the DHCP server checks whether an expired or conflicted IP address exists. If yes, it assigns an available IP address to the client. If not, it reports an error.

3. **ARP Entry Check**

The ARP entry check function can be used together with the ping mechanism to detect IP address conflicts. If a firewall is enabled on hosts in an actual environment, the ping operation for address conflict detection of a DHCP server becomes invalid. DHCP clients that dynamically apply for IP addresses may be assigned with the same IP address. Address conflict may occur. If the ARP entry check function is enabled, the DHCP server queries the ARP entries after detecting an IP address conflict by using the ping operation. If an ARP entry exists for the IP address to be assigned and is inconsistent with the MAC address of the client to which the IP address is assigned, the DHCP server regards that the IP address is occupied by another user.

You are not advised to enable the ARP entry check function in an environment with ARP attacks. Otherwise, the IP address assignment is affected, resulting in slow or failed IP address assignment.

4. **Compulsory NAK Reply**

In wireless applications, DHCP clients usually move from one network to another. When receiving a REQUEST packet from a client for lease renewal, a DHCP server replies with a NAK packet for the client if the server finds that the network segment of the client is changed or the lease expires. Such practice avoids the DHCP client from repeatedly sending REQUEST packets and avoids the DHCP client from obtaining an IP address only after the REQUEST packet times out.

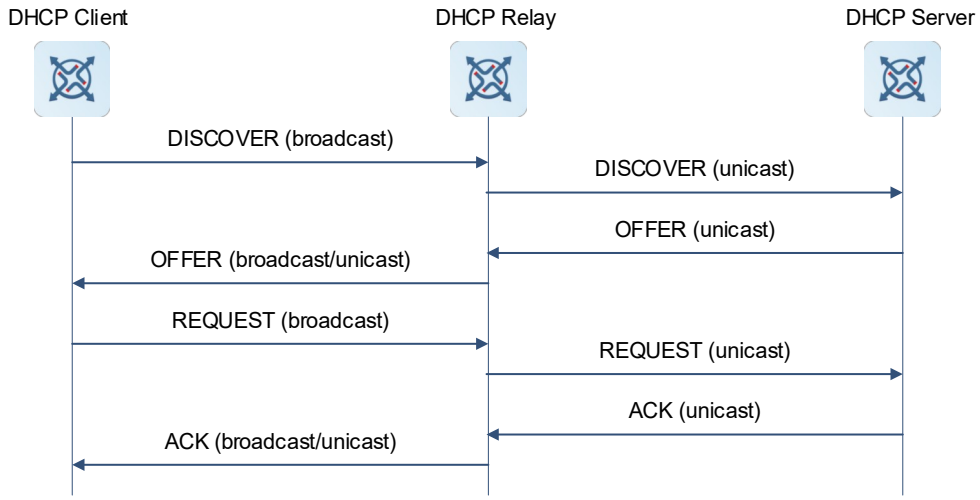
However, the DHCP server can send NAK packets only to its managed DHCP clients because it has lease records of its managed clients only. When a DHCP client moves from another network to the local network, if the DHCP server cannot find the corresponding lease record locally, the DHCP server does not reply with a NAK packet. In this case, the DHCP client needs to send REQUEST packets repeatedly. The client can obtain an IP address again only when the request times out. The time for obtaining an IP address is lengthened. This case also occurs when a client requires lease renewal but the DHCP server loses the lease record of the client due to a restart. In this case, you can configure compulsory NAK reply for the DHCP server if no lease record is found, so as to ensure that the client can obtain an IP address quickly.

1.2.5 DHCP Relay Agent

1. Principles

A DHCP relay agent helps to implement dynamic IP address assignment across network segments. The DHCP relay agent transparently forwards DHCP packets in unicast mode between a DHCP server and DHCP clients that reside on diverse network segments. It serves as a repeater. The Client-Relay-Server mode achieves dynamic management of IP addresses across multiple network segments with only one DHCP server.

Figure 1-1Working Process

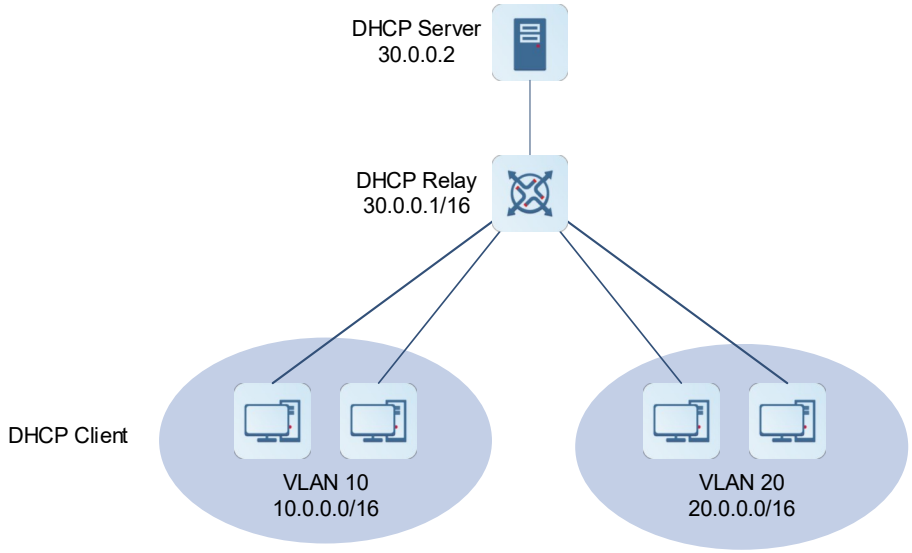


(1) After a DHCP relay agent receives a DHCP DISCOVER or DHCP REQUEST packet broadcast by a DHCP client, the DHCP relay agent adds its own IP address to the **giaddr** field of the packet and forwards the packet to a specified DHCP server in unicast mode.

(2) Based on the **giaddr** field, the DHCP server assigns an IP address and other configurations to the client, so that the DHCP relay agent forwards the configurations to the client, ensuring dynamic client configuration.

2. **Typical Applications**

Figure 1-1DHCP Relay Application Scenario



VLAN 10 and VLAN 20 are on the network segments 10.0.0.1/16 and 20.0.0.1/16, respectively. A DHCP server with the IP address 30.0.0.2 is in network segment 30.0.0.1/16. To achieve dynamic management of IP addresses in VLAN 10 and VLAN 20 by the DHCP server, you only need to enable the DHCP relay function on a gateway and configure the IP address 30.0.0.2 for the DHCP server.

3. **Option 82**

As defined in RFC 3046, a DHCP relay agent can add the DHCP relay agent information option to indicate a DHCP client's network information, so that a DHCP server can assign IP addresses of various privileges based on more accurate information. The option is called Option 82.

Based on the physical port that receives DHCP request packets and the MAC address of the device, the DHCP relay agent constructs Option 82. Option 82 can contain a maximum of 255 sub-options. If Option 82 is defined, it should contain at least one sub-option. Currently, the device supports sub-option 1 (**Circuit ID**) and sub-option 2 (**Remote ID**). Figure 1-1 and Figure 1-2 show the formats of the two sub-options.

Figure 1-1Option 82 Circuit ID

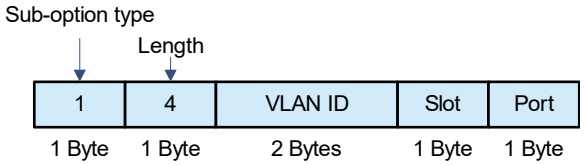
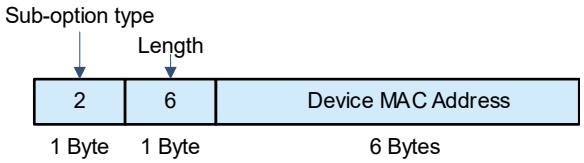


Figure 1-2Option 82 Remote ID



4. **Custom Option 82**

Option 82 can be customized. A DHCP relay agent can form an Option 82 based on the physical port that receives DHCP request packets and the MAC address and the name of the device. Figure 1-1 and Figure 1-2 show the formats of the sub-options.

Figure 1-1Custom Option 82 Circuit ID

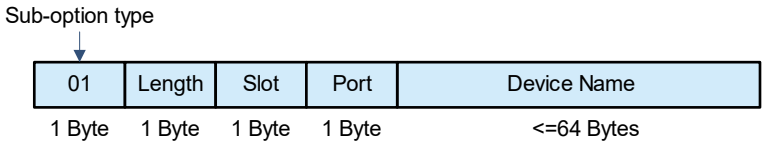
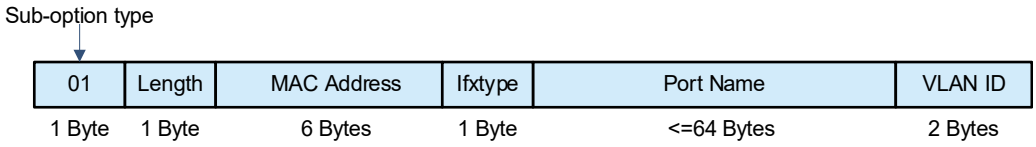


Figure 1-2Custom Option 82 Remote ID

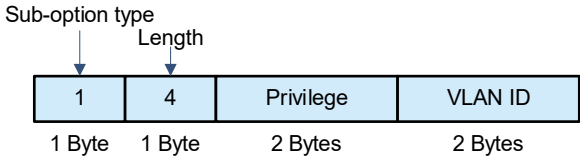


5. **Option Dot1x**

Option Dot1x should be used in combination with 802.1X authentication and Orion_B26Q's Orion-SAM authentication and accounting management system.

A DHCP relay agent constructs the **Circuit ID** sub-option based on the IP privilege delivered during 802.1X authentication and the VLAN ID of a DHCP client. Figure 1-1 shows the option format.

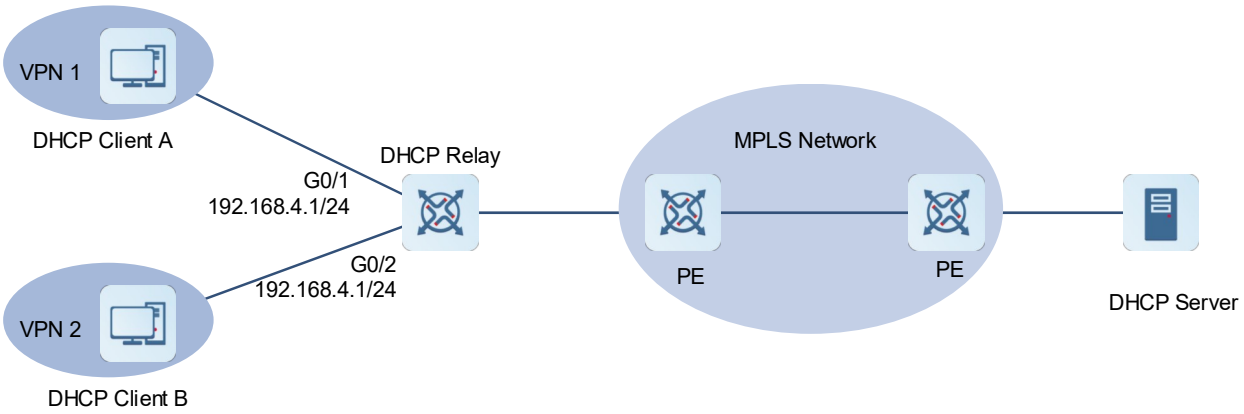
Figure 1-1Option Dot1x Circuit ID Sub-option



6. **Option VPN**

Option virtual private network (VPN) should be used in combination with Multiprotocol Label Switching (MPLS) VPN functions.

Figure 1-1Application in an MPLS VPN Environment



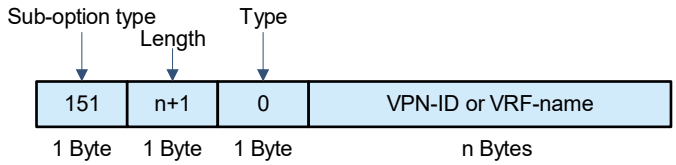
As shown in Figure 1-1, in an MPLS VPN environment, DHCP Client A is connected to GigabitEthernet 0/1 on a DHCP relay agent, and DHCP Client B is connected to GigabitEthernet 0/2 on the DHCP relay. GigabitEthernet 0/1 and GigabitEthernet 0/2 belong to different virtual routing and forwarding (VRF) instances. DHCP Client A and DHCP Client B obtain IP addresses through DHCP. According to the network plan, VPN 1 and VPN 2 share the network segment 192.168.4.0/24. In this case, traditional DHCP application cannot meet the deployment requirement.

To support DHCP Relay in the MPLS VPN environment, Option VPN is introduced, which includes three sub-options, namely, **VPN-ID**, **Subnet-Selection**, and **Server-Identifier-Override**.

- VPN-ID

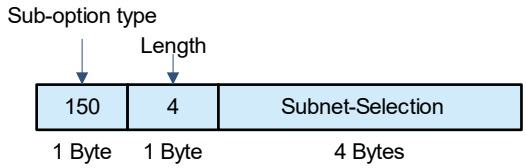
  When a DHCP relay agent receives a DHCP request packet, it adds the VPN information of the DHCP client to the packet as an option. The DHCP server retains **VPN-ID** in a reply packet, so that the DHCP relay agent forwards the packet to the correct VRF instance based on the option. Figure 1-2 shows the option format.

Figure 1-2VPN-ID



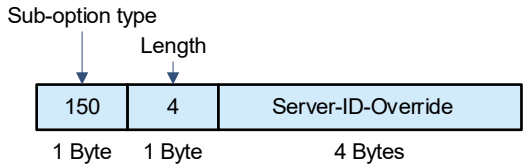
- **Subnet-Selection**: In a traditional DHCP Relay environment, the **giaddr** field is used to indicate information about a client's network and the addresses of a DHCP server and a DHCP relay agent. In an MPLS VPN environment, set **giaddr** to the IP address of an interface on a DHCP relay agent connected to a DHCP server, so that the server can communicate directly with the relay. The client's subnet must be indicated by the **Subnet-Selection** option. Figure 1-3 shows the option format.

Figure 1-3Subnet-Selection



- **Server-ID-Override**: In an MPLS VPN environment, request packets from a DHCP client cannot be directly sent to a DHCP server. A DHCP relay agent uses this option to carry the IP address of the interface directly connected to the DHCP client. When the server sends a reply packet, this option overrides the **Server-Identifier** option. In this way, the DHCP client sends packets to the DHCP relay agent, and the DHCP relay agent forwards them to the DHCP server. Figure 1-4 shows the option format.

Figure 1-4Server-Identifier-Override



1.2.6 DHCP Associated with VRRP Monitoring

In a Virtual Router Redundancy Protocol (VRRP) scenario, DHCP provides a command to monitor the VRRP status of the current interface. For interfaces configured with a VRRP address and VRRP monitoring, a DHCP server processes DHCP clients' request packets from an interface on a master device but discards the request packets from an interface on a backup device. If no VRRP address is configured on an interface, the DHCP server does not monitor the VRRP status and processes all DHCP request packets from this interface. VRRP monitoring is configured only on Layer 3 interfaces. It is disabled by default, namely, only the master device provides the DHCP service.

- Assigning IP addresses based on VLANs and ports

  In an environment with an IP address pool, a specified IP address range is assigned for each VLAN and port. A valid address is selected when the normal dynamic address assignment logic is met. There are three scenarios.

  - Global default configuration: Globally configured addresses are assigned by default.
  - Configuration based on VLANs and ports: Addresses in a specified IP address range are assigned only to the clients with specified VLANs and ports.
  - Hybrid configuration: Clients with specified VLANs and ports are assigned with the addresses in the specified IP address range, and the other clients are assigned with default global addresses.

- Preferentially assigning the DNS address obtained from an external DHCP server

  When some ports on the device operate in Point-to-Point Protocol over Ethernet (PPPoE) or DHCP client mode, the device can automatically obtain a DNS address from an external DHCP server and configure the address on the DHCP server of the local device, so that users do not need to perform DNS configuration. When the device serves as a DHCP server, it preferentially uses the DNS server address

obtained from an external DHCP server as the DNS server address in configuration information sent to the DHCP client.

1.2.7 Protocols and Standards

- RFC 2131: Dynamic Host Configuration Protocol
- RFC 2132: DHCP Options and BOOTP Vendor Extensions
- RFC 3046: DHCP Relay Agent Information Option
- RFC 3442: Classless Static Route Option for DHCPv4

1.3 Configuring DHCP Server

1.3.1 Overview

Configure the device as a DHCP server to assign IP addresses to DHCP clients and manage these IP addresses and other configurations. You can also configure other custom functions for the DHCP server as required to customize DHCP services.

1.3.2 Configuration Task Summary

(1) Enabling DHCP Server

(2) (Optional) Configuring Static IP Address Assignment

(3) Configuring Dynamic Assignment of IP Addresses and Network Parameters

(4) (Optional) Configuring DHCP Address Pool Management Function

(5) (Optional) Providing the Boot Image File Name

(6) (Optional) Assigning IP Addresses Based on Class Rules

(7) (Optional) Assigning IP Addresses Based on AM Rules

(8) Configuring security functions of a DHCP server: All the configuration tasks below are optional. Perform the configuration tasks as required.

- Refreshing Trusted ARP Entries
- Configuring Rogue DHCP Server Detection

(9) Configuring other custom functions of the DHCP server: All the configuration tasks below are optional. Perform the configuration tasks as required.

- Configuring IP Address Conflict Detection
- Configuring Compulsory NAK Reply
- Configuring VRRP Monitoring
- Configuring ARP-based Go-Offline Detection
- Saving Historical Leases

1.3.3 Enabling DHCP Server

1. **Overview**

For the device to function as a DHCP server and assign IP addresses and other network parameters to DHCP clients, enable the DHCP Server function on the device.

2. **Restrictions and Guidelines**

The **service dhcp** command enables both the DHCP server and DHCP relay functions. When the device is configured with a valid address pool, it acts as a server and directly processes packets. Otherwise, it serves as a relay and forwards the packets.

3. **Procedure**

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the DHCP server function.

service dhcp

The DHCP server function is disabled by default.

1.3.4 Configuring Static IP Address Assignment

1. **Overview**

Deliver specific IP addresses and configurations to specific DHCP clients, such as servers and printers.

2. **Procedure**

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an address pool and enter the DHCP address pool configuration mode.

ip dhcp pool *dhcp-pool*

(4) Configure the IP address and network mask of a client host.

host *ip-address* [*netmask*]

No IP address or network mask is configured for a client host by default.

If no network mask is defined, the DHCP server uses the natural mask of the IP address as the network mask.

(5) Configure the hardware address or unique ID of a client. Select either of the following configuration tasks.

- Configure a client hardware address.

  hardware-address *hardware-address* [*type*]

No hardware address is configured by default. If no hardware platform protocol is defined when the hardware address is configured, the default protocol is **ethernet**.

- Configure a unique client ID.

  client-identifier [*unique-identifier*]

  No DHCP client ID is configured by default.

  A client ID consists of the media type, MAC address, and interface name.

(6) (Optional) Configure a client name.

client-name *client-name*

No client name is configured by default. A client name can be any characters in the American Standard Code for Information Interchange (ASCII) character set. The name should not contain the domain name.

1.3.5 Configuring Dynamic Assignment of IP Addresses and Network Parameters

1. **Overview**

Configure address pool attributes, such as the address lease time, DNS address, and custom options. A DHCP server can use options to send the information to clients, so as to ensure dynamic network parameter assignment.

2. **Procedure**

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an address pool and enter the DHCP address pool configuration mode.

ip dhcp pool *dhcp-pool*

(4) Configure the primary network segment for dynamic assignment in a DHCP address pool.

network *network-number net-mask* [*low-ip-address high-ip-address*]

No primary network segment for dynamic assignment in a DHCP address pool is configured by default.

(5) (Optional) Configure the default gateway for a client.

default-router { *ip-address*&<1-8> }

No default gateway is configured for a DHCP client by default.

The gateway address that a DHCP server specifies for a DHCP client must be in the same network segment as the address assigned to the client.

(6) (Optional) Configure the domain name for a client.

domain-name *domain-name*

No domain name is configured for a DHCP client by default.

After a DHCP client obtains a specified domain name, it can directly use its host name to access a host whose name contains the same domain name.

(7) (Optional) Configure the DNS server to be assigned to a DHCP client.

dns-server { *ip-address*&<1-8> }

No DNS server is configured for a DHCP client by default.

When multiple DNS servers are defined, the first defined DNS server has the highest priority. A DHCP client selects the next DNS server only when it fails to communicate with the first defined DNS server.

(8) (Optional) Configure the NetBIOS WINS server for a DHCP client.

netbios-name-server { *ip-address*&<1-8> }

No NetBIOS WINS server is configured for a DHCP client by default.

When multiple NetBIOS WINS servers are defined, the first defined NetBIOS WINS server has the highest priority. A DHCP client selects the next NetBIOS WINS server only when it fails to communicate with the first defined NetBIOS WINS server.

(9) (Optional) Configure the type of a NetBIOS node to be assigned to a DHCP client.

netbios-node-type *type*

The default node type of a DHCP client running a Microsoft operating system is broadcast or hybrid. If no WINS server is configured, the client is a broadcast node. Otherwise, it is a hybrid node.

(10) (Optional) Define DHCP server options.

option *code* { **ascii** *string* | **hex** *string* | **ip** *ip-address* }

No DHCP server option is defined by default.

1.3.6 Configuring DHCP Address Pool Management Function

1. Configuration Tasks

All the configuration tasks below are optional. Perform the configuration tasks as required.

- Configuring an Address Lease Time
- Adding Trusted ARP Entries During Address Assignment
- Forcibly Disabling Gateway Assignment
- Enabling or Disabling an Address Pool
- Configuring an Alarm Threshold for an Address Pool

2. Configuring an Address Lease Time

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an address pool and enter the DHCP address pool configuration mode.

ip dhcp pool *dhcp-pool*

(4) Configure an address lease time.

lease { *days* [*hours*] [*minutes*] | **infinite** }

The default lease time of a static address pool is permanent by default. The default lease time of other address pools is 1 day.

3. Adding Trusted ARP Entries During Address Assignment

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an address pool and enter the DHCP address pool configuration mode.

ip dhcp pool *dhcp-pool*

(4) Add trusted ARP entries.

update arp

No trusted ARP entry is added during DHCP address assignment by default.

4. Forcibly Disabling Gateway Assignment

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an address pool and enter the DHCP address pool configuration mode.

ip dhcp pool *dhcp-pool*

(4) Forcibly disable gateway assignment.

force-no-router

A DHCP server assigns a gateway to a DHCP client by default.

5. Enabling or Disabling an Address Pool

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an address pool and enter the DHCP address pool configuration mode.

ip dhcp pool *dhcp-pool*

(4) Enable or disable the address pool.

pool-status { **enable** | **disable** }

A created address pool is enabled by default.

6. Configuring an Alarm Threshold for an Address Pool

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an address pool and enter the DHCP address pool configuration mode.

ip dhcp pool *dhcp-pool*

(4) Configure an alarm threshold for the address pool.

lease-threshold *threshold-percentage*

The default alarm threshold is 90% for the address pool.

1.3.7 Providing the Boot Image File Name

1. **Overview**

Some DHCP clients need to download the operating system or configuration file in the boot process. A DHCP server must provide the required image file name during boot for a DHCP client to download the file from the corresponding server.

2. **Procedure**

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the DHCP address pool configuration mode.

ip dhcp pool *dhcp-pool*

(4) (Optional) Configure the list of boot servers that a DHCP client needs to access during boot.

next-server { *ip-address*&<1-8> }

No list of boot servers that a DHCP client needs to access during boot is configured by default.

When multiple boot servers are defined, the first defined boot server has the highest priority. A DHCP client selects the next boot server only when it fails to communicate with the first defined boot server.

(5) (Optional) Configure the boot file name for a DHCP client.

bootfile *file-name*

No boot file name is configured for a DHCP client by default.

1.3.8 Assigning IP Addresses Based on Class Rules

1. **Overview**

In DHCP relay scenarios, addresses in a DHCP address pool can be assigned based on Option 82. When clients apply for IP addresses through different access points (APs), Option 82 carried in packets of the clients may be different. After class rules are configured on a DHCP server, the DHCP server can assign IP addresses in different network segments to clients based on Option 82 carried in the packets of the clients.

During address assignment, a DHCP server first determines an available address pool based on the network segment of a client. Then, it determines the class of the client based on Option 82, and assigns an IP address from the network segment corresponding to the class. When a request packet matches multiple classes in the address pool, the DHCP server assigns an IP address from the network segments corresponding to the classes based on the class configuration sequence. If the number of assigned IP addresses of a class reaches the limit, the DHCP server assigns an IP address based on the next matching class.

2. Restrictions and Guidelines

A DHCP address pool can be associated with multiple classes.

Each class corresponds to one network segment. Network segments are assigned in ascending order, and the network segments of multiple classes can overlap. If a class is associated with an address pool but no network segment is configured for the class, the default network segment of the class is the same as the network segment of the address pool.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a class rule and enter the class configuration mode.

ip dhcp class *class-name*

No class rule is configured by default.

(4) (Optional) Configure identification information for a class.

remark *class-remark*

No identification information is configured for a class by default.

(5) Enter the Option 82 information configuration mode.

relay agent information

(6) Configure an Option 82 information matching rule for a class.

relay-information hex *hex-string* [*]

No Option 82 matching rule is configured by default.

(7) Return to the global configuration mode.

exit

(8) Enter the DHCP address pool configuration mode.

ip dhcp pool *dhcp-pool*

(9) Associate an address pool with a class.

class *class-name*

No class is associated with a DHCP address pool by default.

(10) (Optional) Configure the IP address range corresponding to a class rule.

address range *low-ip-address high-ip-address*

The IP address range corresponding to a class rule is the network segment of the associated address pool by default.

(11) Return to the global configuration mode.

exit

(12) Enable address assignment based on class rules.

ip dhcp use class

Address assignment based on class rules is not configured by default.

1.3.9 Assigning IP Addresses Based on AM Rules

1. **Overview**

In super VLAN scenarios, address management (AM) rules can be used to plan IP address ranges for DHCP clients in different VLANs or DHCP clients using different ports, so that IP addresses can be assigned effectively and more flexibly. After an AM rule is configured, all DHCP clients from the specified VLANs and ports can obtain IP addresses. If a DHCP client is from a VLAN or port that is not specified, there are two cases: If a default AM rule is configured, the client obtains an IP address from the default IP address range; if no default AM rule is configured, the client cannot obtain an IP address.

2. **Restrictions and Guidelines**

This function can be configured only on Ethernet, Frame Relay (FR), Point-to-Point Protocol (PPP), or High-level Data Link Control (HDLC) interfaces.

3. **Procedure**

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the AM rule configuration mode.

address-manage

(4) Configure an AM rule. Select at least one of the following configuration steps.

- Configure the default IP address range matched with an AM rule.

  match ip default *ip-address netmask*

- Configure dynamic address assignment based on the VLAN and port.

  match ip *ip-address netmask* [*interface-type interface-number*] [**add | remove**] **vlan** *vlan-id*

- Configure static address assignment based on the VLAN.

  match ip *ip-address netmask* [**add** | **remove**] **vlan** *vlan-id*

  No AM matching rule is configured by default.

(5) (Optional) Configure the loose mode for an AM rule.

match ip loose

The loose mode of AM rules is disabled by default.

If the loose mode is configured, clients that match no AM rule can obtain IP addresses in the way same as the case with no AM rule configured.

1.3.10 Refreshing Trusted ARP Entries

1. **Overview**

Trusted ARP entries protect a gateway from ARP spoofing. Orion_B26Q devices with DHCP enabled provide a configuration command to determine whether trusted ARP entries are delivered during address assignment. After the function of adding trusted ARP entries is configured, a DHCP server adds trusted ARP entries during address assignment to prevent ARP spoofing. A trusted ARP entry has a higher priority than a dynamic ARP entry and is not overridden by the dynamic ARP entry.

After the function of refreshing trusted ARP entries is configured, a DHCP server refreshes trusted ARP entries only for clients assigned with addresses from an address pool that is configured with the **update arp** command.

2. **Procedure**

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Refresh trusted ARP entries.

ip dhcp refresh arp

1.3.11 Configuring Rogue DHCP Server Detection

1. **Overview**

If a DHCP server is deployed illegally, when clients request IP addresses from this server, clients are assigned with wrong addresses. This server is a rogue server. Orion_B26Q devices with DHCP enabled provide a command to enable rogue server detection. After rogue server detection is enabled, DHCP packets are checked for Option 54 (**Server Identifier**). If Option 54 is carried and its value is different from the actual DHCP server identifier, the IP address of the rogue server and the port receiving the packets are recorded. Rogue server detection is only a post-event detection function for security and cannot prevent an illegal DHCP server from assigning IP addresses to clients.

After rogue server detection is configured, rogue servers in a network are recorded into logs.

2. **Procedure**

(2) Enter the privileged EXEC mode.

enable

(3) Enter the global configuration mode.

configure terminal

(1) Configure rogue server detection.

ip dhcp server detect

Rogue server detection is disabled by default.

1.3.12 Configuring IP Address Conflict Detection

1. Overview

An excluded address is an IP address or address segment excluded from the address pool of a DHCP server, so that the DHCP server does not assign this IP address or address segment to a client. Excluding IP addresses can improve the address assignment efficiency.

When the DHCP server attempts to assign an IP address from the address pool, it uses the ping operation to check whether the IP address is occupied by another host. If yes, the DHCP server records the IP address. If not, the DHCP server assigns the IP address to a DHCP client.

The ARP entry check function can be used with the ping operation to detect IP address conflicts. If a client is configured with a static IP address and Layer 2 isolation is configured in an environment and the ping operation for IP address conflict detection becomes invalid (for example, a firewall is enabled on the client), this IP address may be assigned to another client that dynamically requests an address, resulting in an IP address conflict.

2. Configuration Tasks

All the configuration tasks below are optional. Perform the configuration tasks as required.

- Configuring Excluded IP Addresses
- Configuring the Number of Ping Operations Executed for Address Conflict Detection
- Configuring the Timeout Time of a Ping Operation Executed for Address Conflict Detection
- Configuring ARP Entry Check

3. Configuring Excluded IP Addresses

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure excluded IP addresses.

ip dhcp excluded-address *low-ip-address* [*high-ip-address*]

No excluded IP address is configured by default. A DHCP server assigns all addresses from an IP address pool to DHCP clients.

4. Configuring the Number of Ping Operations Executed for Address Conflict Detection

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the number of ping operations executed by a DHCP server when it detects IP address conflicts.

ip dhcp ping packets [*ping-times*]

A DHCP server pings a conflicted IP address two times by default.

5. **Configuring the Timeout Time of a Ping Operation Executed for Address Conflict Detection**

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the timeout time of a ping operation executed when a DHCP server detects address conflicts.

ip dhcp ping timeout *time*

The default timeout time of a ping operation for detecting address conflicts is 500 ms.

6. **Configuring ARP Entry Check**

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the ARP entry check.

ip dhcp arp-probe

The ARP entry check is disabled by default.

1.3.13 Configuring Compulsory NAK Reply

1. **Overview**

When a DHCP client moves from another network to the local network, the DHCP server does not reply with a NAK packet because it cannot find the corresponding lease record locally. In this case, the DHCP client needs to send REQUEST packets repeatedly. The client can obtain an IP address again only when the request times out, and the time for obtaining an IP address is lengthened. This case also occurs when a client requires lease renewal but the DHCP server loses the lease record of the client due to a restart. In this case, you can configure compulsory NAK reply for the DHCP server if no lease record is found, so as to ensure that the client can obtain an IP address quickly.

2. **Restrictions and Guidelines**

When compulsory NAK reply is enabled, enable only one DHCP server in a broadcast domain. Configuring compulsory NAK reply may cause exceptions to other servers.

3. **Procedure**

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure compulsory NAK reply for a DHCP server.

ip dhcp force-send-nak

Compulsory NAK reply is enabled by default.

1.3.14 Configuring VRRP Monitoring

1. Overview

After VRRP monitoring is enabled in VRRP application scenarios, only the master server processes DHCP packets.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the Layer 3 interface configuration mode.

interface *interface-type interface-number*

(4) Enable VRRP monitoring.

ip dhcp monitor-vrrp-state

VRRP monitoring is disabled for an interface by default.

1.3.15 Configuring ARP-based Go-Offline Detection

1. Overview

Orion_B26Q devices with DHCP enabled provide a command to enable ARP-based go-offline detection. After this function is enabled, a DHCP server receives an ARP entry aging notification when a client goes offline, and reclaims the client's IP address. If the client does not go online within a period of time (5 minutes by default), the DHCP server reclaims the IP address and assigns it to another client. If the client goes online again within the specified period, it can still use the original IP address.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure ARP-based go-offline detection.

ip dhcp server arp-detect

ARP-based go-offline detection is not configured for a DHCP server by default.

1.3.16 Saving Historical Leases

1. Overview

After a DHCP server assigns an IP address to a client and the client goes offline, the DHCP server saves the IP address lease of the client to the database. When the client goes online again, the DHCP server assigns this address to the client again. Historical leases are saved when a DHCP process restarts or the device performs a hot backup switchover.

2. **Procedure**

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of saving historical leases.

ip dhcp save-history-enable

The function of saving historical leases is disabled by default.

1.4 Configuring DHCP Relay

1.4.1 Overview

When a DHCP client and a DHCP server are in different network segments, a DHCP relay agent is required for dynamic IP address management.

1.4.2 Configuration Task Summary

(1) Configuring Basic DHCP Relay Functions

(2) Configuring extended DHCP relay functions: All the configuration tasks below are optional. Perform the configuration tasks as required.

- Configuring Option 82
- Configuring Server-ID Check
- Enabling DHCP Relay Suppression
- Configuring Multiple Gateway IP Addresses
- Forcing a DHCP Relay to Send a Reply Packet
- Configuring the Source IP Address of DHCP Relay Packets

1.4.3 Configuring Basic DHCP Relay Functions

1. **Overview**

Generally, the DHCP relay function is implemented by an interface. The IP address of the server should be specified on the DHCP relay agent. In this case, DHCP broadcast packets received over this interface are sent to the specified server.

2. **Restrictions and Guidelines**

To enable DHCP relay, configure IPv4 unicast routing in a network.

3. **Procedure**

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the DHCP relay function.

service dhcp

The DHCP relay function is disabled by default.

(4) Configure the IP address of the DHCP server.

ip helper-address { **cycle-mode** | [**vrf** *vrf-name*] *ip-address* }

The IP address of the DHCP server is not configured for the DHCP relay agent by default.

The DHCP server address can be globally configured or configured on an Layer 3 interface. A maximum of 20 DHCP server addresses can be globally configured or configured on each Layer 3 interface. When an interface receives a DHCP request packet, the DHCP server list on the interface prevails over that configured globally. If the interface is not configured with the DHCP server list, the global DHCP server list takes effect.

1.4.4 Configuring Option 82

1. **Overview**

A DHCP relay agent can use Option 82 to identify network information of DHCP clients, so that a DHCP server can assign IP addresses of different privileges to the clients more accurately based on this option.

2. **Procedure**

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable DHCP Option 82.

ip dhcp relay information option82

DHCP Option 82 is disabled by default.

(4) Configure sub-options of DHCP Option 82. All the configuration steps below are optional. Select configuration steps as required.

- Customize information in **Circuit ID**.

  ip dhcp relay information option82 user-defined circuit-id *circuit-id-text*

  No custom information is configured for **Circuit ID** of DHCP Option 82 by default.

- Customize information in **Remote ID**.

  ip dhcp relay information option82 user-defined remote-id *remote-id-text*

  No custom information is configured for **Remote ID** of DHCP Option 82 by default.

(5) (Optional) Customize the MAC address format.

ip dhcp relay information option82 user-defined mac-format *mac-format-type*

The default MAC address format is H.H.H.

1.4.5 Configuring Server-ID Check

1. **Overview**

In a DHCP relay application environment, multiple DHCP servers are configured in each network to provide server backup, thereby helping ensure uninterrupted network operation. When a DHCP client has selected a DHCP server to send a DHCP REQUEST packet, a **Server-ID** option is carried in the packet. To reduce server load in specific environments, enable the **Server-ID** check function on the DHCP relay agent, so as to send the DHCP REQUEST packet only to the DHCP server specified in this option.

In this case, the DHCP relay agent sends DHCP request packets only to the specified server. If this function is not configured, the DHCP relay agent sends DHCP request packets to all configured DHCP servers.

2. **Procedure**

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable a DHCP relay agent to check **Server-ID**.

ip dhcp relay check server-id

The **Server-ID** check function is disabled by default.

1.4.6 Enabling DHCP Relay Suppression

1. **Overview**

After you enable DHCP relay suppression on an interface, DHCP request packets received over the interface are filtered out, but the other DHCP requests are forwarded.

2. **Procedure**

(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) Enable the DHCP relay suppression function.

ip dhcp relay suppression

The DHCP relay suppression function is disabled on all interfaces by default.

1.4.7 Configuring Multiple Gateway IP Addresses

1. **Overview**

After the function of configuring multiple gateway IP addresses is enabled, a DHCP relay agent can use multiple interface IP addresses to send address requests to a DHCP server. Generally, the primary IP address

is used as the gateway IP address, and the DHCP server assigns a network segment based on the gateway IP address. When a client fails to apply for an IP address through the gateway by using the primary IP address, it applies for an IP address through the gateway by using a secondary IP address.

After the automatic gateway switchover function is enabled, the DHCP relay agent adds another address to the **giaddr** field if it does not receive a reply for three consecutive DISCOVER packets.

2. **Procedure**

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of configuring multiple gateway IP addresses on a DHCP relay agent.

ip dhcp relay multiple-giaddr

The function of configuring multiple gateway IP addresses on a DHCP relay agent is disabled by default.

(4) (Optional) Enable the automatic gateway switchover function.

ip dhcp smart-relay

The automatic gateway switchover function is disabled by default.

1.4.8 Forcing a DHCP Relay to Send a Reply Packet

1. **Overview**

After the function of forcing a DHCP relay agent to send a reply packet is enabled, a DHCP relay agent forcibly specifies a gateway interface to send a reply if it fails to find a MAC address egress. When the function is disabled, the DHCP relay agent discards packets if it fails to find a MAC address egress.

2. **Restrictions and Guidelines**

You must enable basic DHCP Relay functions.

3. **Procedure**

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of forcing a DHCP relay agent to send a reply packet.

ip dhcp relay force-send-reply-pack

The function of forcing a DHCP relay agent to send a reply packet is disabled by default.

1.4.9 Configuring the Source IP Address of DHCP Relay Packets

1. **Overview**

You can run the **ip dhcp relay source** command on an interface to configure the source IP address of DHCP relay packets.

2. **Restrictions and Guidelines**

- Only one source IP address can be specified for DHCP relay packets on each interface.
- To assign correct subnet addresses to clients, this function should be used with Option 82.

3. **Procedure**

(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 source IP address for DHCP relay packets.

ip dhcp relay source *ip-address*

No source address is configured for DHCP relay packets by default.

1.5 Monitoring

Run the **show** command to check the configuration.

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

Caution

The output of debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

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

Caution

Running the **clear** commands may lose vital information and thus interrupt services.

Table 1-1Monitoring

Command	Purpose
clear ip dhcp binding { * | *ip-address* }	Clears DHCP address binding records.
clear ip dhcp conflict { * | *ip-address* }	Clears DHCP address conflict records.
clear ip dhcp history { * | *mac-address* }	Clears DHCP historical records.
clear ip dhcp server detect { * | *ip-address* }	Clears rogue DHCP server detection records.
clear ip dhcp server rate	Clears DHCP server performance statistics.
clear ip dhcp server statistics	Clears DHCP server statistics.
clear ip dhcp relay statistics	Clears DHCP relay statistics.

show ip dhcp binding	Displays DHCP address bindings.
show ip dhcp conflict	Displays address conflict records of a DHCP server.
show ip dhcp history	Displays DHCP historical lease records.
show ip dhcp identifier	Displays the address pool ID and address usage of a DHCP server.
show ip dhcp pool [*pool-name*]	Displays the address pool status and utilization of a DHCP server.
show ip dhcp relay-statistic	Displays DHCP relay statistics.
show ip dhcp server detect	Displays rogue DHCP server detection information.
show ip dhcp server statistic	Displays DHCP server statistics.
show ip dhcp socket	Displays DHCP socket indexes.
debug ip dhcp server agent	Debugs a DHCP server.
debug ip dhcp server ha	Debugs DHCP hot backup.
debug ip dhcp server pool	Debugs DHCP address pools.
debug ip dhcp server vrrp	Debugs association between a DHCP server and a VRRP group.
debug ip dhcp server all	Debugs all DHCP servers.
debug ip dhcp relay	Debugs a DHCP relay.

1.6 Configuration Examples

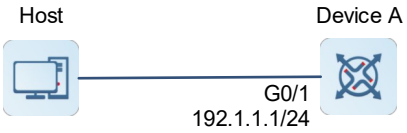
1.6.1 Configuring Static Address Binding

1. **Requirements**

As shown in Figure 1-1, a host that serves as a DHCP client obtains a statically bound IP address from Device A that serves as a DHCP server. The MAC address of the host is 0050.56b0.2f50.

2. **Topology**

Figure 1-1Static Address Binding



3. Notes

Configure Device A:

- Configure the IP address of the interface.
- Enable the DHCP server service and configure address pool parameters.

4. Procedure

(1) Configure Device A:

Configure the IP address of the interface.

```
DeviceA> enable
DeviceA # configure terminal
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ip address 192.1.1.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

Enable the DHCP server service.

```
DeviceA(config)# service dhcp
```

Create an address pool named **pool1**.

```
DeviceA(config)# ip dhcp pool pool1
```

Assign a statically bound IP address to the host.

```
DeviceA(dhcp-config)# host 192.1.1.99 255.255.255.0
DeviceA(dhcp-config)# hardware-address 0050.56b0.2f50
```

(2) Configure the host:

Enable DHCP on the host to obtain an IP address. (Omitted)

5. Verification

Check that the host has obtained the IP address 192.1.1.99/24.

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
 interface gigabitethernet 0/1
 ip address 192.1.1.1 255.255.255.0
!
 service dhcp
!
 ip dhcp pool pool1
 host 192.1.1.99 255.255.255.0
 hardware-address 0050.56b0.2f50
!
```

7. Common Errors

- No address pool is configured.

- The DHCP Server service is not enabled.

1.6.2 Dynamically Assigning IP Addresses

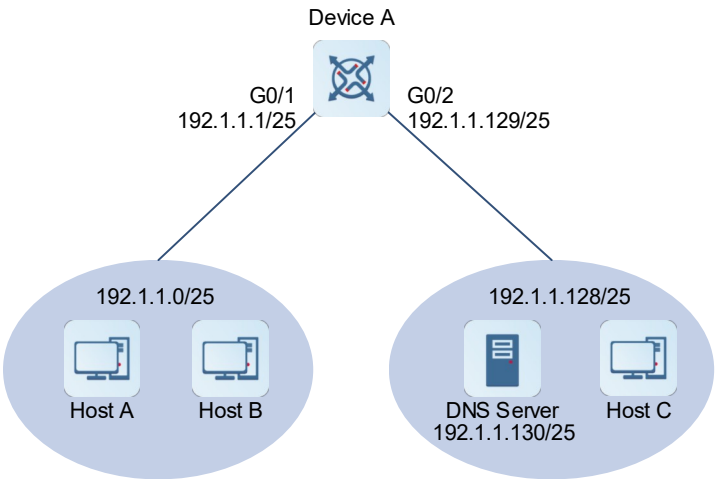
1. Requirements

As shown in Figure 1-1, Device A serving as a DHCP server dynamically assigns IP addresses to clients in the same network segment. The address pool is divided into two network segments: 192.1.1.0/25 and 192.1.1.128/25.

The lease time of IP addresses in network segment 192.1.1.0/25 is 5 days, the domain name suffix is **test.com**, the DNS address is 192.1.1.130, and the gateway address is 192.1.1.1. The lease time of IP addresses in network segment 10.1.1.128/25 is 3 days, the domain name suffix is **test.com**, the DNS address is 192.1.1.130, and the gateway address is 192.1.1.129.

2. Topology

Figure 1-1Dynamically Assigning IP Addresses



3. Notes

Configure Device A:

- Configure the IP address of the interface for connecting to the host.
- Enable the DHCP Server service and configure parameters of two address pools.

4. Procedure

(1) Configure Device A:

Configure the IP address of the interface for connecting to the host.

```
DeviceA> enable
DeviceA # configure terminal
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ip address 192.1.1.1 255.255.255.128
DeviceA(config-if-GigabitEthernet 0/1)# exit
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# ip address 192.1.1.129 255.255.255.128
```

```
DeviceA(config-if-GigabitEthernet 0/2)# exit
```

Enable the DHCP Server service.

```
DeviceA(config)# service dhcp
```

Configure network parameters of pool 1.

```
DeviceA(config)# ip dhcp pool pool1
DeviceA(dhcp-config)# network 192.1.1.0 255.255.255.128
DeviceA(dhcp-config)# default-router 192.1.1.1
DeviceA(dhcp-config)# dns-server 192.1.1.130
DeviceA(dhcp-config)# domain-name test.com
DeviceA(dhcp-config)# lease 5
DeviceA(dhcp-config)# exit
```

Configure network parameters of pool 2.

```
DeviceA(config)# ip dhcp pool pool2
DeviceA(dhcp-config)# network 192.1.1.128 255.255.255.128
DeviceA(dhcp-config)# default-router 192.1.1.129
DeviceA(dhcp-config)# dns-server 192.1.1.130
DeviceA(dhcp-config)# domain-name test.com
DeviceA(dhcp-config)# lease 3
```

(2) Configure the DNS server:

Set the DNS server IP address to 192.1.1.130/25. (Omitted)

(3) Configure the host:

Enable DHCP on Host A, Host B, and Host C to obtain IP addresses. (Omitted)

5. **Verification**

Check that Host A and Host B have obtained addresses in network segment 192.1.1.0/25.

Check that Host C has obtained an address in network segment 192.1.1.128/25.

Run the **show ip dhcp pool** command on Device A to display address pool configurations and usage.

```
DeviceA(config)# show ip dhcp pool
Pool  name       Total     Distributed  Remained   Percentage
------------  -----------  -----------  --------   -----------
pool1         126          2            124        0.98413
pool2         126          1            125        0.99206
```

6. **Configuration Files**

Device A configuration file

```
hostname DeviceA
!
 interface gigabitethernet 0/1
 ip address 192.1.1.1 255.255.255.128
!
 interface gigabitethernet 0/2
 ip address 192.1.1.129 255.255.255.128
!
```

```
service dhcp
!
ip dhcp pool pool1
network 192.1.1.0 255.255.255.128
default-router 192.1.1.1
dns-server 192.1.1.130
domain-name test.com
lease 5
!
ip dhcp pool pool2
network 192.1.1.128 255.255.255.128
default-router 192.1.1.129
dns-server 192.1.1.130
domain-name test.com
lease 3
!
```

7. **Common Errors**

- No address pool is configured.
- The DHCP Server service is not enabled.

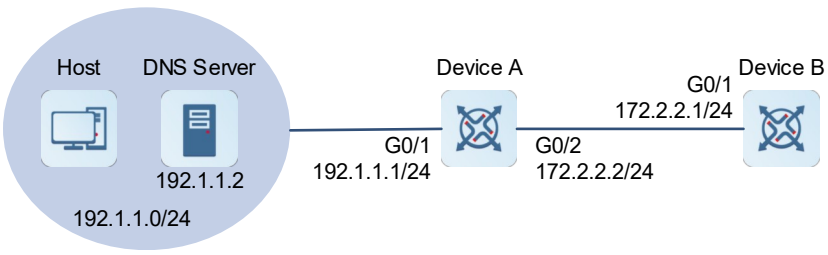
1.6.3 Configuring DHCP Relay

1. **Requirements**

As shown in Figure 1-1, a host serving as a DHCP client is located in network segment 192.1.1.0/24, Device A is the gateway, and Device B is a DHCP server. To apply for an IP address and other configurations from the DHCP server, the DHCP client needs to use the gateway as a DHCP relay agent, so that the DHCP relay agent forwards DHCP packets to the DHCP server.

2. **Topology**

Figure 1-1Configuring DHCP Relay



3. **Notes**

- Configure Device A:
  - Configure the IP address of the interface.
  - Enable the DHCP relay function.
- Configure Device B:

- Configure the IP address of the interface.
- Configure a route from Device B to GigabitEthernet 0/1 on Device A.
- Enable the DHCP server service and configure address pool parameters.

4. **Procedure**

(1) Configure Device A:

Configure the IP address of the interface.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ip address 192.1.1.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/1)# exit
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# ip address 172.2.2.2 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/2)# exit
```

Enable the DHCP relay function.

```
DeviceA(config)# service dhcp
```

Add the DHCP server address to the DHCP relay agent.

```
DeviceA(config)# ip helper-address 172.2.2.1
```

(2) Configure Device B:

Configure the IP address of the interface.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface gigabitethernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# ip address 172.2.2.1 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/1)# exit
```

Configure a static route to network segment 192.1.1.0/24.

```
DeviceB(config)# ip route 192.1.1.0 255.255.255.0 gigabitethernet 0/1
```

Enable the DHCP server function.

```
DeviceB(config)# service dhcp
```

Configure network parameters of pool 1.

```
DeviceB(config)# ip dhcp pool pool1
DeviceB(dhcp-config)# network 192.1.1.0 255.255.255.0
DeviceB(dhcp-config)# default-router 192.1.1.1
DeviceB(dhcp-config)# dns-server 192.1.1.2
DeviceB(dhcp-config)# exit
```

(3) Enable DHCP on the host to obtain an IP address. (Omitted)

5. **Verification**

Check that the host has obtained an address in network segment 192.1.1.0/24.

Run the **show ip dhcp pool** command on Device B to display the address pool configurations and usage.

```
DeviceB(config)# show ip dhcp pool
Pool  name       Total     Distributed  Remained   Percentage
------------  -----------  -----------  --------   -----------
pool1         126          1            125        0.99206
```

6. **Configuration Files**

- Device A configuration file

```
hostname DeviceA
!
 interface gigabitethernet 0/1
 ip address 192.1.1.1 255.255.255.0
!
 interface gigabitethernet 0/2
!
 service dhcp
 ip helper-address 172.2.2.1
!
```

- Device B configuration file

```
hostname DeviceB
!
 interface gigabitethernet 0/1
 ip address 172.2.2.1 255.255.255.0
!
 ip route 192.1.1.0 255.255.255.0 gigabitethernet 0/1
 service dhcp
!
 ip dhcp pool pool1
 network 192.1.1.0 255.255.255.0
 default-router 192.1.1.1
 dns-server 192.1.1.2
!
```

7. **Common Errors**

- The DHCP relay function is disabled on the DHCP relay agent.
- No route is configured between the DHCP relay agent and DHCP server.
- The IP address of the DHCP server is configured on the DHCP relay agent.

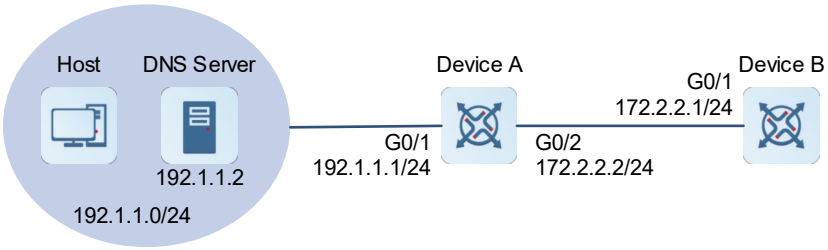
1.6.4 Assigning IP Addresses Based on Class Rules

1. **Requirements**

As shown in Figure 1-1, Device A serves as a DHCP server to assign IP addresses and other network configurations to clients, and Device B serves as a DHCP relay agent to forward DHCP packets between the clients and server. It is required that Device A assign an IP address in the range of 192.1.1.200 to 192.1.1.254 if a DHCP request packet carries Option 82 and assigns an IP address in the range of 192.1.1.1 to 192.1.1.199 if a DHCP request packet does not carry Option 82.

2. Topology

Figure 1-1Assigning IP Addresses Based on Class Rules



3. Notes

- Configure Device A:
  - Configure the IP address of the interface.
  - Enable the DHCP relay function.
  - Enable the Option 82 function.
- Configure Device B:
  - Configure the IP address of the interface.
  - Configure a route from Device B to GigabitEthernet 0/1 on Device A.
  - Enable the DHCP server service and configure address pool parameters.
  - Add a specific class rule.

4. Procedure

(1) Configure Device A:

Configure the IP address of the interface.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ip address 192.1.1.1 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/1)# exit
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# ip address 172.2.2.2 255.255.255.0
DeviceA(config-if-GigabitEthernet 0/2)# exit
```

Enable the DHCP relay function.

```
DeviceA(config)# service dhcp
```

Add the DHCP server address.

```
DeviceA(config)# ip helper-address 172.2.2.1
```

Enable Option 82.

```
DeviceA(config)# ip dhcp relay information option82
```

(2) Configure Device B:

Configure the IP address of the interface.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface gigabitethernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# ip address 172.2.2.1 255.255.255.0
DeviceB(config-if-GigabitEthernet 0/1)# exit
```

Configure a static route to network segment 192.1.1.0/24.

```
DeviceB(config)# ip route 192.1.1.0 255.255.255.0 gigabitethernet 0/1
```

Enable the DHCP Server function.

```
DeviceB(config)# service dhcp
```

Configure a class rule.

```
DeviceB(config)# ip dhcp class myclass
DeviceB(config-dhcp-class)# relay agent information
DeviceB(config-dhcp-class-relayinfo)# relay-information hex 060223*
```

Create an address pool and configure related network parameters.

```
DeviceB(config)# ip dhcp pool pool1
DeviceB(dhcp-config)# network 192.1.1.0 255.255.255.0
DeviceB(dhcp-config)# default-router 192.1.1.1
DeviceB(dhcp-config)# dns-server 192.1.1.2
```

Configure the network segment for assigning an IP address when a class is matched.

```
DeviceB(dhcp-config)# class myclass
DeviceB(config-dhcp-pool-class)# address range 192.1.1.200 192.1.1.254
DeviceB(config-dhcp-pool-class)# exit
```

(3) Enable DHCP on the host to obtain an IP address. (Omitted)

5. **Verification**

Capture packets on Device B and check that clients that match Option 82 rules in a class rule have obtained IP addresses in the range of 192.1.1.200 to 192.1.1.254 and clients that do not match Option 82 rules in the class rule have obtained IP addresses in the range of 192.1.1.1 to 192.1.1.199.

6. **Configuration Files**

- Device A configuration file

```
hostname DeviceA
!
 service dhcp
 ip helper-address 172.2.2.1
 ip dhcp relay information option82
!
 interface gigabitethernet 0/1
 ip address 192.1.1.1 255.255.255.0
 exit
 interface gigabitethernet 0/2
 ip address 172.2.2.2 255.255.255.0
```

```
!
```

- Device B configuration file

```
hostname DeviceB
!
 ip route 192.1.1.0 255.255.255.0 gigabitethernet 0/1
 service dhcp
!
 interface gigabitethernet 0/1
 ip address 172.2.2.1 255.255.255.0
!
 ip dhcp class myclass
 relay agent information
 relay-information hex 060223*
!
 ip dhcp pool pool1
 network 192.1.1.0 255.255.255.0
 default-router 192.1.1.1
 dns-server 192.1.1.2
 class myclass
   address range 192.1.1.200 192.1.1.254
!
```

7. **Common Errors**

- The DHCP Relay function is disabled.
- No route is configured between the DHCP relay agent and DHCP server.
- No DHCP server IP address is configured.