Contents

1 Configuring DHCPv6

1.1 Introduction

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) is a protocol that allows a DHCPv6 server to transfer configurations to IPv6 nodes, such as IPv6 address, domain name server (DNS) address, network information service (NIS) server address, and Simple Network Time Protocol (SNTP) server address.

Compared with other IPv6 address assignment methods, such as manual configuration and Stateless Address Autoconfiguration (SLAAC), DHCPv6 has the following advantages:

- DHCPv6 provides the address assignment, prefix delegation (PD), and configuration parameter allocation functions.
- DHCPv6 is a Stateful Address Autoconfiguration (SAAC) protocol for flexibly adding and reusing network addresses. It can record assigned addresses, which enhances network manageability.
- By using DHCPv6 PD, uplink network devices can assign address prefixes to downlink network devices, ensuring flexible station-level automatic configuration and flexible control of station address space.
- DHCPv6 configuration parameter allocation solves the problem that parameters cannot be obtained through the SLAAC protocol and allows a DHCPv6 server to assign DNS addresses and domain names to hosts.
- DHCPv6 is a protocol based on the client/server model. A DHCPv6 client is used to obtain various configurations, whereas a DHCPv6 server is used to provide various configurations. If the DHCPv6 client and DHCPv6 server are not on the same network link, they can interact with each other by using a DHCPv6 relay.

1.2 Principles

1.2.1 Basic Concepts

1. **IPv6 address assignment methods**
   - Manual configuration: IPv6 addresses/prefixes and other network configuration parameters are manually configured.
   - SLAAC: A host uses the prefix carried in a received Router Advertisement (RA) message and the local interface ID to automatically generate an IPv6 address.
   - SAAC (DHCPv6): DHCPv6 includes the following three types:
     - DHCPv6 SAAC: A DHCPv6 server automatically configures IPv6 addresses/prefixes and other network configuration parameters.
     - DHCPv6 SLAAC: A host automatically generates an IPv6 address by using an RA message. The DHCPv6 server assigns configuration parameters other than IPv6 addresses.
     - DHCPv6 PD: A lower-layer network router applies for a prefix from an upper-layer network router, and the upper-layer network router assigns a proper address prefix to the lower-layer network router. The lower-

layer network router automatically divides the delegated prefix (less than 64 bits) into subnet segments with a 64-bit prefix and assigns these prefixes to the links directly connected to IPv6 hosts through RA messages, ensuring automatic address configuration for the hosts.

2. DUID

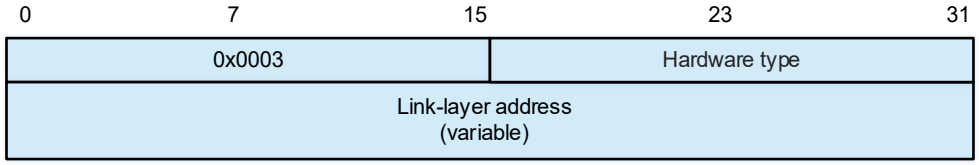
A DHCP Unique Identifier (DUID) uniquely identifies a DHCPv6 device (DHCPv6 client, relay, or server). It is used for mutual authentication during DHCPv6 message exchanges.

RFC 3315 defines three types of DUIDs:

- DUID Based on Link-Layer address plus Time (DUID-LLT)
- DUID Assigned by Vendor Based on Enterprise Number (DUID-EN)
- Link-Layer address (DUID-LL)

Orion_B26Q DHCPv6 devices use DUID-LLs.

Figure 1-1DUID-LL Structure



DUID type is set to **0x0003**, **Hardware type** is set to **0x0001** (indicating the supported hardware type of Ethernet), and **Link-layer address** is set to the Media Access Control (MAC) address of the interface with the minimum serial number on the device.

3. Multicast address

In DHCP, clients broadcast DHCP packets to servers. To prevent broadcast storms, DHCPv6 uses multicast packets instead of broadcast packets. DHCPv6 uses the following multicast addresses:

- FF02::1:2: a link-scoped multicast address used by a client to communicate with neighboring relay agents and servers. All DHCPv6 servers and relay agents on the link are members of this multicast group.
- FF05::1:3: a site-scoped multicast address used by a DHCPv6 relay agent to communicate with servers. All DHCPv6 servers within the site are members of this multicast group.

4. Identity association (IA)

A DHCPv6 server uses IAs to assign addresses to DHCPv6 clients. Each IA is uniquely identified by an identity association identifier (IAID). IAIDs are generated by DHCPv6 clients. One-to-one mappings are established between IAs and clients. An IA may contain several addresses, which can be allocated by the client to other interfaces. An IA may contain one of the following types of addresses:

- Non-temporary addresses (NAs), namely, globally unique addresses
- Temporary addresses (TAs), which are hardly used
- PD, prefix delegation

Based on the address type, IAs are classified into IA_NA, IA_TA, and IA_PD types. Orion_B26Q DHCPv6 servers support only IA_NA and IA_PD.

5. **Binding**

A DHCPv6 binding is a manageable address information structure. An address binding on a DHCPv6 server records the IA and other configurations of a client. A client can request multiple bindings. The address binding data on a server is presented in the form of an address binding table. Bindings that contain IAs use DUID, IA-Type, or IAID as the index, and bindings that contain configurations use DUID as the index.

6. **DHCPv6 address pool**

A DHCPv6 server uses address pools to save IP addresses and network parameters to be assigned to clients.

7. **Sequence for selecting addresses/prefixes**

A DHCPv6 server selects to-be-assigned IPv6 addresses/prefixes based on the following sequence:

(1) Addresses/prefixes previously assigned to the client

(2) Idle address/prefixes in the address pool/prefix pool that meet the client's requirements

(3) Other idle addresses/prefixes in the address pool/prefix pool

(4) Expired or previously conflicted addresses/prefixes

(5) If no address is available, the DHCPv6 server does not assign an address to the client.

8. **Address conflict**

When an address assigned to a DHCPv6 client is conflicted, the client sends a DECLINE packet to notify the DHCPv6 server that the address is rebound. Then, the server adds the address to the address conflict queue. The server does not assign addresses in the address conflict queue to clients, and can display and clear address information in the address conflict queue.

9. **Packet type**

DHCPv6 uses User Datagram Protocol (UDP) ports 546 and 547 for packet exchanges. Specifically, a DHCPv6 client uses port 546 for receiving packets, while a DHCPv6 server and a DHCPv6 relay agent use port 547 for receiving packets. The following describes types of packets that can be exchanged among a DHCPv6 server, client, and relay agent:

- Packets that may be sent from a DHCPv6 client to a DHCPv6 server include SOLICIT, REQUEST, CONFIRM, RENEW, REBIND, RELEASE, DECLINE, and INFORMATION-REQUEST packets.
- Packets that may be sent from a DHCPv6 server to a DHCPv6 client include ADVERTISE, REPLY, and RECONFIGURE packets.
- Packets that may be sent from a DHCPv6 relay agent to another DHCPv6 relay agent or a DHCPv6 server include RELAY-FORWARD packets.
- Packets that may be sent from a DHCPv6 server or DHCPv6 relay agent to another DHCPv6 relay agent include RELAY-REPLY packets.

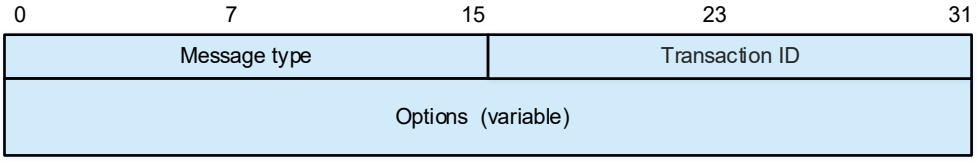
Note

- Orion_B26Q DHCPv6 servers do not support RECONFIGURE packets.
- Orion_B26Q DHCPv6 clients do not support CONFIRM and RECONFIGURE packets.

1.2.2 Packet Format

1. **Format of Packets Exchanged Between a DHCPv6 Client and a DHCPv6 Server**

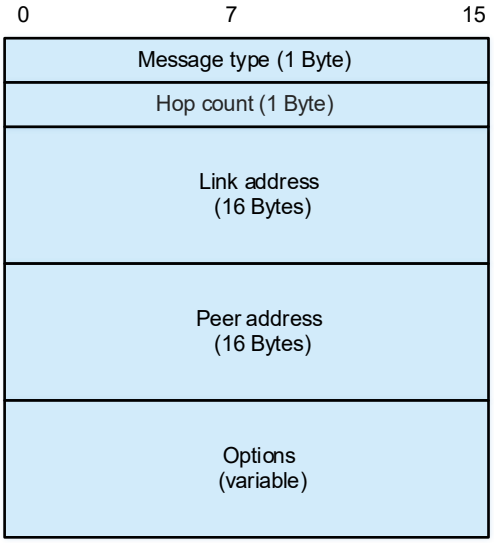
Figure 1-1Format of Packets Exchanged Between a DHCPv6 Client and a DHCPv6 Server



- **Message type**: Identifies the message type of a DHCPv6 packet.
- **Transaction ID**: Identifies a DHCPv6 packet exchange.
- **Options**: variable-length options carried in a packet.

2. **Format of Packets Exchanged Between a DHCPv6 Relay Agent and a DHCPv6 Server**

Figure 1-1Format of Packets Exchanged Between a DHCPv6 Relay Agent and a DHCPv6 Server



- **Message type**: Identifies the message type of a DHCPv6 packet. Only RELAY-FORWARD and RELAY-REPLY packets can be exchanged between a DHCPv6 relay agent and a DHCPv6 server.
- **Hop count**: Number of relays that a packet passes through.
- **Link address**: Used by a DHCPv6 server to identify the access link of a client. It is a global IPv6 unicast address or link-local address.
- **Peer address**: Source address of a relayed packet, that is, the address of a client or a relay agent.
- **Options**: Variable-length options. The **Relay message** option is mandatory, and a relay agent can add other options.

1.2.3 Requesting/Allocating Addresses

A DHCPv6 client can request an IPv6 address from a DHCPv6 server.

After being configured with available addresses, a DHCPv6 server can assign IPv6 addresses to hosts in the network and record the assigned addresses to improve the network manageability.

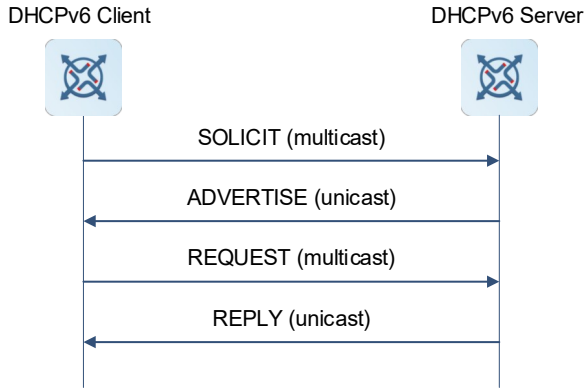
1. Principles

Network hosts serve as DHCPv6 clients and DHCPv6 servers to implement address assignment, update, confirmation, and release through message exchanges.

2. Four-Way Message Exchange

Generally, a DHCPv6 client and a DHCPv6 server implement address, prefix, and parameter configuration through a four-way message exchange.

Figure 1-1Process of Four-Way Message Exchange



(1) A DHCPv6 client sends a SOLICIT message with the destination address FF02::1:2 and destination port 547 on the local link in multicast mode to request an address, a prefix, and configuration parameters. All DHCPv6 servers or DHCPv6 relay agents on the link receive this SOLICIT message.

(2) After receiving the SOLICIT message, the DHCPv6 server sends an ADVERTISE message in unicast mode if it can provide the information requested in the SOLICIT message. The ADVERTISE message includes the requested address, prefix, and configuration parameters.

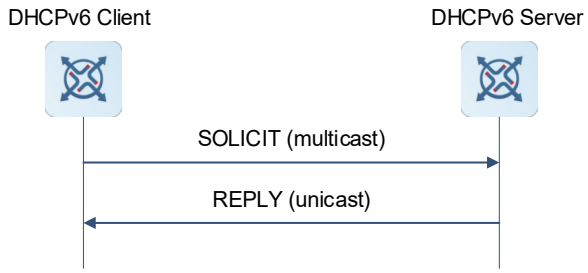
(3) The DHCPv6 client may receive the ADVERTISE messages from multiple DHCPv6 servers. Generally, the DHCPv6 client selects the server from which it first receives the ADVERTISE message as the DHCPv6 server. Then, the DHCPv6 client sends a REQUEST message with the destination address FF02::1:2 and destination port 547 to request an address, a prefix, and configuration parameters.

(4) After receiving the REQUEST message, the DHCPv6 server creates a binding locally and sends a REPLY message in unicast mode. The REPLY message includes the address, prefix and configuration parameters that the DHCPv6 server assigns to the DHCPv6 client. The DHCPv6 client completes address, prefix, or parameter configuration based on the information in the REPLY message.

3. Two-Way Message Exchange

The two-message exchange can be used to complete address, prefix, and parameter configuration for DHCPv6 clients more quickly.

Figure 1-1Two-Way Message Exchange



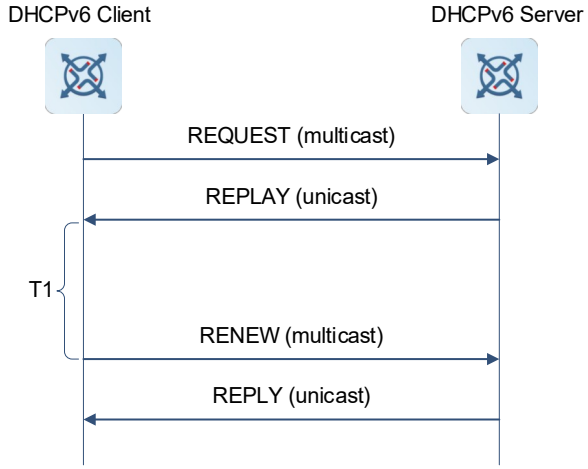
(1) A DHCPv6 client sends a SOLICIT message with the destination address FF02::1:2 and destination port 547 on the local link to request an address, a prefix, and configuration parameters. The SOLICIT message contains the **Rapid Commit** option.

(2) If a DHCPv6 server supports the **Rapid Commit** option, the DHCPv6 server creates a binding locally and sends a REPLY message in unicast mode. The REPLY message includes the address, prefix, and configuration parameters to be assigned to the DHCPv6 client. The DHCPv6 client completes configuration based on the information in the REPLY message. If the DHCPv6 server does not support the **Rapid Commit** option, that is, it does not support rapid assignment, the process of four-way message exchange is used to assign an IPv6 address/a prefix and other network configuration parameters to the client.

4. **Update and Rebinding**

The DHCPv6 server provides the control address and the updated T1 and T2 in the IA of the REPLY message sent to the DHCPv6 client.

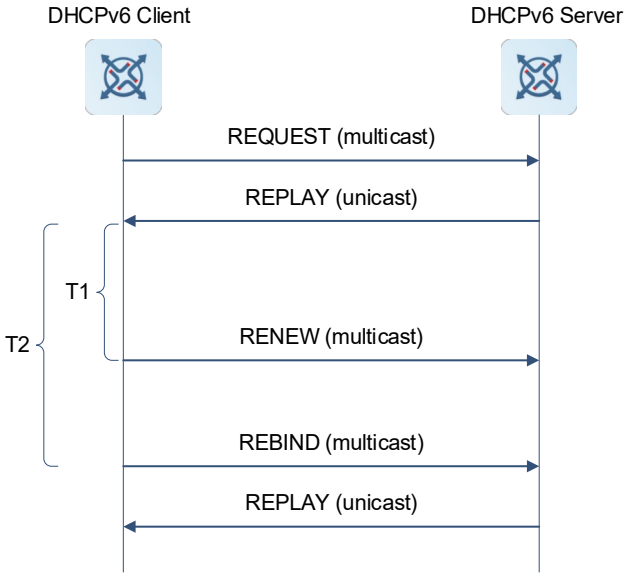
Figure 1-1Update



(1) The DHCPv6 client sends a RENEW multicast message to the DHCPv6 server for updating the address and prefix after T1 seconds. The RENEW message contains the DUID of the DHCPv6 server and the IA information to be updated.

(2) After receiving the RENEW message, the DHCPv6 server checks whether the DUID value in the RENEW message is the same as its DUID. If yes, the DHCPv6 server updates the local binding and sends a REPLY message in unicast mode. The REPLY message contains the new T1 and other parameters.

Figure 1-1Rebinding



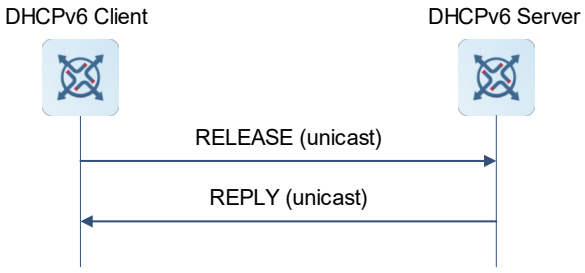
(1) If no response is received within T2 after the DHCPv6 client sends a RENEW message to the DHCPv6 server, the DHCPv6 client sends a REBIND multicast message to the DHCPv6 server for rebinding the address and prefix.

(3) After receiving the REBIND message, the DHCPv6 server (perhaps a new DHCPv6 server) sends a REPLY message based on the content of the REBIND message.

5. **Release**

If a DHCPv6 client needs to release an address or a prefix, the DHCPv6 client needs to notify the DHCPv6 server of the to-be-released address or prefix. In this way, the DHCPv6 server can assign the address or prefix to other DHCPv6 clients.

Figure 1-1Release



(1) A DHCPv6 client sends a RELEASE message to a DHCPv6 server to notify the DHCPv6 server that it no longer needs to use an address or prefix, that is, to release the address or prefix.

(2) After receiving RELEASE message, the DHCPv6 server removes the corresponding binding based on the address or prefix in the RELEASE message and sends a REPLY message carrying the state option to the DHCPv6 client.

6. Confirmation

After moving to a new link or encountering a restart, a DHCPv6 client needs to confirm whether the original address is still available.

Figure 1-1Confirmation

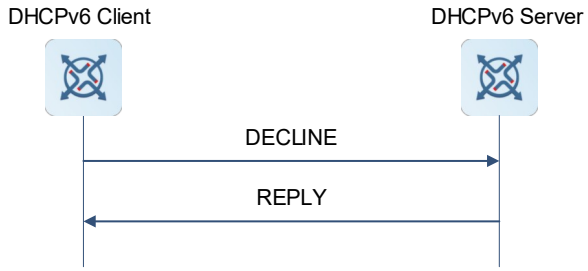
(1) The DHCPv6 client sends a CONFIRM message to the DHCPv6 server on the new link to check whether the original address is still available.

(2) After receiving the CONFIRM message, the DHCPv6 server performs confirmation based on the address information contained in the CONFIRM message and sends a REPLY message carrying the state option to the DHCPv6 client. If the confirmation indicates unavailability, the DHCPv6 client may initiate a new address assignment request.

7. Address conflict

If a DHCPv6 client finds that the assigned address has been occupied on the link, the DHCPv6 client sends a DECLINE message to notify the DHCPv6 server of the address conflict.

Figure 1-1Address conflict



(1) The DHCPv6 client sends a DECLINE message to the DHCPv6 server. The DECLINE message includes the IA information of the conflicted address.

(2) After receiving the DECLINE message, the DHCPv6 server marks the address in the DECLINE message as **Declined** and does not assign the address to other clients. Then, the DHCPv6 server sends a REPLY message carrying the state option to the DHCPv6 client. You can manually clear addresses marked as **Declined** to facilitate re-assignment.

1.2.4 Requesting/Allocating Prefixes

After available prefixes are configured on a DHCPv6 server, uplink network devices can assign the address prefixes to downlink network devices by serving as the PD of the DHCPv6 server. This ensures flexible station-level automatic address configuration and flexible control of station address space.

Downlink network devices serve as DHCPv6 clients to exchange messages with the DHCPv6 server to implement prefix assignment, update, and release. Downlink network devices obtain, update, rebind, and release prefixes by using the four-way or two-way message exchange mechanism similar to that for assigning addresses. However, prefix assignment is different from address assignment in the following aspects:

- In message exchanges via PD, the CONFIRM and DECLINE messages are not used.
- If a DHCPv6 client connects to a new link and needs to check whether the prefix is available, it performs confirmation by exchanging the REBIND and REPLY messages.
- These messages use IA_PD.

Note

For message exchanges via PD, see section 1.2.3 "Requesting/Allocating Addresses."

1.2.5 Stateless Service

When a DHCPv6 client only needs configuration parameters, the DHCPv6 stateless service can be used to obtain related configuration parameters. This solves the problem that configuration parameters such as the DNS address cannot be obtained through the SLAAC protocol.

Figure 1-1Message Exchange Using the Stateless Service

(1) A DHCPv6 client sends an INFORMATION-REQUEST message to a DHCPv6 server to request stateless information. Usually, this message does not contain the DUID of a specific DHCPv6 server.

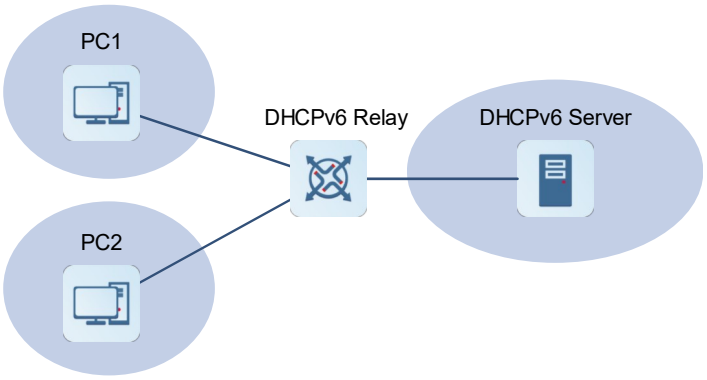
(2) The DHCPv6 server sends a REPLY message containing the configuration parameters to the DHCPv6 client.

(3) The DHCPv6 client checks whether information provided in the REPLY message is consistent with configuration parameters requested in the INFORMATION-REQUEST message. If yes, the DHCPv6 client performs network configuration based on parameters provided in the REPLY message. Otherwise, it ignores the message. If the DHCPv6 client receives multiple REPLY messages that match the request, the DHCPv6 client completes stateless configuration based on parameters provided in the first received REPLY message.

1.2.6 DHCPv6 Relay Agent

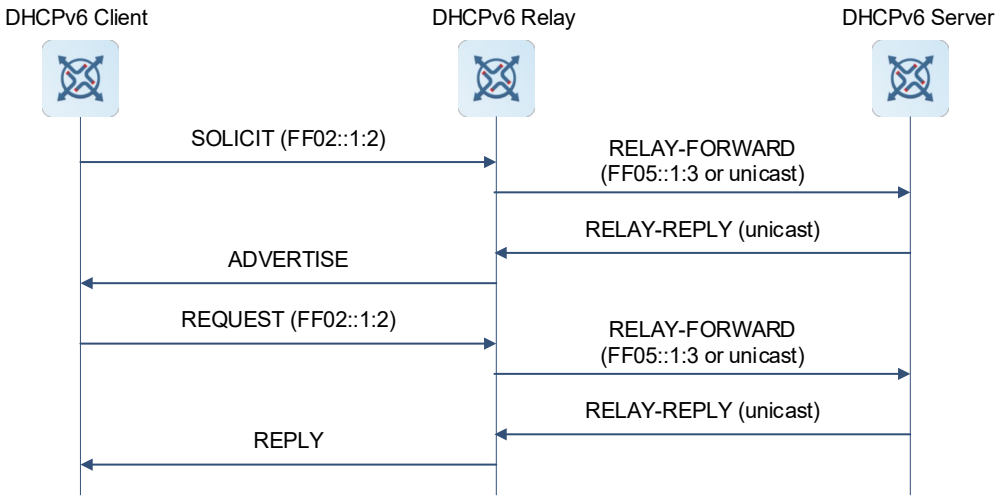
A DHCPv6 client usually discovers a DHCPv6 server by sending Solicit packets with a multicast address as the destination address. Therefore, the DHCPv6 client and DHCPv6 server must be able to directly communicate with each other, that is, they must be deployed on the same link. This may cause inconvenience to management and upgrade and resource waste. The DHCPv6 relay agent function can solve these problems by enabling a DHCPv6 client to send packets to a DHCPv6 server on a different link. A DHCP relay agent is often deployed on the link where a DHCPv6 client resides. It is used to forward interaction packets between the DHCPv6 client and a DHCPv6 server. The DHCP relay agent is transparent to the DHCPv6 client.

Figure 1-1DHCPv6 Relay Agent



2. **Principles**

Figure 1-1Packet Exchange Among a DHCPv6 Client, DHCPv6 Relay Agent, and DHCPv6 Server



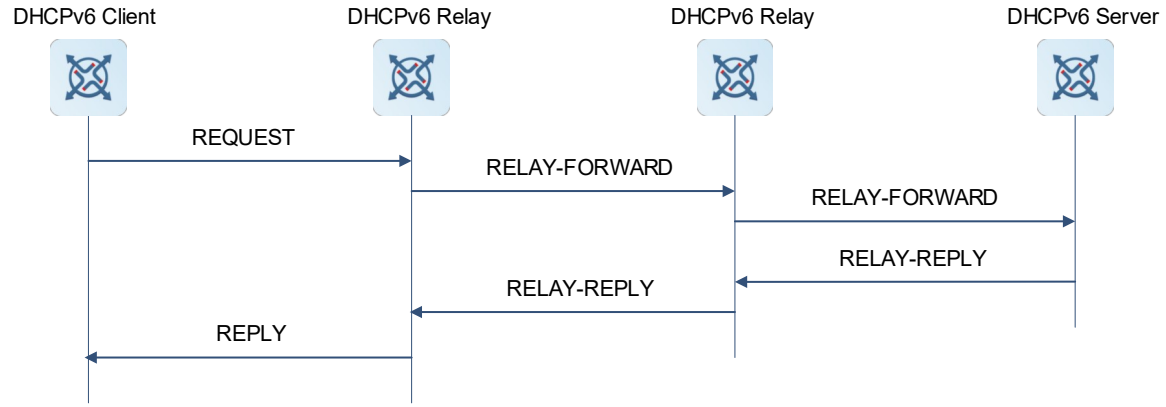
(1) When receiving a SOLICIT or REQUEST message from the DHCPv6 client, a DHCPv6 relay agent creates a RELAY-FORWARD message. This message contains the original message from the DHCPv6 client and some options added by the relay agent. Then, the DHCP relay agent sends the RELAY-FORWARD message to a specified DHCPv6 server or a specific multicast address FF05::1:3.

(2) After receiving the RELAY-FORWARD message, the DHCPv6 server extracts the original message for processing. Then, the DHCPv6 server constructs a response to the original message, encapsulates the response in a RELAY-REPLY message, and sends the RELAY-REPLY message to the DHCPv6 relay agent.

(3) After receiving the RELAY-REPLY message, the DHCPv6 relay agent extracts the original message from the DHCPv6 server and forwards it to the DHCPv6 client.

3. Multi-Level DHCPv6 Relay Agents

Figure 1-1Multi-Level DHCPv6 Relay Agents



A DHCPv6 relay agent encapsulates and decapsulates messages between a DHCPv6 client and a DHCPv6 server on different links to enable communication between them. Multi-level relay agents are allowed between a DHCPv6 client and a DHCPv6 server.

4. Options Supported by a DHCPv6 Relay Agent

- Interface-ID (Option 18)

  A DHCPv6 relay agent can use **Interface-ID** to identify the interface that receives messages from the client. A DHCPv6 server configures parameters based on the value of **Interface-ID** and copies **Interface-ID** to the RELAY-REPLY message to be sent to the DHCPv6 relay agent. After receiving the RELAY-REPLY message, the DHCPv6 relay agent forwards the message through the interface identified by **Interface-ID**. **Interface-ID** exists only in RELAY-FORWARD and RELAY-REPLY packets.

- Remote-ID (Option 37)

  A DHCPv6 relay agent can use **Remote-ID** to carry the DUID, port, and virtual local area network (VLAN) information. Based on the value of **Remote-ID**, a DHCPv6 server performs address assignment, parameter configuration, and prefix delegation.

- Subscriber-ID (Option 38)

  A DHCPv6 relay agent can use **Subscriber-ID** to carry a client's MAC address and other physical information. Based on the value of **Subscriber-ID**, a DHCPv6 server performs address assignment, parameter configuration, and prefix delegation.

1.2.7 Address Advertisement

A DHCPv6 server advertises a client's IPv6 address and MAC address to the authentication module for auditing.

In a subnet without a DHCPv6 relay, a DHCPv6 server can be configured with the IA_NA address assignment and advertisement functions. When receiving a DHCPv6 packet from a DHCPv6 client, the DHCPv6 server can identify the client's MAC address based on the source MAC address in the packet. When assigning an IPv6 address to the client or renewing the lease of this address, the DHCPv6 server advertises the MAC address and IPv6 address to the authentication module. The authentication module integrates the address information with IPv4 authentication information of the client and synchronizes the information to the authentication server. The authentication server authenticates or records the client based on the information.

1.2.8 Protocols and Standards

- RFC 3315: Dynamic Host Configuration Protocol for IPv6
- RFC 3633: IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) Version 6
- RFC 3646: DNS Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 3736: Stateless DHCP Service for IPv6
- RFC 5417: Control And Provisioning of Wireless Access Points (CAPWAP) Access Controller DHCP Option

1.3 Restrictions and Guidelines

- To provide the DHCPv6 service, specify a DHCPv6 address pool.
- The DHCPv6 service can be configured only on a Switch Virtual Interface (SVI), L3 Ethernet interface, or L3 aggregate port (AP).

1.4 Configuration Task Summary

DHCPv6 configuration includes the following tasks:

- Configuring the DHCPv6 server

a Configuring the DHCPv6 Server to Assign Addresses

b (Optional) Configuring the DHCPv6 Server to Assign Other Network Parameters

c

- Configuring the DHCPv6 relay

  a Configuring the DHCPv6 Relay

d (Optional) Configuring Source Interface Designation Function on a DHCPv6 Relay Agent

1.5 Configuring the DHCPv6 Server to Assign Addresses

1.5.1 Overview

Configure the device as a DHCPv6 server to assign IPv6 addresses or prefixes to DHCPv6 clients.

1.5.2 Configuration Tasks

(1) Configuring the DHCPv6 Server to Assign Addresses Perform either of the following configuration tasks.

- Configuring the IA_NA Address Prefix to Be Assigned from a DHCPv6 Server to a DHCPv6 Client
- Configuring the Prefix of a Statically Bound Address to Be Assigned from a DHCPv6 Server to a DHCPv6 Client
- Configuring a DCHPv6 Server to Assign Prefixes from a Local Prefix Pool

(2) (Optional) Configuring Excluded Addresses on a DHCPv6 Server

(3) Enabling the DHCPv6 Server Service

1.5.3 Configuring the IA_NA Address Prefix to Be Assigned from a DHCPv6 Server to a DHCPv6 Client

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a DHCPv6 address pool and enter the DHCPv6 address pool configuration mode.

ipv6 dhcp pool *pool-name*

No DHCPv6 address pool is configured by default.

(4) Configure the IA_NA address prefix to be assigned from a DHCPv6 server to a DHCPv6 client.

iana-address prefix *ipv6-address/prefix-length* [**lifetime** { *valid-lifetime* | **infinite** } { *preferred-lifetime* | **infinite** } }]

No IA_NA address prefix is configured by default.

1.5.4 Configuring the Prefix of a Statically Bound Address to Be Assigned from a DHCPv6 Server to a DHCPv6 Client

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a DHCPv6 address pool and enter the DHCPv6 address pool configuration mode.

ipv6 dhcp pool *pool-name*

No DHCPv6 address pool is configured by default.

(4) Configure the prefix of a statically bound address to be assigned from a DHCPv6 server to a DHCPv6 client.

prefix-delegation *ipv6-address/prefix-length client*-DUID [**lifetime** { *valid-lifetime* | **infinite** } { *preferred-lifetime* | **infinite** }]

No static address prefix is configured by default.

1.5.5 Configuring a DCHPv6 Server to Assign Prefixes from a Local Prefix Pool

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a local prefix pool for the PD service of a DHCPv6 server.

ipv6 local pool *pool-name prefix*/*prefix-length assigned-length*

No local prefix pool is configured for the PD service of a DHCPv6 server by default.

(4) Create a DHCPv6 address pool and enter the DHCPv6 address pool configuration mode.

ipv6 dhcp pool *pool-name*

(5) Configure the local prefix pool associated with the DHCPv6 server.

prefix-delegation pool *pool-name* [**lifetime** { *valid-lifetime* | **infinite** } { *preferred-lifetime* | **infinite** }]

No local prefix pool associated with the DHCPv6 server is configured by default.

1.5.6 Configuring Excluded Addresses on a DHCPv6 Server

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create a DHCPv6 address pool and enter the DHCPv6 address pool configuration mode.

ipv6 dhcp pool *pool-name*

No DHCPv6 address pool is configured by default.

(4) Configure excluded addresses on a DHCPv6 server.

excluded-address *start-ipv6-address* [*end-ipv6-address*]

No excluded address is configured on a DHCPv6 server by default.

1.5.7 Enabling the DHCPv6 Server Service

(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 DHCPv6 Server service.

ipv6 dhcp server *pool-name* [**rapid-commit**] [**preference** *preference-value*]

The DHCPv6 Server service is disabled by default.

1.6 Configuring the DHCPv6 Server to Assign Other Network Parameters

1.6.1 Overview

A DHCPv6 server can automatically assign configuration parameters, such as the DNS address, domain name, boot file, and Option 52 to DHCPv6 clients.

The DHCPv6 server uses Option 52 to specify the IPv6 address of a Control and Provisioning of Wireless Access Points (CAPWAP) access controller (AC).

1.6.2 Configuration Tasks

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

- Configuring the DNS Address to Be Assigned from a DHCPv6 Server to a DHCPv6 Client
- Configuring the Domain Name to Be Assigned from a DHCPv6 Server to a DHCPv6 Client
- Configuring the Boot File URL to Be Assigned from a DHCPv6 Server to a DHCPv6 Client
- Configuring Option 52 on a DHCPv6 Server

1.6.3 Configuring the DNS Address to Be Assigned from a DHCPv6 Server to a DHCPv6 Client

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the DHCPv6 address pool configuration mode.

ipv6 dhcp pool *pool-name*

No DHCPv6 address pool is configured by default.

(4) Configure the DNS address to be assigned from a DHCPv6 server a DHCPv6 client.

dns-server *ipv6-address*

No DNS address is configured by default.

1.6.4 Configuring the Domain Name to Be Assigned from a DHCPv6 Server to a DHCPv6 Client

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the DHCPv6 address pool configuration mode.

ipv6 dhcp pool *pool-name*

No DHCPv6 address pool is configured by default.

(4) Configure the domain name to be assigned from a DHCPv6 to a DHCPv6 client.

domain-name *domain*

No domain name is configured by default.

1.6.5 Configuring the Boot File URL to Be Assigned from a DHCPv6 Server to a DHCPv6 Client

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the DHCPv6 address pool configuration mode.

ipv6 dhcp pool *pool-name*

No DHCPv6 address pool is configured by default.

(4) Configure the boot file Uniform Resource Locator (URL) to be assigned from a DHCPv6 server to a DHCPv6 client.

bootfile-url *url-string*

No boot file URL is configured by default.

1.6.6 Configuring Option 52 on a DHCPv6 Server

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the DHCPv6 address pool configuration mode.

ipv6 dhcp pool *pool-name*

No DHCPv6 address pool is configured by default.

(4) Configure Option 52 on a DHCPv6 server.

option52 *ipv6-address*

Option 52 is not configured on a DHCPv6 server by default.

1.7 Configuring the DHCPv6 Relay

1.7.1 Overview

A DHCPv6 relay agent can be configured for address assignment, prefix delegation, and parameter allocation between a DHCPv6 client and a DHCPv6 server on different links.

1.7.2 Restrictions and Guidelines

A destination address must be configured for the device with the DHCPv6 relay function enabled. If the destination address is a multicast address (such as FF05::1:3), an egress interface needs to be configured.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Configure the format of **Interface-ID** on a DHCPv6 relay agent.

ipv6 dhcp relay option interface-id format user-defined *text*

The interface name is specified in **Interface-ID** on a DHCPv6 relay agent by default.

(4) (Optional) Configure the format of the MAC address in user-defined options on a DHCPv6 relay agent.

ipv6 dhcp relay option mac-str-format *type*

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

(5) (Optional) Add **the Remote-ID** to DHCPv6 relay packets.

ipv6 dhcp relay option remote-id enable

DHCPv6 relay packets do not carry **Remote-ID** by default.

(6) (Optional) Configure the format of **Remote-ID** in DHCPv6 relay packets.

ipv6 dhcp relay option remote-id format user-defined *text*

The device DUID is specified for **Remote-ID** in DHCPv6 relay packets by default.

(7) Enter the interface configuration mode.

interface *interface-type interface-number*

(8) Enable the DHCPv6 Relay function.

ipv6 dhcp relay destination [**vrf** *vrf-name*] *ipv6-address* [*interface-type interface-number*]

The DHCPv6 Relay function is disabled by default. No destination address or interface over which packets are routed to the destination address is configured.

1.8 Configuring Source Interface Designation Function on a DHCPv6 Relay Agent

1.8.1 Overview

In some device redundancy scenarios, a DHCPv6 server regards uplink interface IP addresses of multiple DHCPv6 relay agents as one IP address. As a result, the DHCPv6 server cannot identify unique DHCPv6 relay agents by their uplink interface IP addresses. The source interface can be designated to differentiate between different DHCPv6 relay agents to ensure normal packet forwarding.

The source interface designation function allows designating an IP address or interface. When a DHCPv6 relay agent forwards a RELAY-FORWARD packet to a DHCPv6 server, specified information is filled in the source IP address and link address fields of the RELAY-FORWARD packet but the destination IP address is still the IP address of the DHCPv6 server. After receiving the RELAY-FORWARD packet, the DHCPv6 server records the source IP address of the packet and uses it as the destination address of the RELAY-REPLY packet. That is, the response packet is destined for the IP address or interface specified by using the source

interface designation function of the relay agent, so as to bypass the uplink interface of the DHCPv6 relay agent.

1.8.2 Restrictions and Guidelines

The source interface designation function can be configured in global configuration mode and interface configuration mode. The source interface designation type in interface configuration mode is prior to that in global configuration mode. In one configuration mode, the last configured source interface designation type prevails.

1.8.3 Procedure (Global Configuration Mode)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the source interface designation function.

ipv6 dhcp relay source { **source-ip-address** | **gateway-address** } { *ipv6-address* | *interface-type interface-number* }

The source interface designation function is not configured by default.

1.8.4 Procedure (Interface Configuration Mode)

(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 interface designation function.

ipv6 dhcp relay source { **source-ip-address** | **gateway-address** } { *ipv6-address* | *interface-type interface-number* }

The source interface designation function is not configured by default.

1.9 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

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

Caution

The output 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 ipv6 dhcp binding [*ipv6-address*]	Clears bindings on a DHCPv6 server.
clear ipv6 dhcp server statistics	Clears statistics of different types of packets on a DHCPv6 server.
clear ipv6 dhcp conflict { *ipv6-address* | * }	Clears conflicted addresses on a DHCPv6 server.
clear ipv6 dhcp relay statistics	Clears statistics of different types of packets on a DHCPv6 relay agent.
show ipv6 dhcp	Displays the DUID of a DHCPv6 device.
show ipv6 dhcp binding [*ipv6-address*]	Displays address bindings on a DHCPv6 server.
show ipv6 dhcp interface [*interface-type interface-number*]	Displays interfaces on a DHCPv6 server.
show ipv6 dhcp pool [*pool-name*]	Displays address pools on a DHCPv6 server.
show ipv6 dhcp conflict	Displays conflicted addresses on a DHCPv6 server.
show ipv6 dhcp server statistics	Displays DHCPv6 server statistics.
show ipv6 dhcp relay agent { *ipv6-address* | * }	Displays source interfaces on a DHCPv6 relay agent.
show ipv6 dhcp relay destination { **all** | *interface-type interface-number* }	Displays destination addresses on a DHCPv6 relay agent.
show ipv6 dhcp relay source	Displays the source interface designation configuration on a DHCPv6 relay agent.
show ipv6 dhcp relay statistics	Displays statistics of different types of packets on a DHCPv6 relay agent.
show ipv6 local pool [*pool-name*]	Displays local prefix pool configurations and usage on a device.
debug ipv6 dhcp [**detail**]	Debugs DHCPv6.
debug ipv6 dhcp relay	Debugs a DHCPv6 relay agent.
debug ipv6 dhcp server	Debugs a DHCPv6 server.

1.10 Configuration Examples

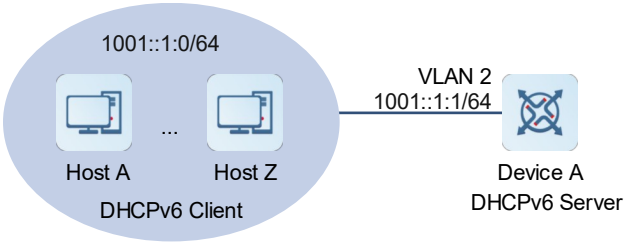
1.10.1 Dynamically Assigning IPv6 Addresses

1. **Requirements**

As shown in Figure 1-1, a DHCPv6 client in network segment 1001::1:0/64 requests address information from a DHCPv6 server (Device A) in the same subnet. Assignable IPv6 addresses, DNS address, domain name, and other configuration parameters are configured on the DHCPv6 server.

2. **Topology**

Figure 1-1Dynamically Assigning IPv6 Addresses



3. Notes

Run the DHCPv6 server on Device A and configure addresses and other parameters for automatic address and parameter assignment.

4. **Procedure**

(1) Configure Device A:

Configure DHCPv6 address pool parameters.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ipv6 dhcp pool v6
DeviceA(dhcp-config)# iana-address prefix 1001::1:0/64
DeviceA(dhcp-config)# excluded-address 1001::1:1 1001::1:2
DeviceA(dhcp-config)# dns-server 1001::1:2
DeviceA(dhcp-config)# domain-name example.com
```

Configure an interface address and enable the DHCPv6 Server service.

```
DeviceA(config)# interface vlan 2
DeviceA(config-if-VLAN 2)# ipv6 enable
DeviceA(config-if-VLAN 2)# ipv6 address 1001::1:1/64
DeviceA(config-if-VLAN 2)# ipv6 dhcp server v6
```

Cancel suppression of RA messages released on the device.

```
DeviceA(config-if-VLAN 2)# no ipv6 nd suppress-ra
```

Set the configuration flag of managed addresses to **1**, that is, enable hosts to obtain IPv6 addresses from the DHCPv6 server.

```
DeviceA(config-if-VLAN 2)# ipv6 nd managed-config-flag
```

Set the configuration flags of other information to **1**, that is, enable hosts to obtain other information except IPv6 addresses from the DHCPv6 server.

```
DeviceA(config-if-VLAN 2)# ipv6 nd other-config-flag
```

(2) Configure the hosts:

Enable the dynamic address acquisition function. (Omitted)

5. **Verification**

Check whether the clients have applied for IPv6 addresses in network segment 1001::1:0/64.

6. **Configuration Files**

Device A configuration file

```
hostname DeviceA
!
 ipv6 dhcp pool v6
 iana-address prefix 1001::1:0/64
 excluded-address 1001::1:1 1001::1:2
 dns-server 1001::1:2
 domain-name example.com
!
 interface vlan 2
 ipv6 address 1001::1:1/64
 ipv6 dhcp server v6
!
```

7. **Common Errors**

- The address pool name exceeds 256 characters.
- The number of configured address pools exceeds 256.
- The number of interfaces configured with the DHCPv6 Server service exceeds 256.
- The number of configured DNS addresses exceeds 10.
- The number of configured domain names exceeds 10.

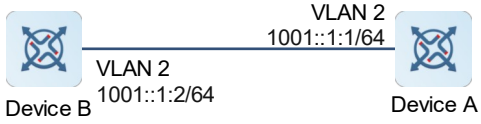
1.10.2 Dynamically Assigning IPv6 Address Prefixes

1. **Requirements**

As shown in Figure 1-1, Device B is a DHCPv6 client and requests an IPv6 address prefix (2001::1/64), DNS address, domain name, and other network parameters from Device A (a DHCPv6 server).

2. **Topology**

Figure 1-1Dynamically Assigning IPv6 Address Prefixes



3. Notes

- Run the DHCPv6 Server service and the PD service on Device A.
- Enable the DHCPv6 Client service on Device B.
- Deploy IPv6 neighbor discovery (ND) between the server and the client to configure host addresses in the subnet through RA messages.

4. Procedure

(1) Configure Device A:

Configure a prefix pool.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)#ipv6 local pool myprefix 2001::1/64 64
```

Configure DHCPv6 address pool parameters and associate it with the prefix pool.

```
DeviceA(config)# ipv6 dhcp pool v6_pd
DeviceA(dhcp-config)# dns-server 1001::1:2
DeviceA(dhcp-config)# domain-name example.com
DeviceA(dhcp-config)# prefix-delegation pool myprefix
DeviceA(dhcp-config)# exit
```

Configure an interface address and enable the DHCPv6 Server service.

```
DeviceA(config)# interface vlan 2
DeviceA(config-if-VLAN 2)# ipv6 enable
DeviceA(config-if-VLAN 2)# ipv6 address 1001::1:1/64
DeviceA(config-if-VLAN 2)# ipv6 dhcp server v6_pd
```

Cancel suppression of RA messages released on the device.

```
DeviceA(config-if-VLAN 2)# no ipv6 nd suppress-ra
```

Set the configuration flag of managed addresses to **1**, that is, enable hosts to obtain IPv6 addresses from the DHCPv6 server.

```
DeviceA(config-if-VLAN 2)# ipv6 nd managed-config-flag
```

Set the configuration flags of other information to **1**, that is, enable hosts to obtain other information except IPv6 addresses from the DHCPv6 server.

```
DeviceA(config-if-VLAN 2)# ipv6 nd other-config-flag
```

(2) Configure Device B:

Configure an interface address.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface vlan 2
DeviceB(config-if-VLAN 2)# ipv6 enable
DeviceB(config-if-VLAN 2)# ipv6 address 1001::1:2/64
```

Enable the DHCPv6 Client service and request address/prefix information from the DHCPv6 server.

```
DeviceB(config-if-VLAN 2)# ipv6 dhcp client pd mypd
```

5. **Verification**

Check whether the DHCPv6 Server function is enabled on VLAN 2 of Device A.

```
DeviceA# show ipv6 dhcp interface
VLAN 2 is in server mode
  Server pool: v6_pd
  Rapid-Commit: disable
```

Check whether the DHCPv6 Client function is enabled on VLAN 2 of Device B.

```
DeviceB# show ipv6 dhcp interface
VLAN 2 is in client mode
  State is IDLE
  next packet will be send in : 43049 seconds
  List of known servers:
    DUID: 00:03:00:01:00:50:56:b0:05:98
    Reachable via address: ::
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x2, T1 43200, T2 69120
        Prefix: 2001::/64
          preferred lifetime 86400, valid lifetime 86400
          expires at Jan 15 2020 16:0 (86249 seconds)
  Prefix name: mypd
  DNS server: 1001::1:2
  Domain name: example.com
  Rapid-Commit: disable
```

Check the common prefix of Device B.

```
DeviceB# show ipv6 general-prefix
There is 1 general prefix.
IPv6 general prefix mypd, acquired via DHCP Prefix Discovery
  2001::/64 valid lifetime 86368, preferred lifetime 86368
```

6. **Configuration Files**

- Device A configuration file

```
hostname DeviceA
!
 ipv6 local pool myprefix 2001::1/64 64
!
 ipv6 dhcp pool v6_pd
 dns-server 1001::1:2
 domain-name example.com
 prefix-delegation pool myprefix
!
 interface vlan 2
 ipv6 address 1001::1:1/64
 ipv6 dhcp server v6_pd
```

```
 no ipv6 nd suppress-ra
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
!
```

- Device B configuration file

```
hostname DeviceB
!
 interface vlan 2
 ipv6 address 1001::1:2/64
 ipv6 dhcp client pd mypd
!
```

7. **Common Errors**

- The specified address pool name is too long.
- The number of configured address pools exceeds 256.
- The configuration is performed on other interfaces than a SVI, routing port, or L3 AP.
- The number of interfaces configured with the DHCPv6 Server service exceeds 256.
- The number of configured DNS addresses exceeds 10.
- The number of configured domain names exceeds 10.

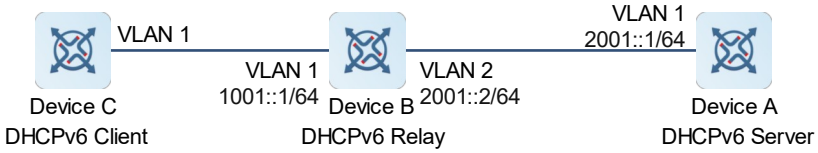
1.10.3 Configuring DHCP Relay

1. **Requirements**

As shown in Figure 1-1, Device C (a DHCPv6 client) is in network segment 1001::/64, and the address of Device A (a DHCPv6 server) is 2001::1/64. Device B (a DHCPv6 relay agent) provides the relay service for the DHCPv6 client and DHCPv6 server on different links to enable communication between them.

2. **Topology**

Figure 1-1Configuring DHCPv6 Relay



3. **Notes**

- Enable the DHCPv6 Server function on Device A and configure addresses and other parameters.
- Enable the DHCPv6 Relay function on Device B with the destination address pointed to VLAN 1 on Device A.
- Enable the DHCPv6 Client function on Device C.

4. **Procedure**

(1) Configure Device A:

Configure DHCPv6 address pool parameters.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ipv6 dhcp pool v6
DeviceA(dhcp-config)# iana-address prefix 1001::/64
DeviceA(dhcp-config)# excluded-address 1001::1 1001::2
DeviceA(dhcp-config)# dns-server 1001::2
DeviceA(dhcp-config)# domain-name example.com
```

Configure an interface address and enable the DHCPv6 Server service.

```
DeviceA(config)# interface vlan 1
DeviceA(config-if-VLAN 1)# ipv6 enable
DeviceA(config-if-VLAN 1)# ipv6 address 2001::1/64
DeviceA(config-if-VLAN 1)# ipv6 dhcp server v6
```

Cancel suppression of RA messages released on the device.

```
DeviceA(config-if-VLAN 1)# no ipv6 nd suppress-ra
```

Set the configuration flag of managed addresses to **1**, that is, enable hosts to obtain IPv6 addresses from the DHCPv6 server.

```
DeviceA(config-if-VLAN 1)# ipv6 nd managed-config-flag
```

Set the configuration flags of other information to **1**, that is, enable hosts to obtain other information except IPv6 addresses from the DHCPv6 server.

```
DeviceA(config-if-VLAN 1)# ipv6 nd other-config-flag
```

(2) Configure Device B:

Configure an uplink interface address.

```
DeviceB> enable
DeviceB#configure terminal
DeviceB(config)# interface vlan 2
DeviceB(config-if-VLAN 2)# ipv6 enable
DeviceB(config-if-VLAN 2)# ipv6 address 2001::2/64
DeviceB(config-if-VLAN 2)# exit
```

Configure a downlink interface address and enable the DHCPv6 Relay function.

```
DeviceB(config)#interface vlan 1
DeviceB(config-if-VLAN 1)# ipv6 enable
DeviceB(config-if-VLAN 1)# ipv6 address 1001::1/64
DeviceB(config-if-VLAN 1)# ipv6 dhcp relay destination 2001::2
```

(3) Configure Device C:

Enable the DHCPv6 Client function to apply for an IP address.

```
DeviceC> enable
DeviceC# configure terminal
DeviceC(config)#interface vlan 1
DeviceC(config-if-VLAN 1)#ipv6 dhcp client ia
```

5. **Verification**

Check whether Device C has applied for an IPv6 address in network segment 1001::/64.

```
DeviceC# show ipv6 interface

interface VLAN 1 is Up, ifindex: 2, vrf_id 0
  address(es):
    Mac Address: 00:50:56:b0:2f:50
    INET6: 1001::3 [ TENTATIVE ], subnet is 1001::/64
      valid lifetime 86400 sec, preferred lifetime 86400 sec
  Joined group address(es):
    FF01::1
    FF02::1
    FF02::2
    FF02::1:FF00:0
    FF02::1:FF00:3
    FF02::1:FFB0:2F50
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND stale time is 3600 seconds
  ND advertised reachable time is 0 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 600 seconds<480--720>
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
```

6. **Configuration Files**

- Device A configuration file

```
hostname DeviceA
!
 ipv6 dhcp pool v6
 iana-address prefix 1001::/64
 excluded-address 1001::1 1001::2
 dns-server 1001::2
 domain-name example.com
!
 interface vlan 1
 ipv6 address 2001::1/64
 ipv6 dhcp server v6
 no ipv6 nd suppress-ra
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
```

```
!
```

- Device B configuration file

```
hostname DeviceB
!
 interface vlan 2
 ipv6 enable
 ipv6 address 2001::2/64
!
 interface vlan 1
 ipv6 address 1001::1/64
 ipv6 dhcp relay destination 2001::2
!
```

- Device C configuration file

```
hostname DeviceC
!
 interface vlan 1
 ipv6 dhcp client ia
!
```