

# Contents

DHCPv6 overview.....	1
DHCPv6 address/prefix assignment .....	1
Rapid assignment involving two messages .....	1
Assignment involving four messages.....	1
Address/prefix lease renewal.....	2
Stateless DHCPv6 .....	3
DHCPv6 options.....	3
Option 18.....	3
Option 37.....	4
Protocols and standards .....	5
Configuring the DHCPv6 server.....	6
About DHCPv6 server.....	6
IPv6 address assignment.....	6
IPv6 prefix assignment.....	6
Concepts.....	7
DHCPv6 address pool.....	7
IPv6 address/prefix allocation sequence.....	8
DHCPv6 server tasks at a glance .....	9
Configuring IPv6 prefix assignment .....	9
Configuring IPv6 address assignment .....	11
Configuring network parameters assignment .....	12
About network parameters assignment.....	12
Configuring network parameters in a DHCPv6 address pool.....	13
Configuring network parameters in a DHCPv6 option group .....	13
Configuring the DHCPv6 server on an interface.....	14
Configuring a DHCPv6 policy for IPv6 address and prefix assignment.....	15
Setting the DSCP value for DHCPv6 packets sent by the DHCPv6 server .....	16
Configuring DHCPv6 binding auto backup.....	16
Enabling the DHCPv6 server to advertise IPv6 prefixes.....	17
Applying a DHCPv6 address pool to a VPN instance.....	17
Enabling DHCPv6 logging on the DHCPv6 server.....	18
Display and maintenance commands for DHCPv6 server.....	18
DHCPv6 server configuration examples .....	19
Example: Configuring dynamic IPv6 prefix assignment .....	19
Example: Configuring dynamic IPv6 address assignment.....	22
Configuring the DHCPv6 relay agent.....	24
About DHCPv6 relay agent.....	24
Typical application.....	24
DHCPv6 relay agent operating process.....	24
DHCPv6 relay agent tasks at a glance .....	25
Enabling the DHCPv6 relay agent on an interface .....	25
Specifying DHCPv6 servers on the relay agent.....	26
Specifying DHCPv6 server IP addresses.....	26
Specifying DHCPv6 servers for a DHCPv6 address pool on the DHCPv6 relay agent .....	26
Specifying a gateway address for DHCPv6 clients.....	27
Setting the DSCP value for DHCPv6 packets sent by the DHCPv6 relay agent .....	27
Specifying a padding mode for the Interface-ID option.....	28
Enabling the DHCPv6 relay agent to advertise IPv6 prefixes.....	28
Specifying the source IPv6 address for relayed DHCPv6 requests.....	28
Display and maintenance commands for DHCPv6 relay agent.....	29
DHCPv6 relay agent configuration examples .....	30
Example: Configuring DHCPv6 relay agent.....	30
Configuring the DHCPv6 client .....	32
About the DHCPv6 client .....	32

Restrictions and guidelines: DHCPv6 client configuration .....	32
DHCPv6 client tasks at a glance .....	32
Configuring the DHCPv6 client DUID .....	32
Configuring IPv6 address acquisition .....	33
Configuring IPv6 prefix acquisition .....	33
Configuring IPv6 address and prefix acquisition .....	33
Configuring acquisition of configuration parameters except IP addresses and prefixes .....	34
Setting the DSCP value for DHCPv6 packets sent by the DHCPv6 client .....	34
Display and maintenance commands for DHCPv6 client .....	35
DHCPv6 client configuration examples .....	35
Example: Configuring IPv6 address acquisition .....	35
Example: Configuring IPv6 prefix acquisition .....	37
Example: Configuring IPv6 address and prefix acquisition .....	38
Example: Configuring stateless DHCPv6 .....	40
<b>Configuring DHCPv6 snooping .....</b>	<b>43</b>
About DHCPv6 snooping .....	43
Application of trusted and untrusted ports .....	43
Restrictions and guidelines: DHCPv6 snooping configuration .....	44
DHCPv6 snooping tasks at a glance .....	44
Configuring basic DHCPv6 snooping features .....	45
Configuring basic DHCPv6 snooping features in a common network .....	45
Configuring DHCP snooping support for Option 18 .....	45
Configuring DHCP snooping support for Option 37 .....	46
Configuring DHCPv6 snooping entry auto backup .....	46
Setting the maximum number of DHCPv6 snooping entries .....	47
Configuring DHCPv6 packet rate limit .....	47
Enabling DHCPv6-REQUEST check .....	48
Configuring a DHCPv6 packet blocking port .....	48
Enabling DHCPv6 snooping logging .....	49
Display and maintenance commands for DHCPv6 snooping .....	49
DHCPv6 snooping configuration examples .....	50
Example: Configuring DHCPv6 snooping .....	50

# DHCPv6 overview

DHCPv6 provides a framework to assign IPv6 prefixes, IPv6 addresses, and other configuration parameters to hosts.

## DHCPv6 address/prefix assignment

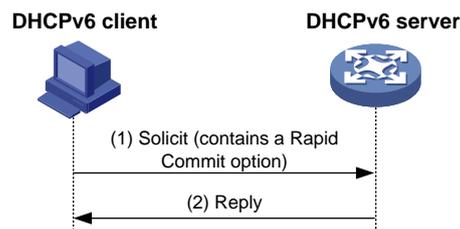
An address/prefix assignment process involves two or four messages.

### Rapid assignment involving two messages

As shown in [Figure 1](#), rapid assignment operates in the following steps:

1. The DHCPv6 client sends to the DHCPv6 server a Solicit message that contains a Rapid Commit option to prefer rapid assignment.
2. If the DHCPv6 server supports rapid assignment, it responds with a Reply message containing the assigned IPv6 address/prefix and other configuration parameters. If the DHCPv6 server does not support rapid assignment, [Assignment involving four messages](#) is performed.

**Figure 1 Rapid assignment involving two messages**

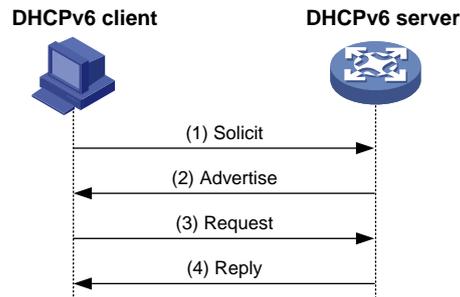


### Assignment involving four messages

As shown in [Figure 2](#), four-message assignment operates using the following steps:

1. The DHCPv6 client sends a Solicit message to request an IPv6 address/prefix and other configuration parameters.
2. The DHCPv6 server responds with an Advertise message that contains the assignable address/prefix and other configuration parameters if either of the following conditions exists:
  - o The Solicit message does not contain a Rapid Commit option.
  - o The DHCPv6 server does not support rapid assignment even though the Solicit message contains a Rapid Commit option.
3. The DHCPv6 client might receive multiple Advertise messages offered by different DHCPv6 servers. It selects an offer according to the receiving sequence and server priority, and sends a Request message to the selected server for confirmation.
4. The DHCPv6 server sends a Reply message to the client, confirming that the address/prefix and other configuration parameters are assigned to the client.

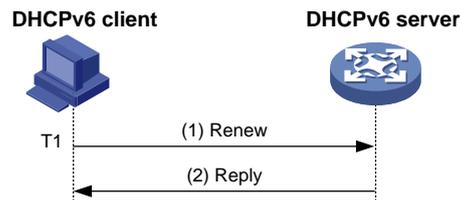
**Figure 2 Assignment involving four messages**



## Address/prefix lease renewal

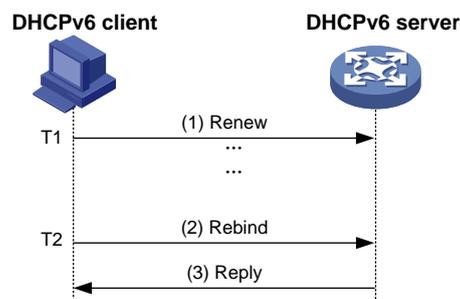
An IPv6 address/prefix assigned by a DHCPv6 server has a valid lifetime. After the valid lifetime expires, the DHCPv6 client cannot use the IPv6 address/prefix. To use the IPv6 address/prefix, the DHCPv6 client must renew the lease time.

**Figure 3 Using the Renew message for address/prefix lease renewal**



As shown in [Figure 3](#), at T1, the DHCPv6 client sends a Renew message to the DHCPv6 server. The recommended value of T1 is half the preferred lifetime. The DHCPv6 server responds with a Reply message, informing the client whether the lease is renewed.

**Figure 4 Using the Rebind message for address/prefix lease renewal**



As shown in [Figure 4](#):

- If the DHCPv6 client does not receive a response from the DHCPv6 server after sending a Renew message at T1, it multicasts a Rebind message to all DHCPv6 servers at T2. Typically, the value of T2 is 0.8 times the preferred lifetime.
- The DHCPv6 server responds with a Reply message, informing the client whether the lease is renewed.
- If the DHCPv6 client does not receive a response from any DHCPv6 server before the valid lifetime expires, the client stops using the address/prefix.

For more information about the valid lifetime and the preferred lifetime, see "Configuring basic IPv6 settings."

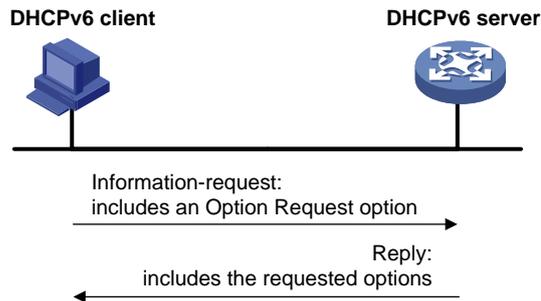
# Stateless DHCPv6

Stateless DHCPv6 enables a device that has obtained an IPv6 address/prefix to get other configuration parameters from a DHCPv6 server.

The device performs stateless DHCPv6 if an RA message with the following flags is received from the router during stateless address autoconfiguration:

- The managed address configuration flag (M flag) is set to 0.
- The other stateful configuration flag (O flag) is set to 1.

**Figure 5 Stateless DHCPv6 operation**



As shown in [Figure 5](#), stateless DHCPv6 operates in the following steps:

1. The DHCPv6 client sends an Information-request message to the multicast address of all DHCPv6 servers and DHCPv6 relay agents. The Information-request message contains an Option Request option that specifies the requested configuration parameters.
2. The DHCPv6 server returns to the client a Reply message containing the requested configuration parameters.
3. The client checks the Reply message. If the obtained configuration parameters match those requested in the Information-request message, the client uses these parameters to complete configuration. If not, the client ignores the configuration parameters. If the client receives multiple replies with configuration parameters matching those requested in the Information-request message, it uses the first received reply.

## DHCPv6 options

### Option 18

Option 18, also called the interface-ID option, is used by the DHCPv6 relay agent to determine the interface to use to forward RELAY-REPLY message.

The DHCPv6 snooping device adds Option 18 to the received DHCPv6 request message before forwarding it to the DHCPv6 server. The server then assigns IP address to the client based on the client information in Option 18.

**Figure 6 Option 18 format**

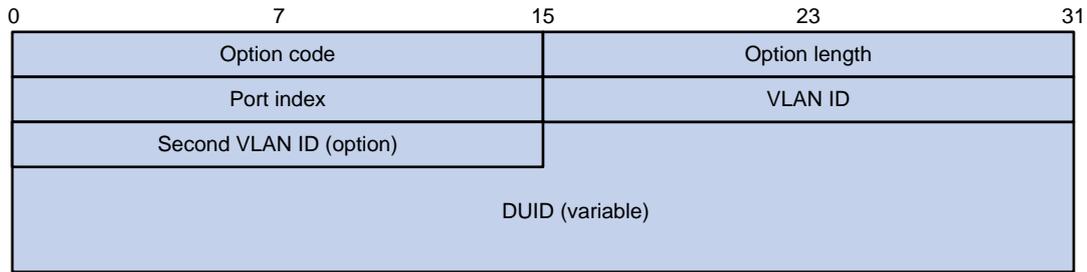


Figure 6 shows the Option 18 format, which includes the following fields:

- **Option code**—Option code. The value is 18.
- **Option length**—Size of the option data.
- **Port index**—Port that receives the DHCPv6 request from the client.
- **VLAN ID**—ID of the outer VLAN.
- **Second VLAN ID**—ID of the inner VLAN. This field is optional. If the received DHCPv6 request does not contain a second VLAN, Option 18 also does not contain it.
- **DUID**—DUID of the DHCPv6 client.

## Option 37

Option 37, also called the remote-ID option, is used to identify the client.

The DHCPv6 snooping device adds Option 37 to the received DHCPv6 request message before forwarding it to the DHCPv6 server. This option provides client information about address allocation.

**Figure 7 Option 37 format**

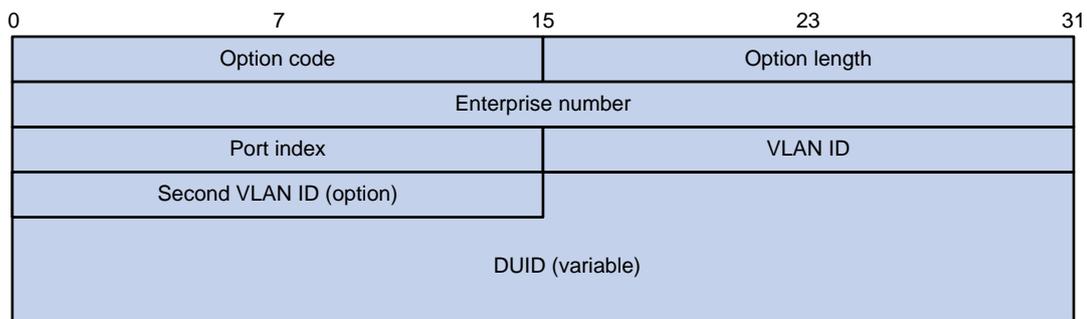


Figure 7 shows the Option 37 format, which includes the following fields:

- **Option code**—Option code. The value is 37.
- **Option length**—Size of the option data.
- **Enterprise number**—Enterprise number.
- **Port index**—Port that receives the DHCPv6 request from the client.
- **VLAN ID**—ID of the outer VLAN.
- **Second VLAN ID**—ID of the inner VLAN. This field is optional. If the received DHCPv6 request does not contain a second VLAN, Option 37 also does not contain it.
- **DUID**—DUID of the DHCPv6 client.

# Protocols and standards

- RFC 3736, *Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6*
- RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*
- RFC 2462, *IPv6 Stateless Address Autoconfiguration*
- RFC 3633, *IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*

# Configuring the DHCPv6 server

## About DHCPv6 server

A DHCPv6 server can assign IPv6 addresses, IPv6 prefixes, and other configuration parameters to DHCPv6 clients.

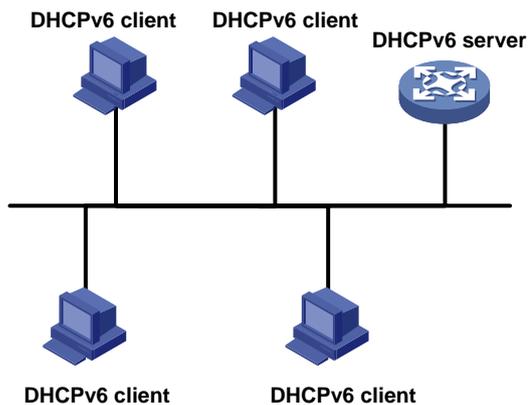
## IPv6 address assignment

As shown in [Figure 8](#), the DHCPv6 server assigns IPv6 addresses, domain name suffixes, DNS server addresses, and other configuration parameters to DHCPv6 clients.

The IPv6 addresses assigned to the clients include the following types:

- **Temporary IPv6 addresses**—Frequently changed without lease renewal.
- **Non-temporary IPv6 addresses**—Correctly used by DHCPv6 clients, with lease renewal.

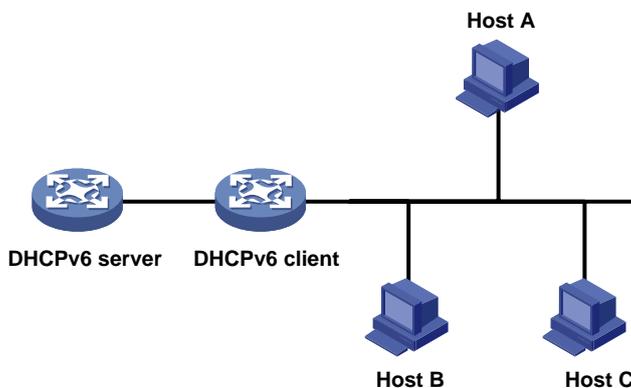
**Figure 8 IPv6 address assignment**



## IPv6 prefix assignment

As shown in [Figure 9](#), the DHCPv6 server assigns an IPv6 prefix to the DHCPv6 client. The client advertises the prefix information in a multicast RA message so that hosts on the subnet can automatically configure their IPv6 addresses by using the prefix.

**Figure 9 IPv6 prefix assignment**



# Concepts

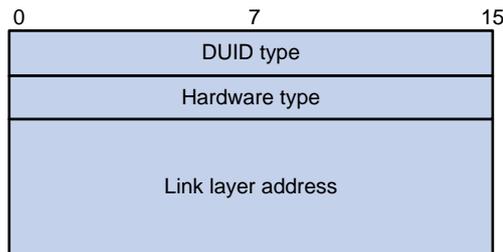
## Multicast addresses used by DHCPv6

DHCPv6 uses the multicast address FF05::1:3 to identify all site-local DHCPv6 servers. It uses the multicast address FF02::1:2 to identify all link-local DHCPv6 servers and relay agents.

## DUID

A DHCP unique identifier (DUID) uniquely identifies a DHCPv6 device (DHCPv6 client, server, or relay agent). A DHCPv6 device adds its DUID in a sent packet.

**Figure 10 DUID-LL format**



The device supports the DUID format based on link-layer address (DUID-LL) defined in RFC 3315. [Figure 10](#) shows the DUID-LL format, which includes the following fields:

- **DUID type**—The device supports the DUID type of DUID-LL with the value of 0x0003.
- **Hardware type**—The device supports the hardware type of Ethernet with the value of 0x0001.
- **Link layer address**—Takes the value of the bridge MAC address of the device.

## IA

Identified by an IAID, an identity association (IA) provides a construct through which a client manages the obtained addresses, prefixes, and other configuration parameters. A client can have multiple IAs, for example, one for each of its interfaces.

## IAID

An IAID uniquely identifies an IA. It is chosen by the client and must be unique on the client.

## PD

The DHCPv6 server creates a prefix delegation (PD) for each assigned prefix to record the following details:

- IPv6 prefix.
- Client DUID.
- IAID.
- Valid lifetime.
- Preferred lifetime.
- Lease expiration time.
- IPv6 address of the requesting client.

## DHCPv6 address pool

The DHCP server selects IPv6 addresses, IPv6 prefixes, and other parameters from an address pool, and assigns them to the DHCP clients.

## Address allocation mechanisms

DHCPv6 supports the following address allocation mechanisms:

- **Static address allocation**—To implement static address allocation for a client, create a DHCPv6 address pool, and manually bind the DUID and IAID of the client to an IPv6 address in the DHCPv6 address pool. When the client requests an IPv6 address, the DHCPv6 server assigns the IPv6 address in the static binding to the client.
- **Dynamic address allocation**—To implement dynamic address allocation for clients, create a DHCPv6 address pool, specify a subnet for the pool, and divide the subnet into temporary and non-temporary IPv6 address ranges. Upon receiving a DHCP request, the DHCPv6 server selects an IPv6 address from the temporary or non-temporary IPv6 address range based on the address type in the client request.

## Prefix allocation mechanisms

DHCPv6 supports the following prefix allocation mechanisms:

- **Static prefix allocation**—To implement static prefix allocation for a client, create a DHCPv6 address pool, and manually bind the DUID and IAID of the client to an IPv6 prefix in the DHCPv6 address pool. When the client requests an IPv6 prefix, the DHCPv6 server assigns the IPv6 prefix in the static binding to the client.
- **Dynamic prefix allocation**—To implement dynamic prefix allocation for clients, create a DHCPv6 address pool and a prefix pool, specify a subnet for the address pool, and apply the prefix pool to the address pool. Upon receiving a DHCP request, the DHCPv6 server dynamically selects an IPv6 prefix from the prefix pool in the address pool.

## Address pool selection

The DHCPv6 server observes the following principles when selecting an IPv6 address or prefix for a client:

1. If there is an address pool where an IPv6 address is statically bound to the DUID or IAID of the client, the DHCPv6 server selects this address pool. It assigns the statically bound IPv6 address or prefix and other configuration parameters to the client.
2. If the receiving interface has an address pool applied, the DHCP server selects an IPv6 address or prefix and other configuration parameters from this address pool.
3. If the receiving interface has a DHCP policy and the DHCP client matches a user class, the DHCP server selects the address pool that is bound to the matching user class. If no matching user class is found, the server assigns an IP address and other parameters from the default DHCP address pool. If no default address pool is specified or the default address pool does not have assignable IP addresses, the address assignment fails.
4. If the above conditions are not met, the DHCPv6 server selects an address pool depending on the client location.
  - **Client on the same subnet as the server**—The DHCPv6 server compares the IPv6 address of the receiving interface with the subnets of all address pools. It selects the address pool with the longest-matching subnet.
  - **Client on a different subnet than the server**—The DHCPv6 server compares the IPv6 address of the DHCPv6 relay agent interface closest to the client with the subnets of all address pools. It also selects the address pool with the longest-matching subnet.

To make sure IPv6 address allocation functions correctly, keep the subnet used for dynamic assignment consistent with the subnet where the interface of the DHCPv6 server or DHCPv6 relay agent resides.

## IPv6 address/prefix allocation sequence

The DHCPv6 server selects an IPv6 address/prefix for a client in the following sequence:

1. IPv6 address/prefix statically bound to the client's DUID and IAID and expected by the client.

2. IPv6 address/prefix statically bound to the client's DUID and IAID.
3. IPv6 address/prefix statically bound to the client's DUID and expected by the client.
4. IPv6 address/prefix statically bound to the client's DUID.
5. IPv6 address/prefix that was ever assigned to the client.
6. EUI-64 IPv6 address generated based on the client MAC address if EUI-64 address allocation is enabled.
7. Assignable IPv6 address/prefix in the address pool/prefix pool expected by the client.
8. Assignable IPv6 address/prefix in the address pool/prefix pool.
9. IPv6 address/prefix that was a conflict or passed its lease duration. If no IPv6 address/prefix is assignable, the server does not respond.

If a client moves to another subnet, the DHCPv6 server selects an IPv6 address/prefix from the address pool that matches the new subnet.

Conflicted IPv6 addresses can be assigned to other DHCPv6 clients only after the addresses are in conflict for one hour.

## DHCPv6 server tasks at a glance

To configure the DHCPv6 server, perform the following tasks:

1. Configuring the DHCPv6 server to assign IPv6 prefixes, IPv6 addresses, and other network parameters

Choose the following tasks as needed:

- [Configuring IPv6 prefix assignment](#)
- [Configuring IPv6 address assignment](#)
- [Configuring network parameters assignment](#)

2. Modifying the address pool selection method on the DHCPv6 server

Choose the following tasks as needed:

- [Configuring the DHCPv6 server on an interface](#)
- [Configuring a DHCPv6 policy for IPv6 address and prefix assignment](#)

3. (Optional.) [Setting the DSCP value for DHCPv6 packets sent by the DHCPv6 server](#)
4. (Optional.) [Configuring DHCPv6 binding auto backup](#)
5. (Optional.) [Enabling the DHCPv6 server to advertise IPv6 prefixes](#)
6. (Optional.) [Applying a DHCPv6 address pool to a VPN instance](#)
7. (Optional.) [Enabling DHCPv6 logging on the DHCPv6 server](#)

## Configuring IPv6 prefix assignment

### About IPv6 prefix assignment

Use the following methods to configure IPv6 prefix assignment:

- **Configure a static IPv6 prefix binding in an address pool**—If you bind a DUID and an IAID to an IPv6 prefix, the DUID and IAID in a request must match those in the binding before the DHCPv6 server can assign the IPv6 prefix to the DHCPv6 client. If you only bind a DUID to an IPv6 prefix, the DUID in the request must match the DUID in the binding before the DHCPv6 server can assign the IPv6 prefix to the DHCPv6 client.
- **Apply a prefix pool to an address pool**—The DHCPv6 server dynamically assigns an IPv6 prefix from the prefix pool in the address pool to a DHCPv6 client.

## Restrictions and guidelines

When you configure IPv6 prefix assignment, follow these restrictions and guidelines:

- An IPv6 prefix can be bound to only one DHCPv6 client. You cannot modify bindings that have been created. To change the binding for a DHCPv6 client, you must delete the existing binding first.
- One address pool can have only one prefix pool applied. You cannot modify prefix pools that have been applied. To change the prefix pool for an address pool, you must remove the prefix pool application first.
- You can apply a prefix pool that has not been created to an address pool. The setting takes effect after the prefix pool is created.

## Procedure

1. Enter system view.

```
system-view
```

2. (Optional.) Specify the IPv6 prefixes excluded from dynamic assignment.

```
ipv6 dhcp server forbidden-prefix start-prefix/prefix-len  
[ end-prefix/prefix-len ] [ vpn-instance vpn-instance-name ]
```

By default, no IPv6 prefixes in the prefix pool are excluded from dynamic assignment.

If the excluded IPv6 prefix is in a static binding, the prefix still can be assigned to the client.

3. Create a prefix pool.

```
ipv6 dhcp prefix-pool prefix-pool-number prefix { prefix-number |  
prefix/prefix-len } assign-len assign-len [ vpn-instance  
vpn-instance-name ]
```

This step is required for dynamic prefix assignment.

If you specify an IPv6 prefix by its ID, make sure the IPv6 prefix is in effect. Otherwise, the configuration does not take effect.

4. Enter DHCP address pool view.

```
ipv6 dhcp pool pool-name
```

5. Specify an IPv6 subnet for dynamic assignment.

```
network { prefix/prefix-length | prefix prefix-number  
[ sub-prefix/sub-prefix-length ] } [ preferred-lifetime  
preferred-lifetime valid-lifetime valid-lifetime ]
```

By default, no IPv6 subnet is specified for dynamic assignment.

The IPv6 subnets cannot be the same in different address pools.

If you specify an IPv6 prefix by its ID, make sure the IPv6 prefix is in effect. Otherwise, the configuration does not take effect.

6. Configure the prefix assignment. Choose the options to configure as needed:

- Configure a static prefix binding:

```
static-bind prefix prefix/prefix-len duid duid [ iaid iaid ]  
[ preferred-lifetime preferred-lifetime valid-lifetime  
valid-lifetime ]
```

By default, no static prefix binding is configured.

To add multiple static IPv6 prefix bindings, repeat this step.

- Apply the prefix pool to the address pool:

```
prefix-pool prefix-pool-number [ preferred-lifetime  
preferred-lifetime valid-lifetime valid-lifetime ]
```

By default, static or dynamic prefix assignment is not configured for an address pool.

# Configuring IPv6 address assignment

## About IPv6 address assignment

Use one of the following methods to configure IPv6 address assignment:

- Configure a static IPv6 address binding in an address pool.  
If you bind a DUID and an IAID to an IPv6 address, the DUID and IAID in a request must match those in the binding before the DHCPv6 server can assign the IPv6 address to the requesting client. If you only bind a DUID to an IPv6 address, the DUID in a request must match the DUID in the binding before the DHCPv6 server can assign the IPv6 address to the requesting client.
- Specify a subnet and address ranges in an address pool.
  - **Non-temporary address assignment**—The server selects addresses from the non-temporary address range specified by the **address range** command. If no non-temporary address range is specified, the server selects addresses on the subnet specified by the **network** command.
  - **Temporary address assignment**—The server selects addresses from the temporary address range specified by the **temporary address range** command. If no temporary address range is specified in the address pool, the DHCPv6 server cannot assign temporary addresses to clients.

## Restrictions and guidelines

- You can specify only one non-temporary address range and one temporary address range in an address pool.
- The address ranges specified by the **address range** and **temporary address range** commands must be on the subnet specified by the **network** command. Otherwise, the addresses are unassignable.
- Only one prefix pool can be applied to an address pool. You can apply a prefix pool that has not been created to an address pool. The setting takes effect after the prefix pool is created.
- An IPv6 address can be bound to only one DHCPv6 client. You cannot modify bindings that have been created. To change the binding for a DHCPv6 client, you must delete the existing binding first.
- Only one subnet can be specified in an address pool. If you use the **network** command multiple times in a DHCPv6 address pool, the most recent configuration takes effect. If you use this command to specify only new lifetimes, the settings do not affect existing leases. The IPv6 addresses assigned after the modification will use the new lifetimes.

## Procedure

1. Enter system view.  
**system-view**
2. (Optional.) Specify the IPv6 addresses excluded from dynamic assignment.  
**ipv6 dhcp server forbidden-address** *start-ipv6-address*  
[ *end-ipv6-address* ] [ **vpn-instance** *vpn-instance-name* ]  
By default, all IPv6 addresses except for the DHCPv6 server's IP address in a DHCPv6 address pool are assignable.  
If the excluded IPv6 address is in a static binding, the address still can be assigned to the client.
3. Enter DHCPv6 address pool view.  
**ipv6 dhcp pool** *pool-name*
4. Specify an IPv6 subnet for dynamic assignment.

```
network { prefix/prefix-length | prefix prefix-number  
[ sub-prefix/sub-prefix-length ] } [ preferred-lifetime  
preferred-lifetime valid-lifetime valid-lifetime ]
```

By default, no IPv6 address subnet is specified.

The IPv6 subnets cannot be the same in different address pools.

If you specify an IPv6 prefix by its ID, make sure the IPv6 prefix is in effect. Otherwise, the configuration does not take effect.

5. (Optional.) Specify a non-temporary IPv6 address range.

```
address range start-ipv6-address end-ipv6-address  
[ preferred-lifetime preferred-lifetime valid-lifetime  
valid-lifetime ]
```

By default, no non-temporary IPv6 address range is specified, and all unicast addresses on the subnet are assignable.

6. (Optional.) Specify a temporary IPv6 address range.

```
temporary address range start-ipv6-address end-ipv6-address  
[ preferred-lifetime preferred-lifetime valid-lifetime  
valid-lifetime ]
```

By default, no temporary IPv6 address range is specified, and the DHCPv6 server cannot assign temporary IPv6 addresses.

7. (Optional.) Enable EUI-64 address allocation mode.

```
address-alloc-mode eui-64
```

By default, EUI-64 address allocation mode is disabled.

This feature enables the DHCPv6 server to obtain the client MAC address in the DHCP request and generates an EUI-64 IPv6 address to assign to the client.

8. (Optional.) Create a static binding.

```
static-bind address ipv6-address/addr-prefix-length duid duid [ iaid  
iaid ] [ preferred-lifetime preferred-lifetime valid-lifetime  
valid-lifetime ]
```

By default, no static binding is configured.

To add more static bindings, repeat this step.

## Configuring network parameters assignment

### About network parameters assignment

In addition to IPv6 prefixes and IPv6 addresses, you can configure the following network parameters in an address pool:

- A maximum of eight DNS server addresses.
- One domain name.
- A maximum of eight SIP server addresses.
- A maximum of eight SIP server domain names.

You can configure network parameters on a DHCPv6 server by using one of the following methods:

- Configure network parameters in a DHCPv6 address pool.
- Configure network parameters in a DHCPv6 option group, and specify the option group for a DHCPv6 address pool.

Network parameters configured in a DHCPv6 address pool take precedence over those configured in a DHCPv6 option group.

# Configuring network parameters in a DHCPv6 address pool

1. Enter system view.  
**system-view**
2. Enter DHCPv6 address pool view.  
**ipv6 dhcp pool** *pool-name*
3. Specify an IPv6 subnet for dynamic assignment.  
**network** { *prefix/prefix-length* | **prefix** *prefix-number* [ *sub-prefix/sub-prefix-length* ] } [ **preferred-lifetime** *preferred-lifetime* **valid-lifetime** *valid-lifetime* ]  
By default, no IPv6 subnet is specified.  
The IPv6 subnets cannot be the same in different address pools.  
If you specify an IPv6 prefix by its ID, make sure the IPv6 prefix is in effect. Otherwise, the configuration does not take effect.
4. Specify a DNS server address.  
**dns-server** *ipv6-address*  
By default, no DNS server address is specified.
5. Specify a domain name.  
**domain-name** *domain-name*  
By default, no domain name is specified.
6. Specify a SIP server address or domain name.  
**sip-server** { **address** *ipv6-address* | **domain-name** *domain-name* }  
By default, no SIP server address or domain name is specified.
7. Configure a self-defined DHCPv6 option.  
**option** *code* **hex** *hex-string*  
By default, no self-defined DHCPv6 option is configured.

# Configuring network parameters in a DHCPv6 option group

## About network parameters assignment in a DHCPv6 option group

A DHCPv6 option group can be created by using the following methods:

- Create a static DHCPv6 option group by using the **ipv6 dhcp option-group** command. The static DHCPv6 option group takes precedence over the dynamic DHCPv6 option group.
- When the device acts as a DHCPv6 client, it automatically creates a dynamic DHCPv6 option group for saving the obtained parameters. For more information about creating a dynamic DHCPv6 option group, see "[Configuring the DHCPv6 client.](#)"

## Procedure

1. Enter system view.  
**system-view**
2. Create a static DHCPv6 option group and enter its view.  
**ipv6 dhcp option-group** *option-group-number*
3. Specify a DNS server address.  
**dns-server** *ipv6-address*  
By default, no DNS server address is specified.
4. Specify a domain name suffix.

**domain-name** *domain-name*

By default, no domain name suffix is specified.

5. Specify a SIP server address or domain name.

**sip-server** { **address** *ipv6-address* | **domain-name** *domain-name* }

By default, no SIP server address or domain name is specified.

6. Configure a self-defined DHCPv6 option.

**option** *code* **hex** *hex-string*

By default, no self-defined DHCPv6 option is configured.

7. Return to system view.

**quit**

8. Enter DHCPv6 address pool view.

**ipv6 dhcp pool** *pool-name*

9. Specify a DHCPv6 option group.

**option-group** *option-group-number*

By default, no DHCPv6 option group is specified.

# Configuring the DHCPv6 server on an interface

## About configuring the DHCPv6 server on an interface

Enable the DHCP server and configure one of the following address/prefix assignment methods on an interface:

- **Apply an address pool on the interface**—The DHCPv6 server selects an IPv6 address/prefix from the applied address pool for a requesting client. If there is no assignable IPv6 address/prefix in the address pool, the DHCPv6 server cannot assign an IPv6 address/prefix to a client.
- **Configure global address assignment on the interface**—The DHCPv6 server selects an IPv6 address/prefix in the global DHCPv6 address pool that matches the server interface address or the DHCPv6 relay agent address for a requesting client.

If you configure both methods on an interface, the DHCPv6 server uses the specified address pool for address assignment without performing global address assignment.

## Restrictions and guidelines

- An interface cannot act as a DHCPv6 server and DHCPv6 relay agent at the same time.
- Do not enable DHCPv6 server and DHCPv6 client on the same interface.
- You can apply an address pool that has not been created to an interface. The setting takes effect after the address pool is created.

## Procedure

1. Enter system view.

**system-view**

2. Enter interface view.

**interface** *interface-type interface-number*

3. Enable the DHCPv6 server on the interface.

**ipv6 dhcp select server**

By default, the interface does not act as a DHCP server or a DHCP relay agent, and discards DHCPv6 packets from DHCPv6 clients.

4. Configure an assignment method.

- Configure global address assignment.

```
ipv6 dhcp server { allow-hint | preference preference-value | rapid-commit } *
```

By default, desired address/prefix assignment and rapid assignment are disabled, and the default preference is 0.

- Apply a DHCPv6 address pool to the interface.

```
ipv6 dhcp server apply pool pool-name [ allow-hint | preference preference-value | rapid-commit ] *
```

# Configuring a DHCPv6 policy for IPv6 address and prefix assignment

## About DHCPv6 policy for IPv6 address and prefix assignment

In a DHCPv6 policy, each DHCPv6 user class has a bound DHCPv6 address pool. Clients matching different user classes obtain IPv6 addresses, IPv6 prefixes, and other parameters from different address pools. When receiving a DHCPv6 request, the DHCPv6 server compares the packet against the user classes in the order that they are configured.

If a match is found and the bound address pool has assignable IPv6 addresses or prefixes, the server uses the address pool for assignment. If the bound address pool does not have assignable IPv6 addresses or prefixes, the assignment fails.

If no match is found, the server uses the default DHCPv6 address pool for assignment. If no default address pool is specified or the default address pool does not have assignable IPv6 addresses or prefixes, the assignment fails.

For successful assignment, make sure the applied DHCPv6 policy and the bound address pools exist.

A match rule cannot match an option added by the DHCPv6 device, for example, Option 18 or Option 37.

## Procedure

1. Enter system view.

```
system-view
```

2. Create a DHCPv6 user class and enter DHCPv6 user class view.

```
ipv6 dhcp class class-name
```

3. Configure a match rule for the DHCPv6 user class.

```
if-match rule rule-number { option option-code [ ascii ascii-string [ offset offset | partial ] | hex hex-string [ mask mask | offset offset length length | partial ] ] | relay-agent gateway-ipv6-address }
```

By default, no match rule is configured for a DHCPv6 user class.

4. Return to system view.

```
quit
```

5. Create a DHCPv6 policy and enter DHCPv6 policy view.

```
ipv6 dhcp policy policy-name
```

The DHCPv6 policy takes effect only after it is applied to the interface that acts as the DHCPv6 server.

6. Specify a DHCPv6 address pool for a DHCPv6 user class.

```
class class-name pool pool-name
```

By default, no address pool is specified for a user class.

7. (Optional.) Specify the default DHCPv6 address pool.  
**default pool** *pool-name*  
 By default, the default address pool is not specified.
8. Return to system view.  
**quit**
9. Enter interface view.  
**interface** *interface-type interface-number*
10. Apply the DHCPv6 policy to the interface.  
**ipv6 dhcp apply-policy** *policy-name*  
 By default, no DHCPv6 policy is applied to an interface.

## Setting the DSCP value for DHCPv6 packets sent by the DHCPv6 server

### About setting the DSCP value for DHCPv6 packets sent by the DHCPv6 server

The DSCP value of a packet specifies the priority level of the packet and affects the transmission priority of the packet.

#### Procedure

1. Enter system view.  
**system-view**
2. Set the DSCP value for DHCPv6 packets sent by the DHCPv6 server.  
**ipv6 dhcp dscp** *dscp-value*  
 By default, the DSCP value in DHCPv6 packets sent by the DHCPv6 server is 56.

## Configuring DHCPv6 binding auto backup

### About DHCPv6 binding auto backup

The auto backup feature saves DHCPv6 bindings to a backup file, and allows the DHCPv6 server to download the bindings from the backup file at the server reboot. The bindings include the lease bindings and conflicted IPv6 addresses. They cannot survive a reboot on the DHCPv6 server.

The DHCPv6 server does not provide services during the download process. If a connection error occurs during the process and cannot be repaired in a short amount of time, you can terminate the download operation. Manual interruption allows the DHCPv6 server to provide services without waiting for the connection to be repaired.

#### Procedure

1. Enter system view.  
**system-view**
2. Configure the DHCPv6 server to back up the bindings to a file.  
**ipv6 dhcp server database filename** { *filename* | **url** *url* [ **username** *username* [ **password** { **cipher** | **simple** } *string* ] ] }  
 By default, the DHCPv6 server does not back up the DHCPv6 bindings.  
 With this command executed, the DHCPv6 server backs up its bindings immediately and runs auto backup.
3. (Optional.) Manually save the DHCPv6 bindings to the backup file.

**ipv6 dhcp server database update now**

4. (Optional.) Set the waiting time after a DHCPv6 binding change for the DHCPv6 server to update the backup file.

**ipv6 dhcp server database update interval *interval***

By default, the DHCP server waits 300 seconds to update the backup file after a DHCP binding change. If no DHCP binding changes, the backup file is not updated.

5. (Optional.) Terminate the download of DHCPv6 bindings from the backup file.

**ipv6 dhcp server database update stop**

This command only triggers one termination.

## Enabling the DHCPv6 server to advertise IPv6 prefixes

### About IPv6 prefixes advertisement

A DHCPv6 client can obtain an IPv6 prefix through DHCPv6 and use this IPv6 prefix to assign IPv6 addresses for clients in a downstream network. If the IPv6 prefix is in a different subnet than the IPv6 address of the DHCPv6 client's upstream interface, the clients in the downstream network cannot access the external network. If the DHCPv6 server is on the same link as the DHCPv6 client, enable the DHCPv6 server to advertise the IPv6 prefix.

### Procedure

1. Enter system view.

**system-view**

2. Enable the DHCPv6 server to advertise IPv6 prefixes.

**ipv6 dhcp advertise pd-route**

By default, the DHCPv6 server does not advertise IPv6 prefixes.

## Applying a DHCPv6 address pool to a VPN instance

### About DHCPv6 address pool application to a VPN instance

If a DHCPv6 address pool is applied to a VPN instance, the DHCPv6 server assigns IPv6 addresses in this address pool to clients in the VPN instance. Addresses in this address pool will not be assigned to clients on the public network.

The DHCPv6 server can obtain the VPN instance to which a DHCPv6 client belongs from the following information:

- The client's VPN information stored in authentication modules.
- The VPN information of the DHCPv6 server's interface that receives DHCPv6 packets from the client.

The VPN information from authentication modules takes priority over the VPN information of the receiving interface.

An MCE acting as the DHCP server can assign IP addresses not only to clients on public networks, but also to clients on private networks. The IP address ranges of public and private networks or those of private networks on the DHCP server cannot overlap. For more information about MCE, see *MCE Configuration Guide*.

## Procedure

1. Enter system view.  
**system-view**
2. Enter DHCP address pool view.  
**ipv6 dhcp pool** *pool-name*
3. Apply the address pool to a VPN instance.  
**vpn-instance** *vpn-instance-name*  
By default, the address pool is not applied to any VPN instance.

# Enabling DHCPv6 logging on the DHCPv6 server

## About DHCPv6 server logging

The DHCPv6 logging feature enables the DHCPv6 server to generate DHCPv6 logs and send them to the information center. The information helps administrators locate and solve problems. For information about the log destination and output rule configuration in the information center, see *Network Management and Monitoring Configuration Guide*.

## Restrictions and guidelines

As a best practice, disable this feature if the log generation affects the device performance or reduces the address and prefix allocation efficiency. For example, this situation might occur when a large number of clients frequently come online or go offline.

## Procedure

1. Enter system view.  
**system-view**
2. Enable DHCPv6 logging.  
**ipv6 dhcp log enable**  
By default, DHCPv6 logging is disabled.

# Display and maintenance commands for DHCPv6 server

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display the DUID of the local device.	<b>display ipv6 dhcp duid</b>
Display information about a DHCPv6 option group.	<b>display ipv6 dhcp option-group</b> [ <i>option-group-number</i> ]
Display DHCPv6 address pool information.	<b>display ipv6 dhcp pool</b> [ <i>pool-name</i>   <b>vpn-instance</b> <i>vpn-instance-name</i> ]
Display prefix pool information.	<b>display ipv6 dhcp prefix-pool</b> [ <i>prefix-pool-number</i> ] [ <b>vpn-instance</b> <i>vpn-instance-name</i> ]
Display DHCPv6 server information on an interface.	<b>display ipv6 dhcp server</b> [ <b>interface</b> <i>interface-type interface-number</i> ]

Task	Command
Display information about IPv6 address conflicts.	<code>display ipv6 dhcp server conflict [ address ipv6-address ] [ vpn-instance vpn-instance-name ]</code>
Display information about DHCPv6 binding auto backup	<code>display ipv6 dhcp server database</code>
Display information about expired IPv6 addresses.	<code>display ipv6 dhcp server expired [ [ address ipv6-address ] [ vpn-instance vpn-instance-name ]   pool pool-name ]</code>
Display information about IPv6 address bindings.	<code>display ipv6 dhcp server ip-in-use [ [ address ipv6-address ] [ vpn-instance vpn-instance-name ]   pool pool-name ]</code>
Display information about IPv6 prefix bindings.	<code>display ipv6 dhcp server pd-in-use [ pool pool-name   [ prefix prefix/prefix-len ] [ vpn-instance vpn-instance-name ] ]</code>
Display packet statistics on the DHCPv6 server.	<code>display ipv6 dhcp server statistics [ pool pool-name   vpn-instance vpn-instance-name ]</code>
Clear information about IPv6 address conflicts.	<code>reset ipv6 dhcp server conflict [ address ipv6-address ] [ vpn-instance vpn-instance-name ]</code>
Clear information about expired IPv6 address bindings.	<code>reset ipv6 dhcp server expired [ [ address ipv6-address ] [ vpn-instance vpn-instance-name ]   pool pool-name ]</code>
Clear information about IPv6 address bindings.	<code>reset ipv6 dhcp server ip-in-use [ [ address ipv6-address ] [ vpn-instance vpn-instance-name ]   pool pool-name ]</code>
Clear information about IPv6 prefix bindings.	<code>reset ipv6 dhcp server pd-in-use [ pool pool-name   [ prefix prefix/prefix-len ] [ vpn-instance vpn-instance-name ] ]</code>
Clear packets statistics on the DHCPv6 server.	<code>reset ipv6 dhcp server statistics [ vpn-instance vpn-instance-name ]</code>

## DHCPv6 server configuration examples

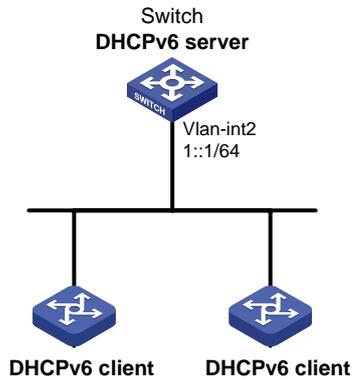
### Example: Configuring dynamic IPv6 prefix assignment

#### Network configuration

As shown in [Figure 11](#), the switch acts as a DHCPv6 server to assign an IPv6 prefix, a DNS server address, a domain name, a SIP server address, and a SIP server name to each DHCPv6 client.

The switch assigns prefix 2001:0410:0201::/48 to the client whose DUID is 00030001CA0006A40000, and assigns prefixes in the range of 2001:0410::/48 to 2001:0410:FFFF::/48 (excluding 2001:0410:0201::/48) to other clients. The DNS server address is 2::2:3. The DHCPv6 clients reside in the domain **aaa.com**. The SIP server address is 2:2::4, and the SIP server name is **bbb.com**.

**Figure 11 Network diagram**



## Procedure

# Specify an IPv6 address for VLAN-interface 2.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ipv6 address 1::1/64
```

# Disable RA message suppression on VLAN-interface 2.

```
[Switch-Vlan-interface2] undo ipv6 nd ra halt
```

# Set the M flag to 1 in RA advertisements to be sent on VLAN-interface 2. Hosts that receive the RA advertisements will obtain IPv6 addresses through DHCPv6.

```
[Switch-Vlan-interface2] ipv6 nd autoconfig managed-address-flag
```

# Set the O flag to 1 in RA advertisements to be sent on VLAN-interface 2. Hosts that receive the RA advertisements will obtain information other than IPv6 address through DHCPv6.

```
[Switch-Vlan-interface2] ipv6 nd autoconfig other-flag
[Switch-Vlan-interface2] quit
```

# Create prefix pool 1, and specify the prefix 2001:0410::/32 with the assigned prefix length 48.

```
[Switch] ipv6 dhcp prefix-pool 1 prefix 2001:0410::/32 assign-len 48
```

# Create address pool 1.

```
[Switch] ipv6 dhcp pool 1
```

# In address pool 1, configure subnet 1::/64 where VLAN interface-2 resides.

```
[Switch-dhcp6-pool-1] network 1::/64
```

# Apply prefix pool 1 to address pool 1, and set the preferred lifetime to one day, and the valid lifetime to three days.

```
[Switch-dhcp6-pool-1] prefix-pool 1 preferred-lifetime 86400 valid-lifetime 259200
```

# In address pool 1, bind prefix 2001:0410:0201::/48 to the client DUID 00030001CA0006A40000, and set the preferred lifetime to one day, and the valid lifetime to three days.

```
[Switch-dhcp6-pool-1] static-bind prefix 2001:0410:0201::/48 duid 00030001CA0006A40000
preferred-lifetime 86400 valid-lifetime 259200
```

# Configure the DNS server address 2:2::3.

```
[Switch-dhcp6-pool-1] dns-server 2:2::3
```

# Configure the domain name as aaa.com.

```
[Switch-dhcp6-pool-1] domain-name aaa.com
```

# Configure the SIP server address as 2:2::4, and the SIP server name as bbb.com.

```
[Switch-dhcp6-pool-1] sip-server address 2:2::4
```

```
[Switch-dhcp6-pool-1] sip-server domain-name bbb.com
[Switch-dhcp6-pool-1] quit
```

**# Enable the DHCPv6 server on VLAN-interface 2, enable desired prefix assignment and rapid prefix assignment, and set the preference to the highest.**

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ipv6 dhcp select server
[Switch-Vlan-interface2] ipv6 dhcp server allow-hint preference 255 rapid-commit
```

## Verifying the configuration

**# Display DHCPv6 server configuration on VLAN-interface 2.**

```
[Switch-Vlan-interface2] display ipv6 dhcp server interface vlan-interface 2
Using pool: global
Preference value: 255
Allow-hint: Enabled
Rapid-commit: Enabled
```

**# Display information about address pool 1.**

```
[Switch-Vlan-interface2] display ipv6 dhcp pool 1
DHCPv6 pool: 1
  Network: 1::/64
    Preferred lifetime 604800, valid lifetime 2592000
  Prefix pool: 1
    Preferred lifetime 86400, valid lifetime 259200
  Static bindings:
    DUID: 00030001ca0006a40000
    IAID: Not configured
    Prefix: 2001:410:201::/48
      Preferred lifetime 86400, valid lifetime 259200
  DNS server addresses:
    2:2::3
  Domain name:
    aaa.com
  SIP server addresses:
    2:2::4
  SIP server domain names:
    bbb.com
```

**# Display information about prefix pool 1.**

```
[Switch-Vlan-interface2] display ipv6 dhcp prefix-pool 1
Prefix: 2001:410::/32
Assigned length: 48
Total prefix number: 65536
Available: 65535
In-use: 0
Static: 1
```

**# After the client with the DUID 00030001CA0006A40000 obtains an IPv6 prefix, display the binding information on the DHCPv6 server.**

```
[Switch-Vlan-interface2] display ipv6 dhcp server pd-in-use
Pool: 1
  IPv6 prefix                                     Type      Lease expiration
```

```

2001:410:201::/48                               Static(C) Jul 10 19:45:01 2009
# After the other client obtains an IPv6 prefix, display binding information on the DHCPv6 server.
[Switch-Vlan-interface2] display ipv6 dhcp server pd-in-use
Pool: 1
IPv6 prefix                                     Type      Lease expiration
2001:410:201::/48                             Static(C) Jul 10 19:45:01 2009
2001:410::/48                                 Auto(C)   Jul 10 20:44:05 2009

```

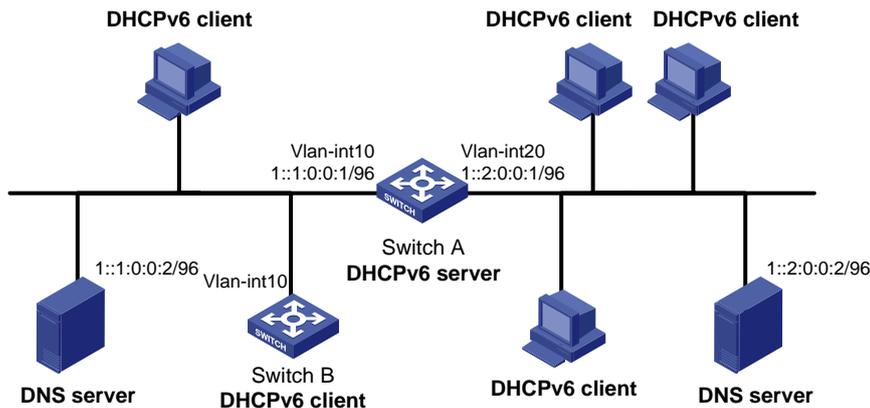
## Example: Configuring dynamic IPv6 address assignment

### Network configuration

As shown in [Figure 12](#), Switch A acts as a DHCPv6 server to assign IPv6 addresses to the clients on subnets 1::1:0:0/96 and 1::2:0:0/96.

On Switch A, configure the IPv6 address 1::1:0:0:1/96 for VLAN-interface 10 and 1::2:0:0:1/96 for VLAN-interface 20. The lease duration of the addresses on subnet 1::1:0:0/96 is 172800 seconds (two days), the valid time is 345600 seconds (four days), the domain name suffix is aabbcc.com, and the DNS server address is 1::1:0:0:2/96. The lease duration of the addresses on subnet 1::2:0:0/96 is 432000 seconds (five days), the valid time is 864000 seconds (ten days), the domain name is aabbcc.com, and the DNS server address is 1::2:0:0:2/96.

**Figure 12 Network diagram**



### Procedure

- Configure the interfaces on the DHCPv6 server:
  - # Specify an IPv6 address for VLAN-interface 10.

```

<SwitchA> system-view
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ipv6 address 1::1:0:0:1/96

```

  - # Disable RA message suppression on VLAN-interface 10.

```

[SwitchA-Vlan-interface10] undo ipv6 nd ra halt

```

  - # Set the M flag to 1 in RA advertisements to be sent on VLAN-interface 10. Hosts that receive the RA advertisements will obtain IPv6 addresses through DHCPv6.

```

[SwitchA-Vlan-interface10] ipv6 nd autoconfig managed-address-flag

```

  - # Set the O flag to 1 in RA advertisements to be sent on VLAN-interface 10. Hosts that receive the RA advertisements will obtain information other than IPv6 address through DHCPv6.

```

[SwitchA-Vlan-interface10] ipv6 nd autoconfig other-flag
[SwitchA-Vlan-interface10] quit

```

**# Specify an IPv6 address for VLAN-interface 20.**

```
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] ipv6 address 1::2:0:0:1/96
```

**# Disable RA message suppression on VLAN-interface 20.**

```
[SwitchA-Vlan-interface20] undo ipv6 nd ra halt
```

**# Set the M flag to 1 in RA advertisements to be sent on VLAN-interface 20. Hosts that receive the RA advertisements will obtain IPv6 addresses through DHCPv6.**

```
[SwitchA-Vlan-interface20] ipv6 nd autoconfig managed-address-flag
```

**# Set the O flag to 1 in RA advertisements to be sent on VLAN-interface 20. Hosts that receive the RA advertisements will obtain information other than IPv6 address through DHCPv6.**

```
[SwitchA-Vlan-interface20] ipv6 nd autoconfig other-flag
```

```
[SwitchA-Vlan-interface20] quit
```

## 2. Enable DHCPv6:

**# Enable DHCPv6 server on VLAN-interface 10 and VLAN-interface 20.**

```
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ipv6 dhcp select server
[SwitchA-Vlan-interface10] quit
```

```
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] ipv6 dhcp select server
[SwitchA-Vlan-interface20] quit
```

**# Exclude the DNS server addresses from dynamic assignment.**

```
[SwitchA] ipv6 dhcp server forbidden-address 1::1:0:0:2
[SwitchA] ipv6 dhcp server forbidden-address 1::2:0:0:2
```

**# Configure the DHCPv6 address pool 1 to assign IPv6 addresses and other configuration parameters to clients on subnet 1::1:0:0/96.**

```
[SwitchA] ipv6 dhcp pool 1
[SwitchA-dhcp6-pool-1] network 1::1:0:0:0/96 preferred-lifetime 172800
valid-lifetime 345600
[SwitchA-dhcp6-pool-1] domain-name aabbcc.com
[SwitchA-dhcp6-pool-1] dns-server 1::1:0:0:2
[SwitchA-dhcp6-pool-1] quit
```

**# Configure the DHCPv6 address pool 2 to assign IPv6 addresses and other configuration parameters to clients on subnet 1::2:0:0/96.**

```
[SwitchA] ipv6 dhcp pool 2
[SwitchA-dhcp6-pool-2] network 1::2:0:0:0/96 preferred-lifetime 432000
valid-lifetime 864000
[SwitchA-dhcp6-pool-2] domain-name aabbcc.com
[SwitchA-dhcp6-pool-2] dns-server 1::2:0:0:2
[SwitchA-dhcp6-pool-2] quit
```

## Verifying the configuration

**# Verify that the clients on subnets 1::1:0:0/96 and 1::2:0:0/96 can obtain IPv6 addresses and all other configuration parameters from the DHCPv6 server (Switch A). (Details not shown.)**

**# On the DHCPv6 server, display IPv6 addresses assigned to the DHCPv6 clients.**

```
[SwitchA] display ipv6 dhcp server ip-in-use
```

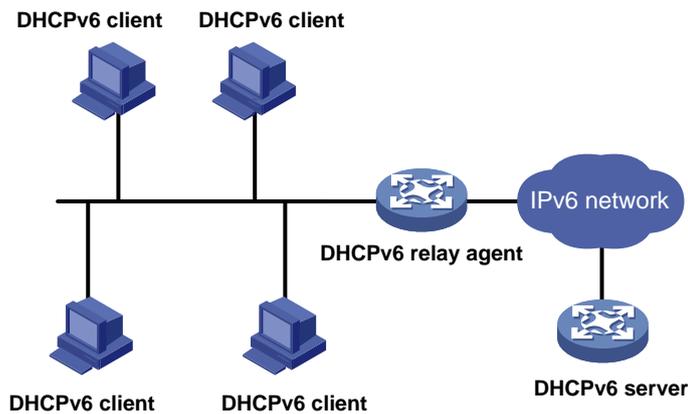
# Configuring the DHCPv6 relay agent

## About DHCPv6 relay agent

### Typical application

A DHCPv6 client usually uses a multicast address to contact the DHCPv6 server on the local link to obtain an IPv6 address and other configuration parameters. As shown in [Figure 13](#), if the DHCPv6 server resides on another subnet, the DHCPv6 clients need a DHCPv6 relay agent to contact the server. The relay agent feature avoids deploying a DHCPv6 server on each subnet.

**Figure 13 Typical DHCPv6 relay agent application**

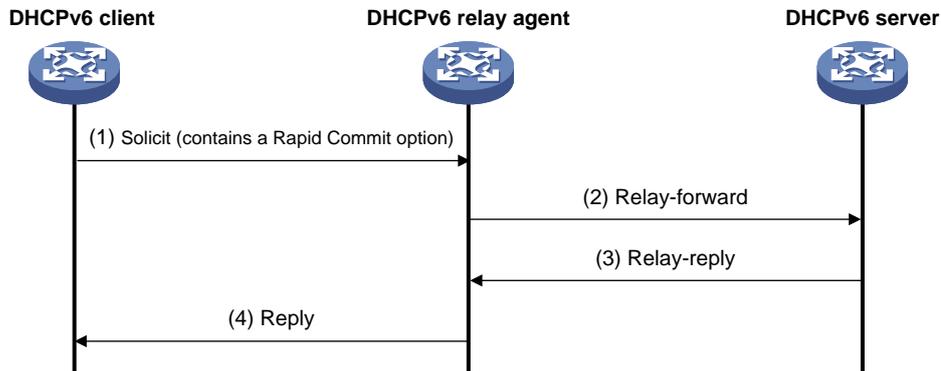


### DHCPv6 relay agent operating process

As shown in [Figure 14](#), a DHCPv6 client obtains an IPv6 address and other network configuration parameters from a DHCPv6 server through a DHCPv6 relay agent. The following example uses rapid assignment to describe the process:

- The DHCPv6 client sends a Solicit message containing the Rapid Commit option to the multicast address FF02::1:2 of all the DHCPv6 servers and relay agents.
- After receiving the Solicit message, the DHCPv6 relay agent encapsulates the message into the Relay Message option of a Relay-forward message, and sends the message to the DHCPv6 server.
- After obtaining the Solicit message from the Relay-forward message, the DHCPv6 server performs the following tasks:
  - Selects an IPv6 address and other required parameters.
  - Adds them to a reply that is encapsulated within the Relay Message option of a Relay-reply message.
  - Sends the Relay-reply message to the DHCPv6 relay agent.
- The DHCPv6 relay agent obtains the reply from the Relay-reply message and sends the reply to the DHCPv6 client.
- The DHCPv6 client uses the IPv6 address and other network parameters assigned by the DHCPv6 server to complete network configuration.

Figure 14 Operating process of a DHCPv6 relay agent



## DHCPv6 relay agent tasks at a glance

To configure a DHCPv6 relay agent, perform the following tasks:

1. [Enabling the DHCPv6 relay agent on an interface](#)
2. [Specifying DHCPv6 servers on the relay agent](#)
3. (Optional.) [Specifying a gateway address for DHCPv6 clients](#)
4. (Optional.) [Setting the DSCP value for DHCPv6 packets sent by the DHCPv6 relay agent](#)
5. (Optional.) [Specifying a padding mode for the Interface-ID option](#)
6. (Optional.) [Enabling the DHCPv6 relay agent to advertise IPv6 prefixes](#)
7. (Optional.) [Specifying the source IPv6 address for relayed DHCPv6 requests](#)

## Enabling the DHCPv6 relay agent on an interface

### Restrictions and guidelines

As a best practice, do not enable DHCPv6 relay agent and DHCPv6 client on the same interface.

### Procedure

1. Enter system view.  
**system-view**
2. Enter interface view.  
**interface** *interface-type interface-number*
3. Enable DHCPv6 relay agent on the interface.  
**ipv6 dhcp select relay**  
By default, the DHCPv6 relay agent is disabled on the interface.

# Specifying DHCPv6 servers on the relay agent

## Specifying DHCPv6 server IP addresses

### Restrictions and guidelines

- You can use the **ipv6 dhcp relay server-address** command to specify a maximum of eight DHCPv6 servers on the DHCPv6 relay agent interface. The DHCPv6 relay agent forwards DHCP requests to all the specified DHCPv6 servers.
- If a DHCPv6 server address is a link-local address or multicast address, you must specify an outgoing interface by using the **interface** keyword in this command. Otherwise, DHCPv6 packets might fail to reach the DHCPv6 server.

### Procedure

1. Enter system view.  
**system-view**
  2. Enter interface view.  
**interface** *interface-type interface-number*
  3. Specify a DHCPv6 server.  
**ipv6 dhcp relay server-address** *ipv6-address* [ **interface** *interface-type interface-number* ] [ **public** | **vpn-instance** *vpn-instance-name* ]
- By default, no DHCPv6 server is specified.

## Specifying DHCPv6 servers for a DHCPv6 address pool on the DHCPv6 relay agent

### About specifying DHCPv6 servers for a DHCPv6 address pool on the DHCPv6 relay agent

This feature allows DHCPv6 clients of the same type to obtain IPv6 addresses, IPv6 prefixes, and other configuration parameters from the DHCPv6 servers in the matching DHCPv6 address pool.

It applies to scenarios where the DHCPv6 relay agent connects to clients of the same access type but classified into different types by their locations. In this case, the relay interface typically has no IPv6 address configured. You can use the **gateway-list** command to specify the gateway addresses for clients matching the same DHCPv6 address pool.

Upon receiving a DHCPv6 Solicit or Request from a client that matches a DHCPv6 address pool, the relay agent processes the packet as follows:

- Fills the **link-address** field of the packet with a specified gateway address.
- Forwards the packet to all DHCPv6 servers in the matching DHCPv6 address pool.

The DHCPv6 servers select a DHCPv6 address pool according to the gateway address.

### Restrictions and guidelines

- You can specify a maximum of eight DHCPv6 servers for one DHCPv6 address pool for high availability. The relay agent forwards DHCPv6 Solicit and Request packets to all DHCPv6 servers in the DHCPv6 address pool.

### Procedure

1. Enter system view.  
**system-view**
2. Create a DHCPv6 address pool and enter its view.

**ipv6 dhcp pool** *pool-name*

3. Specify gateway addresses for the clients matching the DHCPv6 address pool.

**gateway-list** *ipv6-address*<1-8>

By default, no gateway address is specified.

4. Specify DHCPv6 servers for the DHCPv6 address pool.

**remote-server** *ipv6-address* [ **interface** *interface-type*  
*interface-number* ]

By default, no DHCPv6 server is specified for the DHCPv6 address pool.

## Specifying a gateway address for DHCPv6 clients

### About specifying a gateway address for DHCPv6 client

By default, the DHCPv6 relay agent fills the **link-address** field of DHCPv6 Solicit and Request packets with the first IPv6 address of the relay interface. You can specify a gateway address on the relay agent for DHCPv6 clients. The DHCPv6 relay agent uses the specified gateway address to fill the **link-address** field of DHCPv6 Solicit and Request packets.

#### Procedure

1. Enter system view.

**system-view**

2. Enter interface view.

**interface** *interface-type* *interface-number*

3. Specify a gateway address for DHCPv6 clients.

**ipv6 dhcp relay gateway** *ipv6-address*

By default, the DHCPv6 relay agent uses the first IPv6 address of the relay interface as the clients' gateway address.

## Setting the DSCP value for DHCPv6 packets sent by the DHCPv6 relay agent

### About setting the DSCP value for DHCPv6 packets

The DSCP value of a packet specifies the priority level of the packet and affects the transmission priority of the packet.

#### Procedure

1. Enter system view.

**system-view**

2. Set the DSCP value for DHCPv6 packets sent by the DHCPv6 relay agent.

**ipv6 dhcp dscp** *dscp-value*

The default DSCP value is 56.

# Specifying a padding mode for the Interface-ID option

## About specifying a padding mode for the Interface-ID option

This feature enables the relay agent to fill the Interface-ID option in the specified mode. When receiving a DHCPv6 packet from a client, the relay agent fills the Interface-ID option in the mode and then forwards the packet to the DHCPv6 server.

### Procedure

1. Enter system view.  
**system-view**
2. Enter interface view.  
**interface** *interface-type* *interface-number*
3. Specify a padding mode for the Interface-ID option.  
**ipv6 dhcp relay interface-id** { **bas** | **interface** }

By default, the relay agent fills the Interface-ID option with the interface index of the interface.

# Enabling the DHCPv6 relay agent to advertise IPv6 prefixes

## About enabling the DHCPv6 relay agent to advertise IPv6 prefixes

A DHCPv6 client can obtain an IPv6 prefix through DHCPv6 and use this IPv6 prefix to assign IPv6 address to clients in a downstream network. If the IPv6 prefix is in a different subnet than the IPv6 address of the DHCPv6 client's upstream interface, the clients in the downstream network cannot access the external network. You can enable the DHCPv6 relay agent that is on the same link as the DHCPv6 client to advertise the IPv6 prefix.

### Procedure

1. Enter system view.  
**system-view**
2. Enable the DHCPv6 relay agent to advertise IPv6 prefixes.  
**ipv6 dhcp advertise pd-route**

By default, the DHCPv6 relay agent does not advertise IPv6 prefixes.

Before using this command, make sure the DHCPv6 relay agent is enabled to record DHCPv6 relay entries.

# Specifying the source IPv6 address for relayed DHCPv6 requests

## About specifying the source IPv6 address for relayed DHCPv6 requests

This task is required if a relay interface does not have routes to DHCPv6 servers. You can specify a global unicast address or the IPv6 address of another interface (typically the loopback interface) as the source IPv6 address for DHCPv6 requests. The relay interface inserts the source IPv6 address in the source IPv6 address field of DHCPv6 requests.

## Procedure

1. Enter system view.  
**system-view**
2. Enter interface view.  
**interface** *interface-type interface-number*
3. Specify the source IPv6 address for relayed DHCPv6 requests.  
**ipv6 dhcp relay source-address** { *ipv6-address* | **interface** *interface-type interface-number* }

By default, the DHCPv6 relay agent uses the IPv6 global unicast address of the interface that connects to the DHCPv6 server as the source IPv6 address for relayed DHCPv6 requests.

If the specified interface does not have an IPv6 global unicast address, the IPv6 address of the output interface is used as the source address for relayed DHCPv6 requests.

## Display and maintenance commands for DHCPv6 relay agent

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display the DUID of the local device.	<b>display ipv6 dhcp duid</b>
Display DHCPv6 server addresses specified on the DHCPv6 relay agent.	<b>display ipv6 dhcp relay server-address</b> [ <b>interface</b> <i>interface-type interface-number</i> ]
Display packet statistics on the DHCPv6 relay agent.	<b>display ipv6 dhcp relay statistics</b> [ <b>interface</b> <i>interface-type interface-number</i> ]
Clear DHCPv6 relay entries that record clients' IPv6 address information.	<b>reset ipv6 dhcp relay client-information address</b> [ <b>interface</b> <i>interface-type interface-number</i>   <b>ipv6</b> <i>ipv6-address</i> ] [ <b>vpn-instance</b> <i>vpn-instance-name</i> ]
Clear DHCPv6 relay entries that record clients' IPv6 prefix information.	<b>reset ipv6 dhcp relay client-information pd</b> [ <b>interface</b> <i>interface-type interface-number</i>   <b>prefix</b> <i>prefix/prefix-len</i> ] [ <b>vpn-instance</b> <i>vpn-instance-name</i> ]
Clear packets statistics on the DHCPv6 relay agent.	<b>reset ipv6 dhcp relay statistics</b> [ <b>interface</b> <i>interface-type interface-number</i> ]

# DHCPv6 relay agent configuration examples

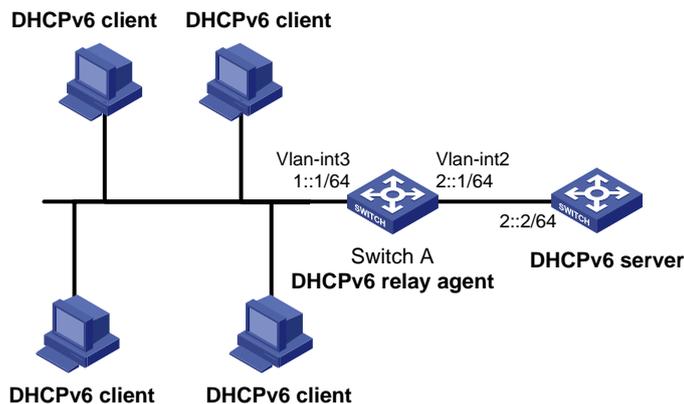
## Example: Configuring DHCPv6 relay agent

### Network configuration

As shown in [Figure 15](#), configure the DHCPv6 relay agent on Switch A to relay DHCPv6 packets between DHCPv6 clients and the DHCPv6 server.

Switch A acts as the gateway of network 1::/64. It sends RA messages to notify the hosts to obtain IPv6 addresses and other configuration parameters through DHCPv6. For more information about RA messages, see "Configuring basic IPv6 settings."

**Figure 15 Network diagram**



### Procedure

# Specify IPv6 addresses for VLAN-interface 2 and VLAN-interface 3.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ipv6 address 2::1 64
[SwitchA-Vlan-interface2] quit
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ipv6 address 1::1 64
```

# Disable RA message suppression on VLAN-interface 3.

```
[SwitchA-Vlan-interface3] undo ipv6 nd ra halt
```

# Set the M flag to 1 in RA advertisements to be sent on VLAN-interface 3. Hosts that receive the RA advertisements will obtain IPv6 addresses through DHCPv6.

```
[SwitchA-Vlan-interface3] ipv6 nd autoconfig managed-address-flag
```

# Set the O flag to 1 in RA advertisements to be sent on VLAN-interface 3. Hosts that receive the RA advertisements will obtain information other than IPv6 address through DHCPv6.

```
[SwitchA-Vlan-interface3] ipv6 nd autoconfig other-flag
```

# Enable the DHCPv6 relay agent on VLAN-interface 3 and specify the DHCPv6 server on the relay agent.

```
[SwitchA-Vlan-interface3] ipv6 dhcp select relay
[SwitchA-Vlan-interface3] ipv6 dhcp relay server-address 2::2
```

### Verifying the configuration

# Display DHCPv6 server address information on Switch A.

```
[SwitchA-Vlan-interface3] display ipv6 dhcp relay server-address
Interface: Vlan-interface3
  Server address      Outgoing Interface      Public/VRF name
  2::2                --/--
```

**# Display packet statistics on the DHCPv6 relay agent.**

```
[SwitchA-Vlan-interface3] display ipv6 dhcp relay statistics
Packets dropped          : 0
Packets received        : 14
  Solicit                 : 0
  Request                 : 0
  Confirm                 : 0
  Renew                  : 0
  Rebind                  : 0
  Release                 : 0
  Decline                 : 0
  Information-request     : 7
  Relay-forward           : 0
  Relay-reply             : 7
Packets sent             : 14
  Advertise               : 0
  Reconfigure             : 0
  Reply                   : 7
  Relay-forward           : 7
  Relay-reply             : 0
```

# Configuring the DHCPv6 client

## About the DHCPv6 client

With DHCPv6 client configured, an interface can obtain configuration parameters from the DHCPv6 server.

A DHCPv6 client can use DHCPv6 to complete the following functions:

- Obtain an IPv6 address, an IPv6 prefix, or both, and obtain other configuration parameters. If DHCPv6 server is enabled on the device, the client can automatically save the obtained parameters to a DHCPv6 option group. With the obtained IPv6 prefix, the client can generate its global unicast address.
- Support stateless DHCPv6 to obtain configuration parameters except IPv6 address and IPv6 prefix. The client obtains an IPv6 address through stateless IPv6 address autoconfiguration. If the client receives an RA message with the M flag set to 0 and the O flag set to 1 during address acquisition, stateless DHCPv6 starts.

## Restrictions and guidelines: DHCPv6 client configuration

Do not configure the DHCPv6 client on the same interface as the DHCPv6 server or the DHCPv6 relay agent.

## DHCPv6 client tasks at a glance

To configure a DHCPv6 client, perform the following tasks:

1. (Optional.) [Configuring the DHCPv6 client DUID](#)
2. Configuring the DHCPv6 client to obtain IPv6 addresses, IPv6 prefixes and other network parameters

Choose the following tasks as needed:

- [Configuring IPv6 address acquisition](#)
  - [Configuring IPv6 prefix acquisition](#)
  - [Configuring IPv6 address and prefix acquisition](#)
  - [Configuring acquisition of configuration parameters except IP addresses and prefixes](#)
3. (Optional.) [Setting the DSCP value for DHCPv6 packets sent by the DHCPv6 client](#)

## Configuring the DHCPv6 client DUID

### About the DHCPv6 client DUID

The DUID of a DHCPv6 client is the globally unique identifier of the client. The client pads its DUID into Option 1 of the DHCPv6 packet that it sends to the DHCPv6 server. The DHCPv6 server can assign specific IPv6 addresses or prefixes to DHCPv6 clients with specific DUIDs.

### Restrictions and guidelines

Make sure the DUID that you configure is unique.

## Procedure

1. Enter system view.  
**system-view**
2. Enter interface view.  
**interface** *interface-type interface-number*
3. Configure the DHCPv6 client DUID.  
**ipv6 dhcp client duid** { *ascii string* | *hex string* | **mac** *interface-type interface-number* }  
By default, the interface uses the device bridge MAC address to generate its DHCPv6 client DUID.

## Configuring IPv6 address acquisition

1. Enter system view.  
**system-view**
2. Enter interface view.  
**interface** *interface-type interface-number*
3. Configure the interface to use DHCPv6 to obtain an IPv6 address and other configuration parameters.  
**ipv6 address dhcp-alloc** [ **option-group** *group-number* | **rapid-commit** ]  
\*  
By default, the interface does not use DHCPv6 for IPv6 address acquisition.

## Configuring IPv6 prefix acquisition

1. Enter system view.  
**system-view**
2. Enter interface view.  
**interface** *interface-type interface-number*
3. Configure the interface to use DHCPv6 to obtain an IPv6 prefix and other configuration parameters.  
**ipv6 dhcp client pd** *prefix-number* [ **option-group** *group-number* | **rapid-commit** ] \*  
By default, the interface does not use DHCPv6 for IPv6 prefix acquisition.

## Configuring IPv6 address and prefix acquisition

1. Enter system view.  
**system-view**
2. Enter interface view.  
**interface** *interface-type interface-number*
3. Configure the interface to use DHCPv6 to obtain an IPv6 address, an IPv6 prefix, and other configuration parameters.  
**ipv6 dhcp client stateful prefix** *prefix-number* [ **option-group** *option-group-number* | **rapid-commit** ] \*  
By default, the interface does not use DHCPv6 for IPv6 address and prefix acquisition.

# Configuring acquisition of configuration parameters except IP addresses and prefixes

## About acquisition of configuration parameters except IP addresses and prefixes

When a DHCPv6 client has obtained an IPv6 address and prefix, you can configure the following methods for the client to obtain other network configuration parameters:

- Execute the **ipv6 address auto** command to enable an interface to automatically generate an IPv6 global unicast address and a link-local address. Then stateless DHCPv6 will be triggered when the M flag is set to 0 and the O flag is set to 1 in a received RA message. For more information about the commands, see *Layer 3—IP services Command Reference*.
- Executing the **ipv6 dhcp client stateless enable** command on an interface to enable the interface to act as a DHCPv6 client to obtain configuration parameters from a DHCPv6 server.

If you execute both the **ip address auto** and **ipv6 dhcp client stateless enable** commands, the interface acts as follows:

- Generate a global unicast address and a link-local address.
- Obtain other configuration parameters from a DHCPv6 server.

## Procedure

1. Enter system view.  
**system-view**
2. Enter interface view.  
**interface** *interface-type* *interface-number*
3. Configure the interface to support stateless DHCPv6. Choose the options to configure as needed:
  - Enable stateless IPv6 address autoconfiguration:  
**ipv6 address auto**
  - Configure the client to obtain network parameters from DHCPv6 servers:  
**ipv6 dhcp client stateless enable**

By default, the interface does not support stateless DHCPv6.

# Setting the DSCP value for DHCPv6 packets sent by the DHCPv6 client

## About setting the DSCP value for DHCPv6 packets

The DSCP value of a packet specifies the priority level of the packet and affects the transmission priority of the packet.

## Procedure

1. Enter system view.  
**system-view**
2. Set the DSCP value for DHCPv6 packets sent by the DHCPv6 client.  
**ipv6 dhcp client dscp** *dscp-value*

By default, the DSCP value in DHCPv6 packets sent by the DHCPv6 client is 56.

# Display and maintenance commands for DHCPv6 client

Execute the **display** commands in any view, and execute the **reset** command in user view.

Task	Command
Display the DHCPv6 client information.	<b>display ipv6 dhcp client</b> [ <b>interface</b> <i>interface-type interface-number</i> ]
Display the DHCPv6 client statistics.	<b>display ipv6 dhcp client statistics</b> [ <b>interface</b> <i>interface-type interface-number</i> ]
Clear the DHCPv6 client statistics.	<b>reset ipv6 dhcp client statistics</b> [ <b>interface</b> <i>interface-type interface-number</i> ]

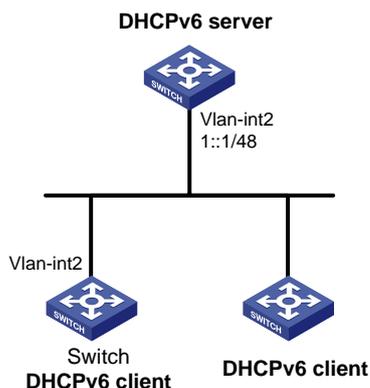
## DHCPv6 client configuration examples

### Example: Configuring IPv6 address acquisition

#### Network configuration

As shown in [Figure 16](#), configure the switch to use DHCPv6 to obtain configuration parameters from the DHCPv6 server. The parameters include IPv6 address, DNS server address, domain name suffix, SIP server address, and SIP server domain name.

**Figure 16 Network diagram**



#### Procedure

You must configure the DHCPv6 server first before configuring the DHCPv6 client. For information about configuring DHCPv6 server, see "[Configuring the DHCPv6 server.](#)"

# Configure VLAN-interface 2 as a DHCPv6 client for IPv6 address acquisition. Configure the DHCPv6 client to support DHCPv6 rapid address assignment. Configure the DHCPv6 client to create a dynamic DHCPv6 option group for saving configuration parameters.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ipv6 address dhcp-alloc rapid-commit option-group 1
[Switch-Vlan-interface2] quit
```

## Verifying the configuration

# Verify that the client has obtained an IPv6 address and other configuration parameters from the server.

```
[Switch] display ipv6 dhcp client
Vlan-interface2:
  Type: Stateful client requesting address
  State: OPEN
  Client DUID: 0003000100e002000000
  Preferred server:
    Reachable via address: FE80::2E0:1FF:FE00:18
    Server DUID: 0003000100e001000000
  IA_NA: IAID 0x00000642, T1 50 sec, T2 80 sec
  Address: 1:1::2/128
  Preferred lifetime 100 sec, valid lifetime 200 sec
  Will expire on Mar 27 2014 at 08:06:57 (198 seconds left)
  DNS server addresses:
    2000::FF
  Domain name:
    example.com
  SIP server addresses:
    2:2::4
  SIP server domain names:
    bbb.com
```

# After DHCPv6 server is enabled on the device, verify that configuration parameters are saved in a dynamic DHCPv6 option group.

```
[Switch] display ipv6 dhcp option-group 1
DHCPv6 option group: 1
  DNS server addresses:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: Vlan-interface2
    2000::FF
  Domain name:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: Vlan-interface2
    example.com
  SIP server addresses:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: Vlan-interface2
    2:2::4
  SIP server domain names:
    Type: Dynamic (DHCPv6 address allocation)
    Interface: Vlan-interface2
    bbb.com
```

# Verify that the DHCPv6 client has obtained an IPv6 address..

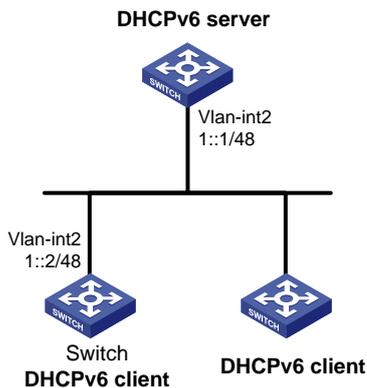
```
[Switch] display ipv6 interface brief
*down: administratively down
(s): spoofing
Interface                               Physical  Protocol  IPv6 Address
```

## Example: Configuring IPv6 prefix acquisition

### Network configuration

As shown in [Figure 17](#), configure the switch to use DHCPv6 to obtain configuration parameters from the DHCPv6 server. The parameters include IPv6 prefix, DNS server address, domain name suffix, SIP server address, and SIP server domain name.

**Figure 17 Network diagram**



### Procedure

You must configure the DHCPv6 server first before configuring the DHCPv6 client. For information about configuring DHCPv6 server, see ["Configuring the DHCPv6 server."](#)

# Configure an IPv6 address for VLAN-interface 2 that is connected to the DHCPv6 server.

```

<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ipv6 address 1::2/48
  
```

# Configure VLAN-interface 2 as a DHCPv6 client for IPv6 prefix acquisition. Configure the DHCPv6 client to support DHCPv6 rapid prefix assignment. Configure the DHCPv6 client to assign an ID to the obtained IPv6 prefix and create a dynamic DHCPv6 option group for saving configuration parameters.

```

[Switch-Vlan-interface2] ipv6 dhcp client pd 1 rapid-commit option-group 1
[Switch-Vlan-interface2] quit
  
```

### Verifying the configuration

# Verify that the DHCPv6 client has obtained an IPv6 prefix and other configuration parameters from the DHCPv6 server.

```

[Switch] display ipv6 dhcp client
Vlan-interface2:
  Type: Stateful client requesting prefix
  State: OPEN
  Client DUID: 0003000100e002000000
  Preferred server:
    Reachable via address: FE80::2E0:1FF:FE00:18
    Server DUID: 0003000100e001000000
  IA_PD: IAID 0x00000642, T1 50 sec, T2 80 sec
  Prefix: 12:34::/48
    Preferred lifetime 100 sec, valid lifetime 200 sec
  
```

Will expire on Feb 4 2014 at 15:37:20(80 seconds left)

DNS server addresses:

2000::FF

Domain name:

example.com

SIP server addresses:

2:2::4

SIP server domain names:

bbb.com

# Verify that the client has obtained an IPv6 prefix.

```
[Switch] display ipv6 prefix 1
```

Number: 1

Type : Dynamic

Prefix: 12:34::/48

Preferred lifetime 100 sec, valid lifetime 200 sec

# After DHCPv6 server is enabled on the device, verify that configuration parameters are saved in a dynamic DHCPv6 option group.

```
[Switch] display ipv6 dhcp option-group 1
```

DHCPv6 option group: 1

DNS server addresses:

Type: Dynamic (DHCPv6 prefix allocation)

Interface: Vlan-interface2

2000::FF

Domain name:

Type: Dynamic (DHCPv6 prefix allocation)

Interface: Vlan-interface2

example.com

SIP server addresses:

Type: Dynamic (DHCPv6 prefix allocation)

Interface: Vlan-interface2

2:2::4

SIP server domain names:

Type: Dynamic (DHCPv6 prefix allocation)

Interface: Vlan-interface2

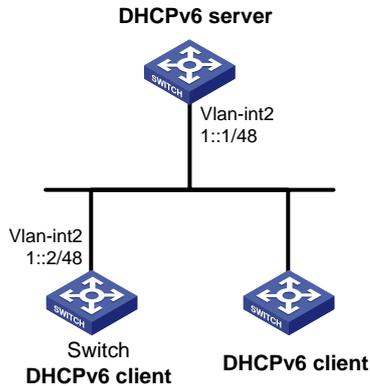
bbb.com

## Example: Configuring IPv6 address and prefix acquisition

### Network configuration

As shown in [Figure 18](#), configure the switch to use DHCPv6 to obtain configuration parameters from the DHCPv6 server. The parameters include IPv6 address, IPv6 prefix, DNS server address, domain name suffix, SIP server address, and SIP server domain name.

**Figure 18 Network diagram**



## Procedure

You must configure the DHCPv6 server before configuring the DHCPv6 client. For information about configuring the DHCPv6 server, see ["Configuring the DHCPv6 server."](#)

# Configure an IPv6 address for VLAN-interface 2 that is connected to the DHCPv6 server.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ipv6 address 1::2/48
```

# Configure VLAN-interface 2 as a DHCPv6 client for IPv6 address and prefix acquisition. Specify IDs for the dynamic IPv6 prefix and dynamic DHCPv6 option group, and configure the client to support rapid address and prefix assignment.

```
[Switch-Vlan-interface2] ipv6 dhcp client stateful prefix 1 rapid-commit option-group 1
[Switch-Vlan-interface2] quit
```

## Verifying the configuration

# Verify that the DHCPv6 client has obtained an IPv6 address, an IPv6 prefix, and other configuration parameters from the DHCPv6 server.

```
[Switch] display ipv6 dhcp client
Vlan-interface2:
  Type: Stateful client requesting address and prefix
  State: OPEN
  Client DUID: 0003000100e002000000
  Preferred server:
    Reachable via address: FE80::2E0:1FF:FE00:18
    Server DUID: 0003000100e001000000
  IA_NA: IAID 0x00000642, T1 50 sec, T2 80 sec
  Address: 1:1::2/128
    Preferred lifetime 100 sec, valid lifetime 200 sec
    Will expire on Mar 27 2014 at 08:02:00 (199 seconds left)
  IA_PD: IAID 0x00000642, T1 50 sec, T2 80 sec
  Prefix: 12:34::/48
    Preferred lifetime 100 sec, valid lifetime 200 sec
    Will expire on Mar 27 2014 at 08:02:00 (199 seconds left)
  DNS server addresses:
    2000::FF
  Domain name:
    example.com
```

```

SIP server addresses:
  2:2::4
SIP server domain names:
  bbb.com

# Verify that the DHCPv6 client has obtained an IPv6 address.
[Switch] display ipv6 interface brief
*down: administratively down
(s): spoofing
Interface                               Physical   Protocol   IPv6 Address
Vlan-interface2                         up        up         1:1::2

```

# Verify that the client has obtained an IPv6 prefix.

```

[Switch] display ipv6 prefix 1
Number: 1
Type   : Dynamic
Prefix: 12:34::/48
Preferred lifetime 100 sec, valid lifetime 200 sec

```

# After DHCPv6 server is enabled on the device, verify that configuration parameters are saved in a dynamic DHCPv6 option group.

```

[Switch] display ipv6 dhcp option-group 1
DNS server addresses:
  Type: Dynamic (DHCPv6 address and prefix allocation)
  Interface: Vlan-interface2
  2000::FF
Domain name:
  Type: Dynamic (DHCPv6 address and prefix allocation)
  Interface: Vlan-interface2
  example.com
SIP server addresses:
  Type: Dynamic (DHCPv6 address and prefix allocation)
  Interface: Vlan-interface2
  2:2::4
SIP server domain names:
  Type: Dynamic (DHCPv6 address and prefix allocation)
  Interface: Vlan-interface2
  bbb.com

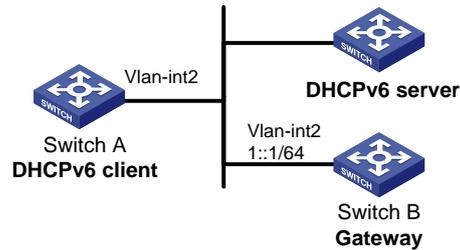
```

## Example: Configuring stateless DHCPv6

### Network configuration

As shown in [Figure 19](#), configure Switch A to use stateless DHCPv6 to obtain configuration parameters except IPv6 address and IPv6 prefix. Switch B acts as the gateway and advertises RA messages periodically.

**Figure 19 Network diagram**



## Procedure

You must configure the DHCPv6 server first before configuring the DHCPv6 client. For information about configuring DHCPv6 server, see "[Configuring the DHCPv6 server.](#)"

1. Configure the gateway Switch B.

# Configure an IPv6 address for VLAN-interface 2.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address 1::1 64
```

# Set the O flag to 1 in RA advertisements to be sent on VLAN-interface 2. Hosts that receive the RA advertisements will obtain information other than IPv6 address through DHCPv6.

```
[SwitchB-Vlan-interface2] ipv6 nd autoconfig other-flag
```

# Disable RA message suppression on GigabitEthernet 1/0/1.

```
[SwitchB-Vlan-interface2] undo ipv6 nd ra halt
```

2. Configure the DHCPv6 client Switch A.

# Enable stateless IPv6 address autoconfiguration on VLAN-interface 2.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ipv6 address auto
```

With stateless IPv6 address autoconfiguration enabled, but no IPv6 address configured for VLAN-interface 2, Switch A automatically generates a link local address. It sends an RS message to Switch B to request configuration information for IPv6 address generation. Upon receiving the RS message, Switch B sends back an RA message. After receiving an RA message with the M flag set to 0 and the O flag set to 1, Switch A performs stateless DHCPv6 to get other configuration parameters.

## Verifying the configuration

# Display the DHCPv6 client information.

```
[SwitchA-Vlan-interface2] display ipv6 dhcp client interface vlan-interface 2
```

Vlan-interface2:

Type: Stateless client

State: OPEN

Client DUID: 00030001000fe2ff0000

Preferred server:

Reachable via address: FE80::213:7FFF:FEF6:C818

Server DUID: 0003000100137ff6c818

DNS server addresses:

1:2:4::5

1:2:4::7

Domain name:

abc.com

# Display the DHCPv6 client statistics.

```
[SwitchA-Vlan-interface2] display ipv6 dhcp client statistics
```

```
Interface                : Vlan-interface2
Packets received        : 1
    Reply                 : 1
    Advertise             : 0
    Reconfigure          : 0
    Invalid              : 0
Packets sent            : 5
    Solicit               : 0
    Request               : 0
    Renew                 : 0
    Rebind                : 0
    Information-request   : 5
    Release                : 0
    Decline               : 0
```

# Configuring DHCPv6 snooping

## About DHCPv6 snooping

It guarantees that DHCPv6 clients obtain IPv6 addresses or prefixes from authorized DHCPv6 servers. Also, it records IP-to-MAC bindings of DHCPv6 clients (called DHCPv6 snooping address entries) and prefix-to-port bindings of DHCPv6 clients (called DHCPv6 snooping prefix entries) for security purposes.

DHCPv6 snooping defines trusted and untrusted ports to make sure that clients obtain IPv6 addresses only from authorized DHCPv6 servers.

- **Trusted**—A trusted port can forward DHCPv6 messages correctly to make sure the clients get IPv6 addresses from authorized DHCPv6 servers.
- **Untrusted**—An untrusted port discards received messages sent by DHCPv6 servers to prevent unauthorized servers from assigning IPv6 addresses.

DHCPv6 snooping reads DHCP-ACK messages received from trusted ports and DHCP-REQUEST messages to create DHCPv6 snooping entries. A DHCPv6 snooping entry can be an address entry or a prefix entry.

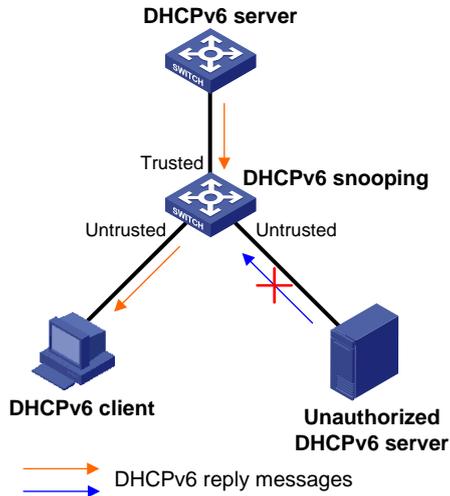
- A DHCPv6 address entry includes the MAC and IP addresses of a client, the port that connects to the DHCPv6 client, and the VLAN. You can use the **display ipv6 dhcp snooping binding** command to display the IP addresses of users for management.
- A DHCPv6 prefix entry includes the prefix and lease information assigned to the client, the port that connects to the DHCPv6 client, and the VLAN. You can use the **display ipv6 dhcp snooping pd binding** command to display the prefixes of the users for management.

## Application of trusted and untrusted ports

Configure ports facing the DHCPv6 server as trusted ports, and configure other ports as untrusted ports.

As shown in [Figure 20](#), configure the DHCPv6 snooping device's port that is connected to the DHCPv6 server as a trusted port. The trusted port forwards response messages from the DHCPv6 server to the client. The untrusted port connected to the unauthorized DHCPv6 server discards incoming DHCPv6 response messages.

Figure 20 Trusted and untrusted ports



## Restrictions and guidelines: DHCPv6 snooping configuration

DHCPv6 snooping works between the DHCPv6 client and server, or between the DHCPv6 client and DHCPv6 relay agent.

DHCPv6 snooping does not work between the DHCPv6 server and DHCPv6 relay agent.

## DHCPv6 snooping tasks at a glance

To configure DHCPv6 snooping, perform the following tasks:

1. [Configuring basic DHCPv6 snooping features](#)
2. (Optional.) [Configuring DHCP snooping support for Option 18](#)
3. (Optional.) [Configuring DHCP snooping support for Option 37](#)
4. (Optional.) [Configuring DHCPv6 snooping entry auto backup](#)
5. (Optional.) [Setting the maximum number of DHCPv6 snooping entries](#)
6. (Optional.) [Configuring DHCPv6 packet rate limit](#)
7. (Optional.) [Enabling DHCPv6-REQUEST check](#)
8. (Optional.) [Configuring a DHCPv6 packet blocking port](#)
9. (Optional.) [Enabling DHCPv6 snooping logging](#)

# Configuring basic DHCPv6 snooping features

## Configuring basic DHCPv6 snooping features in a common network

### Restrictions and guidelines

- To make sure DHCPv6 clients can obtain valid IPv6 addresses, specify the ports connected to authorized DHCPv6 servers as trusted ports. The trusted ports and the ports connected to DHCPv6 clients must be in the same VLAN.
- If you configure DHCPv6 snooping settings on a Layer 2 Ethernet interface that is a member port of a Layer 2 aggregate interface, the settings do not take effect unless the interface is removed from the aggregation group.

### Enabling DHCPv6 snooping

1. Enter system view.  
**system-view**
2. Enable DHCPv6 snooping.  
**ipv6 dhcp snooping enable**  
By default, DHCPv6 snooping is disabled.

### Specifying a DHCPv6 snooping trusted port

3. Enter interface view.  
**interface** *interface-type interface-number*  
This interface must connect to the DHCPv6 server.
4. Specify the port as a trusted port.  
**ipv6 dhcp snooping trust**  
By default, all ports are untrusted ports after DHCPv6 snooping is enabled.

### Enabling recording DHCPv6 snooping entries

5. Enter system view.  
**system-view**
6. Enter interface view.  
**interface** *interface-type interface-number*  
This interface must connect to the DHCPv6 clients.
7. Enable recording DHCPv6 snooping entries. Choose the following tasks as needed:
  - Enable recording DHCPv6 snooping address entries.  
**ipv6 dhcp snooping binding record**  
By default, recording of DHCPv6 snooping address entries is disabled.
  - Enable recording DHCPv6 snooping prefix entries.  
**ipv6 dhcp snooping pd binding record**  
By default, recording of DHCPv6 snooping prefix entries is disabled.

## Configuring DHCP snooping support for Option 18

1. Enter system view.  
**system-view**

2. Enter interface view.  
**interface** *interface-type interface-number*
3. Enable DHCP snooping support for Option 18.  
**ipv6 dhcp snooping option interface-id enable**  
By default, DHCP snooping support for Option 18 is disabled.
4. (Optional.) Specify the content as the interface ID.  
**ipv6 dhcp snooping option interface-id [ vlan *vlan-id* ] string *interface-id***  
By default, the DHCPv6 snooping device uses its DUID as the content for Option 18.

## Configuring DHCP snooping support for Option 37

1. Enter system view.  
**system-view**
2. Enter interface view.  
**interface** *interface-type interface-number*
3. Enable DHCP snooping support for Option 37.  
**ipv6 dhcp snooping option remote-id enable**  
By default, DHCP snooping support for Option 37 is disabled.
4. (Optional.) Specify the content as the remote ID.  
**ipv6 dhcp snooping option remote-id [ vlan *vlan-id* ] string *remote-id***  
By default, the DHCPv6 snooping device uses its DUID as the content for Option 37.

## Configuring DHCPv6 snooping entry auto backup

### About DHCPv6 snooping entry auto backup

The auto backup feature saves DHCPv6 snooping entries to a backup file, and allows the DHCPv6 snooping device to download the entries from the backup file at reboot. The entries on the DHCPv6 snooping device cannot survive a reboot. The auto backup helps the security features provide services if these features (such as IP source guard) must use DHCPv6 snooping entries for user authentication.

### Restrictions and guidelines

- If you disable DHCPv6 snooping with the **undo ipv6 dhcp snooping enable** command, the device deletes all DHCPv6 snooping entries, including those stored in the backup file.
- If you execute the **ipv6 dhcp snooping binding database filename** command, the DHCPv6 snooping device backs up DHCPv6 snooping entries immediately and runs auto backup. This command automatically creates the file if you specify a non-existent file.
- The waiting period starts when a DHCPv6 snooping entry is learned, updated, or removed. The DHCPv6 snooping device updates the backup file when the specified waiting period is reached. All changed entries during the period will be saved to the backup file. If no DHCPv6 snooping entry changes, the backup file is not updated.

### Procedure

1. Enter system view.  
**system-view**
2. Configure the DHCPv6 snooping device to back up DHCPv6 snooping entries to a file.

```
ipv6 dhcp snooping binding database filename { filename | url url
[ username username [ password { cipher | simple } string ] ] }
```

By default, the DHCPv6 snooping device does not back up the DHCPv6 snooping entries.

3. (Optional.) Manually save DHCPv6 snooping entries to the backup file.

```
ipv6 dhcp snooping binding database update now
```

4. (Optional.) Set the waiting time after a DHCPv6 snooping entry change for the DHCPv6 snooping device to update the backup file.

```
ipv6 dhcp snooping binding database update interval interval
```

By default, the DHCP snooping device waits 300 seconds to update the backup file after a DHCP snooping entry change. If no DHCP snooping entry changes, the backup file is not updated.

## Setting the maximum number of DHCPv6 snooping entries

### About setting the maximum number of DHCPv6 snooping entries

Perform this task to prevent the system resources from being overused.

#### Procedure

1. Enter system view.  
**system-view**
2. Enter interface view.  
**interface** *interface-type interface-number*
3. Set the maximum number of DHCPv6 snooping entries for the interface to learn.  
**ipv6 dhcp snooping max-learning-num** *max-number*

By default, the number of DHCPv6 snooping entries for an interface to learn is not limited.

## Configuring DHCPv6 packet rate limit

### About DHCPv6 packet rate limit

This DHCPv6 packet rate limit feature discards exceeding DHCPv6 packets to prevent attacks that send large numbers of DHCPv6 packets.

#### Restrictions and guidelines

The rate set on the Layer 2 aggregate interface applies to all members of the aggregate interface. If a member interface leaves the aggregation group, it uses the rate set in its Ethernet interface view.

#### Procedure

1. Enter system view.  
**system-view**
2. Enter interface view.  
**interface** *interface-type interface-number*
3. Set the maximum rate at which an interface can receive DHCPv6 packets.  
**ipv6 dhcp snooping rate-limit** *rate*

By default, incoming DHCPv6 packets on an interface are not rate limited.

# Enabling DHCPv6-REQUEST check

## About DHCPv6-REQUEST check

Perform this task to use the DHCPv6-REQUEST check feature to protect the DHCPv6 server against DHCPv6 client spoofing attacks. Attackers can forge DHCPv6-RENEW messages to renew leases for legitimate DHCPv6 clients that no longer need the IP addresses. The forged messages disable the victim DHCPv6 server from releasing the IP addresses. Attackers can also forge DHCPv6-DECLINE or DHCPv6-RELEASE messages to terminate leases for legitimate DHCPv6 clients that still need the IP addresses.

The DHCPv6-REQUEST check feature enables the DHCPv6 snooping device to check every received DHCPv6-RENEW, DHCPv6-DECLINE, or DHCPv6-RELEASE message against DHCPv6 snooping entries.

- If any criterion in an entry is matched, the device compares the entry with the message information.
  - If they are consistent, the device considers the message valid and forwards it to the DHCPv6 server.
  - If they are different, the device considers the message forged and discards it.
- If no matching entry is found, the device forwards the message to the DHCPv6 server.

## Procedure

1. Enter system view.  
**system-view**
2. Enter interface view.  
**interface** *interface-type interface-number*
3. Enable DHCPv6-REQUEST check.  
**ipv6 dhcp snooping check request-message**  
By default, DHCPv6-REQUEST check is disabled.

# Configuring a DHCPv6 packet blocking port

## About DHCPv6 packet blocking port

Perform this task to configure a port as a DHCPv6 packet blocking port. The DHCPv6 packet blocking port drops all incoming DHCP requests.

## Procedure

1. Enter system view.  
**system-view**
2. Enter interface view.  
**interface** *interface-type interface-number*
3. Configure the port to block DHCPv6 requests.  
**ipv6 dhcp snooping deny**  
By default, the port does not block DHCPv6 requests.

# Enabling DHCPv6 snooping logging

## About DHCPv6 snooping logging

The DHCPv6 snooping logging feature enables the DHCPv6 snooping device to generate DHCPv6 snooping logs and send them to the information center. The information helps administrators locate and solve problems. For information about the log destination and output rule configuration in the information center, see *Network Management and Monitoring Configuration Guide*.

## Restrictions and guidelines

As a best practice, disable this feature if the log generation affects the device performance.

## Procedure

1. Enter system view.  
**system-view**
2. Enable DHCPv6 snooping logging.  
**ipv6 dhcp snooping log enable**  
By default, DHCPv6 snooping logging is disabled.

# Display and maintenance commands for DHCPv6 snooping

Execute **display** commands in any view, and **reset** commands in user view.

Task	Command
Display DHCPv6 snooping address entries.	<b>display ipv6 dhcp snooping binding</b> [ <b>address</b> <i>ipv6-address</i> [ <b>vlan</b> <i>vlan-id</i> ] ]
Display information about the file that stores DHCPv6 snooping entries.	<b>display ipv6 dhcp snooping binding database</b>
Display DHCPv6 packet statistics for DHCPv6 snooping.	<b>display ipv6 dhcp snooping packet statistics</b> [ <b>slot</b> <i>slot-number</i> ]
Display DHCPv6 snooping prefix entries.	<b>display ipv6 dhcp snooping pd binding</b> [ <b>prefix</b> <i>prefix/prefix-length</i> [ <b>vlan</b> <i>vlan-id</i> ] ]
Display information about trusted ports.	<b>display ipv6 dhcp snooping trust</b>
Clear DHCPv6 snooping address entries.	<b>reset ipv6 dhcp snooping binding</b> { <b>all</b>   <b>address</b> <i>ipv6-address</i> [ <b>vlan</b> <i>vlan-id</i> ] }
Clear DHCPv6 packet statistics for DHCPv6 snooping.	<b>reset ipv6 dhcp snooping packet statistics</b> [ <b>slot</b> <i>slot-number</i> ]
Clear DHCPv6 snooping prefix entries.	<b>reset ipv6 dhcp snooping pd binding</b> { <b>all</b>   <b>prefix</b> <i>prefix/prefix-length</i> [ <b>vlan</b> <i>vlan-id</i> ] }

# DHCPv6 snooping configuration examples

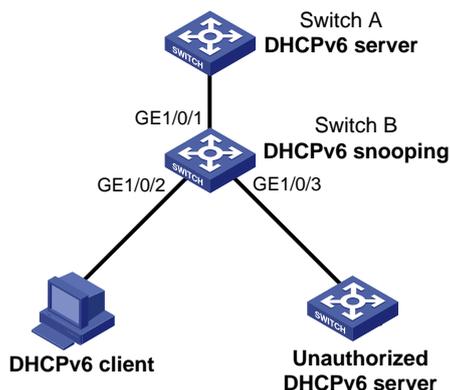
## Example: Configuring DHCPv6 snooping

### Network configuration

As shown in [Figure 21](#), Switch B is connected to the authorized DHCPv6 server through GigabitEthernet 1/0/1, to the unauthorized DHCPv6 server through GigabitEthernet 1/0/3, and to the DHCPv6 client through GigabitEthernet 1/0/2.

Configure only the port connected to the authorized DHCPv6 server to forward the responses from the DHCPv6 server. Enable the DHCPv6 snooping device to record DHCPv6 snooping address entries.

**Figure 21 Network diagram**



### Procedure

# Enable DHCPv6 snooping.

```
<SwitchB> system-view  
[SwitchB] ipv6 dhcp snooping enable
```

# Specify GigabitEthernet 1/0/1 as a trusted port.

```
[SwitchB] interface gigabitethernet 1/0/1  
[SwitchB-GigabitEthernet1/0/1] ipv6 dhcp snooping trust  
[SwitchB-GigabitEthernet1/0/1] quit
```

# Enable recording DHCPv6 snooping address entries on GigabitEthernet 1/0/2.

```
[SwitchB] interface gigabitethernet 1/0/2  
[SwitchB-GigabitEthernet1/0/2] ipv6 dhcp snooping binding record  
[SwitchB-GigabitEthernet1/0/2] quit
```

### Verifying the configuration

# Verify that the DHCPv6 client obtains an IPv6 address and all other configuration parameters only from the authorized DHCPv6 server. (Details not shown.)

# Display DHCPv6 snooping address entries on the DHCPv6 snooping device.

```
[SwitchB] display ipv6 dhcp snooping binding
```