目 录

1 DHCPv6 简介

1.1 DHCPv6概述

DHCPv6（Dynamic Host Configuration Protocol for IPv6，支持 IPv6 的动态主机配置协议）是针对 IPv6 编址方案设计的，为主机分配 IPv6 前缀、IPv6 地址和其他网络配置参数的协议。

与其他 IPv6 地址分配方式（手工配置、通过路由器公告消息中的网络前缀无状态自动配置等）相比，DHCPv6 具有以下优点：

- 更好地控制地址的分配。通过 DHCPv6 不仅可以记录为主机分配的地址，还可以为特定主机分配特定的地址，以便于网络管理。
- 为设备分配前缀，便于全网络的自动配置和管理。
- 除了 IPv6 前缀、IPv6 地址外，还可以为主机分配 DNS 服务器、域名等网络配置参数。

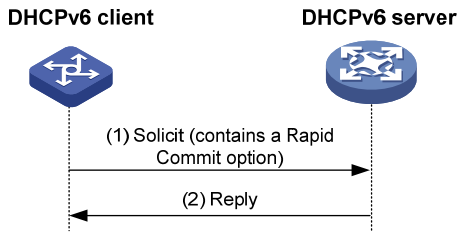
1.2 DHCPv6地址/前缀分配过程

DHCPv6 服务器为客户端分配地址/前缀的过程分为两类：

- 交互两个消息的快速分配过程
- 交互四个消息的分配过程

1.2.1 交互两个消息的快速分配过程

图1-1 地址/前缀快速分配过程



如 图 1-1 所示，地址/前缀快速分配过程为：

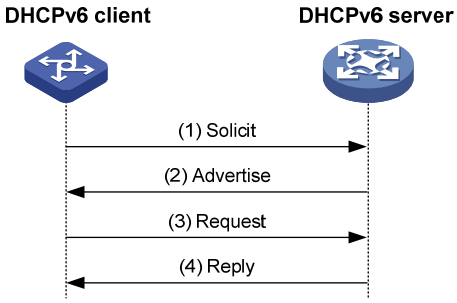
(1) DHCPv6 客户端在发送的 Solicit 消息中携带 Rapid Commit 选项，标识客户端希望服务器能够快速为其分配地址/前缀和网络配置参数；

(2) 如果DHCPv6 服务器支持快速分配过程，则直接返回Reply消息，为客户端分配IPv6 地址/前缀和其他网络配置参数。如果DHCPv6 服务器不支持快速分配过程，则采用“1.2.2 交互四个消息的分配过程”为客户端分配IPv6 地址/前缀和其他网络配置参数。

1.2.2 交互四个消息的分配过程

交互四个消息的分配过程如 图 1-2 所示。

图1-2 交互四个消息的分配过程



交互四个消息分配过程的简述如 表 1-1。

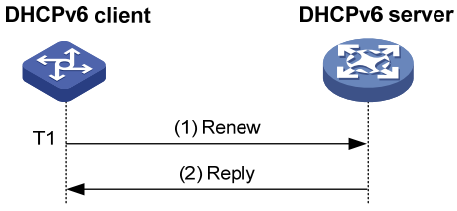
表1-1 交互四个消息的分配过程

步骤	发送的消息	说明
(1)	Solicit	DHCPv6客户端发送该消息，请求DHCPv6服务器为其分配IPv6地址/前缀和网络配置参数
(2)	Advertise	如果Solicit消息中没有携带Rapid Commit选项，或Solicit消息中携带Rapid Commit选项，但服务器不支持快速分配过程，则DHCPv6服务器回复该消息，通知客户端可以为其分配的地址/前缀和网络配置参数
(3)	Request	如果DHCPv6客户端接收到多个服务器回复的Advertise消息，则根据消息接收的先后顺序、服务器优先级等，选择其中一台服务器，并向该服务器发送Request消息，请求服务器确认为其分配地址/前缀和网络配置参数
(4)	Reply	DHCPv6服务器回复该消息，确认将地址/前缀和网络配置参数分配给客户端使用

1.3 地址/前缀租约更新过程

DHCPv6 服务器分配给客户端的 IPv6 地址/前缀具有一定的租借期限。租借期限由有效生命期（Valid Lifetime）决定。地址/前缀的租借时间到达有效生命期后，DHCPv6 客户端不能再使用该地址/前缀。在有效生命期到达之前，如果 DHCPv6 客户端希望继续使用该地址/前缀，则需要更新地址/前缀租约。

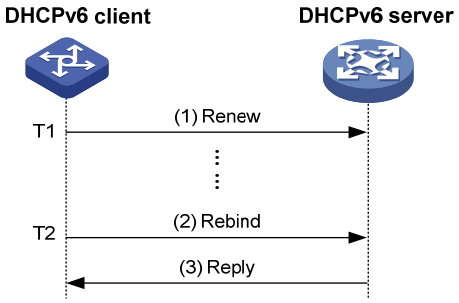
图1-3 通过 Renew 更新地址/前缀租约



如 图 1-3 所示，地址/前缀租借时间到达时间T1（推荐值为首选生命期Preferred Lifetime的一半）时，DHCPv6 客户端会向为它分配地址/前缀的DHCPv6 服务器单播发送Renew报文，以进行地址/前缀租约的更新。如果客户端可以继续使用该地址/前缀，则DHCPv6 服务器回应续约成功的Reply

报文，通知DHCPv6 客户端已经成功更新地址/前缀租约；如果该地址/前缀不可以再分配给该客户端，则DHCPv6 服务器回应续约失败的Reply报文，通知客户端不能获得新的租约。

图1-4 通过 Rebind 更新地址/前缀租约



如 图 1-4 所示，如果在T1 时发送Renew请求更新租约，但是没有收到DHCPv6 服务器的回应报文，则DHCPv6 客户端会在T2（推荐值为首选生命期的 0.8 倍）时，向所有DHCPv6 服务器组播发送Rebind报文请求更新租约。如果客户端可以继续使用该地址/前缀，则DHCPv6 服务器回应续约成功的Reply报文，通知DHCPv6 客户端已经成功更新地址/前缀租约；如果该地址/前缀不可以再分配给该客户端，则DHCPv6 服务器回应续约失败的Reply报文，通知客户端不能获得新的租约；如果DHCPv6 客户端没有收到服务器的应答报文，则到达有效生命期后，客户端停止使用该地址/前缀。

说明

有效生命期和首选生命期的详细介绍请参见“三层技术-IP 业务配置指导”中的“IPv6 基础”。

1.4 DHCPv6无状态配置

1.4.1 DHCPv6 无状态配置简介

DHCPv6 服务器可以为已经具有 IPv6 地址/前缀的客户端分配其他网络配置参数，该过程称为DHCPv6 无状态配置。

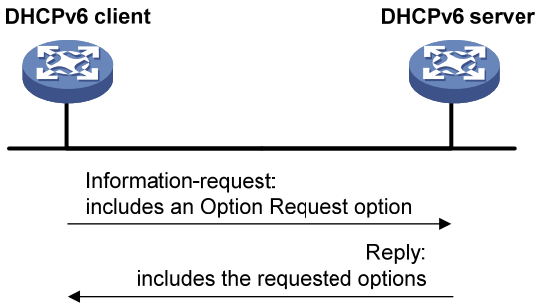
DHCPv6 客户端通过地址无状态自动配置功能成功获取 IPv6 地址后，如果接收到的 RA（Router Advertisement，路由器通告）报文中 M 标志位（Managed address configuration flag，被管理地址配置标志位）为 0、O 标志位（Other stateful configuration flag，其他配置标志位）为 1，则 DHCPv6 客户端会自动启动 DHCPv6 无状态配置功能，以获取除地址/前缀外的其他网络配置参数。

说明

地址无状态自动配置是指节点根据路由器发现/前缀发现所获取的信息，自动配置 IPv6 地址。详细介绍请参见“三层技术-IP 业务配置指导”的“IPv6 基础”。

1.4.2 DHCPv6 无状态配置过程

图1-5 DHCPv6 无状态配置工作过程



如 图 1-5 所示，DHCPv6 无状态配置的具体过程为：

(1) 客户端以组播的方式向 DHCPv6 服务器发送 Information-request 报文，该报文中携带 Option Request 选项，指定客户端需要从服务器获取的配置参数。

(2) 服务器收到 Information-request 报文后，为客户端分配网络配置参数，并单播发送 Reply 报文将网络配置参数返回给客户端。

(3) 客户端检查 Reply 报文中提供的信息，如果与 Information-request 报文中请求的配置参数相符，则按照 Reply 报文中提供的参数进行网络配置；否则，忽略该参数。如果接收到多个 Reply 报文，客户端将选择最先收到的 Reply 报文，并根据该报文中提供的参数完成客户端无状态配置。

1.5 协议规范

与 DHCPv6 相关的协议规范有：

- 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

2 DHCPv6 客户端配置

2.1 DHCPv6客户端简介

设备作为 DHCPv6 客户端时，只支持 DHCPv6 无状态配置，即只能通过 DHCPv6 获取除地址/前缀外的其他网络配置参数，不能获取 IPv6 地址和前缀。

DHCPv6 客户端通过地址无状态自动配置功能成功获取 IPv6 地址后，如果接收到的 RA 报文中 M 标志位为 0、O 标志位为 1，则设备会自动启动 DHCPv6 无状态配置功能，以获取除地址/前缀外的其他网络配置参数。

2.2 配置DHCPv6客户端

2.2.1 配置准备

为了使客户端能够通过 DHCPv6 无状态配置成功获取网络配置参数，需要确保 DHCPv6 服务器可用。

2.2.2 配置步骤

表2-1 配置 DHCPv6 客户端

操作	命令	说明
进入系统视图	**system-view**	-
使能IPv6报文转发功能	**ipv6**	必选
进入接口视图	**interface** *interface-type interface-number*	-
使能IPv6地址无状态自动配置功能	**ipv6 address auto**	必选


说明

ipv6 address auto 命令的详细介绍请参见“三层技术-IP 业务命令参考”中的“IPv6 基础”。

2.3 配置DHCPv6客户端发送的DHCPv6报文的DSCP优先级

在 IPv6 报文头中，包含一个 8bit 的 Traffic class 字段，用于标识 IP 报文的服务类型。RFC 2474 对这 8 个 bit 进行了定义，将前 6 个 bit 定义为 DSCP 优先级，最后 2 个 bit 作为保留位。在报文传输的过程中，DSCP 优先级可以被网络设备识别，并作为报文传输优先程度的参考。

用户可以对 DHCPv6 客户端发送的 DHCPv6 报文的 DSCP 优先级进行配置。

表2-2 配置 DHCPv6 客户端发送的 DHCPv6 报文的 DSCP 优先级

操作	命令	说明
进入系统视图	**system-view**	-
配置DHCPv6客户端发送的DHCPv6报文的DSCP优先级	**ipv6 dhcp client dscp** *dscp-value*	可选 缺省情况下，DHCPv6客户端发送的DHCPv6报文的DSCP优先级为56

2.4 DHCPv6客户端显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 DHCPv6 客户端的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 DHCPv6 客户端的统计信息。

表2-3 DHCPv6 客户端显示和维护

操作	命令
显示DHCPv6客户端的信息	**display ipv6 dhcp client** [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示DHCPv6客户端的统计信息	**display ipv6 dhcp client statistics** [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示本设备DUID	**display ipv6 dhcp duid** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除DHCPv6客户端的统计信息	**reset ipv6 dhcp client statistics** [**interface** *interface-type interface-number*]

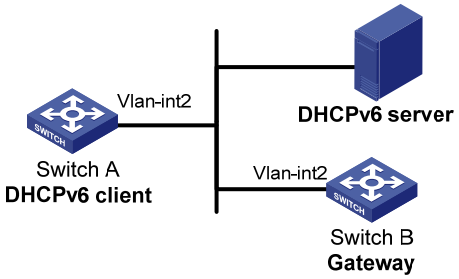
2.5 DHCPv6无状态配置典型配置举例

1. 组网需求

- Switch A 通过 DHCPv6 无状态配置获取域名服务器、域名等信息；
- Switch B 作为网关，周期性发布 RA 消息。

2. 组网图

图2-1 DHCPv6 无状态配置组网图



3. 配置步骤

(1) 配置网关 Switch B

使能 IPv6 报文转发功能。

```
<SwitchB> system-view
[SwitchB] ipv6
```

配置 VLAN 接口 2 的 IPv6 地址。

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address 1::1 64
```

配置 RA 消息中 O 标志位为 1。

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

配置允许发送 RA 消息。

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

(2) 配置 DHCPv6 客户端 Switch A

使能 IPv6 报文转发功能。

```
<SwitchA> system-view
[SwitchA] ipv6
```

在 VLAN 接口 2 上使能 IPv6 地址无状态自动配置功能。

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ipv6 address auto
```

执行此命令后，如果 VLAN 接口 2 下没有配置地址，Switch A 会自动生成本地链路地址，并主动发送 RS（Router Solicitation，路由器请求）报文，请求网关 Switch B 立即回应 RA 报文。

4. 验证配置结果

如果收到的 RA 报文中 M 标志位为 0、O 标志位为 1，Switch A 就会启动 DHCPv6 客户端无状态配置。

可以通过 **display ipv6 dhcp client** 命令查看当前客户端的配置信息，如果从服务器成功获取了配置，将会有类似的显示信息。

```
[SwitchA-Vlan-interface2] display ipv6 dhcp client interface vlan-interface 2
Vlan-interface2 is in stateless DHCPv6 client mode
State is OPEN
Preferred Server:
    Reachable via address     :  FE80::213:7FFF:FEF6:C818
    DUID                      :  0003000100137ff6c818
```

可以通过 **display ipv6 dhcp client statistics** 命令查看当前客户端的统计信息。

```
[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
        Confirm               :  0
        Renew                 :  0
        Rebind                :  0
        Information-request   :  5
        Release               :  0
        Decline               :  0
```

3 DHCPv6 Snooping配置

说明

- 设备只有位于 DHCPv6 客户端与 DHCPv6 服务器之间，或 DHCPv6 客户端与 DHCPv6 中继之间时，DHCPv6 Snooping 功能配置后才能正常工作；设备位于 DHCPv6 服务器与 DHCPv6 中继之间时，DHCPv6 Snooping 功能配置后不能正常工作。
- DHCPv6 Snooping 中对于接口的相关配置，目前只能在二层以太网端口或二层聚合接口上进行。关于聚合接口的详细介绍，请参见“二层技术-以太网交换配置指导”中的“以太网链路聚合”。

3.1 DHCPv6 Snooping简介

DHCPv6 Snooping 是 DHCPv6 的一种安全特性，具有如下功能：

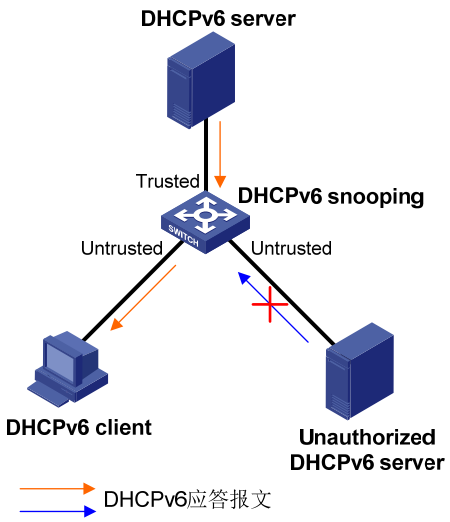
- 保证客户端从合法的服务器获取 IPv6 地址。
- 记录 DHCPv6 客户端 IPv6 地址与 MAC 地址的对应关系。

1. 保证客户端从合法的服务器获取IPv6 地址

网络中如果存在私自架设的伪 DHCPv6 服务器，则可能导致 DHCPv6 客户端获取错误的 IPv6 地址和网络配置参数，无法正常通信。为了使 DHCPv6 客户端能通过合法的 DHCPv6 服务器获取 IPv6 地址，DHCPv6 Snooping 安全机制允许将端口设置为信任端口（Trusted Port）和不信任端口（Untrusted Port）：

- 信任端口正常转发接收到的 DHCPv6 报文。
- 不信任端口接收到 DHCPv6 服务器发送的应答报文后，丢弃该报文。

图3-1 信任端口和非信任端口



连接DHCPv6 服务器、DHCPv6 中继或其他DHCPv6 Snooping设备的端口需要设置为信任端口，其他端口设置为不信任端口，从而保证DHCPv6 客户端只能从合法的DHCPv6 服务器获取地址，私自架设的伪DHCPv6 服务器无法为DHCPv6 客户端分配地址。如 图 3-1 中，将连接DHCPv6 服务器的端口设置为信任端口，其他端口设置为非信任端口。

2. 记录DHCPv6 客户端IPv6 地址与MAC地址的对应关系

DHCPv6 Snooping 通过监听 DHCPv6 报文，记录 DHCPv6 Snooping 表项，其中包括客户端的 MAC 地址、获取到的 IPv6 地址、与 DHCPv6 客户端连接的端口及该端口所属的 VLAN 等信息。网络管理员可以通过 **display ipv6 dhcp snooping user-binding dynamic** 命令查看客户端获取的 IPv6 地址信息，以便了解用户上网时所用的 IPv6 地址，并对其进行管理和监控。

3.2 使能DHCPv6 Snooping

使能 DHCPv6 Snooping 功能，必须首先在系统视图下全局使能 DHCPv6 Snooping 功能。全局使能 DHCPv6 Snooping 功能，并正确地配置信任端口和非信任端口后，可以保证客户端从合法的服务器获取 IPv6 地址。但是，此时不会记录 DHCPv6 Snooping 表项。

如果需要记录 DHCPv6 Snooping 表项，则需要在全局使能 DHCPv6 Snooping 功能的基础上，在 VLAN 视图下使能 VLAN 内的 DHCPv6 Snooping 功能。使能 VLAN 内的 DHCPv6 Snooping 功能，还可以实现 DHCPv6 Snooping 设备接收到该 VLAN 内客户端发送的请求报文后，只通过该 VLAN 内的信任端口转发该请求报文，不会通过其他非信任端口转发请求报文，以减轻网络负担。

表3-1 使能 DHCPv6 Snooping

操作	命令	说明
进入系统视图	**system-view**	-
全局使能DHCPv6 Snooping功能	**ipv6 dhcp snooping enable**	必选 缺省情况下，DHCPv6 Snooping功能处于关闭状态
进入VLAN视图	**vlan** *vlan-id*	-
在VLAN内使能DHCPv6 Snooping功能	**ipv6 dhcp snooping vlan enable**	可选 缺省情况下，VLAN内DHCPv6 Snooping功能处于关闭状态

3.3 配置DHCPv6 Snooping信任端口

DHCPv6 Snooping 将端口分为两种：

- 信任端口：正常转发接收到的 DHCPv6 报文。
- 不信任端口：接收到 DHCPv6 服务器发送的应答报文后，丢弃该报文。

使能 VLAN 内的 DHCPv6 Snooping 功能，DHCPv6 Snooping 设备接收到该 VLAN 内客户端发送的请求报文后，只通过该 VLAN 内的信任端口转发该请求报文，不会通过其他非信任端口转发请求报文，以减轻网络负担。

表3-2 配置 DHCPv6 Snooping 信任端口

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置端口为信任端口	**ipv6 dhcp snooping trust**	必选 缺省情况下，全局使能DHCPv6 Snooping功能后，设备的所有端口均为不信任端口

说明

- 为了使 DHCPv6 客户端能从合法的 DHCPv6 服务器获取 IPv6 地址，必须将与合法 DHCPv6 服务器相连的端口设置为信任端口，且设置的信任端口和与 DHCPv6 客户端相连的端口必须在同一个 VLAN 内。
- 如果二层以太网端口加入了聚合组，则加入聚合组之前和加入聚合组之后在该接口上进行的 DHCPv6 Snooping 相关配置不会生效；该接口退出聚合组后，DHCPv6 Snooping 的配置才会生效。

3.4 配置接口动态学习DHCPv6 Snooping表项的最大数目

通过本配置可以限制接口动态学习 DHCPv6 Snooping 表项的最大数目，以防止接口学习到大量 DHCPv6 Snooping 表项，占用过多地系统资源。

表3-3 配置接口动态学习 DHCPv6 Snooping 表项的最大数目

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置接口动态学习DHCPv6 Snooping表项的最大数目	**ipv6 dhcp snooping max-learning-num** *number*	可选 缺省情况下，不限制接口动态学习DHCPv6 Snooping表项的数目

3.5 配置DHCPv6 Snooping支持Option 18和Option 37

Option 18 称为接口 ID 选项（Interface ID）、Option 37 称为远程 ID 选项（Remote ID），DHCPv6 Snooping 设备接收到 DHCPv6 客户端发送给 DHCPv6 服务器的请求报文后，在该报文中添加 Option 18 或 Option 37，并转发给 DHCPv6 服务器。

图3-2 Option 18 选项格式

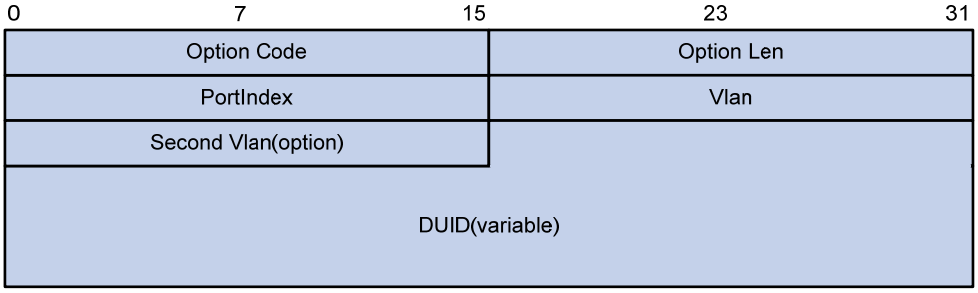
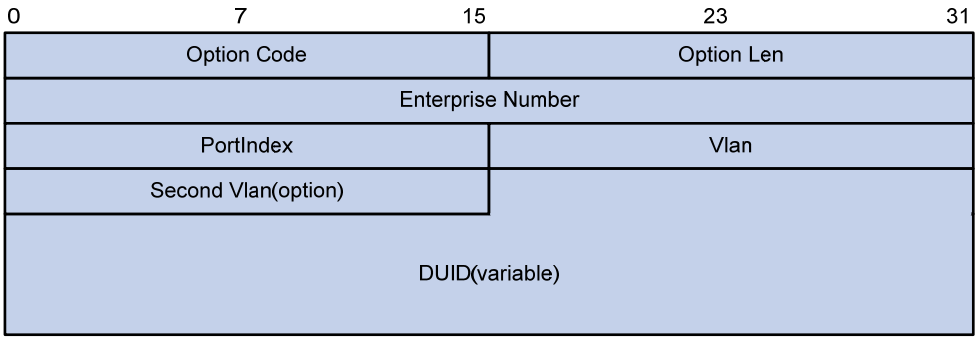


图3-3 Option 37 选项格式



说明

选项格式中的 Second Vlan 字段为可选，如果报文中不含有 Second Vlan，则 Option 18 或 Option 37 中也不包含 Second Vlan 内容。

表3-4 配置 DHCPv6 Snooping 支持 Option 18 和 Option 37

操作	命令	说明
进入系统视图	**system-view**	-
全局使能DHCPv6 Snooping功能	**ipv6 dhcp snooping enable**	必选 缺省情况下，DHCPv6 Snooping功能处于关闭状态
进入VLAN视图	**vlan** *vlan-id*	-
在VLAN内使能DHCPv6 Snooping功能	**ipv6 dhcp snooping vlan enable**	必选 缺省情况下，VLAN内DHCPv6 Snooping功能处于关闭状态
进入二层以太网端口视图或二层聚合接口视图	**interface** *interface-type interface-number*	-
使能DHCPv6 Snooping支持Option 18功能	**ipv6 dhcp snooping option interface-id enable**	必选 缺省情况下，禁止DHCPv6 Snooping支持Option 18功能

操作	命令	说明
配置Option 18选项中的DUID	**ipv6 dhcp snooping option interface-id string** *interface-id*	可选 缺省情况下，Option 18选项中的DUID为本设备的DUID
使能DHCPv6 Snooping支持Option 37功能	**ipv6 dhcp snooping option remote-id enable**	必选 缺省情况下，禁止DHCPv6 Snooping支持Option 37功能
配置Option 37选项中的DUID	**ipv6 dhcp snooping option remote-id string** *remote-id*	可选 缺省情况下，Option 37选项中的DUID为本设备的DUID

3.6 DHCPv6 Snooping显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示 DHCPv6 Snooping 的配置情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 DHCPv6 Snooping 表项信息。

表3-5 DHCPv6 Snooping 显示和维护

操作	命令
显示DHCPv6 Snooping信任端口信息	**display ipv6 dhcp snooping trust** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示DHCPv6 Snooping表项信息	**display ipv6 dhcp snooping user-binding** { *ipv6-address* | **dynamic** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除DHCPv6 Snooping表项	**reset ipv6 dhcp snooping user-binding** { *ipv6-address* | **dynamic** }

3.7 DHCPv6 Snooping典型配置举例

1. 组网需求

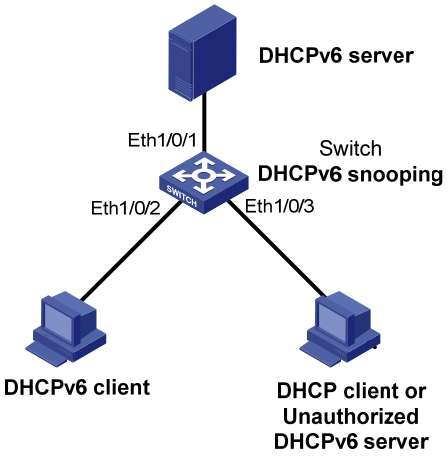
Switch 通过以太网端口 Ethernet1/0/1 连接到 DHCPv6 服务器，通过以太网端口 Ethernet1/0/2、Ethernet1/0/3 连接到 DHCPv6 客户端。Ethernet1/0/1、Ethernet1/0/2 和 Ethernet1/0/3 都属于 VLAN 2。

要求：

- 与 DHCPv6 服务器相连的端口可以转发 DHCPv6 服务器的响应报文，而其他端口不转发 DHCPv6 服务器的响应报文。
- 记录 DHCPv6 客户端 IPv6 地址及 MAC 地址的绑定关系。

2. 组网图

图3-4 DHCPv6 Snooping 组网示意图



3. 配置步骤

全局使能 DHCPv6 Snooping 功能。

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

将端口 Ethernet1/0/1、Ethernet1/0/2 和 Ethernet1/0/3 加入 VLAN 2。

```
[Switch] vlan 2
[Switch-vlan2] port Ethernet 1/0/1 Ethernet 1/0/2 Ethernet 1/0/3
```

在 VLAN 2 内使能 DHCPv6 Snooping 功能。

```
[Switch-vlan2] ipv6 dhcp snooping vlan enable
[Switch] quit
```

配置 Ethernet1/0/1 端口为信任端口。

```
[Switch] interface Ethernet 1/0/1
[Switch-Ethernet1/0/1] ipv6 dhcp snooping trust
```

验证配置结果。

配置完成后，通过 Ethernet1/0/2 连接 DHCPv6 客户端、Ethernet1/0/1 连接 DHCPv6 服务器，则可以发现 DHCPv6 客户端能够从 DHCPv6 服务器获取 IPv6 地址。通过 **display ipv6 dhcp snooping user-binding** 命令可以查看生成的 DHCPv6 Snooping 表项。如果 Ethernet1/0/3 连接私自架设的伪 DHCPv6 服务器，则该服务器无法为 DHCPv6 客户端分配 IPv6 地址。