

# H3C S5130S-SI[LI]&S5120V2-SI[LI]&S5110V2-SI& S5000V3-EI&S5000E-X&S3100V3-SI 系列以太网交换机

## 三层技术-IP 业务配置指导

新华三技术有限公司  
<http://www.h3c.com>

资料版本：6W103-20190822  
产品版本：Release 612x 系列

**Copyright © 2019 新华三技术有限公司及其许可者 版权所有，保留一切权利。**

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

# 前言

本配置指导主要介绍了 IP 业务相关技术的原理及具体配置方法。  
前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [资料意见反馈](#)

## 读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

## 本书约定

### 1. 命令行格式约定






格 式	意 义
<b>粗体</b>	命令行关键字（命令中保持不变、必须照输的部分）采用 <b>加粗</b> 字体表示。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x   y   ... }	表示从多个选项中仅选取一个。
[ x   y   ... ]	表示从多个选项选取一个或者不选。
{ x   y   ... } *	表示从多个选项中至少选取一个。
[ x   y   ... ] *	表示从多个选项选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1~n次。
#	由“#”号开始的行表示为注释行。

### 2. 图形界面格式约定

格 式	意 义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

## 5. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

## 资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

**E-mail: [info@h3c.com](mailto:info@h3c.com)**

感谢您的反馈，让我们做得更好！

# 目 录

<b>1 ARP</b>	<b>1-1</b>
1.1 ARP简介	1-1
1.1.1 ARP报文结构	1-1
1.1.2 ARP地址解析过程	1-1
1.1.3 ARP表项类型	1-2
1.2 ARP配置任务简介	1-3
1.3 手工添加静态ARP表项	1-4
1.3.1 手工添加短静态ARP表项	1-4
1.3.2 手工添加长静态ARP表项	1-4
1.3.3 手工添加多端口ARP表项	1-4
1.4 配置动态ARP表项的相关功能	1-5
1.4.1 配置设备学习动态ARP表项的最大数目	1-5
1.4.2 配置接口学习动态ARP表项的最大数目	1-6
1.4.3 配置动态ARP表项的老化时间	1-6
1.4.4 开启动态ARP表项的检查功能	1-6
1.5 将IRF主设备的ARP表项同步到其他所有IRF从设备	1-7
1.6 开启ARP日志信息功能	1-7
1.7 ARP显示和维护	1-8
1.8 ARP典型配置举例	1-8
1.8.1 长静态ARP表项配置举例	1-8
1.8.2 短静态ARP表项配置举例	1-10
1.8.3 多端口ARP表项配置举例	1-11
<b>2 免费ARP</b>	<b>2-1</b>
2.1 免费ARP简介	2-1
2.1.1 IP地址冲突检测	2-1
2.1.2 免费ARP报文学习	2-1
2.1.3 定时发送免费ARP	2-1
2.2 免费ARP配置任务简介	2-2
2.3 开启源IP地址冲突提示功能	2-2
2.4 开启免费ARP报文学习功能	2-2
2.5 开启定时发送免费ARP功能	2-3
2.6 开启设备收到非同一网段ARP请求时发送免费ARP报文功能	2-3

2.7 配置当接口MAC地址变化时，该接口重新发送免费ARP报文的次数和时间间隔 .....	2-3
<b>3 代理ARP.....</b>	<b>3-1</b>
3.1 代理ARP简介 .....	3-1
3.2 开启普通代理ARP功能 .....	3-1
3.3 开启本地代理ARP功能 .....	3-1
3.4 代理ARP显示和维护 .....	3-1
3.5 代理ARP典型配置举例 .....	3-2
3.5.1 代理ARP基本组网配置举例 .....	3-2
<b>4 ARP Snooping .....</b>	<b>4-1</b>
4.1 ARP Snooping简介 .....	4-1
4.1.1 ARP Snooping表项建立机制 .....	4-1
4.1.2 ARP Snooping表项老化机制 .....	4-1
4.1.3 ARP Snooping表项冲突处理机制 .....	4-1
4.2 开启ARP Snooping功能 .....	4-1
4.3 ARP Snooping显示和维护 .....	4-2
<b>5 ARP直连路由通告.....</b>	<b>5-1</b>
5.1 ARP直连路由通告简介 .....	5-1
5.1.1 工作机制.....	5-1
5.2 开启ARP直连路由通告功能.....	5-1

# 1 ARP

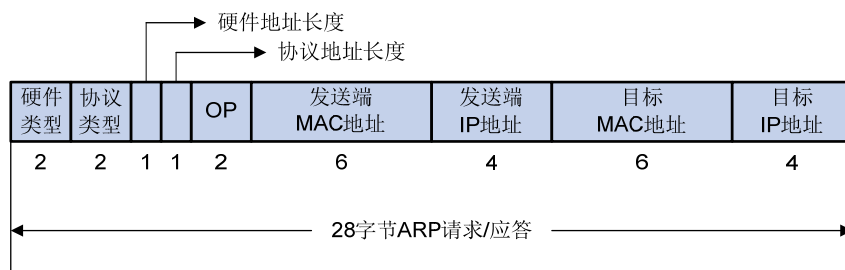
## 1.1 ARP简介

ARP（Address Resolution Protocol，地址解析协议）是将 IP 地址解析为以太网 MAC 地址（或称物理地址）的协议。在网络中，当主机或其它网络设备有数据要发送给另一个主机或设备时，它必须知道对方的网络层地址（即 IP 地址），由于 IP 数据报必须封装成帧才能通过物理网络发送，因此还需要知道对方的物理地址，所以设备上需要存在一个从 IP 地址到物理地址的映射关系。ARP 就是实现这个功能的协议。

### 1.1.1 ARP报文结构

ARP报文分为ARP请求和ARP应答报文，报文格式如 [图 1-1](#) 所示。

图1-1 ARP 报文结构



- 硬件类型：表示硬件地址的类型。它的值为 1 表示以太网地址；
- 协议类型：表示要映射的协议地址类型。它的值为 0x0800 即表示 IP 地址；
- 硬件地址长度和协议地址长度分别指出硬件地址和协议地址的长度，以字节为单位。对于以太网上 IP 地址的 ARP 请求或应答来说，它们的值分别为 6 和 4；
- 操作类型（OP）：1 表示 ARP 请求，2 表示 ARP 应答；
- 发送端 MAC 地址：发送方设备的硬件地址；
- 发送端 IP 地址：发送方设备的 IP 地址；
- 目标 MAC 地址：接收方设备的硬件地址；
- 目标 IP 地址：接收方设备的 IP 地址。

### 1.1.2 ARP地址解析过程

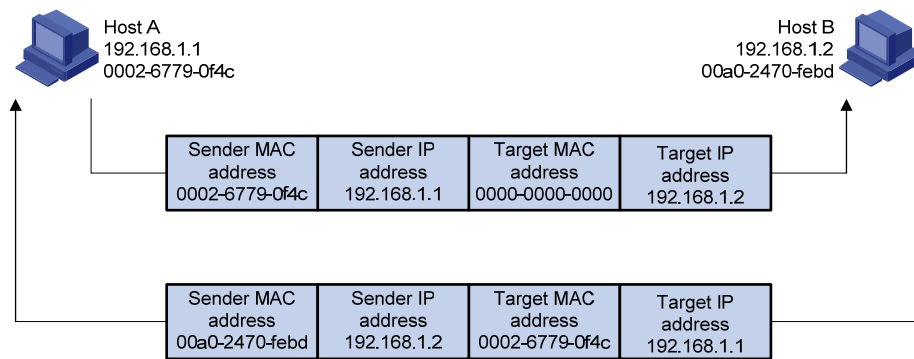
假设主机A和B在同一个网段，主机A要向主机B发送信息。如 [图 1-2](#) 所示，具体的地址解析过程如下：

- (1) 主机 A 首先查看自己的 ARP 表，确定其中是否包含有主机 B 对应的 ARP 表项。如果找到了对应的 MAC 地址，则主机 A 直接利用 ARP 表中的 MAC 地址，对 IP 数据报进行帧封装，并将 IP 数据报发送给主机 B。



- (2) 如果主机 A 在 ARP 表中找不到对应的 MAC 地址，则将缓存该 IP 数据报，然后以广播方式发送一个 ARP 请求报文。ARP 请求报文中的发送端 IP 地址和发送端 MAC 地址为主机 A 的 IP 地址和 MAC 地址，目标 IP 地址和目标 MAC 地址为主机 B 的 IP 地址和全 0 的 MAC 地址。由于 ARP 请求报文以广播方式发送，该网段上的所有主机都可以接收到该请求，但只有被请求的主机（即主机 B）会对该请求进行处理。
- (3) 主机 B 比较自己的 IP 地址和 ARP 请求报文中的目标 IP 地址，当两者相同时进行如下处理：将 ARP 请求报文中的发送端（即主机 A）的 IP 地址和 MAC 地址存入自己的 ARP 表中。之后以单播方式发送 ARP 响应报文给主机 A，其中包含了自己的 MAC 地址。
- (4) 主机 A 收到 ARP 响应报文后，将主机 B 的 MAC 地址加入到自己的 ARP 表中以用于后续报文的转发，同时将 IP 数据报进行封装后发送出去。

图1-2 ARP 地址解析过程



当主机 A 和主机 B 不在同一网段时，主机 A 就会先向网关发出 ARP 请求，ARP 请求报文中的目标 IP 地址为网关的 IP 地址。当主机 A 从收到的响应报文中获得网关的 MAC 地址后，将报文封装并发送给网关。如果网关没有主机 B 的 ARP 表项，网关会广播 ARP 请求，目标 IP 地址为主机 B 的 IP 地址，当网关从收到的响应报文中获得主机 B 的 MAC 地址后，就可以将报文发给主机 B；如果网关已经有主机 B 的 ARP 表项，网关直接把报文发给主机 B。

### 1.1.3 ARP表项类型

设备通过 ARP 解析到目的 MAC 地址后，将会在自己的 ARP 表中增加 IP 地址和 MAC 地址映射关系的表项，以用于后续到同一目的地报文的转发。

ARP 表项分为动态 ARP 表项、静态 ARP 表项、OpenFlow ARP 表项和 Rule ARP 表项。

#### 1. 动态ARP表项

动态 ARP 表项由 ARP 协议通过 ARP 报文自动生成和维护，可以被老化，可以被新的 ARP 报文更新，可以被静态 ARP 表项覆盖。当到达老化时间、接口状态 down 时，系统会删除相应的动态 ARP 表项。

#### 2. 静态ARP表项

静态 ARP 表项通过手工配置和维护，不会被老化，不会被动态 ARP 表项覆盖。

配置静态 ARP 表项可以增加通信的安全性。静态 ARP 表项可以限制和指定 IP 地址的设备通信时只使用指定的 MAC 地址，此时攻击报文无法修改此表项的 IP 地址和 MAC 地址的映射关系，从而保护了本设备和指定设备间的正常通信。

静态 ARP 表项分为短静态 ARP 表项、长静态 ARP 表项和多端口 ARP 表项。

- 长静态 ARP 表项可以直接用于报文转发，除了包括 IP 地址和 MAC 地址外，还需要包括该 ARP 表项所在 VLAN 和出接口。
- 短静态 ARP 表项只包括 IP 地址和 MAC 地址。

如果出接口是 VLAN 虚接口，短静态 ARP 表项不能直接用于报文转发，需要对表项进行解析：当要发送 IP 数据报时，设备先发送 ARP 请求报文，如果收到的响应报文中的发送端 IP 地址和发送端 MAC 地址与所配置的 IP 地址和 MAC 地址相同，则将接收 ARP 响应报文的接口加入该静态 ARP 表项中，此时，该短静态 ARP 表项由未解析状态变为解析状态，之后就可以用于报文转发。

- 多端口 ARP 表项包括 IP 地址、MAC 地址和该 ARP 表项所在的 VLAN，当多端口 ARP 表项中的 MAC 地址和 VLAN 信息与多端口单播 MAC/组播 MAC 地址表项中的 MAC 地址和 VLAN 相同时，该多端口 ARP 表项可用来指导 IP 转发。多端口 ARP 表项通过手工配置和维护，不会被老化，不会被动态 ARP 表项覆盖。组播 MAC 的相关介绍，请参见“IP 组播”的“组播路由与转发”。

一般情况下，ARP 动态执行并自动寻求 IP 地址到以太网 MAC 地址的解析，无需管理员的介入。当希望设备和指定用户只能使用某个固定的 IP 地址和 MAC 地址通信时，可以配置短静态 ARP 表项，当进一步希望限定这个用户只在某 VLAN 内的某个特定接口上连接时就可以配置长静态 ARP 表项。

### 3. OpenFlow ARP表项

OpenFlow ARP 表项由 OpenFlow 添加，不会被老化，不能通过 ARP 报文更新。可以直接用于转发报文。关于 OpenFlow 的介绍，请参见“OpenFlow 配置指导”中的“OpenFlow”。

### 4. Rule ARP表项

Rule ARP 表项不会被老化，不能通过 ARP 报文更新，可以被静态 ARP 表项覆盖，可以直接用于转发报文。Rule ARP 表项可由 Portal 添加，Portal 的详细介绍请参见“安全配置指导”中的“Portal”。

## 1.2 ARP配置任务简介

本节中的所有配置均为可选，请根据实际情况选择配置。

- [手工添加静态ARP表项](#)
  - [手工添加短静态ARP表项](#)
  - [手工添加长静态ARP表项](#)
  - [手工添加多端口ARP表项](#)
- [配置动态ARP表项的相关功能](#)
  - [配置设备学习动态ARP表项的最大数目](#)
  - [配置接口学习动态ARP表项的最大数目](#)
  - [配置动态ARP表项的老化时间](#)
  - [开启动态ARP表项的检查功能](#)
- [将IRF主设备的ARP表项同步到其他所有IRF从设备](#)
- [开启ARP日志信息功能](#)

## 1.3 手工添加静态ARP表项

静态 ARP 表项在设备正常工作期间一直有效。

### 1.3.1 手工添加短静态ARP表项

#### 1. 配置限制和指导

对于已经解析的短静态 ARP 表项，会由于外部事件，比如解析到的出接口状态 down 或设备的 ARP 表项所对应的 VLAN 或 VLAN 接口被删除等原因，恢复到未解析状态。

#### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 手工添加短静态 ARP 表项。

```
arp static ip-address mac-address
```

### 1.3.2 手工添加长静态ARP表项

#### 1. 功能简介

长静态 ARP 表项根据设备的当前状态可能处于有效或无效两种状态。处于无效状态的原因可能是该 ARP 表项对应的 VLAN 接口状态 down 或出接口状态 down、该 ARP 表项中的 IP 地址与本地 IP 地址冲突或设备上没有与该 ARP 表项中的 IP 地址在同一网段的接口地址等原因。处于无效状态的长静态 ARP 表项不能指导报文转发。当长静态 ARP 表项所对应的 VLAN 或 VLAN 接口被删除时，该 ARP 表项会被删除。

#### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 手工添加长静态 ARP 表项。

```
arp static ip-address mac-address [ vlan-id interface-type  
interface-number ]
```

### 1.3.3 手工添加多端口ARP表项

#### 1. 功能简介

多端口 ARP 表项由多端口单播/组播 MAC 地址表项指定 VLAN 和出端口，由多端口 ARP 表项指定 IP 地址。多端口 ARP 表项可以覆盖其它动态、短静态和长静态 ARP 表项；短静态或长静态 ARP 表项也可以覆盖多端口 ARP 表项。

#### 2. 配置限制和指导

当多端口 ARP 表项中 IP 地址与 VLAN 虚接口的 IP 地址属于同一网段，且存在对应的多端口单播 MAC/组播 MAC 时，该多端口 ARP 表项才能正常指导转发。

#### 3. 配置步骤

- (1) 进入系统视图。

**system-view**

- (2) 配置多端口单播 MAC 地址表项或配置组播 MAC 地址表项。请选择其中一项进行配置。

- 配置多端口单播 MAC 地址表项。

```
mac-address multiport mac-address interface interface-list vlan vlan-id
```

多端口单播 MAC 的相关内容, 请参见“二层技术-以太网交换命令参考/MAC 地址表”中的命令 **mac-address**。

- 配置组播 MAC 地址表项。

```
mac-address multicast mac-address interface interface-list vlan vlan-id
```

组播 MAC 的相关内容, 请参见“IP 组播命令参考/IGMP Snooping”中的命令 **mac-address multicast**。

- (3) 手工添加多端口 ARP 表项。

```
arp multiport ip-address mac-address vlan-id
```

本命令中的 *mac-address*, *vlan-id* 应该和多端口单播 MAC 或组播 MAC 中的 *mac-address*, *vlan-id* 一致。

## 1.4 配置动态ARP表项的相关功能

### 1.4.1 配置设备学习动态ARP表项的最大数目

#### 1. 功能简介

设备可以通过 ARP 协议自动生成动态 ARP 表项。为了防止用户占用过多的 ARP 资源, 可以通过设置设备学习动态 ARP 表项的最大数目来进行限制。当设备学习动态 ARP 表项的数目达到所设置的值时, 该设备上将不再学习动态 ARP 表项。

当本命令配置的动态 ARP 表项的最大数目小于设备当前已经学到的动态 ARP 表项数目, 已学到的动态 ARP 表项不会被直接删除, 用户可以通过执行 **reset arp dynamic** 命令直接清除动态 ARP 表项。

#### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置设备允许学习动态 ARP 表项的最大数目。

```
arp max-learning-number max-number slot slot-number
```

缺省情况下, 各系列产品设备允许学习的动态 ARP 表项最大数目为:

- S5130S-SI、S5120V2-SI 系列交换机为 2048 个;
- S5130S-LI、S5120V2-LI、S3100V3-SI 系列交换机为 1024 个;
- S5110V2-SI、S5000V3-EI、S5000E-X 系列交换机为 128 个。

当配置设备允许学习动态 ARP 表项的最大数目为 0 时, 表示禁止本设备学习动态 ARP 表项。

## 1.4.2 配置接口学习动态ARP表项的最大数目

### 1. 功能简介

设备可以通过 ARP 协议自动生成动态 ARP 表项。为了防止部分接口下的用户占用过多的 ARP 资源，可以通过设置接口学习动态 ARP 表项的最大数目来进行限制。当接口学习动态 ARP 表项的数目达到所设置的值时，该接口将不再学习动态 ARP 表项。

如果二层接口及其所属的 VLAN 接口都配置了允许学习动态 ARP 表项的最大数目，则只有二层接口及 VLAN 接口上的动态 ARP 表项数目都没有超过各自配置的最大值时，才会学习 ARP 表项。

设备各接口学习的动态 ARP 表项之和不会超过该设备学习动态 ARP 表项的最大数目。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置接口允许学习动态 ARP 表项的最大数目。

```
arp max-learning-num max-number [ alarm alarm-threshold ]
```

缺省情况下，各系列产品接口允许学习的动态 ARP 表项最大数目为：

- S5130S-SI、S5120V2-SI 系列交换机为 2048 个；
- S5130S-LI、S5120V2-LI、S3100V3-SI 系列交换机为 1024 个；
- S5110V2-SI、S5000V3-EI、S5000E-X 系列交换机为 128 个。

当配置接口允许学习动态 ARP 表项的最大数目为 0 时，表示禁止接口学习动态 ARP 表项。

## 1.4.3 配置动态ARP表项的老化时间

### 1. 功能简介

为适应网络的变化，ARP 表需要不断更新。ARP 表中的动态 ARP 表项并非永远有效，每一条记录都有一个生存周期，到达生存周期仍得不到刷新的记录将从 ARP 表中删除，这个生存周期被称作老化时间。如果在到达老化时间前记录被刷新，则重新计算老化时间。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置动态 ARP 表项的老化时间。

```
arp timer aging { aging-minutes | second aging-seconds }
```

缺省情况下，动态 ARP 表项的老化时间为 20 分钟。

## 1.4.4 开启动态ARP表项的检查功能

### 1. 功能简介

动态 ARP 表项检查功能可以控制设备上是否可以学习 ARP 报文中的发送端 MAC 地址为组播 MAC 的动态 ARP 表项。

- 开启 ARP 表项的检查功能后，设备上不能学习 ARP 报文中发送端 MAC 地址为组播 MAC 的动态 ARP 表项，也不能手工添加 MAC 地址为组播 MAC 的静态 ARP 表项。
- 关闭 ARP 表项的检查功能后，设备可以学习以太网源 MAC 地址为单播 MAC 且 ARP 报文中发送端 MAC 地址为组播 MAC 的动态 ARP 表项，也可以手工添加 MAC 地址为组播 MAC 的静态 ARP 表项。

## 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启动态 ARP 表项的检查功能。

```
arp check enable
```

缺省情况下，动态 ARP 表项的检查功能处于开启状态。

# 1.5 将IRF主设备的ARP表项同步到其他所有IRF从设备

## 1. 功能简介

当 IRF 主从设备间出现了 ARP 表项不一致的异常情况时，可以执行本配置，保证 IRF 主从设备上的 ARP 表项处于一致状态。

## 2. 配置限制和指导

为了防止 IRF 设备在长时间工作后，各设备间的 ARP 表项出现差异的情况，可通过 **schedule** 机制控制 **arp smooth** 命令的起始时间及执行的时间间隔，关于 **schedule** 机制的介绍，请参见“基础配置指导”中的“设备管理”。

## 3. 配置步骤

请在用户视图下执行本命令，将 IRF 主设备的 ARP 表项同步到其他所有 IRF 从设备。

```
arp smooth
```

# 1.6 开启ARP日志信息功能

## 1. 功能简介

ARP 日志可以方便管理员定位问题和解决问题，对处理 ARP 报文的信息进行的记录。例如，ARP 日志可以记录如下事件：

- 设备未使能 ARP 代理功能时收到目的 IP 不是设备接口 IP 地址或 VRRP 备份组中的虚拟 IP 地址；
- 收到的 ARP 报文中源地址和接收接口 IP 地址或 VRRP 备份组中的虚拟 IP 地址冲突，且此报文不是 ARP 请求报文等。

设备生成的 ARP 日志信息会交给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

## 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 ARP 日志信息功能。
- arp check log enable**
- 缺省情况下，ARP 日志信息功能处于关闭状态。

1.7 ARP显示和维护



清除 ARP 表项，将取消 IP 地址和 MAC 地址的映射关系，可能导致无法正常通信。清除前请务必仔细确认。

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 ARP 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，用户可以执行 **reset** 命令清除 ARP 表项。

表1-1 ARP 显示和维护

操作	命令
显示ARP表项	<b>display arp</b> [ [ <b>all</b>   <b>dynamic</b>   <b>multiport</b>   <b>static</b> ] [ <b>slot slot-number</b> ]   <b>vlan</b> <i>vlan-id</i>   <b>interface</b> <i>interface-type interface-number</i> ] [ <b>count</b>   <b>verbose</b> ]
显示设备支持ARP表项的最大数目	<b>display arp entry-limit</b>
显示指定IP地址的ARP表项	<b>display arp ip-address</b> [ <b>slot slot-number</b> ] [ <b>verbose</b> ]
显示OpenFlow类型ARP表项个数	<b>display arp openflow count</b> [ <b>slot slot-number</b> ]
显示动态ARP表项的老化时间	<b>display arp timer aging</b>
清除ARP表项	<b>reset arp</b> { <b>all</b>   <b>dynamic</b>   <b>interface</b> <i>interface-type interface-number</i>   <b>multiport</b>   <b>slot slot-number</b>   <b>static</b> }

1.8 ARP典型配置举例

1.8.1 长静态ARP表项配置举例

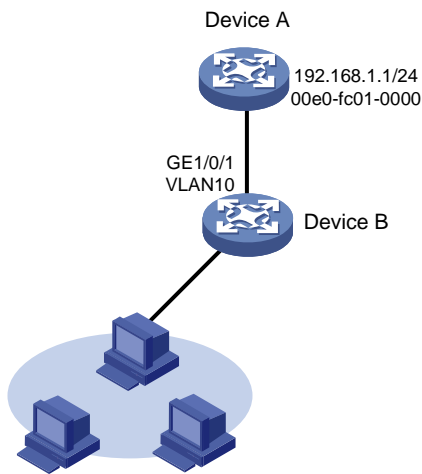
1. 组网需求

- Device B 连接主机，通过接口 GigabitEthernet1/0/1 连接 Device A。接口 GigabitEthernet1/0/1 属于 VLAN 10。
  - Device A 的 IP 地址为 192.168.1.1/24，MAC 地址为 00e0-fc01-0000。
- 为了增加 Device B 和 Device A 通信的安全性，可以在 Device B 上为 Device A 配置一条静态 ARP 表项，从而防止攻击报文修改此表项的 IP 地址和 MAC 地址的映射关系。



2. 组网图

图1-3 长静态 ARP 表项配置组网图



3. 配置步骤

在 Device B 上进行下列配置。

# 创建 VLAN 10。

```
<DeviceB> system-view
[DeviceB] vlan 10
[DeviceB-vlan10] quit
```

# 将接口 GigabitEthernet1/0/1 加入到 VLAN 10 中。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port access vlan 10
[DeviceB-GigabitEthernet1/0/1] quit
```

# 创建接口 Vlan-interface10，并配置 IP 地址。

```
[DeviceB] interface vlan-interface 10
[DeviceB-vlan-interface10] ip address 192.168.1.2 8
[DeviceB-vlan-interface10] quit
```

# 配置一条长静态 ARP 表项，IP 地址为 192.168.1.1，对应的 MAC 地址为 00e0-fc01-0000，此条 ARP 表项对应的出接口为属于 VLAN 10 的接口 GigabitEthernet1/0/1。

```
[DeviceB] arp static 192.168.1.1 00e0-fc01-0000 10 gigabitethernet 1/0/1
```

4. 验证配置

# 查看长静态 ARP 表项信息。

```
[DeviceB] display arp static
```

Type: S-Static	D-Dynamic	O-Openflow	R-Rule	M-Multiport	I-Invalid
IP address	MAC address	VLAN/VSI	Interface/Link ID	Aging	Type
192.168.1.1	00e0-fc01-0000	10	GE1/0/1	--	S



## 1.8.2 短静态ARP表项配置举例

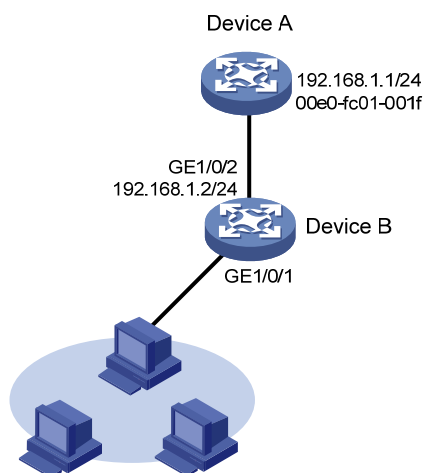
### 1. 组网需求

- Device B 通过接口 GigabitEthernet1/0/1 连接主机，通过接口 GigabitEthernet1/0/2 连接 Device A。
- Device A 的 IP 地址为 192.168.1.1/24，MAC 地址为 00e0-fc01-001f。

网络管理员需要通过某种方法来防止恶意用户对 Device B 进行 ARP 攻击，增加 Device B 和 Device A 通信的安全性。如果 Device A 的 IP 地址和 MAC 地址是固定的，则可以通过在 Device B 上配置静态 ARP 表项的方法，防止恶意用户进行 ARP 攻击。

### 2. 组网图

图1-4 短静态 ARP 表项配置组网图



### 3. 配置步骤

在 Device B 上进行下列配置。

# 在接口 GigabitEthernet1/0/2 配置 IP 地址。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ip address 192.168.1.2 24
[DeviceB-GigabitEthernet1/0/2] quit
```

# 配置一条短静态 ARP 表项，IP 地址是 192.168.1.1，对应的 MAC 地址是 00e0-fc01-001f。

```
[DeviceB] arp static 192.168.1.1 00e0-fc01-001f
```

### 4. 验证配置

# 查看短静态 ARP 表项信息。

```
[DeviceB] display arp static
```

Type: S-Static	D-Dynamic	O-Openflow	R-Rule	M-Multiport	I-Invalid
IP address	MAC address	VLAN/VSI	Interface/Link ID	Aging	Type
192.168.1.1	00e0-fc01-001f	--	--	--	S

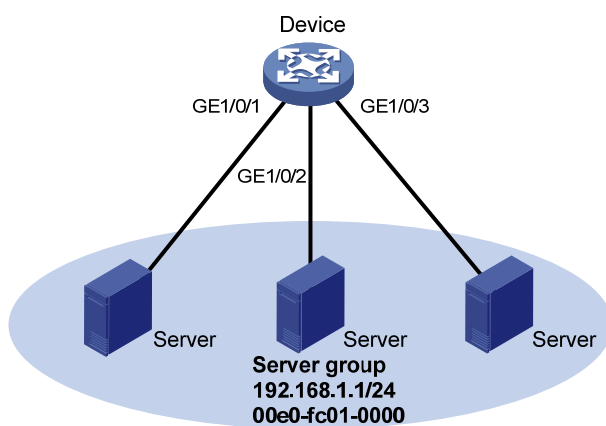
## 1.8.3 多端口ARP表项配置举例

### 1. 组网需求

- Device 连接服务器群，通过属于 VLAN 10 的三个二层接口 GigabitEthernet1/0/1、GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 分别连接三台服务器。
  - 服务器群的共享 IP 地址为 192.168.1.1/24，共享 MAC 地址为 00e0-fc01-0000。
- 配置多端口 ARP 表项，使目的 IP 为 192.168.1.1 的 IP 数据报文能同时发送到三台服务器上。

### 2. 组网图

图1-5 多端口 ARP 表项配置组网图



### 3. 配置步骤

在 Device 上进行下列配置。

# 创建 VLAN 10。

```
<Device> system-view
[Device] vlan 10
[Device-vlan10] quit
```

# 将接口 GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/3 加入到 VLAN 10 中。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port access vlan 10
[Device-GigabitEthernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] port access vlan 10
[Device-GigabitEthernet1/0/2] quit
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] port access vlan 10
[Device-GigabitEthernet1/0/3] quit
```

# 创建接口 Vlan-interface10，并配置 IP 地址。

```
[Device] interface vlan-interface 10
[Device-vlan-interface10] ip address 192.168.1.2 24
[Device-vlan-interface10] quit
```

# 配置多端口单播 MAC 表项,MAC 地址为 00e0-fc01-0000,对应的出接口为 GigabitEthernet1/0/1、GigabitEthernet1/0/2 和 GigabitEthernet1/0/3, 接口属于 VLAN 10。

```
[Device] mac-address multiport 00e0-fc01-0000 interface gigabitethernet 1/0/1 to  
gigabitethernet 1/0/3 vlan 10
```

# 配置一条多端口 ARP 表项, IP 地址为 192.168.1.1, 对应的 MAC 地址为 00e0-fc01-0000。

```
[Device] arp multiport 192.168.1.1 00e0-fc01-0000 10
```

#### 4. 验证配置

# 查看 ARP 表项信息。

```
[Device] display arp
```

Type:	S-Static	D-Dynamic	O-Openflow	R-Rule	M-Multiport	I-Invalid
IP address	MAC address	VLAN/VSI	Interface/Link ID	Aging	Type	
192.168.1.1	00e0-fc01-0000	10	--	--	M	

## 2 免费ARP

### 2.1 免费ARP简介

免费 ARP 报文是一种特殊的 ARP 报文，该报文中携带的发送端 IP 地址和目标 IP 地址都是本机的 IP 地址。设备通过对外发送免费 ARP 报文来确定其他设备的 IP 地址是否与本机的 IP 地址冲突，并实现在设备硬件地址改变时通知其它设备更新 ARP 表项。

#### 2.1.1 IP地址冲突检测

设备接口获取到 IP 地址时可以在接口所在局域网内广播发送免费 ARP 报文。如果设备收到 ARP 应答报文，表示局域网中存在与该设备 IP 地址相同的设备，则设备不会使用此 IP 地址，并打印日志提示管理员修改该 IP 地址。如果设备未收到 ARP 应答报文，表示局域网中不存在与该设备 IP 地址相同的设备，则设备可以正常使用 IP 地址。

#### 2.1.2 免费ARP报文学习

开启了免费 ARP 报文学习功能后，设备会根据收到的免费 ARP 报文中携带的信息（发送端 IP 地址、发送端 MAC 地址）对自身维护的 ARP 表进行修改。设备先判断 ARP 表中是否存在与此免费 ARP 报文中的发送端 IP 地址对应的 ARP 表项：

- 如果没有对应的 ARP 表项，设备会根据该免费 ARP 报文中携带的信息新建 ARP 表项；
- 如果存在对应的 ARP 表项，设备会根据该免费 ARP 报文中携带的信息更新对应的 ARP 表项。

关闭免费 ARP 报文学习功能后，设备不会根据收到的免费 ARP 报文来新建 ARP 表项，但是会更新已存在的对应 ARP 表项。如果用户不希望通过免费 ARP 报文来新建 ARP 表项，可以关闭免费 ARP 报文学习功能，以节省 ARP 表项资源。

#### 2.1.3 定时发送免费ARP

定时发送免费 ARP 功能可以及时通知下行设备更新 ARP 表项或者 MAC 地址表项，主要应用场景如下：

- 防止仿冒网关的 ARP 攻击  
如果攻击者仿冒网关发送免费 ARP 报文，就可以欺骗同网段内的其它主机，使得被欺骗的主机访问网关的流量被重定向到一个错误的 MAC 地址，导致其它主机用户无法正常访问网络。为了降低这种仿冒网关的 ARP 攻击所带来的影响，可以在网关的接口上开启定时发送免费 ARP 功能。开启该功能后，网关接口上将按照配置的时间间隔周期性发送接口主 IP 地址和手工配置的从 IP 地址的免费 ARP 报文。这样，每台主机都可以学习到正确的网关，从而正常访问网络。
- 防止主机 ARP 表项老化  
在实际环境中，当网络负载较大或接收端主机的 CPU 占用率较高时，可能存在 ARP 报文被丢弃或主机无法及时处理接收到的 ARP 报文等现象。这种情况下，接收端主机的动态 ARP

表项会因超时而老化，在其重新学习到发送设备的 ARP 表项之前，二者之间的流量就会发生中断。

为了解决上述问题，可以在网关的接口上开启定时发送免费 ARP 功能。启用该功能后，网关接口上将按照配置的时间间隔周期性发送接口主 IP 地址和手工配置的从 IP 地址的免费 ARP 报文。这样，接收端主机可以及时更新 ARP 映射表，从而防止了上述流量中断现象。

- 防止 VRRP 虚拟 IP 地址冲突

当网络中存在 VRRP 备份组时，需要由 VRRP 备份组的 Master 路由器周期性的向网络内的主机发送免费 ARP 报文，使主机更新本地 ARP 地址表，从而确保网络中不会存在 IP 地址与 Master 路由器 VRRP 虚拟 IP 地址相同的设备。免费 ARP 报文中的发送端 MAC 为 VRRP 虚拟路由器对应的虚拟 MAC 地址。关于 VRRP 的详细介绍，请参见“可靠性配置指导”中的“VRRP”。

## 2.2 免费ARP配置任务简介

本节中的所有配置均为可选，请根据实际情况选择配置。当以下功能均未开启时，免费 ARP 的冲突地址检测功能仍然生效。

- [开启源IP地址冲突提示功能](#)
- [开启免费ARP报文学习功能](#)
- [开启定时发送免费ARP功能](#)
- [开启设备收到非同一网段ARP请求时发送免费ARP报文功能](#)
- [配置当接口MAC地址变化时，该接口重新发送免费ARP报文的次数和时间间隔](#)

## 2.3 开启源IP地址冲突提示功能

### 1. 功能简介

设备接收到其它设备发送的 ARP 报文后，如果发现报文中的源 IP 地址和自己的 IP 地址相同，该设备会根据当前源 IP 地址冲突提示功能的状态，进行如下处理：

- 如果源 IP 地址冲突提示功能处于关闭状态时，设备发送一个免费 ARP 报文确认是否冲突，只有收到对应的 ARP 应答后才提示存在 IP 地址冲突。
- 如果源 IP 地址冲突提示功能处于开启状态时，设备立刻提示存在 IP 地址冲突。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启源 IP 地址冲突提示功能。

```
arp ip-conflict log prompt
```

缺省情况下，源 IP 地址冲突提示功能处于关闭状态。

## 2.4 开启免费ARP报文学习功能

- (1) 进入系统视图。

```
system-view
```

- (2) 开启免费 ARP 报文学习功能。

```
gratuitous-arp-learning enable
```

缺省情况下，免费 ARP 报文的学习功能处于开启状态。

## 2.5 开启定时发送免费ARP功能

### 1. 配置限制和指导

- 设备最多允许同时在 1024 个接口上开启定时发送免费 ARP 功能。
- 开启定时发送免费 ARP 功能后，只有当接口链路状态 up 并且配置 IP 地址后，此功能才真正生效。
- 如果修改了免费 ARP 报文的发送时间间隔，则在下一个发送时间间隔才能生效。
- 如果同时在很多接口下开启定时发送免费 ARP 功能，或者每个接口有大量的从 IP 地址，又或者是两种情况共存的同时又配置很小的发送时间间隔，那么免费 ARP 报文的实际发送时间间隔可能会远远高于用户设定的时间间隔。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 开启定时发送免费 ARP 功能。

```
arp send-gratuitous-arp [ interval interval ]
```

缺省情况下，定时发送免费 ARP 功能处于关闭状态。

## 2.6 开启设备收到非同一网段ARP请求时发送免费ARP报文功能

- (1) 进入系统视图。

```
system-view
```

- (2) 开启设备收到非同一网段 ARP 请求时发送免费 ARP 报文功能。

```
gratuitous-arp-sending enable
```

缺省情况下，设备收到非同一网段的 ARP 请求时发送免费 ARP 报文功能处于关闭状态。

## 2.7 配置当接口MAC地址变化时，该接口重新发送免费ARP报文的次数和时间间隔

### 1. 功能简介

当设备的 MAC 地址发生变化后，设备会通过免费 ARP 报文将修改后的 MAC 地址通告给其他设备。由于目前免费 ARP 报文没有重传机制，其他设备可能无法收到免费 ARP 报文。为了解决这个问题，用户可以配置当接口 MAC 地址变化时，该接口重新发送免费 ARP 报文的次数和时间间隔，保证其他设备可以收到该免费 ARP 报文。

## 2. 配置步骤

- (1) 进入系统视图。

**system-view**

- (2) 配置当接口 MAC 地址变化时，重新发送免费 ARP 报文的次数和时间间隔

**gratuitous-arp mac-change retransmit *times* interval *seconds***

缺省情况下，当设备的接口 MAC 地址变化时，该接口只会发送一次免费 ARP 报文。

## 3 代理ARP

### 3.1 代理ARP简介

如果 ARP 请求是从一个网络的主机发往同一网段却不在同一物理网络上的另一台主机，那么连接它们的具有代理 ARP 功能的设备就可以回答该请求，这个过程称作代理 ARP（Proxy ARP）。

代理 ARP 功能屏蔽了分离的物理网络这一事实，使用户使用起来，好像在同一个物理网络上。

代理 ARP 分为普通代理 ARP 和本地代理 ARP，二者的应用场景有所区别：

- 普通代理 ARP 的应用场景为：想要互通的主机分别连接到设备的不同三层接口上，且这些主机不在同一个广播域中。
- 本地代理 ARP 的应用场景为：想要互通的主机连接到设备的同一个三层接口上，且这些主机不在同一个广播域中。

### 3.2 开启普通代理ARP功能

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

普通代理 ARP 功能可在 VLAN 接口视图下进行配置。

- (3) 开启普通代理 ARP 功能。

```
proxy-arp enable
```

缺省情况下，普通代理 ARP 功能处于关闭状态。

### 3.3 开启本地代理ARP功能

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

本地代理 ARP 功能可在 VLAN 接口视图下进行配置。

- (3) 开启本地代理 ARP 功能。

```
local-proxy-arp enable [ ip-range start-ip-address to end-ip-address ]
```

缺省情况下，本地代理 ARP 功能处于关闭状态。

### 3.4 代理ARP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代理 ARP 的运行情况，查看显示信息验证配置的效果。



表3-1 代理 ARP 显示和维护

操作	命令
显示本地代理ARP的状态	<code>display local-proxy-arp [ interface interface-type interface-number ]</code>
显示普通代理ARP的状态	<code>display proxy-arp [ interface interface-type interface-number ]</code>

### 3.5 代理ARP典型配置举例

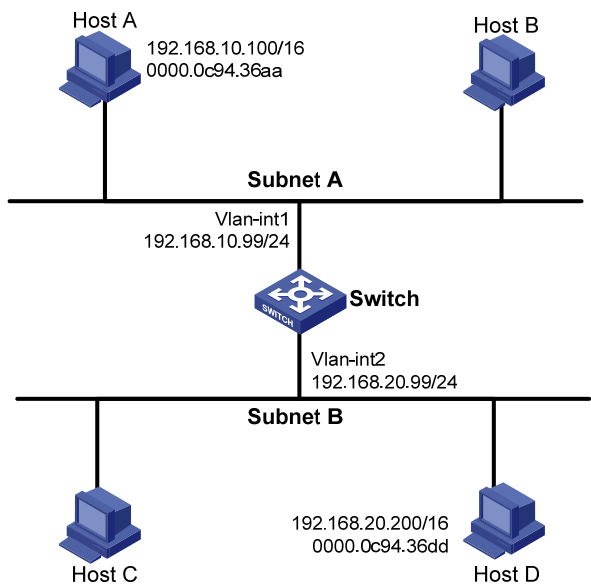
#### 3.5.1 代理ARP基本组网配置举例

##### 1. 组网需求

- Host A 和 Host D 配置为同一网段的主机（Host A 的 IP 地址是 192.168.10.100/16，Host D 的 IP 地址是 192.168.20.200/16），但却被设备 Switch 分在两个不同的子网（Host A 属于 VLAN 1，Host D 属于 VLAN 2）。
- Host A 和 Host D 没有配置缺省网关，要求在设备 Switch 上开启代理 ARP 功能，使处在两个子网的 Host A 和 Host D 能互通。

##### 2. 组网图

图3-1 配置代理 ARP 组网图



##### 3. 配置步骤

# 创建 VLAN 2。

```
<Switch> system-view
[Switch] vlan 2
[Switch-vlan2] quit
```

# 配置接口 Vlan-interface1 的 IP 地址。

```
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.10.99 255.255.255.0
# 开启接口 Vlan-interface1 的代理 ARP 功能。
[Switch-Vlan-interface1] proxy-arp enable
[Switch-Vlan-interface1] quit
# 配置接口 Vlan-interface2 的 IP 地址。
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.20.99 255.255.255.0
# 开启接口 Vlan-interface2 的代理 ARP 功能。
[Switch-Vlan-interface2] proxy-arp enable
```

#### 4. 验证配置

配置完成后，Host A 和 Host D 可以互相 ping 通。

# 4 ARP Snooping

## 4.1 ARP Snooping简介

ARP Snooping 功能是一个用于二层交换网络环境的特性，通过侦听 ARP 报文建立 ARP Snooping 表项，从而提供给 MFF（MAC-Forced Forwarding，MAC 强制转发）使用。关于 MFF 的详细介绍，请参见“安全配置指导”中的“MFF”。

### 4.1.1 ARP Snooping表项建立机制

设备上在一个 VLAN 中启用 ARP Snooping 后，该 VLAN 内接收的 ARP 报文都会被上送到 CPU。CPU 对上送的 ARP 报文进行分析，获取 ARP 报文的发送端 IP 地址、发送端 MAC 地址、VLAN 和入端口信息，建立记录用户信息的 ARP Snooping 表项。

### 4.1.2 ARP Snooping表项老化机制

ARP Snooping 表项的老化时间为 25 分钟，有效时间为 15 分钟。

如果一个 ARP Snooping 表项自最后一次更新后 12 分钟内没有收到 ARP 更新报文，设备会向外主动发送一个 ARP 请求进行探测；若 ARP Snooping 表项自最后一次更新后 15 分钟时，还没有收到 ARP 更新报文，则此表项开始进入失效状态，不再对外提供服务，其他特性查找此表项将会失败。当收到发送端 IP 地址和发送端 MAC 与已存在的 ARP Snooping 表项 IP 地址和 MAC 均相同的 ARP 报文时，此 ARP Snooping 表项进行更新，重新开始生效，并重新老化计时。

当 ARP Snooping 表项达到老化时间后，则将此 ARP Snooping 表项删除。

### 4.1.3 ARP Snooping表项冲突处理机制

如果 ARP Snooping 收到 ARP 报文时检查到相同 IP 的 ARP Snooping 表项已经存在，但是 MAC 地址发生了变化，则认为发生了攻击，此时 ARP Snooping 表项处于冲突状态，表项失效，不再对外提供服务，并在 1 分钟后删除此表项。

## 4.2 开启ARP Snooping功能

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 VLAN 视图。

```
vlan vlan-id
```

- (3) 开启 ARP Snooping 功能。

```
arp snooping enable
```

缺省情况下，ARP Snooping 功能处于关闭状态。

### 4.3 ARP Snooping显示和维护

在完成上述配置后,在任意视图下执行 **display** 命令可以显示配置后 ARP Snooping 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,用户可以执行 **reset** 命令清除 ARP Snooping 表中的表项。

表4-1 ARP Snooping 显示和维护

操作	命令
显示ARP Snooping表项	<b>display arp snooping</b> [ <b>vlan</b> <i>vlan-id</i> ] [ <b>slot</b> <i>slot-number</i> ] [ <b>count</b> ] <b>display arp snooping ip</b> <i>ip-address</i> [ <b>slot</b> <i>slot-number</i> ]
清除ARP Snooping表项	<b>reset arp snooping</b> [ <b>ip</b> <i>ip-address</i>   <b>vlan</b> <i>vlan-id</i> ]

# 5 ARP直连路由通告

## 5.1 ARP直连路由通告简介

### 5.1.1 工作机制

ARP 直连路由通告功能用于使设备从 ARP 表中学到对应的直连路由信息，以便其他路由协议发布该直连路由或指导报文转发。

## 5.2 开启ARP直连路由通告功能

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 开启 ARP 直连路由通告功能。

```
arp route-direct advertise
```

缺省情况下，ARP 直连路由通告功能处于关闭状态。

# 目 录

1 IP地址 .....	1-1
1.1 IP地址简介 .....	1-1
1.1.1 IP地址的表示和分类 .....	1-1
1.1.2 特殊的IP地址 .....	1-2
1.1.3 子网和掩码 .....	1-2
1.1.4 IP地址的获取方式 .....	1-2
1.2 手工指定接口的IP地址 .....	1-3
1.3 配置接口借用IP地址 .....	1-3
1.4 IP地址显示和维护 .....	1-4
1.5 地址典型配置举例 .....	1-4
1.5.1 手工指定IP地址配置举例 .....	1-4

# 1 IP地址

## 1.1 IP地址简介

若非特别指明，本文所指的 IP 地址均为 IPv4 地址。

### 1.1.1 IP地址的表示和分类

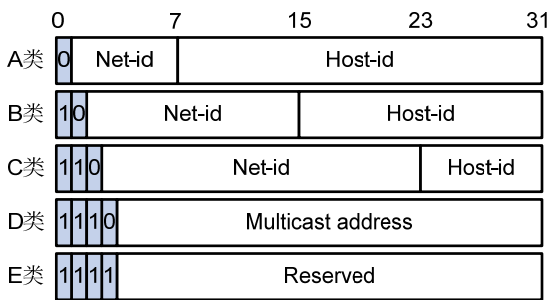
连接到 IPv4 网络上的设备通过 IP 地址标识。IP 地址长度为 32 比特，通常采用点分十进制方式表示，即每个 IP 地址被表示为以小数点隔开的 4 个十进制整数，每个整数对应一个字节，如 10.1.1.1。

IP 地址由两部分组成：

- 网络号码字段（Net-id）：用于区分不同的网络。网络号码字段的前几位称为类别字段（又称为类别比特），用来区分 IP 地址的类型。
- 主机号码字段（Host-id）：用于区分一个网络内的不同主机。

为了方便管理及组网，IP地址分成五类，如 [图 1-1](#)所示，其中蓝色部分为类别字段。

图1-1 五类 IP 地址



上述五类IP地址的地址范围如 [表 1-1](#)所示。目前大量使用的IP地址属于A、B、C三类。

表1-1 IP 地址分类及范围

地址类型	地址范围	说明
A	0.0.0.0~127.255.255.255	IP地址0.0.0.0仅用于主机在系统启动时进行临时通信，并且永远不是有效目的地址 127.0.0.0网段的地址都保留作环回测试，发送到这个地址的分组不会输出到链路上，它们被当作输入分组在内部进行处理
B	128.0.0.0~191.255.255.255	-
C	192.0.0.0~223.255.255.255	-
D	224.0.0.0~239.255.255.255	组播地址
E	240.0.0.0~255.255.255.255	255.255.255.255用于广播地址，其它地址保留今后使用

### 1.1.2 特殊的IP地址

下列 IP 地址具有特殊的用途，不能作为主机的 IP 地址。

- Net-id 为全 0 的地址：表示本网络内的主机。例如，0.0.0.16 表示本网络内 Host-id 为 16 的主机。
- Host-id 为全 0 的地址：网络地址，用于标识一个网络。
- Host-id 为全 1 的地址：网络广播地址。例如，目的地址为 192.168.1.255 的报文，将转发给 192.168.1.0 网络内所有的主机。

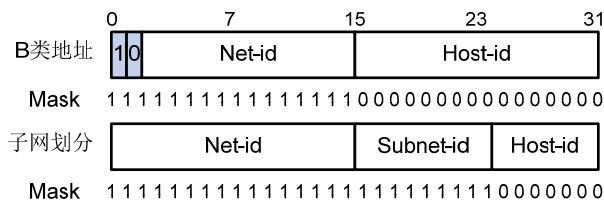
### 1.1.3 子网和掩码

随着 Internet 的快速发展，IP 地址已近枯竭。为了充分利用已有的 IP 地址，可以使用子网掩码将网络划分为更小的部分（即子网）。通过从主机号码字段部分划出一些比特位作为子网号码字段，能够将一个网络划分为多个子网。子网号码字段的长度由子网掩码确定。

子网掩码是一个长度为 32 比特的数字，由一串连续的“1”和一串连续的“0”组成。“1”对应于网络号码字段和子网号码字段，而“0”对应于主机号码字段。

图 1-2 所示是一个 B 类地址划分子网的情况。

图1-2 IP 地址子网划分



多划分出一个子网号码字段会浪费一些 IP 地址。例如，一个 B 类地址可以容纳 65534 ( $2^{16}-2$ ，去掉主机号码字段全 1 的广播地址和主机号码字段全 0 的网段地址) 个主机号码。但划分出 9 比特长的子网字段后，最多可有 512 ( $2^9$ ) 个子网，每个子网有 7 比特的主机号码，即每个子网最多可有 126 ( $2^7-2$ ，去掉主机号码字段全 1 的广播地址和主机号码字段全 0 的网段地址) 个主机号码。因此主机号码的总数是  $512 \times 126 = 64512$  个，比不划分子网时要少 1022 个。

若不进行子网划分，则子网掩码为默认值，此时子网掩码中“1”的长度就是网络号码的长度，即 A、B、C 类 IP 地址对应的子网掩码默认值分别为 255.0.0.0、255.255.0.0 和 255.255.255.0。

### 1.1.4 IP地址的获取方式

接口获取 IP 地址有以下几种方式：

- 通过手动指定 IP 地址，本手册只介绍通过手动指定 IP 地址的方式。
- 通过 BOOTP 分配得到 IP 地址，通过 BOOTP 分配得到 IP 地址方式的介绍请参见“三层技术-IP 业务配置指导”中的“BOOTP 客户端”。
- 通过 DHCP 分配得到 IP 地址，通过 DHCP 分配得到 IP 地址方式的介绍请参见“三层技术-IP 业务配置指导”中的“DHCP 客户端”。



这几种方式是互斥的,通过新的配置方式获取的 IP 地址会覆盖通过原有方式获取的 IP 地址。例如,首先通过手动指定了 IP 地址,然后使用 DHCP 协议申请 IP 地址,那么手动指定的 IP 地址会被删除,接口的 IP 地址是通过 DHCP 协议分配的。

## 1.2 手工指定接口的IP地址

### 1. 功能简介

设备的每个接口可以配置多个 IP 地址,其中一个为主 IP 地址,其余为从 IP 地址。

一般情况下,一个接口只需配置一个主 IP 地址,但在有些特殊情况下需要配置从 IP 地址。比如,一台设备通过一个接口连接了一个局域网,但该局域网中的计算机分别属于 2 个不同的子网,为了使设备与局域网中的所有计算机通信,就需要在该接口上配置一个主 IP 地址和一个从 IP 地址。

### 2. 配置限制和指导

- 一个接口只能有一个主 IP 地址。新配置的主 IP 地址将覆盖原有主 IP 地址。
- 当接口被配置为通过 BOOTP、DHCP 方式获取 IP 地址或借用其它接口的 IP 地址后,则不能再给该接口配置从 IP 地址。
- 同一接口的主、从 IP 地址可以在同一网段,但不同接口之间不可以在同一网段。
- 设备支持在不同接口上配置掩码不同但最短掩码对应网络位相同的地址,比如地址 1.1.1.1/16 和 1.1.2.1/24,这两个地址的最短掩码 16 对应的网络位都是 1.1.0.0。缺省连接这两个接口上的用户不能互通,如需互通,需要配置普通代理 ARP 功能,关于普通代理 ARP 的描述,请参见“三层技术-IP 业务配置指导”中的“ARP”。

### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置接口的 IP 地址。

```
ip address ip-address { mask-length | mask } [ sub ]
```

缺省情况下,未配置接口 IP 地址。

## 1.3 配置接口借用IP地址

### 1. 功能简介

IP 地址借用是指一个接口上未配置 IP 地址,但为了使该接口能正常使用,就向同一设备上其它有 IP 地址的接口借用一个 IP 地址。IP 地址借用的使用场景如下:

- 在 IP 地址资源比较匮乏的环境下,为了节约 IP 地址资源,可以配置某个接口借用其它接口的 IP 地址。
- 如果某个接口只是偶尔使用,可以配置该接口借用其它接口的 IP 地址,而不必让其一直占用一个单独的 IP 地址。

### 2. 配置限制和指导

- Loopback 接口的 IP 地址可被其它接口借用,但本身不能借用其它接口的地址。

- 被借用接口的地址本身不能为借用地址。
- 一个接口的地址可以借给多个接口。
- 如果被借用接口有多个手动配置的 IP 地址，则只有手动配置的主 IP 地址能被借用。
- 由于借用方接口本身没有 IP 地址，无法在此接口上启用动态路由协议。所以必须手动配置一条到对端网段的静态路由，才能实现设备间的连通。

### 3. 配置准备

被借用接口的 IP 地址已经配置，配置方法可以为手动指定、通过 BOOTP 或 DHCP 动态获取。

### 4. 配置步骤

- (1) 进入系统视图。  
`system-view`
- (2) 进入接口视图。  
`interface interface-type interface-number`
- (3) 配置本接口借用指定接口的 IP 地址。  
`ip address unnumbered interface interface-type interface-number`  
缺省情况下，本接口未借用其它接口的 IP 地址。

## 1.4 IP地址显示和维护

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 IP 地址的运行情况，通过查看显示信息验证配置的效果。

表1-2 IP 地址的显示和维护

操作	命令
显示三层接口与IP相关的简要信息	<code>display ip interface [ interface-type [ interface-number ] ] brief [ description ]</code>
显示三层接口与IP相关的配置和统计信息	<code>display ip interface [ interface-type interface-number ]</code>

## 1.5 地址典型配置举例

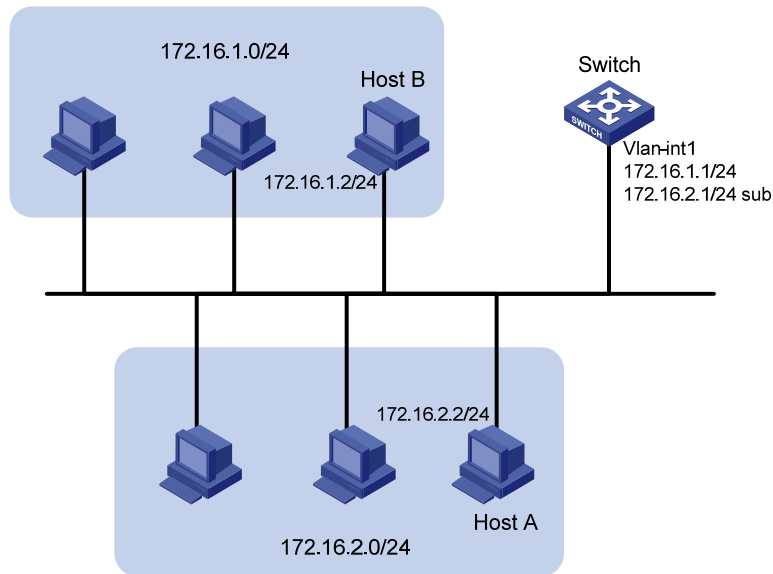
### 1.5.1 手工指定IP地址配置举例

#### 1. 组网需求

Switch 的端口(属于 VLAN 1)连接一个局域网，局域网中的计算机分别属于 2 个网段：172.16.1.0/24 和 172.16.2.0/24。要求这两个网段的主机都可以通过 Switch 与外部网络通信，且这两个网段中的主机能够互通。

## 2. 组网图

图1-3 IP 地址配置组网图



## 3. 配置步骤

针对上述的需求，如果在 **Switch** 的 **VLAN** 接口 1 上只配置一个 IP 地址，则只有一部分主机能够通过 **Switch** 与外部网络通信。为了使局域网内的所有主机都能够通过 **Switch** 访问外部网络，需要配置 **VLAN** 接口 1 的从 IP 地址。为了使两个网段中的主机能够互通，两个网段中的主机都需要将 **Switch** 设置为网关。

# 配置 **VLAN** 接口 1 的主 IP 地址和从 IP 地址。

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch-Vlan-interfacel] ip address 172.16.1.1 255.255.255.0
[Switch-Vlan-interfacel] ip address 172.16.2.1 255.255.255.0 sub
```

# 在 172.16.1.0/24 网段中的主机上配置网关为 172.16.1.1；在 172.16.2.0/24 网段中的主机上配置网关为 172.16.2.1。

## 4. 验证配置

# 使用 **ping** 命令检测 **Switch** 与网络 172.16.1.0/24 内主机的连通性。

```
<Switch> ping 172.16.1.2
Ping 172.16.1.2 (172.16.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 172.16.1.2: icmp_seq=0 ttl=128 time=7.000 ms
56 bytes from 172.16.1.2: icmp_seq=1 ttl=128 time=2.000 ms
56 bytes from 172.16.1.2: icmp_seq=2 ttl=128 time=1.000 ms
56 bytes from 172.16.1.2: icmp_seq=3 ttl=128 time=1.000 ms
56 bytes from 172.16.1.2: icmp_seq=4 ttl=128 time=2.000 ms

--- Ping statistics for 172.16.1.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/2.600/7.000/2.245 ms
```

显示信息表示 Switch 与网络 172.16.1.0/24 内的主机可以互通。

# 使用 **ping** 命令检测 Switch 与网络 172.16.2.0/24 内主机的连通性。

```
<Switch> ping 172.16.2.2
Ping 172.16.2.2 (172.16.2.2): 56 data bytes, press CTRL_C to break
56 bytes from 172.16.2.2: icmp_seq=0 ttl=128 time=2.000 ms
56 bytes from 172.16.2.2: icmp_seq=1 ttl=128 time=7.000 ms
56 bytes from 172.16.2.2: icmp_seq=2 ttl=128 time=1.000 ms
56 bytes from 172.16.2.2: icmp_seq=3 ttl=128 time=2.000 ms
56 bytes from 172.16.2.2: icmp_seq=4 ttl=128 time=1.000 ms

--- Ping statistics for 172.16.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/2.600/7.000/2.245 ms
```

显示信息表示 Switch 与网络 172.16.2.0/24 内的主机可以互通。

# 使用 **ping** 命令检测网络 172.16.1.0/24 和网络 172.16.2.0/24 内主机的连通性。在 Host A 上可以 ping 通 Host B。

# 目 录

<b>1 DHCP概述 .....</b>	<b>1-1</b>
1.1 DHCP组网模型 .....	1-1
1.2 DHCP的IP地址分配 .....	1-1
1.2.1 IP地址分配策略 .....	1-1
1.2.2 IP地址获取过程 .....	1-2
1.2.3 IP地址的租约更新 .....	1-2
1.3 DHCP报文格式 .....	1-3
1.4 DHCP选项介绍 .....	1-4
1.5 DHCP常用选项 .....	1-4
1.6 自定义DHCP选项 .....	1-5
1.6.1 厂商特定信息选项（Option 43） .....	1-5
1.6.2 中继代理信息选项（Option 82） .....	1-6
1.6.3 Option 184 .....	1-7
1.7 协议规范 .....	1-7
<b>2 DHCP服务器 .....</b>	<b>2-1</b>
2.1 DHCP服务器简介 .....	2-1
2.1.1 地址池的地址管理方式 .....	2-1
2.1.2 地址池的选取原则 .....	2-2
2.1.3 DHCP服务器分配IP地址的优先次序 .....	2-2
2.2 DHCP服务器与硬件适配关系 .....	2-3
2.3 DHCP服务器配置任务简介 .....	2-3
2.4 创建DHCP用户类 .....	2-4
2.5 配置DHCP服务器的地址池 .....	2-4
2.5.1 DHCP服务器地址池配置任务简介 .....	2-4
2.5.2 创建DHCP地址池 .....	2-5
2.5.3 配置一个主网段多个地址范围的动态地址管理方式 .....	2-5
2.5.4 配置一个主网段多个从网段的动态地址管理方式 .....	2-6
2.5.5 配置静态地址绑定 .....	2-8
2.5.6 配置DHCP客户端使用的网关地址 .....	2-8
2.5.7 配置DHCP客户端使用的域名后缀 .....	2-9
2.5.8 配置DHCP客户端使用的DNS服务器地址 .....	2-10
2.5.9 配置DHCP客户端使用的WINS服务器地址和NetBIOS节点类型 .....	2-10

2.5.10 配置DHCP客户端使用的BIMS服务器信息 .....	2-11
2.5.11 配置DHCP客户端使用的远程启动文件信息 .....	2-11
2.5.12 配置DHCP客户端使用的下一个提供服务的服务器IP地址 .....	2-12
2.5.13 配置DHCP客户端使用的Option 184 参数 .....	2-12
2.5.14 自定义DHCP选项 .....	2-13
2.5.15 配置DHCP用户类白名单功能 .....	2-15
2.6 配置接口引用地址池 .....	2-15
2.7 配置DHCP策略动态分配地址和其他参数 .....	2-16
2.8 开启DHCP服务 .....	2-17
2.9 配置接口工作在DHCP服务器模式 .....	2-17
2.10 配置IP地址冲突检测功能 .....	2-17
2.11 配置Option 82 的处理方式 .....	2-18
2.12 配置DHCP服务器安全功能 .....	2-18
2.12.1 配置限制和指导 .....	2-18
2.12.2 配置防止DHCP饿死攻击 .....	2-19
2.13 配置DHCP服务器兼容性 .....	2-19
2.13.1 配置DHCP服务器始终以广播方式回复请求报文 .....	2-19
2.13.2 配置DHCP服务器忽略BOOTP请求报文 .....	2-20
2.13.3 配置DHCP服务器以RFC 1048 规定的格式发送BOOTP应答报文 .....	2-20
2.14 配置DHCP服务器发送DHCP报文的DSCP优先级 .....	2-21
2.15 配置DHCP服务器租约固化功能 .....	2-21
2.16 开启DHCP服务器的用户下线探测功能 .....	2-22
2.17 配置DHCP告警功能 .....	2-22
2.18 开启DHCP服务器日志信息功能 .....	2-23
2.19 DHCP服务器显示和维护 .....	2-23
2.20 DHCP服务器典型配置举例 .....	2-24
2.20.1 静态绑定地址配置举例 .....	2-24
2.20.2 动态分配地址配置举例 .....	2-25
2.20.3 按用户类分配地址配置举例 .....	2-27
2.20.4 用户类白名单功能配置举例 .....	2-29
2.20.5 主从网段配置举例 .....	2-30
2.20.6 自定义DHCP选项配置举例 .....	2-31
2.21 DHCP服务器常见故障处理 .....	2-33
2.21.1 DHCP客户端获取到冲突的IP地址 .....	2-33
<b>3 DHCP中继 .....</b>	<b>3-1</b>
3.1 DHCP中继简介 .....	3-1

3.1.2 DHCP中继的基本原理 .....	3-1
3.1.3 DHCP中继支持Option 82 功能 .....	3-2
3.1.4 DHCP中继支持MCE .....	3-2
3.2 DHCP中继与硬件适配关系 .....	3-2
3.3 DHCP中继配置任务简介 .....	3-2
3.4 开启DHCP服务 .....	3-3
3.5 配置接口工作在DHCP中继模式 .....	3-3
3.6 指定DHCP服务器的地址 .....	3-4
3.6.1 指定DHCP中继对应的DHCP服务器地址 .....	3-4
3.6.2 指定中继地址池对应的DHCP服务器地址 .....	3-4
3.6.3 配置DHCP中继选择DHCP服务器方式 .....	3-5
3.7 配置DHCP中继的安全功能 .....	3-6
3.7.1 配置DHCP中继用户地址表项记录功能 .....	3-6
3.7.2 配置DHCP中继动态用户地址表项定时刷新功能 .....	3-7
3.7.3 配置防止DHCP饿死攻击 .....	3-7
3.7.4 配置DHCP中继支持代理功能 .....	3-8
3.7.5 配置DHCP中继的用户下线探测功能 .....	3-9
3.8 配置通过DHCP中继释放客户端的IP地址 .....	3-9
3.9 配置DHCP中继支持Option 82 功能 .....	3-10
3.10 配置DHCP中继发送DHCP报文的DSCP优先级 .....	3-10
3.11 配置DHCP中继在DHCP报文中填充的中继地址 .....	3-11
3.11.1 手工指定在DHCP报文中填充的中继地址 .....	3-11
3.11.2 通过smart-relay功能指定DHCP报文中填充的中继地址 .....	3-11
3.12 指定DHCP中继向DHCP服务器转发报文的源地址 .....	3-12
3.13 DHCP中继显示和维护 .....	3-12
3.14 DHCP中继典型配置举例 .....	3-13
3.14.1 DHCP中继基本组网配置举例 .....	3-13
3.14.2 DHCP中继支持Option 82 配置举例 .....	3-14
3.14.3 DHCP中继选择DHCP服务器方式配置举例 .....	3-15
3.15 DHCP中继常见故障处理 .....	3-16
3.15.1 DHCP客户端无法通过DHCP中继获取配置信息 .....	3-16
<b>4 DHCP客户端 .....</b>	<b>4-1</b>
4.1 DHCP客户端简介 .....	4-1
4.2 DHCP客户端配置限制和指导 .....	4-1
4.3 DHCP客户端配置任务简介 .....	4-1
4.4 配置接口通过DHCP协议获取IP地址 .....	4-1

4.5 配置接口使用的DHCP客户端ID .....	4-2
4.6 开启地址冲突检查功能 .....	4-2
4.7 配置DHCP客户端发送DHCP报文的DSCP优先级 .....	4-3
4.8 DHCP客户端显示和维护 .....	4-3
4.9 DHCP客户端典型配置举例 .....	4-3
4.9.1 DHCP客户端基本组网配置举例 .....	4-3
<b>5 DHCP Snooping .....</b>	<b>5-1</b>
5.1 DHCP Snooping简介 .....	5-1
5.1.1 DHCP Snooping作用 .....	5-1
5.1.2 信任端口的典型应用环境 .....	5-2
5.1.3 DHCP Snooping支持Option 82 功能 .....	5-3
5.2 DHCP Snooping配置限制和指导 .....	5-3
5.3 DHCP Snooping配置任务简介 .....	5-4
5.4 配置DHCP Snooping基本功能 .....	5-4
5.4.1 在普通组网中配置DHCP Snooping基本功能 .....	5-4
5.5 配置DHCP Snooping支持Option 82 功能 .....	5-5
5.6 配置DHCP Snooping表项固化功能 .....	5-6
5.7 配置接口动态学习DHCP Snooping表项的最大数目 .....	5-7
5.8 配置DHCP Snooping报文限速功能 .....	5-7
5.9 配置DHCP Snooping安全功能 .....	5-8
5.9.1 配置防止DHCP饿死攻击 .....	5-8
5.9.2 配置防止伪造DHCP请求方向报文攻击 .....	5-9
5.9.3 开启DHCP Snooping报文阻断功能 .....	5-9
5.10 开启DHCP Snooping日志信息功能 .....	5-10
5.11 关闭接口的DHCP Snooping功能 .....	5-10
5.12 DHCP Snooping显示和维护 .....	5-11
5.13 DHCP Snooping典型配置举例 .....	5-11
5.13.1 全局开启DHCP Snooping配置举例 .....	5-11
5.13.2 按VLAN开启DHCP Snooping配置举例 .....	5-12
5.13.3 DHCP Snooping支持Option 82 配置举例 .....	5-13
<b>6 BOOTP客户端 .....</b>	<b>6-1</b>
6.1 BOOTP客户端简介 .....	6-1
6.1.1 BOOTP客户端的应用环境 .....	6-1
6.1.2 IP地址动态获取过程 .....	6-1
6.1.3 协议规范 .....	6-1
6.2 配置接口通过BOOTP协议获取IP地址 .....	6-1



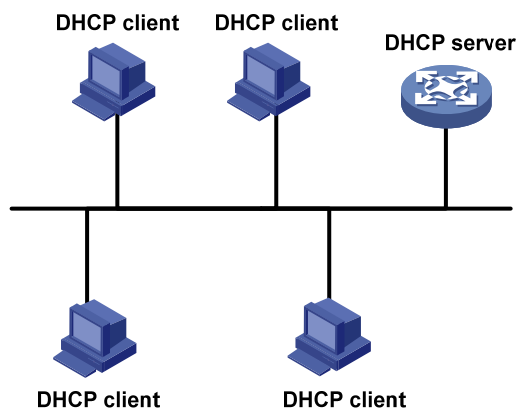
6.3 BOOTP客户端显示和维护 .....	6-2
6.4 BOOTP客户端典型配置举例 .....	6-2
6.4.1 BOOTP客户端典型配置举例.....	6-2

# 1 DHCP概述

## 1.1 DHCP组网模型

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）采用客户端/服务器模式，由服务器为网络设备动态地分配IP地址等网络配置参数。DHCP客户端和DHCP服务器处于不同物理网段时，客户端可以通过DHCP中继与服务器通信，获取IP地址及其他配置信息。DHCP中继的详细介绍，请参见“[3.1 DHCP中继简介](#)”。

图1-1 同网段 DHCP 组网应用



## 1.2 DHCP的IP地址分配

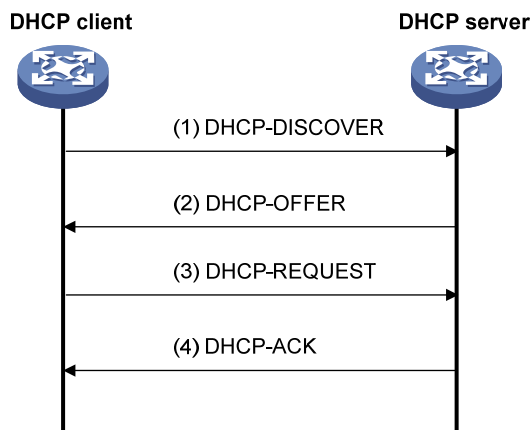
### 1.2.1 IP地址分配策略

针对客户端的不同需求，DHCP 提供三种 IP 地址分配策略：

- 手工分配地址：由管理员为少数特定客户端（如 WWW 服务器等）静态绑定固定的 IP 地址。通过 DHCP 将配置的固定 IP 地址分配给客户端。
- 自动分配地址：DHCP 为客户端分配租期为无限长的 IP 地址。
- 动态分配地址：DHCP 为客户端分配具有一定有效期限的 IP 地址，到达使用期限后，客户端需要重新申请地址。绝大多数客户端得到的都是这种动态分配的地址。

## 1.2.2 IP地址获取过程

图1-2 IP 地址动态获取过程



如 [图 1-2](#) 所示，DHCP 客户端从 DHCP 服务器获取 IP 地址，主要通过四个阶段进行：

- (1) 发现阶段，即 DHCP 客户端寻找 DHCP 服务器的阶段。客户端以广播方式发送 DHCP-DISCOVER 报文。
- (2) 提供阶段，即 DHCP 服务器提供 IP 地址的阶段。DHCP 服务器接收到客户端的 DHCP-DISCOVER 报文后，根据 IP 地址分配的优先次序选出一个 IP 地址，与其他参数一起通过 DHCP-OFFER 报文发送给客户端。
- (3) 选择阶段，即 DHCP 客户端选择 IP 地址的阶段。如果有多台 DHCP 服务器向该客户端发来 DHCP-OFFER 报文，客户端只接受第一个收到的 DHCP-OFFER 报文，然后以广播方式发送 DHCP-REQUEST 报文，该报文中包含 DHCP 服务器在 DHCP-OFFER 报文中分配的 IP 地址。
- (4) 确认阶段，即 DHCP 服务器确认 IP 地址的阶段。DHCP 服务器收到 DHCP 客户端发来的 DHCP-REQUEST 报文后，只有 DHCP 客户端选择的服务器会进行如下操作：如果确认将地址分配给该客户端，则返回 DHCP-ACK 报文；否则返回 DHCP-NAK 报文，表明地址不能分配给该客户端。

客户端收到服务器返回的 DHCP-ACK 确认报文后，会以广播的方式发送免费 ARP 报文，探测是否有主机使用服务器分配的 IP 地址，如果在规定的时间内未收到回应，并且客户端上不存在与该地址同网段的其他地址时，客户端才使用此地址。否则，客户端会发送 DHCP-DECLINE 报文给 DHCP 服务器，并重新申请 IP 地址。

如果网络中存在多个 DHCP 服务器，除 DHCP 客户端选中的服务器外，其它 DHCP 服务器中本次未分配出的 IP 地址仍可分配给其他客户端。

## 1.2.3 IP地址的租约更新

DHCP 服务器分配给客户端的 IP 地址具有一定的租借期限（除自动分配的 IP 地址），该租借期限称为租约。当租借期满后服务器会收回该 IP 地址。如果 DHCP 客户端希望继续使用该地址，则 DHCP 客户端需要申请延长 IP 地址租约。

在 DHCP 客户端的 IP 地址租约期限达到一半左右时间时，DHCP 客户端会向为它分配 IP 地址的 DHCP 服务器单播发送 DHCP-REQUEST 报文，以进行 IP 租约的更新。如果客户端可以继续使用此 IP 地址，则 DHCP 服务器回应 DHCP-ACK 报文，通知 DHCP 客户端已经获得新 IP 租约；如果此 IP 地址不可以再分配给该客户端，则 DHCP 服务器回应 DHCP-NAK 报文，通知 DHCP 客户端不能获得新的租约。

如果在租约的一半左右时间进行的续约操作失败，DHCP 客户端会在租约期限达到 7/8 时，广播发送 DHCP-REQUEST 报文进行续约。DHCP 服务器的处理方式同上，不再赘述。

### 1.3 DHCP报文格式

DHCP有 8 种类型的报文，每种报文的格式都相同，只是某些字段的取值不同。DHCP的报文格式如 图 1-3 所示，括号中的数字表示该字段所占的字节。

图1-3 DHCP 报文格式

0	7	15	23	31
op (1)	htype (1)	hlen (1)	hops (1)	
xid (4)				
secs (2)		flags (2)		
ciaddr (4)				
yiaddr (4)				
siaddr (4)				
giaddr (4)				
chaddr (16)				
sname (64)				
file (128)				
options (variable)				

各字段的解释如下：

- op: 报文的操作类型，分为请求报文和响应报文，1 为请求报文；2 为响应报文。具体的报文类型在 options 字段中标识。
- htype、hlen: DHCP 客户端的硬件地址类型及长度。
- hops: DHCP 报文经过的 DHCP 中继的数目。DHCP 请求报文每经过一个 DHCP 中继，该字段就会增加 1。
- xid: 客户端发起一次请求时选择的随机数，用来标识一次地址请求过程。
- secs: DHCP 客户端开始 DHCP 请求后所经过的时间。目前没有使用，固定为 0。
- flags: 第一个比特为广播响应标识位，用来标识 DHCP 服务器响应报文是采用单播还是广播方式发送，0 表示采用单播方式，1 表示采用广播方式。其余比特保留不用。
- ciaddr: DHCP 客户端的 IP 地址。如果客户端有合法和可用的 IP 地址，则将其添加到此字段，否则字段设置为 0。此字段不用于客户端申请某个特定的 IP 地址。
- yiaddr: DHCP 服务器分配给客户端的 IP 地址。
- siaddr: DHCP 客户端获取启动配置信息的服务器 IP 地址。

- giaddr: DHCP 客户端发出请求报文后经过的第一个 DHCP 中继的 IP 地址。
- chaddr: DHCP 客户端的硬件地址。
- sname: DHCP 客户端获取启动配置信息的服务器名称。
- file: DHCP 服务器为 DHCP 客户端指定的启动配置文件名称及路径信息。
- options: 可选变长选项字段，包含报文的类型、有效租期、DNS 服务器的 IP 地址、WINS 服务器的 IP 地址等配置信息。

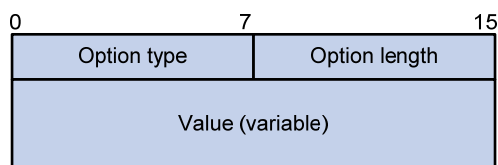
## 1.4 DHCP选项介绍

为了与 BOOTP (Bootstrap Protocol, 自举协议) 兼容, DHCP 保留了 BOOTP 的消息格式。DHCP 和 BOOTP 消息的不同主要体现在选项 (Options) 字段。DHCP 在 BOOTP 基础上增加的功能, 通过 Options 字段来实现。

DHCP 利用 Options 字段传递控制信息和网络配置参数, 实现地址动态分配的同时, 为客户端提供更加丰富的网络配置信息。

DHCP选项的格式如 [图 1-4](#) 所示。

图1-4 DHCP 选项格式



## 1.5 DHCP常用选项

常见的 DHCP 选项有：

- Option 3: 路由器选项, 用来指定为客户端分配的网关地址。
- Option 6: DNS 服务器选项, 用来指定为客户端分配的 DNS 服务器地址。
- Option 33: 静态路由选项。该选项中包含一组有分类静态路由 (即目的网络地址的掩码固定为自然掩码, 不能划分子网), 客户端收到该选项后, 将在路由表中添加这些静态路由。如果 Option 33 和 Option 121 同时存在, 则忽略 Option 33。
- Option 51: IP 地址租约选项。
- Option 53: DHCP 消息类型选项, 标识 DHCP 消息的类型。
- Option 55: 请求参数列表选项。客户端利用该选项指明需要从服务器获取哪些网络配置参数。该选项内容为客户端请求的参数对应的选项值。
- Option 60: 厂商标识选项。客户端利用该选项标识自己所属的厂商; DHCP 服务器可以根据该选项区分客户端所属的厂商, 并为其分配特定范围的 IP 地址。
- Option 66: TFTP 服务器名选项, 用来指定为客户端分配的 TFTP 服务器的域名。
- Option 67: 启动文件名选项, 用来指定为客户端分配的启动文件名。

- **Option 121:** 无分类路由选项。该选项中包含一组无分类静态路由（即目的网络地址的掩码为任意值，可以通过掩码来划分子网），客户端收到该选项后，将在路由表中添加这些静态路由。如果 **Option 33** 和 **Option 121** 同时存在，则忽略 **Option 33**。
  - **Option 150:** TFTP 服务器地址选项，用来指定为客户端分配的 TFTP 服务器的地址。
- 更多 DHCP 选项的介绍，请参见 RFC 2132 和 RFC 3442。

## 1.6 自定义DHCP选项

有些选项的内容，RFC 2132 中没有统一规定，例如 **Option 43**、**Option 82** 和 **Option 184**。下面将介绍设备上定义的几种选项。

### 1.6.1 厂商特定信息选项（Option 43）

#### 1. Option 43 的作用

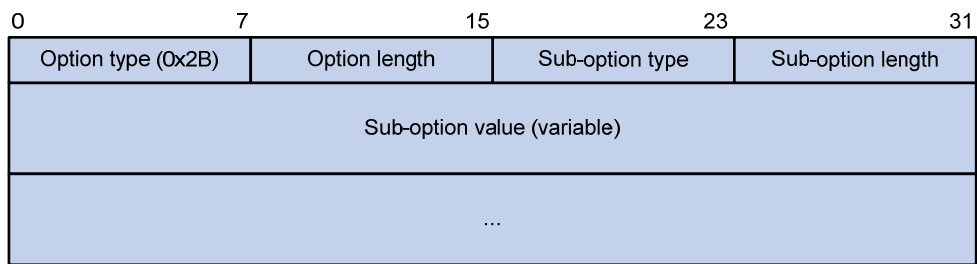
**Option 43** 称为厂商特定信息选项。DHCP 服务器和 DHCP 客户端通过 **Option 43** 交换厂商特定的信息。

设备作为 DHCP 客户端时，可以通过 **Option 43** 获取：

- **ACS**（Auto-Configuration Server，自动配置服务器）的参数，包括 URL 地址、用户名和密码。
- 服务提供商标识，**CPE**（Customer Premises Equipment，用户侧设备）从 DHCP 服务器获取该信息后，将该信息通告给 ACS，以便 ACS 选择服务提供商特有的配置和参数等。**CPE** 和 ACS 的详细介绍，请参见“网络管理和监控配置指导”中的“CWMP（TR-069）”。
- **PXE**（Preboot eXecution Environment，预启动执行环境）引导服务器地址，以便客户端从 PXE 引导服务器获取启动文件或其他控制信息。

#### 2. Option 43 格式

图1-5 Option 43 格式



为了提供可扩展性，通过**Option 43** 为客户端分配更多的信息，**Option 43** 采用子选项的形式，通过不同的子选项为用户分配不同的网络配置参数。如 [图 1-5](#) 所示。子选项中各字段的含义为：

- **Sub-option type:** 子选项类型。目前，子选项类型值可以为 0x01 表示 ACS 参数子选项，0x02 表示服务提供商标识子选项，0x80 表示 PXE 引导服务器地址子选项。
- **Sub-option length:** 子选项的长度，不包括子选项类型和子选项长度字段。
- **Sub-option value:** 子选项的取值。不同类型的子选项，取值格式有所不同。

3. Option 43 子选项取值字段的格式

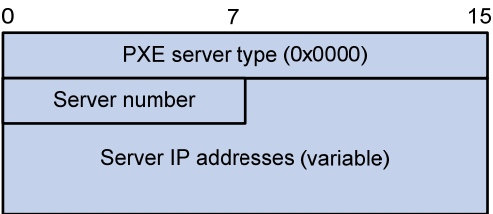
- ACS参数子选项的取值字段格式如 图 1-6 所示。ACS的URL地址、用户名和密码长度可变，每个参数之间用空格（十六进制数为 20）隔开。

图1-6 ACS 参数子选项取值字段的格式

URL of ACS (variable)	20
User name of ACS (variable)	20
Password of ACS (variable)	

- 服务提供商标识子选项的取值字段内容为服务提供商的标识。
- PXE引导服务器地址子选项的取值字段格式如 图 1-7 所示。其中，PXE服务器类型目前取值只能为 0；Server number为子选项中包含的PXE服务器地址的数目；Server IP addresses为PXE服务器的IP地址。

图1-7 PXE 引导服务器地址子选项取值字段的格式



1.6.2 中继代理信息选项（Option 82）

Option 82 称为中继代理信息选项，该选项记录了 DHCP 客户端的位置信息。DHCP 中继或 DHCP Snooping 设备接收到 DHCP 客户端发送给 DHCP 服务器的请求报文后，在该报文中添加 Option 82，并转发给 DHCP 服务器。

管理员可以从 Option 82 中获得 DHCP 客户端的位置信息，以便定位 DHCP 客户端，实现对客户端的安全和计费控制。支持 Option 82 的服务器还可以根据该选项的信息制定 IP 地址和其他参数的分配策略，提供更加灵活的地址分配方案。

Option 82 最多可以包含 255 个子选项。若定义了 Option 82，则至少要定义一个子选项。目前设备只支持两个子选项：sub-option 1（Circuit ID，电路 ID 子选项）、sub-option 2（Remote ID，远程 ID 子选项）和 sub-option 5（Link Selection，链路选择子选项）等。

由于 Option 82 的内容没有统一规定，不同厂商通常根据需要进行填充。

设备上，Circuit ID 的填充模式有以下几种：

- 采用 string 模式填充：sub-option 1 的内容是用户配置的字符串。
- 采用 normal 模式填充：sub-option 1 的内容是接收到 DHCP 客户端请求报文的接口所属的 VLAN ID 以及接口编号。
- 采用 verbose 模式填充：sub-option 1 的内容包括用户配置的接入节点标识，接收到 DHCP 客户端请求报文的接口类型、接口编号和接口所属的 VLAN ID。

Remote ID 的填充模式有以下几种：

- 采用 **string** 模式填充：sub-option 2 的内容是用户配置的字符串。
- 采用 **normal** 模式填充：sub-option 2 的内容是接收到 DHCP 客户端请求报文的接口 MAC 地址（DHCP 中继）或设备的桥 MAC 地址（DHCP Snooping）。
- 采用 **sysname** 模式填充：sub-option 2 的内容是设备的系统名称。设备的系统名称可以通过系统视图下的 **sysname** 命令配置。

Link Selection 的填充内容是 **giaddr** 字段或开启 DHCP 中继功能接口的地址。在中继上配置 **dhcp relay information enable** 命令开启支持 Option 82 功能，并配置 **dhcp relay source-address { ip-address | interface interface-type interface-number }** 指定 DHCP 中继向 DHCP 服务器转发报文的源地址时，DHCP 中继转发的 DHCP 报文中的 Option 82 选项中会携带此子选项。

### 1.6.3 Option 184

Option 184 是 RFC 中规定的保留选项，用户可以自定义该选项中携带的信息。设备上，Option 184 携带了语音呼叫所需的信息。通过 Option 184，可以实现在为具有语音功能的 DHCP 客户端提供语音呼叫相关信息。

目前 Option 184 支持四个子选项，承载的内容如下：

- sub-option 1: 网络呼叫处理器的 IP 地址，用来标识作为网络呼叫控制源及应用程序下载的服务器。只有定义了 sub-option 1（网络呼叫处理器的 IP 地址子选项），其他子选项才能生效。
- sub-option 2: 备用服务器的 IP 地址，当 sub-option 1 中携带的网络呼叫处理器不可达或不合法时，DHCP 客户端使用该选项指定的备用服务器作为网络呼叫处理器。
- sub-option 3: 语音 VLAN 信息，指定语音 VLAN 的 ID 及 DHCP 客户端是否会将所指定的 VLAN 作为语音 VLAN。
- sub-option 4: 自动故障转移呼叫路由，指定故障转移呼叫路由的 IP 地址及其关联的拨号串，即 SIP（Session Initiation Protocol，会话初始协议）用户之间互相通信时对端的 IP 地址和呼叫号码。当网络呼叫处理器和备用服务器均不可达时，SIP 用户可以使用对端 IP 地址及呼叫号码直接与对端 SIP 用户建立连接并通信。

## 1.7 协议规范

与 DHCP 相关的协议规范有：

- RFC 2131: Dynamic Host Configuration Protocol
- RFC 2132: DHCP Options and BOOTP Vendor Extensions
- RFC 1542: Clarifications and Extensions for the Bootstrap Protocol
- RFC 3046: DHCP Relay Agent Information Option
- RFC 3442: The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4



## 2 DHCP服务器

### 2.1 DHCP服务器简介

DHCP 服务器通过地址池保存 IP 地址和网络参数，从地址池中选择 IP 地址和网络参数分配给客户端。

#### 2.1.1 地址池的地址管理方式

地址池的地址管理方式有以下几种：静态绑定 IP 地址，即通过将客户端的 MAC 地址或客户端 ID 与 IP 地址绑定的方式，实现为特定的客户端分配特定的 IP 地址；动态选择 IP 地址，即在地址池中指定可供分配的 IP 地址范围，当收到客户端的 IP 地址申请时，从该地址范围中动态选择 IP 地址，分配给该客户端。

在地址池中指定可供分配的 IP 地址范围，有以下几种方法：

##### 1. 为地址池指定一个主网段，并将该网段划分为多个地址范围。

多个地址范围是指一个地址池动态分配的 IP 地址范围（公共地址范围）和多个为 DHCP 用户类分配的 IP 地址范围。

DHCP 服务器通过定义 DHCP 用户类，实现为满足特定条件的客户端分配特定地址范围的 IP 地址。DHCP 服务器根据客户端发送的请求报文，判断 DHCP 客户端所属的用户类。每个用户类可以配置多个匹配条件，只要客户端发送的 DHCP 请求报文满足任意一个匹配条件，就认为该客户端属于该用户类。在地址池下，可以为不同的用户类指定不同的地址范围。如果 DHCP 客户端属于某个用户类，则从该用户类的地址范围内选择地址分配给该客户端。

采用这种地址管理方式时，地址选择过程为：

- (1) 按照地址池下用户类地址范围的配置顺序，将 DHCP 客户端和用户类进行匹配。
- (2) 如果 DHCP 客户端属于某个用户类，则从该用户类的地址范围中选择地址分配给客户端。
- (3) 如果该用户类中没有可供分配的地址，则继续匹配下一个用户类。如果所有匹配上的用户类地址范围都没有可供分配的地址，则从公共地址范围中选择地址分配给客户端。
- (4) 如果 DHCP 客户端不属于任何一个 DHCP 用户类，则会从地址池动态分配的 IP 地址范围（通过 **address range** 命令配置）中选择地址分配给 DHCP 客户端。
- (5) 如果动态分配的 IP 地址范围内也没有空闲地址，或者未配置动态分配的 IP 地址范围，则地址分配失败，即 DHCP 服务器无法为 DHCP 客户端分配地址。



说明

每个地址范围内的地址都必须属于指定的主网段，否则无法分配该范围内的地址。

---

## 2. 为地址池指定一个主网段，并指定多个从网段。

采用此种地址分配方式时，地址选择的过程是：首先从地址池主网段中查找可供分配的 IP 地址。如果主网段中没有可供分配的 IP 地址，则按照该地址池下从网段的配置顺序，依次查找可供分配的 IP 地址。

### 2.1.2 地址池的选取原则

DHCP 服务器为客户端分配 IP 地址时，按照如下顺序选择地址池：

- (1) 如果存在将客户端 MAC 地址或客户端 ID 与 IP 地址静态绑定的地址池，则选择该地址池，并将静态绑定的 IP 地址和其他网络参数分配给客户端。
- (2) 如果接收到 DHCP 请求报文的接口引用了某个地址池，则选择该地址池，从该地址池中选取 IP 地址和其他网络参数分配给客户端。
- (3) 如果配置了 DHCP 策略，则 DHCP 客户端匹配某个 DHCP 用户类时，DHCP 服务器选择与该 DHCP 用户类关联的 DHCP 地址池；DHCP 客户端未匹配到 DHCP 用户类时，若配置了默认 DHCP 地址池，则选择该 DHCP 地址池；若未配置默认 DHCP 地址池或 DHCP 默认地址池不存在可供分配的 IP 地址时，IP 地址或其他参数分配失败。
- (4) 如果上述条件均不满足，则使用以下方法选择 DHCP 地址池：
  - 如果客户端与服务器在同一网段，则将 DHCP 请求报文接收接口的 IP 地址与所有地址池配置的主网段进行匹配，并选择最长匹配的主网段所对应的地址池。如果未匹配到主网段，则将 DHCP 请求报文接收接口的 IP 地址与所有地址池配置的从网段进行匹配，并选择最长匹配的网段所对应的地址池。
  - 如果客户端与服务器不在同一网段，即客户端通过 DHCP 中继获取 IP 地址，则将 DHCP 请求报文中 giaddr 字段指定的 IP 地址与所有地址池配置的主网段进行匹配，并选择最长匹配的网段所对应的地址池。如果未匹配到主网段，则将 DHCP 请求报文中 giaddr 字段指定的 IP 地址与所有地址池配置的从网段进行匹配，并选择最长匹配的网段所对应的地址池。

例如，DHCP 服务器上配置了两个地址池，动态分配的网段分别是 1.1.1.0/24 和 1.1.1.0/25，如果接收 DHCP 请求报文的接口 IP 地址为 1.1.1.1/25，且未引用地址池，服务器将从 1.1.1.0/25 地址池中选择 IP 地址分配给客户端，1.1.1.0/25 地址池中如果没有可供分配的 IP 地址，则服务器无法为客户端分配地址；如果接收 DHCP 请求报文的接口 IP 地址为 1.1.1.130/25，服务器将从 1.1.1.0/24 地址池中选择 IP 地址分配给客户端。



#### 说明

配置地址池动态分配的网段和 IP 地址范围时，请尽量保证其与 DHCP 服务器接口或 DHCP 中继接口地址的网段一致，以免分配错误的 IP 地址。

建议合理规划 DHCP 服务器上各地址池中主网段的配置，尽量避免客户端匹配不到主网段、直接匹配从网段的情况发生。

---

### 2.1.3 DHCP服务器分配IP地址的优先次序

DHCP 服务器为客户端分配 IP 地址的优先次序如下：

- (1) 与客户端 MAC 地址或客户端 ID 静态绑定的 IP 地址。

- (2) DHCP 服务器记录的曾经分配给客户端的 IP 地址。
- (3) 客户端发送的 DHCP-DISCOVER 报文中 Option 50 字段指定的 IP 地址。Option 50 为客户端请求的 IP 地址选项（Requested IP Address），客户端通过在 DHCP-DISCOVER 报文中添加该选项来指明客户端希望获取的 IP 地址。该选项的内容由客户端决定。
- (4) 按照“[2.1.1 地址池的地址管理方式](#)”和“[2.1.2 地址池的选取原则](#)”中所述的动态分配地址选择原则，顺序查找可供分配的IP地址，选择最先找到的IP地址。
- (5) 如果未找到可用的 IP 地址，则从当前匹配地址池中依次查询租约过期、曾经发生过冲突的 IP 地址，如果找到则进行分配，否则将不予处理。



#### 说明

如果客户端所在的网段发生变化，服务器不会为客户端分配曾经分配给它的 IP 地址，而是从匹配新网段的地址池中重新选择 IP 地址。

使用曾经发生过冲突的 IP 地址时，只有冲突状态超过一小时的 IP 地址才能够被服务器分配给新的 DHCP 客户端。

## 2.2 DHCP服务器与硬件适配关系

S5110V2-SI、S5000V3-EI 和 S5000E-X 系列交换机不支持本特性。

## 2.3 DHCP服务器配置任务简介

DHCP 服务器配置任务如下：

- (1) （可选）[创建DHCP用户类](#)
- (2) [配置DHCP服务器的地址池](#)
- (3) （可选）修改 DHCP 服务器的地址池选择方式
  - [配置接口引用地址池](#)
  - [配置DHCP策略动态分配地址和其他参数](#)
- (4) [开启DHCP服务](#)
- (5) [配置接口工作在DHCP服务器模式](#)
- (6) （可选）配置高级功能
  - [配置IP地址冲突检测功能](#)
  - [配置Option 82 的处理方式](#)
  - [配置DHCP服务器安全功能](#)
  - [配置DHCP服务器兼容性](#)
  - [配置DHCP服务器发送DHCP报文的DSCP优先级](#)
  - [配置DHCP服务器租约固化功能](#)
  - [开启DHCP服务器的用户下线探测功能](#)
- (7) （可选）配置告警及日志功能
  - [配置DHCP告警功能](#)

- [开启DHCP服务器日志信息功能](#)

## 2.4 创建DHCP用户类

### 1. 功能简介

DHCP 用户类通过 DHCP 请求报文中的硬件地址、Option 信息或 Giaddr 字段来匹配一组特定的 DHCP 客户端，以实现为特定的 DHCP 客户端分配特定的 IP 地址和其他参数。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建 DHCP 用户类，并进入 DHCP 用户类视图。

```
dhcp class class-name
```

- (3) 配置 DHCP 用户类的匹配规则。

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

缺省情况下，未配置 DHCP 用户类的匹配规则。

## 2.5 配置DHCP服务器的地址池

### 2.5.1 DHCP服务器地址池配置任务简介

DHCP 服务器地址池配置任务如下：

- (1) [创建DHCP地址池](#)

- (2) 配置为 DHCP 客户端分配地址

同一个地址池中不能同时配置两种动态地址管理方式，但可以同时配置动态地址管理方式和静态地址绑定。

- [配置一个主网段多个地址范围的动态地址管理方式](#)
- [配置一个主网段多个从网段的动态地址管理方式](#)
- [配置静态地址绑定](#)

- (3) 配置为 DHCP 客户端分配其他参数

- [配置DHCP客户端使用的网关地址](#)
- [配置DHCP客户端使用的域名后缀](#)
- [配置DHCP客户端使用的DNS服务器地址](#)
- [配置DHCP客户端使用的WINS服务器地址和NetBIOS节点类型](#)
- [配置DHCP客户端使用的BIMS服务器信息](#)
- [配置DHCP客户端使用的远程启动文件信息](#)
- [配置DHCP客户端使用的下一个提供服务的服务器IP地址](#)
- [配置DHCP客户端使用的Option 184 参数](#)

- [自定义DHCP选项](#)
- (4) (可选) [配置DHCP用户类白名单功能](#)

## 2.5.2 创建DHCP地址池

- (1) 进入系统视图。  
**system-view**
- (2) 创建 DHCP 地址池，并进入 DHCP 地址池视图。

```
dhcp server ip-pool pool-name
```

## 2.5.3 配置一个主网段多个地址范围的动态地址管理方式

### 1. 功能简介

在某些组网应用中，需要将一个网段下的不同客户端，按照一定的规则划分到不同的地址范围中。此时，可以按照客户端划分规则创建对应的 DHCP 用户类，并在地址池内为不同的用户类配置不同的地址范围，从而实现为特定的客户端分配特定范围的地址。在这种情况下，还可以配置一个公共地址范围，为不匹配任何用户类的客户端分配给该范围的地址。如果不配置公共地址范围，则不匹配任何用户类的客户端将无法获取到 IP 地址。

如果不需要对客户端进行分类，而仅需要限制网段内可分配的动态地址范围，则可以只配置公共地址范围，而不配置用户类的地址范围。

### 2. 配置限制和指导

配置为客户端分配的 IP 地址时，需要注意：

- 在同一个 DHCP 地址池中，如果多次执行 **network** 或 **address range** 命令，新的配置会覆盖已有配置；如果多次执行 **class** 命令，则可以为多个用户类指定不同的地址范围；多次执行 **forbidden-ip** 命令，可以配置多个不参与自动分配的 IP 地址。
- 在 DHCP 地址池视图下通过 **forbidden-ip** 命令配置不参与自动分配的 IP 地址后，只有当前的地址池不能分配这些 IP 地址，其他地址池仍然可以分配这些 IP 地址；通过 **dhcp server forbidden-ip** 命令指定不参与自动分配的 IP 地址后，所有地址池都不能分配这些 IP 地址。
- 当用户配置 **class range** 命令修改已存在的为 DHCP 用户类动态分配的 IP 地址范围，且新的 IP 地址范围包括之前 IP 地址范围中已分配的地址租约时，如果 DHCP 服务器收到该地址租约的续约需求，DHCP 服务器会给该 DHCP 客户端分配新的 IP 地址租约，已分配的地址租约会继续老化等待超期释放。如果需要已分配的地址租约立即释放，则需配置 **reset dhcp server ip-in-use** 命令进行清除地址租约操作。

### 3. 配置步骤

- (1) 进入系统视图。  
**system-view**
- (2) 进入 DHCP 地址池视图。  
**dhcp server ip-pool** pool-name
- (3) 配置 DHCP 地址池动态分配的主网段。  
**network** network-address [ mask-length | **mask** mask ]

缺省情况下，未配置主网段。

- (4) (可选) 配置地址池动态分配的 IP 地址范围，即公共地址范围。

**address range** *start-ip-address end-ip-address*

缺省情况下，未配置动态分配的 IP 地址范围。

- (5) (可选) 配置 DHCP 地址池为指定 DHCP 用户类动态分配的 IP 地址范围。

**class** *class-name range start-ip-address end-ip-address*

缺省情况下，未配置为指定 DHCP 用户类动态分配的 IP 地址范围。

**class** 命令中指定的 DHCP 用户类，必须通过 **dhcp class** 命令创建。否则，无法为该用户类分配指定范围的地址。

- (6) (可选) 配置动态分配的 IP 地址的租约有效期限。

**expired** { **day** *day* [ **hour** *hour* [ **minute** *minute* [ **second** *second* ] ] ] | **unlimited** }

缺省情况下，IP 地址租约有效期限为 1 天。

- (7) (可选) 配置 DHCP 地址池中不参与自动分配的 IP 地址。

**forbidden-ip** *ip-address*&<1-8>

缺省情况下，DHCP 地址池中的所有 IP 地址都参与自动分配。

- (8) (可选) 在系统视图配置全局不参与自动分配的 IP 地址。

- a. 退回系统视图。

**quit**

- b. 配置全局不参与自动分配的 IP 地址。

**dhcp server forbidden-ip** *start-ip-address* [ *end-ip-address* ]

缺省情况下，除 DHCP 服务器接口的 IP 地址外，DHCP 地址池中的所有 IP 地址都参与自动分配。

## 2.5.4 配置一个主网段多个从网段的动态地址管理方式

### 1. 功能简介

在配置了一个主网段和多个从网段的地址池中，从网段的作用是对主网段地址空间的补充。当主网段中没有空闲地址分配给客户端时，服务器会从该地址池中的从网段获取地址分配给客户端。

### 2. 配置限制和指导

在 DHCP 地址池视图下通过 **forbidden-ip** 命令配置不参与自动分配的 IP 地址后，只有当前的地址池不能分配这些 IP 地址，其他地址池仍然可以分配这些 IP 地址；通过 **dhcp server forbidden-ip** 命令指定不参与自动分配的 IP 地址后，所有地址池都不能分配这些 IP 地址。

### 3. 在地址池中配置一个主网段和多个从网段

- (1) 进入系统视图。

**system-view**

- (2) 进入 DHCP 地址池视图。

**dhcp server ip-pool** *pool-name*

- (3) 配置 DHCP 地址池动态分配的主网段。

```
network network-address [ mask-length | mask mask ]
```

缺省情况下，未配置主网段。

每个 DHCP 地址池中只能配置一个主网段，如果多次执行 **network** 命令配置主网段，则新的配置会覆盖已有配置。

- (4) （可选）配置 DHCP 地址池动态分配的从网段。

```
network network-address [ mask-length | mask mask ] secondary
```

缺省情况下，未配置从网段。

每个 DHCP 地址池中，最多可以配置 32 个从网段。

- (5) （可选）退回地址池视图。

```
quit
```

#### 4. 在地址池中配置动态分配的IP地址的租约有效期限

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 DHCP 地址池视图。

```
dhcp server ip-pool pool-name
```

- (3) 配置动态分配的 IP 地址的租约有效期限。

```
expired { day day [ hour hour [ minute minute [ second second ] ] ] |  
unlimited }
```

缺省情况下，IP 地址租约有效期限为 1 天。

#### 5. 配置不参与自动分配的地址

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 DHCP 地址池视图。

```
dhcp server ip-pool pool-name
```

- (3) 配置 DHCP 地址池中不参与自动分配的 IP 地址。

```
forbidden-ip ip-address&<1-8>
```

缺省情况下，DHCP 地址池中的所有 IP 地址都参与自动分配。

多次执行 **forbidden-ip** 命令，可以配置多个不参与自动分配的 IP 地址段。

- (4) （可选）在系统视图下配置全局不参与自动分配的 IP 地址。

- a. 退回系统视图。

```
quit
```

- b. 配置全局不参与自动分配的 IP 地址。

```
dhcp server forbidden-ip start-ip-address [ end-ip-address ]
```

缺省情况下，除 DHCP 服务器接口的 IP 地址外，DHCP 地址池中的所有 IP 地址都参与自动分配。

多次执行 **dhcp server forbidden-ip** 命令，可以配置多个不参与自动分配的 IP 地址段。



## 2.5.5 配置静态地址绑定

### 1. 功能简介

某些客户端（如 Web 服务器等）需要固定的 IP 地址，通过以下几种方式可以实现为特定的客户端分配特定的 IP 地址：

- 将客户端的硬件地址与 IP 地址绑定：当具有此 MAC 地址的客户端申请 IP 地址时，DHCP 服务器将根据客户端的 MAC 地址查找到对应的 IP 地址，并分配给客户端。
- 将客户端 ID 与 IP 地址绑定：某些客户端在向 DHCP 服务器发送 DHCP-DISCOVER 报文申请 IP 地址时，会构建客户端 ID 并添加到报文中一起发送。如果在 DHCP 服务器上将客户端 ID 与 IP 地址绑定，则当该客户端申请 IP 地址时，DHCP 服务器将根据客户端 ID 查找到对应的 IP 地址并分配给客户端。

### 2. 配置限制和指导

- 静态绑定的 IP 地址不能是 DHCP 服务器的接口 IP 地址，否则会导致 IP 地址冲突，被绑定的客户端将无法正常工作获取到 IP 地址。
- 如果作为 DHCP 客户端的设备，接口的 MAC 地址相同，则为了区分不同接口，采用静态绑定方式进行地址分配时，需要在服务器上配置静态绑定的客户端 ID，而不能配置静态绑定的客户端 MAC 地址，否则可能导致客户端无法成功获取 IP 地址。

### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 DHCP 地址池视图。

```
dhcp server ip-pool pool-name
```

- (3) 配置静态地址绑定。

```
static-bind ip-address ip-address [ mask-length | mask mask ]  
{ client-identifier client-identifier | hardware-address  
hardware-address [ ethernet | token-ring ] }
```

缺省情况下，未配置静态地址绑定。

同一地址只能绑定给一个客户端。不允许通过重复执行 **static-bind ip-address** 命令的方式修改 IP 地址与客户端的绑定关系。只有删除了某个地址的绑定关系，才能将该地址与其他客户端绑定。

- (4) （可选）配置静态绑定 IP 地址的租约有效期限。

```
expired { day day [ hour hour [ minute minute [ second second ] ] ] |  
unlimited }
```

缺省情况下，IP 地址租约有效期限为 1 天。

## 2.5.6 配置DHCP客户端使用的网关地址

### 1. 功能简介

DHCP 客户端访问本网段以外的服务器或主机时，数据必须通过网关进行转发。DHCP 服务器可以为客户端指定网关的地址。



## 2. 配置限制和指导

- 在 DHCP 服务器上，可以为每个地址池分别指定客户端对应的网关地址。目前，每个 DHCP 地址池视图下、每个从网段视图下最多可以配置 64 个网关地址。
- DHCP 地址池视图下执行 **gateway-list** 命令，配置的是为地址池中所有 DHCP 客户端分配的网关地址。如果用户需要为地址池下某个从网段的 DHCP 客户端分配其它的网关地址，可以在地址池的从网段视图下执行 **gateway-list** 命令。如果在地址池视图和从网段视图下都配置了网关地址，则优先将从网段视图下配置的网关地址分配给从网段的 DHCP 客户端。

## 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 DHCP 地址池视图。

```
dhcp server ip-pool pool-name
```

- (3) 配置为 DHCP 客户端分配的网关地址。

```
gateway-list ip-address&<1-64>
```

缺省情况下，未配置为 DHCP 客户端分配的网关地址。

- (4) （可选）在从网段视图中配置为 DHCP 客户端分配的网关地址。

- a. 进入从网段视图。

```
network network-address [ mask-length | mask mask ] secondary
```

- b. 配置为 DHCP 客户端分配的网关地址。

```
gateway-list ip-address&<1-64>
```

缺省情况下，未配置为 DHCP 客户端分配的网关地址。

## 2.5.7 配置DHCP客户端使用的域名后缀

### 1. 功能简介

在 DHCP 服务器上，可以为每个地址池指定客户端使用的域名后缀。

在客户端进行域名解析时，用户只需要输入域名的部分字段，客户端会自动将输入的域名加上从 DHCP 服务器获得的域名后缀进行解析。有关域名后缀的详细介绍，请参见“三层技术-IP 业务配置指导”中的“域名解析”。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 DHCP 地址池视图。

```
dhcp server ip-pool pool-name
```

- (3) 配置为 DHCP 客户端分配的域名后缀。

```
domain-name domain-name
```

缺省情况下，未配置为 DHCP 客户端分配的域名后缀。

## 2.5.8 配置DHCP客户端使用的DNS服务器地址

### 1. 功能简介

为了使 DHCP 客户端能够通过域名访问 Internet 上的主机，DHCP 服务器应在为客户端指定 DNS（Domain Name System，域名系统）服务器地址。目前，每个 DHCP 地址池视图下最多可以配置 8 个 DNS 服务器地址。

### 2. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 进入 DHCP 地址池视图。

```
dhcp server ip-pool pool-name
```

(3) 配置为 DHCP 客户端分配的 DNS 服务器地址。

```
dns-list ip-address&<1-8>
```

缺省情况下，未配置为 DHCP 客户端分配的 DNS 服务器地址。

## 2.5.9 配置DHCP客户端使用的WINS服务器地址和NetBIOS节点类型

### 1. 功能简介

对于使用 Microsoft Windows 操作系统的客户端，由 WINS（Windows Internet Naming Service，Windows Internet 名称服务）服务器为通过 NetBIOS 协议通信的主机提供主机名到 IP 地址的解析。所以，大部分 Windows 网络客户端需要进行 WINS 的设置。

为了使 DHCP 客户端实现主机名到 IP 地址的解析，DHCP 服务器应该为客户端指定 WINS 服务器地址。

DHCP 客户端在网络上使用 NetBIOS 协议通信时，需要在主机名和 IP 地址之间建立映射关系。根据获取映射关系方式的不同，NetBIOS 节点分为四种：

- **b 类节点（b-node）**：“b”代表广播（broadcast），即此类节点采用广播方式获取映射关系。源节点通过发送带有目的节点主机名的广播报文来获取目的节点的 IP 地址，目的节点收到广播报文后，就将自己的 IP 地址返回给源节点。
- **p 类节点（p-node）**：“p”代表端到端（peer-to-peer），即此类节点采用发送单播报文与 WINS 服务器通信的方式获取映射关系。源节点给 WINS 服务器发送单播报文，WINS 服务器收到单播报文后，返回源节点请求的目的节点名所对应的 IP 地址。
- **m 类节点（m-node）**：“m”代表混合（mixed），是具有部分广播特性的 p 类节点。即此类节点首先发送广播报文来获取映射关系，如果没有获取到，则再发送单播报文与 WINS 服务器通信来获取映射关系。
- **h 类节点（h-node）**：“h”代表混合（hybrid），是具备“端到端”通信机制的 b 类节点。即此类节点首先发送单播报文与 WINS 服务器通信来获取映射关系，如果没有获取到，再发送广播报文来获取映射关系。

### 2. 配置步骤

(1) 进入系统视图。

```
system-view
```

- (2) 进入 DHCP 地址池视图。

```
dhcp server ip-pool pool-name
```

- (3) 配置为 DHCP 客户端分配的 WINS 服务器地址。

```
nbns-list ip-address&<1-8>
```

缺省情况下，未配置为 DHCP 客户端分配的 WINS 服务器地址。

对于 b 类节点，为可选；其他情况下，为必选。每个 DHCP 地址池视图下最多可以配置 8 个 WINS 服务器地址。

- (4) 配置为 DHCP 客户端分配的 NetBIOS 节点类型。

```
netbios-type { b-node | h-node | m-node | p-node }
```

缺省情况下，未配置为 DHCP 客户端分配的 NetBIOS 节点类型。

## 2.5.10 配置DHCP客户端使用的BIMS服务器信息

### 1. 功能简介

为了使 DHCP 客户端通过 BIMS（Branch Intelligent Management System，分支网点智能管理系统）服务器进行软件的备份和升级等操作，DHCP 服务器需要将 BIMS 服务器的 IP 地址、端口号以及加密的共享密钥等信息发给 DHCP 客户端。之后，DHCP 客户端就可以定期向 BIMS 服务器发送连接请求，从 BIMS 服务器上获取配置文件，进行软件的备份和升级等操作。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 DHCP 地址池视图。

```
dhcp server ip-pool pool-name
```

- (3) 配置为 DHCP 客户端分配的 BIMS 服务器的 IP 地址、端口及共享密钥信息。

```
bims-server ip ip-address [ port port-number ] sharekey { cipher | simple } string
```

缺省情况下，未配置为 DHCP 客户端分配的 BIMS 服务器信息。

## 2.5.11 配置DHCP客户端使用的远程启动文件信息

### 1. 功能简介

服务器自动配置功能在空配置启动的设备上不需要进行任何配置，但需要在 DHCP 服务器上配置一些必需的参数，包括 TFTP 服务器地址、TFTP 服务器名和启动文件名或远程启动文件的 HTTP 形式 URL 等。

### 2. 配置DHCP客户端使用的TFTP服务器地址及启动文件名

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 DHCP 地址池视图。

```
dhcp server ip-pool pool-name
```

- (3) 配置 DHCP 客户端使用的 TFTP 服务器信息。请选择其中至少一项进行配置。

- 配置 DHCP 客户端使用的 TFTP 服务器地址。

**tftp-server ip-address** *ip-address*

缺省情况下，未配置 DHCP 客户端使用的 TFTP 服务器地址。

- 配置 DHCP 客户端使用的 TFTP 服务器名。

**tftp-server domain-name** *domain-name*

缺省情况下，未配置 DHCP 客户端使用的 TFTP 服务器名。

- (4) 配置 DHCP 客户端使用的启动文件名。

**bootfile-name** *bootfile-name*

缺省情况下，未配置 DHCP 客户端使用的启动文件名。

### 3. 配置DHCP客户端使用的远程启动文件的HTTP形式URL

- (1) 进入系统视图。

**system-view**

- (2) 进入 DHCP 地址池视图。

**dhcp server ip-pool** *pool-name*

- (3) 配置 DHCP 客户端使用的远程启动文件的 HTTP 形式 URL。

**bootfile-name** *url*

缺省情况下，未配置 DHCP 客户端使用的远程启动文件的 HTTP 形式 URL。

## 2.5.12 配置DHCP客户端使用的下一个提供服务的服务器IP地址

### 1. 功能简介

设备在启动后，可能需要访问某些服务器获取设备运行需要的信息，例如从 TFTP 服务器上获取配置文件。通过本配置可以指定 DHCP 服务器为 DHCP 客户端分配的下一个提供服务的服务器 IP 地址，以便客户端启动后访问该服务器，获取必要的信息。

### 2. 配置步骤

- (1) 进入系统视图。

**system-view**

- (2) 进入 DHCP 地址池视图。

**dhcp server ip-pool** *pool-name*

- (3) 配置 DHCP 地址池为 DHCP 客户端分配的下一个提供服务的服务器 IP 地址。

**next-server** *ip-address*

缺省情况下，未配置 DHCP 地址池为 DHCP 客户端分配的下一个提供服务的服务器 IP 地址。

## 2.5.13 配置DHCP客户端使用的Option 184 参数

### 1. 功能简介

为了使具有语音功能的DHCP客户端能够在通过DHCP获取IP地址的同时，获取到语音呼叫所需的相关信息，需要在DHCP服务器上配置Option 184。Option 184 内容的详细介绍，请参见“[1.6.3 Option 184](#)”。

2. 配置步骤

- (1)

进入系统视图。  
**system-view**
- (2)

进入 DHCP 地址池视图。  
**dhcp server ip-pool pool-name**
- (3)

配置网络呼叫处理器的地址。  
**voice-config ncp-ip ip-address**  
缺省情况下，未配置网络呼叫处理器的地址。  
只有配置了网络呼叫处理器的地址，其他配置才能生效。
- (4)

（可选）配置备用服务器的地址。  
**voice-config as-ip ip-address**  
缺省情况下，未配置备用服务器的地址。
- (5)

（可选）配置语音 VLAN。  
**voice-config voice-vlan vlan-id { disable | enable }**  
缺省情况下，未配置语音 VLAN。
- (6)

（可选）配置自动故障转移呼叫路由。  
**voice-config fail-over ip-address dialer-string**  
缺省情况下，未配置自动故障转移呼叫路由。

2.5.14 自定义DHCP选项

1. 自定义DHCP选项应用场景

本配置为 DHCP 服务器提供了灵活的选项配置方式，使得 DHCP 服务器可以为 DHCP 客户端提供更加丰富的选项内容。在以下情况下，可以使用本命令自定义 DHCP 选项：

- 随着 DHCP 的不断发展，新的 DHCP 选项会陆续出现。通过自定义 DHCP 选项，可以方便地添加新的 DHCP 选项。
- 有些选项的内容，RFC 中没有统一规定。厂商可以根据需要定义选项的内容，如 Option 43。通过自定义 DHCP 选项，可以为 DHCP 客户端提供厂商指定的信息。
- 设备上只提供了有限的选项配置命令（如 **gateway-list**、**dns-list** 命令），对于没有专门命令来配置的 DHCP 选项，可以通过 **option** 命令配置选项内容。例如，可以通过 **option 4 ip-address 1.1.1.1** 命令指定为 DHCP 客户端分配的时间服务器地址为 1.1.1.1。
- 扩展已有的 DHCP 选项。当前已提供的方式无法满足用户需求时（比如通过 **dns-list** 命令最多只能配置 8 个 DNS 服务器地址，如果用户需要配置的 DNS 服务器地址数目大于 8，则该命令无法满足需求），可以通过自定义 DHCP 选项的方式进行扩展。

2. 常用Option选项

[表 2-1](#) 中列出了常用的DHCP选项名称、对应的配置命令和推荐的Option命令参数信息。

表2-1 常用 Option 选项信息

选项编号	选项名称	对应的配置命令	推荐的 option 命令参数
3	Router Option	<b>gateway-list</b>	<b>ip-address</b>

选项编号	选项名称	对应的配置命令	推荐的 option 命令参数
6	Domain Name Server Option	<b>dns-list</b>	<b>ip-address</b>
15	Domain Name	<b>domain-name</b>	<b>ascii</b>
44	NetBIOS over TCP/IP Name Server Option	<b>nbns-list</b>	<b>ip-address</b>
46	NetBIOS over TCP/IP Node Type Option	<b>netbios-type</b>	<b>hex</b>
66	TFTP server name	<b>tftp-server</b>	<b>ascii</b>
67	Bootfile name	<b>bootfile-name</b>	<b>ascii</b>
43	Vendor Specific Information	-	<b>hex</b>

### 3. 配置限制和指导

- 自定义 DHCP 选项时, 取值的获取比较复杂, 配置错误可能会对 DHCP 的工作过程造成影响, 请谨慎使用该功能。
- 用户可在 DHCP 地址池中自定义选项信息。
- 用户可在 DHCP 选项组中自定义选项信息, 并在 DHCP 地址池中配置 DHCP 用户类和 DHCP 选项组关联, 为 DHCP 客户端分配选项信息。

### 4. 自定义DHCP地址池选项

- 进入系统视图。

```
system-view
```

- 进入 DHCP 地址池视图。

```
dhcp server ip-pool pool-name
```

- 自定义 DHCP 地址池选项。

```
option code { ascii ascii-string | hex hex-string | ip-address  
ip-address&<1-8> }
```

缺省情况下, 未自定义 DHCP 地址池选项。

DHCP 服务器在应答 DHCP 客户端报文时, 如果 DHCP 选项组的选项编号和 DHCP 地址池选项编号相同且匹配用户类时, 以 DHCP 选项组的选项为准。

### 5. 自定义DHCP选项组选项

- 进入系统视图。

```
system-view
```

- 创建 DHCP 选项组, 并进入 DHCP 选项组视图。

```
dhcp option-group option-group-number
```

- 自定义 DHCP 选项组选项。

```
option code { ascii ascii-string | hex hex-string | ip-address  
ip-address&<1-8> }
```

缺省情况下, 未定义 DHCP 选项组的选项。

DHCP 服务器在应答客户端报文时，如果多个 DHCP 选项组的选项编号相同时，以最先匹配的 DHCP 用户类对应的 DHCP 选项组的选项为准。

- (4) 返回系统视图。

```
quit
```

- (5) 进入 DHCP 地址池视图。

```
dhcp server ip-pool pool-name
```

- (6) 配置 DHCP 用户类与 DHCP 选项组的关联。

```
class class-name option-group option-group-number
```

缺省情况下，未配置指定 DHCP 用户类与 DHCP 选项组的关联。

## 2.5.15 配置DHCP用户类白名单功能

### 1. 功能简介

配置 DHCP 用户类白名单功能，DHCP 服务器只有收到属于用户类白名单的 DHCP 客户端发送的请求报文，才会进行处理。

### 2. 配置限制和指导

如果 DHCP 客户端请求的是静态绑定租约，则 DHCP 服务器不进行白名单检查直接进行处理。

### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 DHCP 地址池视图。

```
dhcp server ip-pool pool-name
```

- (3) 开启 DHCP 用户类白名单功能。

```
verify class
```

缺省情况下，DHCP 用户类白名单功能处于关闭状态。

- (4) 配置 DHCP 用户类白名单包括的用户类名。

```
valid class class-name&<1-8>
```

缺省情况下，未配置 DHCP 用户类白名单包括的用户类名。

## 2.6 配置接口引用地址池

### 1. 功能简介

创建地址池，并在接口引用该地址池后，接口接收到 DHCP 请求，将优先为客户端分配静态绑定的 IP 地址；如果不存在静态绑定的 IP 地址，则从引用的地址池中选择 IP 地址分配给客户端。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```



- (3) 配置接口引用地址池。

```
dhcp server apply ip-pool pool-name
```

缺省情况下，接口未引用地址池。

如果接口引用的地址池不存在，将导致无法动态分配地址。

## 2.7 配置DHCP策略动态分配地址和其他参数

### 1. 功能简介

创建 DHCP 策略，并在接口引用该策略后，该接口接收到 DHCP 请求报文时，则根据配置顺序逐个匹配 DHCP 策略中通过 **class ip-pool** 命令指定的 DHCP 用户类。匹配情况如下：

- 若匹配 DHCP 用户类成功，当该 DHCP 用户类关联的 DHCP 地址池中存在可供分配的地址信息时，则从该 DHCP 地址池中分配 IP 地址和其他参数；当该 DHCP 用户类关联的 DHCP 地址池中不存在可供分配的地址信息时，IP 地址和其他参数分配失败。
- 若匹配 DHCP 策略中的所有 DHCP 用户类失败，当配置了默认 DHCP 地址池时，则从该地址池中分配 IP 地址和其他参数；当未配置默认 DHCP 地址池或默认 DHCP 地址池中不存在可供分配的地址信息时，IP 地址和其他参数分配失败。

若接收 DHCP 请求报文的接口引用的 DHCP 策略不存在或匹配的 DHCP 用户类关联的 DHCP 地址池不存在时，IP 地址和其他参数分配失败。

### 2. 配置限制和指导

DHCP 策略需要在接口上引用才生效。

### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建 DHCP 策略，并进入 DHCP 策略视图。

```
dhcp policy policy-name
```

- (3) 指定 DHCP 用户类关联的 DHCP 地址池。

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

缺省情况下，未指定 DHCP 用户类关联的 DHCP 地址池。

- (4) 指定默认 DHCP 地址池。

```
default ip-pool pool-name
```

缺省情况下，未指定默认 DHCP 地址池。

- (5) 退回系统视图。

```
quit
```

- (6) 进入接口视图。

```
interface interface-type interface-number
```

- (7) 指定接口引用的 DHCP 策略。

```
dhcp apply-policy policy-name
```

缺省情况下，接口未引用 DHCP 策略。



## 2.8 开启DHCP服务

### 1. 配置限制和指导

只有开启 DHCP 服务后，其它相关的 DHCP 服务器配置才能生效。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 DHCP 服务。

```
dhcp enable
```

缺省情况下，DHCP 服务处于关闭状态。

## 2.9 配置接口工作在DHCP服务器模式

### 1. 功能简介

配置接口工作在 DHCP 服务器模式后，当接口收到 DHCP 客户端发来的 DHCP 报文时，将从 DHCP 服务器的地址池中分配地址等参数。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置接口工作在 DHCP 服务器模式。

```
dhcp select server
```

缺省情况下，接口工作在 DHCP 服务器模式。

## 2.10 配置IP地址冲突检测功能

### 1. 功能简介

为防止 IP 地址重复分配导致地址冲突，DHCP 服务器为客户端分配地址前，需要先对该地址进行检测。

DHCP 服务器的地址探测是通过 ping 功能实现的，通过检测是否能在指定时间内得到 ping 响应来判断是否存在地址冲突。DHCP 服务器发送目的地址为待分配地址的 ICMP 回显请求报文。如果在指定时间内收到 ICMP 回显响应报文，则认为存在地址冲突。DHCP 服务器从地址池中选择新的 IP 地址，并重复上述操作。如果在指定时间内未收到 ICMP 回显响应报文，则继续发送 ICMP 回显请求报文，直到发送的 ICMP 回显显示报文数目达到最大值。如果仍然未收到 ICMP 回显响应报文，则将地址分配给客户端，从而确保客户端获得的 IP 地址唯一。

DHCP 服务器通过 ping 操作来检测是否发生地址冲突，而 DHCP 客户端则通过发送免费 ARP 报文检测是否发生地址冲突。

## 2. 配置步骤

- (1) 进入系统视图。

**system-view**

- (2) （可选）配置 DHCP 服务器发送 ICMP 回显请求报文的最大数目。

**dhcp server ping packets** *number*

缺省情况下，DHCP 服务器发送 ICMP 回显请求报文的最大数目为 1。

0 表示 DHCP 服务器将 IP 地址分配给 DHCP 客户端之前，不会通过 ping 操作探测该地址是否冲突。

- (3) （可选）配置 DHCP 服务器等待 ICMP 回显响应报文的超时时间。

**dhcp server ping timeout** *milliseconds*

缺省情况下，DHCP 服务器等待 ICMP 回显响应报文的超时时间为 500 毫秒。

0 表示 DHCP 服务器将 IP 地址分配给 DHCP 客户端之前，不会通过 ping 操作探测该地址是否冲突。

## 2.11 配置Option 82的处理方式

### 1. 功能简介

如果配置 DHCP 服务器处理 Option 82，则当 DHCP 服务器收到带有 Option 82 的报文后，会在响应报文中携带 Option 82，并为客户端分配 IP 地址等信息。

如果配置 DHCP 服务器忽略 Option 82，则当 DHCP 服务器收到带有 Option 82 的报文后，不会在响应报文中携带 Option 82，只为客户端分配 IP 地址等信息。

为使Option 82 功能正常使用，需要在DHCP服务器和DHCP中继上都进行相应配置。DHCP中继支持Option 82 功能的相关配置请参见“[3.9 配置DHCP中继支持Option 82 功能](#)”。

### 2. 配置步骤

- (1) 进入系统视图。

**system-view**

- (2) 配置 DHCP 服务器处理 Option 82。

**dhcp server relay information enable**

缺省情况下，DHCP 服务器处理 Option 82。

## 2.12 配置DHCP服务器安全功能

### 2.12.1 配置限制和指导

如果网络中存在DHCP中继，DHCP服务器收到的DHCP请求报文中源MAC地址会被DHCP中继替换。所以这种组网情况下DHCP服务器安全功能不适用，只能开启DHCP中继的安全功能。关于DHCP中继的安全功能的介绍，请参见“[3.7 配置DHCP中继的安全功能](#)”。

## 2.12.2 配置防止DHCP饿死攻击

### 1. 功能简介

DHCP饿死攻击是指攻击者伪造chaddr字段各不相同的DHCP请求报文，向DHCP服务器申请大量的IP地址，导致DHCP服务器地址池中的地址耗尽，无法为合法的DHCP客户端分配IP地址，或导致DHCP服务器消耗过多的系统资源，无法处理正常业务。DHCP报文字段的相关内容请参见“[1.3 DHCP报文格式](#)”。

如果封装 DHCP 请求报文的数据帧的源 MAC 地址各不相同，则通过 **mac-address max-mac-count** 命令限制端口可以学习到的 MAC 地址数，并配置学习到的 MAC 地址数达到最大值时，丢弃源 MAC 地址不在 MAC 地址表里的报文，能够避免攻击者申请过多的 IP 地址，在一定程度上阻止了 DHCP 饿死攻击。此时，不存在 DHCP 饿死攻击的端口下的 DHCP 客户端可以正常获取 IP 地址，但存在 DHCP 饿死攻击的端口下的 DHCP 客户端仍可能无法获取 IP 地址。

如果封装 DHCP 请求报文的数据帧的 MAC 地址都相同，则通过 **mac-address max-mac-count** 命令无法防止 DHCP 饿死攻击。在这种情况下，需要开启 DHCP 服务器的 MAC 地址检查功能。开启该功能后，DHCP 服务器检查接收到的 DHCP 请求报文中的 chaddr 字段和数据帧的源 MAC 地址字段是否一致。如果一致，则认为该报文合法，进行后续处理；如果不一致，则丢弃该报文。**mac-address max-mac-count** 命令的详细介绍，请参见“二层技术-以太网交换”中的“MAC 地址表”。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 开启 DHCP 服务器源 MAC 检查功能。

```
dhcp server check mac-address
```

缺省情况下，DHCP 服务器的 MAC 地址检查功能处于关闭状态。

## 2.13 配置DHCP服务器兼容性

当 DHCP 客户端的行为不符合 RFC 协议规定时，为了与之兼容，需要配置 DHCP 服务器兼容性功能。

### 2.13.1 配置DHCP服务器始终以广播方式回复请求报文

#### 1. 功能简介

一般情况下，只有 DHCP 请求报文的广播标志位为 1 的时候，DHCP 服务器才会以广播的方式发送应答报文。如果 DHCP 客户端发送的请求报文中广播标志位为 0，且该客户端不支持接收单播的应答报文，则可以配置 DHCP 服务器忽略请求报文的广播标志位，始终以广播方式发送应答报文。

当已经存在 IP 地址的客户端发出请求报文（即报文中 ciaddr 字段不为 0）时，无论是否开启 DHCP 服务器的广播回应报文功能，DHCP 服务器都会以单播形式将回应报文发送给 DHCP 客户端（即目的地址为 ciaddr）。

当请求报文通过 DHCP 中继转发到 DHCP 服务器（即报文中 giaddr 字段不为 0）时，无论是否开启 DHCP 服务器的广播回应报文功能，DHCP 服务器都会以单播形式将回应报文发送给 DHCP 中继（即目的地址为 giaddr）。

## 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 DHCP 服务器的广播回应报文功能。

```
dhcp server always-broadcast
```

缺省情况下，DHCP 服务器的广播回应报文功能处于关闭状态。DHCP 服务器根据请求报文中的广播标志位来决定以广播还是单播的形式发送应答报文。

### 2.13.2 配置DHCP服务器忽略BOOTP请求报文

#### 1. 功能简介

BOOTP 客户端申请到的地址租约是无限期的。在某些组网环境中，可能不希望出现无限期的地址租约。此时，可以通过配置 DHCP 服务器忽略 BOOTP 请求报文，避免分配无限期的地址租约。

#### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 DHCP 服务器忽略 BOOTP 请求报文。

```
dhcp server bootp ignore
```

缺省情况下，DHCP 服务器不会忽略 BOOTP 请求报文。

### 2.13.3 配置DHCP服务器以RFC 1048 规定的格式发送BOOTP应答报文

#### 1. 功能简介

有些 BOOTP 客户端发送的请求报文中，vend 字段的格式不符合 RFC 1048 的要求。对于这种报文，DHCP 服务器的缺省处理方法是不解析 vend 字段内容，将报文中 vend 字段的内容拷贝到回复报文中的 vend 字段回应给 BOOTP 客户端。

开启 DHCP 服务器的回应 RFC 1048 格式报文功能后，对于这种格式不符合 RFC 1048 要求的报文，DHCP 服务器会将需要回应的选项以符合 RFC 1048 要求的格式，封装到回复报文的 vend 字段，并回应给 BOOTP 客户端。

#### 2. 配置限制和指导

本配置只在客户端通过 BOOTP 报文申请静态绑定地址时有效。

#### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 DHCP 服务器回应 RFC 1048 格式报文功能。

```
dhcp server bootp reply-rfc-1048
```

缺省情况下，DHCP 服务器回应 RFC 1048 格式报文功能处于关闭状态。

## 2.14 配置DHCP服务器发送DHCP报文的DSCP优先级

### 1. 功能简介

DSCP 优先级用来体现报文自身的优先等级，决定报文传输的优先程度。通过本配置可以指定 DHCP 服务器发送的 DHCP 报文的 DSCP 优先级。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 DHCP 服务器发送 DHCP 报文的 DSCP 优先级。

```
dhcp dscp dscp-value
```

缺省情况下，DHCP 服务器发送 DHCP 报文的 DSCP 优先级为 56。

## 2.15 配置DHCP服务器租约固化功能

### 1. 功能简介

DHCP 服务器重启后，设备上记录的租约信息将丢失，会影响 DHCP 服务器的正常业务。

DHCP 服务器租约固化功能将 DHCP 服务器的在用地址租约和冲突表项保存到指定的文件中，DHCP 服务器设备重启后，自动根据该文件恢复 DHCP 服务器的租约信息，从而保证 DHCP 服务器的租约信息不会丢失。

当 DHCP 服务器设备重启后，自动根据该文件恢复 DHCP 服务器的租约信息，租约恢复的过程中，DHCP 服务器不能提供 DHCP 业务。所以当恢复过程出现问题导致恢复过程无法结束时，用户可配置 **dhcp server database update stop** 命令终止当前的 DHCP 服务器表项恢复操作，以便 DHCP 服务器能及时提供 DHCP 服务。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 指定存储 DHCP 服务器表项的文件名称。

```
dhcp server database filename { filename | url url [ username username  
[ password { cipher | simple } string ] ] }
```

缺省情况下，未指定存储 DHCP 服务器表项的文件名称。

执行本命令后，会立即触发一次表项备份。

- (3) （可选）将当前的 DHCP 服务器表项保存到用户指定的文件中。

```
dhcp server database update now
```

本命令只用来触发一次 DHCP 服务器表项的备份。

- (4) （可选）配置刷新 DHCP 服务器表项存储文件的延迟时间。

```
dhcp server database update interval interval
```

缺省情况下，若 DHCP 服务器表项不变化，则不刷新存储文件；若 DHCP 服务器表项发生变化，默认在 300 秒之后刷新存储文件。

- (5) （可选）终止当前的 DHCP 服务器表项恢复操作。

**dhcp server database update stop**

本命令只用来触发一次终止 DHCP 服务器表项信息的恢复。

## 2.16 开启DHCP服务器的用户下线探测功能

### 1. 功能简介

DHCP 服务器的用户下线探测功能以 ARP 表项老化功能为基础，当 ARP 表项老化时认为该表项对应的用户已下线。

如果在接口上开启了 DHCP 服务器的用户下线探测功能，则当 ARP 表项老化时，系统会删除该表项对应用户的地址绑定信息。

### 2. 配置限制和指导

手工删除 ARP 表项，不会触发 DHCP 服务器删除对应用户的地址绑定信息。

### 3. 配置步骤

- (1) 进入系统视图。

**system-view**

- (2) 进入接口视图。

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

- (3) 开启 DHCP 服务器的用户下线探测功能。

**dhcp client-detect**

缺省情况下，DHCP 服务器的用户下线探测功能处于关闭状态。

## 2.17 配置DHCP告警功能

### 1. 功能简介

为了避免地址池地址耗尽，导致用户无法上线，用户可以设置地址池使用率的告警阈值，当地址池中地址使用率超过阈值时，系统发送告警信息到设备的信息中心，通过设置信息中心的告警信息的发送参数，最终决定日志报文的输出规则（即是否允许输出以及输出方向），提醒管理员进行地址池合理规划。有关信息中心参数的配置，请参见“网络管理和监控配置指导”中的“信息中心”。

### 2. 配置步骤

- (1) 进入系统视图。

**system-view**

- (2) 进入 DHCP 地址池视图。

**dhcp server ip-pool** *pool-name*

- (3) （可选）设置地址池使用率告警门限阈值。

**ip-in-use threshold** *threshold-value*

缺省情况下，地址池使用率告警门限阈值为 100%。

## 2.18 开启DHCP服务器日志信息功能

### 1. 功能简介

DHCP 服务器日志可以方便管理员定位问题和解决问题。设备生成 DHCP 日志信息会交给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

### 2. 配置限制和指导

比如大量 DHCP 客户端发生上下线操作时，DHCP 服务器会输出大量日志信息，这可能会降低设备性能，影响 DHCP 服务器分配 IP 地址的速度。为了避免该情况的发生，用户可以关闭 DHCP 服务器日志信息功能，使得 DHCP 服务器不再输出日志信息。

### 3. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 开启 DHCP 服务器日志信息功能。

```
dhcp log enable
```

缺省情况下，DHCP 服务器日志信息功能处于关闭状态。

## 2.19 DHCP服务器显示和维护



提示

DHCP 服务器重启或使用 **reset dhcp server ip-in-use** 命令清除租约后，DHCP 服务器上不存在租约信息。此时客户端如果发出续约请求将会被拒绝，客户端需要重新申请 IP 地址。

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 DHCP 服务器的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令清除 DHCP 服务器的相关信息。

表2-2 DHCP 服务器显示和维护

操作	命令
显示DHCP的地址冲突信息	<b>display dhcp server conflict</b> [ ip ip-address ]
显示DHCP服务器的表项备份信息	<b>display dhcp server database</b>
显示租约过期的地址绑定信息	<b>display dhcp server expired</b> [ ip ip-address   pool pool-name ]
显示DHCP地址池的空闲地址信息	<b>display dhcp server free-ip</b> [ pool pool-name ]
显示DHCP地址绑定信息	<b>display dhcp server ip-in-use</b> [ ip ip-address   pool pool-name ]
显示DHCP地址池的信息	<b>display dhcp server pool</b> [ pool-name ]
显示DHCP服务器的统计信息	<b>display dhcp server statistics</b> [ pool pool-name ]



操作	命令
清除DHCP的地址冲突信息	<code>reset dhcp server conflict [ ip ip-address ]</code>
清除租约过期的地址绑定信息	<code>reset dhcp server expired [ ip ip-address   pool pool-name ]</code>
清除DHCP的正式绑定和临时绑定信息	<code>reset dhcp server ip-in-use [ ip ip-address   pool pool-name ]</code>
清除DHCP服务器的统计信息	<code>reset dhcp server statistics</code>

## 2.20 DHCP服务器典型配置举例

### 2.20.1 静态绑定地址配置举例

#### 1. 组网需求

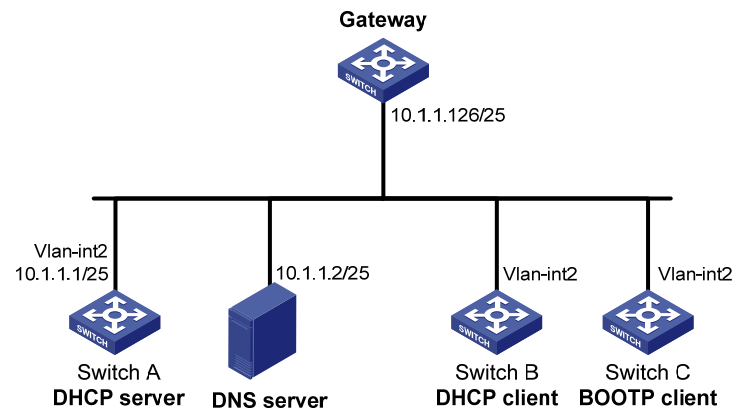
Switch B 和 Switch C 分别作为 DHCP 客户端和 BOOTP 客户端，从 DHCP 服务器 Switch A 获取静态绑定的 IP 地址、域名服务器、网关地址等信息。

其中：

- Switch B 上 VLAN 接口 2 的客户端 ID 为：  
0030-3030-662e-6532-3030-2e30-3030-322d-4574-6865-726e-6574；
- Switch C 上 VLAN 接口 2 的 MAC 地址为：000f-e200-01c0。

#### 2. 组网图

图2-1 静态绑定地址组网图



#### 3. 配置步骤

##### (1) 配置接口的 IP 地址

```

<SwitchA> system-view
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 10.1.1.1 25
[SwitchA-Vlan-interface2] quit

```

##### (2) 配置 DHCP 服务

```

# 创建 DHCP 地址池 0。

```



```
[SwitchA] dhcp server ip-pool 0
# 配置采用静态绑定方式为 Switch B 分配 IP 地址。
[SwitchA-dhcp-pool-0] static-bind ip-address 10.1.1.5 25 client-identifier
0030-3030-662e-6532-3030-2e30-3030-322d-4574-6865-726e-6574
# 配置采用静态绑定方式为 Switch C 分配 IP 地址。
[SwitchA-dhcp-pool-0] static-bind ip-address 10.1.1.6 25 hardware-address
000f-e200-01c0
# 配置域名服务器、网关地址。
[SwitchA-dhcp-pool-0] dns-list 10.1.1.2
[SwitchA-dhcp-pool-0] gateway-list 10.1.1.126
[SwitchA-dhcp-pool-0] quit
# 开启 DHCP 服务。
[SwitchA] dhcp enable
# 配置 VLAN 接口 2 工作在 DHCP 服务器模式。
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] dhcp select server
[SwitchA-Vlan-interface2] quit
```

#### 4. 验证配置

配置完成后，Switch B 和 Switch C 可以从 DHCP 服务器 Switch A 分别申请到 IP 地址 10.1.1.5 和 10.1.1.6，并获取相关网络配置参数。通过 **display dhcp server ip-in-use** 命令可以查看 DHCP 服务器为客户端分配的 IP 地址。

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

IP address	Client identifier/ Hardware address	Lease expiration	Type
10.1.1.5	0030-3030-662e-6532-3030-2e30-3030-322d-4574-6865-726e-6574	Jan 21 14:27:27 2014	Static(C)
10.1.1.6	000f-e200-01c0	Unlimited	Static(C)

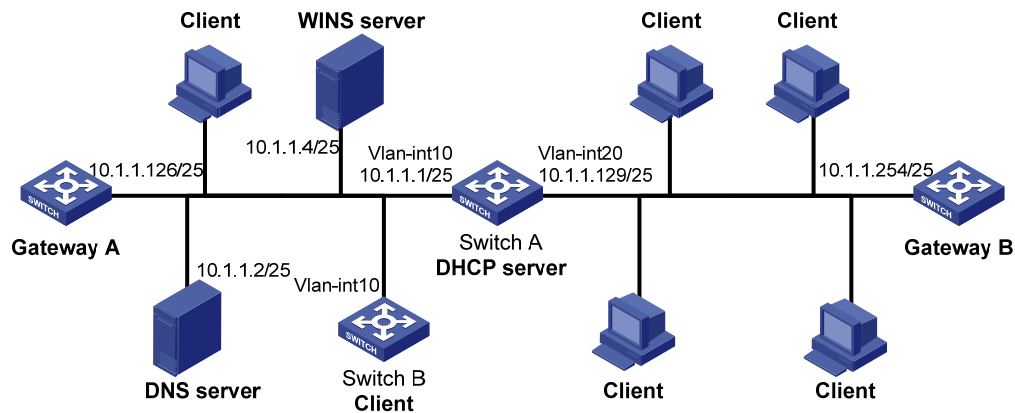
## 2.20.2 动态分配地址配置举例

### 1. 组网需求

- 作为 DHCP 服务器的 Switch A 为网段 10.1.1.0/24 中的客户端动态分配 IP 地址，该地址池网段分为两个子网网段：10.1.1.0/25 和 10.1.1.128/25；
- Switch A 的两个 VLAN 接口，VLAN 接口 10 和 VLAN 接口 20 的地址分别为 10.1.1.1/25 和 10.1.1.129/25；
- 10.1.1.0/25 网段内的地址租用期限为 10 天 12 小时，域名后缀为 aabbcc.com，DNS 服务器地址为 10.1.1.2/25，WINS 服务器地址为 10.1.1.4/25，网关的地址为 10.1.1.126/25；
- 10.1.1.128/25 网段内的地址租用期限为 5 天，域名后缀为 aabbcc.com，DNS 服务器地址为 10.1.1.2/25，无 WINS 服务器地址，网关的地址为 10.1.1.254/25。

## 2. 组网图

图2-2 DHCP 组网图



## 3. 配置步骤

- (1) 配置端口属于 VLAN 及对应 VLAN 接口的 IP 地址（略）
- (2) 配置 DHCP 服务

# 配置不参与自动分配的 IP 地址（DNS 服务器、WINS 服务器和网关地址）。

```
<SwitchA> system-view
[SwitchA] dhcp server forbidden-ip 10.1.1.2
[SwitchA] dhcp server forbidden-ip 10.1.1.4
[SwitchA] dhcp server forbidden-ip 10.1.1.126
[SwitchA] dhcp server forbidden-ip 10.1.1.254
```

# 配置 DHCP 地址池 1，用来为 10.1.1.0/25 网段内的客户端分配 IP 地址和网络配置参数。

```
[SwitchA] dhcp server ip-pool 1
[SwitchA-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.128
[SwitchA-dhcp-pool-1] expired day 10 hour 12
[SwitchA-dhcp-pool-1] domain-name aabbcc.com
[SwitchA-dhcp-pool-1] dns-list 10.1.1.2
[SwitchA-dhcp-pool-1] gateway-list 10.1.1.126
[SwitchA-dhcp-pool-1] nbns-list 10.1.1.4
[SwitchA-dhcp-pool-1] quit
```

# 配置 DHCP 地址池 2，用来为 10.1.1.128/25 网段内的客户端分配 IP 地址和网络配置参数。

```
[SwitchA] dhcp server ip-pool 2
[SwitchA-dhcp-pool-2] network 10.1.1.128 mask 255.255.255.128
[SwitchA-dhcp-pool-2] expired day 5
[SwitchA-dhcp-pool-2] domain-name aabbcc.com
[SwitchA-dhcp-pool-2] dns-list 10.1.1.2
[SwitchA-dhcp-pool-2] gateway-list 10.1.1.254
[SwitchA-dhcp-pool-2] quit
```

# 开启 DHCP 服务。

```
[SwitchA] dhcp enable
```

# 配置 VLAN 接口 10 和 VLAN 接口 20 工作在 DHCP 服务器模式。

```
[SwitchA] interface vlan-interface 10
```

```
[SwitchA-Vlan-interface10] dhcp select server
[SwitchA-Vlan-interface10] quit
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] dhcp select server
[SwitchA-Vlan-interface20] quit
```

#### 4. 验证配置

配置完成后，10.1.1.0/25 和 10.1.1.128/25 网段的客户端可以从 DHCP 服务器 Switch A 申请到相应网段的 IP 地址和网络配置参数。通过 **display dhcp server ip-in-use** 命令可以查看 DHCP 服务器为客户端分配的 IP 地址。

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

IP address	Client identifier/ Hardware address	Lease expiration	Type
10.1.1.3	0031-3865-392e-6262-3363-2e30-3230-352d-4745-302f-30	Jan 14 22:25:03 2015	Auto(C)
10.1.1.5	0031-fe65-4203-7e02-3063-5b30-3230-4702-620e-712f-5e	Jan 14 22:25:03 2015	Auto(C)
10.1.1.130	3030-3030-2e30-3030-662e-3030-3033-2d45-7568-6572-1e	Jan 9 10:45:11 2015	Auto(C)
10.1.1.131	3030-0020-fe02-3020-7052-0201-2013-1e02-0201-9068-23	Jan 9 10:45:11 2015	Auto(C)
10.1.1.132	2020-1220-1102-3021-7e52-0211-2025-3402-0201-9068-9a	Jan 9 10:45:11 2015	Auto(C)
10.1.1.133	2021-d012-0202-4221-8852-0203-2022-55e0-3921-0104-31	Jan 9 10:45:11 2015	Auto(C)

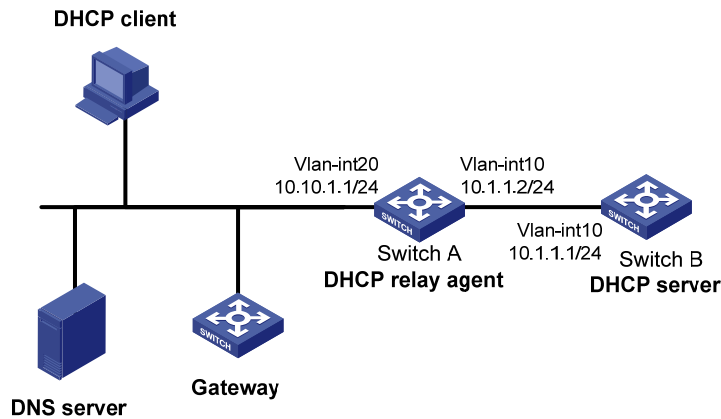
### 2.20.3 按用户类分配地址配置举例

#### 1. 组网需求

- Switch A 作为 DHCP 中继转发 DHCP 报文。在 Switch A 上配置 DHCP 中继支持 Option 82 功能，使得 Switch A 能够为 DHCP 客户端发送的请求报文添加 Option 82。
- Switch B 作为 DHCP 服务器为客户端分配 IP 地址和其他网络配置参数。如果 Switch B 接收到的请求报文中带有 Option 82，则为该客户端分配地址范围 10.10.1.2 到 10.10.1.10 内的 IP 地址。如果 Router B 接收到的请求报文匹配硬件地址 aabb-aabb-aab0，硬件地址掩码为 ffff-ffff-fff0，则为该客户端分配地址范围 10.10.1.11 到 10.10.1.26 内的 IP 地址。
- Switch B 为 10.10.1.0/24 网段内的客户端分配的 DNS 服务器地址为 10.10.1.20/24，网关的地址为 10.10.1.254/24。

## 2. 组网图

图2-3 按 DHCP 用户类分配地址组网图



## 3. 配置步骤

- (1) 配置 DHCP server 和 DHCP relay agent 各个接口的 IP 地址（略）
- (2) 配置 DHCP 服务

# 创建 DHCP 用户类 tt，设置匹配规则编号为 1，匹配请求报文中带有 Option 82 的客户端。

```
<SwitchB> system-view
[SwitchB] dhcp class tt
[SwitchB-dhcp-class-tt] if-match rule 1 option 82
[SwitchB-dhcp-class-tt] quit
```

# 创建 DHCP 用户类 ss，设置匹配规则编号 1，匹配硬件地址 aabb-aabb-aab0，硬件地址掩码 ffff-ffff-fff0 的请求报文。

```
[SwitchB] dhcp class ss
[SwitchB-dhcp-class-ss] if-match rule 1 hardware-address aabb-aabb-aab0 mask
ffff-ffff-fff0
[SwitchB-dhcp-class-ss] quit
```

# 创建 DHCP 地址池 aa，配置地址范围和用户类 tt 的地址范围，配置网关和 DNS 服务器的地址。

```
[SwitchB] dhcp server ip-pool aa
[SwitchB-dhcp-pool-aa] network 10.10.1.0 mask 255.255.255.0
[SwitchB-dhcp-pool-aa] address range 10.10.1.2 10.10.1.100
[SwitchB-dhcp-pool-aa] class tt range 10.10.1.2 10.10.1.10
[SwitchB-dhcp-pool-aa] class ss range 10.10.1.11 10.10.1.26
[SwitchB-dhcp-pool-aa] gateway-list 10.10.1.254
[SwitchB-dhcp-pool-aa] dns-list 10.10.1.20
[SwitchB-dhcp-pool-aa] quit
```

# 开启 DHCP 服务，且配置 DHCP 服务器处理 Option 82 信息。

```
[SwitchB] dhcp enable
[SwitchB] dhcp server relay information enable
```

# 配置 VLAN 接口 10 工作在 DHCP 服务器模式。

```
[SwitchB] interface vlan-interface 10
```

```
[SwitchB-Vlan-interface10] dhcp select server
[SwitchB-Vlan-interface10] quit
```

#### 4. 验证配置

配置完成后，10.10.1.0/24 网段的客户端通过用户类分配方式可以从 DHCP 服务器 Switch B 申请到相应地址范围的 IP 地址和网络配置参数。通过 **display dhcp server ip-in-use** 命令可以查看 DHCP 服务器为它分配的 IP 地址。

```
[SwitchB] display dhcp server ip-in-use
```

IP address	Client identifier/ Hardware address	Lease expiration	Type
10.10.1.2	0031-3865-392e-6262-3363-2e30-3230-352d-4745-302f-30	Jan 14 22:25:03 2015	Auto(C)
10.10.1.11	aabb-aabb-aabl	Jan 14 22:25:03 2015	Auto(C)

### 2.20.4 用户类白名单功能配置举例

#### 1. 组网需求

Switch B 作为 DHCP 服务器只为局域网中匹配硬件地址 aabb-aabb-0000，硬件地址掩码为 ffff-ffff-0000 的 DHCP 客户端动态分配网段为 10.1.1.0/24 的 IP 地址。

#### 2. 组网图

图2-4 用户类白名单功能组网图



#### 3. 配置步骤

- (1) 配置 DHCP 服务器接口的 IP 地址（略）
- (2) 配置 DHCP 服务

# 创建 DHCP 用户类 ss，设置匹配规则编号 1，匹配硬件地址为 aabb-aabb-0000，硬件地址掩码为 ffff-ffff-0000

```
<SwitchB> system-view
[SwitchB] dhcp class ss
[SwitchB-dhcp-class-ss] if-match rule 1 hardware-address aabb-aabb-0000 mask
ffff-ffff-0000
[SwitchB-dhcp-class-ss] quit
```

# 创建 DHCP 地址池 aa，配置可分配的地址范围为 10.1.1.0/24，开启用户类白名单功能，配置白名单中包括的用户类为 ss

```
[SwitchB] dhcp server ip-pool aa
[SwitchB-dhcp-pool-aa] network 10.1.1.0 mask 255.255.255.0
[SwitchB-dhcp-pool-aa] verify class
[SwitchB-dhcp-pool-aa] valid class ss
[SwitchB-dhcp-pool-aa] quit
```

```
# 开启 DHCP 服务
[SwitchB] dhcp enable
# 配置 VLAN 接口 2 工作在 DHCP 服务器模式
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] dhcp select server
[SwitchB-Vlan-interface2] quit
```

#### 4. 验证配置

配置完成后，匹配地址 **aabb-aabb-0000**，掩码 **ffff-ffff-0000** 的客户端可以从 DHCP 服务器 Switch B 申请到地址范围为 **10.1.1.0/24** 网段的 IP 地址。通过 **display dhcp server ip-in-use** 命令可以查看 DHCP 服务器分配的 IP 地址。

```
[SwitchB] display dhcp server ip-in-use
```

IP address	Client identifier/ Hardware address	Lease expiration	Type
10.1.1.2	aabb-aabb-ab01	Jan 14 22:25:03 2015	Auto(C)

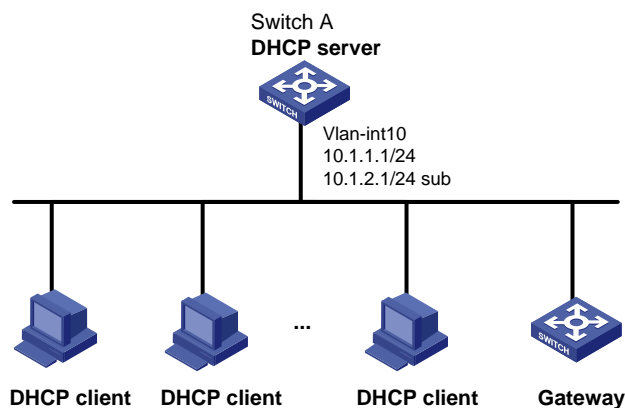
### 2.20.5 主从网段配置举例

#### 1. 组网需求

- 作为 DHCP 服务器的 **Switch A** 为局域网中的客户端动态分配 IP 地址。
- DHCP 服务器地址池中有两个网段的地址：**10.1.1.0/24** 和 **10.1.2.0/24**。当 **10.1.1.0/24** 网段没有空闲地址后，DHCP 服务器继续从 **10.1.2.0/24** 网段中选择 IP 地址分配给客户端。
- Switch A 为网段 **10.1.1.0/24** 内的客户端分配的网关地址为 **10.1.1.254/24**；为网段 **10.1.2.0/24** 内的客户端分配的网关地址为和 **10.1.2.254/24**。

#### 2. 组网图

图2-5 主从网段组网图



#### 3. 配置步骤

# 创建 DHCP 地址池 **aa**，配置主网段地址范围和从网段地址范围，配置网关地址。

```
<SwitchA> system-view
[SwitchA] dhcp server ip-pool aa
[SwitchA-dhcp-pool-aa] network 10.1.1.0 mask 255.255.255.0
[SwitchA-dhcp-pool-aa] gateway-list 10.1.1.254
```

```
[SwitchA-dhcp-pool-aa] network 10.1.2.0 mask 255.255.255.0 secondary
[SwitchA-dhcp-pool-aa-secondary] gateway-list 10.1.2.254
[SwitchA-dhcp-pool-aa-secondary] quit
[SwitchA-dhcp-pool-aa] quit
```

# 开启 DHCP 服务。

```
[SwitchA] dhcp enable
```

# 配置 VLAN 接口 10 的主从 IP 地址，并配置该接口工作在 DHCP 服务器模式。

```
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ip address 10.1.1.1 24
[SwitchA-Vlan-interface10] ip address 10.1.2.1 24 sub
[SwitchA-Vlan-interface10] dhcp select server
[SwitchA-Vlan-interface10] quit
```

#### 4. 验证配置

配置完成后，当 DHCP 服务器地址池主网段中没有空闲地址分配给客户端时，服务器会从该地址池中的从网段获取地址分配给客户端 IP 地址和网络配置参数。通过 **display dhcp server ip-in-use** 命令可以查看 DHCP 服务器已分配的主从网段 IP 地址。（此处只截取部分显示信息）

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

IP address	Client identifier/ Hardware address	Lease expiration	Type
10.1.1.2	0031-3865-392e-6262- 3363-2e30-3230-352d- 4745-302f-30	Jan 14 22:25:03 2015	Auto(C)
10.1.2.2	3030-3030-2e30-3030- 662e-3030-3033-2d45- 7568-6572-1e	Jan 14 22:25:03 2015	Auto(C)

## 2.20.6 自定义DHCP选项配置举例

### 1. 组网需求

DHCP 客户端 Switch B 从 DHCP 服务器 Switch A 获取 IP 地址和 PXE 引导服务器地址信息：

- IP 地址所在网段为 10.1.1.0/24；
- 匹配硬件地址 aabb-aabb-0000，硬件地址掩码 ffff-ffff-0000 的客户端的 PXE 引导服务器地址为 2.3.4.5 和 3.3.3.3，其他客户端的 PXE 引导服务器地址为 1.2.3.4 和 2.2.2.2。

DHCP 服务器需要通过自定义 DHCP 选项的方式配置 Option 43 的内容，从而实现为客户端分配 PXE 引导服务器地址。Option 43 和 PXE 服务器地址列表的格式分别如 [图 1-5](#) 和 [图 1-7](#)。DHCP 服务器上地址池中配置的 Option 43 选项内容为 80 0B 00 00 02 01 02 03 04 02 02 02 02，其中 80 为子选项类型（Sub-option type），0B 为子选项长度（Sub-option length），00 00 为 PXE 服务器类型（PXE server type），02 为服务器数目（Server number），01 02 03 04 02 02 02 02 为服务器的 IP 地址 1.2.3.4 和 2.2.2.2。

## 2. 组网图

图2-6 自定义 DHCP 选项配置举例



## 3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置 DHCP 服务

# 创建 DHCP 用户类 **ss**，设置匹配规则编号 **1**，匹配硬件地址 **aabb-aabb-0000**，硬件地址掩码为 **ffff-ffff-0000**。

```
<SwitchA> system-view
[SwitchA] dhcp class ss
[SwitchA-dhcp-class-ss] if-match rule 1 hardware-address aabb-aabb-0000 mask
ffff-ffff-0000
[SwitchA-dhcp-class-ss] quit
```

# 创建 DHCP 选项组 **1**，配置选项信息。

```
[SwitchA] dhcp option-group 1
[SwitchA-dhcp-option-group-1] option 43 hex 800B0000020203040503030303
```

# 配置 VLAN 接口 **2** 工作在 DHCP 服务器模式。

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] dhcp select server
[SwitchA-Vlan-interface2] quit
```

# 配置 DHCP 地址池 **0**。

```
[SwitchA] dhcp server ip-pool 0
[SwitchA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
[SwitchA-dhcp-pool-0] option 43 hex 800B0000020102030402020202
[SwitchA-dhcp-pool-0] class ss option-group 1
[SwitchA-dhcp-pool-0] quit
```

# 开启 DHCP 服务。

```
[SwitchA] dhcp enable
```

## 4. 验证配置

配置完成后，Switch B 可以从 DHCP 服务器 Switch A 获取到 10.1.1.0/24 网段的 IP 地址和 PXE 引导服务器地址。通过 **display dhcp server ip-in-use** 命令可以查看 DHCP 服务器为客户端分配的 IP 地址。

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

IP address	Client identifier/ Hardware address	Lease expiration	Type
10.1.1.2	aabb-aabb-ab01	Jan 14 22:25:03 2015	Auto(C)



## 2.21 DHCP服务器常见故障处理

### 2.21.1 DHCP客户端获取到冲突的IP地址

#### 1. 故障现象

客户端从 DHCP 服务器动态获得的 IP 地址与其他主机 IP 地址冲突。

#### 2. 故障分析

可能是网络上有主机私自配置了 IP 地址，导致冲突。

#### 3. 故障处理

- (1) 禁用客户端的网卡或断开其网线，从另外一台主机执行 **ping** 操作，检查网络中是否已经存在该 IP 地址的主机。
- (2) 如果能够收到 **ping** 操作的响应消息，则说明该 IP 地址已由用户静态配置。在 DHCP 服务器上执行 **dhcp server forbidden-ip** 命令，禁止该 IP 地址参与动态地址分配。
- (3) 重新启用客户端的网卡或连接好其网线，在客户端释放并重新获取 IP 地址。以 Windows XP 为例，在 Windows 环境下运行 **cmd** 进入 DOS 环境，使用 **ipconfig /release** 命令释放 IP 地址，之后使用 **ipconfig /renew** 重新获取 IP 地址。

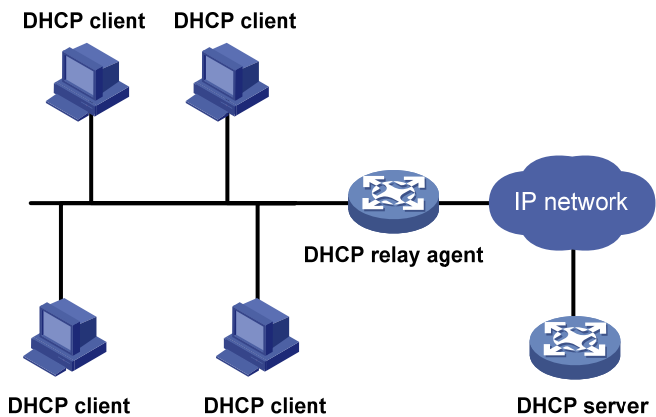
# 3 DHCP中继

## 3.1 DHCP中继简介

DHCP 客户端和 DHCP 服务器处于不同物理网段时，客户端可以通过 DHCP 中继与 DHCP 服务器通信，获取 IP 地址及其他配置信息。

[图 3-1](#) 是 DHCP 中继的典型应用示意图。

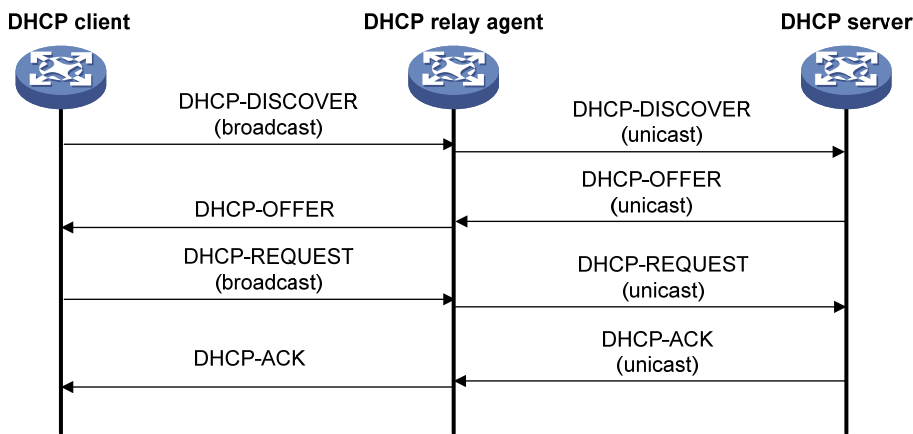
图3-1 DHCP 中继的典型组网应用



### 3.1.2 DHCP中继的基本原理

通过 DHCP 中继完成动态配置的过程中，DHCP 客户端与 DHCP 服务器的处理方式与不通过 DHCP 中继时的处理方式基本相同。下面只说明 DHCP 中继的转发过程，报文的具体交互过程请参见“[1.2.2 IP地址获取过程](#)”。

图3-2 DHCP 中继的工作过程



如 [图 3-2](#) 所示，DHCP 中继的工作过程为：

- (1) 具有 DHCP 中继功能的网络设备收到 DHCP 客户端以广播方式发送的 DHCP-DISCOVER 或 DHCP-REQUEST 报文后，将报文中的 giaddr 字段填充为 DHCP 中继的 IP 地址，并根据配置将报单播转发给指定的 DHCP 服务器。
- (2) DHCP 服务器根据 giaddr 字段为客户端分配 IP 地址等参数，并通过 DHCP 中继将配置信息转发给客户端，完成对客户端的动态配置。

3.1.3 DHCP中继支持Option 82 功能

Option 82 记录了DHCP客户端的位置信息。管理员可以利用该选项定位DHCP客户端，实现根据Option 82 为客户端分配特定范围的地址、对客户端进行安全和计费等控制。Option 82 的详细介绍请参见“[1.6.2 中继代理信息选项（Option 82）](#)”。

如果DHCP中继支持Option 82 功能，则当DHCP中继接收到DHCP请求报文后，将根据报文中是否包含Option 82 以及用户配置的处理策略及填充模式等对报文进行相应的处理，并将处理后的报文转发给DHCP服务器。具体的处理方式见 [表 3-1](#)。

如果 DHCP 中继收到的应答报文中带有 Option 82，则会将 Option 82 删除后再转发给 DHCP 客户端。

表3-1 DHCP 中继支持 Option 82 的处理方式

收到 DHCP 请求报文	处理策略	DHCP 中继对报文的处理
收到的报文中带有 Option 82	Drop	丢弃报文
	Keep	保持报文中的Option 82不变并进行转发
	Replace	根据DHCP中继上配置的填充模式、内容、格式等填充Option 82，替换报文中原有的Option 82并进行转发
收到的报文中不带有Option 82	-	根据DHCP中继上配置的填充模式、内容、格式等填充Option 82，添加到报文中并进行转发

3.1.4 DHCP中继支持MCE

设备作为 MCE（Multi-VPN-instance Customer Edge，多 VPN 实例用户网络边界设备）时，在设备上配置 DHCP 中继功能，不仅可以为公网上的 DHCP 服务器和 DHCP 客户端转发 DHCP 报文，还可以实现为私网内的 DHCP 服务器和 DHCP 客户端转发 DHCP 报文。MCE 的详细介绍，请参见“MCE 配置指导”中的“MCE”。

3.2 DHCP中继与硬件适配关系

S5110V2-SI 系列交换机不支持本特性。  
S5000V3-EI 和 S5000E-X 系列交换机仅 Release 6127 及以上版本支持本特性。

3.3 DHCP中继配置任务简介

DHCP 中继配置任务如下：

- (1) [开启DHCP服务](#)
- (2) [配置接口工作在DHCP中继模式](#)
- (3) [指定DHCP服务器的地址](#)
- (4) (可选) [配置DHCP中继的安全功能](#)
- (5) (可选) [配置通过DHCP中继释放客户端的IP地址](#)
- (6) (可选) [配置DHCP中继支持Option 82 功能](#)
- (7) (可选) [配置DHCP中继发送DHCP报文的DSCP优先级](#)
- (8) (可选) [配置DHCP中继在DHCP报文中填充的中继地址](#)
- (9) (可选) [指定DHCP中继向DHCP服务器转发报文的源地址](#)

## 3.4 开启DHCP服务

### 1. 配置限制和指导

只有开启 DHCP 服务后，其它相关的 DHCP 中继配置才能生效。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 DHCP 服务。

```
dhcp enable
```

缺省情况下，DHCP 服务处于关闭状态。

## 3.5 配置接口工作在DHCP中继模式

### 1. 功能简介

配置接口工作在DHCP中继模式后，当接口收到 DHCP 客户端发来的 DHCP 报文时，会将报文转发给 DHCP 服务器，由服务器分配地址。

DHCP 客户端通过 DHCP 中继获取 IP 地址时，DHCP 服务器上需要配置与 DHCP 中继连接 DHCP 客户端的接口 IP 地址所在网段（网络号和掩码）匹配的地址池，否则会导致 DHCP 客户端无法获得正确的 IP 地址。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置接口工作在 DHCP 中继模式。

```
dhcp select relay
```

缺省情况下，开启 DHCP 服务后，接口工作在 DHCP 服务器模式。

## 3.6 指定DHCP服务器的地址

### 3.6.1 指定DHCP中继对应的DHCP服务器地址

#### 1. 功能简介

为了提高可靠性，可以在一个网络中设置多个 DHCP 服务器。DHCP 中继上配置多个 DHCP 服务器后，DHCP 中继会将客户端发来的 DHCP 报文转发给所有的服务器。

#### 2. 配置限制和指导

指定的 DHCP 服务器的 IP 地址不能与 DHCP 中继的接口 IP 地址在同一网段。否则，可能导致客户端无法获得 IP 地址。

#### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 指定 DHCP 中继对应的 DHCP 服务器地址。

```
dhcp relay server-address ip-address [class class-name ]
```

缺省情况下，未指定 DHCP 服务器的地址。

通过多次执行 **dhcp relay server-address** 命令可以指定多个 DHCP 服务器，一个接口下最多可以指定 8 个 DHCP 服务器。

### 3.6.2 指定中继地址池对应的DHCP服务器地址

#### 1. 功能简介

对于某些特定的用户接入方式，基于用户接入位置信息的不同，网络中存在大量不同类型的用户。为了使相同类型的用户可以从指定的 DHCP 服务器申请 IP 地址等网络参数，IPoE 模块根据用户注册信息，使不同的用户选择不同的 DHCP 中继地址池，并从中继地址池下配置的 DHCP 服务器获取 IP 地址等网络参数。

为了提高可靠性，一个 DHCP 中继地址池下配置多个 DHCP 服务器地址，当 DHCP 客户端匹配该中继地址池后，DHCP 中继会将 DHCP 客户端发来的 DHCP 报文转发给该地址池对应所有的 DHCP 服务器。

一台 DHCP 中继的一个接口下可能连接不同类型的用户，当 DHCP 中继转发 DHCP 客户端请求报文给 DHCP 服务器时，不能再以中继接口的 IP 地址作为选择地址池的依据。为了解决这个问题，需要使用 **gateway-list** 命令指定某个类型用户所在的网段，并将该地址添加到转发给 DHCP 服务器的报文字段中，为 DHCP 服务器选择地址池提供依据。

#### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建 DHCP 中继地址池，并进入中继地址池视图。

```
dhcp server ip-pool pool-name
```

- (3) 指定匹配该地址池的 DHCPv4 客户端所在的网段地址。

**gateway-list** *ip-address*&<1-64>

缺省情况下，未指定匹配该地址池的 DHCP 客户端所在的网段地址。

- (4) 指定中继地址池对应的 DHCP 服务器地址。

**remote-server** *ip-address*&<1-8>

缺省情况下，未指定中继地址池对应的 DHCP 服务器的地址。

通过执行 **remote-server** 命令一次最多可以指定 8 个 DHCP 服务器的地址信息。

### 3.6.3 配置DHCP中继选择DHCP服务器方式

#### 1. 功能简介

一般来说，DHCP 中继是向所有 DHCP 服务器转发 DHCP 请求报文（即 **polling** 方式），且 DHCP 客户端会选择最快收到 DHCP 应答报文。如果用户想指定一台 DHCP 服务器作为主用 DHCP 服务器，其他 DHCP 服务器只在主用 DHCP 服务器不可用或没有空闲地址时才起作用，就需要 DHCP 中继支持优先选择用户期望的 DHCP 服务器作为主用 DHCP 服务器的功能。

当 DHCP 中继使用主备方式选择 DHCP 服务器后，会优先向配置的第一个 DHCP 服务器地址转发 DHCP 请求报文。当该 DHCP 服务器确定无法分配 IP 地址时，DHCP 中继将之后的 DHCP 请求报文向下一个 DHCP 服务器地址转发。如果 DHCP 中继已切换到配置的最后一个 DHCP 服务器地址且发现该 DHCP 服务器仍不可用，则重新选择第一个配置的 DHCP 服务器地址进入下一个循环。

主备方式有两种配置方法：

- 对于普通组网，用户可以在 DHCP 中继接口上指定多个 DHCP 服务器地址。这样当配置 DHCP 中继主备方式选择 DHCP 服务器时，配置的第一个地址对应的 DHCP 服务器为主用 DHCP 服务器，之后配置的地址对应的 DHCP 服务器为备用 DHCP 服务器。
- 对于某些用户接入方式，用户必须配置中继地址池，并指定多个 DHCP 服务器地址。这样当配置 DHCP 中继主备方式选择 DHCP 服务器时，配置的第一个地址对应的 DHCP 服务器为主用 DHCP 服务器，之后配置的地址对应的 DHCP 服务器为备用 DHCP 服务器。

此外，本特性还支持配置以下功能：

- 配置 DHCP 服务器应答超时切换时间，缺省应答超时切换时间为 30 秒。当 DHCP 中继向 DHCP 服务器转发 DHCP 请求报文，如果超过配置的应答超时切换时间后还未收到该 DHCP 服务器的应答报文，则 DHCP 中继认为该 DHCP 服务器已不可用，并切换到下一个 DHCP 服务器。
- 配置回切主用 DHCP 服务器并指定回切延迟时间，缺省 DHCP 中继是不回切的。当用户在 DHCP 中继配置了回切主用 DHCP 服务器延迟时间且当前生效的不是主用 DHCP 服务器时，经过该回切延迟时间后，DHCP 服务器会将 DHCP 请求报文转发到主用 DHCP 服务器。如果主用 DHCP 服务器不可用或没有空闲地址时则重新使用当前生效的 DHCP 服务器；如果主用 DHCP 服务器可用则继续使用主用 DHCP 服务器。

#### 2. 配置DHCP中继选择DHCP服务器方式（接口视图）

- (1) 进入系统视图。

**system-view**

- (2) 进入接口视图。

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

- (3) 配置 DHCP 中继选择 DHCP 服务器方式。

```
dhcp relay server-address algorithm { master-backup | polling }
```

缺省情况下，DHCP 中继同时向所有 DHCP 服务器转发 DHCP 请求报文（polling 方式）。

- (4) （可选）配置 DHCP 服务器应答超时切换时间。

```
dhcp relay dhcp-server timeout time
```

缺省情况下，DHCP 服务器应答超时切换时间为 30 秒。

- (5) （可选）配置回切主用 DHCP 服务器并指定回切延迟时间。

```
dhcp relay master-server switch-delay delay-time
```

缺省情况下，DHCP 中继不回切到主用 DHCP 服务器。

### 3. 配置 DHCP 中继选择 DHCP 服务器方式（中继地址池视图）

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 DHCP 地址池视图。

```
dhcp server ip-pool pool-name
```

- (3) 配置 DHCP 中继选择 DHCP 服务器方式。

```
remote-server algorithm { master-backup | polling }
```

缺省情况下，DHCP 中继同时向所有 DHCP 服务器转发 DHCP 请求报文（polling 方式）。

- (4) （可选）配置 DHCP 服务器应答超时切换时间。

```
dhcp-server timeout time
```

缺省情况下，DHCP 服务器应答超时切换时间为 30 秒。

- (5) （可选）配置回切主用 DHCP 服务器并指定回切延迟时间。

```
master-server switch-delay delay-time
```

缺省情况下，DHCP 中继不回切到主用 DHCP 服务器。

## 3.7 配置 DHCP 中继的安全功能

### 3.7.1 配置 DHCP 中继用户地址表项记录功能

#### 1. 功能简介

为了防止非法主机静态配置一个 IP 地址并访问外部网络，设备支持 DHCP 中继用户地址表项记录功能。

开启该功能后，当客户端通过 DHCP 中继从 DHCP 服务器获取到 IP 地址时，DHCP 中继可以自动记录客户端 IP 地址与硬件地址的绑定关系，生成 DHCP 中继的用户地址表项。

本功能与其他 IP 地址安全功能（如 ARP 地址检查、授权 ARP 和 IP Source Guard）配合，可以实现只允许匹配用户地址表项中绑定关系的报文通过 DHCP 中继。从而，保证非法主机不能通过 DHCP 中继与外部网络通信。

#### 2. 配置限制和指导

同异步串口作为 DHCP 客户端申请 IP 地址时，DHCP 中继不会记录该客户端对应的用户地址表项。



### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 DHCP 中继的用户地址表项记录功能。

```
dhcp relay client-information record
```

缺省情况下，DHCP 中继用户地址表项记录功能处于关闭状态。

### 3.7.2 配置DHCP中继动态用户地址表项定时刷新功能

#### 1. 功能简介

DHCP 客户端释放动态获取的 IP 地址时，会向 DHCP 服务器单播发送 DHCP-RELEASE 报文，DHCP 中继不会处理该报文的内容。如果此时 DHCP 中继上记录了该 IP 地址与 MAC 地址的绑定关系，则会造成 DHCP 中继的用户地址表项无法实时刷新。为了解决这个问题，DHCP 中继支持动态用户地址表项的定时刷新功能。

DHCP 中继动态用户地址表项定时刷新功能开启时，DHCP 中继每隔指定时间采用客户端获取到的 IP 地址向 DHCP 服务器发送 DHCP-REQUEST 报文：

- 如果 DHCP 中继接收到 DHCP 服务器响应的 DHCP-ACK 报文或在指定时间内未接收到 DHCP 服务器的响应报文，则表明这个 IP 地址已经可以进行分配，DHCP 中继会删除动态用户地址表中对应的表项。为了避免地址浪费，DHCP 中继收到 DHCP-ACK 报文后，会发送 DHCP-RELEASE 报文释放申请到的 IP 地址。
- 如果 DHCP 中继接收到 DHCP 服务器响应的 DHCP-NAK 报文，则表示该 IP 地址的租约仍然存在，DHCP 中继不会删除该 IP 地址对应的表项。

#### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 DHCP 中继动态用户地址表项定时刷新功能。

```
dhcp relay client-information refresh enable
```

缺省情况下，DHCP 中继动态用户地址表项定时刷新功能处于开启状态。

- (3) （可选）配置 DHCP 中继动态用户地址表项的定时刷新周期。

```
dhcp relay client-information refresh [ auto | interval interval ]
```

缺省情况下，定时刷新周期为 **auto**，即根据表项的数目自动计算刷新时间间隔。

### 3.7.3 配置防止DHCP饿死攻击

#### 1. 功能简介

DHCP 饿死攻击是指攻击者伪造 chaddr 字段各不相同的 DHCP 请求报文，向 DHCP 服务器申请大量的 IP 地址，导致 DHCP 服务器地址池中的地址耗尽，无法为合法的 DHCP 客户端分配 IP 地址，或导致 DHCP 服务器消耗过多的系统资源，无法处理正常业务。

如果封装 DHCP 请求报文的数据帧的源 MAC 地址各不相同，则限制三层接口上可以学习到的 ARP 表项数，或限制二层端口上可以学习到的 MAC 地址数，并配置学习到的 MAC 地址数达到最大值时，



丢弃源 MAC 地址不在 MAC 地址表里的报文，能够避免攻击者申请过多的 IP 地址，在一定程度上缓解 DHCP 饿死攻击。

如果封装 DHCP 请求报文的数据帧的源 MAC 地址都相同，则通过上述方法无法防止 DHCP 饿死攻击。在这种情况下，需要开启 DHCP 中继的 MAC 地址检查功能。开启该功能后，DHCP 中继检查接收到的 DHCP 请求报文中的 `chaddr` 字段和数据帧的源 MAC 地址字段是否一致。如果一致，则认为该报文合法，将其转发给 DHCP 服务器；如果不一致，则丢弃该报文。

因为 DHCP 中继转发 DHCP 报文时会修改报文的源 MAC 地址，所以只能在靠近 DHCP 客户端的第一跳 DHCP 中继设备上开启 MAC 地址检查功能。

设备支持配置 DHCP 中继的 MAC 地址检查表项老化时间，当老化时间到达以后，该表项信息会被老化掉，DHCP 中继收到该 MAC 地址对应的 DHCP 请求报文后重新进行合法性检查。

## 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 DHCP 中继的 MAC 地址检查表项的老化时间。

```
dhcp relay check mac-address aging-time time
```

缺省情况下，DHCP 中继的 MAC 地址检查表项的老化时间为 30 秒。

如果未通过 `dhcp relay check mac-address` 命令开启 DHCP 中继的 MAC 地址检查功能，则本命令的配置不会生效。

- (3) 进入接口视图。

```
interface interface-type interface-number
```

- (4) 开启 DHCP 中继的 MAC 地址检查功能。

```
dhcp relay check mac-address
```

缺省情况下，DHCP 中继的 MAC 地址检查功能处于关闭状态。

## 3.7.4 配置DHCP中继支持代理功能

### 1. 功能简介

设备可以通过配置 DHCP 中继支持代理功能，来防止非法用户攻击 DHCP 服务器。

开启该功能后，DHCP 中继收到 DHCP 服务器的应答报文，会把报文中的 DHCP 服务器地址修改为中继的接口地址，并转发给 DHCP 客户端。当 DHCP 客户端通过 DHCP 中继从 DHCP 服务器获取到 IP 地址等网络参数后，DHCP 客户端会把 DHCP 中继当做自己的服务器，来进行后续的 DHCP 功能的报文交互。从而达到了把真正的 DHCP 服务器和 DHCP 客户端隔离开，保护 DHCP 服务器的目的。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置 DHCP 中继支持代理功能。

```
dhcp select relay proxy
```

缺省情况下，开启 DHCP 服务后，接口工作在 DHCP 服务器模式。

### 3.7.5 配置DHCP中继的用户下线探测功能

#### 1. 功能简介

DHCP 中继的用户下线探测功能以 ARP 表项老化功能为基础，当 ARP 表项老化时认为该表项对应的用户已经下线。

如果在接口上配置了 DHCP 中继的用户下线检测功能，则当 ARP 表项老化时，DHCP 中继认为该表项对应的用户已经下线，删除对应的用户地址表项，并通过发送 Release 报文通知 DHCP 服务器删除下线用户的 IP 地址租约。

#### 2. 配置限制和指导

手工删除 ARP 表项，不会触发 DHCP 中继删除对应的用户地址表项。

#### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 DHCP 中继的用户地址表项记录功能。

```
dhcp relay client-information record
```

缺省情况下，DHCP 中继用户地址表项记录功能处于关闭状态。

用户需要开启 DHCP 中继用户地址表项记录功能，否则用户下线探测功能无法完全生效。

- (3) 进入接口视图。

```
interface interface-type interface-number
```

- (4) 配置接口工作在 DHCP 中继模式。

```
dhcp select relay
```

缺省情况下，开启 DHCP 服务后，接口工作在 DHCP 服务器模式。

- (5) 开启 DHCP 中继的用户下线探测功能。

```
dhcp client-detect
```

缺省情况下，DHCP 中继的用户下线探测功能处于关闭状态。

### 3.8 配置通过DHCP中继释放客户端的IP地址

#### 1. 功能简介

在某些情况下，可能需要通过 DHCP 中继手工释放客户端申请到的 IP 地址。如果 DHCP 中继上存在客户端 IP 地址对应的动态用户地址表项，则配置通过 DHCP 中继释放该客户端 IP 地址后，DHCP 中继会主动向 DHCP 服务器发送 DHCP-RELEASE 报文。DHCP 服务器收到该报文后，将会释放指定 IP 地址的租约。DHCP 中继也会删除该动态用户地址表项。

释放的客户端 IP 地址必须是动态用户地址表项中存在的 IP 地址，否则 DHCP 中继无法释放该 IP 地址。

#### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 向 DHCP 服务器请求释放客户端申请到的 IP 地址。

```
dhcp relay release ip ip-address
```

## 3.9 配置DHCP中继支持Option 82功能

### 1. 配置限制和指导

为使Option 82 功能正常使用，需要在DHCP服务器和DHCP中继上都进行相应配置。DHCP服务器的相关配置请参见“[2.11 配置Option 82 的处理方式](#)”。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 开启 DHCP 中继支持 Option 82 功能。

```
dhcp relay information enable
```

缺省情况下，DHCP 中继支持 Option 82 功能处于关闭状态。

- (4) （可选）配置 DHCP 中继对包含 Option 82 的请求报文的处理策略。

```
dhcp relay information strategy { drop | keep | replace }
```

缺省情况下，处理策略为 **replace**。

DHCP 中继对包含 Option 82 请求报文的处理策略为 **replace** 时，需要配置 Option 82 的填充模式和填充格式；处理策略为 **keep** 或 **drop** 时，不需要配置 Option 82 的填充模式和填充格式。

- (5) （可选）配置 Circuit ID 子选项的填充模式和填充格式。

```
dhcp relay information circuit-id { bas | string circuit-id | { normal |  
verbose [ node-identifier { mac | sysname | user-defined  
node-identifier } ] [ interface ] } [ format { ascii | hex } ] }
```

缺省情况下，Circuit ID 子选项的填充模式为 Normal，填充格式为 hex。

如果以设备的系统名称（**sysname**）作为节点标识填充 DHCP 报文的 Option 82，则系统名称中不能包含空格；否则，DHCP 中继添加或替换 Option 82 失败。

- (6) （可选）配置 Remote ID 子选项的填充模式和填充格式。

```
dhcp relay information remote-id { normal [ format { ascii | hex } ] |  
string remote-id | sysname }
```

缺省情况下，Remote ID 子选项的填充模式为 Normal；填充格式为 hex。

## 3.10 配置DHCP中继发送DHCP报文的DSCP优先级

### 1. 功能简介

DSCP 优先级用来体现报文自身的优先等级，决定报文传输的优先程度。通过本配置可以指定 DHCP 中继发送的 DHCP 报文的 DSCP 优先级。

## 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 DHCP 中继发送 DHCP 报文的 DSCP 优先级。

```
dhcp dscp dscp-value
```

缺省情况下，DHCP 中继发送的 DHCP 报文的 DSCP 优先级为 56。

## 3.11 配置DHCP中继在DHCP报文中填充的中继地址

### 3.11.1 手工指定在DHCP报文中填充的中继地址

#### 1. 功能简介

当未开启该功能时，DHCP 中继收到 DHCP 客户端的请求报文后，只能将接口的主 IP 地址添加到报文中，然后转发给 DHCP 服务器。对于某些特定需求，DHCP 中继需要添加指定的地址到报文中，这时就需要配置此功能。

#### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 手工指定在 DHCP 报文中填充的中继地址。

```
dhcp relay gateway ip-address
```

缺省情况下，DHCP 中继填充的中继地址是接口下的主 IP 地址。

### 3.11.2 通过smart-relay功能指定DHCP报文中填充的中继地址

#### 1. 功能简介

当 DHCP 中继收到 DHCP 客户端发来的请求报文时，会使用中继接口的主 IP 地址填充请求报文的 **giaddr** 字段，然后转发给 DHCP 服务器，DHCP 服务器根据 **giaddr** 字段中的地址选择合适的地址池为客户端分配 IP 地址。当 DHCP 服务器中该网段地址分配完毕后，不管 DHCP 服务器上是否存在其他网段的地址，都不会再为该 DHCP 中继下的其他 DHCP 客户端分配 IP 地址。

DHCP 中继通过 **smart-relay** 解决上述问题，开启该功能后，DHCP 中继可以使用除中继接口主地址外的其他 IP 地址来填充 **giaddr** 字段，从而使 DHCP 客户端可以获取到其他网段的 IP 地址。

DHCP 中继转发 3 次 DHCP-DISCOVER 报文后，若还未收到 DHCP 服务器的应答报文，DHCP 中继将使用下一个可用 IP 地址来填充 **giaddr** 字段。DHCP 中继使用所有配置的 IP 地址填充 **giaddr** 字段之后，将重新选择第一个配置的 IP 地址进入下一个循环。

#### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 DHCP 中继支持 **smart-relay** 功能。

```
dhcp smart-relay enable
```

缺省情况下，DHCP 中继支持 smart-relay 功能处于关闭状态。

## 3.12 指定DHCP中继向DHCP服务器转发报文的源地址

### 1. 功能简介

在某些组网中，多个 DHCP 中继接口 IP 地址相同或者中继接口 IP 到服务器没有可达路由，用户需要配置本命令指定一个 IP 地址或选择中继设备上的另一个接口（一般选择的是 Loopback 口）的 IP 地址填充到发送到 DHCP 服务器的 DHCP 请求报文中的源地址字段和 Giaddr 中。

当多个 DHCP 中继接口 IP 地址相同时，导致 DHCP 中继转发 DHCP 应答报文时无法根据目的 IP 地址找到唯一的出接口。配置本功能时需要先开启 DHCP 中继支持 Option 82 功能，DHCP 中继收到 DHCP 请求报文时在 Option 82 中的子选项 sub-option5 填充正确的子网网段，服务器可以根据中继填充的 sub-option5 来分配地址，之后 DHCP 中继处理 DHCP 应答报文时通过 MAC 地址表中的接口信息转发 DHCP 报文。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 指定 DHCP 中继向 DHCP 服务器转发报文的源地址。

```
dhcp relay source-address { ip-address | interface interface-type  
interface-number }
```

缺省情况下，DHCP 中继向 DHCP 服务器转发报文的源地址为向 DHCP 服务器转发报文出接口的地址。

## 3.13 DHCP中继显示和维护

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 DHCP 中继的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令清除 DHCP 中继的统计信息。

表3-2 DHCP 中继显示和维护

操作	命令
显示DHCP中继的MAC地址检查表项	<b>display dhcp relay check mac-address</b>
显示DHCP中继的用户地址表项信息	<b>display dhcp relay client-information</b> [ <b>interface</b> interface-type interface-number   <b>ip</b> ip-address ]
显示DHCP中继上的Option 82配置信息	<b>display dhcp relay information</b> [ <b>interface</b> interface-type interface-number ]
显示接口上指定的DHCP服务器地址信息	<b>display dhcp relay server-address</b> [ <b>interface</b> interface-type interface-number ]

操作	命令
显示DHCP中继的相关报文统计信息	<b>display dhcp relay statistics</b> [ <b>interface</b> <i>interface-type interface-number</i> ]
清除DHCP中继的用户地址表项信息	<b>reset dhcp relay client-information</b> [ <b>interface</b> <i>interface-type interface-number</i>   <b>ip</b> <i>ip-address</i> ]
清除DHCP中继的相关报文统计信息	<b>reset dhcp relay statistics</b> [ <b>interface</b> <i>interface-type interface-number</i> ]

## 3.14 DHCP中继典型配置举例

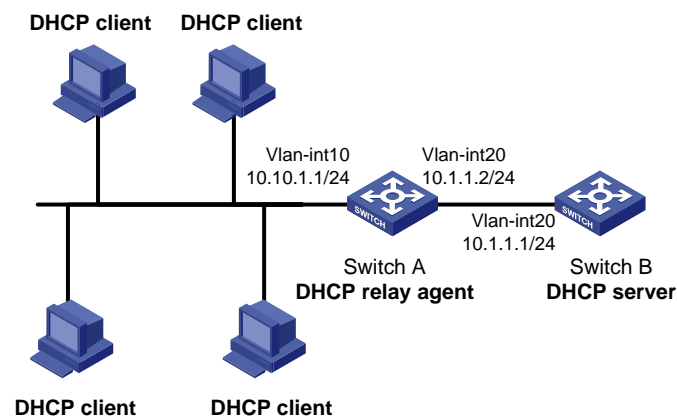
### 3.14.1 DHCP中继基本组网配置举例

#### 1. 组网需求

- DHCP 客户端所在网段为 10.10.1.0/24，DHCP 服务器的 IP 地址为 10.1.1.1/24；
- 由于 DHCP 客户端和 DHCP 服务器不在同一网段，因此，需要在客户端所在网段设置 DHCP 中继设备，以便客户端可以从 DHCP 服务器申请到 10.10.1.0/24 网段的 IP 地址及相关配置信息；
- Switch A 作为 DHCP 中继通过端口（属于 VLAN10）连接到 DHCP 客户端所在的网络，交换机 VLAN 接口 10 的 IP 地址为 10.10.1.1/24，VLAN 接口 20 的 IP 地址为 10.1.1.2/24。

#### 2. 组网图

图3-3 DHCP 中继组网示意图



#### 3. 配置步骤

# 配置各接口的 IP 地址（略）。

# 开启 DHCP 服务。

```
<SwitchA> system-view
[SwitchA] dhcp enable
```

# 配置 VLAN 接口 10 工作在 DHCP 中继模式。

```
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] dhcp select relay
```

# 配置 DHCP 服务器的地址。

```
[SwitchA-Vlan-interface10] dhcp relay server-address 10.1.1.1
```

配置完成后，DHCP 客户端可以通过 DHCP 中继从 DHCP 服务器获取 IP 地址及相关配置信息。通过 **display dhcp relay statistics** 命令可以显示 DHCP 中继转发的 DHCP 报文统计信息；如果在 DHCP 中继上通过 **dhcp relay client-information record** 命令开启了 DHCP 中继的用户地址表项记录功能，则可以通过 **display dhcp relay client-information** 命令可以显示通过 DHCP 中继获取 IP 地址的客户端信息。

---



说明

由于 DHCP 中继连接客户端的接口 IP 地址与 DHCP 服务器的 IP 地址不在同一网段，因此需要在 DHCP 服务器上通过静态路由或动态路由协议保证两者之间路由可达。

为了使 DHCP 客户端能从 DHCP 服务器获得 IP 地址，还需要在 DHCP 服务器上进行一些配置。DHCP 服务器的配置方法，请参见“[2.20 DHCP 服务器典型配置举例](#)”。

---

### 3.14.2 DHCP 中继支持 Option 82 配置举例

#### 1. 组网需求

- 在 DHCP 中继 Switch A 上开启 Option 82 功能；
- 对包含 Option 82 的请求报文的处理策略为 **replace**；
- Circuit ID 填充内容为 company001，Remote ID 填充内容为 device001；
- Switch A 将添加 Option 82 的 DHCP 请求报文转发给 DHCP 服务器 Switch B，使得 DHCP 客户端可以获取到 IP 地址。

#### 2. 组网图

如 [图 3-3](#) 所示。

#### 3. 配置步骤

# 配置各接口的 IP 地址（略）。

# 开启 DHCP 服务。

```
<SwitchA> system-view
```

```
[SwitchA] dhcp enable
```

# 配置 VLAN 接口 10 工作在 DHCP 中继模式。

```
[SwitchA] interface vlan-interface 10
```

```
[SwitchA-Vlan-interface10] dhcp select relay
```

# 指定 DHCP 服务器的地址。

```
[SwitchA-Vlan-interface10] dhcp relay server-address 10.1.1.1
```

# 配置 Option 82 的处理策略和填充内容。

```
[SwitchA-Vlan-interface10] dhcp relay information enable
```

```
[SwitchA-Vlan-interface10] dhcp relay information strategy replace
```

```
[SwitchA-Vlan-interface10] dhcp relay information circuit-id string company001
```

```
[SwitchA-Vlan-interface10] dhcp relay information remote-id string device001
```





说明

为使 Option 82 功能正常使用，DHCP 服务器也需要进行相应配置。

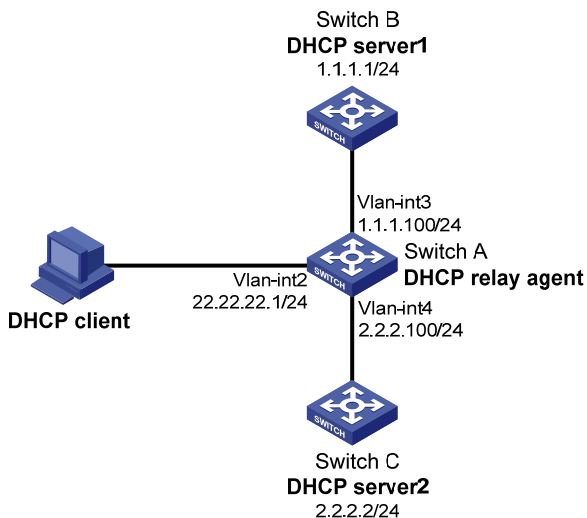
### 3.14.3 DHCP中继选择DHCP服务器方式配置举例

#### 1. 组网需求

- DHCP 客户端所在网段为 22.22.22.0/24;
- 由于 DHCP 客户端和 DHCP 服务器不在同一网段，需要在客户端所在网段设置 DHCP 中继，以便 DHCP 客户端可以从 DHCP 服务器申请到 22.22.22.0/24 网段的 IP 地址及相关配置信息;
- DHCP 中继 Switch A 通过 VLAN 接口 2 连接到 DHCP 客户端所在的网络，VLAN 接口 2 的 IP 地址为 22.22.22.1/24，通过 VLAN 接口 3 连接 Switch B，VLAN 接口 3 的 IP 地址为 1.1.1.100/24，通过 VLAN 接口 4 连接 Switch C，VLAN 接口 4 的 IP 地址为 2.2.2.100/24;
- Switch B 配置了 22.22.22.0 网段的地址池，但未开启 DHCP 服务；Switch C 配置了 22.22.22.0 网段的地址池，也未开启 DHCP 服务。

#### 2. 组网图

图3-4 DHCP 中继组网示意图



#### 3. 配置步骤

- (1) 配置各设备上各接口的 IP 地址（略）。
- (2) 配置 DHCP 服务器 Switch B 和 Switch C（略）。
- (3) 配置 DHCP 中继 Switch A。

# 开启 DHCP 服务。

```
<SwitchA> system-view
```

```
[SwitchA] dhcp enable
```

# 配置 VLAN 接口 2 工作在 DHCP 中继模式。



```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] dhcp select relay
# 指定 DHCP 服务器的 IP 地址。
[SwitchA-Vlan-interface2] dhcp relay server-address 1.1.1.1
[SwitchA-Vlan-interface2] dhcp relay server-address 2.2.2.2
# 指定 DHCP 中继选择 DHCP 服务器方式为主备方式。
[SwitchA-Vlan-interface2] dhcp relay server-address algorithm master-backup
# 配置回切主用 DHCP 服务器并指定回切延迟时间为 3 分钟。
[SwitchA-Vlan-interface2] dhcp relay master-server switch-delay 3
```

#### 4. 验证配置

# 配置完成后，DHCP 客户端一开始不能申请到 IP 地址，等待大约 30 秒后打印日志信息。

```
DHCPR/3/DHCPR_SERVERCHANGE: -MDC=1;
Switched to the server at 2.2.2.2 because the current server did not respond.
```

# 用户开启 Switch B 的 DHCP 服务。

# 此时 DHCP 客户端无法申请到 IP 地址，再等待大约 3 分钟后打印日志信息。

```
DHCPR/3/DHCPR_SWITCHMASTER: -MDC=1;
Switched to the master DHCP server at 1.1.1.1.
```

# 此时 DHCP 客户端可以成功申请到 IP 地址。

### 3.15 DHCP中继常见故障处理

#### 3.15.1 DHCP客户端无法通过DHCP中继获取配置信息

##### 1. 故障现象

DHCP 客户端无法通过 DHCP 中继获得配置信息。

##### 2. 故障分析

DHCP 中继或 DHCP 服务器的配置可能有问题。可以打开调试开关显示调试信息，并通过执行 **display** 命令显示接口状态信息的方法来分析定位。

##### 3. 故障处理

- 检查 DHCP 服务器和 DHCP 中继是否开启了 DHCP 服务。
- 检查 DHCP 服务器是否配置有 DHCP 客户端所在网段的地址池。
- 检查具有 DHCP 中继功能的网络设备和 DHCP 服务器是否配置有相互可达的路由。
- 检查具有 DHCP 中继功能的网络设备是否在连接 DHCP 客户端所在网段的接口上指定了正确的 DHCP 服务器地址。

# 4 DHCP客户端

## 4.1 DHCP客户端简介

为了方便用户配置和集中管理，可以指定设备的接口作为 DHCP 客户端，使用 DHCP 协议从 DHCP 服务器动态获得 IP 地址等参数。

## 4.2 DHCP客户端配置限制和指导

DHCP 客户端中对于接口的相关配置，目前只能在 VLAN 接口上进行。

## 4.3 DHCP客户端配置任务简介

DHCP 客户端配置任务如下：

- (1) [配置接口通过DHCP协议获取IP地址](#)
- (2) [配置接口使用的DHCP客户端ID](#)

DHCP 客户端使用客户端 ID 从 DHCP 服务器获取特定地址时配置。

- (3) （可选）[开启地址冲突检查功能](#)
- (4) （可选）[配置DHCP客户端发送DHCP报文的DSCP优先级](#)

## 4.4 配置接口通过DHCP协议获取IP地址

### 1. 配置限制和指导

配置接口通过 DHCP 协议获取 IP 地址，需要注意：

- 某些产品上，接口作为 DHCP 客户端多次申请 IP 地址失败后，将停止申请，并为接口配置缺省 IP 地址。
- 接口可以采用多种方式获得 IP 地址，新的配置方式会覆盖原有的配置方式。
- 当接口被配置为通过 DHCP 动态获取 IP 地址后，不能再给该接口配置从 IP 地址。
- 如果 DHCP 服务器为接口分配的 IP 地址与设备上其他接口的 IP 地址在同一网段，则该接口不会使用该 IP 地址，且会再向 DHCP 服务器重新申请 IP 地址。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置接口通过 DHCP 协议获取 IP 地址。

```
ip address dhcp-alloc
```

缺省情况下，接口不通过 DHCP 协议获取 IP 地址。

## 4.5 配置接口使用的DHCP客户端ID

### 1. 功能简介

DHCP 客户端 ID 用来填充 DHCP 报文 Option 61，作为识别 DHCP 客户端的唯一标识。DHCP 服务器可以根据客户端 ID 为特定的客户端分配特定的 IP 地址。DHCP 客户端 ID 包括类型和取值两部分，用户可以通过 ASCII 字符串、十六进制数和指定接口的 MAC 地址来指定 DHCP 客户端 ID：

- 当客户端 ID 的取值为 ASCII 字符串时，对应的类型值为 00；
- 当客户端 ID 的取值为十六进制数时，对应的类型值为该十六进制数的前两个字符；
- 当客户端 ID 使用指定接口的 MAC 地址时，对应的类型值为 01。

DHCP 客户端 ID 类型值可通过命令 **display dhcp server ip-in-use** 或 **display dhcp client** 进行查看。

### 2. 配置限制和指导

用户在指定客户端 ID 时，需要确保不同客户端的客户端 ID 不能相同。

### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置接口使用的 DHCP 客户端 ID。

```
dhcp client identifier { ascii ascii-string | hex hex-string | mac  
interface-type interface-number }
```

缺省情况下，根据本接口 MAC 地址生成 DHCP 客户端 ID，如果本接口没有 MAC 地址，则获取设备第一个以太接口的 MAC 地址生成 DHCP 客户端 ID。

## 4.6 开启地址冲突检查功能

### 1. 功能简介

通常情况下，DHCP 客户端上开启地址冲突检查功能，通过发送和接收 ARP 报文，对 DHCP 服务器分配的 IP 地址进行地址冲突检测。

如果攻击者仿冒地址拥有者进行 ARP 应答，就可以欺骗 DHCP 客户端，导致 DHCP 客户端无法正常使用分配到的 IP 地址。在网络中存在上述攻击者时，建议在客户端上关闭地址冲突检查功能。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启地址冲突检查功能。

```
dhcp client dad enable
```

缺省情况下，地址冲突检查功能处于开启状态。

## 4.7 配置DHCP客户端发送DHCP报文的DSCP优先级

### 1. 功能简介

DSCP 优先级用来体现报文自身的优先等级，决定报文传输的优先程度。通过本配置可以指定 DHCP 客户端发送的 DHCP 报文的 DSCP 优先级。

### 2. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 配置 DHCP 客户端发送 DHCP 报文的 DSCP 优先级。

```
dhcp client dscp dscp-value
```

缺省情况下，DHCP 客户端发送的 DHCP 报文的 DSCP 优先级为 56。

## 4.8 DHCP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 DHCP 客户端的信息，通过查看显示信息验证配置的效果。

表4-1 DHCP 客户端显示和维护

操作	命令
显示DHCP客户端的相关信息	<b>display dhcp client</b> [ <b>verbose</b> ] [ <b>interface</b> <i>interface-type interface-number</i> ]

## 4.9 DHCP客户端典型配置举例

### 4.9.1 DHCP客户端基本组网配置举例

#### 1. 组网需求

Switch B 的端口（属于 VLAN2）接入局域网，VLAN 接口 2 通过 DHCP 协议从 DHCP 服务器获取 IP 地址、DNS 服务器地址和静态路由信息：

- DHCP 客户端的 IP 地址所在网段为 10.1.1.0/24；
- DNS 服务器地址为 20.1.1.1；
- 静态路由信息为到达 20.1.1.0/24 网段的下一跳地址是 10.1.1.2。

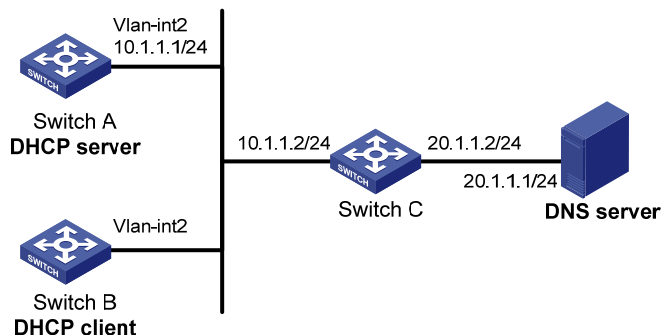
DHCP服务器需要通过自定义选项的方式配置Option 121 的内容，以便为客户端分配静态路由信息。Option 121 的格式如 [图 4-1](#) 所示。其中，目的描述符由子网掩码长度和目的网络地址两部分组成。在本例中，目的描述符字段取值为 18 14 01 01（十六进制数值，表示子网掩码长度为 24，目的网络地址为 20.1.1.0）；下一跳地址字段取值为 0A 01 01 02（十六进制数值，表示下一跳地址为 10.1.1.2）。

图4-1 Option 121 选项格式

0	7	15
Option type (0x79)		Option length
Destination descriptor (variable)		Next hop address

## 2. 组网图

图4-2 DHCP 客户端配置举例组网图



## 3. 配置步骤

### (1) 配置 DHCP 服务器 Switch A

# 配置接口的 IP 地址。

```

<SwitchA> system-view
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 10.1.1.1 24
[SwitchA-Vlan-interface2] quit

```

# 配置不参与自动分配的 IP 地址。

```

[SwitchA] dhcp server forbidden-ip 10.1.1.2

```

# 配置 DHCP 地址池 0，采用动态绑定方式分配 IP 地址。可分配的网段为 10.1.1.0/24，租约有效期限为 10 天，DNS 服务器地址为 20.1.1.1，到达 20.1.1.0/24 网段的下一跳地址是 10.1.1.2。

```

[SwitchA] dhcp server ip-pool 0
[SwitchA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
[SwitchA-dhcp-pool-0] expired day 10
[SwitchA-dhcp-pool-0] dns-list 20.1.1.1
[SwitchA-dhcp-pool-0] option 121 hex 181401010A010102
[SwitchA-dhcp-pool-0] quit

```

# 开启 DHCP 服务。

```

[SwitchA] dhcp enable

```

### (2) 配置 DHCP 客户端 Switch B

# 配置 VLAN 接口 2 通过 DHCP 动态获取地址。

```

<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address dhcp-alloc

```

```
[SwitchB-Vlan-interface2] quit
```

#### 4. 验证配置

# 通过 **display dhcp client** 命令可以查看 Switch B 申请到的 IP 地址和网络配置参数。

```
[SwitchB] display dhcp client verbose
Vlan-interface2 DHCP client information:
Current state: BOUND
Allocated IP: 10.1.1.3 255.255.255.0
Allocated lease: 864000 seconds, T1: 331858 seconds, T2: 756000 seconds
Lease from May 21 19:00:29 2012 to May 31 19:00:29 2012
DHCP server: 10.1.1.1
Transaction ID: 0xcde72232
Classless static routes:
  Destination: 20.1.1.0, Mask: 255.255.255.0, NextHop: 10.1.1.2
DNS servers: 20.1.1.1
Client ID type: ascii(type value=00)
Client ID value: 000c.29d3.8659-Vlan2
Client ID (with type) hex: 0030-3030-632e-3239-
                           6433-2e38-3635-392d-
                           4574-6830-2f30-2f32
T1 will timeout in 3 days 19 hours 48 minutes 43 seconds
```

# 通过 **display ip routing-table** 命令可以查看 Switch B 的路由表中添加了到达 20.1.1.0/24 网络的静态路由。

```
[SwitchB] display ip routing-table
```

```
Destinations : 11          Routes : 11
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.1.1.0/24	Direct	0	0	10.1.1.3	Vlan2
10.1.1.3/32	Direct	0	0	127.0.0.1	InLoop0
20.1.1.0/24	Static	70	0	10.1.1.2	Vlan2
10.1.1.255/32	Direct	0	0	10.1.1.3	Vlan2
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

# 5 DHCP Snooping

## 5.1 DHCP Snooping简介

DHCP Snooping 是 DHCP 的一种安全特性。

DHCP Snooping 设备只有位于 DHCP 客户端与 DHCP 服务器之间，或 DHCP 客户端与 DHCP 中继之间时，DHCP Snooping 功能配置后才能正常工作；设备位于 DHCP 服务器与 DHCP 中继之间时，DHCP Snooping 功能配置后不能正常工作。

### 5.1.1 DHCP Snooping作用

#### 1. 保证客户端从合法的服务器获取IP地址

网络中如果存在私自架设的非法 DHCP 服务器，则可能导致 DHCP 客户端获取到错误的 IP 地址和网络配置参数，从而无法正常通信。为了使 DHCP 客户端能通过合法的 DHCP 服务器获取 IP 地址，DHCP Snooping 安全机制允许将端口设置为信任端口和不信任端口：

- 信任端口正常转发接收到的 DHCP 报文。
- 不信任端口接收到 DHCP 服务器响应的 DHCP-ACK 和 DHCP-OFFER 报文后，丢弃该报文。

在 DHCP Snooping 设备上指向 DHCP 服务器方向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 DHCP 客户端只能从合法的 DHCP 服务器获取 IP 地址，私自架设的伪 DHCP 服务器无法为 DHCP 客户端分配 IP 地址。

#### 2. 记录DHCP客户端IP地址与MAC地址的对应关系

DHCP Snooping 通过监听 DHCP-REQUEST 报文和信任端口收到的 DHCP-ACK 报文，记录 DHCP Snooping 表项，其中包括客户端的 MAC 地址、DHCP 服务器为 DHCP 客户端分配的 IP 地址、与 DHCP 客户端连接的端口及 VLAN 等信息。利用这些信息可以实现：

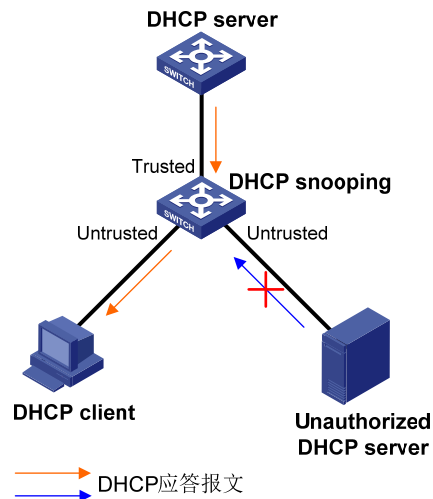
- **ARP Detection**：根据 DHCP Snooping 表项来判断发送 ARP 报文的用户是否合法，从而防止非法用户的 ARP 攻击。ARP Detection 的详细介绍请参见“安全配置指导”中的“ARP 攻击防御”。
- **MFF (MAC-Forced Forwarding)**：在 MFF 的自动方式中，设备截获到用户发送的 ARP 请求后，根据 DHCP Snooping 表项查找该用户对应的网关地址，并回复网关的 MAC 地址，强制用户将所有流量发送到网关，使得网关可以监控用户之间的数据流量，从而防止用户之间的恶意攻击，更好的保障网络安全。MFF 的详细介绍请参见“安全配置指导”中的“MFF”。
- **IP Source Guard**：通过动态获取 DHCP Snooping 表项对端口转发的报文进行过滤，防止非法报文通过该端口。IP Source Guard 的详细介绍请参见“安全配置指导”中的“IP Source Guard”。
- **VLAN 映射**：发送给用户的报文通过查找指定 VLAN 对应的 DHCP Snooping 表项中的 DHCP 客户端 IP 地址、MAC 地址和原始 VLAN 的信息，将报文的指定 VLAN 修改为原始 VLAN。VLAN 映射的详细介绍请参见“二层技术-以太网交换配置指导”中的“VLAN 映射”。

## 5.1.2 信任端口的典型应用环境

### 1. DHCP Snooping直联DHCP服务器和DHCP客户端网络

如 图 5-1 所示，在DHCP Snooping设备上指向DHCP服务器方向的端口需要设置为信任端口，以便DHCP Snooping设备正常转发DHCP服务器的应答报文，保证DHCP客户端能够从合法的DHCP服务器获取IP地址。

图5-1 信任端口和非信任端口



### 2. DHCP Snooping级联网络

在多个 DHCP Snooping 设备级联的网络中，为了节省系统资源，不需要每台 DHCP Snooping 设备都记录所有 DHCP 客户端的 IP 地址和 MAC 地址的绑定信息，只需在与客户端直接相连不信任端口上记录绑定信息。间接与 DHCP 客户端相连的不信任端口不需要记录 IP 地址和 MAC 地址绑定信息。

图5-2 DHCP Snooping 级联组网图

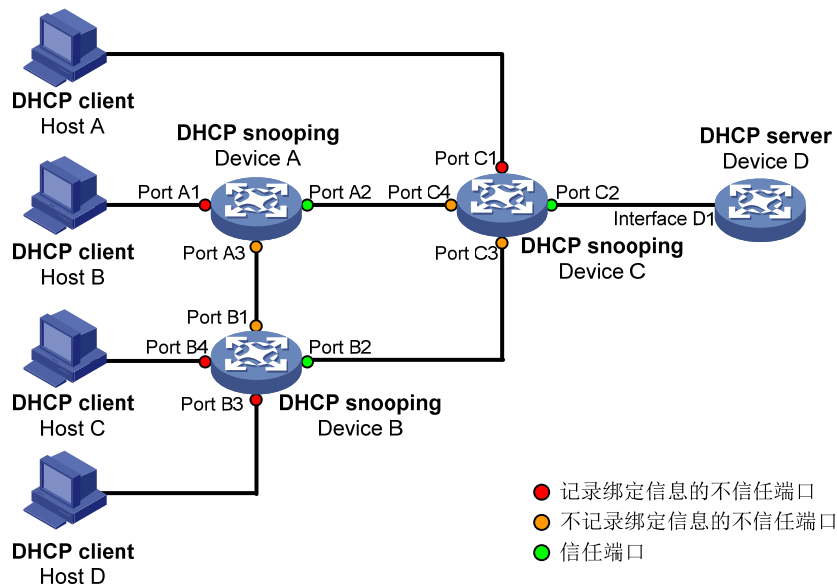




图 5-2 中设备各端口的角色如 表 5-1 所示。

表5-1 端口的角色

设备	记录绑定信息的不信任端口	不记录绑定信息的不信任端口	信任端口
Device A	Port A1	Port A3	Port A2
Device B	Port B3和Port B4	Port B1	Port B2
Device C	Port C1	Port C3和Port C4	Port C2

### 5.1.3 DHCP Snooping支持Option 82 功能

Option 82 记录了DHCP客户端的位置信息。管理员可以利用该选项定位DHCP客户端，实现对客户端的安全和计费等控制。Option 82 的详细介绍请参见 “1.6.2 中继代理信息选项（Option 82）”。

如果DHCP Snooping支持Option 82 功能，则当设备接收到DHCP请求报文后，将根据报文中是否包含Option 82 以及用户配置的处理策略及填充模式等对报文进行相应的处理，并将处理后的报文转发给DHCP服务器。具体的处理方式见 表 5-2。DHCP Snooping对Option 82 的处理策略、填充模式与DHCP中继相同。

当设备接收到 DHCP 服务器的响应报文时，如果报文中含有 Option 82，则删除 Option 82，并转发给 DHCP 客户端；如果报文中不含有 Option 82，则直接转发。

表5-2 DHCP Snooping 支持 Option 82 的处理方式

收到 DHCP 请求报文	处理策略	DHCP Snooping 对报文的处理
收到的报文中带有Option 82	Drop	丢弃报文
	Keep	保持报文中的Option 82不变并进行转发
	Replace	根据DHCP Snooping上配置的填充模式、内容、格式等填充Option 82，替换报文中原有的Option 82并进行转发
收到的报文中不带有Option 82	-	根据DHCP Snooping上配置的填充模式、内容、格式等填充Option 82，添加到报文中并进行转发

## 5.2 DHCP Snooping配置限制和指导

配置 DHCP Snooping 基本功能时，需要注意：

- 如果二层以太网接口加入聚合组，则在该接口上进行的 DHCP Snooping 相关配置不会生效；该接口退出聚合组后，之前的配置才会生效。
- 为了使 DHCP 客户端能从合法的 DHCP 服务器获取 IP 地址，必须将与合法 DHCP 服务器相连的端口设置为信任端口，设置的信任端口和与 DHCP 客户端相连的端口必须在同一个 VLAN 内。
- 目前，可以设置为 DHCP Snooping 信任端口的接口类型包括：二层以太网接口、二层聚合接口，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”。

## 5.3 DHCP Snooping配置任务简介

DHCP Snooping 配置任务如下：

- (1) [配置DHCP Snooping基本功能](#)
- (2) （可选）[配置DHCP Snooping支持Option 82 功能](#)
- (3) （可选）[配置DHCP Snooping表项固化功能](#)
- (4) （可选）[配置接口动态学习DHCP Snooping表项的最大数目](#)
- (5) （可选）[配置DHCP Snooping报文限速功能](#)
- (6) （可选）[配置DHCP Snooping安全功能](#)
- (7) （可选）[开启DHCP Snooping日志信息功能](#)
- (8) （可选）[关闭接口的DHCP Snooping功能](#)

## 5.4 配置DHCP Snooping基本功能

### 5.4.1 在普通组网中配置DHCP Snooping基本功能

#### 1. 功能简介

在一台 DHCP Snooping 设备上，如果全局开启了 DHCP Snooping 功能，则设备上所有 VLAN 内的 DHCP Snooping 功能也同时开启。

对于某些组网来说，管理员只需要在设备在某些特定 VLAN 内开启 DHCP Snooping 功能，而不需要在整个设备上开启 DHCP Snooping 功能。为了满足此需求，设备支持在指定 VLAN 内开启 DHCP Snooping 功能，并在 VLAN 内配置 DHCP Snooping 信任端口和开启端口的 DHCP Snooping 表项记录功能。

#### 2. 配置限制和指导

在一台设备上，全局 DHCP Snooping 功能和 VLAN 内的 DHCP Snooping 功能关系如下：

- 如果全局开启了 DHCP Snooping 基本功能（包括开启 DHCP Snooping 功能、配置信任端口和配置 DHCP Snooping 表项记录功能），只能使用对应的全局命令关闭功能，使用 VLAN 内的命令关闭功能不生效；
- 如果 VLAN 内开启了 DHCP Snooping 基本功能（包括开启 DHCP Snooping 功能、配置信任端口和配置 DHCP Snooping 表项记录功能），只能使用对应的 VLAN 内命令关闭功能，使用全局命令关闭功能不生效。

#### 3. 全局开启DHCP Snooping功能

- (1) 进入系统视图。

```
system-view
```

- (2) 全局开启 DHCP Snooping 功能。

```
dhcp snooping enable
```

缺省情况下，DHCP Snooping 功能处于关闭状态。

- (3) 进入接口视图。

```
interface interface-type interface-number
```

此接口为连接 DHCP 服务器的接口。

- (4) 配置端口为信任端口。

**dhcp snooping trust**

缺省情况下，在开启 DHCP Snooping 功能后，设备的所有端口均为不信任端口。

- (5) （可选）开启端口的 DHCP Snooping 表项记录功能。

- a. 退回系统视图。

**quit**

- b. 进入接口视图。

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

此接口为连接 DHCP 客户端的接口。

- c. 开启 DHCP Snooping 表项记录功能。

**dhcp snooping binding record**

缺省情况下，DHCP Snooping 表项记录功能处于关闭状态。

#### 4. 在VLAN中配置DHCP Snooping基本功能

- (1) 进入系统视图。

**system-view**

- (2) 在指定 VLAN 内开启 DHCP Snooping 功能。

**dhcp snooping enable vlan** *vlan-id-list*

缺省情况下，所有 VLAN 内的 DHCP Snooping 功能处于关闭状态。

- (3) 进入 VLAN 视图。

**vlan** *vlan-id*

该 VLAN 为开启了 DHCP Snooping 功能的 VLAN。

- (4) 配置指定接口为 VLAN 下 DHCP Snooping 功能的信任端口。

**dhcp snooping trust interface** *interface-type interface-number*

缺省情况下，在开启 DHCP Snooping 功能后，VLAN 内的所有接口均为不信任端口。

- (5) （可选）开启 VLAN 的 DHCP Snooping 表项记录功能。

**dhcp snooping binding record**

缺省情况下，VLAN 的 DHCP Snooping 表项记录功能处于关闭状态。

## 5.5 配置DHCP Snooping支持Option 82功能

### 1. 配置限制和指导

配置 DHCP Snooping 支持 Option 82 功能时，需要注意：

- 如果二层以太网接口加入聚合组，则在该接口上进行的 DHCP Snooping 支持 Option 82 功能的配置不会生效；该接口退出聚合组后，之前的配置才会生效。
- 为使Option 82 功能正常使用，需要在DHCP服务器和DHCP Snooping设备上都进行相应配置。DHCP服务器的相关配置请参见“[2.11 配置Option 82 的处理方式](#)”。
- 如果以设备名称（**sysname**）作为节点标识填充 DHCP 报文的 Option 82，则设备名称中不能包含空格；否则，DHCP Snooping 将不处理该报文。用户可以通过 **sysname** 命令配置设备名称，该命令的详细介绍请参见“基本配置命令参考”中的“设备管理”。

- DHCP Snooping 功能和 QinQ 功能同时使用，或 DHCP Snooping 设备接收到的 DHCP 报文带有两层 VLAN Tag 时，如果采用 verbose 模式填充 Option 82，则 sub-option 1 中 VLAN ID 字段的格式为“第一层 VLAN Tag.第二层 VLAN Tag”。例如，第一层 VLAN Tag 为 10（十六进制值为 a），第二层 VLAN Tag 为 20（十六进制值为 14），则 VLAN ID 字段的内容为“000a.0014”。

## 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 开启 DHCP Snooping 支持 Option 82 功能。

```
dhcp snooping information enable
```

缺省情况下，DHCP Snooping 支持 Option 82 功能处于关闭状态。

- (4) （可选）配置 DHCP Snooping 对包含 Option 82 的请求报文的处理策略。

```
dhcp snooping information strategy { drop | keep | replace }
```

缺省情况下，对带有 Option 82 的请求报文的处理策略为 **replace**。

DHCP Snooping 对包含 Option 82 请求报文的处理策略为 **replace** 时，需要配置 Option 82 的填充模式和填充格式；处理策略为 **keep** 或 **drop** 时，不需要配置 Option 82 的填充模式和填充格式。

- (5) （可选）配置 Circuit ID 子选项的填充模式和填充格式。

```
dhcp snooping information circuit-id { [ vlan vlan-id ] string circuit-id | { normal | verbose [ node-identifier { mac | sysname | user-defined node-identifier } ] } [ format { ascii | hex } ] }
```

缺省情况下，Circuit ID 子选项的填充模式为 Normal，填充格式为 hex。

如果以设备的系统名称（**sysname**）作为节点标识填充 DHCP 报文的 Option 82，则系统名称中不能包含空格；否则，DHCP Snooping 添加或替换 Option 82 失败。

- (6) （可选）配置 Remote ID 子选项的填充模式和填充格式。

```
dhcp snooping information remote-id { normal [ format { ascii | hex } ] | [ vlan vlan-id ] string remote-id | sysname }
```

缺省情况下，Remote ID 子选项的填充模式为 Normal，填充格式为 hex。

## 5.6 配置DHCP Snooping表项固化功能

### 1. 功能简介

DHCP Snooping 设备重启后，设备上记录的 DHCP Snooping 表项将丢失，DHCP Snooping 与安全模块（如 IP Source Guard）配合使用，则表项丢失会导致安全模块无法通过 DHCP Snooping 获取到相应的表项，进而导致 DHCP 客户端不能顺利通过安全检查、正常访问网络。

DHCP Snooping 表项固化功能将 DHCP Snooping 表项保存到指定的文件中，DHCP Snooping 设备重启后，自动根据该文件恢复 DHCP Snooping 表项，从而保证 DHCP Snooping 表项不会丢失。

## 2. 配置限制和指导

执行 **undo dhcp snooping enable** 命令关闭 DHCP Snooping 功能后，设备会删除所有 DHCP Snooping 表项，文件中存储的 DHCP Snooping 表项也将被删除。

## 3. 配置步骤

- (1) 进入系统视图。

**system-view**

- (2) 指定存储 DHCP Snooping 表项的文件名称。

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

缺省情况下，未指定存储文件名称。

执行本命令后，会立即触发一次表项备份。

- (3) （可选）将当前的 DHCP Snooping 表项保存到用户指定的文件中。

**dhcp snooping binding database update now**

本命令只用来触发一次 DHCP Snooping 表项的备份。

- (4) （可选）配置刷新 DHCP Snooping 表项存储文件的延迟时间。

**dhcp snooping binding database update interval** *interval*

缺省情况下，若 DHCP Snooping 表项不变化，则不刷新存储文件；若 DHCP Snooping 表项发生变化，默认在 300 秒之后刷新存储文件。

## 5.7 配置接口动态学习DHCP Snooping表项的最大数目

### 1. 功能简介

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

### 2. 配置步骤

- (1) 进入系统视图。

**system-view**

- (2) 进入接口视图。

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

- (3) 配置接口动态学习 DHCP Snooping 表项的最大数目。

**dhcp snooping max-learning-num** *max-number*

缺省情况下，不限制接口动态学习 DHCP Snooping 表项的数目。

## 5.8 配置DHCP Snooping报文限速功能

### 1. 功能简介

为了避免非法用户发送大量 DHCP 报文，对网络造成攻击，DHCP Snooping 支持报文限速功能，限制接口接收 DHCP 报文的速率。当接口接收的 DHCP 报文速率超过限制的最高速率时，DHCP Snooping 设备将丢弃超过速率限制的报文。

## 2. 配置限制和指导

如果二层以太网接口加入了聚合组，则该接口采用对应二层聚合接口下的 DHCP Snooping 报文限速配置，如果二层以太网接口离开聚合组，则该接口采用二层以太网接口下的 DHCP Snooping 报文限速配置。

## 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 开启 DHCP Snooping 的报文限速功能。

```
dhcp snooping rate-limit rate
```

缺省情况下，DHCP Snooping 的报文限速功能处于关闭状态，即不限制接口接收 DHCP 报文的速率。

# 5.9 配置DHCP Snooping安全功能

## 5.9.1 配置防止DHCP饿死攻击

### 1. 功能简介

DHCP饿死攻击是指攻击者伪造chaddr字段各不相同的DHCP请求报文，向DHCP服务器申请大量的IP地址，导致DHCP服务器地址池中的地址耗尽，无法为合法的DHCP客户端分配IP地址，或导致DHCP服务器消耗过多的系统资源，无法处理正常业务。DHCP报文字段的相关内容请参见“[1.3 DHCP报文格式](#)”。

如果封装 DHCP 请求报文的数据帧的源 MAC 地址各不相同，则通过 **mac-address max-mac-count** 命令限制端口可以学习到的 MAC 地址数，并配置学习到的 MAC 地址数达到最大值时，丢弃源 MAC 地址不在 MAC 地址表里的报文，能够避免攻击者申请过多的 IP 地址，在一定程度上缓解 DHCP 饿死攻击。此时，不存在 DHCP 饿死攻击的端口下的 DHCP 客户端可以正常获取 IP 地址，但存在 DHCP 饿死攻击的端口下的 DHCP 客户端仍可能无法获取 IP 地址。

如果封装 DHCP 请求报文的数据帧的 MAC 地址都相同，则通过 **mac-address max-mac-count** 命令无法防止 DHCP 饿死攻击。在这种情况下，需要开启 DHCP Snooping 的 MAC 地址检查功能。开启该功能后，DHCP Snooping 设备检查接收到的 DHCP 请求报文中的 chaddr 字段和数据帧的源 MAC 地址字段是否一致。如果一致，则认为该报文合法，将其转发给 DHCP 服务器；如果不一致，则丢弃该报文。**mac-address max-mac-count** 命令的详细介绍，请参见“二层技术-以太网交换”中的“MAC 地址表”。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 开启 DHCP Snooping 的 MAC 地址检查功能。



## **dhcp snooping check mac-address**

缺省情况下，DHCP Snooping 的 MAC 地址检查功能处于关闭状态。

### 5.9.2 配置防止伪造DHCP请求方向报文攻击

#### 1. 功能简介

本功能用来检查 DHCP 续约报文、DHCP-DECLINE 和 DHCP-RELEASE 三种 DHCP 请求方向的报文，以防止非法客户端伪造这三种报文对 DHCP 服务器进行攻击。

伪造 DHCP 续约报文攻击是指攻击者冒充合法的 DHCP 客户端，向 DHCP 服务器发送伪造的 DHCP 续约报文，导致 DHCP 服务器和 DHCP 客户端无法按照自己的意愿及时释放 IP 地址租约。如果攻击者冒充不同的 DHCP 客户端发送大量伪造的 DHCP 续约报文，则会导致大量 IP 地址被长时间占用，DHCP 服务器没有足够的地址分配给新的 DHCP 客户端。

伪造 DHCP-DECLINE/DHCP-RELEASE 报文攻击是指攻击者冒充合法的 DHCP 客户端，向 DHCP 服务器发送伪造的 DHCP-DECLINE/DHCP-RELEASE 报文，导致 DHCP 服务器错误终止 IP 地址租约。

在 DHCP Snooping 设备上开启 DHCP 请求方向报文检查功能，可以有效地防止伪造 DHCP 请求方向报文攻击。如果开启了该功能，则 DHCP Snooping 设备接收到上述报文后，检查本地是否存在与请求方向报文匹配的 DHCP Snooping 表项。若存在，则接收报文信息与 DHCP Snooping 表项信息一致时，认为该报文为合法的 DHCP 请求方向报文，将其转发给 DHCP 服务器；不一致时，认为该报文为伪造的 DHCP 请求方向报文，将其丢弃。若不存在，则认为该报文合法，将其转发给 DHCP 服务器。

#### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 开启 DHCP Snooping 的 DHCP 请求方向报文检查功能。

```
dhcp snooping check request-message
```

缺省情况下，DHCP Snooping 的 DHCP 请求方向报文检查功能处于关闭状态。

### 5.9.3 开启DHCP Snooping报文阻断功能

#### 1. 功能简介

在某些组网环境下，用户需要在 DHCP Snooping 设备的某一端口上丢弃该端口收到的所有 DHCP 请求方向报文，而又不影响其他端口正常接收 DHCP 报文。这时，用户可以在该端口上开启 DHCP Snooping 报文阻断功能。

当端口上开启了 DHCP Snooping 报文阻断功能后，该端口收到的所有 DHCP 请求方向的报文都将被丢弃。

#### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 开启 DHCP Snooping 报文阻断功能。

```
dhcp snooping deny
```

缺省情况下，DHCP Snooping 报文阻断功能处于关闭状态。

## 5.10 开启DHCP Snooping日志信息功能

### 1. 功能简介

DHCP Snooping 日志可以方便管理员定位问题和解决问题。DHCP Snooping 设备生成 DHCP Snooping 日志信息会交给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

### 2. 配置限制和指导

当 DHCP Snooping 设备输出大量日志信息时，可能会降低设备性能。为了避免该情况的发生，用户可以关闭 DHCP Snooping 日志信息功能，使得 DHCP Snooping 设备不再输出日志信息。

### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 DHCP Snooping 日志信息功能。

```
dhcp snooping log enable
```

缺省情况下，DHCP Snooping 日志信息功能处于关闭状态。

## 5.11 关闭接口的DHCP Snooping功能

### 1. 功能简介

当管理员在设备或 VLAN 中开启 DHCP Snooping 功能后，该设备或整个 VLAN 内的所有接口也都开启了 DHCP Snooping 功能。为了灵活控制 DHCP Snooping 功能生效的接口范围，用户可以通过本功能关闭某个接口上的 DHCP Snooping 功能。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图

```
interface interface-type interface-number
```

- (3) 关闭接口的 DHCP Snooping 功能。

```
dhcp snooping disable
```

缺省情况下，当接口所在 VLAN 或设备上已经开启 DHCP Snooping 功能，接口的 DHCP Snooping 功能是开启的；当接口所在 VLAN 或设备上未开启 DHCP Snooping 功能，接口的 DHCP Snooping 功能是关闭的。



# 5.12 DHCP 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 DHCP 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 DHCP Snooping 的统计信息。

表5-3 DHCP Snooping 显示和维护

操作	命令
显示DHCP Snooping表项信息	<b>display dhcp snooping binding</b> [ ip ip-address [ vlan vlan-id ] ] [ verbose ]
显示DHCP Snooping表项备份信息	<b>display dhcp snooping binding database</b>
显示DHCP Snooping上Option 82的配置信息	<b>display dhcp snooping information</b> { all   interface interface-type interface-number }
显示DHCP Snooping设备上的DHCP报文统计信息	<b>display dhcp snooping packet statistics</b> [ slot slot-number ]
显示信任端口信息	<b>display dhcp snooping trust</b>
清除DHCP Snooping表项	<b>reset dhcp snooping binding</b> { all   ip ip-address [ vlan vlan-id ] }
清除DHCP Snooping设备上的DHCP报文统计信息	<b>reset dhcp snooping packet statistics</b> [ slot slot-number ]

# 5.13 DHCP Snooping典型配置举例

## 5.13.1 全局开启DHCP Snooping配置举例

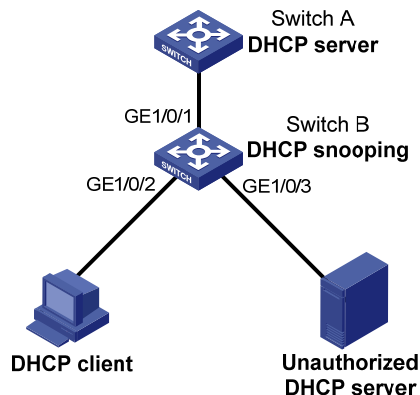
### 1. 组网需求

Switch B 通过以太网端口 GigabitEthernet1/0/1 连接到合法 DHCP 服务器，通过以太网端口 GigabitEthernet1/0/3 连接到非法 DHCP 服务器，通过 GigabitEthernet1/0/2 连接到 DHCP 客户端。要求：

- 与合法 DHCP 服务器相连的端口可以转发 DHCP 服务器的响应报文，而其他端口不转发 DHCP 服务器的响应报文。
- 记录 DHCP-REQUEST 报文和信任端口收到的 DHCP-ACK 报文中 DHCP 客户端 IP 地址及 MAC 地址的绑定信息。

## 2. 组网图

图5-3 DHCP Snooping 组网示意图



## 3. 配置步骤

# 全局开启 DHCP Snooping 功能。

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

# 设置 GigabitEthernet1/0/1 端口为信任端口。

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

# 在 GigabitEthernet1/0/2 上开启 DHCP Snooping 表项功能。

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

## 4. 验证配置

配置完成后，DHCP 客户端只能从合法 DHCP 服务器获取 IP 地址和其它配置信息，非法 DHCP 服务器无法为 DHCP 客户端分配 IP 地址和其他配置信息。且使用 **display dhcp snooping binding** 可查询到获取到的 DHCP Snooping 表项。

### 5.13.2 按VLAN开启DHCP Snooping配置举例

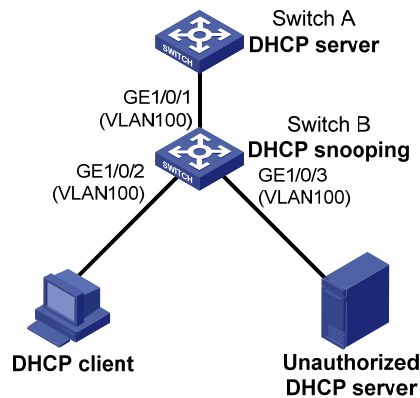
#### 1. 组网需求

Switch B 通过以太网端口 GigabitEthernet1/0/1 连接到合法 DHCP 服务器，通过以太网端口 GigabitEthernet1/0/3 连接到非法 DHCP 服务器，通过 GigabitEthernet1/0/2 连接到 DHCP 客户端。  
要求：

- VLAN 100 上与合法 DHCP 服务器相连的端口可以转发 DHCP 服务器的响应报文，而其他端口不转发 DHCP 服务器的响应报文。
- 记录 DHCP-REQUEST 报文和信任端口收到的 DHCP-ACK 报文中 DHCP 客户端 IP 地址及 MAC 地址的绑定信息。

## 2. 组网图

图5-4 按 VLAN 开启 DHCP Snooping 配置组网示意图



## 3. 配置步骤

# 配置端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 为 Access 端口，允许 VLAN 100 通过。

```
<SwitchB> system-view
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[SwitchB-vlan100] quit
```

# 在 VLAN100 内开启 DHCP Snooping 功能。

```
[SwitchB] dhcp snooping enable vlan 100
```

# 指定端口 GigabitEthernet1/0/1 为 VLAN 100 下 DHCP Snooping 功能的信任端口。

```
[SwitchB] vlan 100
[SwitchB-vlan100] dhcp snooping trust gigabitethernet 1/0/1
```

# 在 VLAN 100 内开启 DHCP Snooping 表项记录功能。

```
[SwitchB-vlan100] dhcp snooping binding record
[SwitchB-vlan100] quit
```

## 4. 验证配置

配置完成后，DHCP 客户端只能从合法 DHCP 服务器获取 IP 地址和其它配置信息，非法 DHCP 服务器无法为 DHCP 客户端分配 IP 地址和其他配置信息。且使用 **display dhcp snooping binding** 可查询到获取到的 DHCP Snooping 表项。

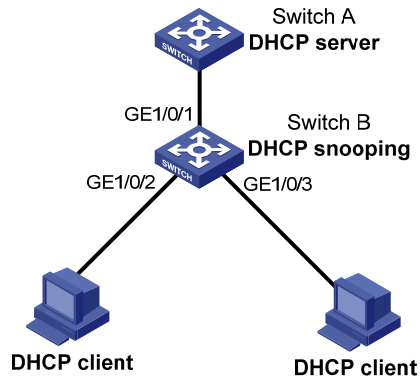
### 5.13.3 DHCP Snooping支持Option 82 配置举例

#### 1. 组网需求

- Switch B 上开启 DHCP Snooping 功能，并支持 Option 82 功能；
- 对包含 Option 82 的请求报文的处理策略为 **replace**；
- 在 GigabitEthernet1/0/2 上配置 Circuit ID 填充内容为 company001，Remote ID 填充内容为 device001；
- 在 GigabitEthernet1/0/3 上配置 Circuit ID 以 verbose 模式填充，接入节点标识为 **sysname**，填充格式为 ASCII 格式，Remote ID 填充内容为 device001；

## 2. 组网图

图5-5 DHCP Snooping 支持 Option 82 配置示意图



## 3. 配置步骤

# 开启 DHCP Snooping 功能。

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

# 设置 GigabitEthernet1/0/1 端口为信任端口。

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

# 在 GigabitEthernet1/0/2 上配置 DHCP Snooping 支持 Option 82 功能。

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] dhcp snooping information enable
[SwitchB-GigabitEthernet1/0/2] dhcp snooping information strategy replace
[SwitchB-GigabitEthernet1/0/2] dhcp snooping information circuit-id string company001
[SwitchB-GigabitEthernet1/0/2] dhcp snooping information remote-id string device001
[SwitchB-GigabitEthernet1/0/2] quit
```

# 在端口 GigabitEthernet1/0/3 上配置 DHCP Snooping 支持 Option 82 功能。

```
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] dhcp snooping information enable
[SwitchB-GigabitEthernet1/0/3] dhcp snooping information strategy replace
[SwitchB-GigabitEthernet1/0/3] dhcp snooping information circuit-id verbose node-identifier
sysname format ascii
[SwitchB-GigabitEthernet1/0/3] dhcp snooping information remote-id string device001
```

## 4. 验证配置

配置完成后，使用 **display dhcp snooping information** 命令可查看到 DHCP Snooping 在端口 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 上 Option 82 的配置信息。

# 6 BOOTP客户端

## 6.1 BOOTP客户端简介

### 6.1.1 BOOTP客户端的应用环境

BOOTP 是 Bootstrap Protocol（自举协议）的简称。指定设备的接口作为 BOOTP 客户端后，该接口可以通过 BOOTP 协议从 BOOTP 服务器获取 IP 地址等信息，从而方便用户配置。

使用 BOOTP 协议时，管理员需要在 BOOTP 服务器上为每个 BOOTP 客户端配置 BOOTP 参数文件，该文件包括 BOOTP 客户端的 MAC 地址及其对应的 IP 地址等信息。当 BOOTP 客户端向 BOOTP 服务器发起请求时，服务器会查找 BOOTP 参数文件，并返回相应的配置信息。

由于 BOOTP 协议需要在 BOOTP 服务器上为每个客户端事先配置参数文件，BOOTP 一般运行在相对稳定的环境中。当网络变化频繁时，推荐采用 DHCP 协议。

由于 DHCP 服务器可以与 BOOTP 客户端进行交互，因此用户可以不配置 BOOTP 服务器，而使用 DHCP 服务器为 BOOTP 客户端分配 IP 地址。

### 6.1.2 IP地址动态获取过程

BOOTP 客户端从 BOOTP 服务器动态获取 IP 地址的具体过程如下：

- (1) BOOTP 客户端以广播方式发送 BOOTP 请求报文，其中包含了 BOOTP 客户端的 MAC 地址；
- (2) BOOTP 服务器接收到请求报文后，根据报文中的 BOOTP 客户端 MAC 地址，从配置文件数据库中查找对应的 IP 地址等信息，并向客户端返回包含这些信息的 BOOTP 响应报文；
- (3) BOOTP 客户端从接收到的响应报文中即可获得 IP 地址等信息。

在下面的 IP 地址动态获取过程中，BOOTP 服务器的功能可以用 DHCP 服务器替代。

### 6.1.3 协议规范

与 BOOTP 相关的协议规范有：

- RFC 951: Bootstrap Protocol (BOOTP)
- RFC 2132: DHCP Options and BOOTP Vendor Extensions
- RFC 1542: Clarifications and Extensions for the Bootstrap Protocol

## 6.2 配置接口通过BOOTP协议获取IP地址

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

BOOTP 客户端中对于接口的相关配置，目前只能在 VLAN 接口上进行。

- (3) 配置接口通过 BOOTP 协议获取 IP 地址。

**ip address bootp-alloc**

缺省情况下，接口不通过 BOOTP 协议获取 IP 地址。

## 6.3 BOOTP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 BOOTP 客户端的运行情况，通过查看显示信息验证配置的效果。

表6-1 BOOTP 客户端显示和维护

操作	命令
显示BOOTP客户端的相关信息	<b>display bootp client</b> [ <b>interface</b> <i>interface-type</i> <i>interface-number</i> ]

## 6.4 BOOTP客户端典型配置举例

### 6.4.1 BOOTP客户端典型配置举例

#### 1. 组网需求

Switch B 的端口（属于 VLAN10）接入局域网，VLAN 接口 10 通过 BOOTP 协议从 DHCP 服务器获取 IP 地址。

#### 2. 组网图

如 [图 2-2](#) 所示。

#### 3. 配置步骤

下面只列出 [图 2-2](#) 中，作为客户端的Switch B的配置。

# 配置 VLAN 接口 10 通过 BOOTP 动态获取地址。

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 10
[SwitchB-Vlan-interface10] ip address bootp-alloc
```

通过 **display bootp client** 命令可以查看 BOOTP 客户端申请到的 IP 地址。



#### 说明

为了使BOOTP客户端能从DHCP服务器获得IP地址，还需要在DHCP服务器上进行一些配置，具体内容请参见“[2.20 DHCP服务器典型配置举例](#)”。

# 目 录

1 域名解析.....	1-1
1.1 域名解析简介.....	1-1
1.1.1 域名解析类型.....	1-1
1.1.2 静态域名解析.....	1-1
1.1.3 动态域名解析.....	1-1
1.1.4 DNS代理.....	1-2
1.1.5 DNS spoofing.....	1-4
1.2 域名解析配置任务简介.....	1-5
1.3 配置DNS客户端.....	1-5
1.3.1 配置静态域名解析.....	1-5
1.3.2 配置动态域名解析.....	1-5
1.4 配置DNS proxy.....	1-6
1.5 配置DNS spoofing.....	1-7
1.6 配置DNS报文的源接口.....	1-8
1.7 配置DNS信任接口.....	1-8
1.8 指定DNS报文的DSCP优先级.....	1-9
1.9 域名解析显示和维护.....	1-9
1.10 IPv4 域名解析典型配置举例.....	1-9
1.10.1 静态域名解析配置举例.....	1-9
1.10.2 动态域名解析配置举例.....	1-10
1.10.3 DNS proxy配置举例.....	1-15
1.11 IPv6 域名解析典型配置举例.....	1-16
1.11.1 静态域名解析配置举例.....	1-16
1.11.2 动态域名解析配置举例.....	1-17
1.11.3 DNS proxy配置举例.....	1-21
1.12 域名解析常见故障处理.....	1-22
1.12.1 无法解析到正确的IP地址.....	1-22
1.12.2 无法解析到正确的IPv6 地址.....	1-22

# 1 域名解析

## 1.1 域名解析简介

DNS（Domain Name System，域名系统）是一种用于 TCP/IP 应用程序的分布式数据库，提供域名与 IP 地址之间的转换。通过域名系统，用户进行某些应用时，可以直接使用便于记忆的、有意义的域名，而由网络中的域名解析服务器将域名解析为正确的 IP 地址。

### 1.1.1 域名解析类型

域名解析分为静态域名解析和动态域名解析，二者可以配合使用。在解析域名时，首先采用静态域名解析（查找静态域名解析表），如果静态域名解析不成功，再采用动态域名解析。由于动态域名解析需要域名服务器（DNS server）的配合，会花费一定的时间，因而可以将一些常用的域名放入静态域名解析表中，这样可以大大提高域名解析效率。

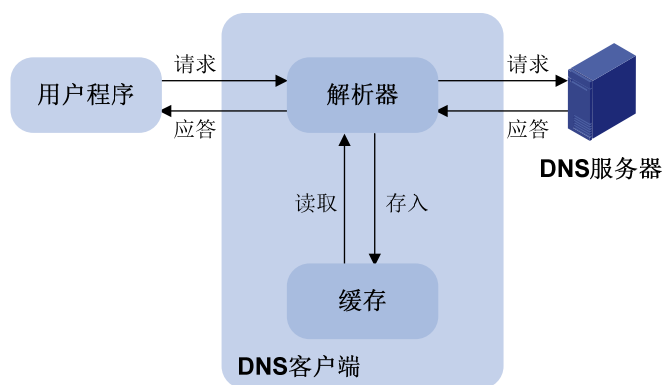
### 1.1.2 静态域名解析

静态域名解析就是手工建立域名和 IP 地址之间的对应关系。当用户使用域名进行某些应用（如 telnet 应用）时，系统查找静态域名解析表，从中获取指定域名对应的 IP 地址。

### 1.1.3 动态域名解析

#### 1. 体系结构

图1-1 动态域名解析



用户程序、DNS客户端及域名服务器的关系如 图1-1 所示，其中解析器和缓存构成DNS客户端。用户程序、DNS客户端在同一台设备上，而DNS客户端和域名服务器一般分布在两台设备上。

目前，设备只能作为 DNS 客户端，不能作为 DNS 服务器。





## 说明

如果域名服务器上配置了域名的别名，设备也可以通过别名来解析主机的 IP 地址。

## 2. 解析过程

动态域名解析通过向域名服务器查询域名和 IP 地址之间的对应关系来实现将域名解析为 IP 地址。动态域名解析过程如下：

- (1) 当用户使用域名进行某些应用时，用户程序首先向 DNS 客户端中的解析器发出请求。
- (2) DNS 客户端收到请求后，首先查询本地的域名缓存。如果存在已解析成功的映射项，就将域名对应的 IP 地址返回给用户程序；如果未发现所要查找的映射项，就向域名服务器发送查询请求。
- (3) 域名服务器首先从自己的数据库中查找域名对应的 IP 地址。如果判断该域名不属于本域范围，就将请求交给其他域名服务器处理，直到完成解析，并将解析的结果返回给 DNS 客户端。
- (4) DNS 客户端收到域名服务器的响应报文后，将解析结果返回用户程序。

## 3. 缓存功能

动态域名解析支持缓存功能。每次动态解析成功的域名与 IP 地址的映射均存放在 DNS 客户端的动态域名缓存区中，当下一次查询相同域名的时候，就可以直接从缓存区中读取，不用再向域名服务器进行请求。缓存区中的映射在一段时间后会老化而被删除，以保证及时从域名服务器得到最新的内容。老化时间由域名服务器设置，DNS 客户端从域名服务器的应答报文中获得老化时间。

## 4. 域名后缀列表功能

动态域名解析支持域名后缀列表功能。用户可以预先设置一些域名后缀，在域名解析的时候，用户只需要输入域名的部分字段，系统会自动将输入的域名加上不同的后缀进行解析。例如，用户想查询域名 **aabbcc.com**，那么可以先在后缀列表中配置 **com**，然后输入 **aabbcc** 进行查询，系统会自动将输入的域名与后缀连接成 **aabbcc.com** 进行查询。

使用域名后缀的时候，根据用户输入域名方式的不同，查询方式分成以下几种情况：

- 如果用户输入的域名中没有“.”，比如 **aabbcc**，系统认为这是一个主机名，会首先加上域名后缀进行查询，如果所有加后缀的域名查询都失败，将使用最初输入的域名（如 **aabbcc**）进行查询。
- 如果用户输入的域名中间有“.”，比如 **www.aabbcc**，系统直接用它进行查询，如果查询失败，再依次加上各个域名后缀进行查询。
- 如果用户输入的域名最后有“.”，比如 **aabbcc.com.**，表示不需要进行域名后缀添加，系统直接用输入的域名进行查询，不论成功与否都直接返回结果。就是说，如果用户输入的字符中最后一个字符为“.”，就只根据用户输入的字符进行查找，而不会去匹配用户预先设置的域名后缀，因此最后这个“.”，也被称为查找终止符。带有查询终止符的域名，称为 FQDN（Fully Qualified Domain Name，完全合格域名）。

### 1.1.4 DNS代理

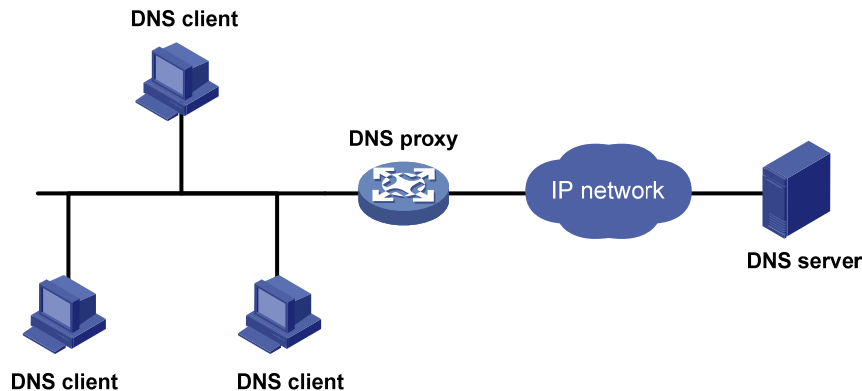
DNS 代理（DNS proxy）用来在 DNS client 和 DNS server 之间转发 DNS 请求和应答报文。局域网内的 DNS client 把 DNS proxy 当作 DNS server，将 DNS 请求报文发送给 DNS proxy。DNS proxy

将该请求报文转发到真正的 DNS server，并将 DNS server 的应答报文返回给 DNS client，从而实现域名解析。

使用 DNS proxy 功能后，当 DNS server 的地址发生变化时，只需改变 DNS proxy 上的配置，无需改变局域网内每个 DNS client 的配置，从而简化了网络管理。

DNS proxy 的典型应用环境如 图 1-2 所示。

图1-2 DNS 代理典型组网应用



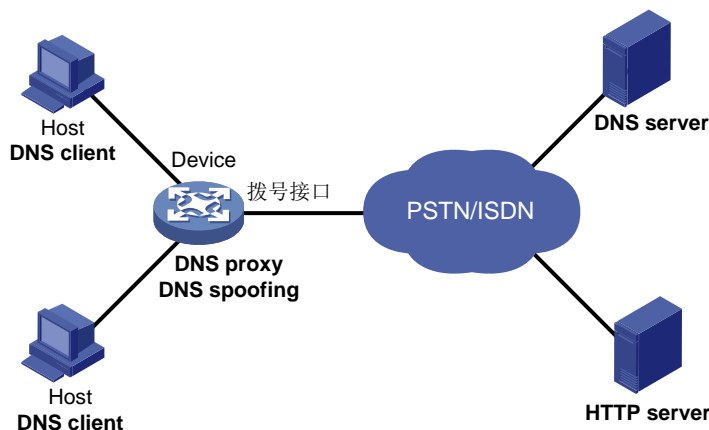
DNS 代理的工作过程如下：

- (1) DNS client 把 DNS proxy 当作 DNS server，将 DNS 请求报文发送给 DNS proxy，即请求报文的地址为 DNS proxy 的 IP 地址。
- (2) DNS proxy 收到请求报文后，首先查找本地的静态域名解析表和动态域名解析缓存表，如果存在请求的信息，则 DNS proxy 直接通过 DNS 应答报文将域名解析结果返回给 DNS client。
- (3) 如果不存在请求的信息，则 DNS proxy 将报文转发给 DNS server，通过 DNS server 进行域名解析。
- (4) DNS proxy 收到 DNS server 的应答报文后，记录域名解析的结果，并将报文转发给 DNS client。DNS client 利用域名解析的结果进行相应的处理。

只有 DNS proxy 上存在域名服务器地址，并存在到达域名服务器的路由，DNS proxy 才会向 DNS server 发送域名解析请求。

### 1.1.5 DNS spoofing

图1-3 DNS spoofing 典型应用场景



DNS spoofing（DNS欺骗）主要应用于图 1-3 所示的拨号网络。在该网络中：

- Device 通过拨号接口连接到 PSTN/ISDN 等拨号网络。只有存在通过拨号接口转发的报文时，才会触发拨号接口建立连接。
- Device 作为 DNS proxy。在 Host 上将 Device 指定为 DNS 服务器；拨号接口建立连接后，Device 通过 DHCP 等方式动态获取 DNS 服务器地址。

Device 上未开启 DNS spoofing 功能时，Device 接收到 Host 发送的域名解析请求报文后，如果不存在对应的域名解析表项，则需要向 DNS server 发送域名解析请求。但是，由于此时拨号接口尚未建立连接，Device 上不存在 DNS server 地址，Device 不会向 DNS server 发送域名解析请求，也不会应答 DNS client 的请求。从而导致域名解析失败，且没有流量触发拨号接口建立连接。

DNS spoofing 功能可以解决上述问题。使能 DNS spoofing 功能后，即便 Device 上不存在 DNS server 地址或到达 DNS server 的路由，Device 也会利用指定的 IP 地址作为域名解析结果，应答 DNS client 的域名解析请求。DNS client 后续发送的报文可以用来触发拨号接口建立连接。

图 1-3 所示网络中，Host 访问 HTTP server 的报文处理流程为：

- (1) Host 通过域名访问 HTTP server 时，首先向 Device 发送域名解析请求，将 HTTP server 的域名解析为 IP 地址。
- (2) Device 接收到域名解析请求后，如果拨号接口尚未建立连接，Device 上不存在 DNS server 地址，或者设备上配置的 DNS server 地址均不可达，则 Device 利用 DNS spoofing 中指定的 IP 地址作为域名解析结果，应答 DNS client 的域名解析请求。该域名解析应答的老化时间为 0。并且，应答的 IP 地址满足如下条件：Device 上存在到达该 IP 地址的路由，且路由的出接口为拨号接口。
- (3) Host 接收到 Device 的应答报文后，向应答的 IP 地址发送 HTTP 请求。
- (4) Device 通过拨号接口转发 HTTP 请求时，触发拨号接口建立连接，并通过 DHCP 等方式动态获取 DNS server 的地址。
- (5) 域名解析应答老化后，Host 再次发送域名解析请求。
- (6) 之后，Device 的处理过程与 DNS proxy 工作过程相同，请参见“[1.1.4 DNS 代理](#)”。
- (7) Host 获取到正确的 HTTP server 地址后，可以正常访问 HTTP server。



## 说明

由于 DNS spoofing 功能指定的 IP 地址并不是待解析域名对应的 IP 地址，为了防止 DNS client 上保存错误的域名解析表项，该 IP 地址对应域名解析应答的老化时间为 0。

## 1.2 域名解析配置任务简介

域名解析配置任务如下：

(1) [配置DNS客户端](#)

请至少选择其中一项进行配置。

○ [配置静态域名解析](#)

○ [配置动态域名解析](#)

(2) （可选）[配置DNS proxy](#)

(3) （可选）[配置DNS spoofing](#)

本功能用于拨号网络。

(4) （可选）[配置DNS报文的源接口](#)

(5) （可选）[配置DNS信任接口](#)

(6) （可选）[指定DNS报文的DSCP优先级](#)

## 1.3 配置DNS客户端

### 1.3.1 配置静态域名解析

#### 1. 配置限制和指导

一个主机名只能对应一个 IPv4 地址和 IPv6 地址。

最多可以配置 2048 个主机名和地址的对应关系。

#### 2. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 配置主机名和对应的地址。请至少选择其中一项进行配置。

（IPv4 网络）

```
ip host host-name ip-address
```

（IPv6 网络）

```
ipv6 host host-name ipv6-address
```

### 1.3.2 配置动态域名解析

#### 1. 配置限制和指导

- 设备上允许配置的域名服务器数目限制为：

- 系统视图下，最多可以配置 6 个域名服务器的 IPv4 地址。
- 系统视图下，最多可以配置 6 个域名服务器的 IPv6 地址。
- 接口视图下，最多可以配置 6 个域名服务器的 IPv4 地址。
- 如果同时配置域名服务器的 IPv4 地址和 IPv6 地址，DNS 客户端向域名服务器发送请求的处理方式如下：
  - 查询主机名对应的 IPv4 地址时，优先向域名服务器的 IPv4 地址发送查询请求。如果查询失败，则再向域名服务器的 IPv6 地址发送查询请求；
  - 查询主机名对应的 IPv6 地址时，优先向域名服务器的 IPv6 地址发送查询请求。如果查询失败，则再向域名服务器的 IPv4 地址发送查询请求。
- 域名服务器的优先级顺序为：系统视图下配置的域名服务器优先级高于接口视图下配置的域名服务器；先配置的域名服务器优先级高于后配置的域名服务器；设备上手工配置的域名服务器优先级高于通过 DHCP 等方式动态获取的域名服务器。设备首先向优先级最高的域名服务器发送查询请求，失败后再根据优先级从高到低的次序向其他域名服务器发送查询请求。
- 配置域名解析后缀时，需要注意：
  - 最多可以配置 16 个域名后缀。
  - 添加域名后缀的优先级顺序为：先配置的域名后缀优先级高于后配置的域名后缀；设备上手工配置的域名后缀优先级高于通过 DHCP 等方式动态获取的域名后缀。设备首先添加优先级最高的域名后缀，查询失败后再根据优先级从高到低的次序添加其他域名后缀。

## 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) （可选）配置域名后缀。

```
dns domain domain-name
```

缺省情况下，未配置域名后缀，即只根据用户输入的域名信息进行解析。

- (3) 配置域名服务器的地址。

（IPv4 网络）

```
dns server ip-address
```

（IPv6 网络）

```
ipv6 dns server ipv6-address [ interface-type interface-number ]
```

缺省情况下，未配置域名服务器的地址。

## 1.4 配置DNS proxy

### 1. 配置限制和指导

可以指定多个 DNS server。DNS proxy 接收到客户端的查询请求后，首先向优先级最高的 DNS server 转发查询请求，失败后再依次向其他 DNS server 转发查询请求。

DNS proxy 可同时配置域名服务器的 IPv4 地址和 IPv6 地址。无论 DNS proxy 接收到的查询请求是来自 IPv4 客户端还是来自 IPv6 客户端，DNS proxy 都会按照优先级顺序向域名服务器的 IPv4 地址和 IPv6 地址转发查询请求。如果查询请求是 IPv4 报文，则优先向域名服务器的 IPv4 地址转发查询请求。如果查询请求是 IPv6 报文，则优先向域名服务器的 IPv6 地址转发查询请求。

## 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 DNS proxy 功能。

```
dns proxy enable
```

缺省情况下，DNS proxy 功能处于关闭状态。

- (3) 配置域名服务器的地址。

(IPv4 网络)

```
dns server ip-address
```

(IPv6 网络)

```
ipv6 dns server ipv6-address [ interface-type interface-number ]
```

缺省情况下，未配置域名服务器的地址。

## 1.5 配置DNS spoofing

### 1. 配置限制和指导

只能配置 1 个 DNS spoofing 应答的 IPv4 地址和 1 个 DNS spoofing 应答的 IPv6 地址。重复配置时，新的配置会覆盖原有配置。

DNS spoofing 功能生效时，即使设备上配置了静态域名解析，也会使用 DNS spoofing 指定的 IP 地址来应答 DNS 请求。

### 2. 配置准备

设备上启用了 DNS proxy 功能。

设备上未指定域名服务器地址或不存在到达域名服务器的路由。

### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 启用 DNS proxy 功能。

```
dns proxy enable
```

缺省情况下，DNS proxy 功能处于关闭状态。

- (3) 开启 DNS Snooping 功能，并指定 DNS spoofing 应答地址。

(IPv4 网络)

```
dns spoofing ip-address
```

(IPv6 网络)

```
ipv6 dns spoofing ipv6-address
```

缺省情况下，未开启 DNS Snooping 功能。

## 1.6 配置DNS报文的源接口

### 1. 功能简介

缺省情况下，设备根据域名服务器的地址，通过路由表查找请求报文的出接口，并将该出接口的主 IP 地址作为发送到该服务器的 DNS 请求报文的源地址。根据域名服务器的地址不同，发送报文的源地址可能会发生变化。在某些特殊的组网环境中，域名服务器只应答来自特定源地址的 DNS 请求报文。这种情况下，必须指定 DNS 报文的源接口。如果为设备配置了 DNS 报文的源接口，则设备在发送 DNS 报文时，将固定使用该接口的主 IP 地址作为报文的源地址。

### 2. 配置限制和指导

发送 IPv4 DNS 报文时，将使用源接口的主 IPv4 地址作为 DNS 报文的源地址。发送 IPv6 DNS 报文时，将根据 RFC 3484 中定义的规则从源接口上选择 IPv6 地址作为 DNS 报文的源地址。如果源接口上未配置对应的地址，则将导致报文发送失败。

只能配置 1 个源接口。重复配置时，新的配置会覆盖原有配置。

### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 指定 DNS 报文的源接口。

```
dns source-interface interface-type interface-number
```

缺省情况下，未指定 DNS 报文的源接口。

## 1.7 配置DNS信任接口

### 1. 功能简介

缺省情况下，任意接口通过 DHCP 等协议动态获得的域名后缀和域名服务器信息都将作为有效信息，用于域名解析。如果网络攻击者通过 DHCP 服务器为设备分配错误的域名后缀和域名服务器地址，则会导致设备域名解析失败，或解析到错误的结果。通过本配置指定信任接口后，域名解析时只采用信任接口动态获得的域名后缀和域名服务器信息，非信任接口获得的信息不能用于域名解析，从而在一定程度上避免这类攻击。

### 2. 配置限制和指导

设备最多可以配置 128 个 DNS 信任接口。

### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 指定 DNS 信任接口。

```
dns trust-interface interface-type interface-number
```

缺省情况下，未指定任何接口为信任接口。



## 1.8 指定DNS报文的DSCP优先级

### 1. 功能简介

DSCP 优先级用来体现报文自身的优先等级，决定报文传输的优先程度。通过本配置可以指定设备发送的 DNS 报文的 DSCP 优先级。

### 2. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 指定 DNS 客户端或 DNS proxy 发出的 DNS 报文的 DSCP 优先级。

(IPv4 网络)

```
dns dscp dscp-value
```

缺省情况下，DNS 报文的 DSCP 优先级为 0。

(IPv6 网络)

```
ipv6 dns dscp dscp-value
```

缺省情况下，IPv6 DNS 报文的 DSCP 优先级为 0。

## 1.9 域名解析显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示域名解析配置后的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **reset** 命令可以清除动态域名缓存信息。

表1-1 域名解析显示和维护

操作	命令
显示域名后缀信息	<b>display dns domain [ dynamic ]</b>
显示域名解析表信息	<b>display dns host [ ip   ipv6 ]</b>
显示域名服务器的IPv4地址信息	<b>display dns server [ dynamic ]</b>
显示域名服务器的IPv6地址信息	<b>display ipv6 dns server [ dynamic ]</b>
清除动态域名解析缓存信息	<b>reset dns host [ ip   ipv6 ]</b>

## 1.10 IPv4域名解析典型配置举例

### 1.10.1 静态域名解析配置举例

#### 1. 组网需求

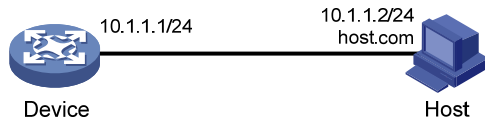
为了避免记忆复杂的 IP 地址，Device 希望通过便于记忆的主机名访问某一主机。在 Device 上手工配置 IP 地址对应的主机名，利用静态域名解析功能，就可以实现通过主机名访问该主机。

在本例中，Device 访问的主机 IP 地址为 10.1.1.2，主机名为 host.com。



## 2. 组网图

图1-4 静态域名解析配置组网图



## 3. 配置步骤

# 配置主机名 **host.com** 对应的 IP 地址为 **10.1.1.2**。

```
<Sysname> system-view
```

```
[Sysname] ip host host.com 10.1.1.2
```

# 执行 **ping host.com** 命令，Device 通过静态域名解析可以解析到 **host.com** 对应的 IP 地址为 **10.1.1.2**。

```
[Sysname] ping host.com
```

```
Ping host.com (10.1.1.2): 56 data bytes, press CTRL_C to break
```

```
56 bytes from 10.1.1.2: icmp_seq=0 ttl=255 time=1.000 ms
```

```
56 bytes from 10.1.1.2: icmp_seq=1 ttl=255 time=1.000 ms
```

```
56 bytes from 10.1.1.2: icmp_seq=2 ttl=255 time=1.000 ms
```

```
56 bytes from 10.1.1.2: icmp_seq=3 ttl=255 time=1.000 ms
```

```
56 bytes from 10.1.1.2: icmp_seq=4 ttl=255 time=2.000 ms
```

```
--- Ping statistics for host.com ---
```

```
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
```

```
round-trip min/avg/max/std-dev = 1.000/1.200/2.000/0.400 ms
```

## 1.10.2 动态域名解析配置举例

### 1. 组网需求

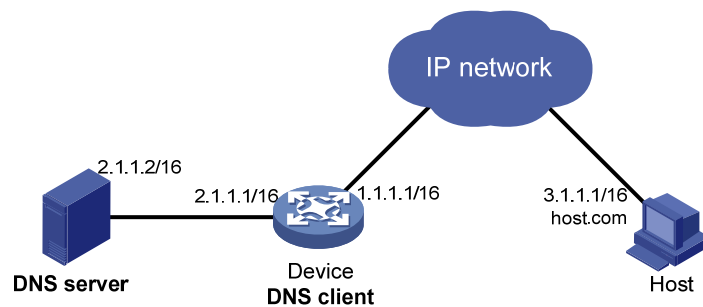
为了避免记忆复杂的 IP 地址，Device 希望通过便于记忆的域名访问某一主机。如果网络中存在域名服务器，则可以利用动态域名解析功能，实现通过域名访问主机。

在本例中：

- 域名服务器的 IP 地址是 **2.1.1.2/16**，域名服务器上存在 **com** 域，且 **com** 域中包含域名“**host**”和 IP 地址 **3.1.1.1/16** 的对应关系。
- Device 作为 DNS 客户端，使用动态域名解析功能，将域名解析为 IP 地址。
- Device 上配置域名后缀 **com**，以便简化访问主机时输入的域名，例如通过输入 **host** 即可访问域名为 **host.com**、IP 地址为 **3.1.1.1/16** 的主机 Host。

## 2. 组网图

图1-5 动态域名解析组网图



## 3. 配置步骤



### 说明

- 在开始下面的配置之前，假设备与主机之间的路由可达，设备和主机都已经配置完毕，接口IP地址如 [图 1-5](#) 所示。
- 不同域名服务器的配置方法不同，下面仅以 Windows Server 2008 R2 为例，说明域名服务器的配置方法。

### (1) 配置域名服务器

# 进入域名服务器配置界面。

在开始菜单中，选择[程序/管理工具/DNS]。

# 创建区域 com。

如 [图 1-6](#) 所示，右键点击[正向查找区域]，选择[新建区域]，按照提示创建新的区域com。

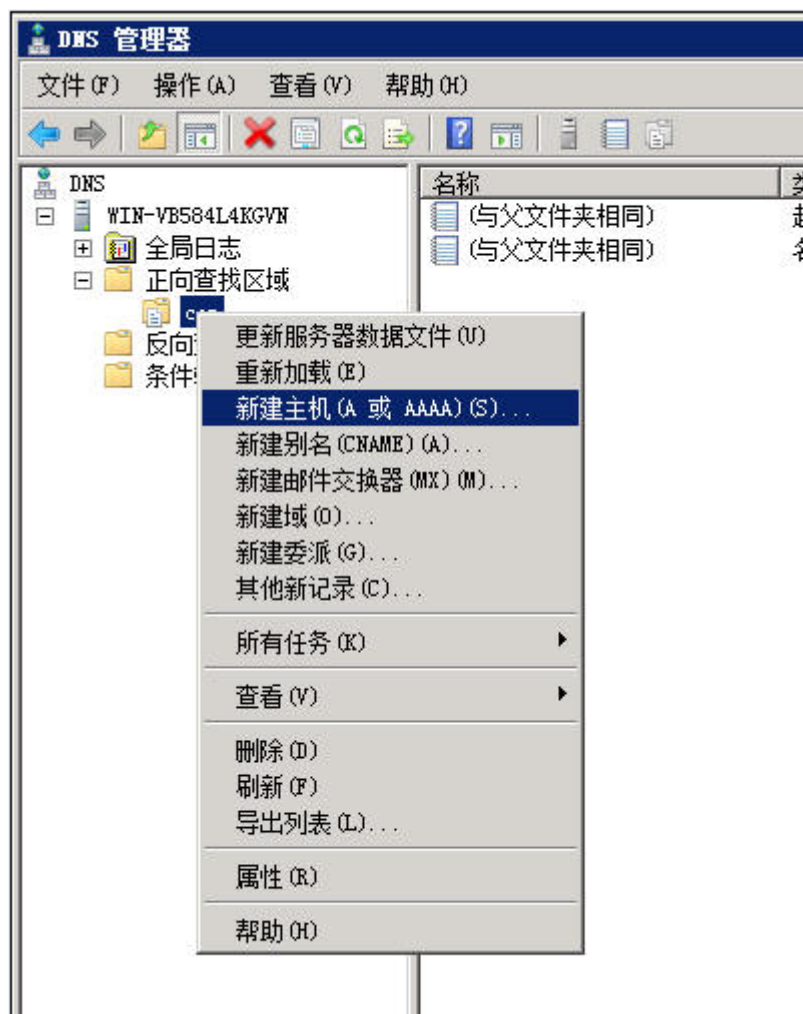
图1-6 创建区域



# 添加域名和 IP 地址的映射。

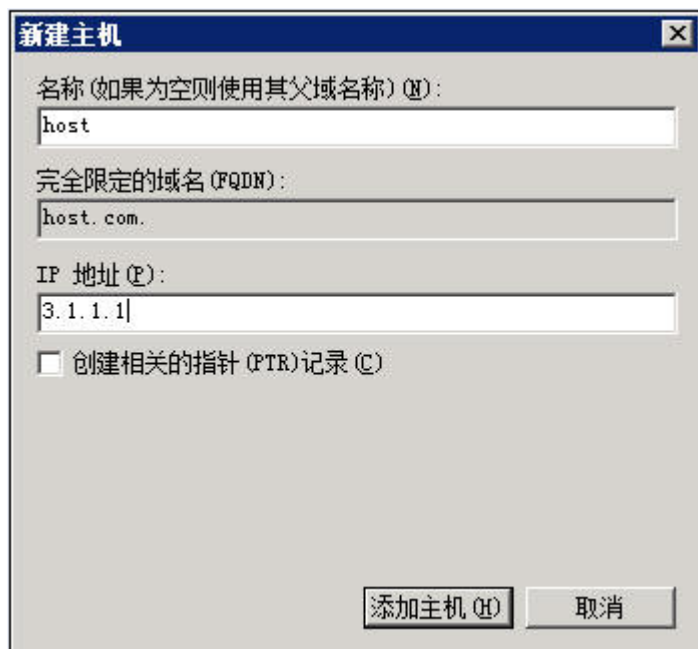
如 [图 1-7](#) 所示，右键点击区域[com]。

图1-7 新建主机



选择[新建主机]，弹出如 [图 1-8](#) 的对话框。按照 [图 1-8](#) 输入域名host和IP地址 3.1.1.1。单击<添加主机>可完成操作。

图1-8 添加域名和 IP 地址的映射



新建主机

名称 (如果为空则使用其父域名称) (N):  
host

完全限定的域名 (FQDN):  
host.com.

IP 地址 (I):  
3.1.1.1

☐ 创建相关的指针 (PTR) 记录 (C)

添加主机 (H) 取消

## (2) 配置 DNS 客户端 Device

```
<Sysname> system-view
```

```
# 配置域名服务器的 IP 地址为 2.1.1.2。
```

```
[Sysname] dns server 2.1.1.2
```

```
# 配置域名后缀 com。
```

```
[Sysname] dns domain com
```

## 4. 验证配置

# 在设备上执行 **ping host** 命令，可以 ping 通主机，且对应的目的地址为 3.1.1.1。

```
[Sysname] ping host
```

```
Ping host.com (3.1.1.1): 56 data bytes, press CTRL_C to break
```

```
56 bytes from 3.1.1.1: icmp_seq=0 ttl=255 time=1.000 ms
```

```
56 bytes from 3.1.1.1: icmp_seq=1 ttl=255 time=1.000 ms
```

```
56 bytes from 3.1.1.1: icmp_seq=2 ttl=255 time=1.000 ms
```

```
56 bytes from 3.1.1.1: icmp_seq=3 ttl=255 time=1.000 ms
```

```
56 bytes from 3.1.1.1: icmp_seq=4 ttl=255 time=2.000 ms
```

```
--- Ping statistics for host ---
```

```
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
```

```
round-trip min/avg/max/std-dev = 1.000/1.200/2.000/0.400 ms
```

### 1.10.3 DNS proxy配置举例

#### 1. 组网需求

某局域网内拥有多台设备，每台设备上都指定了域名服务器的 IP 地址，以便直接通过域名访问外部网络。当域名服务器的 IP 地址发生变化时，网络管理员需要更改局域网内所有设备上配置的域名服务器 IP 地址，工作量将会非常巨大。

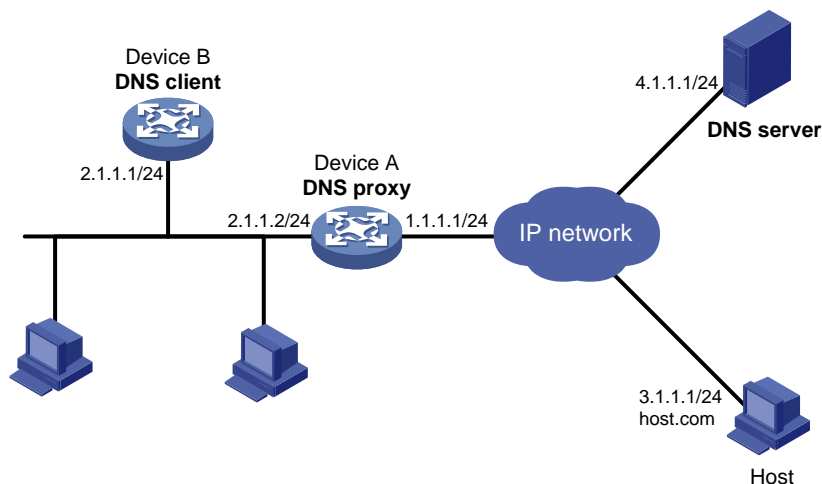
通过 DNS proxy 功能，可以大大减少网络管理员的工作量。当域名服务器 IP 地址改变时，只需更改 DNS proxy 上的配置，即可实现局域网内设备通过新的域名服务器解析域名。

在本例中，具体配置步骤为：

- (1) 局域网中的某台设备 Device A 配置为 DNS proxy，DNS proxy 上指定域名服务器 IP 地址为真正的域名服务器的地址 4.1.1.1。
- (2) 局域网中的其他设备（如 Device B）上，域名服务器的 IP 地址配置为 DNS proxy 的地址，域名解析报文将通过 DNS proxy 转发给真正的域名服务器。

#### 2. 组网图

图1-9 DNS proxy 组网图



#### 3. 配置步骤



##### 说明

在开始下面的配置之前，假设设备与域名服务器、主机之间的路由可达，并已按照 [图 1-9](#) 配置各接口的 IP 地址。

##### (1) 配置域名服务器

不同的域名服务器的配置方法不同。Windows Server 2008 R2 作为域名服务器时，配置方法请参见“[1.10.2 动态域名解析配置举例](#)”。

##### (2) 配置 DNS 代理 Device A

# 配置域名服务器的 IP 地址为 4.1.1.1。

```
<DeviceA> system-view
```

```
[DeviceA] dns server 4.1.1.1
# 开启 DNS proxy 功能。
[DeviceA] dns proxy enable
(3) 配置 DNS 客户端 Device B
<DeviceB> system-view
# 配置域名服务器的 IP 地址为 2.1.1.2。
[DeviceB] dns server 2.1.1.2
```

#### 4. 验证配置

# 在 Device B 上执行 **ping host.com** 命令，可以 ping 通主机，且对应的目的地址为 3.1.1.1。

```
[DeviceB] ping host.com
Ping host.com (3.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 3.1.1.1: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=2 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=4 ttl=255 time=2.000 ms

--- Ping statistics for host.com ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/1.200/2.000/0.400 ms
```

## 1.11 IPv6域名解析典型配置举例

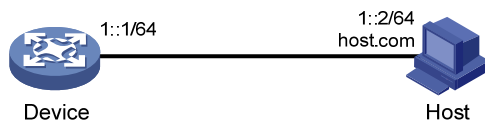
### 1.11.1 静态域名解析配置举例

#### 1. 组网需求

为了避免记忆复杂的 IPv6 地址，Device 希望通过便于记忆的主机名访问某一主机。在 Device 上手工配置 IPv6 地址对应的主机名，利用静态域名解析功能，就可以实现通过主机名访问该主机。在本例中，Device 访问的主机 IPv6 地址为 1::2，主机名为 host.com。

#### 2. 组网图

图1-10 静态域名解析配置组网图



#### 3. 配置步骤

# 配置主机名 host.com 对应的 IPv6 地址为 1::2。

```
<Sysname> system-view
[Sysname] ipv6 host host.com 1::2
```

# 执行 **ping ipv6 host.com** 命令，Device 通过静态域名解析可以解析到 host.com 对应的 IPv6 地址为 1::2。

```
[Sysname] ping ipv6 host.com
```

```

Ping6(56 data bytes) 1::1 --> 1::2, press CTRL_C to break
56 bytes from 1::2, icmp_seq=0 hlim=128 time=1.000 ms
56 bytes from 1::2, icmp_seq=1 hlim=128 time=0.000 ms
56 bytes from 1::2, icmp_seq=2 hlim=128 time=1.000 ms
56 bytes from 1::2, icmp_seq=3 hlim=128 time=1.000 ms
56 bytes from 1::2, icmp_seq=4 hlim=128 time=0.000 ms

--- Ping6 statistics for host.com ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.600/1.000/0.490 ms

```

## 1.11.2 动态域名解析配置举例

### 1. 组网需求

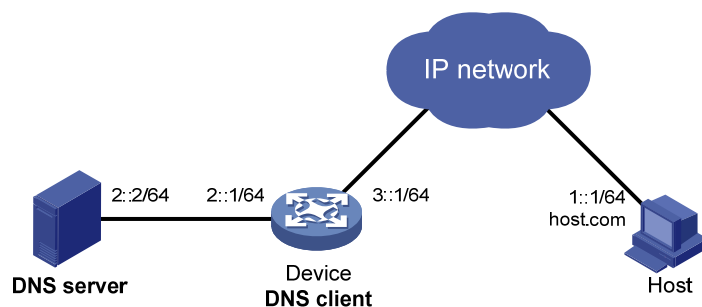
为了避免记忆复杂的 IPv6 地址，Device 希望通过便于记忆的域名访问某一主机。如果网络中存在域名服务器，则可以利用动态域名解析功能，实现通过域名访问主机。

在本例中：

- 域名服务器的 IPv6 地址是 2::2/64，域名服务器上存在 com 域，且 com 域中包含域名“host”和 IPv6 地址 1::1/64 的对应关系。
- Device 作为 DNS 客户端，使用动态域名解析功能，将域名解析为 IPv6 地址。
- Device 上配置域名后缀 com，以便简化访问主机时输入的域名，例如通过输入 host 即可访问域名为 host.com、IPv6 地址为 1::1/64 的主机 Host。

### 2. 组网图

图1-11 动态域名解析组网图



### 3. 配置步骤



说明

- 在开始下面的配置之前，假设设备与主机之间的路由可达，设备和主机都已经配置完毕，接口 IPv6 地址如 [图 1-11](#) 所示。
- 不同域名服务器的配置方法不同，下面仅以 Windows Server 2008 R2 为例，说明域名服务器的配置方法。配置之前，需确保 DNS 服务器支持 IPv6 DNS 功能，以便处理 IPv6 域名解析报文；且 DNS 服务器的接口可以转发 IPv6 报文。



(1) 配置域名服务器

# 进入域名服务器配置界面。

在开始菜单中，选择[程序/管理工具/DNS]。

# 创建区域 com。

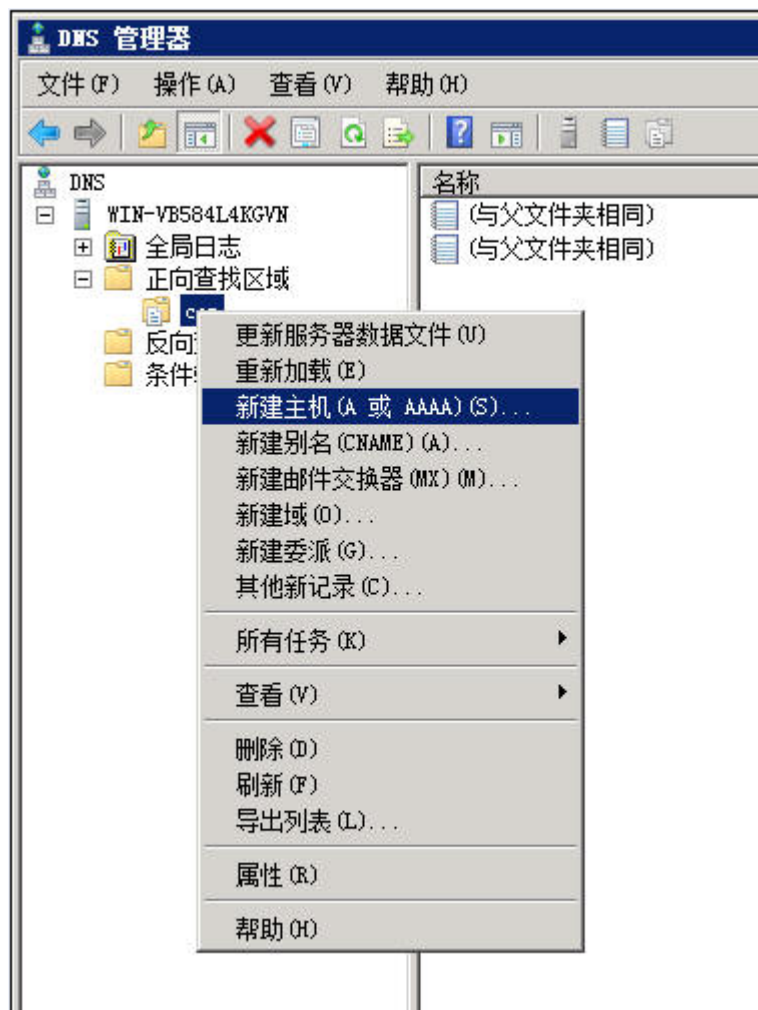
如 图 1-12 所示，右键单击[正向查找区域]，选择[新建区域]，按照提示创建新的区域com。

图1-12 创建区域



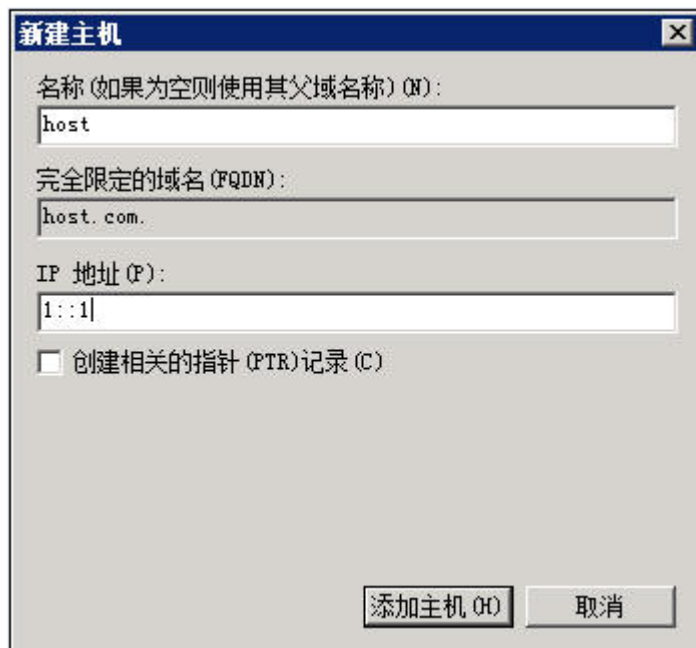
如 图 1-13 所示，右键单击区域[com]。

图1-13 新建主机



选择[新建主机]，弹出如 [图 1-14](#) 的对话框，输入域名和IPv6 地址 1::1。单击<添加主机>可完成操作。

图1-14 添加域名和 IPv6 地址的映射



## (2) 配置 DNS 客户端 Device

# 配置域名服务器的 IPv6 地址为 2::2。

```
<Device> system-view
```

```
[Device] ipv6 dns server 2::2
```

# 配置域名后缀 com。

```
[Device] dns domain com
```

## 4. 验证配置

# 在设备上执行 **ping ipv6 host** 命令，可以 ping 通主机，且对应的目的地址为 1::1。

```
[Device] ping ipv6 host
```

```
Ping6(56 data bytes) 3::1 --> 1::1, press CTRL_C to break
```

```
56 bytes from 1::1, icmp_seq=0 hlim=128 time=1.000 ms
```

```
56 bytes from 1::1, icmp_seq=1 hlim=128 time=0.000 ms
```

```
56 bytes from 1::1, icmp_seq=2 hlim=128 time=1.000 ms
```

```
56 bytes from 1::1, icmp_seq=3 hlim=128 time=1.000 ms
```

```
56 bytes from 1::1, icmp_seq=4 hlim=128 time=0.000 ms
```

```
--- Ping6 statistics for host ---
```

```
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
```

```
round-trip min/avg/max/std-dev = 0.000/0.600/1.000/0.490 ms
```

### 1.11.3 DNS proxy配置举例

#### 1. 组网需求

某局域网内拥有多台设备，每台设备上都指定了域名服务器的 IPv6 地址，以便直接通过域名访问外部网络。当域名服务器的 IPv6 地址发生变化时，网络管理员需要更改局域网内所有设备上配置的域名服务器 IPv6 地址，工作量将会非常巨大。

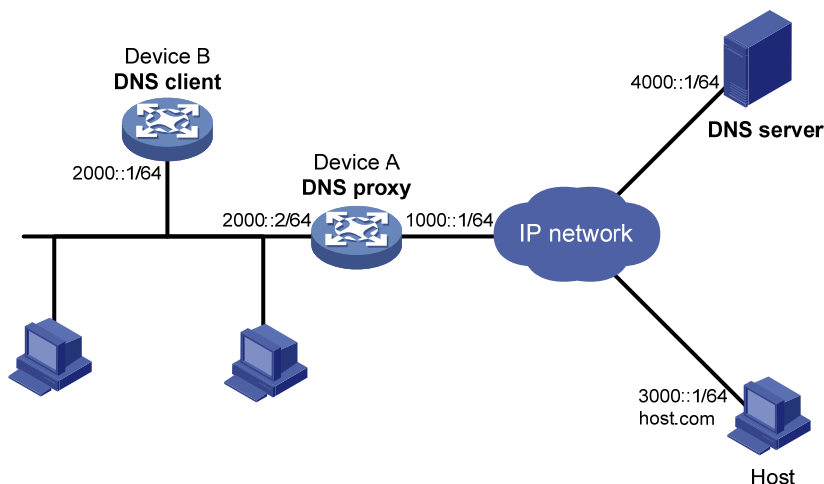
通过 DNS proxy 功能，可以大大减少网络管理员的工作量。当域名服务器 IPv6 地址改变时，只需更改 DNS proxy 上的配置，即可实现局域网内设备通过新的域名服务器解析域名。

在本例中，具体配置步骤为：

- (1) 局域网中的某台设备 Device A 配置为 DNS proxy，DNS proxy 上指定域名服务器 IPv6 地址为真正的域名服务器的地址 4000::1
- (2) 局域网中的其他设备（如 Device B）上，域名服务器的 IPv6 地址配置为 DNS proxy 的地址，域名解析报文将通过 DNS proxy 转发给真正的域名服务器。

#### 2. 组网图

图1-15 DNS proxy 组网图



#### 3. 配置步骤



说明

在开始下面的配置之前，假设设备与域名服务器、主机之间的路由可达，并已按照 [图 1-9](#) 配置各接口的IPv6 地址。

##### (1) 配置域名服务器

不同的域名服务器的配置方法不同。Windows Server 2008 R2 作为域名服务器时，配置方法请参见“[1.11.2 动态域名解析配置举例](#)”。

##### (2) 配置 DNS 代理 Device A

# 配置域名服务器的 IPv6 地址为 4000::1。

```
<DeviceA> system-view
```

```
[DeviceA] ipv6 dns server 4000::1
# 开启 DNS proxy 功能。
[DeviceA] dns proxy enable
(3) 配置 DNS 客户端 Device B
# 配置域名服务器的 IPv6 地址为 2000::2。
<DeviceB> system-view
[DeviceB] ipv6 dns server 2000::2
```

#### 4. 验证配置

# 在 Device B 上执行 **ping host.com** 命令，可以 ping 通主机，且对应的目的地址为 3000::1。

```
[DeviceB] ping host.com
Ping6(56 data bytes) 2000::1 --> 3000::1, press CTRL_C to break
56 bytes from 3000::1, icmp_seq=0 hlim=128 time=1.000 ms
56 bytes from 3000::1, icmp_seq=1 hlim=128 time=0.000 ms
56 bytes from 3000::1, icmp_seq=2 hlim=128 time=1.000 ms
56 bytes from 3000::1, icmp_seq=3 hlim=128 time=1.000 ms
56 bytes from 3000::1, icmp_seq=4 hlim=128 time=0.000 ms

--- Ping6 statistics for host com ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.600/1.000/0.490 ms
```

## 1.12 域名解析常见故障处理

### 1.12.1 无法解析到正确的IP地址

#### 1. 故障现象

配置了动态域名解析，但不能根据域名解析到正确的 IP 地址。

#### 2. 故障分析

DNS 客户端需要和域名服务器配合使用，才能根据域名解析到正确的 IP 地址。

#### 3. 处理过程

- 执行命令 **display dns host ip**，检查动态域名缓存信息是否存在指定域名。
- 如果不存在要解析的域名，检查 DNS 客户端是否和域名服务器通信正常，域名服务器是否工作正常。
- 如果存在要解析的域名，但地址不对，则检查 DNS 客户端所配置的域名服务器的 IP 地址是否正确。
- 检查域名服务器所设置的域名和地址映射表是否正确。

### 1.12.2 无法解析到正确的IPv6 地址

#### 1. 故障现象

配置了动态域名解析，但不能根据域名解析到正确的 IPv6 地址。

## 2. 故障分析

DNS 客户端需要和域名服务器配合使用，才能根据域名解析到正确的 IPv6 地址。

## 3. 处理过程

- 执行命令 **display dns host ipv6**，检查动态域名缓存信息是否存在指定域名。
- 如果不存在要解析的域名，检查 DNS 客户端是否和域名服务器通信正常，域名服务器是否工作正常。
- 如果存在要解析的域名，但地址不对，则检查 DNS 客户端所配置的域名服务器的 IPv6 地址是否正确。
- 检查域名服务器所设置的域名和地址映射表是否正确。

# 目 录

1 IP转发基础.....	1-1
1.1 IP转发表简介.....	1-1
1.2 将当前的IP转发表项保存到用户指定的文件中 .....	1-1
1.3 IP转发表显示和维护 .....	1-2

# 1 IP转发基础

## 1.1 IP转发表简介

FIB（Forwarding Information Base，转发信息库）表用来指导 IP 报文转发。

路由器通过路由表选择路由，把优选路由下发到 FIB 表中，通过 FIB 表指导 IP 报文转发。FIB 表中每条转发表项都指明了要到达某子网或某主机的报文的下一跳 IP 地址以及出接口。

关于路由表的详细介绍，请参见“三层技术-IP 路由配置指导”中的“IP 路由基础”。

通过命令 **display fib** 可以查看 FIB 表的信息，例如：

```
<Sysname> display fib
```

```
Destination count: 4 FIB entry count: 4
```

Flag:

U:Usable G:Gateway H:Host B:Blackhole D:Dynamic S:Static  
R:Relay F:FRR

Destination/Mask	NextHop	Flag	OutInterface/Token	Label
10.2.0.0/16	10.2.1.1	U	GE1/0/1	Null
10.2.1.1/32	127.0.0.1	UH	InLoop0	Null
127.0.0.0/8	127.0.0.1	U	InLoop0	Null
127.0.0.1/32	127.0.0.1	UH	InLoop0	Null

FIB 表中包含了下列关键项：

- **Destination:** 目的地址。用来标识 IP 报文的目的地址或目的网络。
- **Mask:** 网络掩码。与目的地址一起来标识目的主机或路由器所在的网段的地址。将目的地址和网络掩码“逻辑与”后可得到目的主机或路由器所在网段的地址。例如：目的地址为 192.168.1.40、掩码为 255.255.255.0 的主机或路由器所在网段的地址为 192.168.1.0。掩码由若干个连续“1”构成，既可以用点分十进制法表示，也可以用掩码中连续“1”的个数来表示。
- **NextHop:** 转发的下一跳地址。
- **Flag:** 路由的标志。
- **OutInterface:** 转发接口。指明 IP 报文将从哪个接口转发。
- **Token:** LSP（Label Switched Path，标签交换路径）索引号。
- **Label:** 内层标签值。

## 1.2 将当前的IP转发表项保存到用户指定的文件中

### 1. 配置限制和指导

保存 IP 转发表项信息到用户指定的文件中时，如果指定的文件不存在，系统会先创建该文件，再保存；如果已存在，则会覆盖原文件。



本功能只用来触发一次 IP 转发表项保存到用户指定的文件中。

如果需要周期性地自动保存 IP 转发表，可以通过配置定时执行任务功能，采用循环执行方式，让设备在指定时间到达时，自动执行命令。关于配置定时执行任务功能的详细介绍，请参见“基础配置指导”中“设备管理”。

2. 配置步骤

可在任意视图下执行本命令，将当前的 IP 转发表项保存到用户指定的文件中。

```
ip forwarding-table save filename filename
```

1.3 IP转发表显示和维护

查看转发表的信息是定位转发问题的基本方法。在任意视图下执行 **display** 命令可以显示转发表信息。

表1-1 IP 转发表显示和维护

操作	命令
显示FIB表项的信息	<b>display fib</b> [ <i>ip-address</i> [ <i>mask</i>   <i>mask-length</i> ] ]

# 目 录

1 快速转发.....	1-1
1.1 快速转发简介.....	1-1
1.2 快速转发配置限制和指导.....	1-1
1.3 配置快速转发表项的老化时间.....	1-1
1.4 配置快速转发负载分担.....	1-1
1.5 快速转发显示和维护.....	1-2

# 1 快速转发

## 1.1 快速转发简介

报文转发效率是衡量设备性能的一项关键指标。按照常规流程，设备收到一个报文后，根据报文的目地址寻找路由表中与之匹配的路由，然后确定一条最佳的路径，同时还将报文按照数据链路层上使用的协议进行封装，最后进行报文转发。

快速转发是采用高速缓存来处理报文，采用了基于数据流的技术。

快速转发根据报文中的信息（比如源 IP 地址、目的 IP 地址、源端口、目的端口、IP 协议号等）来标识一条数据流。当一条数据流的第一个报文通过查找路由表转发后，在高速缓存中生成相应的转发信息，该数据流后续报文的转发就可以通过直接查找快速转发表进行转发。这样便大大缩减了 IP 报文的排队流程，减少报文的转发时间，提高 IP 报文的转发速率。

## 1.2 快速转发配置限制和指导

快速转发能处理已经分片的 IP 报文，但不支持对 IP 报文的再分片。

## 1.3 配置快速转发表项的老化时间

### 1. 功能简介

快速转发表中的表项并非永远有效，每一条记录都有一个生存周期，到达生存周期仍得不到刷新的记录将从快速转发表中删除，这个生存周期被称作老化时间。如果在到达老化时间前纪录被刷新，则重新计算老化时间。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置快速转发表项的老化时间。

```
ip fast-forwarding aging-time aging-time
```

缺省情况下，快速转发表项的老化时间为 30 秒。

## 1.4 配置快速转发负载分担

### 1. 功能简介

缺省情况下，快速转发负载分担功能处于开启状态，快速转发根据报文中的信息来标识一条数据流；关闭快速转发负载分担功能后，快速转发根据报文中的信息和入接口来标识一条数据流。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置快速转发负载分担功能。请选择其中一项进行配置。

- 开启快速转发负载分担功能。

**ip fast-forwarding load-sharing**

- 关闭快速转发负载分担功能。

**undo ip fast-forwarding load-sharing**

缺省情况下，快速转发负载分担功能处于开启状态。

## 1.5 快速转发显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示快速转发配置后的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除快速转发表中的内容。

表1-1 快速转发显示和维护

操作	命令
显示快速转发表项的老化时间	<b>display ip fast-forwarding aging-time</b>
显示快速转发表信息	<b>display ip fast-forwarding cache</b> [ <i>ip-address</i> ] [ <b>slot</b> <i>slot-number</i> ]
显示分片报文快速转发表信息	<b>display ip fast-forwarding fragcache</b> [ <i>ip-address</i> ] [ <b>slot</b> <i>slot-number</i> ]
清除快速转发表信息	<b>reset ip fast-forwarding cache</b> [ <b>slot</b> <i>slot-number</i> ]

# 目 录

1 IP性能优化 .....	1-1
1.1 IP性能优化配置任务简介 .....	1-1
1.2 配置允许接口转发直连网段的定向广播报文 .....	1-1
1.2.1 功能简介 .....	1-1
1.2.2 配置步骤 .....	1-1
1.2.3 允许接口转发直连网段的定向广播报文典型配置举例 .....	1-2
1.3 配置接口发送IPv4报文的MTU .....	1-3
1.4 开启IP分片报文本地重组功能 .....	1-3
1.5 配置ICMP差错报文发送功能 .....	1-3
1.5.1 功能简介 .....	1-3
1.5.2 开启ICMP重定向报文发送功能 .....	1-4
1.5.3 开启ICMP超时报文发送功能 .....	1-4
1.5.4 开启ICMP目的不可达报文发送功能 .....	1-5
1.6 配置ICMP差错报文发送的令牌刷新周期和令牌桶容量 .....	1-5
1.7 配置ICMP分片报文转发功能 .....	1-6
1.8 指定ICMP报文源地址 .....	1-6
1.9 配置接口的TCP最大报文段长度 .....	1-7
1.10 配置TCP连接的Path MTU探测功能 .....	1-7
1.11 开启SYN Cookie功能 .....	1-8
1.12 配置TCP连接的缓冲区大小 .....	1-9
1.13 配置TCP定时器 .....	1-9
1.14 IP性能优化显示和维护 .....	1-9

# 1 IP性能优化

## 1.1 IP性能优化配置任务简介

如下所有配置均为可选，请根据实际情况选择配置。

- 配置 IP 报文功能
  - [配置允许接口转发直连网段的定向广播报文](#)
  - [配置接口发送IPv4报文的MTU](#)
  - [开启IP分片报文本地重组功能](#)  
本功能适用于 IRF 组网环境。
- 配置 ICMP 报文功能
  - [配置ICMP差错报文发送功能](#)
  - [配置ICMP差错报文发送的令牌刷新周期和](#)
  - [配置ICMP分片报文转发功能](#)
  - [指定ICMP报文源地址](#)
- 配置 TCP 报文功能
  - [配置接口的TCP最大报文段长度](#)
  - [配置TCP连接的Path MTU探测功能](#)
  - [开启SYN Cookie功能](#)
  - [配置TCP连接的缓冲区大小](#)
  - [配置TCP定时器](#)

## 1.2 配置允许接口转发直连网段的定向广播报文

### 1.2.1 功能简介

定向广播报文是指发送给特定网络的广播报文。该报文的目的 IP 地址中网络号码字段为特定网络的网络号，主机号码字段为全 1。

在转发定向广播报文的情况下，如果在接口上配置了此命令，设备从其他接口接收到目的地址为此接口直连网段的定向广播报文时，会从此接口转发此类报文。

黑客可以利用定向广播报文来攻击网络系统，给网络的安全带来了很大的隐患。但在某些应用环境下，设备接口需要转发这类定向广播报文，例如：

- 使用 UDP Helper 功能，将广播报文转换为单播报文发送给指定的服务器。
- 使用 Wake on LAN（网络唤醒）功能，发送定向广播报文唤醒远程网络中的计算机。

在上述情况下，用户可以通过命令配置接口允许转发直连网段的定向广播报文。

### 1.2.2 配置步骤

- (1) 进入系统视图。

**system-view**

- (2) 进入接口视图。

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

- (3) 配置允许接口转发面向直连网段的定向广播报文。

**ip forward-broadcast** [ **acl** *acl-number* ]

缺省情况下，设备禁止转发直连网段的定向广播报文。

### 1.2.3 允许接口转发直连网段的定向广播报文典型配置举例

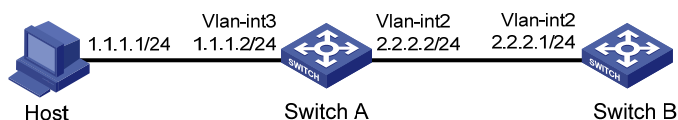
#### 1. 组网需求

如 图 1-1 所示，Host 的接口和 Switch A 的 VLAN 接口 3 处于同一个网段（1.1.1.0/24），Switch A 的 VLAN 接口 2 和 Switch B 的 VLAN 接口 2 处于另外一个网段（2.2.2.0/24）。Host 上配置默认网关为 Switch A 的 VLAN 接口 3 的地址（1.1.1.2/24）。

要求通过配置使得 Switch B 可以收到 Host 发送的定向广播报文。

#### 2. 组网图

图1-1 配置转发定向广播报文组网图



#### 3. 配置步骤

- (1) 配置 Switch A

# 配置 VLAN 接口 3 和 VLAN 接口 2 的 IP 地址。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ip address 1.1.1.2 24
[SwitchA-Vlan-interface3] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 2.2.2.2 24
```

# 配置允许 VLAN 接口 2 转发面向直连网段的定向广播报文。

```
[SwitchA-Vlan-interface2] ip forward-broadcast
```

- (2) 配置 Switch B

# 配置 Switch B 到 Host 的静态路由

```
<SwitchB> system-view
[SwitchB] ip route-static 1.1.1.1 24 2.2.2.2
```

# 配置 VLAN 接口 2 的 IP 地址。

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 2.2.2.1 24
```

配置完成以后，在 Host 上 ping Switch A 的 VLAN 接口 2 所在子网网段的广播地址（2.2.2.255）时，Switch B 的 VLAN 接口 2 可以收到该报文。取消掉 **ip forward-broadcast** 的配置，Switch B 的 VLAN 接口 2 就不能收到该报文。

## 1.3 配置接口发送IPv4报文的MTU

### 1. 功能简介

当设备使用某个接口发送报文时，发现报文长度大于该接口的发送 IPv4 报文的 MTU 值，则进行下列处理：

- 如果报文不允许分片，则将报文丢弃；
- 如果报文允许分片，则将报文进行分片转发。

为了减轻转发设备在传输过程中的分片和重组数据包的压力，更高效的利用网络资源，请根据实际组网环境设置合适的接口 MTU 值，以减少分片的发生。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置发送 IPv4 报文的 MTU。

```
ip mtu mtu-size
```

缺省情况下，未配置接口发送 IPv4 报文的 MTU。

## 1.4 开启IP分片报文本地重组功能

### 1. 功能简介

多台设备组成的 IRF 环境下，当某成员设备收到目的为本 IRF 设备的 IP 分片报文时，需要把分片报文送到主设备进行重组，这样会导致报文重组性能较低的问题。当开启 IP 分片报文本地重组功能后，分片报文会在该成员设备上直接进行报文重组，这样就能提高分片报文的重组性能。开启 IP 分片报文本地重组功能后，如果分片报文是从设备上不同的成员设备进入的，会导致 IP 分片报文本地无法重组成功。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 IP 分片报文本地重组功能。

```
ip reassemble local enable
```

缺省情况下，IP 分片报文本地重组功能处于关闭状态。

## 1.5 配置ICMP差错报文发送功能

### 1.5.1 功能简介

ICMP 报文通常被网络层或传输层协议用来在异常情况发生时通知相应设备，从而便于进行控制管理。ICMP 差错报文的发送虽然方便了网络的控制管理，但是也存在缺陷：发送大量的 ICMP 报文，增大网络流量；如果有用户发送 ICMP 差错报文进行恶意攻击，会导致设备性能下降或影响正常工



作。为了避免上述现象发生，缺省情况下，ICMP 差错报文发送功能处于关闭状态，用户可以根据需要开启 ICMP 差错报文发送功能。

ICMP 差错报文包括重定向报文、超时报文和目的不可达报文。

## 1.5.2 开启ICMP重定向报文发送功能

### 1. 功能简介

ICMP 重定向报文发送功能可以简化主机的管理，使具有很少选路信息的主机逐渐建立较完善的路由表，从而找到最佳路由。

主机启动时，它的路由表中可能只有一条到缺省网关的缺省路由。当满足一定的条件时，缺省网关会向源主机发送 ICMP 重定向报文，通知主机重新选择正确的下一跳进行后续报文的发送。

满足下列条件时，设备会发送 ICMP 重定向报文：

- 接收和转发数据报文的接口是同一接口；
- 被选择的路由本身没有被 ICMP 重定向报文创建或修改过；
- 被选择的路由不是到默认目的地（0.0.0.0）的路由；
- 数据报文中没有源路由选项。

ICMP 重定向报文发送功能可以简化主机的管理，使具有很少选路信息的主机逐渐建立较完善的路由表，从而找到最佳路由。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 ICMP 重定向报文发送功能。

```
ip redirects enable
```

缺省情况下，ICMP 重定向报文发送功能处于关闭状态。

## 1.5.3 开启ICMP超时报文发送功能

### 1. 功能简介

ICMP 超时报文发送功能是在设备收到 IP 数据报文后，如果发生超时差错，则将报文丢弃并给源端发送 ICMP 超时差错报文。

设备在满足下列条件时会发送 ICMP 超时报文：

- 设备收到 IP 数据报文后，如果报文的目的地不是本地且报文的 TTL 字段是 1，则发送“TTL 超时”ICMP 差错报文；
- 设备收到目的地址为本地的 IP 数据报文的第一个分片后，启动定时器，如果所有分片报文到达之前定时器超时，则会发送“重组超时”ICMP 差错报文。

### 2. 配置限制和指导

关闭 ICMP 超时报文发送功能后，设备不会再发送“TTL 超时”ICMP 差错报文，但“重组超时”ICMP 差错报文仍会正常发送。

### 3. 配置步骤

- (1) 进入系统视图。

**system-view**

- (2) 开启 ICMP 超时报文发送功能。

**ip ttl-expires enable**

缺省情况下，ICMP 超时报文发送功能处于关闭状态。

## 1.5.4 开启ICMP目的不可达报文发送功能

### 1. 功能简介

ICMP 目的不可达报文发送功能是在设备收到 IP 数据报文后，如果发生目的不可达的差错，则将报文丢弃并给源端发送 ICMP 目的不可达差错报文。

设备在满足下列条件时会发送目的不可达报文：

- 设备在转发报文时，如果在路由表中未找到对应的转发路由，且路由表中没有缺省路由，则给源端发送“网络不可达”ICMP 差错报文；
- 设备收到目的地址为本地的数据报文时，如果设备不支持数据报文采用的传输层协议，则给源端发送“协议不可达”ICMP 差错报文；
- 设备收到目的地址为本地、传输层协议为 UDP 的数据报文时，如果报文的端口号与正在使用的进程不匹配，则给源端发送“端口不可达”ICMP 差错报文；
- 源端如果采用“严格的源路由选择”发送报文，当中间设备发现源路由所指定的下一个设备不在其直接连接的网络上，则给源端发送“源站路由失败”的 ICMP 差错报文；
- 设备在转发报文时，如果转发接口的 MTU 小于报文的长度，但报文被设置了不可分片，则给源端发送“需要进行分片但设置了不分片比特”ICMP 差错报文。

### 2. 配置限制和指导

设备开启 DHCP 服务后，在未发送 ICMP 回显请求(ECHO-REQUEST)报文情况下，收到非法 ICMP 回显应答(ECHO-REPLY)报文，此时设备不会回应“协议不可达”ICMP 差错报文。关于 DHCP 的详细介绍，请参见“三层技术-IP 业务配置指导”中的“DHCP”。

### 3. 配置步骤

- (1) 进入系统视图。

**system-view**

- (2) 开启 ICMP 目的不可达报文发送功能。

**ip unreachable enable**

缺省情况下，ICMP 目的不可达报文发送功能处于关闭状态。

## 1.6 配置ICMP差错报文发送的令牌刷新周期和令牌桶容量

### 1. 功能简介

如果网络中短时间内发送的 ICMP 差错报文过多，将可能导致网络拥塞。为了避免这种情况，用户可以控制设备在指定时间内发送 ICMP 差错报文的数目，目前采用令牌桶算法来实现。

用户可以设置令牌桶的容量，即令牌桶中可以同时容纳的令牌数；同时可以设置令牌桶的刷新周期，即每隔多长时间发放一个令牌到令牌桶中，直到令牌桶中的令牌数达到配置的容量。一个令牌表示允许发送一个 ICMP 差错报文，每当发送一个 ICMP 差错报文，则令牌桶中减少一个令牌。如果连

续发送的 ICMP 差错报文超过了令牌桶的容量，则后续的 ICMP 差错报文将不能被发送出去，直到按照所设置的刷新频率将新的令牌放入令牌桶中。

## 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置发送 ICMP 差错报文对应的令牌刷新周期和令牌桶容量。

```
ip icmp error-interval interval [ bucket-size ]
```

缺省情况下，令牌刷新周期为 100 毫秒，令牌桶容量为 10。

刷新周期为 0 时，表示不限制 ICMP 差错报文的发送。

## 1.7 配置ICMP分片报文转发功能

### 1. 配置限制和指导

为了防止 ICMP 分片报文攻击，用户可以关闭设备的 ICMP 分片报文转发功能，对于收到的 ICMP 分片报文不进行转发。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 关闭 ICMP 分片报文转发功能。

```
ip icmp fragment discarding
```

缺省情况下，ICMP 分片报文转发功能处于开启状态。

## 1.8 指定ICMP报文源地址

### 1. 功能简介

在网络中 IP 地址配置较多的情况下，收到 ICMP 报文时，用户很难根据报文的源 IP 地址判断报文来自哪台设备。为了简化这一判断过程，可以指定 ICMP 报文源地址。用户配置特定地址（如环回口地址）为 ICMP 报文的源地址，可以简化判断。

设备发送 ICMP 差错报文（TTL 超时、端口不可达和参数错误等）和 ping echo request 报文时，都可以通过上述命令指定报文的源地址。

### 2. 配置限制和指导

用户发送 ping echo request 报文时，如果 ping 命令中已经指定源地址，则使用该源地址，否则使用 `ip icmp source` 配置的源地址。

### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 指定 ICMP 报文源地址。

```
ip icmp source ip-address
```

缺省情况下，未指定 ICMP 报文源地址。设备使用出接口 IP 地址作为 ICMP 报文源地址。

## 1.9 配置接口的TCP最大报文段长度

### 1. 功能简介

TCP 最大报文段长度 (Maximum Segment Size, MSS) 表示 TCP 连接的对端发往本端的最大 TCP 报文段的长度，目前作为 TCP 连接建立时的一个选项来协商：当一个 TCP 连接建立时，连接的双方要将 MSS 作为 TCP 报文的一个选项通告给对端，对端会记录下这个 MSS 值，后续在发送 TCP 报文时，会限制 TCP 报文的大小不超过该 MSS 值。当对端发送的 TCP 报文的长度小于本端的 TCP 最大报文段长度时，TCP 报文不需要分段；否则，对端需要对 TCP 报文按照最大报文段长度进行分段处理后再发给本端。

### 2. 配置限制和指导

- 用户可以通过下面的命令配置接口的 TCP 最大报文段长度，配置后该接口接收和发送的 TCP 报文的大小都不能超过该值。
- 该配置仅对新建的 TCP 连接生效，对于配置前已建立的 TCP 连接不生效。
- 该配置仅对 IP 报文生效。

### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置接口的 TCP 最大报文段长度。

```
tcp mss value
```

缺省情况下，未配置接口的 TCP 最大报文段长度。

## 1.10 配置TCP连接的Path MTU探测功能

### 1. 功能简介

通过开启 TCP 连接的 Path MTU 探测功能，用户可确定 TCP 路径上从源端到目的端的最小 MTU (Path MTU)，按照 Path MTU 组织 TCP 分段长度，避免 IP 分片的发生。为了在 Path MTU 增大时，减少资源浪费，可以开启 Path MTU 老化定时器，保证设备尽量按照 TCP 路径允许的最大报文长度发送数据。

RFC 1191 中规定的 TCP 连接的 Path MTU 探测机制如下：

- (1) TCP 源端将发送的 TCP 数据段的外层 IP 报文设置 DF（不可分片）标记。
- (2) 如果 TCP 路径上某路由器的出接口 MTU 值小于该 IP 报文长度，则会丢弃报文，并给 TCP 源端发送 ICMP 差错报文，报文中会携带该出接口 MTU 值。
- (3) TCP 源端通过解析该 ICMP 差错报文，可知 TCP 路径上当前最小的单向 MTU 值。
- (4) 后续 TCP 源端发送数据段的长度不超过 MSS。其中， $MSS = \text{最小 MTU 值} - \text{IP 头部长度} - \text{TCP 头部长度}$ 。

当 MSS 已经达到系统规定的最小的 32 字节后，如果再次收到减少 MSS 的 ICMP 差错报文，系统将允许该 TCP 连接发送的报文进行分片。

产生 ICMP 差错报文的路由器可能不支持 RFC 1191，其产生的 ICMP 差错报文中的出接口 MTU 字段值为 0，对于这种报文，TCP 源端将按照 RFC 1191 中规定的 MTU 表获取比当前路径 MTU 更小的值作为计算 TCP MSS 的基础。MTU 表的内容为（单位为字节）：68、296、508、1006、1280、1492、2002、4352、8166、17914、32000、65535（由于系统规定的 TCP 最小 MSS 为 32，所以对应最小的 MTU 实际为 72 字节）。

Path MTU 的老化机制如下：

- 当 TCP 源端收到 ICMP 差错报文后，除了减小 Path MTU 值，同时会为该 Path MTU 值启动老化定时器。
- 当该定时器超时时，系统将按照 RFC 1191 规定的 MTU 表依次递增 TCP 的 MSS 值。
- 如果增加一次 MSS 之后的 2 分钟内未收到 ICMP 差错报文，则继续递增，直到 MSS 增长到对端在 TCP 三次握手阶段通告的 MSS 值。

## 2. 配置准备

TCP 连接的 Path MTU 探测功能依赖 IP 报文的 DF 标记位设置后触发 ICMP 差错报文，因此需要 TCP 路径上的所有设备打开 ICMP 差错报文发送功能(`ip unreachable enable`)，以确保 ICMP 差错报文可以发送到 TCP 源端。

## 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 TCP 连接的 Path MTU 探测功能。

```
tcp path-mtu-discovery [ aging age-time | no-aging ]
```

缺省情况下，TCP 连接的 Path MTU 探测功能处于关闭状态。

# 1.11 开启 SYN Cookie 功能

## 1. 功能简介

SYN Cookie 功能用来防止 SYN Flood 攻击。SYN Flood 攻击中，攻击者向设备发送大量请求建立 TCP 连接的 SYN 报文，而不回应设备的 SYN ACK 报文，导致设备上建立了大量的 TCP 半连接。从而，达到耗费设备资源，使设备无法处理正常业务的目的。配置 SYN Cookie 功能后，当设备收到 TCP 连接请求时，不建立 TCP 半连接，而直接向发起者回复 SYN ACK 报文。设备接收到发起者回应的 ACK 报文后，建立连接，并进入 ESTABLISHED 状态。通过这种方式，可以避免在设备上建立大量的 TCP 半连接，防止设备受到 SYN Flood 攻击。

## 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 SYN Cookie 功能。

```
tcp syn-cookie enable
```

缺省情况下，SYN Cookie 功能处于关闭状态。

## 1.12 配置TCP连接的缓冲区大小

- (1) 进入系统视图。

**system-view**

- (2) 配置 TCP 连接的接收和发送缓冲区的大小。

**tcp window window-size**

缺省情况下，TCP 连接的接收和发送缓冲区大小为 63KB。

## 1.13 配置TCP定时器

### 1. TCP定时器简介

可以配置的 TCP 定时器包括：

- **synwait 定时器**：当发送 SYN 报文时，TCP 启动 synwait 定时器和重传 SYN 报文定时器，当 synwait 定时器超时且 SYN 报文重传未达到最大次数时，如果设备未收到回应报文，则 TCP 连接建立不成功；当 synwait 定时器未超时但是 SYN 报文重传达到最大次数时，如果设备未收到回应报文，则 TCP 连接建立不成功。
- **finwait 定时器**：当 TCP 的连接状态为 FIN\_WAIT\_2 时，启动 finwait 定时器，如果在定时器超时前未收到报文，则 TCP 连接终止；如果收到 FIN 报文，则 TCP 连接状态变为 TIME\_WAIT 状态；如果收到非 FIN 报文，则从收到的最后一个非 FIN 报文开始重新计时，在超时后中止连接。

### 2. 配置步骤

- (1) 进入系统视图。

**system-view**

- (2) 配置 TCP 的 synwait 定时器超时时间。

**tcp timer syn-timeout time-value**

缺省情况下，synwait 定时器超时时间为 75 秒。

- (3) 配置 TCP 的 finwait 定时器超时时间。

**tcp timer fin-timeout time-value**

缺省情况下，finwait 定时器超时时间为 675 秒。

## 1.14 IP性能优化显示和维护

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 IP 性能优化功能后的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令清除 IP、TCP 和 UDP 的流量统计信息。

表1-1 IP 性能优化显示和维护

操作	命令
显示ICMP流量统计信息	<b>display icmp statistics [ slot slot-number ]</b>
显示IP报文统计信息	<b>display ip statistics [ slot slot-number ]</b>

操作	命令
显示RawIP连接摘要信息	<b>display rawip</b> [ <b>slot</b> <i>slot-number</i> ]
显示RawIP连接详细信息	<b>display rawip verbose</b> [ <b>slot</b> <i>slot-number</i> [ <b>pcb</b> <i>pcb-index</i> ] ]
显示TCP连接摘要信息	<b>display tcp</b> [ <b>slot</b> <i>slot-number</i> ]
显示TCP连接的流量统计信息	<b>display tcp statistics</b> [ <b>slot</b> <i>slot-number</i> ]
显示TCP连接详细信息	<b>display tcp verbose</b> [ <b>slot</b> <i>slot-number</i> [ <b>pcb</b> <i>pcb-index</i> ] ]
显示UDP连接摘要信息	<b>display udp</b> [ <b>slot</b> <i>slot-number</i> ]
显示UDP流量统计信息	<b>display udp statistics</b> [ <b>slot</b> <i>slot-number</i> ]
显示UDP连接详细信息	<b>display udp verbose</b> [ <b>slot</b> <i>slot-number</i> [ <b>pcb</b> <i>pcb-index</i> ] ]
清除IP报文统计信息	<b>reset ip statistics</b> [ <b>slot</b> <i>slot-number</i> ]
清除TCP连接的流量统计信息	<b>reset tcp statistics</b>
清除UDP流量统计信息	<b>reset udp statistics</b>

# 目 录

1 UDP Helper.....	1-1
1.1 UDP Helper简介.....	1-1
1.2 UDP Helper与硬件适配关系.....	1-1
1.3 配置广播转单播UDP Helper.....	1-1
1.4 配置广播转组播UDP Helper.....	1-2
1.5 UDP Helper显示和维护.....	1-3
1.6 UDP Helper典型配置举例.....	1-3
1.6.1 广播转单播UDP Helper配置举例 .....	1-3
1.6.2 广播转组播UDP Helper配置举例 .....	1-4



# 1 UDP Helper

## 1.1 UDP Helper简介

UDP Helper（UDP 中继转发）功能包括以下部分：

- 广播转单播 UDP Helper：将指定 UDP 端口的广播报文转换为单播报文。
- 广播转组播 UDP Helper：将指定 UDP 端口的广播报文转换为组播报文。

## 1.2 UDP Helper与硬件适配关系

S5110V2-SI、S5000V3-EI 和 S5000E-X 系列交换机不支持本特性。

## 1.3 配置广播转单播UDP Helper

### 1. 功能简介

当网络中的主机需要通过发送广播报文，来获得网络配置或查询网络中其他设备的名称，但是，主机与服务器或待查询的设备不在同一个广播域时，主机就无法获得所需要的信息。

为解决上述问题，设备提供了广播转单播 UDP Helper 功能。通过该功能可以实现对指定 UDP 端口的广播报文进行中继转发，即将指定 UDP 端口的广播报文转换为单播报文发送给指定的目的服务器，起到中继的作用。

开启广播转单播 UDP Helper 功能后，如果设备接收到 UDP 广播报文，将根据报文的 UDP 目的端口号来判断是否要对其中继转发，并进行相应的处理：

- 如果报文的 UDP 目的端口号与配置的需要中继转发的 UDP 端口号匹配，则复制一份报文，修改 IP 报文头的目的 IP 地址，将报文发给指定的目的服务器；
- 如果报文的 UDP 目的端口号与配置的需要中继转发的 UDP 端口号不匹配，则不对报文进行处理。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 UDP Helper 功能。

```
udp-helper enable
```

缺省情况下，UDP Helper 功能处于关闭状态。

- (3) 配置需要中继转发的报文的目的 UDP 端口。

```
udp-helper port { port-number | dns | netbios-ds | netbios-ns | tacacs |  
tftp | time }
```

缺省情况下，未配置需要中继转发的报文的目的 UDP 端口。

UDP Helper 功能不能中继转发 DHCP 广播报文，即中继转发的 UDP 端口不能配置为 67 和 68。

设备上最多可以配置 256 个需要中继转发的 UDP 端口。

- (4) 进入接口视图。

```
interface interface-type interface-number
```

- (5) 配置广播转单播中继转发的目的服务器。

```
udp-helper server ip-address
```

缺省情况下，未配置广播转单播中继转发的目的服务器。

请在接收广播报文的入接口上配置广播转单播中继转发目的服务器。

一个接口上最多可以配置的广播中继个数为 20 个（包括广播转单播和广播转组播）。

## 1.4 配置广播转组播UDP Helper

### 1. 功能简介

在某些特定组网下，网络中的中间设备通过广播转发报文，边缘设备通过组播转发报文，在广播转发的最后一跳可以通过配置广播转组播 UDP Helper 将广播报文转换成组播报文。

配置广播转组播 UDP Helper 功能后，当设备收到 UDP 广播报文时，如果该报文的 UDP 目的端口号与配置的需要中继转发的 UDP 端口号匹配，则查找配置的广播到组播的映射，如果查找成功则复制一份报文，修改 IP 报文头的目的 IP 地址为组播地址，将报文组播出去。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 UDP Helper 功能。

```
udp-helper enable
```

缺省情况下，UDP Helper 功能处于关闭状态。

- (3) 配置需要中继转发的报文的目的 UDP 端口。

```
udp-helper port { port-number | dns | netbios-ds | netbios-ns | tacacs | tftp | time }
```

缺省情况下，未配置需要中继转发的报文的目的 UDP 端口。

UDP Helper 功能不能中继转发 DHCP 广播报文，即中继转发的 UDP 端口不能配置为 67 和 68。

设备上最多可以配置 256 个需要中继转发的 UDP 端口。

- (4) 进入接口视图。

```
interface interface-type interface-number
```

- (5) 配置广播转组播中继转发。

```
udp-helper broadcast-map multicast-address [ acl acl-number ]
```

缺省情况下，未配置广播转组播中继转发。

请在接收广播报文的入接口上配置广播转组播中继转发。

一个接口上最多可以配置的广播中继个数为 20 个（包括广播转单播和广播转组播）。

# 1.5 UDP Helper显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置广播转单播 UDP Helper 功能后的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **reset** 命令可以清除广播转单播中继转发的报文统计数目。

表1-1 UDP Helper 显示和维护

操作	命令
显示广播转单播中继转发的相关信息	<b>display udp-helper interface</b> <i>interface-type interface-number</i>
清除广播转单播中继转发的报文统计数目	<b>reset udp-helper statistics</b>

# 1.6 UDP Helper典型配置举例

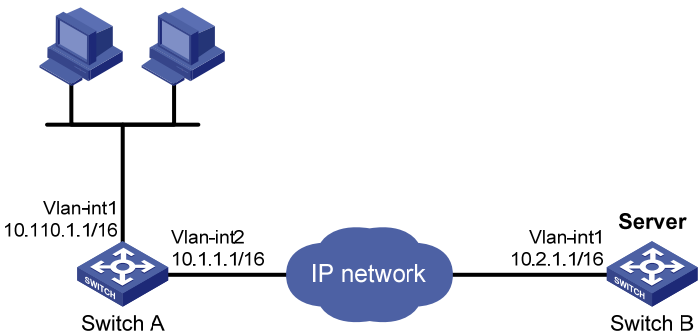
## 1.6.1 广播转单播UDP Helper配置举例

### 1. 组网需求

如 [图 1-1](#) 所示，Switch A的VLAN接口 1 的IP地址为 10.110.1.1/16，连接到网段 10.110.0.0/16。配置将目的UDP端口号为 55 的广播报文，中继转发到目的服务器 10.2.1.1/16。

### 2. 组网图

图1-1 广播转单播 UDP Helper 配置举例组网图



### 3. 配置步骤



说明

用户需保证 Switch A 到网段 10.2.0.0/16 路由可达。

# 开启 UDP Helper 功能。

```
<SwitchA> system-view
```

```
[SwitchA] udp-helper enable
```

# 配置需要中继转发的报文的目的 UDP 端口为 55。

```
[SwitchA] udp-helper port 55
```

# 配置接口地址为 10.110.1.1/16，且接口允许接收定向广播报文。

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 10.110.1.1 16
[SwitchA-Vlan-interface1] ip forward-broadcast
# 配置广播转单播中继转发的目的服务器地址为 10.2.1.1。
[SwitchA-Vlan-interface1] udp-helper server 10.2.1.1
```

#### 4. 验证配置

# 显示 VLAN 接口 1 的 UDP 中继转发相关信息。

```
[SwitchA-Vlan-interface1] display udp-helper interface vlan-interface 1
```

Interface	Server VPN instance	Server address	Packets sent
Vlan-interface1	N/A	10.2.1.1	5

### 1.6.2 广播转组播UDP Helper配置举例

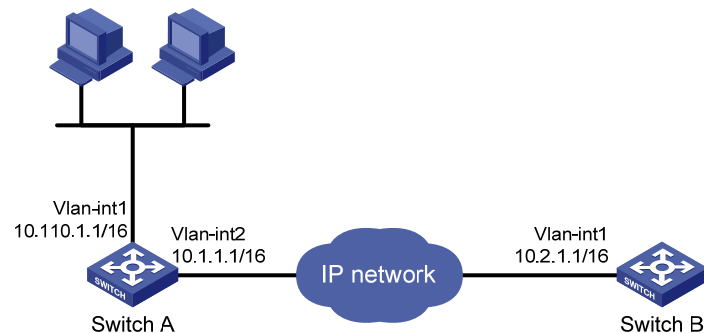
#### 1. 组网需求

如图 1-2 所示，Switch A 的 VLAN 接口 1 的 IP 地址为 10.110.1.1/16，连接到网段 10.110.0.0/16，Switch B 的 VLAN 接口 1 在组播组 225.1.1.1 里。

配置将目的 UDP 端口号为 55 的广播报文，转换为目的地址为 225.1.1.1 的组播报文。

#### 2. 组网图

图1-2 UDP Helper 广播转组播配置举例组网图



#### 3. 配置步骤



说明

用户需保证 Switch A 到网段 10.2.0.0/16 路由可达。

# 开启 UDP Helper 功能。

```
<SwitchA> system-view
[SwitchA] udp-helper enable
```

# 配置需要中继转发的报文的目的 UDP 端口为 55。

```
[SwitchA] udp-helper port 55
```

# 配置接口地址为 10.110.1.1/16，且接口允许接收定向广播报文。

```
[SwitchA] interface vlan-interface 1
```

```
[SwitchA-Vlan-interface1] ip address 10.110.1.1 16
[SwitchA-Vlan-interface1] ip forward-broadcast
# 配置广播转组播中继转发的组播地址为 225.1.1.1。
[SwitchA-Vlan-interface1] udp-helper broadcast-map 225.1.1.1
[SwitchA-Vlan-interface1] quit
# 全局配置开启组播路由，在广播报文的入接口上配置组播协议 PIM-DM，允许组播转发，并将入
接口加入组播组 225.1.1.1。
[SwitchA] multicast routing
[SwitchA-mrib] quit
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] pim dm
[SwitchA-Vlan-interface1] igmp enable
[SwitchA-Vlan-interface1] igmp static-group 225.1.1.1
[SwitchA-Vlan-interface1] quit
# 在交换机 A 的 VLAN 接口 2 上配置组播协议，允许转换后的组播报文从该口出。
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] pim dm
[SwitchA-Vlan-interface2] igmp enable
[SwitchA-Vlan-interface2] igmp static-group 225.1.1.1
```

#### 4. 验证配置

通过抓包，分析发现 Switch B 能接收到来自 SwitchA 转发的组播报文。

# 目 录

1 IPv6 基础 .....	1-1
1.1 IPv6 简介 .....	1-1
1.1.1 IPv6 协议特点 .....	1-1
1.1.2 IPv6 地址介绍 .....	1-2
1.1.3 IPv6 PMTU发现 .....	1-5
1.1.4 IPv6 过渡技术介绍 .....	1-5
1.1.5 协议规范 .....	1-6
1.2 IPv6 基础配置任务简介 .....	1-7
1.3 配置IPv6 全球单播地址 .....	1-7
1.3.1 功能简介 .....	1-7
1.3.2 采用EUI-64 格式形成IPv6 地址 .....	1-8
1.3.3 手工指定IPv6 地址 .....	1-8
1.3.4 无状态自动配置IPv6 地址 .....	1-8
1.3.5 引用前缀生成接口上的IPv6 地址，并将此前缀分配给终端设备 .....	1-9
1.4 配置IPv6 链路本地地址 .....	1-10
1.4.1 功能简介 .....	1-10
1.4.2 配置限制和指导 .....	1-10
1.4.3 配置自动生成链路本地地址 .....	1-10
1.4.4 手工指定接口的链路本地地址 .....	1-11
1.5 配置IPv6 任播地址 .....	1-11
1.6 配置PMTU发现 .....	1-11
1.6.1 配置接口MTU .....	1-11
1.6.2 配置指定地址的静态PMTU .....	1-12
1.6.3 配置PMTU老化时间 .....	1-12
1.7 配置ICMPv6 报文发送功能 .....	1-12
1.7.1 配置发送ICMPv6 差错报文对应的令牌桶容量和令牌刷新周期 .....	1-12
1.7.2 配置允许回复组播形式的Echo request报文 .....	1-13
1.7.3 配置ICMPv6 目的不可达差错报文发送功能 .....	1-13
1.7.4 配置ICMPv6 超时差错报文发送功能 .....	1-14
1.7.5 配置ICMPv6 重定向报文发送功能 .....	1-14
1.7.6 配置ICMPv6 报文指定源地址功能 .....	1-15
1.8 开启IPv6 分片报文本本地重组功能 .....	1-15
1.9 IPv6 基础显示和维护 .....	1-16

1.10 IPv6 基础典型配置举例 .....	1-17
1.10.1 IPv6 基本组网配置举例 .....	1-17
<b>2 IPv6 邻居发现 .....</b>	<b>2-1</b>
2.1 IPv6 邻居发现简介 .....	2-1
2.1.1 IPv6 邻居发现使用的ICMPv6 消息 .....	2-1
2.1.2 地址解析 .....	2-1
2.1.3 验证邻居是否可达 .....	2-2
2.1.4 重复地址检测 .....	2-2
2.1.5 路由器发现/前缀发现及地址无状态自动配置 .....	2-2
2.1.6 重定向功能 .....	2-3
2.1.7 协议规范 .....	2-3
2.2 IPv6 邻居发现配置任务简介 .....	2-3
2.3 配置静态邻居表项 .....	2-4
2.4 配置接口上允许动态学习的邻居的最大个数 .....	2-4
2.5 配置STALE状态ND表项的老化时间 .....	2-5
2.6 配置链路本地ND表项资源占用最小化 .....	2-5
2.7 配置设备的跳数限制 .....	2-6
2.8 配置允许发布RA消息及相关参数 .....	2-6
2.8.1 RA消息及相关参数介绍 .....	2-6
2.8.2 配置限制和指导 .....	2-7
2.8.3 配置允许发布RA消息 .....	2-7
2.8.4 配置RA消息中的相关参数 .....	2-7
2.9 配置重复地址检测时发送邻居请求消息的次数 .....	2-9
2.10 配置ND Snooping功能 .....	2-9
2.10.1 功能简介 .....	2-9
2.10.2 配置步骤 .....	2-10
2.11 配置ND Proxy功能 .....	2-11
2.11.1 功能简介 .....	2-11
2.11.2 配置普通ND Proxy功能 .....	2-12
2.11.3 配置本地ND Proxy功能 .....	2-13
2.12 IPv6 邻居发现显示和维护 .....	2-13
2.13 ND Snooping典型配置举例 .....	2-13
2.13.1 ND Snooping基本组网配置举例 .....	2-13

# 1 IPv6 基础

## 1.1 IPv6简介

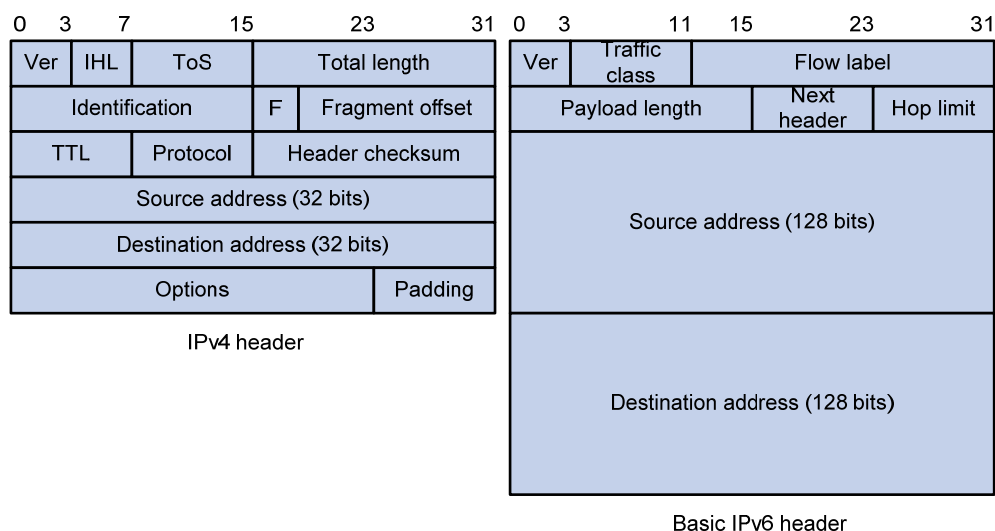
IPv6（Internet Protocol Version 6，互联网协议版本 6）是网络层协议的第二代标准协议，也被称为 IPng（IP Next Generation，下一代互联网协议），它是 IETF（Internet Engineering Task Force，互联网工程任务组）设计的一套规范，是 IPv4 的升级版本。IPv6 和 IPv4 之间最显著的区别为：IP 地址的长度从 32 比特增加到 128 比特。

### 1.1.1 IPv6 协议特点

#### 1. 简化的报文头格式

通过将 IPv4 报文头中的某些字段裁减或移入到扩展报文头，减小了 IPv6 基本报文头的长度。IPv6 使用固定长度的基本报文头，从而简化了转发设备对 IPv6 报文的处理，提高了转发效率。尽管 IPv6 地址长度是 IPv4 地址长度的四倍，但 IPv6 基本报文头的长度只有 40 字节，为 IPv4 报文头长度（不包括选项字段）的两倍。

图1-1 IPv4 报文头和 IPv6 基本报文头格式比较



#### 2. 充足的地址空间

IPv6 的源地址与目的地址长度都是 128 比特（16 字节）。它可以提供超过  $3.4 \times 10^{38}$  种可能的地址空间，完全可以满足多层次的地址划分需要，以及公有网络和机构内部私有网络的地址分配。

#### 3. 层次化的地址结构

IPv6 的地址空间采用了层次化的地址结构，有利于路由快速查找，同时可以借助路由聚合，有效减少 IPv6 路由表占用的系统资源。

#### 4. 地址自动配置

为了简化主机配置，IPv6 支持有状态地址配置和无状态地址配置：



- 有状态地址配置是指从服务器（如 DHCPv6 服务器）获取 IPv6 地址及相关信息，详细介绍请参见“三层技术-IP 业务配置指导”中的“DHCPv6”；
- 无状态地址配置是指主机根据自己的链路层地址及路由器发布的前缀信息自动配置 IPv6 地址及相关信息。

同时，主机也可根据自己的链路层地址及默认前缀（FE80::/10）形成链路本地地址，实现与本链路上其他主机的通信。

## 5. 内置安全性

IPv6 将 IPsec 作为它的标准扩展头，可以提供端到端的安全特性。这一特性也为解决网络安全问题提供了标准，并提高了不同 IPv6 应用之间的互操作性。

## 6. 支持QoS

IPv6 报文头的流标签（Flow Label）字段实现流量的标识，允许设备对某一流中的报文进行识别并提供特殊处理。

## 7. 增强的邻居发现机制

IPv6 的邻居发现协议是通过一组 ICMPv6（Internet Control Message Protocol for IPv6，IPv6 互联网控制消息协议）消息实现的，管理着邻居节点间（即同一链路上的节点）信息的交互。它代替了 ARP（Address Resolution Protocol，地址解析协议）、ICMPv4 路由器发现和 ICMPv4 重定向消息，并提供了一系列其他功能。

## 8. 灵活的扩展报文头

IPv6 取消了 IPv4 报文头中的选项字段，并引入了多种扩展报文头，在提高处理效率的同时还大大增强了 IPv6 的灵活性，为 IP 协议提供了良好的扩展能力。IPv4 报文头中的选项字段最多只有 40 字节，而 IPv6 扩展报文头的大小只受到 IPv6 报文大小的限制。

# 1.1.2 IPv6 地址介绍

## 1. IPv6 地址表示方式

IPv6 地址被表示为以冒号（:）分隔的一连串 16 比特的十六进制数。每个 IPv6 地址被分为 8 组，每组的 16 比特用 4 个十六进制数来表示，组和组之间用冒号隔开，比如：2001:0000:130F:0000:0000:09C0:876A:130B。

为了简化 IPv6 地址的表示，对于 IPv6 地址中的“0”可以有下面的处理方式：

- 每组中的前导“0”可以省略，即上述地址可写为 2001:0:130F:0:0:9C0:876A:130B。
- 如果地址中包含一组或连续多组均为 0 的组，则可以用双冒号“::”来代替，即上述地址可写为 2001:0:130F::9C0:876A:130B。



### 说明

在一个 IPv6 地址中只能使用一次双冒号“::”，否则当设备将“::”转变为 0 以恢复 128 位地址时，将无法确定“::”所代表的 0 的个数。

IPv6 地址由两部分组成：地址前缀与接口标识。其中，地址前缀相当于 IPv4 地址中的网络号码字段部分，接口标识相当于 IPv4 地址中的主机号码部分。

地址前缀的表示方式为：**IPv6 地址/前缀长度**。其中，前缀长度是一个十进制数，表示 IPv6 地址最左边多少位为地址前缀。

2. IPv6 的地址分类

IPv6 主要有三种类型的地址：单播地址、组播地址和任播地址。

- 单播地址：用来唯一标识一个接口，类似于 IPv4 的单播地址。发送到单播地址的数据报文将被传送给此地址所标识的接口。
- 组播地址：用来标识一组接口（通常这组接口属于不同的节点），类似于 IPv4 的组播地址。发送到组播地址的数据报文被传送给此地址所标识的所有接口。
- 任播地址：用来标识一组接口（通常这组接口属于不同的节点）。发送到任播地址的数据报文被传送给此地址所标识的一组接口中距离源节点最近（根据使用的路由协议进行度量）的一个接口。

IPv6 中没有广播地址，广播地址的功能通过组播地址来实现。

IPv6 地址类型是由地址前面几位（称为格式前缀）来指定的，主要地址类型与格式前缀的对应关系如 [表 1-1](#) 所示。

表1-1 地址类型与格式前缀的对应关系

地址类型		格式前缀（二进制）	IPv6 前缀标识
单播地址	未指定地址	00...0 (128 bits)	::/128
	环回地址	00...1 (128 bits)	::1/128
	链路本地地址	1111111010	FE80::/10
	全球单播地址	其他形式	-
组播地址		11111111	FF00::/8
任播地址		从单播地址空间中进行分配，使用单播地址的格式	

3. 单播地址的类型

IPv6 单播地址的类型可有多种，包括全球单播地址、链路本地地址等。

- 全球单播地址等同于 IPv4 公网地址，提供给网络服务提供商。这种类型的地址允许路由前缀的聚合，从而限制了全球路由表项的数量。
- 链路本地地址用于邻居发现协议和无状态自动配置中链路本地上节点之间的通信。使用链路本地地址作为源或目的地址的数据报文不会被转发到其他链路上。
- 环回地址：单播地址 0:0:0:0:0:0:0:1（简化表示为::1）称为环回地址，不能分配给任何物理接口。它的作用与在 IPv4 中的环回地址相同，即节点用来给自己发送 IPv6 报文。
- 未指定地址：地址 “::” 称为未指定地址，不能分配给任何节点。在节点获得有效的 IPv6 地址之前，可在发送的 IPv6 报文的源地址字段填入该地址，但不能作为 IPv6 报文中的目的地址。

4. 组播地址

[表 1-2](#) 所示的组播地址，是预留的特殊用途的组播地址。

表1-2 预留的 IPv6 组播地址列表

地址	应用
FF01::1	表示节点本地范围所有节点的组播地址
FF02::1	表示链路本地范围所有节点的组播地址
FF01::2	表示节点本地范围所有路由器的组播地址
FF02::2	表示链路本地范围所有路由器的组播地址

另外，还有一类组播地址：被请求节点（Solicited-Node）地址。该地址主要用于获取同一链路上邻居节点的链路层地址及实现重复地址检测。每一个单播或任播 IPv6 地址都有一个对应的被请求节点地址。其格式为：

FF02:0:0:0:1:FFXX:XXXX

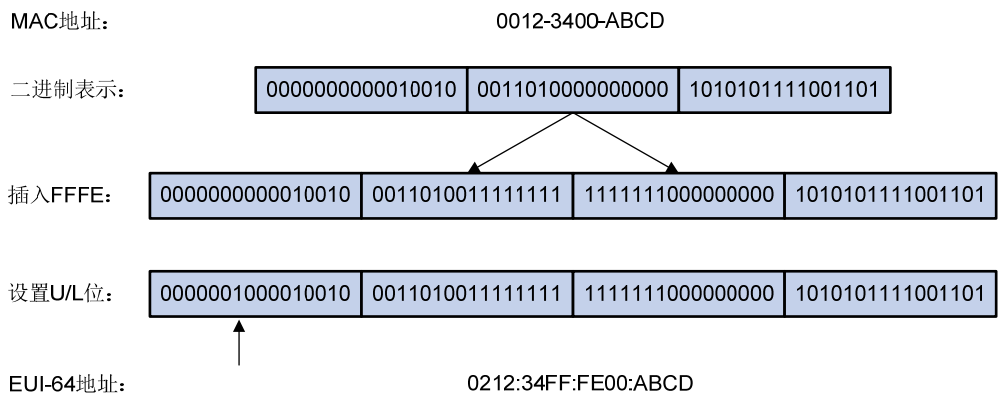
其中，FF02:0:0:0:1:FF 为 104 位固定格式；XX:XXXX 为单播或任播 IPv6 地址的后 24 位。

5. IEEE EUI-64 格式的接口标识符

IPv6 单播地址中的接口标识符用来唯一标识链路上的一个接口。目前 IPv6 单播地址基本上都要求接口标识符为 64 位。

对于所有 IEEE 802 接口类型（例如，VLAN 接口）的接口，IEEE EUI-64 格式的接口标识符是从接口的链路层地址（MAC 地址）变化而来的。IPv6 地址中的接口标识符是 64 位，而 MAC 地址是 48 位，因此需要在 MAC 地址的中间位置（从高位开始的第 24 位后）插入十六进制数 FFFE（111111111111110）。为了使接口标识符的作用范围与原 MAC 地址一致，还要将 Universal/Local (U/L)位（从高位开始的第 7 位）进行取反操作。最后得到的这组数就作为 EUI-64 格式的接口标识符。

图1-2 MAC 地址到 EUI-64 格式接口标识符的转换过程



对于 Tunnel 类型的接口，IEEE EUI-64 格式的接口标识符的低 32 位为 Tunnel 接口的源 IPv4 地址，ISATAP 隧道的接口标识符的高 32 位为 0000:5EFE，其他隧道的接口标识符的高 32 位为全 0。关于各种隧道的介绍，请参见“三层技术-IP 业务配置指导”中的“隧道”。

对于其他接口类型（例如，Serial 接口）的接口，IEEE EUI-64 格式的接口标识符由设备随机生成。

### 1.1.3 IPv6 PMTU发现

报文从源端到目的端的传输路径中所经过的链路可能具有不同的 MTU。在 IPv6 中，当报文的长度大于链路的 MTU 时，报文的分片将在源端进行，从而减轻中间转发设备的处理压力，合理利用网络资源。

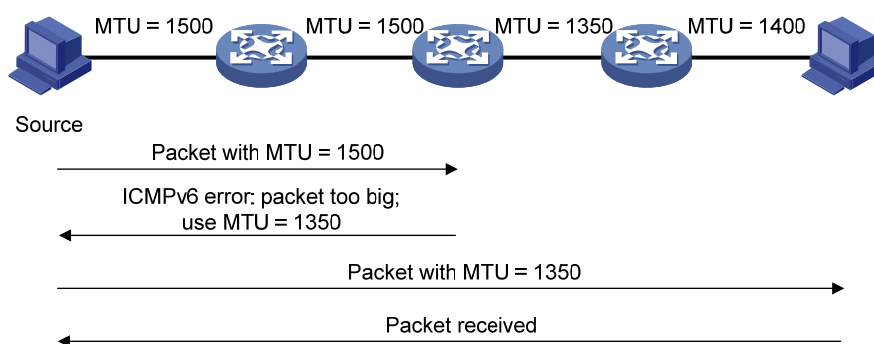
PMTU (Path MTU, 路径MTU) 发现机制的目的就是要找到从源端到目的端的路径上最小的MTU。

如 图 1-3 所示，PMTU的工作过程为：

- (1) 源端主机按照自己的 MTU 对报文进行分片，之后向目的主机发送报文。
- (2) 中间转发设备接收到该报文进行转发时，如果发现转发报文的接口支持的 MTU 值小于报文长度，则会丢弃报文，并给源端返回一个 ICMPv6 差错报文，其中包含了转发失败的接口的 MTU。
- (3) 源主机收到该差错报文后，将按照报文中所携带的 MTU 重新对报文进行分片并发送。

如此反复，直到目的端主机收到这个报文，从而确定报文从源端到目的端路径中的最小 MTU。

图1-3 PMTU 发现工作过程



### 1.1.4 IPv6 过渡技术介绍

在 IPv6 成为主流协议之前，首先使用 IPv6 协议栈的网络希望能与当前仍被 IPv4 支撑着的互联网进行正常通信，因此必须开发出 IPv4 和 IPv6 互通技术以保证 IPv4 能够平稳过渡到 IPv6。互通技术应该对信息传递做到高效无缝。目前已经出现了多种过渡技术，这些技术各有特点，用于解决不同过渡时期、不同环境的通信问题。

#### 1. 双协议栈

双协议栈是一种最简单直接的过渡机制。同时支持 IPv4 协议和 IPv6 协议的网络节点称为双协议栈节点。当双协议栈节点配置 IPv4 地址和 IPv6 地址后，就可以在相应接口上转发 IPv4 和 IPv6 报文。当一个上层应用同时支持 IPv4 和 IPv6 协议时，根据协议要求可以选用 TCP 或 UDP 作为传输层的协议，但在选择网络层协议时，它会优先选择 IPv6 协议栈。双协议栈技术适合 IPv4 网络节点之间或者 IPv6 网络节点之间通信，是所有过渡技术的基础。但是，这种技术要求运行双协议栈的节点有一个全球唯一的地址，实际上没有解决 IPv4 地址资源匮乏的问题。

#### 2. 隧道技术

隧道是一种封装技术，它利用一种网络协议来传输另一种网络协议，即利用一种网络传输协议，将其他协议产生的数据报文封装在它自己的报文中，然后在网络中传输。关于隧道技术的详细介绍，请参见“三层技术-IP 业务配置指导”中的“隧道”。

### 3. NAT-PT

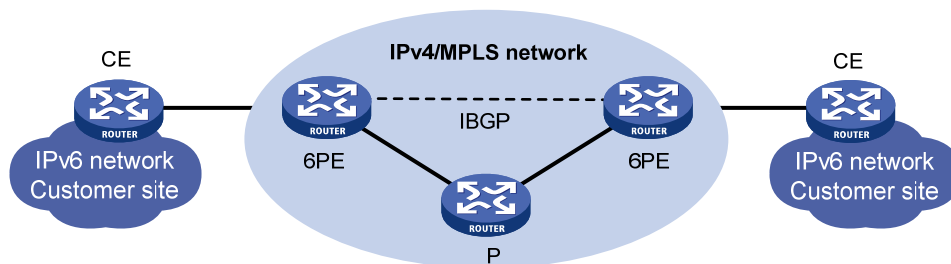
NAT-PT（Network Address Translation-Protocol Translation，附带协议转换的网络地址转换）作用于 IPv4 和 IPv6 网络边缘的设备上，用于实现 IPv6 与 IPv4 报文的转换。NAT-PT 在 IPv4 和 IPv6 网络之间转换 IP 报头的地址，同时根据协议不同对报文做相应的语义翻译，使纯 IPv4 节点和纯 IPv6 节点之间能够透明通信。这种技术适用于仅运行 IPv6 的节点和仅运行 IPv4 的节点之间的通信，具有一定的局限性。

### 4. 6PE

6PE 是一种过渡技术，ISP 可以利用已有的 IPv4 骨干网为分散用户的 IPv6 网络提供接入能力。

6PE 的主要思想是：6PE（IPv6 Provider Edge，IPv6 供应商边缘）路由器将用户的 IPv6 路由信息转换为带有标签的 IPv6 路由信息，并且通过 IBGP（Internal Border Gateway Protocol，内部边界网关协议）会话扩散到 ISP 的 IPv4 骨干网中。6PE 路由器转发 IPv6 报文时，首先会将进入骨干网隧道的数据流打上标签。隧道可以是 GRE 隧道或者 MPLS LSP 等。

图1-4 6PE 组网图



当 ISP 想利用自己原有的 IPv4/MPLS 网络，使其通过 MPLS 具有 IPv6 流量交换能力时，只需要升级 PE 路由器就可以了。所以对于运营商来说，使用 6PE 技术作为 IPv6 过渡机制无疑是一个高效的解决方案，其操作风险也会小得多。

#### 1.1.5 协议规范

相关的协议规范有：

- RFC 1881: IPv6 Address Allocation Management
- RFC 1887: An Architecture for IPv6 Unicast Address Allocation
- RFC 1981: Path MTU Discovery for IP version 6
- RFC 2375: IPv6 Multicast Address Assignments
- RFC 2460: Internet Protocol, Version 6 (IPv6) Specification
- RFC 2464: Transmission of IPv6 Packets over Ethernet Networks
- RFC 2526: Reserved IPv6 Subnet Anycast Addresses
- RFC 3307: Allocation Guidelines for IPv6 Multicast Addresses
- RFC 4191: Default Router Preferences and More-Specific Routes
- RFC 4291: IP Version 6 Addressing Architecture
- RFC 4443: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

## 1.2 IPv6基础配置任务简介

IPv6 基础配置任务如下：

(1) 配置 IPv6 地址

请选择以下至少一项任务进行配置：

- [配置IPv6 全球单播地址](#)
- [配置IPv6 链路本地地址](#)
- [配置IPv6 任播地址](#)

(2) （可选）配置 PMTU 发现

- [配置接口MTU](#)
- [配置指定地址的静态PMTU](#)
- [配置PMTU老化时间](#)

(3) （可选）配置 ICMPv6 报文发送参数

- [配置发送ICMPv6 差错报文对应的令牌桶容量和令牌刷新周期](#)
- [配置允许回复组播形式的Echo request报文](#)
- [配置ICMPv6 目的不可达差错报文发送功能](#)
- [配置ICMPv6 超时差错报文发送功能](#)
- [配置ICMPv6 重定向报文发送功能](#)
- [配置ICMPv6 报文指定源地址功能](#)

(4) （可选）[开启IPv6 分片报文本地重组功能](#)

## 1.3 配置IPv6全球单播地址

### 1.3.1 功能简介

IPv6 全球单播地址可以通过下面几种方式配置：

- 采用 EUI-64 格式形成：当配置采用 EUI-64 格式形成 IPv6 地址时，接口的 IPv6 地址的前缀需要手工配置，而接口 ID 则由接口自动生成。
- 手工配置：用户手工配置 IPv6 全球单播地址。
- 引用前缀生成 IPv6 地址：引用前缀生成 IPv6 地址时，接口的 IPv6 地址的前缀可以通过手工配置或 DHCPv6 动态获取，同时该前缀还会分配给终端设备。
- 无状态自动配置：根据接收到的 RA 报文中携带的地址前缀信息，自动生成 IPv6 全球单播地址。

每个接口可以有多个全球单播地址。

手工配置的全局单播地址（包括采用 EUI-64 格式形成的全局单播地址）的优先级高于自动生成的全局单播地址。如果在接口已经自动生成全局单播地址的情况下，手工配置前缀相同的全局单播地址，不会覆盖之前自动生成的全局单播地址。如果删除手工配置的全局单播地址，设备还可以使用自动生成的全局单播地址进行通信。

### 1.3.2 采用EUI-64 格式形成IPv6 地址

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 采用 EUI-64 格式形成 IPv6 地址。

```
ipv6 address { ipv6-address prefix-length | ipv6-address/prefix-length }  
eui-64
```

缺省情况下，接口上未配置 IPv6 全球单播地址。

### 1.3.3 手工指定IPv6 地址

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 手工指定 IPv6 地址。

```
ipv6 address { ipv6-address prefix-length | ipv6-address/prefix-length }
```

缺省情况下，接口上未配置 IPv6 全球单播地址。

### 1.3.4 无状态自动配置IPv6 地址

#### 1. 功能简介

在配置了无状态自动配置 IPv6 地址功能后，接口会根据接收到的 RA 报文中携带的地址前缀信息和接口 ID，自动生成 IPv6 全球单播地址。如果接口是 IEEE 802 类型的接口（例如，以太网接口、VLAN 接口），其接口 ID 是由 MAC 地址根据一定的规则生成，此接口 ID 具有全球唯一性。对于不同的前缀，接口 ID 部分始终不变，攻击者通过接口 ID 可以很方便的识别出通信流量是由哪台设备产生的，并分析其规律，会造成一定的安全隐患。

如果在地址无状态自动配置时，自动生成接口 ID 不断变化的 IPv6 地址，就可以加大攻击的难度，从而保护网络。为此，设备提供了临时地址功能，使得系统可以生成临时地址。配置该功能后，通过地址无状态自动配置，IEEE 802 类型的接口可以同时生成两类地址：

- 公共地址：地址前缀采用 RA 报文携带的前缀，接口 ID 由 MAC 地址产生。接口 ID 始终不变。
- 临时地址：地址前缀采用 RA 报文携带的前缀，接口 ID 由系统根据 MD5 算法计算产生。接口 ID 不断变化。

在配置了优先选择临时地址功能前提下发送报文，系统将优先选择临时地址作为报文的源地址。当临时地址的有效生命期过期后，这个临时地址将被删除，同时，系统会通过 MD5 算法重新生成一个接口 ID 不同的临时地址。所以，该接口发送报文的源地址的接口 ID 总是在不停变化。如果生成的临时地址因为 DAD 冲突不可用，就采用公共地址作为报文的源地址。

临时地址的首选生命期和有效生命期的确定原则如下：



- 首选生命期是如下两个值之中的较小者：“RA 前缀中的首选生命期”和“配置的临时地址首选生命期减去 DESYNC\_FACTOR”。DESYNC\_FACTOR 是一个 0~600 秒的随机值。
- 有效生命期是如下两个值之中的较小者：“RA 前缀中的有效生命期”和“配置的临时地址有效生命期”。

## 2. 配置限制和指导

如果 RA 报文携带的前缀长度不是 64 位，则该接口自动生成 IPv6 全球单播地址失败。

设备的接口必须启用地址无状态自动配置功能才能生成临时地址，而且临时地址不会覆盖公共地址，因此会出现一个接口下有多个前缀相同但是接口 ID 不同的地址。

如果公共地址生成失败，例如前缀冲突，则不会生成临时地址。

在接口上开启无状态地址自动配置功能后，接口通过无状态自动配置方式生成全球单播地址。如果通过 **undo ipv6 address auto** 命令关闭该功能，将删除该接口上所有自动生成的全球单播地址和链路本地地址。

## 3. 开启无状态自动配置IPv6 地址功能

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 开启无状态地址自动配置功能，使接口通过无状态自动配置方式生成全球单播地址。

```
ipv6 address auto
```

缺省情况下，接口上无状态地址自动配置功能处于关闭状态。

## 4. 配置系统生成临时地址，并优先选择临时地址作为报文的源地址

- (1) 进入系统视图。

```
system-view
```

- (2) 配置系统生成临时地址。

```
ipv6 temporary-address [ valid-lifetime preferred-lifetime ]
```

缺省情况下，系统不生成临时地址。

- (3) 优先选择临时地址作为报文的源地址。

```
ipv6 prefer temporary-address
```

缺省情况下，不会用临时地址作为接口发送报文的源地址。

## 1.3.5 引用前缀生成接口上的IPv6 地址，并将此前缀分配给终端设备

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 IPv6 前缀。请选择其中一项进行配置。

- 手工配置静态的 IPv6 前缀。

```
ipv6 prefix prefix-number ipv6-prefix/prefix-length
```

缺省情况下，未配置静态 IPv6 前缀。

- 配置设备作为 DHCPv6 客户端动态获取 IPv6 前缀，并生成指定编号的 IPv6 前缀。



配置方法请参见“三层技术-IP 业务配置指导”中的“DHCPv6 客户端”。

- (3) 进入接口视图。

```
interface interface-type interface-number
```

- (4) 引用前缀生成接口上的 IPv6 地址，并将此前缀分配给终端设备。

```
ipv6 address prefix-number sub-prefix/prefix-length
```

缺省情况下，接口上未引用前缀，也不会向终端设备分配该前缀。

## 1.4 配置IPv6链路本地地址

### 1.4.1 功能简介

IPv6 的链路本地地址可以通过两种方式获得：

- 自动生成：设备根据链路本地地址前缀（FE80::/10）及接口的链路层地址，自动为接口生成链路本地地址；
- 手工指定：用户手工配置 IPv6 链路本地地址。

### 1.4.2 配置限制和指导

当接口配置了 IPv6 全球单播地址后，同时会自动生成链路本地地址。且与采用 **ipv6 address auto link-local** 命令生成的链路本地地址相同。此时如果手工指定接口的链路本地地址，则手工指定的有效。如果删除手工指定的链路本地地址，则接口的链路本地地址恢复为系统自动生成的地址。

**undo ipv6 address auto link-local** 命令只能删除使用 **ipv6 address auto link-local** 命令生成的链路本地地址。即如果此时已经配置了 IPv6 全球单播地址，由于系统会自动生成链路本地地址，则接口仍有链路本地地址；如果此时没有配置 IPv6 全球单播地址，则接口没有链路本地地址。

每个接口只能有一个链路本地地址，为了避免链路本地地址冲突，推荐使用链路本地地址的自动生成方式。

配置链路本地地址时，手工指定方式的优先级高于自动生成方式。即如果先采用自动生成方式，之后手工指定，则手工指定的地址会覆盖自动生成的地址；如果先手工指定，之后采用自动生成的方式，则自动配置不生效，接口的链路本地地址仍是手工指定的。此时，如果删除手工指定的地址，则自动生成的链路本地地址会生效。

### 1.4.3 配置自动生成链路本地地址

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置自动生成链路本地地址。

```
ipv6 address auto link-local
```

缺省情况下，接口上没有链路本地地址。当接口配置了 IPv6 全球单播地址后，会自动生成链路本地地址。

#### 1.4.4 手工指定接口的链路本地地址

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 手工指定接口的链路本地地址。

```
ipv6 address ipv6-address link-local
```

缺省情况下，未指定接口的链路本地地址。

### 1.5 配置IPv6任播地址

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置 IPv6 任播地址。

```
ipv6 address { ipv6-address prefix-length | ipv6-address/prefix-length }  
anycast
```

缺省情况下，接口上未配置任播地址。

### 1.6 配置PMTU发现

#### 1.6.1 配置接口MTU

##### 1. 功能简介

当设备发送报文时，如果发现报文长度比发送该报文的接口的 MTU 值大，则会将其丢弃。如果设备是作为中间设备转发该报文，同时会将接口的 MTU 值通过 ICMPv6 报文的“Packet Too Big”消息发给源端主机，源端主机以该值重新发送 IPv6 报文。为减少报文被丢弃带来的额外流量开销，需要根据实际组网环境设置合适的接口 MTU 值。

##### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置接口 MTU。

```
ipv6 mtu size
```

缺省情况下，未配置接口上发送 IPv6 报文的 MTU。

## 1.6.2 配置指定地址的静态PMTU

### 1. 功能简介

用户可以为指定的目的IPv6地址配置静态的PMTU值。当设备作为源端从接口发送报文时，将比较该接口的MTU与指定目的IPv6地址的静态PMTU，如果报文长度大于二者中的最小值，则采用此最小值对报文进行分片发送。发送过程中再通过“[1.1.3 IPv6 PMTU发现](#)”中的方法动态确定设备作为源端到目的端主机的PMTU值。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置指定IPv6地址对应的静态PMTU值。

```
ipv6 pathmtu ipv6-address value
```

缺省情况下，未配置静态PMTU值。

## 1.6.3 配置PMTU老化时间

### 1. 功能简介

通过“[1.1.3 IPv6 PMTU发现](#)”中的方法动态确定设备作为源端到目的端主机的PMTU后，设备将使用这个MTU值发送后续报文到目的端主机。当PMTU老化时间超时后，源端主机会通过PMTU机制重新确定发送报文的MTU值。

### 2. 配置限制与指导

该配置对静态PMTU不起作用。

### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置PMTU老化时间。

```
ipv6 pathmtu age age-time
```

缺省情况下，PMTU的老化时间是10分钟。

## 1.7 配置ICMPv6报文发送功能

### 1.7.1 配置发送ICMPv6差错报文对应的令牌桶容量和令牌刷新周期

#### 1. 功能简介

如果网络中短时间内发送的ICMPv6差错报文过多，将可能导致网络拥塞。为了避免这种情况，用户可以控制在指定时间内发送ICMPv6差错报文的最大个数，目前采用令牌桶算法来实现。

用户可以设置令牌桶的容量，即令牌桶中可以同时容纳的令牌数；同时可以设置令牌桶的刷新周期，即每隔多长时间发放一个令牌到令牌桶中，直到令牌桶中的令牌数达到配置的容量。一个令牌表示允许发送一个ICMPv6差错报文，每当发送一个ICMPv6差错报文，则令牌桶中减少一个令牌。如果连续发送的ICMPv6差错报文超过了令牌桶的容量，则后续的ICMPv6差错报文将不能被发送出去，直到按照所设置的刷新频率将新的令牌放入令牌桶中。

## 2. 配置步骤

- (1) 进入系统视图。

**system-view**

- (2) 配置发送 ICMPv6 差错报文对应的令牌桶容量和令牌刷新周期。

**ipv6 icmpv6 error-interval interval [ bucketsize ]**

缺省情况下，令牌桶容量为 10，令牌刷新周期为 100 毫秒。

刷新周期为 0 时，表示不限制 ICMPv6 差错报文的发送。

### 1.7.2 配置允许回复组播形式的Echo request报文

- (1) 进入系统视图。

**system-view**

- (2) 配置设备允许回复组播形式的 Echo request 报文。

**ipv6 icmpv6 multicast-echo-reply enable**

缺省情况下，不允许设备回复组播形式的 Echo request 报文。

### 1.7.3 配置ICMPv6 目的不可达差错报文发送功能

#### 1. 功能简介

ICMPv6 目的不可达报文发送功能是在设备收到 IPv6 数据报文后，如果发生目的不可达的差错，则将报文丢弃并给源端发送 ICMPv6 目的不可达差错报文。

设备在满足下列任一条件时会发送目的不可达报文：

- 设备在转发报文时，如果在路由表中没有找到对应的转发路由，且路由表中没有缺省路由，则给源端发送“没有到达目的地址的路由” ICMPv6 差错报文；
- 设备在转发报文时，如果是因为管理策略（例如防火墙过滤、ACL 等）导致无法发送报文时，则给源端发送“与目的地址的通信被管理策略禁止” ICMPv6 差错报文；
- 设备在转发报文时，如果报文的目的 IPv6 地址超出源 IPv6 地址的范围（例如，报文的源 IPv6 地址为链路本地地址，报文的目的 IPv6 地址为全球单播地址），会导致报文无法到达目的端，此时要给源端发送“超出源地址范围” ICMPv6 差错报文；
- 设备在转发报文时，如果不能解析目的 IPv6 地址对应的链路层地址，则给源端发送“地址不可达” ICMPv6 差错报文；
- 设备收到目的地址为本地、传输层协议为 UDP 的数据报文时，如果报文的目的端口号与正在使用的进程不匹配，则给源端发送“端口不可达” ICMPv6 差错报文。

#### 2. 配置限制和指导

由于 ICMPv6 目的不可达报文传递给用户进程的信息为不可达信息，如果有用户恶意攻击，可能会影响终端用户的正常使用。为了避免上述现象发生，可以关闭设备的 ICMPv6 目的不可达报文发送功能，从而减少网络流量、防止遭到恶意攻击。

## 3. 配置步骤

- (1) 进入系统视图。

**system-view**

- (2) 开启设备的 ICMPv6 目的不可达报文的发送功能。

**ipv6 unreachable enable**

缺省情况下，ICMPv6 目的不可达报文发送功能处于关闭状态。

## 1.7.4 配置ICMPv6 超时差错报文发送功能

### 1. 功能简介

ICMPv6 超时报文发送功能是在设备收到 IPv6 数据报文后，如果发生超时差错，则将报文丢弃并给源端发送 ICMPv6 超时差错报文。

设备在满足下列任一条件时会发送 ICMPv6 超时报文：

- 设备收到 IPv6 数据报文后，如果报文的目的地不是本地且报文的 Hop limit 字段是 1，则发送“Hop limit 超时”ICMPv6 差错报文；
- 设备收到目的地址为本地的 IPv6 数据报文的第一个分片后，启动定时器，如果所有分片报文到达之前定时器超时，则会发送“重组超时”ICMPv6 差错报文。

如果接收到大量需要发送 ICMPv6 差错报文的恶意攻击报文，设备会因为处理大量该类报文而导致性能降低。

### 2. 配置限制和指导

为了避免上述现象发生，可以关闭设备的 ICMPv6 超时报文发送功能，从而减少网络流量、防止遭到恶意攻击。

### 3. 配置步骤

- (1) 进入系统视图。

**system-view**

- (2) 开启设备的 ICMPv6 超时报文的发送功能。

**ipv6 hoplimit-expires enable**

缺省情况下，ICMPv6 超时报文发送功能处于开启状态。

## 1.7.5 配置ICMPv6 重定向报文发送功能

### 1. 功能简介

当主机启动时，它的路由表中可能只有一条到缺省网关的缺省路由。当满足一定的条件时，缺省网关会向源主机发送 ICMPv6 重定向报文，通知主机重新选择更好的下一跳进行后续报文的发送。

同时满足下列条件时，设备会发送 ICMPv6 重定向报文：

- 接收和转发数据报文的接口是同一接口；
- 被选择的路由本身没有被 ICMPv6 重定向报文创建或修改过；
- 被选择的路由不是设备的缺省路由；
- 被转发的 IPv6 数据报文中不包含路由扩展头。

ICMPv6 重定向报文发送功能可以简化主机的管理，使具有很少选路信息的主机逐渐建立较完善的路由表，从而找到最佳路由。但是由于重定向功能会在主机的路由表中增加主机路由，当增加的主机路由很多时，会降低主机性能。因此缺省情况下设备的 ICMPv6 重定向报文发送功能处于关闭状态。

## 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启设备的 ICMPv6 重定向报文发送功能。

```
ipv6 redirects enable
```

缺省情况下，ICMPv6 重定向报文发送功能处于关闭状态。

## 1.7.6 配置ICMPv6 报文指定源地址功能

### 1. 功能简介

在网络中 IPv6 地址配置较多的情况下，收到 ICMPv6 报文时，用户很难根据报文的源 IPv6 地址判断报文来自哪台设备。为了简化这一判断过程，可以配置 ICMPv6 报文指定源地址功能。用可配置特定地址（如环回口地址）为 ICMPv6 报文的源地址，可以简化判断。

设备发送 ICMPv6 差错报文（TTL 超时、报文过大、端口不可达和参数错误等）和 ping echo request 报文时，都可以通过上述命令指定报文的源地址。

### 2. 配置限制与指导

用户发送 ping echo request 报文时，如果 ping 命令中已经指定源地址，则使用该源地址，否则使用 `ipv6 icmpv6 source` 配置的源地址。

### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 ICMPv6 报文指定源地址功能。

```
ipv6 icmpv6 source ipv6-address
```

缺省情况下，ICMPv6 报文指定源地址功能处于关闭状态。

## 1.8 开启IPv6分片报文本地重组功能

### 1. 功能简介

多台设备组成的 IRF 环境下，当某成员设备收到目的为本 IRF 设备的 IPv6 分片报文时，需要把分片报文送到主设备进行重组，这样会导致报文重组性能较低的问题。

当开启 IPv6 分片报文本地重组功能后，分片报文会在该成员设备上直接进行报文重组，这样就能提高分片报文的重组性能。

### 2. 配置限制与指导

开启 IPv6 分片报文本地重组功能后，如果分片报文是从设备上不同的成员设备进入的，会导致 IPv6 分片报文本地无法重组成功。

### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启设备的 IPv6 分片报文本地重组功能。

**ipv6 reassemble local enable**

缺省情况下，IPv6 分片报文本地重组功能处于关闭状态。

## 1.9 IPv6基础显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示 IPv6 配置后的运行情况，用户可以通过查看显示信息验证配置的效果。

在用户视图下，执行 **reset** 命令可以清除相应的统计信息。

**display tcp statistics**、**display udp statistics**、**reset tcp statistics** 和 **reset udp statistics** 命令的详细介绍请参见“三层技术-IP 业务命令参考”中的“IP 性能优化”。

表1-3 IPv6 基础显示和维护

操作	命令
显示IPv6 FIB信息	<b>display ipv6 fib</b> [ <i>ipv6-address</i> [ <i>prefix-length</i> ] ]
显示IPv6 ICMP流量统计信息	<b>display ipv6 icmp statistics</b> [ <i>slot slot-number</i> ]
显示接口的IPv6信息	<b>display ipv6 interface</b> [ <i>interface-type</i> [ <i>interface-number</i> ] ] [ <b>brief</b> ]
显示接口的IPv6前缀信息	<b>display ipv6 interface</b> <i>interface-type</i> <i>interface-number</i> <b>prefix</b>
显示IPv6的PMTU信息	<b>display ipv6 pathmtu</b> { <i>ipv6-address</i>   { <b>all</b>   <b>dynamic</b>   <b>static</b> } [ <i>count</i> ] }
显示IPv6前缀信息	<b>display ipv6 prefix</b> [ <i>prefix-number</i> ]
显示IPv6 RawIP连接摘要信息	<b>display ipv6 rawip</b> [ <i>slot slot-number</i> ]
显示IPv6 RawIP连接详细信息	<b>display ipv6 rawip verbose</b> [ <i>slot slot-number</i> [ <b>pcb</b> <i>pcb-index</i> ] ]
显示IPv6报文及ICMPv6报文的统计信息	<b>display ipv6 statistics</b> [ <i>slot slot-number</i> ]
显示IPv6 TCP连接摘要信息	<b>display ipv6 tcp</b> [ <i>slot slot-number</i> ]
显示IPv6 TCP连接详细信息	<b>display ipv6 tcp verbose</b> [ <i>slot slot-number</i> [ <b>pcb</b> <i>pcb-index</i> ] ]
显示IPv6 UDP连接摘要信息	<b>display ipv6 udp</b> [ <i>slot slot-number</i> ]
显示IPv6 UDP连接详细信息	<b>display ipv6 udp verbose</b> [ <i>slot slot-number</i> [ <b>pcb</b> <i>pcb-index</i> ] ]
显示IPv6 TCP连接的流量统计信息	<b>display tcp statistics</b> [ <i>slot slot-number</i> ]
显示IPv6 UDP流量统计信息	<b>display udp statistics</b> [ <i>slot slot-number</i> ]
清除PMTU值	<b>reset ipv6 pathmtu</b> { <b>all</b>   <b>dynamic</b>   <b>static</b> }
清除IPv6报文及ICMPv6报文的统计信息	<b>reset ipv6 statistics</b> [ <i>slot slot-number</i> ]
清除IPv6 TCP连接的流量统计信息	<b>reset tcp statistics</b>
清除IPv6 UDP流量统计信息	<b>reset udp statistics</b>



## 1.10 IPv6基础典型配置举例

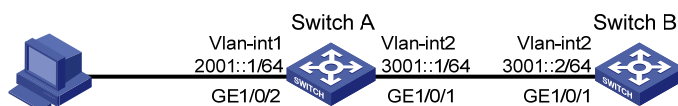
### 1.10.1 IPv6 基本组网配置举例

#### 1. 组网需求

- 如 图 1-5 所示，Host、Switch A和Switch B之间通过以太网端口相连，将以太网端口分别加入相应的VLAN里，在VLAN接口上配置IPv6 地址，验证它们之间的互通性。
- Switch B 有可以到 Host 的路由。
- 在 Host 上安装 IPv6，根据 IPv6 邻居发现协议自动配置 IPv6 地址，有可以到 Switch B 的路由。

#### 2. 组网图

图1-5 IPv6 地址配置组网图



说明

交换机上已经创建相应的 VLAN 接口。

#### 3. 配置步骤

##### (1) 配置 Switch A

# 手工指定 VLAN 接口 2 的全球单播地址。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ipv6 address 3001::1/64
[SwitchA-Vlan-interface2] quit
```

# 手工指定 VLAN 接口 1 的全球单播地址，并允许其发布 RA 消息。（缺省情况下，所有的接口不会发布 RA 消息）

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ipv6 address 2001::1/64
[SwitchA-Vlan-interface1] undo ipv6 nd ra halt
[SwitchA-Vlan-interface1] quit
```

##### (2) 配置 Switch B

# 配置 VLAN 接口 2 的全球单播地址。

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address 3001::2/64
[SwitchB-Vlan-interface2] quit
```

# 配置 IPv6 静态路由，该路由的目的地址为 2001::/64，下一跳地址为 3001::1。

```
[SwitchB] ipv6 route-static 2001:: 64 3001::1
```



### (3) 配置 Host

在 Host 上安装 IPv6，根据 IPv6 邻居发现协议自动配置 IPv6 地址。

# 从 Switch A 上查看端口 GigabitEthernet1/0/2 的邻居信息。

```
[SwitchA] display ipv6 neighbors interface gigabitethernet 1/0/2
Type: S-Static      D-Dynamic      O-Openflow      R-Rule      I-Invalid
IPv6 address          Link Layer      VID  Interface/Link ID      State T Age
FE80::215:E9FF:FEA6:7D14  0015-e9a6-7d14  1    GE1/0/2                STALE D 1238
2001::15B:E0EA:3524:E791  0015-e9a6-7d14  1    GE1/0/2                STALE D 1248
```

通过上面的信息可以知道 Host 上获得的 IPv6 全球单播地址为 2001::15B:E0EA:3524:E791。

### 4. 验证配置

# 显示 Switch A 的接口信息，可以看到各接口配置的 IPv6 全球单播地址。

```
[SwitchA] display ipv6 interface vlan-interface 2
Vlan-interface2 current state: UP
Line protocol current state: UP
IPv6 is enabled, link-local address is FE80::20F:E2FF:FE00:2
Global unicast address(es):
  3001::1, subnet is 3001::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF00:1
  FF02::1:FF00:2
MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND retransmit interval is 1000 milliseconds
Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
InReceives:                25829
InTooShorts:                0
InTruncatedPkts:           0
InHopLimitExceeds:         0
InBadHeaders:               0
InBadOptions:               0
ReasmReqds:                 0
ReasmOKs:                   0
InFragDrops:                0
InFragTimeouts:             0
OutFragFails:               0
InUnknownProtos:           0
InDelivers:                 47
OutRequests:                 89
OutForwDatagrams:           48
InNoRoutes:                  0
InTooBigErrors:              0
OutFragOKs:                  0
OutFragCreates:              0
```

```

InMcastPkts:                6
InMcastNotMembers:          25747
OutMcastPkts:                48
InAddrErrors:                0
InDiscards:                  0
OutDiscards:                  0

[SwitchA] display ipv6 interface vlan-interface 1
Vlan-interface1 current state: UP
Line protocol current state: UP
IPv6 is enabled, link-local address is FE80::20F:E2FF:FE00:1C0
Global unicast address(es):
    2001::1, subnet is 2001::/64
Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FF00:1C0
MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 600 seconds
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
InReceives:                  272
InTooShorts:                  0
InTruncatedPkts:              0
InHopLimitExceeds:            0
InBadHeaders:                  0
InBadOptions:                  0
ReasmReqds:                    0
ReasmOKs:                      0
InFragDrops:                   0
InFragTimeouts:                0
OutFragFails:                   0
InUnknownProtos:               0
InDelivers:                    159
OutRequests:                   1012
OutForwDatagrams:              35
InNoRoutes:                    0
InTooBigErrors:                 0
OutFragOKs:                     0
OutFragCreates:                 0
InMcastPkts:                   79
InMcastNotMembers:             65

```

```

OutMcastPkts:          938
InAddrErrors:          0
InDiscards:            0
OutDiscards:           0
# 显示 Switch B 的接口信息，可以看到接口配置的 IPv6 全球单播地址。
[SwitchB] display ipv6 interface vlan-interface 2
Vlan-interface2 current state: UP
Line protocol current state: UP
IPv6 is enabled, link-local address is FE80::20F:E2FF:FE00:1234
Global unicast address(es):
    3001::2, subnet is 3001::/64
Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:2
    FF02::1:FF00:1234
MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND retransmit interval is 1000 milliseconds
Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
InReceives:            117
InTooShorts:           0
InTruncatedPkts:       0
InHopLimitExceeds:     0
InBadHeaders:           0
InBadOptions:           0
ReasmReqds:             0
ReasmOKs:               0
InFragDrops:            0
InFragTimeouts:         0
OutFragFails:           0
InUnknownProtos:       0
InDelivers:             117
OutRequests:            83
OutForwDatagrams:       0
InNoRoutes:             0
InTooBigErrors:         0
OutFragOKs:             0
OutFragCreates:         0
InMcastPkts:           28
InMcastNotMembers:     0
OutMcastPkts:           7
InAddrErrors:           0
InDiscards:             0
OutDiscards:            0

```

# 在 Host 上使用 Ping 测试和 Switch A 及 Switch B 的互通性; 在 Switch B 上使用 Ping 测试和 Switch A 及 Host 的互通性。

---



#### 说明

在 Ping 链路本地地址时，需要使用 **-i** 参数来指定链路本地地址的接口。

---

```
[SwitchB] ping ipv6 -c 1 3001::1
Ping6(56 data bytes) 3001::2 --> 3001::1, press CTRL_C to break
56 bytes from 3001::1, icmp_seq=0 hlim=64 time=4.404 ms

--- Ping6 statistics for 3001::1 ---
1 packet(s) transmitted, 1 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.404/4.404/4.404/0.000 ms
[SwitchB] ping ipv6 -c 1 2001::15B:E0EA:3524:E791
Ping6(56 data bytes) 3001::2 --> 2001::15B:E0EA:3524:E791, press CTRL_C to break
56 bytes from 2001::15B:E0EA:3524:E791, icmp_seq=0 hlim=64 time=5.404 ms

--- Ping6 statistics for 2001::15B:E0EA:3524:E791 ---
1 packet(s) transmitted, 1 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 5.404/5.404/5.404/0.000 ms
从 Host 上也可以 ping 通 Switch B 和 Switch A，证明它们是互通的。
```

# 2 IPv6 邻居发现

## 2.1 IPv6邻居发现简介

### 2.1.1 IPv6 邻居发现使用的ICMPv6 消息

IPv6 ND（IPv6 Neighbor Discovery，IPv6 邻居发现）协议使用五种类型的 ICMPv6 消息，实现下面一些功能：地址解析、验证邻居是否可达、重复地址检测、路由器发现/前缀发现、地址自动配置和重定向等。

邻居发现协议使用的ICMPv6 消息的类型及作用如 [表 2-1](#) 所示。

表2-1 邻居发现协议使用的 ICMPv6 消息类型及作用

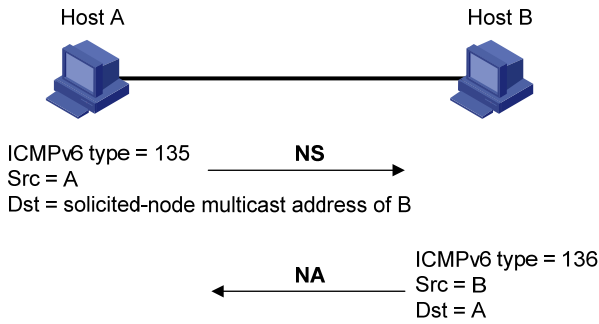
ICMPv6 消息	类型号	作用
邻居请求消息NS（Neighbor Solicitation）	135	获取邻居的链路层地址
		验证邻居是否可达
		进行重复地址检测
邻居通告消息NA（Neighbor Advertisement）	136	对NS消息进行响应
		节点在链路层变化时主动发送NA消息，向邻居节点通告本节点的变化信息
路由器请求消息RS（Router Solicitation）	133	节点启动后，通过RS消息向路由器发出请求，请求前缀和其他配置信息，用于节点的自动配置
路由器通告消息RA（Router Advertisement）	134	对RS消息进行响应
		在没有抑制RA消息发布的条件下，路由器会周期性地发布RA消息，其中包括前缀信息选项和一些标志位的信息
重定向消息（Redirect）	137	当满足一定的条件时，缺省网关通过向源主机发送重定向消息，使主机重新选择正确的下一跳地址进行后续报文的发送

### 2.1.2 地址解析

获取同一链路上邻居节点的链路层地址（与IPv4 的ARP功能相同），通过邻居请求消息NS和邻居通告消息NA实现。如 [图 2-1](#) 所示，节点A要获取节点B的链路层地址的过程为：

- (1) 节点 A 以组播方式发送 NS 消息。NS 消息的源地址是节点 A 的接口 IPv6 地址，目的地址是节点 B 的被请求节点组播地址，消息内容中包含了节点 A 的链路层地址和请求的目标地址。
- (2) 节点 B 收到 NS 消息后，判断报文的目标地址是否为自己的 IPv6 地址。如果是，则节点 B 可以学习到节点 A 的链路层地址，并以单播方式返回 NA 消息，其中包含了自己的链路层地址。
- (3) 节点 A 从收到的 NA 消息中就可获取到节点 B 的链路层地址。

图2-1 地址解析示意图



### 2.1.3 验证邻居是否可达

在获取到邻居节点的链路层地址后，通过邻居请求消息 **NS** 和邻居通告消息 **NA** 可以验证邻居节点是否可达。

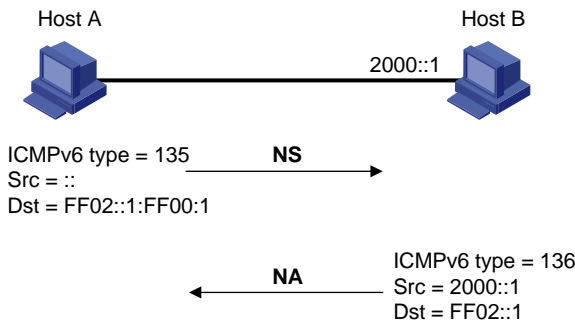
- (1) 节点发送 **NS** 消息，其中目的地址是邻居节点的 **IPv6** 地址。
- (2) 如果收到邻居节点的确认报文，则认为邻居可达；否则，认为邻居不可达。

### 2.1.4 重复地址检测

当节点获取到一个 **IPv6** 地址后，需要使用重复地址检测功能确定该地址是否已被其他节点使用（与 **IPv4** 的免费 **ARP** 功能相似）。如 [图 2-2](#) 所示，通过 **NS** 和 **NA** 实现重复地址检测的过程为：

- (1) 节点 **A** 发送 **NS** 消息，**NS** 消息的源地址是未指定地址 **::**，目的地址是待检测的 **IPv6** 地址对应的被请求节点组播地址，消息内容中包含了待检测的 **IPv6** 地址。
- (2) 如果节点 **B** 已经使用这个 **IPv6** 地址，则会返回 **NA** 消息。其中包含了自己的 **IPv6** 地址。
- (3) 节点 **A** 收到节点 **B** 发来的 **NA** 消息，就知道该 **IPv6** 地址已被使用。反之，则说明该地址未被使用，节点 **A** 就可使用此 **IPv6** 地址。

图2-2 重复地址检测示意图



### 2.1.5 路由器发现/前缀发现及地址无状态自动配置

路由器发现/前缀发现是指节点从收到的 **RA** 消息中获取邻居路由器及所在网络的前缀，以及其他配置参数。

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。

路由器发现/前缀发现通过路由器请求消息 RS 和路由器通告消息 RA 来实现，具体过程如下：

- (1) 节点启动时，通过 RS 消息向路由器发出请求，请求前缀和其他配置信息，以便用于节点的配置。
- (2) 路由器返回 RA 消息，其中包括前缀信息选项（路由器也会周期性地发布 RA 消息）。
- (3) 节点利用路由器返回的 RA 消息中的地址前缀及其他配置参数，自动配置接口的 IPv6 地址及其他信息。

前缀信息选项中不仅包括地址前缀的信息，还包括该地址前缀的首选生命期（preferred lifetime）和有效生命期（valid lifetime）。节点收到周期性发送的 RA 消息后，会根据该消息更新前缀的首选生命期和有效生命期。

- 有效生命期：表示前缀有效期。在有效生命期内，通过该前缀自动生成的地址可以正常使用；有效生命期过期后，通过该前缀自动生成的地址变为无效，将被删除。
- 首选生命期：表示首选通过该前缀无状态自动配置地址的时间。首选生命期过期后，节点通过该前缀自动配置的地址将被废止。节点不能使用被废止的地址建立新的连接，但是仍可以接收目的地址为被废止地址的报文。首选生命期必须小于或等于有效生命期。

### 2.1.6 重定向功能

当主机启动时，它的路由表中可能只有一条到缺省网关的缺省路由。当满足一定的条件时，缺省网关会向源主机发送 ICMPv6 重定向消息，通知主机选择更好的下一跳进行后续报文的发送（与 IPv4 的 ICMP 重定向消息的功能相同）。

同时满足下列条件时，设备会发送 ICMPv6 重定向报文：

- 接收和转发数据报文的接口是同一接口；
- 被选择的路由本身没有被 ICMPv6 重定向报文创建或修改过；
- 被选择的路由不是设备的缺省路由；
- 被转发的 IPv6 数据报文中不包含路由扩展头。

### 2.1.7 协议规范

相关的协议规范有：

- RFC 4861: Neighbor Discovery for IP Version 6 (IPv6)
- RFC 4862: IPv6 Stateless Address Autoconfiguration

## 2.2 IPv6邻居发现配置任务简介

本节中的所有配置均为可选，请根据实际情况选择配置。

- [配置静态邻居表项](#)
- [配置接口上允许动态学习的邻居的最大个数](#)
- [配置STALE状态ND表项的老化时间](#)
- [配置链路本地ND表项资源占用最小化](#)
- [配置设备的跳数限制](#)

- [配置允许发布RA消息及相关参数](#)
- [配置重复地址检测时发送邻居请求消息的次数](#)
- [配置ND Snooping功能](#)
- [配置ND Proxy功能](#)

## 2.3 配置静态邻居表项

### 1. 功能简介

邻居表项保存的是设备在链路范围内的邻居信息，设备邻居表项可以通过邻居请求消息 **NS** 及邻居通告消息 **NA** 来动态创建，也可以通过手工配置来静态创建。

设备根据邻居节点的 **IPv6** 地址和与此邻居节点相连的三层接口号来唯一标识一个静态邻居表项。目前，静态邻居表项有两种配置方式：

- 配置本节点的三层接口相连的邻居节点的 **IPv6** 地址和链路层地址；
- 配置本节点 **VLAN** 中的二层端口相连的邻居节点的 **IPv6** 地址和链路层地址。

### 2. 配置限制与指导

对于 **VLAN** 接口，可以采用上述两种方式配置静态邻居表项：

- 采用第一种方式配置静态邻居表项后，设备还需要解析该 **VLAN** 下的二层端口信息。
- 采用第二种方式配置静态邻居表项后，需要保证 *port-type port-number* 指定的二层端口属于 *vlan-id* 指定的 **VLAN**，且该 **VLAN** 已经创建了 **VLAN** 接口。在配置后，设备会将 **VLAN** 所对应的 **VLAN** 接口与 **IPv6** 地址相对应来唯一标识一个静态邻居表项。

### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置静态邻居表项。

```
ipv6 neighbor ipv6-address mac-address { vlan-id port-type port-number  
| interface interface-type interface-number }
```

缺省情况下，未配置静态邻居表项。

## 2.4 配置接口上允许动态学习的邻居的最大个数

### 1. 功能简介

设备可以通过 **NS** 消息和 **NA** 消息来动态获取邻居节点的链路层地址，并将其加入到邻居表中。为了防止部分接口下的用户占用过多的资源，可以通过设置接口学习动态邻居表项的最大个数来进行限制。当接口学习到的动态邻居表项的个数达到所设置的最大值时，该接口将不再学习动态邻居表项。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。



```
interface interface-type interface-number
```

- (3) 配置接口上允许学习的动态邻居表项的最大个数。

```
ipv6 neighbors max-learning-num max-number
```

各系列产品接口上允许学习的动态邻居表项的最大个数为：

- S5130S-SI 系列交换机、S5120V2-SI 系列交换机为 512。
- S5130S-LI 系列交换机、S5120V2-LI 系列交换机和 S3100V3-SI 系列交换机为 256。
- S5110V2-SI 系列交换机为 128。
- S5000V3-EI 系列交换机、S5000E-X 系列交换机为 64。

## 2.5 配置STALE状态ND表项的老化时间

### 1. 功能简介

为适应网络的变化，ND 表需要不断更新。在 ND 表中，处于 STALE 状态的 ND 表项并非永远有效，而是有一个老化时间。到达老化时间的 STALE 状态 ND 表项将迁移到 DELAY 状态。5 秒钟后 DELAY 状态超时，ND 表项将迁移到 PROBE 状态，并且设备会发送 3 次 NS 报文进行可达性探测。若邻居已经下线，则收不到回应的 NA 报文，此时设备会将该 ND 表项删除。用户可以根据网络实际情况调整老化时间。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 STALE 状态 ND 表项的老化时间。

```
ipv6 neighbor stale-aging aging-time
```

缺省情况下，STALE 状态 ND 表项的老化时间为 240 分钟。

## 2.6 配置链路本地ND表项资源占用最小化

### 1. 功能简介

本功能可以对链路本地 ND 表项（该 ND 表项的 IPv6 地址为链路本地地址）占用的资源进行优化。缺省情况下，所有 ND 表项均会下发硬件表项。配置本功能后，新学习的、未被引用的链路本地 ND 表项（该 ND 表项的链路本地地址不是某条路由的下一跳）不下发硬件表项，以节省资源。本功能只对后续新学习的 ND 表项生效，已经存在的 ND 表项不受影响。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置链路本地 ND 表项资源占用最小化。

```
ipv6 neighbor link-local minimize
```

缺省情况下，所有 ND 表项均会下发硬件表项。

## 2.7 配置设备的跳数限制

### 1. 功能简介

本功能可以对设备发送的 IPv6 数据报文的跳数（即 IPv6 数据报文的 Hop Limit 字段的值）进行配置。

### 2. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 配置设备的跳数限制。

```
ipv6 hop-limit value
```

缺省情况下，设备的跳数限制为 64 跳。

## 2.8 配置允许发布RA消息及相关参数

### 2.8.1 RA消息及相关参数介绍

用户可以根据实际情况，配置接口是否发送RA消息及发送RA消息的时间间隔，同时可以配置RA消息中的相关参数以通告给主机。当主机接收到RA消息后，就可以采用这些参数进行相应操作。可以配置的RA消息中的参数及含义如 [表 2-2](#) 所示。

表2-2 RA 消息中的参数及描述

参数	描述
跳数限制（Hop Limit）	在RA消息中发布本设备的跳数限制，收到该RA消息之后，主机在发送IPv6报文时，将使用该跳数值填充IPv6报文头中的Hop Limit字段。
前缀信息（Prefix Information）	在同一链路上的主机收到设备发布的前缀信息后，可以进行无状态自动配置等操作。
MTU	发布链路的MTU，可以用于确保同一链路上的所有节点采用相同的MTU值。
被管理地址配置标志位（M flag）	用于确定主机是否采用有状态自动配置获取IPv6地址。 如果设置该标志位为1，主机将通过有状态自动配置（例如DHCPv6服务器）来获取IPv6地址；否则，将通过无状态自动配置获取IPv6地址，即根据自己的链路层地址及路由器发布的前缀信息生成IPv6地址。
其他信息配置标志位（O flag）	用于确定主机是否采用有状态自动配置获取除IPv6地址外的其他信息。 如果设置其他信息配置标志位为1，主机将通过有状态自动配置（例如DHCPv6服务器）来获取除IPv6地址外的其他信息；否则，将通过无状态自动配置获取其他信息。
路由器生存时间（Router Lifetime）	用于设置发布RA消息的路由器作为主机的默认路由器的时间。主机根据接收到的RA消息中的路由器生存时间参数值，就可以确定是否将发布该RA消息的路由器作为默认路由器。发布RA消息中路由器生存时间为0的路由器不能作为默认路由器。
邻居请求消息重传时间间隔（Retrans Timer）	设备发送NS消息后，如果未在指定的时间间隔内收到响应，则会重新发送NS消息。

参数	描述
保持邻居可达状态的时间 (Reachable Time)	当通过邻居可达性检测确认邻居可达后，在所设置的可达时间内，设备认为邻居可达；超过设置的时间后，如果需要向邻居发送报文，会重新确认邻居是否可达。
配置路由优先级 (Router Preference)	用于设置发布RA消息的路由器的路由器优先级，主机根据接收到的RA消息中的路由器优先级，可以选择优先级最高的路由器作为默认网关。在路由器的优先级相同的情况下，遵循“先来先用”的原则，优先选择先接收到的RA消息对应的发送路由器作为默认网关。

## 2.8.2 配置限制和指导

RA 消息发布的最大间隔时间应该小于或等于 RA 消息中路由器的生存时间，以保证在路由器失效之前得到更新的 RA 消息。

在接口上配置的邻居请求消息重传时间间隔及保持邻居可达状态的时间，既可作为 RA 消息中的信息发布给主机，也可作为本接口发送邻居请求消息的时间间隔及保持邻居可达状态的时间。

## 2.8.3 配置允许发布RA消息

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 取消对 RA 消息发布的抑制。

```
undo ipv6 nd ra halt
```

缺省情况下，抑制发布 RA 消息。

- (4) 配置 RA 消息发布的最大时间间隔和最小时间间隔。

```
ipv6 nd ra interval max-interval-value min-interval-value
```

缺省情况下，RA 消息发布的最大间隔时间为 600 秒，最小时间间隔为 200 秒。

接口将在最大时间间隔与最小时间间隔之间随机选取一个值来发布 RA 消息。

配置的最小时间间隔应该小于等于最大时间间隔的 0.75 倍。

## 2.8.4 配置RA消息中的相关参数

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置 RA 消息中的前缀信息。

```
ipv6 nd ra prefix { ipv6-prefix prefix-length |  
ipv6-prefix/prefix-length } [ valid-lifetime preferred-lifetime  
[ no-autoconfig | off-link ] * | no-advertise ]
```

缺省情况下，未配置 RA 消息中的前缀信息，此时将使用发送 RA 消息的接口 IPv6 地址作为 RA 消息中的前缀信息，其手工配置地址的有效生命期是 2592000 秒（30 天），首选生命期是 604800（7 天）；其他自动分配地址（如 DHCPv6 分配地址）的有效生命期和首选生命期与地址本身的生命期相同。

- (4) 配置通过 RA 消息发布的前缀使用的缺省参数。

```
ipv6 nd ra prefix default [ valid-lifetime preferred-lifetime  
[ no-autoconfig | off-link ] * | no-advertise ]
```

缺省情况下，未配置通过 RA 消息发布的前缀使用的缺省参数。

- (5) 配置 RA 消息中不携带 MTU 选项。

```
ipv6 nd ra no-advlinkmtu
```

缺省情况下，RA 消息中携带 MTU 选项。

- (6) 配置 RA 消息中不指定跳数限制。

```
ipv6 nd ra hop-limit unspecified
```

缺省情况下，RA 消息中发布本设备的跳数限制，本设备的跳数限制默认为 64 跳。

- (7) 设置被管理地址配置标志位为 1。

```
ipv6 nd autoconfig managed-address-flag
```

缺省情况下，被管理地址标志位为 0，即主机通过无状态自动配置获取 IPv6 地址。

- (8) 设置其他配置标志位为 1。

```
ipv6 nd autoconfig other-flag
```

缺省情况下，其他配置标志位为 0，即主机通过无状态自动配置获取其他信息。

- (9) 配置 RA 消息中路由器的生存时间。

```
ipv6 nd ra router-lifetime time
```

缺省情况下，RA 消息中路由器的生存时间为 1800 秒。

- (10) 配置邻居请求消息重传时间间隔。

```
ipv6 nd ns retrans-timer value
```

缺省情况下，接口发送 NS 消息的时间间隔为 1000 毫秒；接口发布的 RA 消息中 Retrans Timer 字段的值为 0，即不对主机进行指定。

- (11) 配置 RA 消息中路由器的优先级。

```
ipv6 nd router-preference { high | low | medium }
```

缺省情况下，RA 消息中路由器的优先级为 **medium**。

- (12) 配置保持邻居可达状态的时间。

```
ipv6 nd nud reachable-time time
```

缺省情况下，接口保持邻居可达状态的时间为 30000 毫秒；接口发布的 RA 消息中 Reachable Timer 字段的值为 0，即不对主机进行指定。

## 2.9 配置重复地址检测时发送邻居请求消息的次数

### 1. 功能简介

接口获得 IPv6 地址后，将发送邻居请求消息进行重复地址检测。如果在指定的时间内（通过 **ipv6 nd ns retrans-timer** 命令配置）没有收到响应，则继续发送邻居请求消息，当发送的次数达到所设置的次数后，仍未收到响应，则认为该地址可用。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置重复地址检测时发送邻居请求消息的次数。

```
ipv6 nd dad attempts interval
```

缺省情况下，重复地址检测时发送邻居请求报文的次数为 1，当 *interval* 值为 0 时，表示禁止重复地址检测。

## 2.10 配置ND Snooping功能

### 2.10.1 功能简介

ND Snooping 功能用于二层交换网络环境，设备通过侦听 ND 或者数据报文来创建 ND Snooping 表项，该表项内容包括报文的源 IPv6 地址、源 MAC 地址、所属 VLAN 和报文入端口等信息。

ND Snooping 表项可以配合 ND Detection 功能使用。关于 ND Detection 功能的详细介绍，请参见“安全配置指导”的“ND 攻击防御”。

ND Snooping 表项可以配合 IPv6 Source Guard 功能使用。关于 IPv6 Source Guard 功能的详细介绍，请参见“安全配置指导”中的“IP Source Guard”。

下面具体介绍一下 ND Snooping 表项的建立、迁移和老化机制。（以 ND 报文为例）

#### 1. 表项建立机制

当收到未知源地址的 ND 或者数据报文后，设备会新建一个 ND Snooping 表项，此时该表项处于 INVALID 状态，随后通过接收报文的接口所属 VLAN 内的 ND 信任端口（配置了 **ipv6 nd detection trust** 命令的端口）发送两次 DAD NS 报文进行探测，报文发送的时间间隔可以由 **ipv6 nd snooping dad retrans-timer** 命令配置。如果第一次报文发出后，在 INVALID 状态的超时时间（可以由 **ipv6 nd snooping lifetime invalid** 命令配置）内未收到对应的 NA 应答，则说明局域网中不存在冲突的地址，此时该 ND Snooping 表项进入 VALID 状态；如果第一次报文发出后，在 INVALID 状态的超时时间内收到对应的 NA 应答，则说明局域网中存在冲突的地址，此时设备删除该 ND Snooping 表项。

#### 2. 表项迁移机制

表项迁移包括以下两种方式：

- 本设备迁移：当设备从相同 VLAN 内的其他 ND 非信任端口收到相同源地址的 ND 报文时，设备通过学习到 ND Snooping 表项的入端口发送两次 DAD NS 报文进行探测，报文发送的时间

间隔可以由 **ipv6 nd snooping dad retrans-timer** 命令配置。如果第一次报文发出后，在 **INVALID** 状态的超时时间内未收到对应的 **NA** 应答，则说明原用户已经跟入端口断开，则设备把该 **ND Snooping** 表项的入端口修改为收到新报文的端口；如果第一次报文发出后，在 **INVALID** 状态的超时时间内收到对应的 **NA** 应答，则该 **ND Snooping** 表项不发生变化。

- 跨设备迁移：当设备从相同 **VLAN** 内的 **ND** 信任端口收到相同源地址的 **ND** 报文时，设备通过学习到 **ND Snooping** 表项的入端口发送两次 **DAD NS** 报文进行探测。如果第一次报文发出后，在 **INVALID** 状态的超时时间内未收到对应的 **NA** 应答，则说明原用户已经跟入端口断开，则设备删除对应的 **ND Snooping** 表项，而与该 **ND** 信任端口相连的设备会开启表项创建机制并建立 **ND Snooping** 表项，完成表项的跨设备迁移。如果第一次报文发出后，在 **INVALID** 状态的超时时间内收到对应的 **NA** 应答，则说明原用户未跟入端口断开，设备会保留对应的 **ND Snooping** 表项。

### 3. 表项老化机制

如果一个 **ND Snooping** 表项自最后一次更新后，在 **VALID** 状态超时时间（可以由 **ipv6 nd snooping lifetime valid** 命令配置）内未收到 **ND** 更新报文，则进入 **INVALID** 状态，随后设备通过学习到 **ND Snooping** 表项的入端口发送两次 **DAD NS** 报文进行探测。如果第一次报文发出后，在 **INVALID** 状态的超时时间内没有收到对应的 **NA** 应答，则说明原用户已经跟入端口断开，设备删除对应的 **ND Snooping** 表项；如果第一次报文发出后，在 **INVALID** 状态的超时时间内收到对应的 **NA** 应答，则说明原用户未跟入端口断开，设备会保留对应的 **ND Snooping** 表项，重新进入 **VALID** 状态。

## 2.10.2 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 **VLAN** 视图。

```
vlan vlan-id
```

- (3) 开启学习 **ND Snooping** 表项的功能。请至少选择其中一项进行配置。

- 开启学习表项地址类型为全局单播地址的 **ND Snooping** 表项的功能。

```
ipv6 nd snooping enable global
```

- 开启学习表项地址类型为链路本地地址的 **ND Snooping** 表项的功能。

```
ipv6 nd snooping enable link-local
```

缺省情况下，学习表项地址类型为全局单播地址或链路本地地址的 **ND Snooping** 功能处于关闭状态。

- (4) （可选）开启通过 **IPv6** 数据报文学习 **ND Snooping** 表项的功能。

```
ipv6 nd snooping glean source
```

缺省情况下，通过 **IPv6** 数据报文学习 **ND Snooping** 表项的功能处于关闭状态。

本命令开启后，**VLAN** 内 **ND** 非信任端口必须开启 **IPv6 Source Guard** 功能，否则会导致该端口的报文不能正常转发。

- (5) 退回系统视图。

```
quit
```

- (6) 进入二层以太网接口视图或二层聚合接口视图。

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

- (7) (可选) 配置接口下学习 ND Snooping 表项的最大个数。

**ipv6 nd snooping max-learning-num** *max-number*

接口下学习 ND Snooping 表项的最大个数为 1024。

- (8) (可选) 配置接口为上行口, 禁止接口学习 ND Snooping 表项。

**ipv6 nd snooping uplink**

缺省情况下, ND Snooping 功能使能后, 接口上允许学习 ND Snooping 表项。

- (9) 退回系统视图。

**quit**

- (10) (可选) 配置 ND Snooping 表项的超时时间。

**ipv6 nd snooping lifetime** { **invalid** *invalid-lifetime* | **valid** *valid-lifetime* }

缺省情况下, ND Snooping 表项的 INVALID 状态 (TENTATIVE、TESTING\_TPLT 和 TESTING\_VP 状态) 的超时时间为 500 毫秒, VALID 状态的超时时间为 300 秒。

- (11) (可选) 配置发送两次 DAD NS 报文进行探测的时间间隔。

**ipv6 nd snooping dad retrans-timer** *interval*

缺省情况下, 发送两次 DAD NS 报文进行探测的时间间隔为 250 毫秒。

## 2.11 配置ND Proxy功能

### 2.11.1 功能简介

如果 NS 请求是从一个网络的主机发往同一网段却不在同一物理网络上的另一台主机, 那么连接它们的具有代理功能的设备就可以代答该请求, 回应 NA 报文, 这个过程称作 ND 代理 (ND Proxy)。

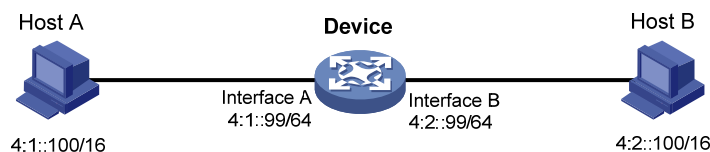
ND Proxy 功能屏蔽了分离的物理网络这一事实, 使用户使用起来, 好像在同一个物理网络上。

ND Proxy 功能根据应用场景不同分为普通 ND Proxy 和本地 ND Proxy。

#### 1. 普通ND Proxy

普通ND Proxy的典型应用环境如 图 2-3 所示。设备Device通过两个三层接口Interface A和Interface B连接两个网络, 两个三层接口的IPv6 地址不在同一个网段, 接口地址分别为 4:1::99/64、4:2::99/64。但是两个网络内的主机Host A和Host B的地址通过掩码的控制, 既与相连设备的接口地址在同一网段, 同时二者也处于同一个网段。

图2-3 普通 ND Proxy 的应用环境



在这种组网情况下, 当 Host A 需要与 Host B 通信时, 由于目的 IPv6 地址与本机的 IPv6 地址为同一网段, 因此 Host A 会直接发出请求 Host B 硬件地址的 NS 请求。但是, 此时的两台主机处于不同的广播域中, Host B 无法收到 Host A 的 NS 请求报文, 当然也就无法应答。

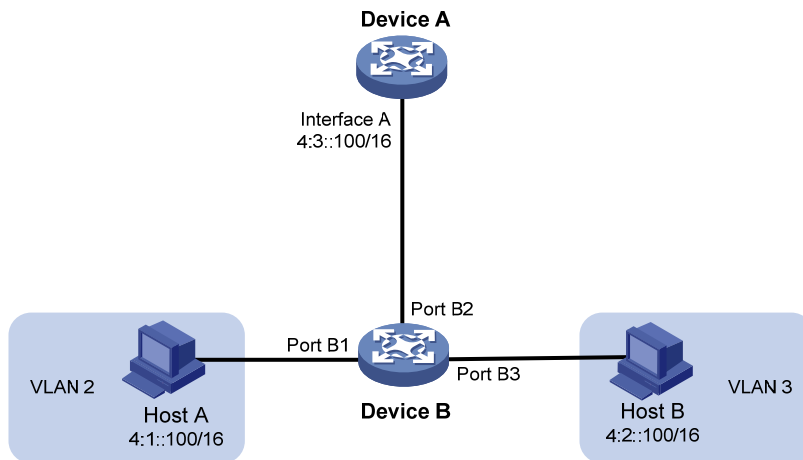


通过在 Device 上启用 ND Proxy 功能，可以解决此问题。在接口 Interface A 和 Interface B 上启用 ND Proxy 后，Device 可以应答 Host A 的 NS 请求。同时，Device 作为 Host B 的代理，把其它主机发送过来的报文转发给 Host B。这样，实现 Host A 与 Host B 之间的通信。

## 2. 本地ND Proxy

本地ND Proxy的应用场景如 图 2-4 所示。Host A属于VLAN 2，Host B属于VLAN 3。但它们分别连接到端口Port B1 和 Port B3 上。

图2-4 本地 ND Proxy 的应用环境



在这种组网情况下，当 Host A 需要与 Host B 通信时，由于目的 IPv6 地址与本机的 IPv6 地址为同一网段，因此 Host A 会直接发出请求 Host B 硬件地址的 NS 请求。但是，因为连接两台主机属于不同的 VLAN 中，Host B 无法收到 Host A 的 NS 请求报文。

通过在 Device A 上启用本地 ND Proxy 功能，可以解决此问题。在接口 Interface A 上启用本地 ND Proxy 后，Device A 会代替 Host B 回应 NA，Host A 发给 Host B 的报文就会通过 Device A 进行转发，从而实现 Host A 与 Host B 之间的通信。

本地 ND Proxy 可以在下列几种情况下实现主机之间的三层互通：

- 想要互通的主机分别连接到同一台设备的不同 VLAN 中的端口下；
- 想要互通的主机分别连接到同一个 VLAN 中的同一个隔离组内的不同二层隔离端口下；
- 开启 Private VLAN 功能后，想要互通的主机属于不同的 Secondary VLAN。

### 2.11.2 配置普通ND Proxy功能

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 开启普通 ND Proxy 功能。

```
proxy-nd enable
```

缺省情况下，ND Proxy 功能处于关闭状态。



### 2.11.3 配置本地ND Proxy功能

- (1) 进入系统视图。  
**system-view**
  - (2) 进入接口视图。  
**interface** *interface-type* *interface-number*
  - (3) 开启本地 ND Proxy 功能。  
**local-proxy-nd enable**
- 缺省情况下，本地 ND Proxy 功能处于关闭状态。

## 2.12 IPv6邻居发现显示和维护

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的运行情况，用户可以通过查看显示信息验证配置的效果。

在用户视图下，执行 **reset** 命令可以清除相应的统计信息。

表2-3 IPv6 邻居发现显示和维护

操作	命令
显示ND Snooping的表项信息	<b>display ipv6 nd snooping</b> [ [ <b>vlan</b> <i>vlan-id</i>   <b>interface</b> <i>interface-type</i> <i>interface-number</i> ] [ <b>global</b>   <b>link-local</b> ] ] [ <i>ipv6-address</i> ] [ <b>verbose</b> ]
显示ND Snooping表项数目	<b>display ipv6 nd snooping count</b> [ <b>interface</b> <i>interface-type</i> <i>interface-number</i> ]
显示邻居表项的个数	<b>display ipv6 neighbors</b> { { <b>all</b>   <b>dynamic</b>   <b>static</b> } [ <b>slot</b> <i>slot-number</i> ]   <b>interface</b> <i>interface-type</i> <i>interface-number</i>   <b>vlan</b> <i>vlan-id</i> } <b>count</b>
显示邻居信息	<b>display ipv6 neighbors</b> { { <i>ipv6-address</i>   <b>all</b>   <b>dynamic</b>   <b>static</b> } [ <b>slot</b> <i>slot-number</i> ]   <b>interface</b> <i>interface-type</i> <i>interface-number</i>   <b>vlan</b> <i>vlan-id</i> } [ <b>verbose</b> ]
显示设备支持的ND表项的最大数目	<b>display ipv6 neighbors entry-limit</b>
清除ND Snooping表项	<b>reset ipv6 nd snooping</b> [ [ <b>vlan</b> <i>vlan-id</i> ] [ <b>global</b>   <b>link-local</b> ]   <b>vlan</b> <i>vlan-id</i> <i>ipv6-address</i> ]
清除IPv6邻居信息	<b>reset ipv6 neighbors</b> { <b>all</b>   <b>dynamic</b>   <b>interface</b> <i>interface-type</i> <i>interface-number</i>   <b>slot</b> <i>slot-number</i>   <b>static</b> }

## 2.13 ND Snooping典型配置举例

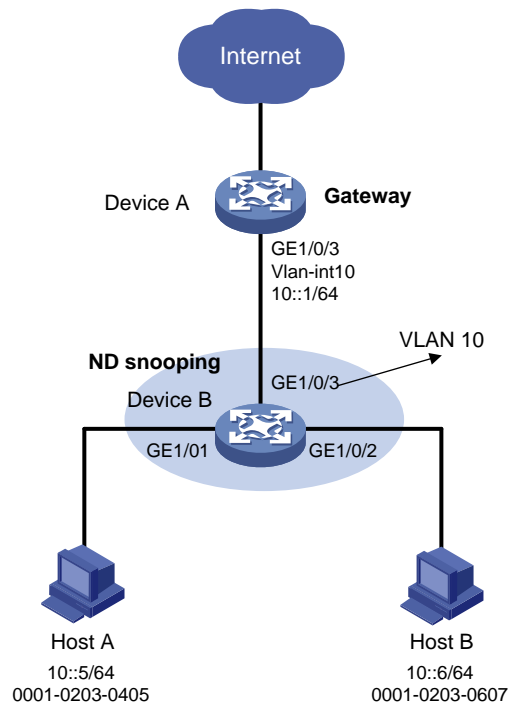
### 2.13.1 ND Snooping基本组网配置举例

#### 1. 组网需求

Host A 和 Host B 通过 Device B 连接到网关设备 Device A。要求 Device B 上可以动态产生 Host A 和 Host B 的 ND Snooping 表项。

## 2. 组网图

图2-5 ND Snooping 组网图



## 3. 配置步骤

### (1) 配置 Device A

# 创建 VLAN 10。

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] quit
```

# 配置端口 GigabitEthernet1/0/3 允许 VLAN 10 的报文通过。

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 10
[DeviceA-GigabitEthernet1/0/3] quit
```

# 配置 VLAN 接口 10 的 IPv6 地址。

```
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] ipv6 address 10::1/64
[DeviceA-Vlan-interface10] quit
```

### (2) 配置 Device B

# 创建 VLAN 10。

```
[DeviceB] vlan 10
[DeviceB-vlan10] quit
```

# 配置端口 GigabitEthernet1/0/1~GigabitEthernet1/0/3 允许 VLAN 10 的报文通过。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type access
```

```
[DeviceB-GigabitEthernet1/0/1] port access vlan 10
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type access
[DeviceB-GigabitEthernet1/0/2] port access vlan 10
[DeviceB-GigabitEthernet1/0/2] quit
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 10
[DeviceB-GigabitEthernet1/0/3] quit
```

# 在 VLAN 10 下开启学习表项类型为全局单播地址和链路本地地址的 ND Snooping 表项的功能。

```
[DeviceB] vlan 10
[DeviceB-vlan10] ipv6 nd snooping enable global
[DeviceB-vlan10] ipv6 nd snooping enable link-local
```

# VLAN 10 下配置 ND Snooping 通过数据报文学习 ND Snooping 表项的功能。

```
[DeviceB-vlan10] ipv6 nd snooping glean source
```

# 将上行端口 GigabitEthernet1/0/3 配置为 ND 信任端口，下行端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 采用缺省配置，即为 ND 非信任端口。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] ipv6 nd detection trust
[DeviceB-GigabitEthernet1/0/3] quit
```

# 配置下行端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 的 ND Snooping 表项最大学习数目 200 条。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ipv6 nd snooping max-learning-num 200
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ipv6 nd snooping max-learning-num 200
[DeviceB-GigabitEthernet1/0/2] quit
```

#### 4. 验证配置

# 在 Device B 上的 VLAN10 内可以查询到获取到的 ND Snooping 表项。

```
[DeviceB] display ipv6 nd snooping vlan 10
```

IPv6 address	MAC address	VID	Interface	Status	Age
10::5	0001-0203-0405	10	GE1/0/1	VALID	157
10::6	0001-0203-0607	10	GE1/0/2	VALID	105

# 目 录

<b>1 DHCPv6 概述 .....</b>	<b>1-1</b>
1.1 DHCPv6 的优点 .....	1-1
1.2 DHCPv6 地址/前缀分配过程.....	1-1
1.2.1 交互两个消息的快速分配过程 .....	1-1
1.2.2 交互四个消息的分配过程 .....	1-1
1.3 地址/前缀租约更新过程 .....	1-2
1.4 DHCPv6 无状态配置 .....	1-3
1.5 DHCPv6 选项介绍 .....	1-4
1.5.1 Option 18.....	1-4
1.5.2 Option 37.....	1-4
1.6 协议规范.....	1-5
<b>2 DHCPv6 服务器 .....</b>	<b>2-1</b>
2.1 DHCPv6 服务器简介 .....	2-1
2.1.1 DHCPv6 服务器应用环境.....	2-1
2.1.2 基本概念 .....	2-2
2.1.3 DHCPv6 地址池.....	2-3
2.1.4 地址/前缀的选择优先次序 .....	2-4
2.2 DHCPv6 服务器与硬件适配关系 .....	2-4
2.3 DHCPv6 服务器配置任务简介 .....	2-4
2.4 配置为DHCPv6 客户端分配IPv6 前缀 .....	2-5
2.5 配置为DHCPv6 客户端分配IPv6 地址 .....	2-6
2.6 配置为DHCPv6 客户端分配网络参数 .....	2-8
2.6.1 功能简介 .....	2-8
2.6.2 直接在DHCPv6 地址池中配置网络参数.....	2-9
2.6.3 通过DHCPv6 选项组配置网络参数.....	2-9
2.7 配置接口工作在DHCPv6 服务器模式，并配置地址/前缀分配方式 .....	2-10
2.8 配置DHCPv6 策略动态分配IPv6 地址、前缀和其他参数 .....	2-11
2.9 配置DHCPv6 服务器发送DHCPv6 报文的DSCP优先级 .....	2-12
2.10 配置DHCPv6 服务器租约固化功能.....	2-13
2.11 开启DHCPv6 服务器发布前缀路由功能 .....	2-13
2.12 开启DHCPv6 服务器的日志信息功能 .....	2-14
2.13 DHCPv6 服务器显示和维护 .....	2-14

2.14 DHCPv6 服务器典型配置举例.....	2-15
2.14.1 动态分配IPv6 前缀配置举例.....	2-15
2.14.2 动态分配IPv6 地址配置举例.....	2-18
<b>3 DHCPv6 中继 .....</b>	<b>3-1</b>
3.1 DHCPv6 中继简介 .....	3-1
3.1.1 应用环境.....	3-1
3.1.2 DHCPv6 中继的工作过程.....	3-1
3.2 DHCPv6 中继配置任务简介 .....	3-2
3.3 配置接口工作在DHCPv6 中继模式 .....	3-2
3.4 指定DHCPv6 服务器的地址 .....	3-2
3.4.1 指定DHCPv6 中继对应的DHCPv6 服务器地址.....	3-2
3.4.2 指定中继地址池上对应的DHCPv6 服务器地址.....	3-3
3.5 配置DHCPv6 中继为DHCPv6 客户端分配的网关地址 .....	3-4
3.6 配置DHCPv6 中继发送DHCPv6 报文的DSCP优先级 .....	3-4
3.7 配置DHCPv6 中继支持的Interface ID选项填充模式 .....	3-4
3.8 开启DHCPv6 中继发布前缀路由功能 .....	3-5
3.9 配置DHCPv6 中继报文填充指定源地址 .....	3-5
3.10 DHCPv6 中继显示和维护.....	3-6
3.11 DHCPv6 中继典型配置举例.....	3-6
3.11.1 DHCPv6 中继基本组网典型配置举例 .....	3-6
<b>4 DHCPv6 客户端 .....</b>	<b>4-1</b>
4.1 DHCPv6 客户端简介 .....	4-1
4.2 DHCPv6 客户端配置限制和指导 .....	4-1
4.3 DHCPv6 客户端配置任务简介 .....	4-1
4.4 配置接口使用的DHCPv6 客户端DUID .....	4-2
4.5 配置DHCPv6 客户端获取IPv6 地址和网络配置参数.....	4-2
4.6 配置DHCPv6 客户端获取IPv6 前缀和网络配置参数.....	4-2
4.7 配置DHCPv6 客户端同时获取IPv6 地址、IPv6 前缀和网络配置参数 .....	4-3
4.8 配置DHCPv6 客户端获取除地址/前缀外的其他网络配置参数.....	4-3
4.9 配置DHCPv6 客户端发送DHCPv6 报文的DSCP优先级 .....	4-4
4.10 DHCPv6 客户端显示和维护.....	4-4
4.11 DHCPv6 客户端典型配置举例.....	4-4
4.11.1 DHCPv6 客户端申请地址及网络参数配置举例 .....	4-4
4.11.2 DHCPv6 客户端申请前缀及网络参数配置举例 .....	4-6
4.11.3 DHCPv6 客户端同时申请地址、前缀及网络参数配置举例 .....	4-8
4.11.4 DHCPv6 无状态配置配置举例 .....	4-11

5 DHCPv6 Snooping.....	5-1
5.1 DHCPv6 Snooping简介 .....	5-1
5.1.1 保证客户端从合法的服务器获取IPv6 地址或IPv6 前缀 .....	5-1
5.1.2 记录DHCPv6 客户端IPv6 地址与MAC地址的对应关系.....	5-1
5.1.3 记录DHCPv6 客户端IPv6 前缀与端口的对应关系 .....	5-2
5.2 DHCPv6 snooping配置限制和指导 .....	5-2
5.3 DHCPv6 Snooping配置任务简介.....	5-2
5.4 配置DHCPv6 Snooping基本功能.....	5-2
5.4.1 在普通组网中配置DHCPv6 Snooping基本功能 .....	5-2
5.5 配置DHCPv6 Snooping支持Option 18 功能 .....	5-3
5.6 配置DHCPv6 Snooping支持Option 37 功能 .....	5-4
5.7 配置DHCPv6 Snooping表项固化功能.....	5-4
5.8 配置接口动态学习DHCPv6 Snooping表项的最大数目 .....	5-5
5.9 开启DHCPv6 Snooping报文限速功能.....	5-5
5.10 开启DHCPv6 Snooping的DHCPv6 请求方向报文检查功能 .....	5-6
5.11 开启DHCPv6 Snooping报文阻断功能 .....	5-6
5.12 开启DHCPv6 Snooping日志信息功能 .....	5-7
5.13 DHCPv6 Snooping显示和维护 .....	5-7
5.14 DHCPv6 Snooping典型配置举例 .....	5-8
5.14.1 DHCPv6 Snooping基本组网配置举例 .....	5-8

# 1 DHCPv6 概述

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

## 1.1 DHCPv6的优点

与其他 IPv6 地址分配方式（包括手工配置、通过路由器公告消息中的网络前缀无状态自动配置等，关于这两种形式的配置，请参见“三层技术-IP 业务配置指导”中的“IPv6 基础”）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。
- 为客户端分配前缀，以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、域名后缀等网络配置参数。

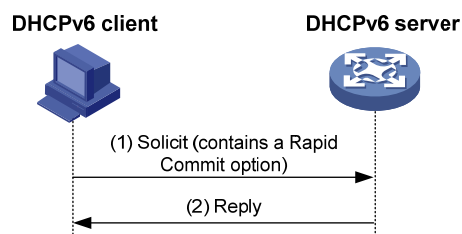
## 1.2 DHCPv6地址/前缀分配过程

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



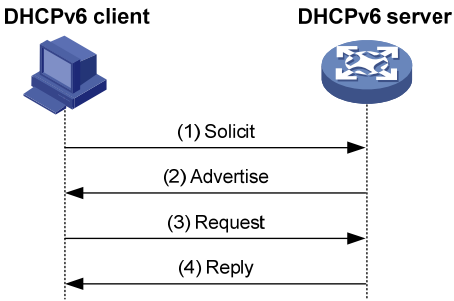
如 [图 1-1](#) 所示，地址/前缀快速分配过程为：

- (2) DHCPv6 客户端在向 DHCPv6 服务器发送的 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/前缀和其他网络配置参数。
- (3) 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](#)。

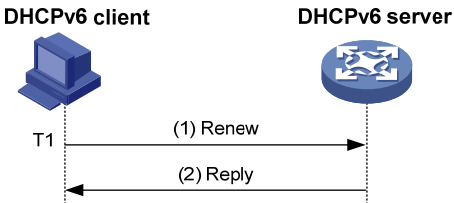
表1-1 交互四个消息的分配过程

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，该租借期限称为租约。租借期限由有效生命期决定。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，则需要申请延长地址/前缀租约。

图1-3 通过 Renew 更新地址/前缀租约

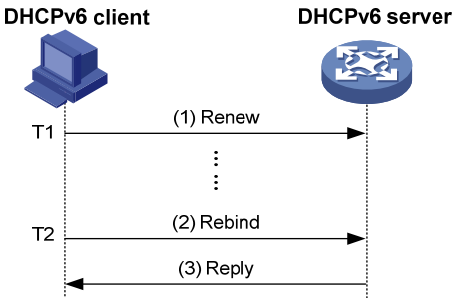


如 [图 1-3](#) 所示，地址/前缀租借时间到达时间T1（推荐值为首选生命期的一半）时，DHCPv6 客户端会向为它分配地址/前缀的DHCPv6 服务器发送Renew报文，以进行地址/前缀租约的更新。如果客户端可以继续使用该地址/前缀，则DHCPv6 服务器回应续约成功的Reply报文，通知DHCPv6 客



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



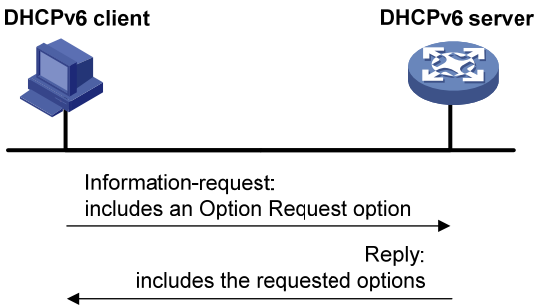
如 图 1-4 所示，如果在T1 时发送Renew请求更新租约，但是未收到DHCPv6 服务器的回应报文，则DHCPv6 客户端会在T2（推荐值为首选生命期的 0.8 倍）时，向所有DHCPv6 服务器组播发送Rebind报文请求更新租约。如果客户端可以继续使用该地址/前缀，则DHCPv6 服务器回应续约成功的Reply报文，通知DHCPv6 客户端已经成功更新地址/前缀租约；如果该地址/前缀不可以再分配给该客户端，则DHCPv6 服务器回应续约失败的Reply报文，通知客户端不能获得新的租约；如果DHCPv6 客户端未收到服务器的应答报文，则到达有效生命期后，客户端停止使用该地址/前缀。有效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

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，即 DHCPv6 客户端根据路由器发现/前缀发现所获取的信息自动配置 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）取值为 0、O 标志位（Other stateful configuration flag，其他配置标志位）取值为 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。

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：

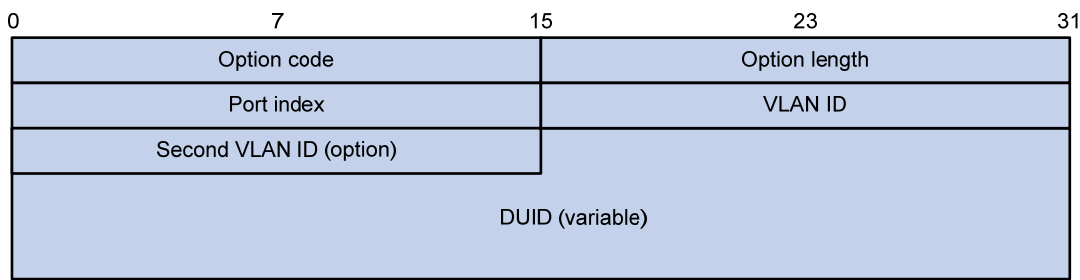
- (1) 客户端以组播的方式向 DHCPv6 服务器发送 Information-request 报文，该报文中携带 Option Request 选项，指定客户端需要从服务器获取的配置参数。
- (2) 服务器收到 Information-request 报文后，为客户端分配网络配置参数，并单播发送 Reply 报文将网络配置参数返回给客户端。
- (3) 客户端检查 Reply 报文中提供的信息，如果与 Information-request 报文中请求的配置参数相符，则按照 Reply 报文中提供的参数进行网络配置；否则，忽略该参数。如果接收到多个与请求相符的 Reply 报文，客户端将选择最先收到的 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 DHCPv6选项介绍

### 1.5.1 Option 18

Option 18 称为接口ID选项（Interface ID），设备接收到DHCPv6 客户端发送的DHCPv6 请求报文后，在该报文中添加Option 18 选项，并转发给DHCPv6 服务器。服务器可根据Option 18 选项中的客户端信息选择合适的地址池为DHCPv6 客户端分配IPv6 地址。[图 1-6](#) 为Option 18 选项格式。

图1-6 Option 18 选项格式



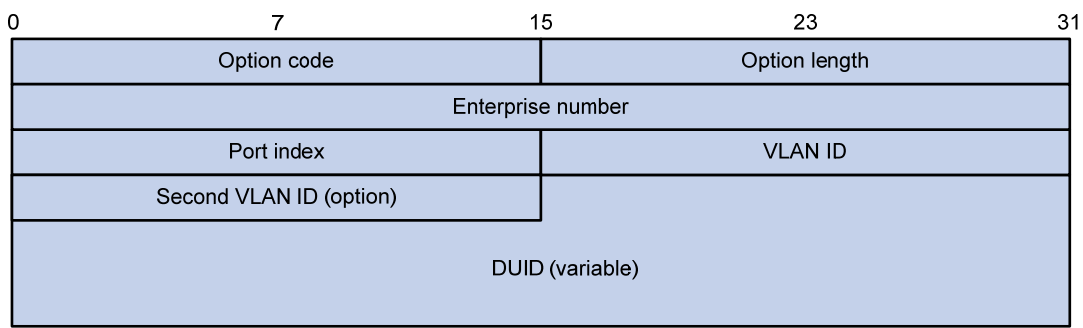
各字段的解释如下：

- Option code: Option 编号，取值为 18。
- Option length: Option 字段长度。
- Port index: DHCPv6 设备收到客户端请求报文的端口索引。
- VLAN ID: 第一层 VLAN 信息。
- Second VLAN ID: 第二层 VLAN 信息。选项格式中的 Second VLAN ID 字段为可选，如果 DHCPv6 报文中不含有 Second VLAN，则 Option 18 中也不包含 Second VLAN ID 内容。
- DUID: DHCPv6 客户端的 DUID 信息。

### 1.5.2 Option 37

Option 37 称为远程ID选项（Remote ID），设备接收到DHCPv6 客户端发送的DHCPv6 请求报文后，在该报文中添加Option 37 选项，并转发给DHCPv6 服务器。服务器可根据Option 37 选项中的信息对DHCPv6 客户端定位，为分配IPv6 地址提供帮助。[图 1-7](#) 为Option 37 选项格式。

图1-7 Option 37 选项格式



各字段的解释如下：

- Option code: Option 编号，取值为 37。
- Option length: Option 字段长度。
- Enterprise number: 企业编号。
- Port index: DHCPv6 设备收到客户端请求报文的端口索引。
- VLAN ID: 第一层 VLAN 信息。
- Second VLAN ID: 第二层 VLAN 信息。选项格式中的 Second VLAN ID 字段为可选，如果 DHCPv6 报文中不含有 Second VLAN，则 Option 37 中也不包含 Second VLAN ID 内容。
- DUID: DHCPv6 客户端的 DUID 信息。

## 1.6 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 服务器

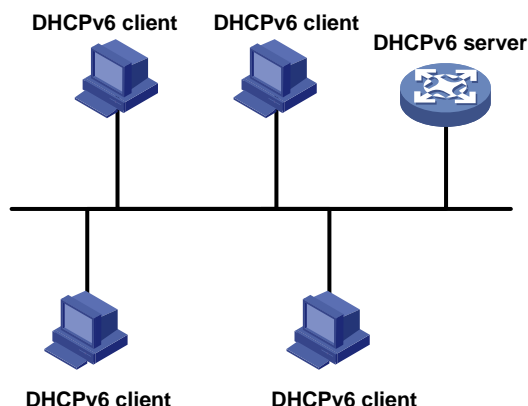
## 2.1 DHCPv6服务器简介

### 2.1.1 DHCPv6 服务器应用环境

DHCPv6 服务器可以为客户端分配 IPv6 地址/前缀和其他网络配置参数。

#### 1. DHCPv6 服务器为客户端分配IPv6 地址和其他网络配置参数

图2-1 DHCPv6 服务器为客户端分配 IPv6 地址和其他网络配置参数应用环境



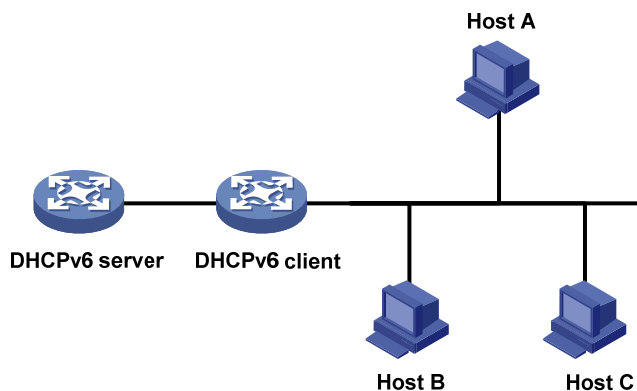
如 [图 2-1](#) 所示，为了便于集中管理IPv6 地址，简化网络配置，DHCPv6 服务器可以用来为DHCPv6 客户端提供诸如IPv6 地址、域名后缀、DNS服务器地址等网络配置参数。DHCPv6 客户端根据服务器分配的参数来实现主机的配置。

DHCPv6 服务器为客户端分配的 IPv6 地址分为以下两类：

- 临时 IPv6 地址：在短期内经常变化且不用续约的地址；
- 非临时 IPv6 地址：正常使用，可以进行续约的地址。

#### 2. DHCPv6 服务器为客户端分配IPv6 前缀

图2-2 DHCPv6 服务器前缀分配应用组网图



如 图 2-2 所示，为了便于集中管理IPv6 地址，简化网络配置，DHCPv6 服务器可以用来为DHCPv6 客户端分配IPv6 前缀。DHCPv6 客户端获取到IPv6 前缀后，向所在网络组播发送包含该前缀信息的RA消息，以便网络内的主机根据该前缀自动配置IPv6 地址。

2.1.2 基本概念

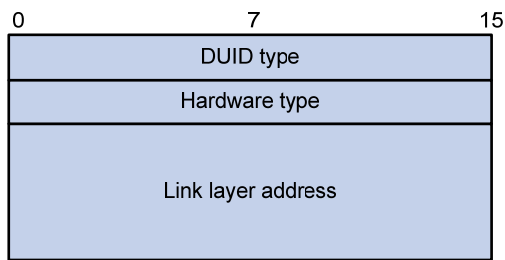
1. DHCPv6 采用的组播地址

DHCPv6 采用组播地址 FF05::1:3 来表示站点本地范围内所有的 DHCPv6 服务器；采用组播地址 FF02::1:2 来表示链路本地范围内所有的 DHCPv6 服务器和中继。

2. DUID

DUID（DHCP Unique Identifier，DHCP 唯一标识符）是一台 DHCPv6 设备（包括客户端、服务器和中继）的唯一标识。在 DHCPv6 报文交互过程中，DHCPv6 客户端、服务器和中继通过在报文中添加 DUID 来标识自己。

图2-3 DUID-LL 结构



目前，设备采用RFC 3315 规定的DUID-LL（DUID Based on Link-layer Address，基于链路层地址的DUID）作为DHCPv6 设备的标识。DUID-LL的结构如 图 2-3 所示：

- DUID type: DUID 类型。设备支持的 DUID 类型为 DUID-LL，取值为 0x0003。
- Hardware type: 硬件类型。设备支持的硬件类型为以太网，取值为 0x0001。
- Link layer address: 链路层地址。取值为设备的桥 MAC 地址。

3. IA

IA（Identity Association，标识联盟）用于管理分配给客户端的一组地址和前缀等信息，通过 IAID 标识。一个客户端可以有多个 IA，如客户端的每个接口拥有一个 IA，IA 用来管理该接口获取的地址和前缀等信息。

4. IAID

IAID 是 IA 的标识符，由客户端选择。在一个客户端上不同 IA 的 IAID 不能相同。

5. PD

PD（Prefix Delegation，前缀授权）是 DHCPv6 服务器为分配的前缀创建的前缀绑定信息，前缀绑定信息中记录了 IPv6 前缀、客户端 DUID、IAID、有效时间、首选时间、租约过期时间、申请前缀的客户端的 IPv6 地址等信息。

### 2.1.3 DHCPv6 地址池

每个 DHCPv6 地址池都拥有一组可供分配的 IPv6 地址、IPv6 前缀和网络配置参数。DHCPv6 服务器从地址池中为客户端选择并分配 IPv6 地址、IPv6 前缀及其他参数。

#### 1. DHCPv6 地址池的地址管理方式

DHCPv6 地址池的地址管理方式有以下几种：

- 静态绑定 IPv6 地址：通过将客户端 DUID 和 IAID 与 IPv6 地址绑定的方式，实现为特定的客户端分配特定的 IPv6 地址；
- 动态选择 IPv6 地址：在地址池中指定可供分配的 IPv6 地址范围，当收到客户端的 IPv6 地址申请时，从该地址范围中动态选择 IPv6 地址，分配给该客户端。

在 DHCPv6 地址池中指定可供分配的 IPv6 地址范围时，需要：

- (1) 指定动态分配的 IPv6 地址网段。
- (2) 将该网段划分为非临时地址范围和临时地址范围。每个地址范围内的地址必须属于该网段，否则无法分配。

采用动态选择 IPv6 地址方式时，如果接收到客户端的地址申请，则 DHCPv6 服务器选择一个合适的地址池，并按照客户端申请的地址类型（非临时地址或临时地址），从该地址池对应的地址范围（非临时地址范围或临时地址范围）中选择合适的 IPv6 地址分配给客户端。

#### 2. DHCPv6 地址池的前缀管理方式

DHCPv6 地址池的前缀管理方式有以下几种：

- 静态绑定 IPv6 前缀：通过将客户端 DUID 和 IAID 与 IPv6 前缀绑定的方式，实现为特定的客户端分配特定的 IPv6 前缀；
- 动态选择 IPv6 前缀：在地址池中指定可供分配的 IPv6 前缀范围，当收到客户端的 IPv6 前缀申请时，从该前缀范围中动态选择 IPv6 前缀，分配给该客户端。

在 DHCPv6 地址池中指定可供分配的 IPv6 前缀范围时，需要：

- (1) 创建前缀池，指定前缀池中包括的 IPv6 前缀范围。
- (2) 在地址池中指定动态分配的 IPv6 地址网段。
- (3) 在地址池中引用前缀池。

#### 3. 地址池的选取原则

DHCPv6 服务器为客户端分配 IPv6 地址或前缀时，按照如下顺序选择地址池：

- (1) 如果存在将客户端 DUID、IAID 与 IPv6 地址或前缀静态绑定的地址池，则选择该地址池，并将静态绑定的 IPv6 地址或前缀、及该地址池中的网络参数分配给客户端。
- (2) 如果接收到 DHCPv6 请求报文的接口引用了某个地址池，则选择该地址池，从该地址池中选取 IPv6 地址或前缀、及网络配置参数分配给客户端。
- (3) 如果配置了 DHCPv6 策略，则 DHCPv6 客户端匹配某个 DHCPv6 用户类时，DHCPv6 服务器选择与该 DHCPv6 用户类关联的 DHCPv6 地址池；DHCPv6 客户端未匹配到 DHCPv6 用户类时，若配置了默认 DHCPv6 地址池，则选择该 DHCPv6 地址池；若未配置默认 DHCPv6 地址池或 DHCPv6 默认地址池不存在可供分配的 IPv6 地址或前缀时，IPv6 地址、前缀或其他参数分配失败。
- (4) 如果上述条件均不满足，则使用以下方法选择 DHCPv6 地址池：

- 如果客户端与服务器在同一网段，则将接收到 DHCPv6 请求报文的接口的 IPv6 地址与所有地址池配置的网段进行匹配，并选择最长匹配的网段所对应的地址池。
- 如果客户端与服务器不在同一网段，即客户端通过 DHCPv6 中继获取 IPv6 地址或前缀，则将离 DHCPv6 客户端最近的 DHCPv6 中继接口的 IPv6 地址与所有地址池配置的网段进行匹配，并选择最长匹配的网段所对应的地址池。

配置地址池动态分配的网段和 IPv6 地址范围时，请尽量保证与 DHCPv6 服务器接口或 DHCPv6 中继接口的 IPv6 地址所在的网段一致，以免分配错误的 IPv6 地址。

### 2.1.4 地址/前缀的选择优先次序

DHCPv6 服务器为客户端分配 IPv6 地址/前缀的优先次序如下：

- (1) DUID、IAID 与客户端 DUID、IAID 匹配，且与客户端期望地址/前缀匹配的静态绑定地址/前缀；
- (2) DUID、IAID 与客户端 DUID、IAID 匹配的静态绑定地址/前缀；
- (3) DUID 与客户端的 DUID 匹配，且与客户端期望地址/前缀匹配的静态绑定地址/前缀，该地址/前缀中未指定客户端的 IAID；
- (4) DUID 与客户端 DUID 匹配的静态绑定地址/前缀，该地址/前缀中未指定客户端的 IAID；
- (5) 服务器记录的曾经分配给客户端的地址/前缀；
- (6) 当配置了 DHCPv6 地址池按照 EUI-64 方式分配 IPv6 地址时，地址池会使用客户端的 MAC 地址按照 EUI-64 方式生成的地址；
- (7) 地址池/前缀池中与客户端期望地址/前缀匹配的空闲地址/前缀；
- (8) 地址池/前缀池中的其他空闲地址/前缀；
- (9) 如果未找到可用的地址/前缀，则依次查询租约过期地址/前缀、曾经发生过冲突的地址，如果找到则进行分配，否则将不予处理。

如果客户端的网段发生变化，服务器不会为客户端分配曾经分配给它的地址/前缀，而是从匹配新网段的地址池中重新选择地址/前缀等信息。



#### 说明

使用曾经发生过冲突的 IPv6 地址时，只有冲突状态超过一小时的地址租约才能够被服务器分配给新的 DHCPv6 客户端。

## 2.2 DHCPv6服务器与硬件适配关系

S5110V2-SI 和 S5000V3-EI 系列交换机不支持本特性。

## 2.3 DHCPv6服务器配置任务简介

DHCPv6 服务器配置任务如下：

- (1) 配置为 DHCPv6 客户端分配 IPv6 前缀、IPv6 地址和其他网络参数  
请至少选择以下一项任务进行配置：



- [配置为DHCPv6 客户端分配IPv6 前缀](#)
  - [配置为DHCPv6 客户端分配IPv6 地址](#)
  - [配置为DHCPv6 客户端分配网络参数](#)
- (2) 修改 DHCPv6 服务器的地址池选择方式  
请至少选择以下一项任务进行配置：
- [配置接口工作在DHCPv6 服务器模式，并配置地址/前缀分配方式](#)
  - [配置DHCPv6 策略动态分配IPv6 地址、前缀和其他参数](#)
- (3) （可选）[配置DHCPv6 服务器发送DHCPv6 报文的DSCP优先级](#)
- (4) （可选）[配置DHCPv6 服务器租约固化功能](#)
- (5) （可选）[开启DHCPv6 服务器发布前缀路由功能](#)
- (6) （可选）[开启DHCPv6 服务器的日志信息功能](#)

## 2.4 配置为DHCPv6客户端分配IPv6前缀

### 1. 功能简介

可以通过以下两种方式配置 DHCPv6 服务器为 DHCPv6 客户端分配 IPv6 前缀：

- 在地址池中配置静态绑定前缀：指定 DUID、IAID 及前缀的静态绑定关系后，如果 DHCPv6 请求报文中的 DUID、IAID 与静态绑定的 DUID、IAID 都相同，则将静态绑定的前缀分配给此 DHCPv6 客户端。如果只指定了 DUID 和前缀的绑定关系，未指定静态绑定的 IAID，则只要请求报文中的 DUID 与静态绑定的 DUID 相同，就将静态绑定的前缀分配给此 DHCPv6 客户端。
- 在地址池中引用包含一定前缀范围的前缀池：接收到 DHCPv6 客户端的前缀分配请求后，DHCPv6 服务器从前缀范围中动态选择可用前缀，分配给客户端。

在实际组网中，某些前缀是保留前缀，不应该动态分配给客户端。通过配置不参与自动分配的前缀，可以避免 DHCPv6 服务器分配这些前缀。

### 2. 配置限制和指导

配置为 DHCPv6 客户端分配 IPv6 前缀时，需要注意：

- 一个 IPv6 前缀只能与一个客户端绑定。不允许通过重复执行 **static-bind prefix** 命令的方式修改 IPv6 前缀与客户端的绑定关系、前缀的首选生命期和有效生命期。只有删除该 IPv6 前缀的静态绑定配置后，才能将该 IPv6 前缀与其他客户端绑定，或修改前缀的首选生命期和有效生命期。
- 一个地址池最多可以引用一个前缀池。
- 地址池可以引用并不存在的前缀池，但是，此时设备无法从该地址池中动态选择前缀分配给客户端。只有创建该前缀池后，才能支持前缀的动态选择。
- 不允许通过重复执行 **prefix-pool** 命令的方式修改地址池引用的前缀池、前缀的首选生命期和有效生命期。只有取消当前地址池引用的前缀池后，才能引用其他的前缀池，或修改首选生命期和有效生命期。

### 3. 配置步骤

- (1) 进入系统视图。



**system-view**

- (2) (可选) 配置不参与自动分配的 IPv6 前缀。

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

缺省情况下，DHCPv6 前缀池中的所有 IPv6 前缀都参与自动分配。

如果通过 **ipv6 dhcp server forbidden-prefix** 命令将已经静态绑定的 IPv6 前缀配置为不参与自动分配的前缀，则该前缀仍然可以分配给静态绑定的用户。

- (3) 创建前缀池。

```
ipv6 dhcp prefix-pool prefix-pool-number prefix { prefix-number |  
prefix/prefix-len } assign-len assign-len
```

仅在 DHCPv6 服务器为 DHCPv6 客户端动态分配 IPv6 前缀时需要进行本配置。

当配置前缀池引用前缀编号时，必须保证指定前缀号有对应的生效前缀，否则配置不生效。

- (4) 创建 DHCPv6 地址池，并进入 DHCPv6 地址池视图。

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

- (5) 配置动态分配的 IPv6 地址网段。

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

缺省情况下，未配置动态分配的 IPv6 地址网段。

不能在不同地址池下使用 **network** 命令配置相同的地址网段。

不能在不同地址池下引用完全一致的前缀编号、子前缀和子前缀长度。

- (6) 配置地址池引用前缀信息。请至少选择其中一项进行配置。

- 配置静态绑定前缀。

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

缺省情况下，未配置地址池的静态绑定前缀。

重复执行 **static-bind prefix** 命令，可以配置多个静态绑定的 IPv6 前缀。

- 配置地址池引用前缀池。

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

缺省情况下，未配置可动态分配的前缀。

## 2.5 配置为DHCPv6客户端分配IPv6地址

### 1. 功能简介

可以通过以下两种方式配置 DHCPv6 服务器为 DHCPv6 客户端分配 IPv6 地址：

- 在地址池中配置静态绑定地址：指定 DUID、IAID 及地址的静态绑定关系后，如果 DHCPv6 请求报文中的 DUID、IAID 与静态绑定的 DUID、IAID 都相同，则将静态绑定的地址分配给此 DHCPv6 客户端。如果只指定了 DUID 和地址的绑定关系，未指定静态绑定的 IAID，则只要

请求报文中的 DUID 与静态绑定的 DUID 相同，就将静态绑定的地址分配给此 DHCPv6 客户端。

- 在地址池中配置动态分配的地址网段和地址范围：
  - 在进行非临时地址分配时，如果未在地址池下通过 **address range** 命令配置动态分配的 IPv6 非临时地址范围，则 **network** 命令指定的网段内的单播地址都可以分配给 DHCPv6 客户端。如果配置了 **address range** 命令，则只会从该地址范围内分配 IPv6 非临时地址，即使该范围内的地址分配完毕，也不会从 **network** 命令指定的地址范围内分配 IPv6 非临时地址。
  - 在进行临时地址分配时，如果未在地址池下通过 **temporary address range** 命令配置动态分配的 IPv6 临时地址范围，则地址池无法分配临时地址。如果配置了 **temporary address range** 命令，则只会从该地址范围内分配 IPv6 临时地址，不会从 **network** 或者 **address range** 命令配置的地址范围内分配临时地址。

在实际组网中，某些地址是服务器的地址或者是保留地址，不应该动态分配给客户端。通过配置不参与自动分配的地址，可以避免 DHCPv6 服务器分配这些地址。

## 2. 配置限制和指导

配置为 DHCPv6 客户端分配 IPv6 地址，需要注意：

- 一个地址池下只能配置一个 IPv6 非临时地址范围和一个 IPv6 临时地址范围。
- **address range** 命令和 **temporary address range** 命令配置的地址范围应该在 **network** 命令配置的网段内，否则地址不能被分配。
- 一个地址池最多可以引用一个前缀池。地址池可以引用并不存在的前缀池，但是，此时设备无法从该地址池中动态选择前缀分配给客户端。只有创建该前缀池后，才能支持前缀的动态选择。
- 一个 IPv6 地址只能与一个客户端绑定。不允许通过重复执行 **static-bind address** 命令的方式修改 IPv6 地址与客户端的绑定关系、地址的首选生命期和有效生命期。只有删除该 IPv6 地址的静态绑定配置后，才能通过重新配置将该 IPv6 地址与其他客户端绑定，或修改地址的首选生命期和有效生命期。
- 每个 DHCPv6 地址池只能配置一个网段，在相同地址池中重复执行 **network** 命令，新的配置会覆盖已有配置。如果相邻两次 **network** 命令配置的地址网段相同而首选生命期和有效生命期不同，则新配置的首选生命期和有效生命期只能在新生成的绑定信息中生效，原有绑定信息不受影响。

## 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) （可选）配置不参与自动分配的 IPv6 地址。

```
ipv6 dhcp server forbidden-address start-ipv6-address  
[ end-ipv6-address ]
```

缺省情况下，除 DHCPv6 服务器接口的 IPv6 地址外，DHCPv6 地址池中的所有 IPv6 地址都参与自动分配。

如果通过 **ipv6 dhcp server forbidden-address** 命令将已经静态绑定的 IPv6 地址配置为不参与自动分配的地址，则该地址仍然可以分配给静态绑定的用户。

- (3) 进入 DHCPv6 地址池视图。

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

- (4) 配置动态分配的 IPv6 地址网段。

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

缺省情况下，未配置动态分配的 IPv6 地址网段。

不能在不同地址池下使用 **network** 命令配置相同的地址网段。

不能在不同地址池下引用完全一致的前缀编号、子前缀和子前缀长度。

- (5) （可选）配置动态分配的 IPv6 非临时地址范围。

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

缺省情况下，未配置地址池中动态分配的 IPv6 非临时地址范围，整个网段内的单播地址都可以作为非临时地址分配给客户端。

- (6) （可选）配置动态分配的 IPv6 临时地址范围。

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

缺省情况下，未配置动态分配的 IPv6 临时地址范围，不能分配 IPv6 临时地址。

- (7) （可选）配置 DHCPv6 地址池按照 EUI-64 方式分配 IPv6 地址。

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

缺省情况下，DHCPv6 地址池不按照 EUI-64 方式分配 IPv6 地址。

配置本命令后，当 DHCPv6 服务器收到 DHCPv6 客户端的请求报文时，DHCPv6 服务器会使用请求报文中的客户端 MAC 地址通过 EUI-64 方式生成 IPv6 地址，并将该 IPv6 地址分配给 DHCPv6 客户端。

- (8) （可选）配置静态绑定的 IPv6 地址。

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

缺省情况下，不存在静态绑定的 IPv6 地址。

重复执行 **static-bind address** 命令，可以配置多个静态绑定的 IPv6 地址。

## 2.6 配置为DHCPv6客户端分配网络参数

### 2.6.1 功能简介

除了分配 IPv6 地址和 IPv6 前缀外，DHCPv6 地址池中还可以配置其他网络参数，如在一个地址池下最多可以配置 8 个 DNS 服务器地址、1 个域名、8 个 SIP 服务器地址和 8 个 SIP 服务器域名等。可以通过如下方式配置为 DHCPv6 客户端分配的网络参数：

- 直接在 DHCPv6 地址池视图下配置网络参数。
- 在 DHCPv6 选项组中配置网络参数，并在 DHCPv6 地址池视图下指定引用的 DHCPv6 选项组。

直接在 DHCPv6 地址池视图下配置的网络参数的优先级高于 DHCPv6 选项组中配置的网络参数。

## 2.6.2 直接在DHCPv6 地址池中配置网络参数

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 DHCPv6 地址池视图。

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

- (3) 配置动态分配的 IPv6 地址网段。

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

缺省情况下，未配置动态分配的 IPv6 地址网段。

不能在不同地址池下使用 **network** 命令配置相同的地址网段。

不能在不同地址池下引用完全一致的前缀编号、子前缀和子前缀长度。

地址池引用前缀编号分配动态地址时必须保证前缀号有对应的生效前缀，否则配置不生效。

- (4) 配置为客户端分配的 DNS 服务器地址。

```
dns-server ipv6-address
```

缺省情况下，未指定为客户端分配的 DNS 服务器地址。

- (5) 配置为客户端分配的域名。

```
domain-name domain-name
```

缺省情况下，未指定为客户端分配的域名。

- (6) 配置为客户端分配的 SIP 服务器地址或域名。

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

缺省情况下，未指定为客户端分配的 SIP 服务器地址或域名。

- (7) 配置 DHCPv6 自定义选项。

```
option code hex hex-string
```

缺省情况下，未配置 DHCPv6 自定义选项。

## 2.6.3 通过DHCPv6 选项组配置网络参数

### 1. 功能简介

DHCPv6 选项组的创建方法有以下几种：

- 通过 **ipv6 dhcp option-group** 命令手工创建静态 DHCPv6 选项组。
- 设备作为 DHCPv6 客户端获取 IPv6 地址、前缀和网络配置参数时，在 DHCPv6 客户端上根据获取的网络配置参数动态创建 DHCPv6 选项组。

手工创建的 DHCPv6 选项组优先级高于动态创建的 DHCPv6 选项组。本节只介绍手工创建静态 DHCPv6 选项组的方法，动态创建 DHCPv6 选项组的方法请参见“三层技术-IP 业务配置指导”中的“DHCPv6 客户端”。

## 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 手工创建静态 DHCPv6 选项组，并进入 DHCPv6 选项组视图。

```
ipv6 dhcp option-group option-group-number
```

- (3) 配置为客户端分配的 DNS 服务器地址。

```
dns-server ipv6-address
```

缺省情况下，未指定为客户端分配的 DNS 服务器地址。

- (4) 配置为客户端分配的域名后缀。

```
domain-name domain-name
```

缺省情况下，未指定为客户端分配的域名后缀。

- (5) 配置为客户端分配的 SIP 服务器地址或域名。

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

缺省情况下，未指定为客户端分配的 SIP 服务器地址或域名。

- (6) 配置 DHCPv6 自定义选项。

```
option code hex hex-string
```

缺省情况下，未配置 DHCPv6 自定义选项。

- (7) 退回系统视图。

```
quit
```

- (8) 进入 DHCPv6 地址池视图。

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

- (9) 配置 DHCPv6 地址池引用选项组。

```
option-group option-group-number
```

缺省情况下，DHCPv6 地址池未引用选项组。

## 2.7 配置接口工作在DHCPv6服务器模式，并配置地址/前缀分配方式

### 1. 功能简介

配置接口工作在 DHCPv6 服务器模式后，当接口未引用地址池时，接口收到 DHCPv6 客户端发来的 DHCPv6 报文时，服务器根据该接口的地址或 DHCPv6 中继接口的地址选择最长匹配的 DHCPv6 地址池，并从该地址池中选择 IPv6 地址或前缀分配给客户端。当接口引用地址池时，则从引用的地址池中选择 IPv6 地址或前缀分配给客户端。如果引用的地址池中不存在可供分配的 IPv6 地址或前缀，则设备将无法为客户端分配 IPv6 地址或前缀。

### 2. 配置限制和指导

配置接口工作在 DHCPv6 服务器模式，并配置地址/前缀分配方式时，需要注意：

- 一个接口不能同时作为 DHCPv6 服务器和 DHCPv6 中继。

- 建议不要在一个接口上同时配置 DHCPv6 服务器和 DHCPv6 客户端功能。
- 接口可以引用并不存在的地址池，但是，此时该接口无法为客户端分配前缀等信息。只有创建该地址池后，才能为客户端分配前缀等信息。

### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置接口工作在 DHCPv6 服务器模式。

```
ipv6 dhcp select server
```

缺省情况下，接口未工作在 DHCPv6 服务器模式，也未工作在 DHCPv6 中继模式，接口接收到 DHCPv6 客户端发来的 DHCPv6 报文后，丢弃该报文。

- (4) 配置地址池选择方式。请选择其中一项进行配置。

- 配置全局查找地址池，并指定全局查找 DHCPv6 地址池时地址或前缀分配方式。

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

缺省情况下，不支持期望地址/前缀分配，缺省优先级为 0，不支持快速分配。

- 配置接口引用 DHCP 地址池。

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

## 2.8 配置DHCPv6策略动态分配IPv6地址、前缀和其他参数

### 1. 功能简介

创建 DHCPv6 策略，并在接口引用该策略后，该接口接收到 DHCPv6 请求报文时，则根据配置顺序逐个匹配 DHCPv6 策略中通过 **class pool** 命令指定的 DHCPv6 用户类。匹配情况如下：

- 若匹配 DHCPv6 用户类成功，当该 DHCPv6 用户类关联的 DHCPv6 地址池中存在可供分配的地址或前缀信息时，则从该 DHCPv6 地址池中分配 IPv6 地址、前缀或其他参数；当该 DHCPv6 用户类关联的 DHCPv6 地址池中不存在可供分配的地址或前缀信息时，IPv6 地址、前缀或其他参数分配失败。
- 若匹配 DHCPv6 策略中的所有 DHCPv6 用户类失败，当配置了默认 DHCPv6 地址池时，则从该 DHCPv6 地址池中分配 IPv6 地址、前缀或网络参数；当未配置默认 DHCPv6 地址池或 DHCPv6 默认地址池不存在可供分配的 IPv6 地址或前缀时，IPv6 地址、前缀或其他参数分配失败。
- 若接收 DHCPv6 请求报文的接口引用的 DHCPv6 策略不存在或匹配的 DHCPv6 用户类关联的 DHCPv6 地址池不存在，IPv6 地址、前缀或其他参数分配失败。
- 匹配规则中不支持匹配 DHCPv6 设备添加的选项，比如 Option 18 或 Option 37。

### 2. 配置步骤

- (1) 进入系统视图。



**system-view**

- (2) 创建 DHCPv6 用户类，并进入 DHCPv6 用户类视图。

**ipv6 dhcp class** *class-name*

- (3) 配置 DHCPv6 用户类的匹配规则。

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

缺省情况下，未配置 DHCPv6 用户类的匹配规则。

- (4) 退回系统视图。

**quit**

- (5) 创建 DHCPv6 策略，并进入 DHCPv6 策略视图。

**ipv6 dhcp policy** *policy-name*

DHCPv6 策略需要在接口上引用才生效。

- (6) 指定 DHCPv6 用户类关联的 DHCPv6 地址池。

**class** *class-name* **pool** *pool-name*

缺省情况下，未指定 DHCPv6 用户类关联的 DHCPv6 地址池。

- (7) （可选）指定默认 DHCPv6 地址池。

**default pool** *pool-name*

缺省情况下，未指定默认 DHCPv6 地址池。

- (8) 退回系统视图。

**quit**

- (9) 进入接口视图。

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

- (10) 指定接口引用的 DHCPv6 策略。

**ipv6 dhcp apply-policy** *policy-name*

缺省情况下，接口未引用 DHCPv6 策略。

## 2.9 配置DHCPv6服务器发送DHCPv6报文的DSCP优先级

### 1. 功能简介

DSCP 优先级用来体现报文自身的优先等级，决定报文传输的优先程度。通过本配置可以指定 DHCPv6 服务器发送的 DHCPv6 报文的 DSCP 优先级。

### 2. 配置步骤

- (1) 进入系统视图。

**system-view**

- (2) 配置 DHCPv6 服务器发送 DHCPv6 报文的 DSCP 优先级。

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

缺省情况下，DHCPv6 服务器发送的 DHCPv6 报文的 DSCP 优先级为 56。

## 2.10 配置DHCPv6服务器租约固化功能

### 1. 功能简介

DHCPv6 服务器重启后，设备上记录的租约信息将丢失，会影响 DHCP 服务器的正常业务。

DHCPv6 服务器租约固化功能将 DHCPv6 服务器的核心运行数据（在用地址租约、冲突表项）保存到指定的文件中，DHCPv6 服务器设备重启后，自动根据该文件恢复 DHCPv6 服务器的租约信息，从而保证 DHCPv6 服务器的租约信息不会丢失。

当 DHCPv6 服务器设备重启后，自动根据该文件恢复 DHCPv6 服务器的租约信息，租约恢复的过程中，DHCPv6 服务器不能提供 DHCPv6 业务。所以当恢复过程出现问题导致恢复过程无法结束时，用户可配置 **ipv6 dhcp server database update stop** 命令终止当前的 DHCPv6 服务器表项恢复操作，以便 DHCPv6 服务器能及时提供 DHCPv6 服务。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 指定存储 DHCPv6 服务器表项的文件名称。

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

缺省情况下，未指定存储文件名称。

执行本命令后，会立即触发一次表项备份。

- (3) （可选）将当前的 DHCPv6 服务器表项保存到用户指定的文件中。

```
ipv6 dhcp server database update now
```

本命令只用来触发一次 DHCPv6 服务器表项的备份。

- (4) （可选）配置刷新 DHCPv6 服务器表项存储文件的延迟时间。

```
ipv6 dhcp server database update interval interval
```

缺省情况下，若 DHCPv6 服务器表项不变化，则不刷新存储文件；若 DHCPv6 服务器表项发生变化，默认在 300 秒之后刷新存储文件。

- (5) （可选）终止当前的 DHCPv6 服务器表项恢复操作。

```
ipv6 dhcp server database update stop
```

本命令只用来触发一次终止 DHCPv6 服务器表项信息的恢复。

## 2.11 开启DHCPv6服务器发布前缀路由功能

### 1. 功能简介

DHCPv6 客户端获取到 IPv6 前缀后，通过该 IPv6 前缀为下行网络内的主机分配 IPv6 地址。此时，DHCPv6 客户端与网络内的主机不在同一网段内，会导致主机无法与外界通信。为了解决这个问题，当 DHCPv6 服务器和 DHCPv6 客户端在同一个链路范围内时，需要在 DHCPv6 服务器上开启发布前缀路由功能。

### 2. 配置步骤

- (1) 进入系统视图。



**system-view**

- (2) 开启 DHCPv6 服务器发布前缀路由功能。

**ipv6 dhcp advertise pd-route**

缺省情况下，DHCPv6 服务器发布前缀路由功能处于关闭状态。

## 2.12 开启DHCPv6服务器的日志信息功能

### 1. 功能简介

DHCPv6 服务器日志可以方便管理员定位问题和解决问题。设备生成 DHCPv6 日志信息会交给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

### 2. 配置限制和指导

大量 DHCPv6 客户端发生上下线操作时，DHCPv6 服务器需要输出大量日志信息，这可能会降低设备性能，影响 DHCPv6 服务器分配 IPv6 前缀或 IPv6 地址的速度。为了避免该情况的发生，用户可以关闭 DHCPv6 服务器日志信息功能，使得 DHCPv6 服务器不再输出日志信息。

### 3. 配置步骤

- (1) 进入系统视图。

**system-view**

- (2) 开启 DHCPv6 服务器日志信息功能。

**ipv6 dhcp log enable**

缺省情况下，DHCPv6 服务器日志信息功能处于关闭状态。

## 2.13 DHCPv6服务器显示和维护

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 服务器的运行情况，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 服务器的统计信息。

表2-1 DHCPv6 服务器显示和维护

操作	命令
显示本设备的DUID	<b>display ipv6 dhcp duid</b>
显示DHCPv6选项组信息	<b>display ipv6 dhcp option-group</b> [ option-group-number ]
显示DHCPv6地址池的信息	<b>display ipv6 dhcp pool</b> [ pool-name ]
显示前缀池的信息	<b>display ipv6 dhcp prefix-pool</b> [ prefix-pool-number ]
显示接口上的DHCPv6服务器信息	<b>display ipv6 dhcp server</b> [ interface interface-type interface-number ]
显示DHCPv6地址冲突信息	<b>display ipv6 dhcp server conflict</b> [ address ipv6-address ]
显示DHCPv6服务器表项备份信息	<b>display ipv6 dhcp server database</b>

操作	命令
显示租约过期的DHCPv6地址绑定信息	<b>display ipv6 dhcp server expired</b> [ <b>address</b> <i>ipv6-address</i>   <b>pool</b> <i>pool-name</i> ]
显示DHCPv6地址绑定信息	<b>display ipv6 dhcp server ip-in-use</b> [ <b>address</b> <i>ipv6-address</i>   <b>pool</b> <i>pool-name</i> ]
显示DHCPv6前缀绑定信息	<b>display ipv6 dhcp server pd-in-use</b> [ <b>pool</b> <i>pool-name</i>   [ <b>prefix</b> <i>prefix/prefix-len</i> ] ]
显示DHCPv6服务器的报文统计信息	<b>display ipv6 dhcp server statistics</b> [ <b>pool</b> <i>pool-name</i> ]
清除DHCPv6地址冲突信息	<b>reset ipv6 dhcp server conflict</b> [ <b>address</b> <i>ipv6-address</i> ]
清除租约过期的DHCPv6地址绑定信息	<b>reset ipv6 dhcp server expired</b> [ <b>address</b> <i>ipv6-address</i>   <b>pool</b> <i>pool-name</i> ]
清除DHCPv6的正式地址绑定和临时地址绑定信息	<b>reset ipv6 dhcp server ip-in-use</b> [ <b>address</b> <i>ipv6-address</i>   <b>pool</b> <i>pool-name</i> ]
清除DHCPv6正式前缀绑定和临时前缀绑定信息	<b>reset ipv6 dhcp server pd-in-use</b> [ <b>pool</b> <i>pool-name</i>   <b>prefix</b> <i>prefix/prefix-len</i> ]
清除DHCPv6服务器的报文统计信息	<b>reset ipv6 dhcp server statistics</b>

## 2.14 DHCPv6服务器典型配置举例

### 2.14.1 动态分配IPv6 前缀配置举例

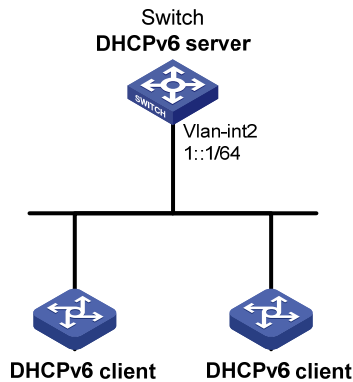
#### 1. 组网需求

DHCPv6 客户端从 DHCPv6 服务器获取 IPv6 地址前缀，以及网络配置参数：DNS 服务器地址、域名、SIP 服务器地址和 SIP 服务器域名。其中：

- Switch 作为 DHCPv6 服务器，地址为 1::1/64。
- DHCPv6 服务器为 DUID 为 00030001CA0006A40000 的客户端固定分配前缀 2001:0410:0201::/48；为其他客户端分配 2001:0410::/48～2001:0410:FFFF::/48 之间除 2001:0410:0201::/48 外的前缀。
- DNS 服务器地址为 2:2::3。
- DHCPv6 客户端所属域的域名后缀为 aaa.com。
- SIP 服务器地址为 2:2::4，域名为 bbb.com。

## 2. 组网图

图2-4 DHCPv6 服务器配置组网图



## 3. 配置步骤

### (1) 配置 DHCPv6 服务器

# 配置 VLAN 接口 2 的 IPv6 地址。取消设备发布 RA 消息的抑制。配置被管理地址的配置标志位为 1，即主机通过 DHCPv6 服务器获取 IPv6 地址。配置其他信息配置标志位为 1，即主机通过 DHCPv6 服务器获取除 IPv6 地址以外的其他信息。

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ipv6 address 1::1/64
[Switch-Vlan-interface2] undo ipv6 nd ra halt
[Switch-Vlan-interface2] ipv6 nd autoconfig managed-address-flag
[Switch-Vlan-interface2] ipv6 nd autoconfig other-flag
[Switch-Vlan-interface2] quit
```

# 配置前缀池 1，包含的前缀为 2001:0410::/32，分配的前缀长度为 48。

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

# 创建地址池 1。

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

# 配置地址池 1 网段为 1::/64，与 VLAN 接口 2 地址所属的网段相同。

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

# 配置地址池 1 引用已存在的前缀池 1，并设置动态分配前缀的首选生命期为 1 天，有效生命期为 3 天。

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

# 在地址池 1 中配置静态绑定前缀：绑定的前缀为 2001:0410:0201::/48，绑定的客户端 DUID 为 00030001CA0006A40000，并设置首选生命期为 1 天，有效生命期为 3 天。

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

# 配置为客户端分配的 DNS 服务器地址为 2:2::3。

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

# 配置为客户端分配的域名为 aaa.com。

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

# 配置为客户端分配的 SIP 服务器地址为 2:2::4，域名为 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
```

# 配置 VLAN 接口 2 工作在 DHCPv6 服务器模式，并在该接口使能期望前缀分配和前缀快速分配功能，并将优先级设置为最高。

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

#### 4. 验证配置

# 完成上述配置后，查看 VLAN 接口 2 上的 DHCPv6 服务器配置信息。

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

# 显示地址池 1 的信息。

```
[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
```

# 显示前缀池 1 的信息。

```
[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
```

# DUID 为 00030001CA0006A40000 的客户端获取 IPv6 前缀后，显示前缀绑定信息。

```
[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
```

# 其他客户端获取 IPv6 前缀后，显示前缀绑定信息。

```
[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
```

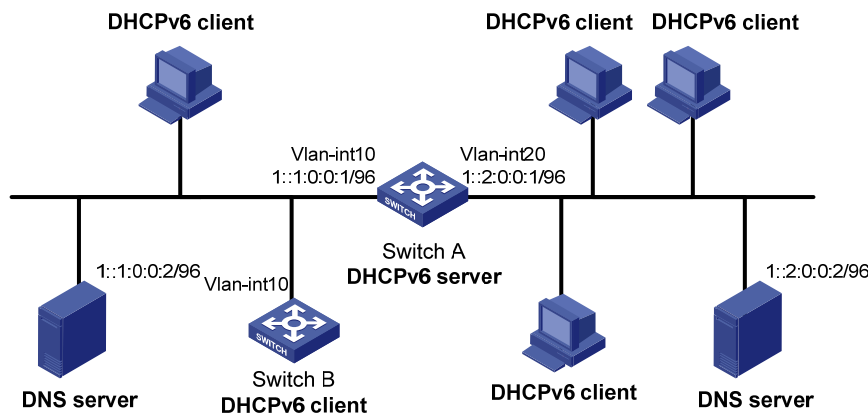
## 2.14.2 动态分配IPv6 地址配置举例

### 1. 组网需求

- 作为 DHCPv6 服务器的 Switch A 为网段 1::1:0:0/96 和 1::2:0:0/96 的客户端动态分配 IPv6 地址；
- Switch A 的两个 VLAN 接口 Vlan-interface10 和 Vlan-interface20 的地址分别为 1::1:0:0:1/96 和 1::2:0:0:1/96；
- 1::1:0:0/96 网段内的地址租约时长为 172800 秒（2 天），有效时长为 345600 秒（4 天），域名后缀为 aabbcc.com，DNS 服务器地址为 1::1:0:0:2/96；
- 1::2:0:0/96 网段内的地址租约时长为 432000 秒（5 天），有效时长为 864000 秒（10 天），域名后缀为 aabbcc.com，DNS 服务器地址为 1::2:0:0:2/96。

### 2. 组网图

图2-5 DHCPv6 组网图



### 3. 配置步骤

- (1) 配置 DHCPv6 server 各接口的 IPv6 地址。取消设备发布 RA 消息的抑制。配置被管理地址的配置标志位为 1，即主机通过 DHCPv6 服务器获取 IPv6 地址。配置其他信息配置标志位为 1，即主机通过 DHCPv6 服务器获取除 IPv6 地址以外的其他信息

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ipv6 address 1::1:0:0:1/96
[SwitchA-Vlan-interface10] undo ipv6 nd ra halt
[SwitchA-Vlan-interface10] ipv6 nd autoconfig managed-address-flag
```

```
[SwitchA-Vlan-interface10] ipv6 nd autoconfig other-flag
[SwitchA-Vlan-interface10] quit
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] ipv6 address 1::2:0:0:1/96
[SwitchA-Vlan-interface20] undo ipv6 nd ra halt
[SwitchA-Vlan-interface20] ipv6 nd autoconfig managed-address-flag
[SwitchA-Vlan-interface20] ipv6 nd autoconfig other-flag
[SwitchA-Vlan-interface20] quit
```

## (2) 配置 DHCPv6 服务

# 配置接口 Vlan-interface10 和 Vlan-interface20 工作在 DHCPv6 服务器模式。

```
[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
```

# 配置不参与自动分配的 IPv6 地址，以避免分配 DNS 服务器的地址。

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

# 配置 DHCPv6 地址池 1，为 1::1:0:0:0/96 网段的客户端分配 IPv6 地址等参数。

```
[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
```

# 配置 DHCPv6 地址池 2，为 1::2:0:0:0/96 网段的客户端分配 IPv6 地址等参数。

```
[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
```

## 4. 验证配置

配置完成后，1::1:0:0:0/96 和 1::2:0:0:0/96 网段的客户端可以从 DHCPv6 服务器 Switch A 申请到相应网段的 IPv6 地址和网络配置参数。通过 **display ipv6 dhcp server ip-in-use** 命令可以查看 DHCPv6 服务器为客户端分配的 IPv6 地址。

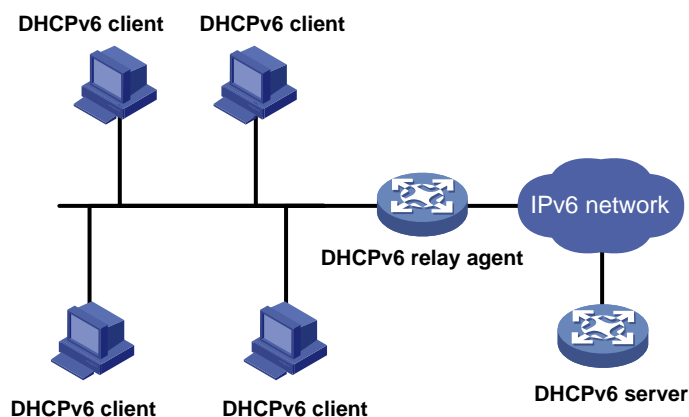
# 3 DHCPv6 中继

## 3.1 DHCPv6 中继简介

### 3.1.1 应用环境

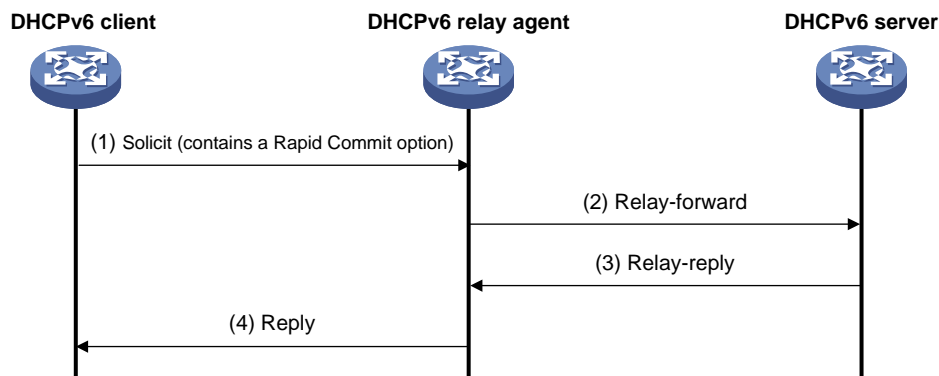
DHCPv6 客户端通常通过链路本地范围的组播地址与DHCPv6 服务器通信，以获取IPv6 地址和其他网络配置参数。如 图 3-1 所示，服务器和客户端不在同一个链路范围内时，服务器和客户端无法直接通信，需要通过DHCPv6 中继来转发报文。部署DHCPv6 中继可以避免在每个链路范围内都部署DHCPv6 服务器，既节省了成本，又便于进行集中管理。

图3-1 DHCPv6 中继应用组网图



### 3.1.2 DHCPv6 中继的工作过程

图3-2 DHCPv6 中继的工作过程



如 图 3-2 所示，以交互两个消息的快速分配过程为例，DHCPv6 客户端通过DHCPv6 中继，从DHCPv6 服务器获取IPv6 地址和其他网络配置参数的过程为：

- (1) DHCPv6 客户端向所有 DHCPv6 服务器和中继的组播地址 FF02::1:2 发送携带 Rapid Commit 选项的 Solicit 消息；

- (2) DHCPv6 中继接收到 Solicit 消息后，将其封装在 Relay-forward 报文的中继消息选项（Relay Message Option）中，并将 Relay-forward 报文发送给 DHCPv6 服务器；
- (3) DHCPv6 服务器从 Relay-forward 报文中解析出客户端的 Solicit 消息，为客户端选取 IPv6 地址和其他参数，构造 Reply 消息，将 Reply 消息封装在 Relay-reply 报文的中继消息选项中，并将 Relay-reply 报文发送给 DHCPv6 中继；
- (4) DHCPv6 中继从 Relay-reply 报文中解析出服务器的 Reply 消息，转发给 DHCPv6 客户端，以便 DHCPv6 客户端根据 DHCPv6 服务器分配的 IPv6 地址和其他参数进行网络配置。

## 3.2 DHCPv6中继配置任务简介

DHCPv6 中继配置任务如下：

- (1) [配置接口工作在DHCPv6 中继模式](#)
- (2) [指定DHCPv6 服务器的地址](#)
- (3) （可选）[配置DHCPv6 中继为DHCPv6 客户端分配的网关地址](#)
- (4) （可选）[配置DHCPv6 中继发送DHCPv6 报文的DSCP优先级](#)
- (5) （可选）[配置DHCPv6 中继支持的Interface ID选项填充模式](#)
- (6) （可选）[开启DHCPv6 中继发布前缀路由功能](#)
- (7) [（可选）配置DHCPv6 中继报文填充指定源地址](#)

## 3.3 配置接口工作在DHCPv6中继模式

### 1. 配置限制和指导

建议不要在一个接口上同时配置 DHCPv6 中继和 DHCPv6 客户端功能。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置接口工作在 DHCPv6 中继模式。

```
ipv6 dhcp select relay
```

缺省情况下，接口未工作在 DHCPv6 中继模式。

## 3.4 指定DHCPv6服务器的地址

### 3.4.1 指定DHCPv6 中继对应的DHCPv6 服务器地址

#### 1. 功能简介

工作在 DHCPv6 中继模式的接口接收到 DHCPv6 客户端发来的报文后，将其封装在 Relay-forward 报文中，并发送给指定的 DHCPv6 服务器，由 DHCPv6 服务器为客户端分配 IPv6 地址、IPv6 前缀和其他网络配置参数。



## 2. 配置限制和指导

- 通过多次执行 **ipv6 dhcp relay server-address** 命令可以指定多个 DHCPv6 服务器，一个接口下最多可以指定 8 个 DHCPv6 服务器。DHCPv6 中继接收到 DHCPv6 客户端报文后，将其转发给所有的 DHCPv6 服务器。
- 如果指定的 DHCPv6 服务器地址为链路本地地址或组播地址，则必须通过 **ipv6 dhcp relay server-address** 命令的 **interface** 参数指定出接口，否则报文可能会无法到达服务器。

## 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 指定 DHCPv6 中继对应的 DHCPv6 服务器地址。

```
ipv6 dhcp relay server-address ipv6-address [ interface interface-type  
interface-number ]
```

缺省情况下，未指定 DHCPv6 中继对应的 DHCPv6 服务器地址。

### 3.4.2 指定中继地址池上对应的DHCPv6 服务器地址

#### 1. 功能简介

对于某些特定的用户接入方式，基于用户接入位置信息的不同，网络中存在大量不同类型的用户。为了使相同类型的用户可以从指定的 DHCPv6 服务器申请 IPv6 地址等网络参数，IPoE 模块根据用户注册信息，使不同的用户选择不同的 DHCPv6 中继地址池，并从中继地址池下配置的 DHCPv6 服务器获取 IPv6 地址等网络参数。

一台 DHCPv6 中继的一个接口下可能连接不同类型的用户，当 DHCPv6 中继转发 DHCPv6 客户端请求报文给 DHCPv6 服务器时，不能再以中继接口的 IPv6 地址作为选择地址池的依据。为了解决这个问题，需要使用 **gateway-list** 命令指定某个类型用户所在的网段，并将该地址添加到转发给 DHCPv6 服务器的报文的 Link-address 字段中，为 DHCPv6 服务器选择地址池提供依据。

## 2. 配置限制和指导

- 为了提高可靠性，一个 DHCPv6 中继地址池下最多可以配置 8 个 DHCPv6 服务器地址，当 DHCPv6 客户端匹配该中继地址池后，DHCPv6 中继会将 DHCPv6 客户端发来的 DHCPv6 报文转发给该地址池对应所有的 DHCPv6 服务器。

## 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建 DHCPv6 中继地址池，并进入 DHCPv6 中继地址池视图。

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

- (3) 指定匹配该地址池的 DHCPv6 客户端所在的网段地址。

```
gateway-list ipv6-address&<1-8>
```

缺省情况下，未指定匹配该地址池的 DHCPv6 客户端所在的网段地址。

- (4) 指定中继地址池对应的 DHCPv6 服务器地址。

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

缺省情况下，未指定中继地址池对应的 DHCPv6 服务器的地址。

## 3.5 配置DHCPv6中继为DHCPv6客户端分配的网关地址

### 1. 功能简介

当未开启该功能时，DHCPv6 中继收到 DHCPv6 客户端的请求报文后，只能将接口的第一个 IPv6 添加到报文中，然后转发给 DHCPv6 服务器。对于某些特定需求，DHCPv6 中继需要添加指定的地址到报文中，这时就需要配置此功能。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置 DHCPv6 中继为 DHCPv6 客户端分配的网关地址。

```
ipv6 dhcp relay gateway ipv6-address
```

缺省情况下，DHCPv6 中继分配接口下的第一个 IPv6 地址作为 DHCPv6 客户端的网关地址。

## 3.6 配置DHCPv6中继发送DHCPv6报文的DSCP优先级

### 1. 功能简介

DSCP 优先级用来体现报文自身的优先等级，决定报文传输的优先程度。通过本配置可以指定 DHCPv6 中继发送的 DHCPv6 报文的 DSCP 优先级。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 DHCPv6 中继发送 DHCPv6 报文的 DSCP 优先级。

```
ipv6 dhcp dscp dscp-value
```

缺省情况下，DHCPv6 中继发送的 DHCPv6 报文的 DSCP 优先级为 56。

## 3.7 配置DHCPv6中继支持的Interface ID选项填充模式

### 1. 功能简介

如果配置了 DHCPv6 中继支持的 Interface ID 选项填充模式，当 DHCPv6 中继接收到客户端发送的 DHCPv6 报文后，会以配置的填充方式将 DHCPv6 客户端的位置信息填充 Option 18 选项，并把填充好的报文转发给 DHCPv6 服务器。

## 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置 DHCPv6 中继支持的 Interface ID 选项填充模式。

```
ipv6 dhcp relay interface-id { bas | interface }
```

缺省情况下，Interface ID 选项的填充模式为接口索引信息。

## 3.8 开启DHCPv6中继发布前缀路由功能

### 1. 功能简介

DHCPv6 客户端获取到 IPv6 前缀后，通过该 IPv6 前缀为下行网络内的主机分配 IPv6 地址。此时，DHCPv6 客户端与网络内的主机不在同一网段内，会导致主机无法与外界通信。为了解决这个问题，需要在和 DHCPv6 客户端处于同一个链路范围内的 DHCPv6 中继上开启发布前缀路由功能。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 DHCPv6 中继发布前缀路由功能。

```
ipv6 dhcp advertise pd-route
```

缺省情况下，DHCPv6 中继发布前缀路由功能处于关闭状态。

开启 DHCPv6 中继发布前缀路由功能前，需要先开启 DHCPv6 中继用户表项记录功能。

## 3.9 配置DHCPv6中继报文填充指定源地址

### 1. 功能简介

在某些组网中，DHCPv6 中继接口到 DHCPv6 服务器没有可达路由，用户需要配置本命令选择 DHCPv6 中继设备上的另一个接口（一般选择的是 Loopback 口）的 IPv6 地址填充到转发给 DHCPv6 服务器的 DHCPv6 请求报文中的源地址字段。

DHCPv6 中继上行报文源地址填充为用户指定的全球单播地址或指定接口的地址。

未配置该功能时，DHCPv6 中继上行报文源地址默认填充为出接口的地址。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置指定源地址。

```
ipv6 dhcp relay source-address { ipv6-address | interface interface-type  
interface-number }
```

缺省情况下，DHCPv6 中继自动选择向 DHCPv6 服务器转发报文出接口的一个全球单播地址作为 DHCPv6 中继向 DHCPv6 服务器转发报文的源地址。

如果指定接口作为源地址，但该接口未配置全球单播地址，则选择默认出接口地址。

## 3.10 DHCPv6中继显示和维护

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 中继的运行情况，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 中继的统计信息。

表3-1 DHCPv6 中继显示和维护

操作	命令
显示本设备DUID	<b>display ipv6 dhcp duuid</b>
显示DHCPv6中继上指定的DHCPv6服务器地址信息	<b>display ipv6 dhcp relay server-address</b> [ <b>interface</b> <i>interface-type</i> <i>interface-number</i> ]
显示DHCPv6中继的相关报文统计信息	<b>display ipv6 dhcp relay statistics</b> [ <b>interface</b> <i>interface-type</i> <i>interface-number</i> ]
清除DHCPv6中继用户地址表项信息	<b>reset ipv6 dhcp relay client-information address</b> [ <b>interface</b> <i>interface-type</i> <i>interface-number</i>   <b>ipv6</b> <i>ipv6-address</i> ]
清除DHCPv6中继用户前缀表项信息	<b>reset ipv6 dhcp relay client-information pd</b> [ <b>interface</b> <i>interface-type</i> <i>interface-number</i>   <b>prefix</b> <i>prefix/prefix-len</i> ]
清除DHCPv6中继的相关报文统计信息	<b>reset ipv6 dhcp relay statistics</b> [ <b>interface</b> <i>interface-type</i> <i>interface-number</i> ]

## 3.11 DHCPv6中继典型配置举例

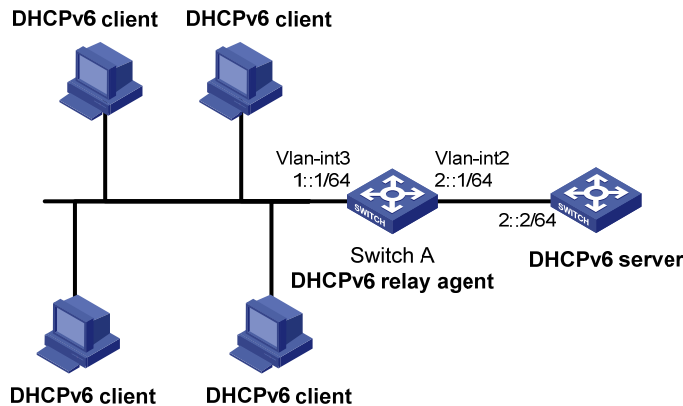
### 3.11.1 DHCPv6 中继基本组网典型配置举例

#### 1. 组网需求

- DHCPv6 客户端所在网络地址为 1::/64，DHCPv6 服务器的地址为 2::2/64。客户端和服务端不在同一个链路范围，需要通过 DHCPv6 中继转发报文。
- Switch A 作为 DHCPv6 中继，为客户端和服务端转发报文。
- Switch A 同时作为 1::/64 网络的网关设备，通过 RA 消息中的 M 标志位和 O 标志位指定该网络中的主机通过 DHCPv6 获取 IPv6 地址和其他网络配置参数。RA 消息的详细介绍，请参见“三层技术-IP 业务配置指导”中的“IPv6 基础”。

## 2. 组网图

图3-3 DHCPv6 中继组网图



## 3. 配置步骤

# 配置 VLAN 接口 2 和 VLAN 接口 3 的 IPv6 地址。取消设备发布 RA 消息的抑制。配置被管理地址的配置标志位为 1，即主机通过 DHCPv6 服务器获取 IPv6 地址。配置其他信息配置标志位为 1，即主机通过 DHCPv6 服务器获取除 IPv6 地址以外的其他信息

```
<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
[SwitchA-Vlan-interface3] undo ipv6 nd ra halt
[SwitchA-Vlan-interface3] ipv6 nd autoconfig managed-address-flag
[SwitchA-Vlan-interface3] ipv6 nd autoconfig other-flag
```

# 配置 VLAN 接口 3 工作在 DHCPv6 中继模式，并指定 DHCPv6 服务器地址。

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

## 4. 验证配置

# 完成上述配置后，查看 DHCPv6 中继上指定的 DHCPv6 服务器地址信息。

```
[SwitchA-Vlan-interface3] display ipv6 dhcp relay server-address
Interface: Vlan-interface3

Server address      Outgoing Interface      Public/VRF name
2::2                --/--
```

# 查看 DHCPv6 中继相关报文的统计信息。

```
[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

# 4 DHCPv6 客户端

## 4.1 DHCPv6客户端简介

设备作为 DHCPv6 客户端时，可以具有如下功能：

- 通过 DHCPv6 获取 IPv6 地址和网络配置参数，IPv6 地址作为开启 DHCPv6 客户端功能的接口地址，当设备开启 DHCPv6 服务器功能后，获取的网络配置参数用来自动创建 DHCPv6 选项组。
- 通过 DHCPv6 获取 IPv6 前缀和网络配置参数，IPv6 前缀作为本地设备的 IPv6 前缀（本地设备根据该前缀生成 IPv6 地址）；当设备开启 DHCPv6 服务器功能后，获取的网络配置参数用来自动创建 DHCPv6 选项组。
- 通过 DHCPv6 同时获取 IPv6 地址、IPv6 前缀和网络配置参数，IPv6 地址作为开启 DHCPv6 客户端功能的接口地址，IPv6 前缀作为本地设备的 IPv6 前缀（本地设备根据该前缀生成 IPv6 地址）；当设备开启 DHCPv6 服务器功能后，获取的网络配置参数用来自动创建 DHCPv6 选项组。
- 通过 DHCPv6 无状态配置获取除 IPv6 地址/前缀外的其他网络配置参数。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 标志位的取值为 0、O 标志位的取值为 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。否则 DHCPv6 客户端不会开启无状态配置过程。

## 4.2 DHCPv6客户端配置限制和指导

建议不要在一个接口上同时配置 DHCPv6 客户端和 DHCPv6 服务器功能，也不要在一个接口上同时配置 DHCPv6 客户端和 DHCPv6 中继功能，否则会影响功能正常使用。

## 4.3 DHCPv6客户端配置任务简介

DHCPv6 客户端配置任务如下：

- (1) （可选）[配置接口使用的DHCPv6 客户端DUID](#)
- (2) 配置 DHCPv6 客户端获取 IPv6 地址、IPv6 前缀和网络配置参数  
请至少选择以下一项任务进行配置：
  - [配置DHCPv6 客户端获取IPv6 地址和网络配置参数](#)
  - [配置DHCPv6 客户端获取IPv6 前缀和网络配置参数](#)
  - [配置DHCPv6 客户端同时获取IPv6 地址、IPv6 前缀和网络配置参数](#)
  - [配置DHCPv6 客户端获取除地址/前缀外的其他网络配置参数](#)
- (3) （可选）[配置DHCPv6 客户端发送DHCPv6 报文的DSCP优先级](#)

## 4.4 配置接口使用的DHCPv6客户端DUID

### 1. 功能简介

DHCPv6 客户端 DUID 用来填充 DHCPv6 报文的 Option 1, 作为识别 DHCPv6 客户端的唯一标识。DHCPv6 服务器可以根据 DHCPv6 客户端 DUID 为特定的 DHCPv6 客户端分配特定的 IPv6 地址。用户可以通过三种方法指定 DHCPv6 客户端 DUID: ASCII 字符串、十六进制数或接口的 MAC 地址。

### 2. 配置限制和指导

用户在指定客户端 ID 时, 需要确保不同客户端的客户端 ID 不能相同。

### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置接口使用的 DHCPv6 客户端 DUID。

```
ipv6 dhcp client duid { ascii ascii-string | hex hex-string | mac  
interface-type interface-number }
```

缺省情况下, 根据设备的桥 MAC 地址生成 DHCPv6 客户端 DUID。

## 4.5 配置DHCPv6客户端获取IPv6地址和网络配置参数

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置接口作为 DHCPv6 客户端, 通过 DHCPv6 方式获取 IPv6 地址和其他网络配置参数。

```
ipv6 address dhcp-alloc [ option-group group-number | rapid-commit ] *
```

缺省情况下, 接口不会作为 DHCPv6 客户端获取 IPv6 地址和网络配置参数。

## 4.6 配置DHCPv6客户端获取IPv6前缀和网络配置参数

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置接口作为 DHCPv6 客户端, 通过 DHCPv6 方式获取 IPv6 前缀和其他网络配置参数。

```
ipv6 dhcp client pd prefix-number [ option-group group-number |  
rapid-commit ] *
```

缺省情况下, 接口不会作为 DHCPv6 客户端获取 IPv6 前缀和网络配置参数。



## 4.7 配置DHCPv6客户端同时获取IPv6地址、IPv6前缀和网络配置参数

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 配置接口作为 DHCPv6 客户端，通过 DHCPv6 方式同时获取 IPv6 地址、IPv6 前缀和其他网络配置参数。

```
ipv6 dhcp client stateful prefix prefix-number [ option-group  
option-group-number | rapid-commit ] *
```

缺省情况下，接口不会作为 DHCPv6 客户端同时获取 IPv6 地址、IPv6 前缀和网络配置参数。

## 4.8 配置DHCPv6客户端获取除地址/前缀外的其他网络配置参数

### 1. 功能简介

DHCPv6 客户端可通过如下方式获取除地址/前缀外的其他网络参数：

- 如果接口上只配置了 **ipv6 address auto** 命令，则接口会通过无状态自动配置方式生成全球单播地址，同时自动生成链路本地地址。只有接收到的 RA 报文中 M 标志位的取值为 0、O 标志位的取值为 1 时，设备才会自动启动 DHCPv6 无状态配置功能。
- 如果接口只配置了 **ipv6 dhcp client stateless enable** 命令，则接口开启了 DHCPv6 客户端功能，并从 DHCPv6 服务器获取除地址/前缀外的其他网络配置参数。
- 如果接口上同时配置了 **ipv6 address auto** 命令和 **ipv6 dhcp client stateless enable** 命令，则接口通过无状态生成全球单播地址，同时自动生成链路本地地址，且直接从 DHCPv6 服务器获取除地址/前缀外的其他网络配置参数。

**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. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 开启无状态自动配置功能。请至少选择其中一项进行配置。

- 开启 IPv6 地址无状态自动配置功能。

```
ipv6 address auto
```

- 开启 DHCPv6 客户端无状态配置功能。

```
ipv6 dhcp client stateless enable
```

缺省情况下，接口不会作为 DHCPv6 客户端获取除地址/前缀外的其他网络配置参数。

## 4.9 配置DHCPv6客户端发送DHCPv6报文的DSCP优先级

### 1. 功能简介

DSCP 优先级用来体现报文自身的优先等级，决定报文传输的优先程度。通过本配置可以指定 DHCPv6 客户端发送的 DHCPv6 报文的 DSCP 优先级。

### 2. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 配置 DHCPv6 客户端发送的 DHCPv6 报文的 DSCP 优先级。

```
ipv6 dhcp client dscp dscp-value
```

缺省情况下，DHCPv6 客户端发送的 DHCPv6 报文的 DSCP 优先级为 56。

## 4.10 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4-1 DHCPv6 客户端显示和维护

操作	命令
显示DHCPv6客户端的信息	<b>display ipv6 dhcp client</b> [ <b>interface</b> <i>interface-type interface-number</i> ]
显示DHCPv6客户端的统计信息	<b>display ipv6 dhcp client statistics</b> [ <b>interface</b> <i>interface-type interface-number</i> ]
清除DHCPv6客户端的统计信息	<b>reset ipv6 dhcp client statistics</b> [ <b>interface</b> <i>interface-type interface-number</i> ]

## 4.11 DHCPv6客户端典型配置举例

### 4.11.1 DHCPv6 客户端申请地址及网络参数配置举例

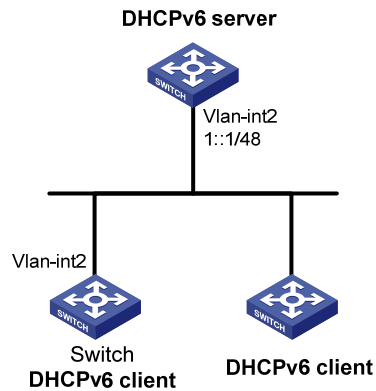
#### 1. 组网需求

DHCPv6 客户端 Switch 从 DHCPv6 服务器获取 IPv6 地址，以及网络配置参数：DNS 服务器地址、域名后缀、SIP 服务器地址和 SIP 服务器域名。

DHCPv6 客户端根据获取到的网络配置参数自动创建 DHCPv6 选项组 1。

## 2. 组网图

图4-1 DHCPv6 客户端申请地址及网络参数配置组网图



## 3. 配置步骤



说明

进行下面的配置前，需要先完成 DHCPv6 服务器的配置。

# 配置 VLAN 接口 2 作为 DHCPv6 客户端获取 IPv6 地址及网络参数，配置 DHCPv6 客户端支持地址快速分配功能，并配置根据获取到的网络配置参数自动创建 DHCPv6 选项组 1。

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

## 4. 验证配置

# 显示 DHCPv6 客户端的信息。可以看出 DHCPv6 客户端已经成功从 DHCPv6 服务器获取 IPv6 地址及网络参数。

```
[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
# 在 DHCPv6 客户端上开启 DHCPv6 服务器功能后，显示动态创建的 DHCPv6 选项组 1 的信息。
[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
# 查看获取到的 IPv6 地址。
[Switch] display ipv6 interface brief
*down: administratively down
(s): spoofing
Interface                                Physical    Protocol    IPv6 Address
Vlan-interface2                          up          up          1:1::2

```

## 4.11.2 DHCPv6 客户端申请前缀及网络参数配置举例

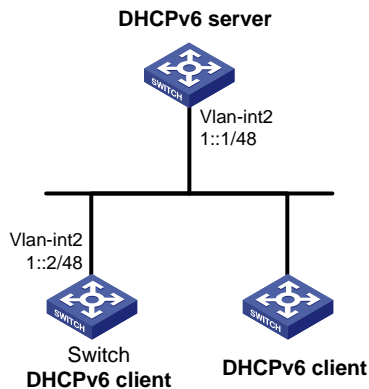
### 1. 组网需求

DHCPv6 客户端 Switch 从 DHCPv6 服务器获取 IPv6 前缀，以及网络配置参数：DNS 服务器地址、域名后缀、SIP 服务器地址和 SIP 服务器域名等。

DHCPv6 客户端 Switch 根据获取到的前缀自动创建 IPv6 前缀 1，根据获取到的网络配置参数自动创建 DHCPv6 选项组 1。

## 2. 组网图

图4-2 DHCPv6 客户端申请前缀及网络参数配置组网图



## 3. 配置步骤



说明

进行下面的配置前，需要先完成 DHCPv6 服务器的配置。

# 在客户端连接到 DHCPv6 服务器的 VLAN 接口 2 上配置 IPv6 地址。

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

# 配置 VLAN 接口 2 作为 DHCPv6 客户端获取 IPv6 前缀及网络参数，配置根据获取到的前缀自动创建 IPv6 前缀 1，根据获取到的网络配置参数自动创建 DHCPv6 选项组 1，并配置 DHCPv6 客户端支持前缀快速分配功能。

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

## 4. 验证配置

# 显示 DHCPv6 客户端的信息。可以看出 DHCPv6 客户端已经成功从 DHCPv6 服务器获取 IPv6 前缀及网络参数。

```
[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
```

# 显示动态创建的 IPv6 前缀 1 的信息。

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

# 在 DHCPv6 客户端上开启 DHCPv6 服务器功能后，显示动态创建的 DHCPv6 选项组 1 的信息。

```
[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
```

### 4.11.3 DHCPv6 客户端同时申请地址、前缀及网络参数配置举例

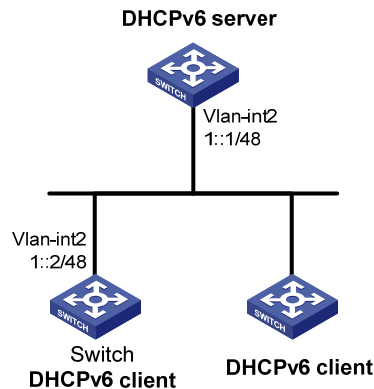
#### 1. 组网需求

DHCPv6 客户端 Switch 从 DHCPv6 服务器同时获取 IPv6 地址、IPv6 前缀，以及网络配置参数：DNS 服务器地址、域名后缀、SIP 服务器地址和 SIP 服务器域名等。

DHCPv6 客户端 Switch 根据获取到的前缀自动创建 IPv6 前缀 1，根据获取到的网络配置参数自动创建 DHCPv6 选项组 1。

## 2. 组网图

图4-3 DHCPv6 客户端同时申请地址、前缀及网络参数配置组网图



## 3. 配置步骤



说明

进行下面的配置前，需要先完成 DHCPv6 服务器的配置。

# 在客户端连接到 DHCPv6 服务器的 VLAN 接口 2 上配置 IPv6 地址。

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

# 配置 VLAN 接口 2 作为 DHCPv6 客户端获取 IPv6 前缀及网络参数，配置根据获取到的前缀自动创建 IPv6 前缀 1，根据获取到的网络配置参数自动创建 DHCPv6 选项组 1，并配置 DHCPv6 客户端支持前缀快速分配功能。

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

## 4. 验证配置

# 显示 DHCPv6 客户端的信息。可以看出 DHCPv6 客户端已经成功从 DHCPv6 服务器获取 IPv6 前缀及网络参数。

```
[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

```

# 查看获取到的 IPv6 地址。

```

[Switch] display ipv6 interface brief
*down: administratively down
(s): spoofing

```

Interface	Physical	Protocol	IPv6 Address
Vlan-interface2	up	up	1:1::2

# 显示动态创建的 IPv6 前缀 1 的信息。

```

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

```

# 在 DHCPv6 客户端上开启 DHCPv6 服务器功能后，显示动态创建的 DHCPv6 选项组 1 的信息。

```

[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

```

以上三条 **display** 命令可以看到客户端获取到的地址信息、前缀信息和网络参数。



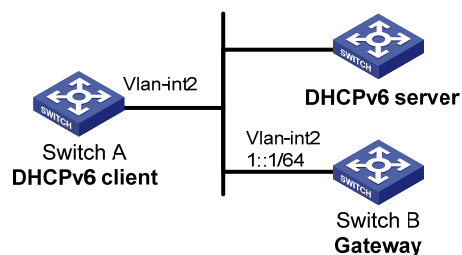
#### 4.11.4 DHCPv6 无状态配置配置举例

##### 1. 组网需求

- DHCPv6 客户端 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4-4 DHCPv6 无状态配置组网图



##### 3. 配置步骤



##### 说明

进行下面的配置前，需要先完成 DHCPv6 服务器的配置。

##### (1) 配置网关 Switch B

# 配置 VLAN 接口 2 的 IPv6 地址。

```
<SwitchB> system-view
[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

# 在 VLAN 接口 2 上使能 IPv6 地址无状态自动配置功能。

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

执行此命令后，如果 VLAN 接口 2 下未配置地址，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

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:

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

# 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

Renew : 0

Rebind : 0

Information-request : 5

Release : 0

Decline : 0

# 5 DHCPv6 Snooping

## 5.1 DHCPv6 Snooping简介

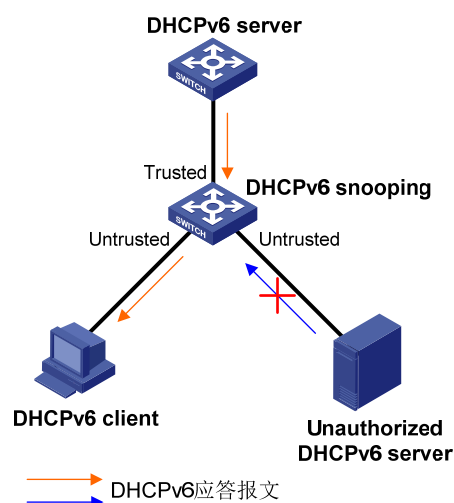
DHCPv6 Snooping 是 DHCPv6 的一种安全特性，用来保证客户端从合法的服务器获取 IPv6 地址或 IPv6 前缀，并可以记录 DHCPv6 客户端 IPv6 地址或 IPv6 前缀与 MAC 地址的对应关系。

### 5.1.1 保证客户端从合法的服务器获取IPv6 地址或IPv6 前缀

网络中如果存在私自架设的非法 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，从而无法正常通信。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和不信任端口：

- 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5-1 信任端口和非信任端口



如 图 5-1 所示，在 DHCPv6 Snooping 设备上指向 DHCPv6 服务器方向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，私自架设的非法 DHCPv6 服务器无法为 DHCPv6 客户端分配地址。

### 5.1.2 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 binding** 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。

### 5.1.3 记录DHCPv6 客户端IPv6 前缀与端口的对应关系

DHCPv6 Snooping 通过监听 DHCPv6 报文中的前缀和收到 DHCPv6 请求报文的端口信息，记录 DHCPv6 Snooping 前缀表项，其中包括客户端获取到的 IPv6 前缀、租约信息、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 pd binding** 命令查看客户端获取的 IPv6 前缀信息，以便了解用户上网时所用的 IPv6 前缀，并对其进行管理和监控。

## 5.2 DHCPv6 snooping配置限制和指导

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。

## 5.3 DHCPv6 Snooping配置任务简介

DHCPv6 Snooping 配置任务如下：

- (1) [配置DHCPv6 Snooping基本功能](#)
- (2) （可选）[配置DHCPv6 Snooping支持Option 18 功能](#)
- (3) （可选）[配置DHCPv6 Snooping支持Option 37 功能](#)
- (4) （可选）[配置DHCPv6 Snooping表项固化功能](#)
- (5) （可选）[配置接口动态学习DHCPv6 Snooping表项的最大数目](#)
- (6) （可选）[开启DHCPv6 Snooping报文限速功能](#)
- (7) （可选）[开启DHCPv6 Snooping的DHCPv6 请求方向报文检查功能](#)
- (8) （可选）[开启DHCPv6 Snooping报文阻断功能](#)
- (9) （可选）[开启DHCPv6 Snooping日志信息功能](#)

## 5.4 配置DHCPv6 Snooping基本功能

### 5.4.1 在普通组网中配置DHCPv6 Snooping基本功能

#### 1. 配置限制和指导

- 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。
- 如果二层以太网接口加入了聚合组，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。

#### 2. 开启DHCPv6 Snooping功能

- (1) 进入系统视图。  
**system-view**
- (2) 开启 DHCPv6 Snooping 功能。

**ipv6 dhcp snooping enable**

缺省情况下，DHCPv6 Snooping 功能处于关闭状态。

### 3. 配置DHCPv6 Snooping信任端口

- (1) 进入系统视图。

**system-view**

- (2) 进入接口视图。

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

此接口为连接 DHCPv6 服务器的接口。

- (3) 配置 DHCPv6 Snooping 信任端口。

**ipv6 dhcp snooping trust**

缺省情况下，开启 DHCPv6 Snooping 功能后，设备的所有端口均为不信任端口。

### 4. 开启端口的DHCPv6 Snooping表项记录功能

- (1) 进入系统视图。

**system-view**

- (2) 进入接口视图。

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

此接口为连接 DHCPv6 客户端的接口。

- (3) 开启端口的 DHCPv6 Snooping 表项记录功能。请至少选择其中一项进行配置。

- 开启端口的 DHCPv6 Snooping 地址表项记录功能。

**ipv6 dhcp snooping binding record**

缺省情况下，端口的 DHCPv6 Snooping 地址表项记录功能处于关闭状态。

- 开启端口的 DHCPv6 Snooping 前缀表项记录功能。

**ipv6 dhcp snooping pd binding record**

缺省情况下，端口的 DHCPv6 Snooping 前缀表项记录功能处于关闭状态。

## 5.5 配置DHCPv6 Snooping支持Option 18功能

- (1) 进入系统视图。

**system-view**

- (2) 进入接口视图。

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

- (3) 开启 DHCPv6 Snooping 支持 Option 18 功能。

**ipv6 dhcp snooping option interface-id enable**

缺省情况下，DHCPv6 Snooping 支持 Option 18 功能处于关闭状态。

- (4) （可选）配置 Option 18 选项中的 DUID。

**ipv6 dhcp snooping option interface-id** [ **vlan** *vlan-id* ] **string** *interface-id*

缺省情况下，Option 18 选项中的 DUID 为本设备的 DUID。

## 5.6 配置DHCPv6 Snooping支持Option 37功能

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 开启 DHCPv6 Snooping 支持 Option 37 功能。

```
ipv6 dhcp snooping option remote-id enable
```

缺省情况下，DHCPv6 Snooping 支持 Option 37 功能处于关闭状态。

- (4) （可选）配置 Option 37 选项中的 DUID。

```
ipv6 dhcp snooping option remote-id [ vlan vlan-id ] string remote-id
```

缺省情况下，Option 37 选项中的 DUID 为本设备的 DUID。

## 5.7 配置DHCPv6 Snooping表项固化功能

### 1. 功能简介

DHCPv6 Snooping 设备重启后，设备上记录的 DHCPv6 Snooping 表项将丢失。如果 DHCPv6 Snooping 与其他特性（如 IP Source Guard）配合使用，表项丢失会导致安全特性无法通过 DHCPv6 Snooping 获取到相应的表项，进而导致 DHCPv6 客户端不能顺利通过安全检查、正常访问网络。

DHCPv6 Snooping 表项备份功能将 DHCPv6 Snooping 表项保存到指定的文件中，DHCPv6 Snooping 设备重启后，自动根据该文件恢复 DHCPv6 Snooping 表项，从而保证 DHCPv6 Snooping 表项不会丢失。

### 2. 配置限制和指导

- 执行 **undo ipv6 dhcp snooping enable** 命令关闭 DHCPv6 Snooping 功能后，设备会删除所有 DHCPv6 Snooping 表项，文件中存储的 DHCPv6 Snooping 表项也将被删除。
- 执行 **ipv6 dhcp snooping binding database filename** 命令后，会立即触发一次表项备份。
  - 如果未配置 **ipv6 dhcp snooping binding database update interval** 命令，若表项发生变化，默认在 300 秒之后刷新存储文件；若表项未发生变化，则不再刷新存储文件。
  - 如果配置了 **ipv6 dhcp snooping binding database update interval** 命令，若表项发生变化，则到达刷新时间间隔后刷新存储文件；若表项未发生变化，则不再刷新存储文件。

### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 指定存储 DHCPv6 Snooping 表项的文件名称。

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

缺省情况下，未指定存储文件名称。

- (3) (可选) 将当前的 DHCPv6 Snooping 表项保存到用户指定的文件中。

**ipv6 dhcp snooping binding database update now**

本命令只用来触发一次 DHCPv6 Snooping 表项的备份。

- (4) (可选) 配置刷新 DHCPv6 Snooping 表项存储文件的延迟时间。

**ipv6 dhcp snooping binding database update interval interval**

缺省情况下, 若 DHCPv6 Snooping 表项不变化, 则不刷新存储文件; 若 DHCPv6 Snooping 表项发生变化, 默认在 300 秒之后刷新存储文件。

## 5.8 配置接口动态学习DHCPv6 Snooping表项的最大数目

### 1. 功能简介

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, 占用过多的系统资源。

### 2. 配置步骤

- (1) 进入系统视图。

**system-view**

- (2) 进入接口视图。

**interface interface-type interface-number**

- (3) 配置接口动态学习 DHCPv6 Snooping 表项的最大数目。

**ipv6 dhcp snooping max-learning-num max-number**

缺省情况下, 不限制接口动态学习 DHCPv6 Snooping 表项的数目。

## 5.9 开启DHCPv6 Snooping报文限速功能

### 1. 功能简介

为了避免非法用户发送大量的 DHCPv6 报文, 对网络造成攻击, DHCPv6 Snooping 支持报文限速功能, 限制接口接收 DHCPv6 报文的速率。当接口接收的 DHCPv6 报文速率超过限制的最高速率时, DHCPv6 Snooping 设备将丢弃超过速率限制的报文。

### 2. 配置限制和指导

如果二层以太网接口加入了聚合组, 则该接口采用对应二层聚合接口下的 DHCPv6 Snooping 的报文限速配置。如果二层以太网接口离开聚合组, 则该接口采用二层以太网接口下的 DHCPv6 Snooping 的报文限速配置。

### 3. 配置步骤

- (1) 进入系统视图。

**system-view**

- (2) 进入接口视图。

**interface interface-type interface-number**

- (3) 开启 DHCPv6 Snooping 的报文限速功能。

**ipv6 dhcp snooping rate-limit rate**

缺省情况下，DHCPv6 Snooping 的报文限速功能处于关闭状态，即不限制接口接收 DHCPv6 报文的速率。

## 5.10 开启DHCPv6 Snooping的DHCPv6请求方向报文检查功能

### 1. 功能简介

本功能用来检查 DHCPv6-Renew、DHCPv6-Dcline 和 DHCPv6-Release 三种 DHCPv6 请求方向的报文，以防止非法客户端伪造这三种报文对 DHCPv6 服务器进行攻击。

伪造 DHCPv6-Renew 报文攻击是指攻击者冒充合法的 DHCPv6 客户端，向 DHCPv6 服务器发送伪造的 DHCPv6-Renew 报文，导致 DHCPv6 服务器和 DHCPv6 客户端无法按照自己的意愿及时释放 IPv6 地址租约。如果攻击者冒充不同的 DHCPv6 客户端发送大量伪造的 DHCPv6-Renew 报文，则会导致大量 IPv6 地址被长时间占用，DHCPv6 服务器没有足够的地址分配给新的 DHCPv6 客户端。

伪造 DHCPv6-Dcline/DHCPv6-Release 报文攻击是指攻击者冒充合法的 DHCPv6 客户端，向 DHCPv6 服务器发送伪造的 DHCPv6-Dcline/DHCPv6-Release 报文，导致 DHCPv6 服务器错误终止 IPv6 地址租约。

在 DHCPv6 Snooping 设备上开启 DHCPv6 请求方向报文检查功能，可以有效地防止伪造 DHCPv6 请求方向报文攻击。如果开启了该功能，则 DHCPv6 Snooping 设备接收到上述报文后，检查本地是否存在与请求方向报文匹配的 DHCPv6 Snooping 表项。若存在，则接收报文信息与 DHCPv6 Snooping 表项信息一致时，认为该报文为合法的 DHCPv6 请求方向报文，将其转发给 DHCPv6 服务器；不一致时，认为该报文为伪造的 DHCPv6 请求方向报文，将其丢弃。若不存在，则认为该报文合法，将其转发给 DHCPv6 服务器。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入接口视图。

```
interface interface-type interface-number
```

- (3) 开启 DHCPv6 Snooping 的 DHCPv6 请求方向报文检查功能。

```
ipv6 dhcp snooping check request-message
```

缺省情况下，DHCPv6 Snooping 的 DHCPv6 请求方向报文检查功能处于关闭状态。

## 5.11 开启DHCPv6 Snooping报文阻断功能

### 1. 功能简介

在某些组网环境下，用户需要在 DHCPv6 Snooping 设备的某一端口上丢弃该端口收到的所有 DHCPv6 请求方向报文，而又不影响其他端口正常接收 DHCPv6 报文。这时，用户可以在该端口上开启 DHCP Snooping 报文阻断功能。

当端口上开启了 DHCPv6 Snooping 报文阻断功能后，该端口收到的所有 DHCPv6 请求方向的报文都将被丢弃。



2. 配置步骤

- (1) 进入系统视图。  
`system-view`
- (2) 进入接口视图。  
`interface interface-type interface-number`
- (3) 开启 DHCPv6 Snooping 报文阻断功能。  
`ipv6 dhcp snooping deny`  
缺省情况下，端口的 DHCPv6 Snooping 报文阻断功能处于关闭状态。

5.12 开启DHCPv6 Snooping日志信息功能

1. 功能简介

DHCPv6 Snooping 日志可以方便管理员定位问题和解决问题。DHCPv6 Snooping 设备生成 DHCPv6 Snooping 日志信息会交给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

2. 配置限制和指导

当 DHCPv6 Snooping 设备输出大量日志信息时，可能会降低设备性能。为了避免该情况的发生，用户可以关闭 DHCPv6 Snooping 日志信息功能，使得 DHCPv6 Snooping 设备不再输出日志信息。

3. 配置步骤

- (1) 进入系统视图。  
`system-view`
- (2) 开启 DHCPv6 Snooping 日志信息功能。  
`ipv6 dhcp snooping log enable`  
缺省情况下，DHCPv6 Snooping 日志信息功能处于关闭状态。

5.13 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5-1 DHCPv6 Snooping 显示和维护

操作	命令
显示DHCPv6 Snooping地址表项信息	<code>display ipv6 dhcp snooping binding [ address ipv6-address [ vlan vlan-id ] ]</code>
显示DHCPv6 Snooping表项备份信息	<code>display ipv6 dhcp snooping binding database</code>
显示DHCPv6 Snooping设备上的DHCPv6报文统计信息	<code>display ipv6 dhcp snooping packet statistics [ slot slot-number ]</code>

操作	命令
显示DHCPv6 Snooping前缀表项信息	<b>display ipv6 dhcp snooping pd binding</b> [ <b>prefix</b> <i>prefix/prefix-length</i> [ <b>vlan</b> <i>vlan-id</i> ] ]
显示DHCPv6 Snooping信任端口信息	<b>display ipv6 dhcp snooping trust</b>
清除DHCPv6 Snooping地址表项信息	<b>reset ipv6 dhcp snooping binding</b> { <b>all</b>   <b>address</b> <i>ipv6-address</i> [ <b>vlan</b> <i>vlan-id</i> ] }
清除DHCPv6 Snooping设备上的DHCPv6报文统计信息	<b>reset ipv6 dhcp snooping packet statistics</b> [ <b>slot</b> <i>slot-number</i> ]
清除DHCPv6 Snooping前缀表项信息	<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> ] }

## 5.14 DHCPv6 Snooping典型配置举例

### 5.14.1 DHCPv6 Snooping基本组网配置举例

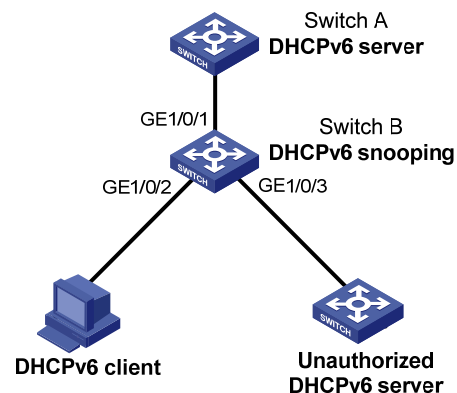
#### 1. 组网需求

Switch B 通过以太网端口 GigabitEthernet1/0/1 连接到合法 DHCPv6 服务器，通过以太网端口 GigabitEthernet1/0/3连接到非法服务器，通过 GigabitEthernet1/0/2 连接到 DHCPv6 客户端。要求：

- 与合法 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5-2 DHCPv6 Snooping 组网示意图



#### 3. 配置步骤

# 开启 DHCPv6 Snooping 功能。

```
<SwitchB> system-view
```

```
[SwitchB] ipv6 dhcp snooping enable
```

# 配置 GigabitEthernet1/0/1 端口为信任端口。

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

# 在 GigabitEthernet1/0/2 上开启安全表项功能。

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

#### 4. 验证配置

配置完成后，DHCPv6 客户端只能够从合法 DHCPv6 服务器获取 IPv6 地址和其他配置信息，非法 DHCPv6 服务器无法为 DHCPv6 客户端分配 IPv6 地址和其他配置信息。且使用 **display ipv6 dhcp snooping binding** 命令可以查看生成的 DHCPv6 Snooping 表项。

# 目 录

1 IPv6 快速转发 .....	1-1
1.1 IPv6 快速转发简介 .....	1-1
1.2 配置IPv6 快速转发表项的老化时间 .....	1-1
1.3 配置IPv6 快速转发负载分担 .....	1-1
1.4 IPv6 快速转发显示和维护 .....	1-2

# 1 IPv6 快速转发

## 1.1 IPv6快速转发简介

报文转发效率是衡量设备性能的一项关键指标。按照常规流程，设备收到一个报文后，根据报文的目地址寻找路由表中与之匹配的路由，然后确定一条最佳的路径，同时还将报文按照数据链路层上使用的协议进行封装，最后进行报文转发。

快速转发是采用高速缓存来处理报文，采用了基于数据流的技术。

IPv6 快速转发根据报文中的信息（比如源 IP 地址、目的 IP 地址、源端口、目的端口、IP 协议号等）来标识一条数据流。当一条数据流的第一个报文通过查找路由表转发后，相应的转发信息将被记录到高速缓存中的快速转发表中，该数据流后续报文就可以通过直接查找快速转发表进行转发。这样便大大缩减了 IPv6 报文的排队流程，减少报文的转发时间，提高 IPv6 报文的转发效率。

## 1.2 配置IPv6快速转发表项的老化时间

### 1. 功能简介

IPv6 快速转发表中的表项并非永远有效，每一条记录都有一个生存周期，到达生存周期仍得不到刷新的记录将从 IPv6 快速转发表中删除，这个生存周期被称作老化时间。如果在到达老化时间前记录被刷新，则重新计算老化时间。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 IPv6 快速转发表项的老化时间。

```
ipv6 fast-forwarding aging-time aging-time
```

缺省情况下，IPv6 快速转发表项的老化时间为 30 秒。

## 1.3 配置IPv6快速转发负载分担

### 1. 功能简介

缺省情况下，IPv6 快速转发负载分担功能处于开启状态，IPv6 快速转发根据报文中的信息来标识一条数据流。关闭 IPv6 快速转发负载分担功能后，IPv6 快速转发根据报文中的信息和入接口来标识一条数据流。

### 2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 IPv6 快速转发负载分担功能。请选择其中一项进行配置。

- 开启 IPv6 快速转发负载分担功能。

```
ipv6 fast-forwarding load-sharing
```

- 关闭 IPv6 快速转发负载分担功能。

**undo ipv6 fast-forwarding load-sharing**

缺省情况下，IPv6 快速转发负载分担功能处于开启状态。

## 1.4 IPv6快速转发显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示 IPv6 快速转发配置后的运行情况，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 IPv6 快速转发表中的内容。

表1-1 IPv6 快速转发显示和维护

操作	命令
显示IPv6快速转发表项的老化时间	<b>display ipv6 fast-forwarding aging-time</b>
显示IPv6快速转发表信息	<b>display ipv6 fast-forwarding cache</b> <b>[ ipv6-address ] [ slot slot-number ]</b>
清除IPv6快速转发表信息	<b>reset ipv6 fast-forwarding cache [ slot</b> <b>slot-number ]</b>

# 目 录

1 HTTP重定向 .....	1-1
1.1 HTTP重定向简介 .....	1-1
1.2 HTTP重定向配置任务简介 .....	1-1
1.3 配置对HTTPS报文进行重定向的内部侦听端口号 .....	1-1
1.4 配置HTTPS重定向服务关联的SSL服务器端策略 .....	1-1

# 1 HTTP重定向

## 1.1 HTTP重定向简介

HTTP 重定向是一种将用户的 HTTP/HTTPS 请求转到某个指定 URL 的方法。目前，HTTP 重定向主要用于 802.1X/MAC 地址认证/Web 认证/端口安全的 URL 重定向功能、802.1X 的 EAD 快速部署以及 Portal 等需要对用户的 HTTP/HTTPS 请求进行重定向的业务。

## 1.2 HTTP重定向配置任务简介

对于 HTTP 请求报文无需进行任何配置，对于需要对用户 HTTPS 请求进行重定向的业务需进行以下配置：

- (1) [配置对HTTPS报文进行重定向的内部侦听端口号](#)
- (2) （可选）[配置HTTPS重定向服务关联的SSL服务器端策略](#)

## 1.3 配置对HTTPS报文进行重定向的内部侦听端口号

### 1. 功能简介

只有配置了对 HTTPS 报文进行重定向的内部侦听端口号，设备才会对 HTTPS 报文进行重定向。

### 2. 配置限制和指导

为了避免端口号冲突导致服务不可用，需确保内部侦听端口号不是知名协议使用的端口号，且不能被其它基于 TCP 协议的服务占用。已被其他服务占用的 TCP 端口号可以通过 **display tcp** 命令查看，该命令的详细介绍请参见“三层业务—IP 业务”中的“IP 性能优化”。

多次执行本命令，最后一次执行的命令生效。

### 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置对 HTTPS 报文进行重定向的内部侦听端口号。

```
http-redirect https-port port-number
```

对于 Release 6126P20 及之前版本，缺省情况下，未配置对 HTTPS 报文进行重定向的内部侦听端口号。对于 Release 6127 及以上版本，缺省情况下，对 HTTPS 报文进行重定向的内部侦听端口号为 6654。

## 1.4 配置HTTPS重定向服务关联的SSL服务器端策略

### 1. 功能简介

SSL 服务器端策略是设备作为 SSL 服务器时使用的 SSL 参数。缺省情况下，HTTPS 重定向服务使用自签名证书，SSL 参数均为缺省值。这种方式简化了配置，但是存在安全隐患。因此，可通过配



置 SSL 服务器端策略，并将其与 HTTPS 重定向服务进行关联，来增强 HTTPS 重定向服务的安全性。关于 SSL 的详细描述，请参见“安全配置指导”中的“SSL”。

## 2. 配置限制和指导

如果关联的 SSL 服务器端策略不存在，则无法完成 HTTPS 报文的重定向。允许用户先关联一个不存在的 SSL 服务器端策略，再对该策略进行相关配置。

修改 SSL 服务器端策略会立即生效。

多次执行本命令，最后一次执行的命令生效。

## 3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 指定 HTTPS 重定向服务关联的 SSL 服务器端策略。

```
http-redirect ssl-server-policy policy-name
```

缺省情况下，HTTPS 重定向服务未与 SSL 服务器端策略关联，HTTPS 重定向服务使用自签名证书。